

Sample Project - Techspire



Enterprise-Grade Azure VNet Integration with Custom Roles Project Summary:

This project focuses on establishing secure and efficient connectivity between internet-facing workloads using Azure Virtual Network (VNet) Peering. Additionally, it involves the implementation of a custom Azure role to manage access and operations for these workloads, ensuring adherence to the principle of least privilege while maintaining operational efficiency.

Techspire Vnet-01

Steps to be followed:

1. Creating Test Virtual Machines and Virtual Networks
2. Establishing Vnet Peering
3. Testing connectivity
4. Creating a custom RBAC Role
5. Adding a user to the Directory and Assign the custom RBAC Role

Step 1: Creating Test Virtual Machines and Virtual Networks

1.1 Sign in to the Azure portal

1.2 Create a virtual network **vnet1** with an IP address space of 10.0.0.0/16. Then, add a subnet (**subnet1**) with a subnet address range of 10.0.0.0/24

Techspire Resource group

Search Overview + Create Manage view Delete resource group Refresh Export to CSV ...

Essentials

Resources Recommendations

Filter for any field... Type equals all Add filter More (1)

Showing 0 to 0 of 0 records. Show hidden types No grouping

List view Name ↑ Type ↑ Location ↑

Activity log Access control (IAM) Tags Resource visualizer Events Settings Cost Management Monitoring Automation Help

Techspire subnet-01

TechSpire-Vnet01 | Subnets Virtual network

Search Overview + Subnet Refresh Manage users Delete

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.

Search subnets

Name ↑	IPv4	IPv6	Available IPs	Delegated to	Security group	Route table
Techspire-Subnet01	10.0.0.0/24	-	251	-	-	-

Techspire Vm-01

Create a virtual machine (**vm1**) in **vnet1** virtual network

Properties	Value
Image	Windows Server 2019 Datacenter - Gen2
Vm Name	vm1
Region	East US
Username	Techspire01
Password	Password01
Size	Ds1V2

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 *

TechSpire-Vnet01

[Create new](#)

Subnet *

Techspire-Subnet01 (10.0.0.0/24)

[Manage subnet configuration](#)

[< Previous](#)

[Next : Management >](#)

Review + create

Basics Disks Networking **Management** Monitoring Advanced Tags Review + create

Price

1 X Standard B1s

by Microsoft

[Terms of use](#) | [Privacy policy](#)

Subscription credits apply

0.0140 USD/hr

[Pricing for other VM sizes](#)

TERMS

[< Previous](#)

[Next >](#)

Create

[Download a template for automation](#)

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 Techspire

Virtual machine name Techspire-VM01

Region East US

Availability options Availability zone

Zone options Self-selected zone

Availability zone 2

Security type Trusted launch virtual machines

[< Previous](#)

[Next >](#)

Create

[Download a template for automation](#)

Give feedback

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](#)

Availability zone	2
Security type	Trusted launch virtual machines
Enable secure boot	Yes
Enable vTPM	Yes
Integrity monitoring	No
Image	Windows Server 2019 Datacenter - Gen2
VM architecture	x64
Size	Standard B1s (1 vcpu, 1 GiB memory)
Enable Hibernation	No
Username	techspire
Public inbound ports	RDP

< Previous Next > **Create**

[Download a template for automation](#) [Give feedback](#)

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](#)

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

< Previous Next > **Create**

[Download a template for automation](#) [Give feedback](#)

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	TechSpire-Vnet01
Subnet	Techspire-Subnet01 (10.0.0.0/24)
Public IP	(new) Techspire-VM01-ip
Accelerated networking	Off
Place this virtual machine behind an existing load balancing solution?	No
Delete public IP and NIC when VM is deleted	Enabled

< Previous Next > **Create**

[Download a template for automation](#) [Give feedback](#)

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 periodic assessment Off

Enable hotpatch Off

Patch orchestration options OS-orchestrated patching: patches will be installed by OS

Monitoring

Alerts Off

Boot diagnostics On

Enable OS guest diagnostics Off

Enable application health monitoring Off

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

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 application health monitoring Off

Advanced

Extensions None

VM applications None

Cloud init No

User data No

Disk controller type SCSI

Proximity placement group None

Capacity reservation group None

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

Home >

Techspire Resource group

Search Create Manage view Delete resource group Refresh Export to CSV Open query Assign tags Move ...

Overview

Showing 1 to 8 of 8 records. Show hidden types

Name	Type	Location
Techspire-VM01-nsg	Network security group	East US
TechSpire-Vnet01	Virtual network	East US
TechSpire-Vnet02	Virtual network	East US
TechspireVM	Virtual machine	East US
TechspireVM-ip	Public IP address	East US
TechspireVM-nsg	Network security group	East US
techspirevm229_z2	Network Interface	East US

< Previous Page 1 of 1 Next > Give feedback

Techspire Vnet-02

Create a virtual network vnet2 with an IP address space of 10.1.0.0/16. Next, add a subnet (subnet2) with a subnet address range of 10.1.0.0/24

TechSpire-Vnet01 Virtual network

Search

Move Delete Refresh Give feedback

JSON View

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

Address space

Connected devices

Subnets

Bastion

Essentials

Resource group ([move](#))
Techspire

Location ([move](#))
East US

Subscription ([move](#))
Azure subscription 1

Subscription ID
4a8937a7-b294-4a1f-8d31-79bbb1a4c17f

Tags ([edit](#))
[Add tags](#)

Address space
10.0.0.0/16

DNS servers
Azure provided DNS service

BGP community string
[Configure](#)

Virtual network ID
f57b0b06-c83d-4d8f-ba0a-88338411636f

Validation passed

Basics Security IP addresses Tags [Review + create](#)

[View automation template](#)

Basics

Subscription	Azure subscription 1
Resource Group	Techspire
Name	TechsSpire-Vnet02
Region	East US

Security

Validation passed

Basics Security IP addresses Tags [Review + create](#)

Azure Bastion
Disabled

Azure Firewall
Disabled

Azure DDoS Network Protection
Disabled

IP addresses

Address space
10.1.0.0/16 (65,536 addresses)

Techspire Subnet-02

TechSpire-Vnet02 | Subnets

Virtual network

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Resource visualizer Settings Address space Connected devices Subnets

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.

Name ↑	IPv4	IPv6	Available IPs	Delegated to	Security group	Route table
TechSpire-...	10.1.0.0/24	-	251	-	-	-

Techspire Vm-02

Create a virtual machine (**Techspirevm1**) in **vnet1** virtual network

Properties	Value
Image	Windows Server 2019 Datacenter - Gen2
Vm Name	vm1
Region	East US
Username	Techspire02
Password	Password02
Size	Ds1V2

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

You have selected ports open to the internet. This is only recommended for testing. If you want to change this setting, go back to Basics tab.

Basics

Subscription	Azure subscription 1
Resource group	Techspire
Virtual machine name	Techspirevm02
Region	East US
Availability options	Availability zone
Zone options	Self-selected zone
Availability zones	2

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

Create a virtual machine

X

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](#)

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 Server 2019 Datacenter - Gen2
VM architecture	x64
Size	Standard B1s (1 vcpu, 1 GiB memory)
Enable Hibernation	No

< Previous Next > **Create**

[Download a template for automation](#) [Give feedback](#)

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](#)

Already have a Windows license?	No
Azure Spot	No

Disk

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

< Previous Next > **Create**

[Download a template for automation](#) [Give feedback](#)

Create a virtual machine

X

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	TechSpire-Vnet02
Subnet	TechSpire-Subnet02 (10.1.0.0/24)
Public IP	(new) Techspirevm02-ip
Accelerated networking	Off
Place this virtual machine behind an existing load balancing solution?	No
Delete public IP and NIC when VM is deleted	Enabled

Management

< Previous Next > **Create**

[Download a template for automation](#) [Give feedback](#)

Create a virtual machine ... X

✓ 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
Enable periodic assessment	Off
Enable hotpatch	Off
Patch orchestration options	OS-orchestrated patching: patches will be installed by OS

[< Previous](#) [Next >](#) [Create](#)

[Download a template for automation](#)

✓ 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 application health monitoring

Advanced

Extensions	None
VM applications	None
Cloud init	No
User data	No
Disk controller type	SCSI
Proximity placement group	None
Capacity reservation group	None

[< Previous](#) [Next >](#) [Create](#)

[Download a template for automation](#)

Manage view Refresh Export to CSV Clear | Assign tags

Group by none

Filter for any field... Subscription equals all Resource Group equals all Type equals all Location equals all + Add filter

<input type="checkbox"/> Name	Type	Location	Resource Group	Subscription	Last accessed
<input type="checkbox"/> Techspirevm02	... Virtual machine		Techspire	Azure subscription 1	30 seconds ago
<input type="checkbox"/> Techspire	... Resource group		Techspire	Azure subscription 1	33 seconds ago
<input type="checkbox"/> TechSpire-Vnet01	... Virtual network	East US	Techspire	Azure subscription 1	18 minutes ago
<input type="checkbox"/> TechspireVM	... Virtual machine	East US	Techspire	Azure subscription 1	36 minutes ago
<input type="checkbox"/> TechSpire-Vnet02	... Virtual network	East US	Techspire	Azure subscription 1	1 hour ago

Step 2: Establishing Vnet peering

- 2.1 Locate the **Techspire vnet1** virtual network
- 2.2 Select **Peering**. Then, add a **peering connection**

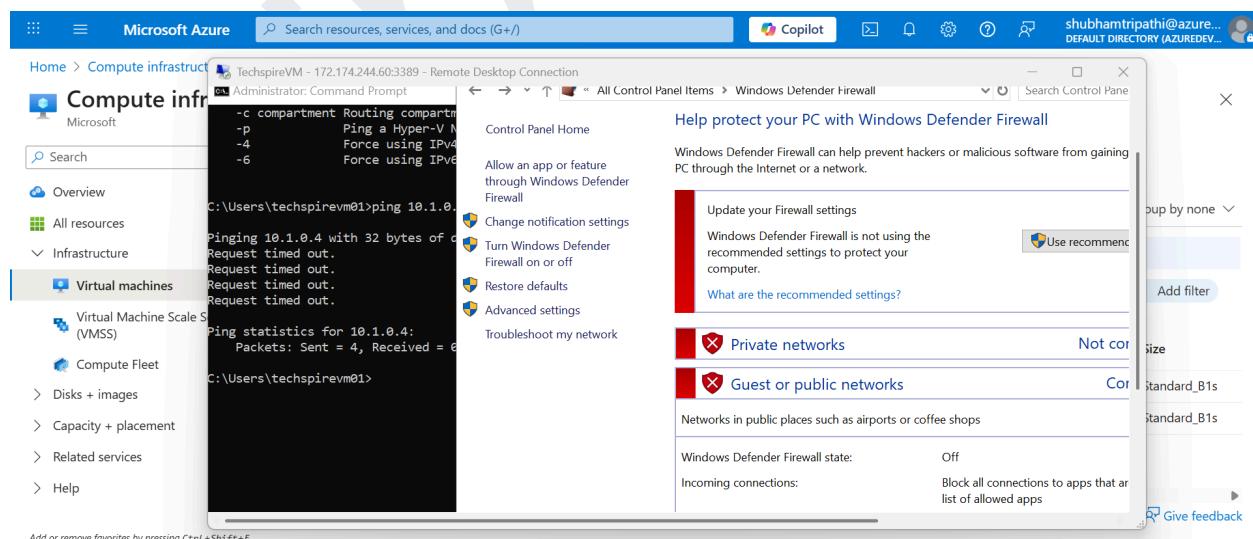
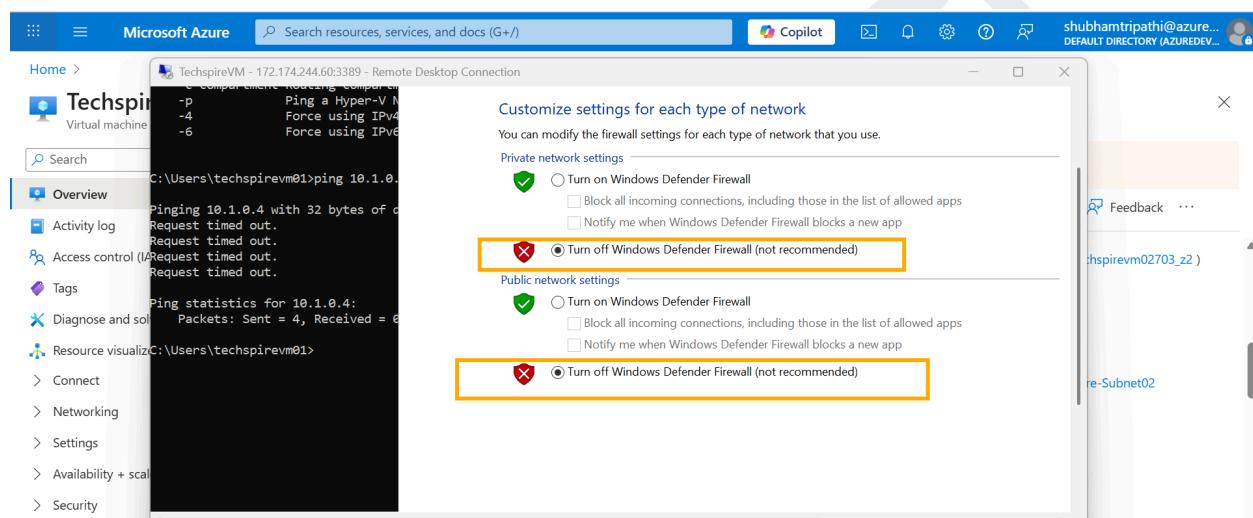
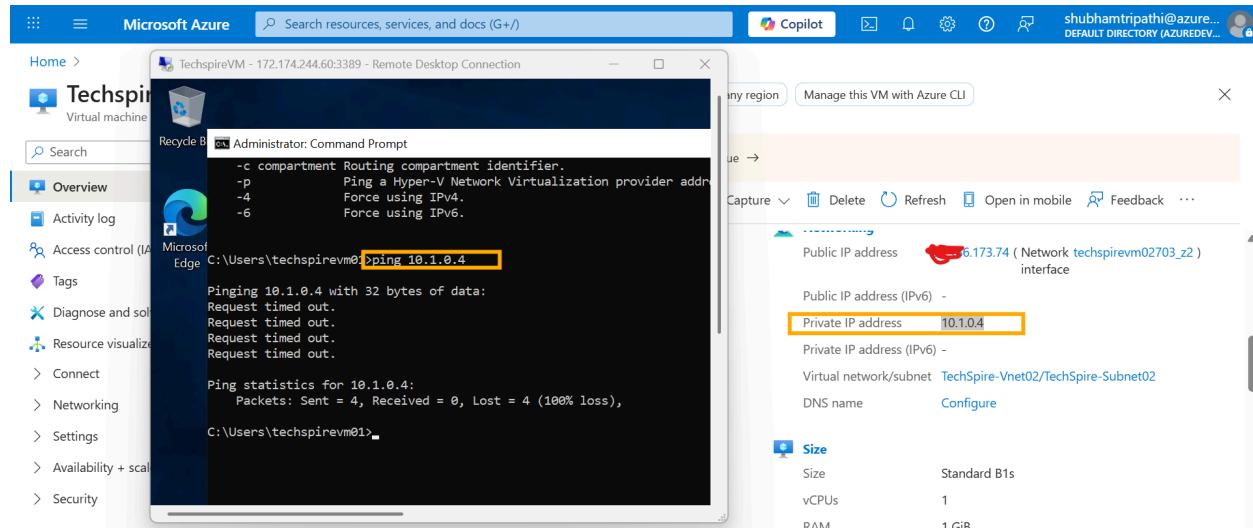
Properties	Value
Peering link name	vnet1toVnet2
Traffic to remote virtual network	Allow
Traffic forwarded from remote virtual network	Allow

Virtual network gateway or Route Server	None
Remote virtual network peering link name	vnet2tovnet1
Virtual network deployment model	Techspire
Subscription	#####
Virtual network	Vnet2

TechspireVM01

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu includes Home, Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Connect, Networking, Settings, Availability + scale, and Security. The main content area displays the 'TechspireVM' virtual machine details. A preview window shows a Windows desktop with a Microsoft Edge browser open. To the right, a 'Notifications' panel shows a single event: 'Started virtual machine' with a timestamp of '2 minutes ago'. The status bar at the bottom indicates the user's email as 'shubhamtripathi@azur...'.

This screenshot is identical to the one above, showing the Microsoft Azure portal interface for the 'TechspireVM01' virtual machine. It displays the same navigation menu, preview window of the VM desktop, and 'Notifications' panel with the 'Started virtual machine' event. The status bar at the bottom also shows the user's email as 'shubhamtripathi@azur...'.



TechspireVM02

Microsoft Azure Search resources, services, and docs (G+/)

Techspirevm02 Virtual machine

Home >

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Resource visualizer > Connect > Networking > Settings > Availability + scale > Security

Add or remove favorites by pressing **Ctrl+Shift+F**

Microsoft Azure Search resources, services, and docs (G+/)

Copilot

shubhamtripathi@azur... DEFAULT DIRECTORY (AZUREDEV...)

Notifications More events in the activity log → Dismiss all

Started virtual machine Successfully started virtual machine 'Techspirevm02'. 2 minutes ago

Started virtual machine Successfully started virtual machine 'Techspirevm02'. 3 minutes ago

Server Manager Dashboard WELCOME TO SERVER MANAGER

Local Server All Servers File and Storage Services > QUICK START Config Add

Azure subscription 1 TechSpire-Vnet02/TechSpire-Subnet02

Subscription ID 4a8937a7-b294-4a1f-8d31-79bbb1a4c17f DNS name Not configured

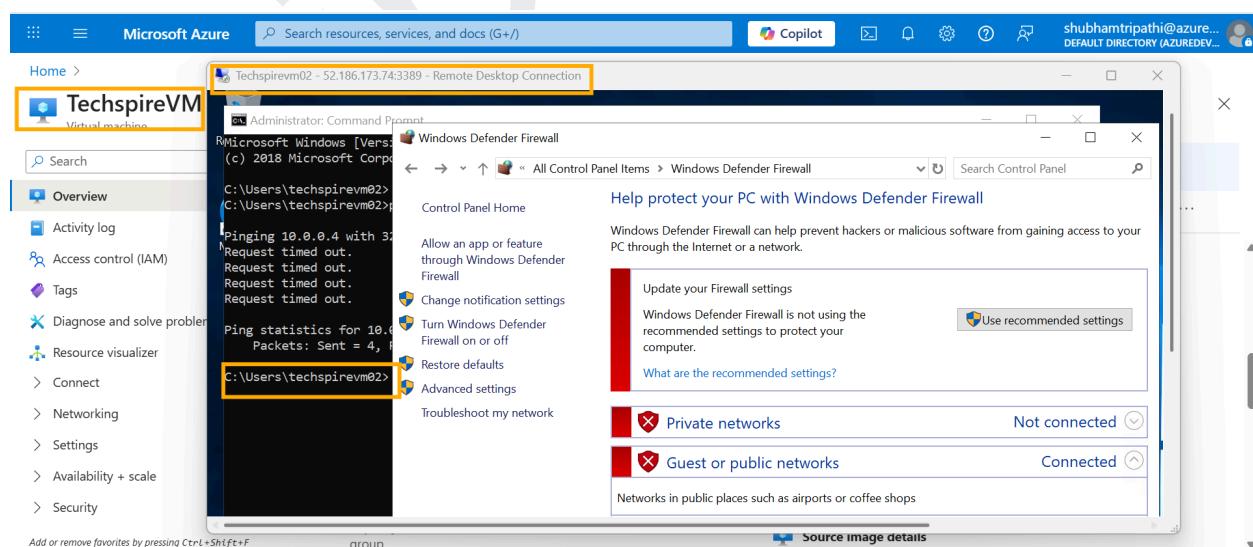
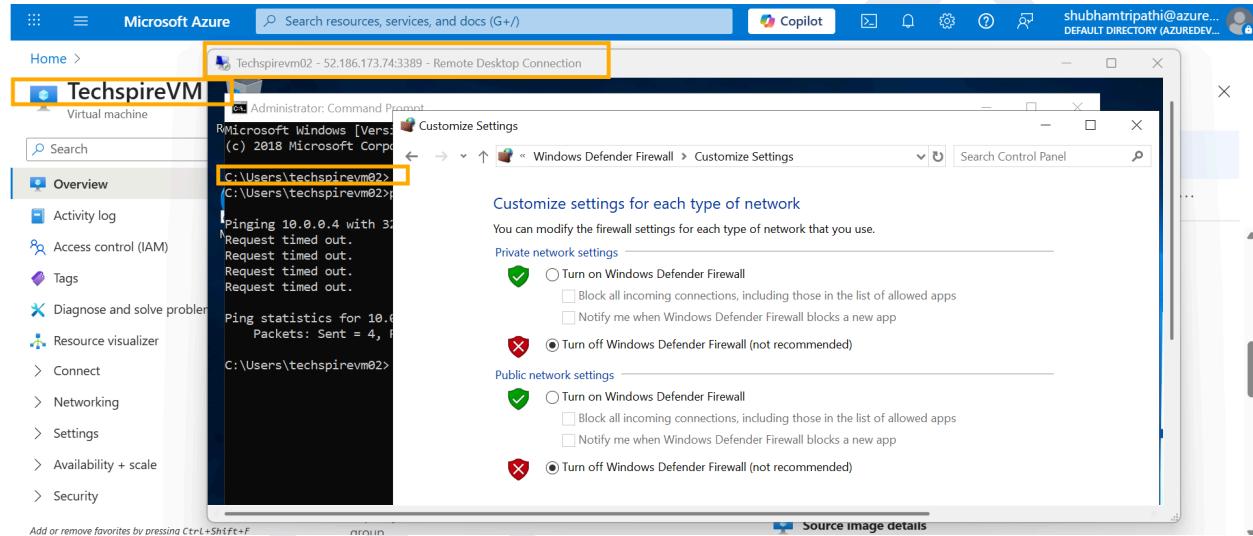
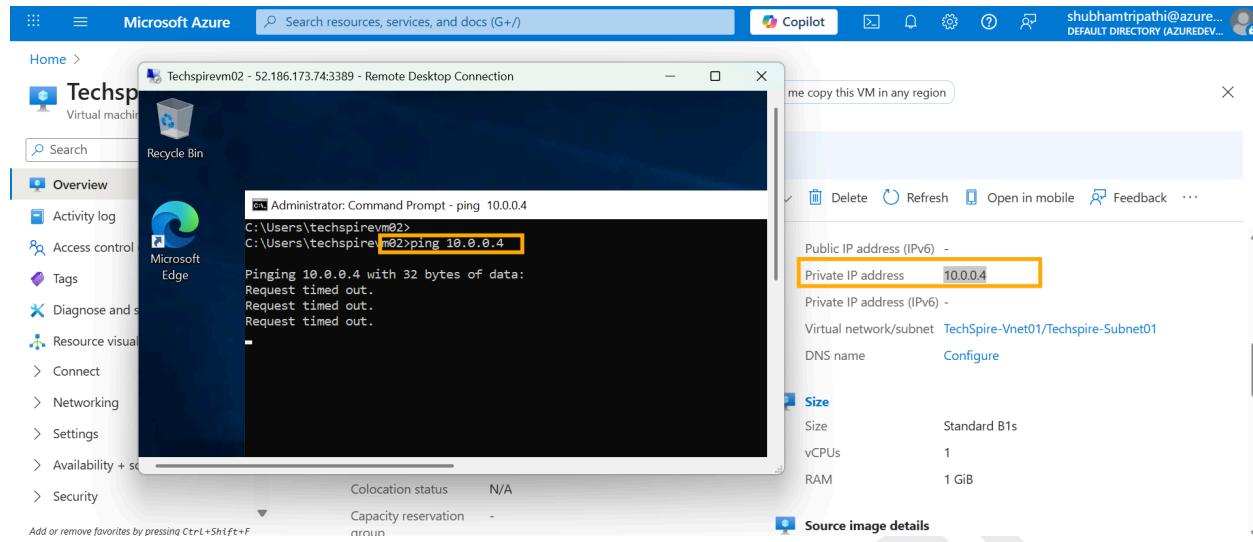
Availability zone 2 Health state -

Administrator: Command Prompt

Open in mobile Feedback JSON View

19 Datacenter) memory)

ubnet02



Establishing VNet Peering Between vnet01 and vnet02 (Same Region)

The screenshot shows two pages from the Microsoft Azure portal:

- Top Page:** Shows the "TechSpire-Vnet01" virtual network details. The "Peering" section in the left sidebar and the "Peering" tab in the main content area are highlighted with orange boxes.
- Bottom Page:** Shows the "TechSpire-Vnet01 | Peerings" page. The "Peering" section in the left sidebar is highlighted with a grey box.

Step 2: Establishing Vnet peering

2.3 Locate the **vnet1** virtual network

2.4 Select **Peering**. Then, add a **peering connection**

Properties	Value
Peering link name	vnet1tovnet2
Traffic to remote virtual network	Allow
Traffic forwarded from remote virtual network	Allow
Virtual network gateway or Route Server	None
Remote virtual network peering link name	vnet2tovnet1

Virtual network deployment model	Techspire
Subscription	#####
Virtual network	Vnet2

Microsoft Azure | Search resources, services, and docs (G+/)

Home > TechSpire-Vnet01 | Peerings >

Add peering

TechSpire-Vnet01

Virtual network peering enables you to seamlessly connect two or more virtual networks in Azure. This will allow resources in either virtual network to directly connect and communicate with resources in the peered virtual network.

Remote virtual network summary

Peering link name * techspirevnet01-to-techspirevnet02

Virtual network deployment model Resource manager Classic

I know my resource ID

Subscription * Azure subscription 1

Add **Cancel** [Give feedback](#)

Microsoft Azure | Search resources, services, and docs (G+/)

Home > TechSpire-Vnet01 | Peerings >

Add peering

TechSpire-Vnet01

Local virtual network peering settings

Allow 'TechSpire-Vnet01' to access 'TechSpire-Vnet02'

Allow 'TechSpire-Vnet01' to receive forwarded traffic from 'TechSpire-Vnet02'

Allow gateway or route server in 'TechSpire-Vnet01' to forward traffic to 'TechSpire-Vnet02'

Enable 'TechSpire-Vnet01' to use 'TechSpire-Vnet02's' remote gateway or route server

Add **Cancel** [Give feedback](#)

Check whether Peering status is connected

Home > TechSpire-Vnet01

TechSpire-Vnet01 | Peerings

Virtual network

Search Subnets Add Refresh Export to CSV Delete Sync

Virtual network peering enables you to seamlessly connect two or more virtual networks in Azure. The virtual networks appear as one for connectivity purposes. [Learn more](#)

Filter by name...

Showing all 1 items

Name	Peering status	Peer IP address	Region	Virtu...	Cross-tenant
techspirevnet01-to...	Fully Synchronized	Connected	TechSpire...	Disabled	No

Give feedback

Notifications

More events in the activity log → Dismiss all

Added virtual network peering X

Successfully added virtual network peering 'techspirevnet01-to-techspirevnet02' to 'TechSpire-Vnet02'.
a few seconds ago

Added virtual network peering X

Successfully added virtual network peering 'techspirevnet01-to-techspirevnet02' to 'TechSpire-Vnet01'.
a few seconds ago

TechspireVM01 TO TechspireVM02

Microsoft Azure Search resources, services, and docs (G+)

shubhamtripathi@azured... DEFAULT DIRECTORY (AZUREDEV...)

Home > TechspireVM - 172.174.244.60:3389 - Remote Desktop Connection

Administrator: Command Prompt

```
Pinging 10.1.0.4 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.1.0.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\techspirevm01>ping 10.1.0.4

Pinging 10.1.0.4 with 32 bytes of data:
Reply from 10.1.0.4: bytes=32 time=1ms TTL=128

Ping statistics for 10.1.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Manage this VM with Azure CLI

Public IP address 52.186.173.74 (Network techspirevm02703_z2) interface

Private IP address 10.1.0.4

Virtual network/subnet TechSpire-Vnet02/TechSpire-Subnet02

DNS name Configure

Size

Standard B1s

vCPUs 1

RAM 1 GiB

Vm02tovm01

Microsoft Azure Search resources, services, and docs (G+)

shubhamtripathi@azured... DEFAULT DIRECTORY (AZUREDEV...)

Home > TechspireVM - 52.186.173.74:3389 - Remote Desktop Connection

Administrator: Command Prompt

```
C:\Users\techspirevm02>
C:\Users\techspirevm02>ping 10.0.0.4

Pinging 10.0.0.4 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\techspirevm02>ping 10.0.0.4

Pinging 10.0.0.4 with 32 bytes of data:
Reply from 10.0.0.4: bytes=32 time=2ms TTL=128
McReply from 10.0.0.4: bytes=32 time=1ms TTL=128
Reply from 10.0.0.4: bytes=32 time=1ms TTL=128
AuReply from 10.0.0.4: bytes=32 time=1ms 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:
```

How can I manage VMs with Copilot Manage this VM with Azure CLI Help me copy this VM in any region

Delete Refresh Open in mobile Feedback

Public IP address (IPv6) -

Private IP address 10.0.0.4

Private IP address (IPv6) -

Virtual network/subnet TechSpire-Vnet01/Techspire-Subnet01

DNS name Configure

Size

Standard B1s

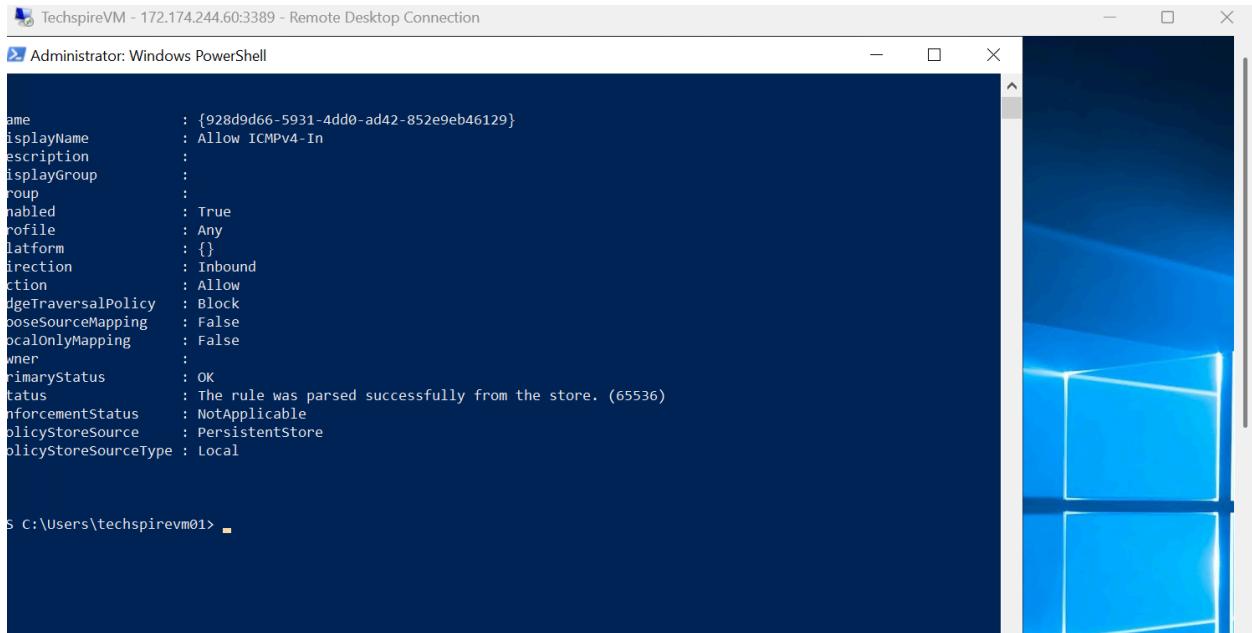
vCPUs 1

RAM 1 GiB

Source image details

Enable ICMP through the Windows firewall so that you can ping vm1 from vm2 by below command

```
New-NetFirewallRule -DisplayName "Allow ICMPv4-In" -Protocol ICMPv4
```

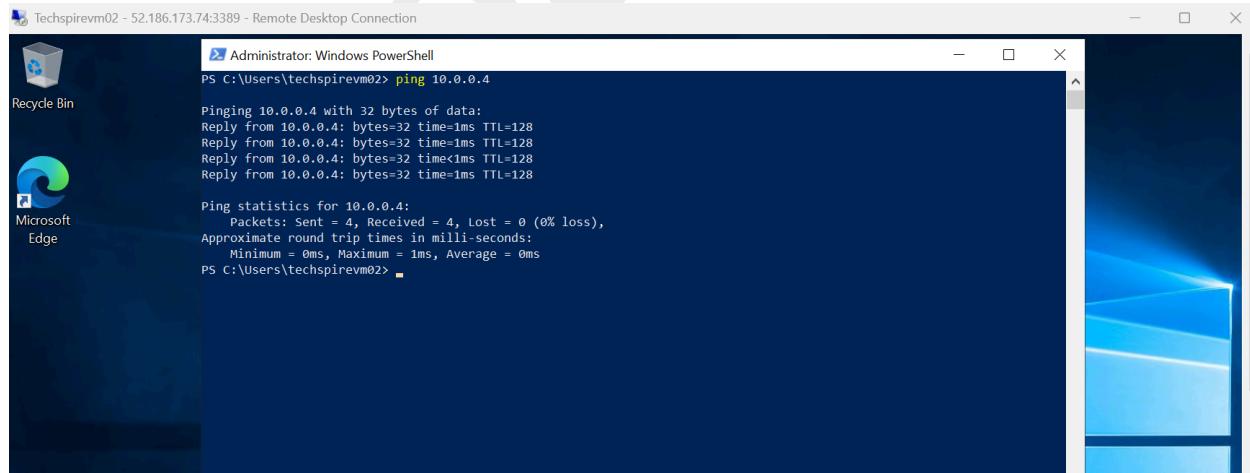


```
name          : {928d9d66-5931-4dd0-ad42-852e9eb46129}
displayName   : Allow ICMPv4-In
description   :
displayGroup :
group        :
enabled      : True
profile      : Any
platform    : {}
direction    : Inbound
action       : Allow
edgeTraversalPolicy : Block
poseSourceMapping : False
localOnlyMapping : False
owner        :
primaryStatus : OK
status        : The rule was parsed successfully from the store. (65536)
enforcementStatus : NotApplicable
policyStoreSource : PersistentStore
policyStoreSourceType : Local

S C:\Users\techspirevm01> ■
```

3.1 Connect to vm2 with RDP and ping vm1

```
ping 10.0.0.4
```



```
Recycle Bin
Microsoft Edge

Techspirevm02 - 52.186.173.74:3389 - Remote Desktop Connection
Administrator: Windows PowerShell
PS C:\Users\techspirevm02> ping 10.0.0.4

Pinging 10.0.0.4 with 32 bytes of data:
Reply from 10.0.0.4: bytes=32 time=1ms TTL=128
Reply from 10.0.0.4: bytes=32 time=1ms TTL=128
Reply from 10.0.0.4: bytes=32 time<1ms TTL=128
Reply from 10.0.0.4: bytes=32 time=1ms 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 = 0ms, Maximum = 1ms, Average = 0ms
PS C:\Users\techspirevm02> ■
```

Step 4: Creating a custom RBAC Role

4.1 Go to Resource Group > Access Control (IAM)

4.2 Select Add custom role

The screenshot shows the Azure Access control (IAM) blade for the 'Techspire' resource group. The 'Check access' tab is selected. On the left, there's a sidebar with various options like Tags, Resource visualizer, Events, Settings, Cost Management, Monitoring, Automation, and Help. The main area has sections for 'My access' (with a 'View my access' button), 'Check access' (with a 'Check access' button), and three cards: 'Grant access to this resource', 'View access to this resource', and 'View deny assignments'.

4.1 Under the Basics tab, provide a custom role name. Next, select Start from scratch

The screenshot shows the 'Create a custom role' blade. The 'Basics' tab is selected. It asks for a 'Custom role name' (set to 'techspire operator') and a 'Description' ('The custom role will be applied to TechSpire only'). Below, under 'Baseline permissions', the 'Start from scratch' radio button is selected. At the bottom, there are buttons for 'Review + create', 'Previous', 'Next', and 'Feedback'.

The screenshot shows the 'Add permissions' blade. The 'Permissions' tab is selected. A search bar shows 'Microsoft.Compute'. Results include 'Microsoft Compute' (described as 'Access cloud compute capacity and scale on demand (such as virtual machines) and only pay for the resources you use.') and 'Microsoft.ComputeSchedule'. At the bottom, there are buttons for 'Review + create', 'Add', 'Cancel', and 'Download all permissions'.

Microsoft Azure Search resources, services, and docs (G+) Copilot shubhamtripathi@azur... DEFAULT DIRECTORY (AZUREDEV...) X

Home > Techspire | A Microsoft.Compute permissions Create a custom role

Basics Permission + Add permission

Click Add permissions To add a wildcard (*) permission, you must manually add the permission on the JSON tab. To exclude specific permissions from a wildcard permission, click Exclude permissions. Learn more

Actions Data Actions

Permission

Microsoft.Compute/virtualMachines

Read : Get Virtual Machine Description Get the properties of a virtual machine

Review + create Add Cancel

Microsoft.Compute/virtualMachines/read

Microsoft.Compute/virtualMachines/start/action

Microsoft.Compute/virtualMachines/restart/action

Microsoft.Network/virtualNetworks/read Microsoft.Storage/storageAccounts/read/

Microsoft.Storage/storageAccounts/blobServices/containers/read

Microsoft.Resources/subscriptions/resourceGroups/read

Microsoft.Resources/subscriptions/read

Home > Techspire | Access control (IAM) >

Create a custom role ...

Click Add permissions to select the permissions you want to add to this custom role.

To add a wildcard (*) permission, you must manually add the permission on the JSON tab. [Learn more](#)

To exclude specific permissions from a wildcard permission, click Exclude permissions. [Learn more](#)

Permission	↑↓	Description	↑↓	Permission type	↑↓
Microsoft.Compute/virtualMachines/read		Get the properties of a virtual machine		Action	
Microsoft.Compute/virtualMachines/start/...		Starts the virtual machine		Action	
Microsoft.Compute/virtualMachines/restar...		Restarts the virtual machine		Action	
Microsoft.Network/virtualNetworks/read		Get the virtual network definition		Action	
Microsoft.Storage/storageAccounts/read		Returns the list of storage accounts or gets...		Action	
Microsoft.Storage/storageAccounts/blobS...		Returns a container		Action	
Microsoft.Resources/subscriptions/resour...		Gets or lists resource groups.		Action	
Microsoft.Resources/subscriptions/read		Gets the list of subscriptions.		Action	

Definitions

Control plane

Actions specify the operations that a role is allowed to perform. NotActions specify the operations that are excluded from the allowed Actions (this is useful if a role has wildcards).

Data plane

DataActions specify the operations that a role is allowed to perform to the data within an object. NotDataActions specify the operations that are excluded from the allowed DataActions (this is useful if a role has wildcards).

Wildcards (*)

A wildcard (*) extends a permission to everything

Review + create

Previous

Next

Feedback

4.1 Under the Review + create tab, select Create

The screenshot shows the Microsoft Azure portal interface for creating a custom role. The top navigation bar includes 'Microsoft Azure', a search bar, 'Copilot', and user information 'shubhamtripathi@azur... DEFAULT DIRECTORY (AZUREDEV...)'. The main title is 'Create a custom role ...'. Below it, a table lists actions:

Action	Actions
Action	Microsoft.Compute/virtualMachines/read
Action	Microsoft.Compute/virtualMachines/start/action
Action	Microsoft.Compute/virtualMachines/restart/action
Action	Microsoft.Network/virtualNetworks/read
Action	Microsoft.Storage/storageAccounts/read
Action	Microsoft.Storage/storageAccounts/blobServices/containers/read
Action	Microsoft.Resources/subscriptions/resourceGroups/read
Action	Microsoft.Resources/subscriptions/read

Assignable Scopes

Scope
/subscriptions/4a8937a7-b294-4a1f-8d31-79bbb1a4c17f/resourceGroups/Techspire

Buttons at the bottom include 'Create' (highlighted in blue), 'Previous', and 'Feedback'.

The second part of the screenshot shows a confirmation message: 'You have successfully created the custom role "techspire operator". It may take the system a few minutes to display your role everywhere.' with an 'OK' button.

Below this, the same list of actions and scope is shown again, along with 'Create' and 'Previous' buttons.

Step 5: Adding a User to the Directory and assign the custom RBAC Role

5.1 Go to Active Directory > All Users

5.2 Select New user

5.3 Under Identity, provide a username and name

5.4 Copy the auto-generated password and keep it for future use

Select Create

5.5 Go to Resource Group > Access control (IAM)

5.6 Select Add role assignment

5.7 Under Role, select the custom role created in the previous step

5.8 Go to Members > Select members. Then, select **TechspireUser**

5.9 Select Review + assign

5.10 Under Role assignments, verify the role that is assigned

5.11 Test the user permissions by logging in to the Azure portal with the user ID

5.12 Update the password when prompted

5.13 Restart **Techspire vm01**. You should be able to restart the vm