

Screenshots

Create virtual network for East US

The screenshot shows the Azure portal interface for creating a new virtual network. The top navigation bar includes 'Microsoft Azure', 'Search resources, services, and docs (G+)', 'Copilot', and user information. A progress bar at the top right indicates 'Initializing deployment...'.

Basics

Subscription	Simplilearn HOL 100766
Resource Group	RG-EastUS-HQ
Name	Vnet-EastUS-HQ
Region	East US

Security

Azure Bastion	Enabled
- Name	(New) Vnet-EastUS-HQ-Bastion
- Public IP Address	(New) vnet-eastus-hq-bastion
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)
Subnet	AzureBastionSubnet (10.0.1.0/26) (64 addresses)

Tags

The screenshot shows the 'Virtual network' blade for 'Vnet-EastUS-HQ'. The top navigation bar includes 'Microsoft Azure', 'Search resources, services, and docs (G+)', 'Copilot', and user information. The main content area displays the virtual network's properties and capabilities.

Essentials

Resource group (move)	: RG-EastUS-HQ
Location (move)	: East US
Subscription (move)	: Simplilearn HOL 100766
Subscription ID	: 57268e08-7b81-4409-9031-ada52a50a03b
Address space	: 10.0.0.0/16
Subnets	: 2 subnets
DNS servers	: Azure provided DNS service
BGP community string	: Configure
Virtual network ID	: 60640750-f634-441f-89b8-74fc28975eb

Capabilities (5)

- DDoS protection**: Configure additional protection from distributed denial of service attacks.
Status: Not configured
- Azure Firewall**: Protect your network with a stateful L3-L7 firewall.
Status: Not configured
- Peergings**: Seamlessly connect two or more virtual networks.
Status: Not configured
- Microsoft Defender for Cloud**: Strengthen the security posture of your environment.
- Private endpoints**: Privately access Azure services without sending traffic across internet.
Status: Not configured

Vnet-EastUS-HQ | Subnets

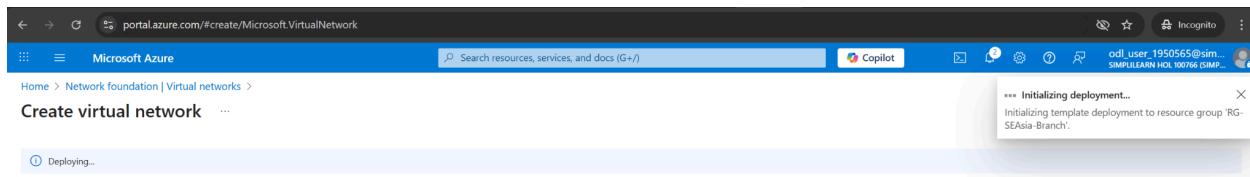
Virtual network

Search subnets

Name	IPv4	IPv6	Available IPs	Delegated to	Security group	Route table
default	10.0.0.0/24	-	251	-	-	-
AzureBastionSubnet	10.0.1.0/26	-	57	-	-	-

Bastian subnet for accessing the VM via bastian box as they will having only private ip's

Create virtual network for South east asia



portal.azure.com/#@simplilearnhol100766.onmicrosoft.com/resource/subscriptions/57268e08-7b81-4409-9031-ada52a50a03b/resourceGroups/RG-SEAsia-Branch/providers/Microsoft.Network/virtualNetworks/Vnet-SEEastAsia-Branch

Microsoft Azure

Home > Vnet-SEEastAsia-Branch Virtual network

Search Move Delete Refresh Give feedback

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Resource visualizer Settings Monitoring Automation Help

What is Azure Firewall Premium SKU Analyze resources connected to this virtual network Analyze traffic within this network

Essentials

Resource group (move) : RG-SEAsia-Branch	Address space : 192.168.0.0/16
Location (move) : Southeast Asia	Subnets : 1 subnet
Subscription (move) : Simplilearn HOL 100766	DNS servers : Azure provided DNS service
Subscription ID : 57268e08-7b81-4409-9031-ada52a50a03b	BGP community string : Configure
	Virtual network ID : 4b9a5d1a-749b-43d2-85bd-f2b88e24c8ac

Tags (edit) : Add tags

Topology Properties Capabilities (5) Recommendations Tutorials

DDoS protection Configure additional protection from distributed denial of service attacks. Not configured

Azure Firewall Protect your network with a stateful L3-L7 firewall. Not configured

Peering Seamlessly connect two or more virtual networks. Not configured

Microsoft Defender for Cloud Strengthen the security posture of your environment.

Private endpoints Privately access Azure services without sending traffic across internet. Not configured

Vnet-SEAsia-Branch | Subnets

Name	IPv4	IPv6	Available IPs	Delegated to	Security group	Route table
default	192.168.0.0/24	-	251	-	-	-

2 Virtual networks are created for respective regions

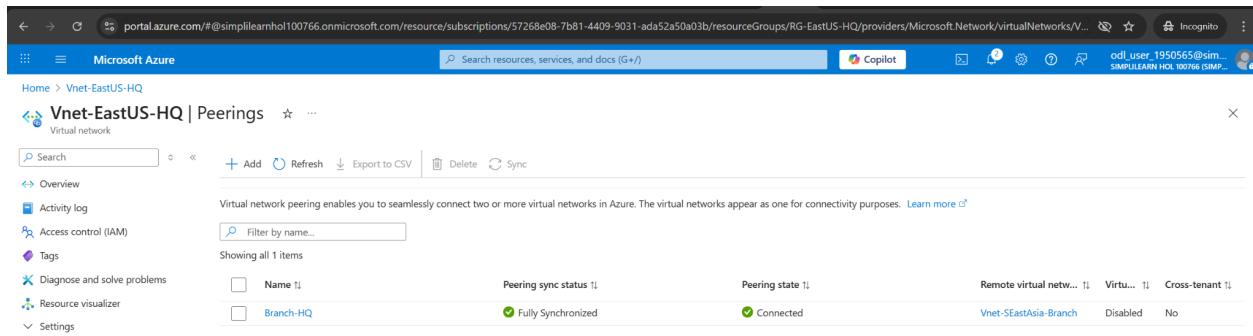
Network foundation | Virtual networks

Name	Resource Group	Location	Subscription
Vnet-EastUS-HQ	RG-EastUS-HQ	East US	Simplilearn HOL 100766
Vnet-SEAsia-Branch	RG-SEAsia-Branch	Southeast Asia	Simplilearn HOL 100766

Vnet peering is the next step
 Open the left hand side blade for the East US and click on peering

Add a peering to link south east asia branch

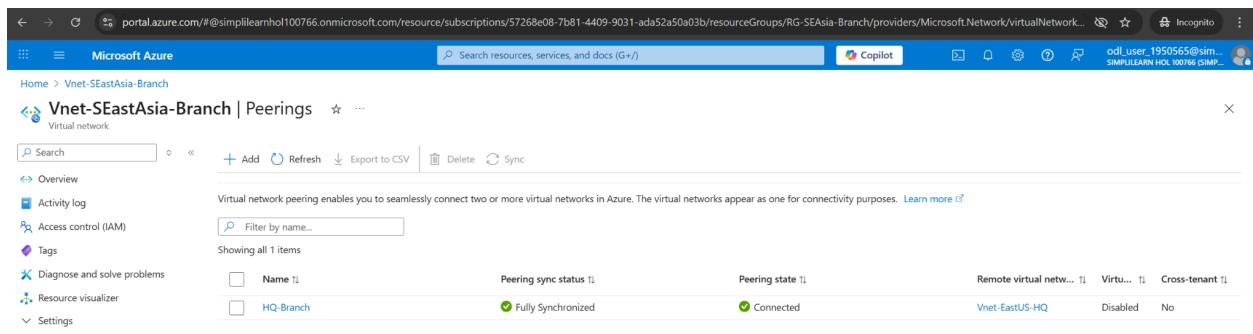
Peering is added successfully from HQ to Branch



The screenshot shows the Azure portal interface for managing virtual network peerings. The URL is <https://portal.azure.com/#@simplelearnhol100766.onmicrosoft.com/resource/subscriptions/57268e08-7b81-4409-9031-ada52a50a03b/resourceGroups/RG-EastUS-HQ/providers/Microsoft.Network/virtualNetworks/Vnet-EastUS-HQ/peering>. The page title is "Vnet-EastUS-HQ | Peerings". The left sidebar includes links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, and Settings. The main content area displays a table with one item:

Name	Peering sync status	Peering state	Remote virtual network	Virt...	Cross-tenant
Branch-HQ	Fully Synchronized	Connected	Vnet-SEastAsia-Branch	Disabled	No

Reverse peer from Branch to HQ is also created



The screenshot shows the Azure portal interface for managing virtual network peerings. The URL is <https://portal.azure.com/#@simplelearnhol100766.onmicrosoft.com/resource/subscriptions/57268e08-7b81-4409-9031-ada52a50a03b/resourceGroups/RG-SEAsia-Branch/providers/Microsoft.Network/virtualNetworks/Vnet-SEastAsia-Branch/peering>. The page title is "Vnet-SEastAsia-Branch | Peerings". The left sidebar includes links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, and Settings. The main content area displays a table with one item:

Name	Peering sync status	Peering state	Remote virtual network	Virt...	Cross-tenant
HQ-Branch	Fully Synchronized	Connected	Vnet-EastUS-HQ	Disabled	No

Both the virtual networks are not peered successfully. Next step is VM creation with no public ip's

Creation of HQ - VM

Basics

Subscription	Simplilearn HOL 100766
Resource group	RG-EastUS-HQ
Virtual machine name	VM-EastUS-HQ
Region	East US
Availability options	No infrastructure redundancy required
Zone options	Self-selected zone
Security type	Trusted launch virtual machines
Enable secure boot	Yes
Enable vTPM	Yes
Integrity monitoring	No
Image	Windows Server 2025 Datacenter - Gen2
VM architecture	x64
Size	Standard DS1 v2 (1 vcpu, 3.5 GiB memory)
Enable Hibernation	No
Username	vm-eastus

Networking

Virtual network	Vnet-EastUS-HQ
Subnet	default
Public IP	None
Accelerated networking	On
Place this virtual machine behind an existing load balancing solution?	No
Delete 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

Deployment is successful . Note down the private ip - 10.0.0.4

The screenshot shows the Azure portal interface for managing a virtual machine named 'VM-EastUS-HQ'. The left sidebar navigation bar is visible, with 'Network settings' selected under the 'Networking' section. The main content area displays the network configuration for the primary interface, 'vm-eastus-hq971 (primary) / ipconfig1 (primary)'. The 'Essentials' section shows the following details:

Setting	Value
Network interface	: vm-eastus-hq971
Virtual network / subnet	: Vnet-EastUS-HQ / default
Public IP address	: - (Configure)
Private IP address	: 10.0.0.4
Admin security rule	: 0 (Configure)
Load balancers	: 0 (Configure)
Application security groups	: 0 (Configure)
Network security group	: VM-EastUS-HQ-nsg
Accelerated networking	: Enabled
Effective security rules	: 0

Below this, the 'Rules' section is expanded, showing a table of network security rules. It includes a header row and three data rows:

Priority ↑	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Creation of branch - VM

portal.azure.com/#create/Microsoft.VirtualMachine-ARM Microsoft Azure Search resources, services, and docs (G+) Copilot odl_user_1950565@sim... SIMPLETEARN HOL 100766 (SIMP...) Incognito

Home > Compute infrastructure | Virtual machines > Create a virtual machine ... Help me create a VM optimized for high availability Help me choose the right VM size for my workload Help me create a low cost VM

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

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), if any, 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 [Azure Marketplace Terms](#) for additional details.

Basics

Subscription	Simpilearn HOL 100766
Resource group	RG-SEAasia-Branch
Virtual machine name	VM-SEAasia-Branch
Region	Southeast Asia
Availability options	No infrastructure redundancy required
Zone options	Self-selected zone
Security type	Trusted launch virtual machines
Enable secure boot	Yes
Enable vTPM	Yes
Integrity monitoring	No
Image	Windows Server 2025 Datacenter - Gen2
VM architecture	x64
Size	Standard DS1 v2 (1 vcpu, 3.5 GiB memory)
Enable Hibernation	No
Username	Vm-eastus
Public inbound ports	None
Already have a Windows license?	No
Azure Spot	No

< Previous Next > Create Download a template for automation Give feedback

portal.azure.com/#create/Microsoft.VirtualMachine-ARM Microsoft Azure Search resources, services, and docs (G+) Copilot odl_user_1950565@sim... SIMPLETEARN HOL 100766 (SIMP...) Incognito

Home > Compute infrastructure | Virtual machines > Create a virtual machine ... Help me create a VM optimized for high availability Help me choose the right VM size for my workload Help me create a low cost VM

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

Disk

OS disk size	Image default
OS disk type	Standard HDD LRS
Use managed disks	Yes
Delete OS disk with VM	Enabled
Ephemeral OS disk	No

Networking

Virtual network	Vnet-SEAsia-Branch
Subnet	default
Public IP	None
Accelerated networking	On
Place this virtual machine behind an existing load balancing solution?	No
Delete NIC when VM is deleted	Disabled

Management

Microsoft Defender for Cloud	None
System assigned managed identity	Off
Login with Microsoft Entra ID	Off
Auto-shutdown	Off
Enable periodic assessment	Off
Enable hotpatch	Off
Patch orchestration options	OS-orchestrated patching: patches will be installed by OS

Monitoring

Alerts	Off
Boot diagnostics	On

< Previous Next > Create Download a template for automation Give feedback

Deployment is successful . Note down the private ip 192.168.0.4

The screenshot shows the Azure portal interface for managing a virtual machine named 'VM-SEAsia-Branch'. The left sidebar navigation bar is visible, showing various options like 'Search', 'Tags', 'Diagnose and solve problems', 'Resource visualizer', 'Connect', 'Bastion', 'Windows Admin Center', 'Networking', 'Network settings' (which is selected), 'Load balancing', 'Application security groups', and 'Network manager'. The main content area displays the 'Network settings' for the VM. It shows the network interface configuration for 'vm-seasia-branch494 (primary) / ipconfig (primary)'. Key details include:

Setting	Value
Network interface	vm-seasia-branch494
Virtual network / subnet	Vnet-SEAsia-Branch / default
Public IP address	- (Configure)
Private IP address	192.168.0.4
Admin security rules	0 (Configure)
Load balancers	0 (Configure)
Application security groups	0 (Configure)
Network security group	VM-SEAsia-Branch-nsg
Accelerated networking	Enabled
Effective security rules	0

Below this, the 'Rules' section shows the Network security group configuration. It lists three inbound port rules and three outbound port rules. The inbound rules allow traffic from the Virtual Network to the VM on ports 65000, 65001, and 65500. The outbound rules deny all traffic from the VM.

Both VM's are now created

The screenshot shows the Azure portal interface for managing virtual machines. The left sidebar navigation bar is visible, showing 'Overview', 'All resources', 'Infrastructure', and 'Virtual machines' (which is selected). The main content area displays a list of virtual machines. The table shows two entries:

Name	Subscription	Resource Group	Location	Status	Operating syst...	Size	Public IP addre...	Disks	Update status
VM-EastUS-HQ	Simplilearn HO...	RG-EastUS-HQ	East US	Running	Windows	Standard_DS1_v2	-	1	Enable periodic...
VM-SEAsia-Branch	Simplilearn HO...	RG-SEAsia-Bran...	Southeast Asia	Running	Windows	Standard_DS1_v2	-	1	Enable periodic...

Set the NSG rule in HQ-VM for ICMP

Go to Networking -> Network settings and go to create inbound port rule

VM-EastUS-HQ | Network settings

Network interface / IP configuration
vm-eastus-hq971 (primary) / ipconfig1 (primary)

Essentials

Network interface	: vm-eastus-hq971	Load balancers	: 0 (Configure)
Virtual network / subnet	: Vnet-EastUS-HQ / default	Application security groups	: 0 (Configure)
Public IP address	: - (Configure)	Network security group	: VM-EastUS-HQ-nsg
Private IP address	: 10.0.0.4	Accelerated networking	: Enabled
Admin security rules	: 0 (Configure)	Effective security rules	: 0

Rules

Network security group VM-EastUS-HQ-nsg (attached to networkInterface: vm-eastus-hq971)
Impacts 0 subnets, 1 network interfaces

Priority ↑	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

+ Create port rule

Inbound port rule

Outbound port rule

ICMP (to enable pinging)

Network security group VM-EastUS-HQ-nsg (attached to networkInterface: vm-eastus-hq971)
Impacts 0 subnets, 1 network interfaces

Priority ↑	Name	Port	Protocol	Source	Destination	Action
100	Allow-ICMP-From-Branch	Any	ICMP	192.168.0.0/24	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

+ Create port rule

Set the NSG rule in Branch-VM for ICMP and to allow RDP from HQ to Branch

The screenshot shows the Azure portal interface for managing network settings of a virtual machine. The left sidebar navigation includes options like Tags, Diagnose and solve problems, Resource visualizer, Connect, Bastion, Windows Admin Center, Networking, Network settings (which is selected), Load balancing, Application security groups, Network manager, Settings, Availability + scale, Security, Backup + disaster recovery, Operations, Monitoring, Automation, Help, Resource health, Boot diagnostics, Serial console, and Reset password.

The main content area displays the 'Network interface / IP configuration' for 'vm-seasia-branch494 (primary) / ipconfig1 (primary)'. Under the 'Essentials' tab, details such as Network interface (vm-seasia-branch494), Virtual network / subnet (Vnet-EastAsia-Branch / default), Public IP address (- Configure), Private IP address (192.168.0.4), and Admin security rules (0 Configure) are listed. The 'Load balancers' and 'Application security groups' sections show 0 configured items each. The 'Network security group' section indicates 'VM-SEAsia-Branch-nsg' is attached to the interface, impacting 0 subnets and 1 network interface. It lists two inbound port rules:

Priority	Name	Port	Protocol	Source	Destination	Action
100	Allow-RDP-From-HQ	3389	TCP	10.0.0.0/24	Any	Allow
200	Allow-ICMP-From-HQ	Any	ICMP	10.0.0.0/24	Any	Allow

There are also sections for Outbound port rules (3) and a summary of 5 total rules.

Login to HQ VM Bastion

The screenshot shows the Azure portal interface for connecting to a virtual machine via Bastion. The left sidebar is collapsed, and the main content area displays the following information:

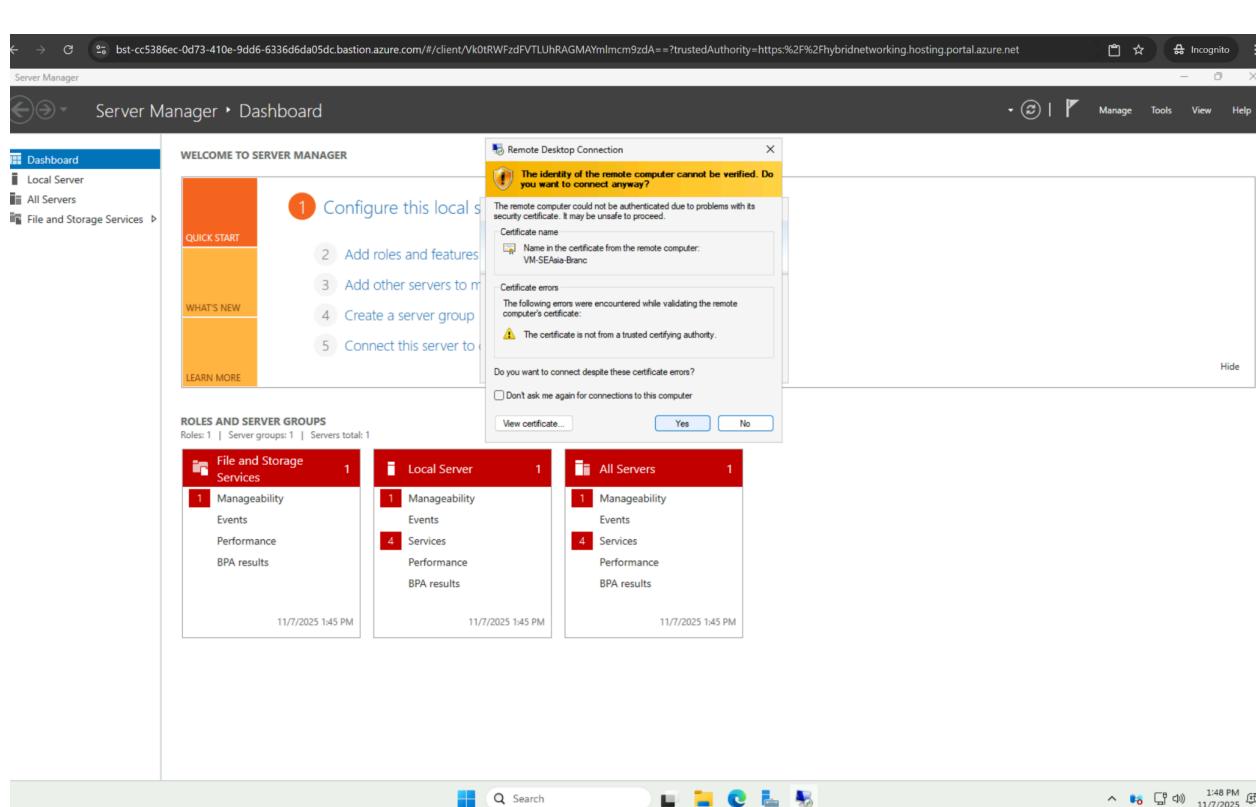
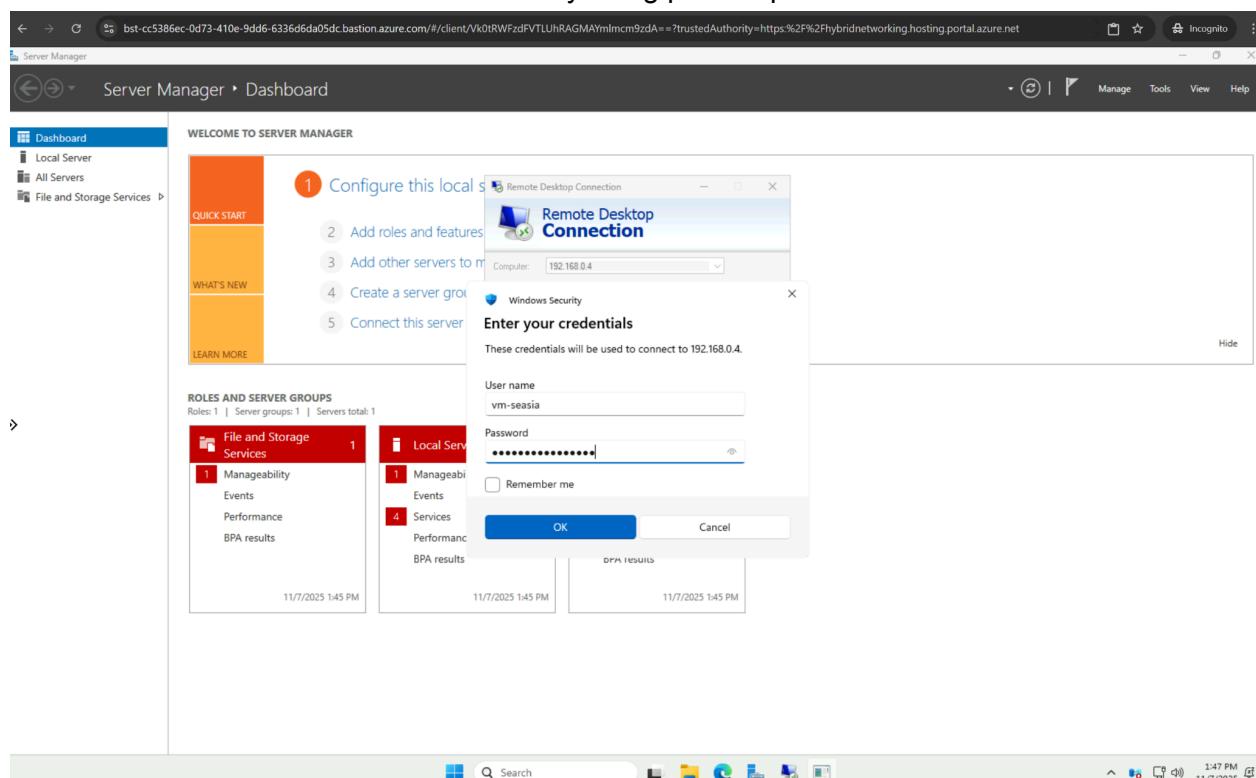
- Bastion** is selected in the navigation menu.
- Using Bastion: Vnet-EastUS-HQ-Bastion**
- Provisioning State: Succeeded**
- Azure Bastion protects your virtual machines by secure and seamless RDP & SSH connectivity without the need to expose them through public IP addresses. [Learn more](#)**
- Connection Settings**:
 - Keyboard Language: English (US)
 - Authentication Type: VM Password
 - Username: Vm-eastus
 - VM Password: [REDACTED]
- Connect** button

Bastion Login

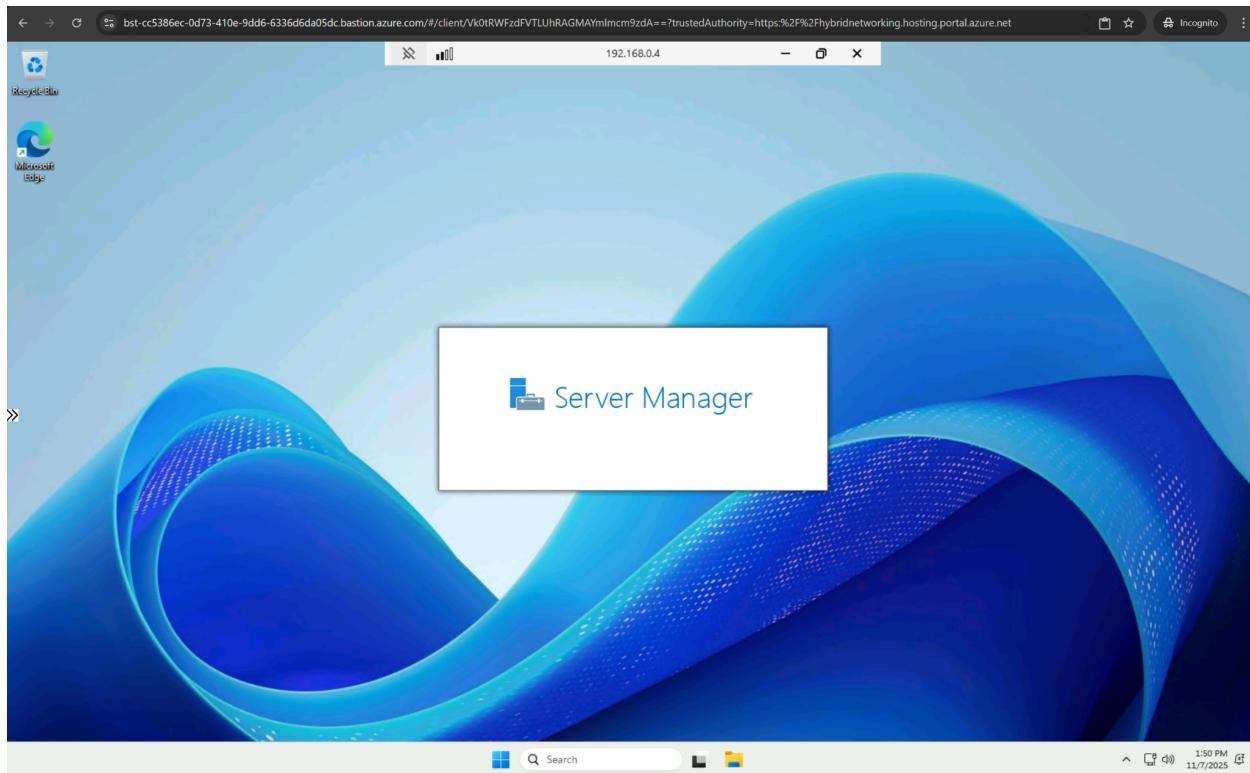
The screenshot shows the Server Manager Dashboard. The left sidebar is collapsed, and the main content area displays the following information:

- WELCOME TO SERVER MANAGER**
- Configure this local server** (Step 1 of 5):
 - 2 Add roles and features
 - 3 Add other servers to manage
 - 4 Create a server group
 - 5 Connect this server to cloud
- QUICK START** (orange box)
- WHAT'S NEW** (orange box)
- LEARN MORE** (orange box)
- ROLES AND SERVER GROUPS**: Roles: 0 | Server groups: 1 | Servers total: 1
 - Local Server** (1): Manageability, Events, Services, Performance, BPA results
 - All Servers**: Manageability, Events, Services, Performance, BPA results

RDP from HQ bastion to Branch machine by using private ip of the branch



Connection established . Peering has worked successfully as HQ is now able to connect to branch where both are in different virtual machines



Run the command for windowsfirewall in HQ

```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
PS C:\Users\vm-eastus> netsh advfirewall firewall add rule name="Allow ICMPv4" protocol=icmpv4:any,any dir=in action=allow
Ok.

PS C:\Users\vm-eastus>
```

The screenshot shows a Server Manager dashboard with a "Dashboard" tile selected. A PowerShell window is open in the center of the dashboard, showing the same command and its execution results:

```
Administrator: Windows PowerShell
PS C:\Windows\system32> netsh advfirewall firewall add rule name="Allow ICMPv4" protocol=icmpv4:any,any dir=in action=allow
Ok.

PS C:\Windows\system32>
```

Ping from HQ to the private ip of Branch(192.168.0.4) is successful

Administrator: Windows PowerShell ISE

```
PS C:\Users\vm-eastus> netsh advfirewall firewall add rule name="Allow ICMPv4" protocol=icmpv4:any,any dir=in action=allow
OK.

PS C:\Users\vm-eastus> ping 192.168.0.4
Pinging 192.168.0.4 with 32 bytes of data:
Reply from 192.168.0.4: bytes=32 time=218ms TTL=128
Reply from 192.168.0.4: bytes=32 time=217ms TTL=128
Reply from 192.168.0.4: bytes=32 time=217ms TTL=128
Reply from 192.168.0.4: bytes=32 time=217ms TTL=128

Ping statistics for 192.168.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 217ms, Maximum = 218ms, Average = 217ms

PS C:\Users\vm-eastus>
```

Commands X

Modules: All

Name:

- Add-AppProvisionedSharedPackageContainer
- Add-AppSharedPackageContainer
- Add-AppClientConnectionGroup
- Add-AppClientPackage
- Add-AppPublishingServer
- Add-AppReplica
- Add-AppProvisionedPackage
- Add-AppVolume
- Add-BCDDataCacheExtension
- Add-BitLockerKeyProtector
- Add-BitFile
- Add-CertificateEnrollmentPolicyServer
- Add-ClusterSCSITargetServerRole
- Add-Computer
- Add-Computer
- Add-DnsClientDnsServerAddress
- Add-DnsClientNtpRule
- Add-DtcClusterTMMapping
- Add-EtwTraceProvider
- Add-History
- Add-IniatorIdToMaskingSet
- Add-IscsiVirtualDiskTargetMapping
- Add-JobTrigger
- Add-KdsRootKey
- Add-LocalGroupMember
- Add-Member
- Add-MpPreference
- Add-MpPreference

Run Insert Copy

Ln 18 Col 24 100% 2:01 PM 11/7/2025

Ping from Branch to the private ip of HQ(10.0.0.4) is successful

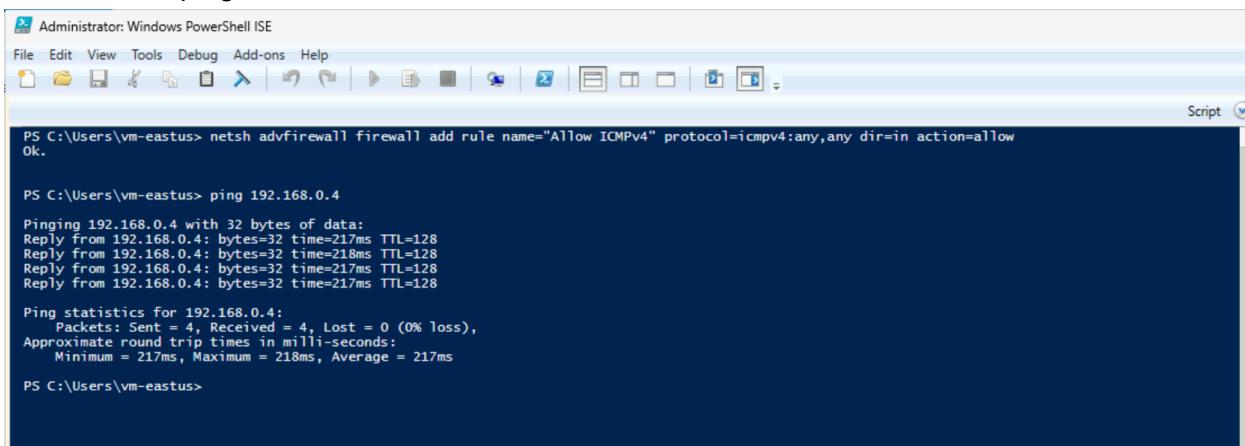
Administrator: Windows PowerShell

```
PS C:\Windows\system32> netsh advfirewall firewall add rule name="Allow ICMPv4" protocol=icmpv4:any,any dir=in action=allow
low

PS C:\Windows\system32> ping 10.0.0.4
Pinging 10.0.0.4 with 32 bytes of data:
Reply from 10.0.0.4: bytes=32 time=217ms TTL=128

Ping statistics for 10.0.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 217ms, Maximum = 217ms, Average = 217ms
PS C:\Windows\system32>
```

HQ-> Branch ping



A screenshot of the Windows PowerShell ISE interface. The title bar says "Administrator: Windows PowerShell ISE". The menu bar includes File, Edit, View, Tools, Debug, Add-ons, Help. The toolbar has icons for file operations like Open, Save, Copy, Paste, and Run. The main pane shows a command-line session:

```
PS C:\Users\vm-eastus> netsh advfirewall firewall add rule name="Allow ICMPv4" protocol=icmpv4:any,any dir=in action=allow
Ok.

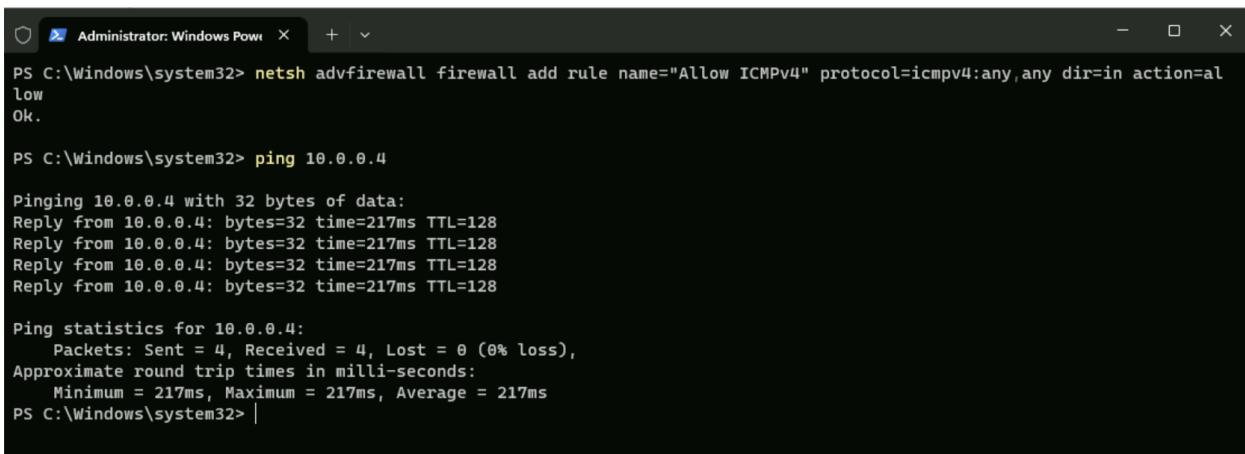
PS C:\Users\vm-eastus> ping 192.168.0.4

Pinging 192.168.0.4 with 32 bytes of data:
Reply from 192.168.0.4: bytes=32 time=217ms TTL=128
Reply from 192.168.0.4: bytes=32 time=218ms TTL=128
Reply from 192.168.0.4: bytes=32 time=217ms TTL=128
Reply from 192.168.0.4: bytes=32 time=217ms TTL=128

Ping statistics for 192.168.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 217ms, Maximum = 218ms, Average = 217ms

PS C:\Users\vm-eastus>
```

Branch-> HQ ping



A screenshot of the Windows PowerShell ISE interface. The title bar says "Administrator: Windows PowerShell ISE". The menu bar includes File, Edit, View, Tools, Debug, Add-ons, Help. The toolbar has icons for file operations like Open, Save, Copy, Paste, and Run. The main pane shows a command-line session:

```
PS C:\Windows\system32> netsh advfirewall firewall add rule name="Allow ICMPv4" protocol=icmpv4:any,any dir=in action=allow
Ok.

PS C:\Windows\system32> ping 10.0.0.4

Pinging 10.0.0.4 with 32 bytes of data:
Reply from 10.0.0.4: bytes=32 time=217ms TTL=128

Ping statistics for 10.0.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 217ms, Maximum = 217ms, Average = 217ms

PS C:\Windows\system32> |
```

End Note -

- VNet-EastUS-HQ ↔ VNet-SEAsia-Branch peering works both ways
- NSG rules allow ICMP between the two VMs
- Windows Firewall ICMP rules applied successfully
- Private-to-private communication over Azure backbone verified
- Topology meets the business requirement (private channel only)