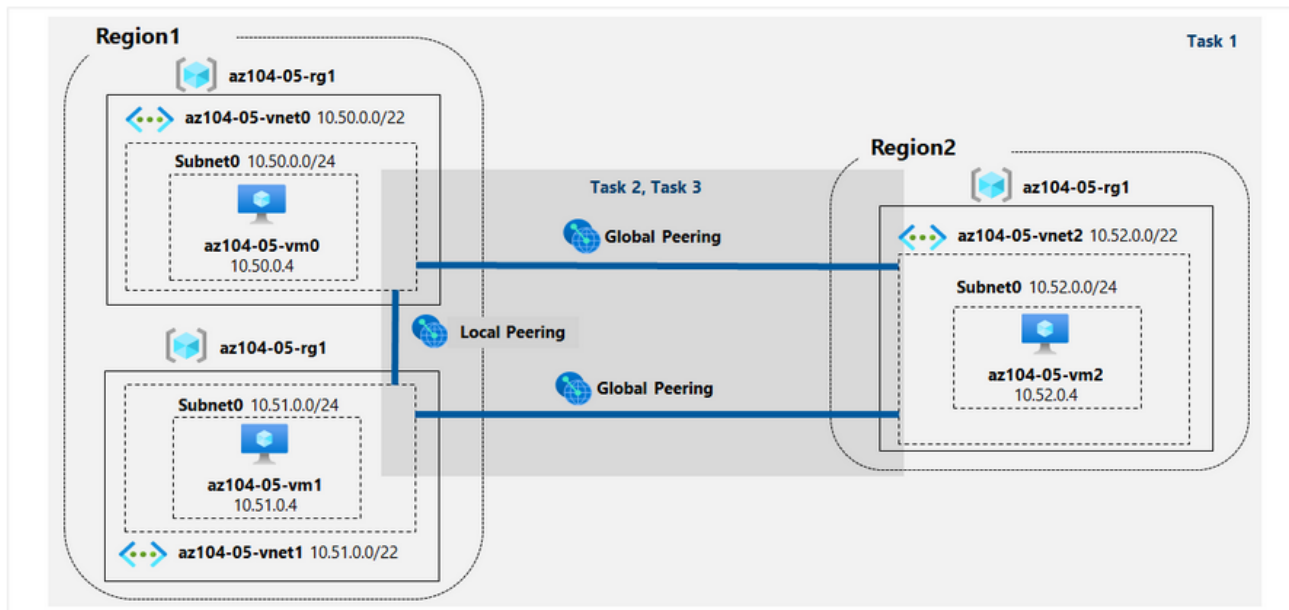


Implement Intersite Connectivity Student

In this lab, you will:

- Task 1: Provision the lab environment
- Task 2: Configure local and global virtual network peering
- Task 3: Test intersite connectivity

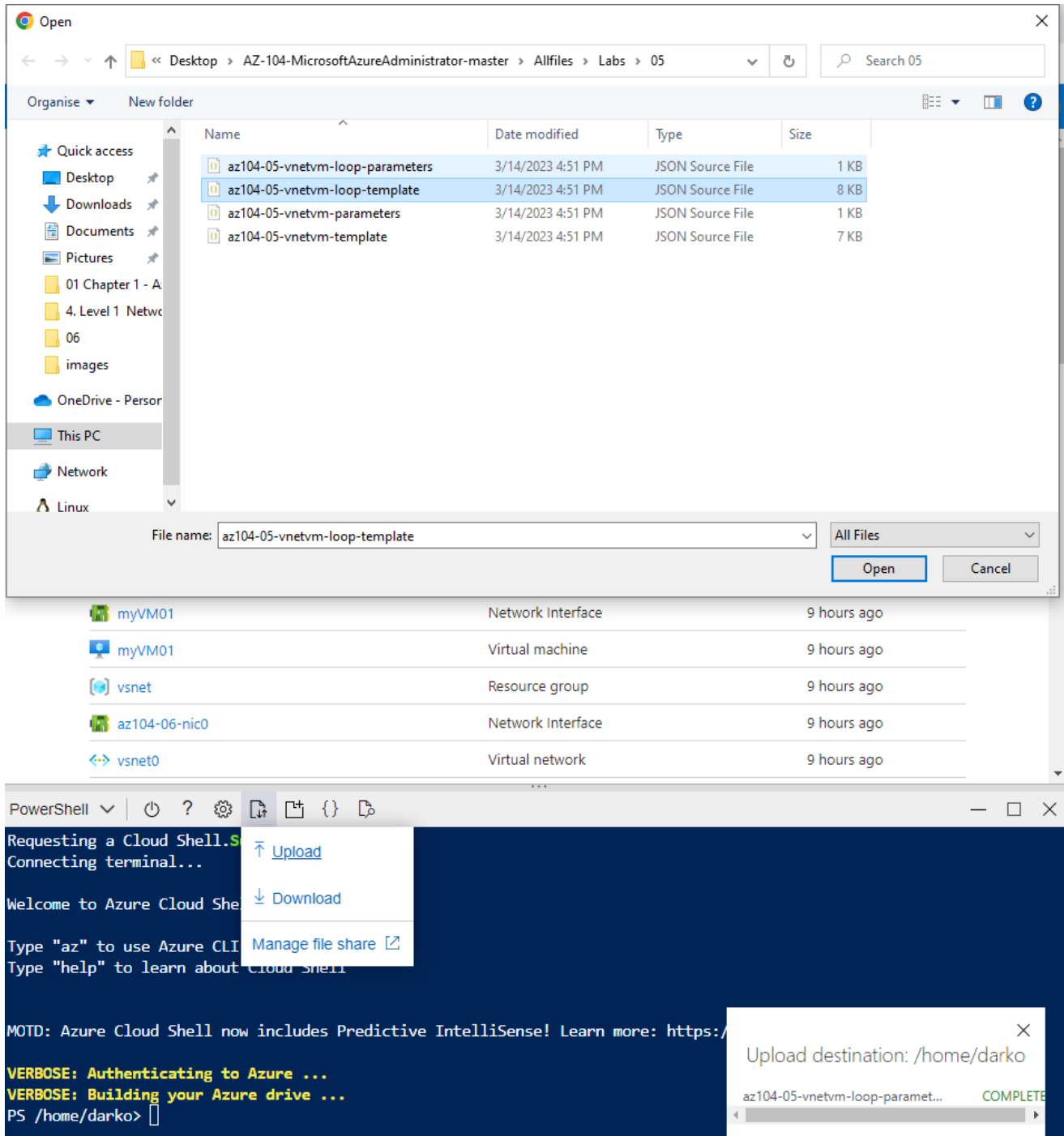


In the Azure portal, open the Azure Cloud Shell

Using powershell upload the files

az104-05-vnetvm-loop-template.json

az104-05-vnetvm-loop-parameters.json



In the powershell type `code .` and vscode will be open in powershell terminal. Edit password, type secure password `az104-05-vnetvm-loop-parameters.json` and save the file.

We have to create new resource group that will be hosting the lab environment. The first two virtual networks and a pair of virtual machines will be deployed in azure region 1, The third virtual network and the third virtual machine will be deployed in the same resource group but another azure region 2.

From the powershell run this commands to create new location and resource group

```

$location1 = 'eastus'

$location2 = 'westus'
  
```

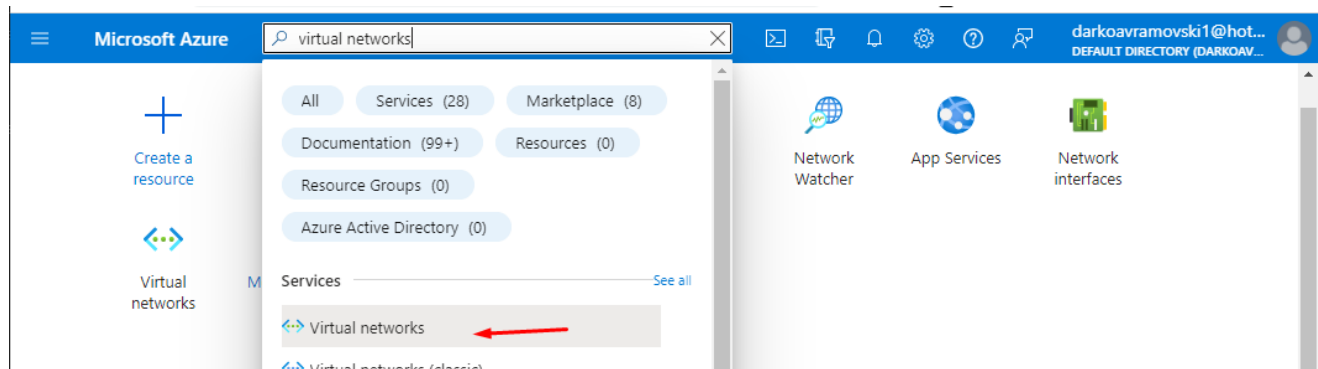
```
$rgName = 'az104-05-rg1'
```

```
New-AzResourceGroup -Name $rgName -Location $location1
```

Then we have to create three virtual networks and deploy VM into then by using templates, run this command in powershell

```
New-AzResourceGroupDeployment `
-ResourceGroupName $rgName `
-TemplateFile $HOME/az104-05-vnetvm-loop-template.json `
-TemplateParameterFile $HOME/az104-05-vnetvm-loop-parameters.json `
-location1 $location1 `
-location2 $location2
```

After deployment has finished we have to configure local and global virtual network peering



In the list of virtual networks, click **az104-05-vnet0**.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with the 'Microsoft Azure' logo and a search bar. Below this, the 'Virtual networks' page is displayed, showing a list of virtual networks. A red arrow points to the first record in the table, 'az104-05-vnet0'.

Name ↑↓	Resource group ↑↓	Location ↑↓	Subscription ↑↓
az104-05-vnet0	az104-05-rg1	East US	Azure Pass - Sponsorship
az104-05-vnet1	az104-05-rg1	East US	Azure Pass - Sponsorship
az104-05-vnet2	az104-05-rg1	West US	Azure Pass - Sponsorship

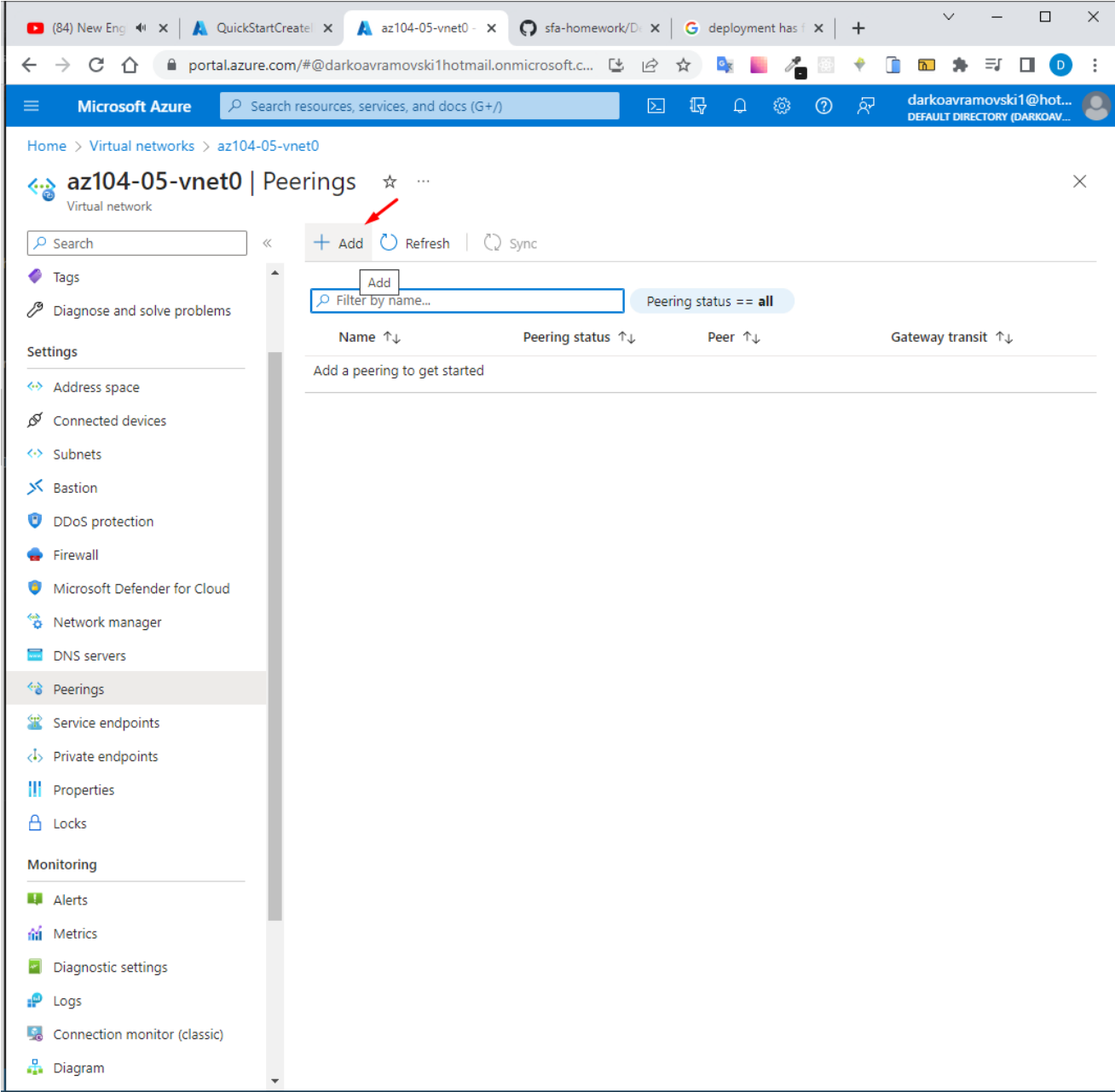
On the **az104-05-vnet0** virtual network blade, in the Settings section, click **Peerings** and then click **+ Add**.

Microsoft Azure portal interface showing the configuration page for a Virtual Network (VNet) named **az104-05-vnet0**.

The left sidebar contains navigation options: Settings, Address space, Connected devices, Subnets, Bastion, DDoS protection, Firewall, Microsoft Defender for Cloud, Network manager, DNS servers, **Peering** (highlighted with a red arrow), Service endpoints, Private endpoints, Properties, Locks, Monitoring, Alerts, Metrics, Diagnostic settings, Logs, and Connection monitor (classic).

The main content area displays the VNet configuration details:

- Essentials** (JSON View):
 - Resource group: [az104-05-rg1](#)
 - Location: [East US](#)
 - Subscription: [Azure Pass - Sponsorship](#)
 - Subscription ID: df86697d-88bc-4474-899b-64b5dfd1d8cf
 - Address space: [10.50.0.0/22](#)
 - DNS servers: [Azure provided DNS service](#)
 - Flow timeout: [Configure](#)
 - BGP community string: [Configure](#)
 - Virtual network ID: 86fee8d9-8951-40f8-b4f0-369d51b18528
- Tags**: [Click here to add tags](#)
- Capabilities (5)**:
 - 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.



This step establishes two local peerings - one from az104-05-vnet0 to az104-05-vnet1 ;

Home >

Add peering

az104-05-vnet0

az104-05-vnet0_to_az104-05-vnet1

Traffic to remote virtual network

☒ Allow (default)

☐ Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network

☐ Allow (default)

☒ Block traffic that originates from outside the remote virtual network

Virtual network gateway or Route Server

☐ Use this virtual network's gateway or Route Server

☐ Use the remote virtual network's gateway or Route Server

☒ None (default)

Remote virtual network

Peering link name *

az104-05-vnet1_to_az104-05-vnet0

Virtual network deployment model

☒ Resource manager

☐ Classic

☐ I know my resource ID

Subscription *

Azure Pass - Sponsorship

Virtual network *

az104-05-vnet1

Traffic to remote virtual network

☒ Allow (default)

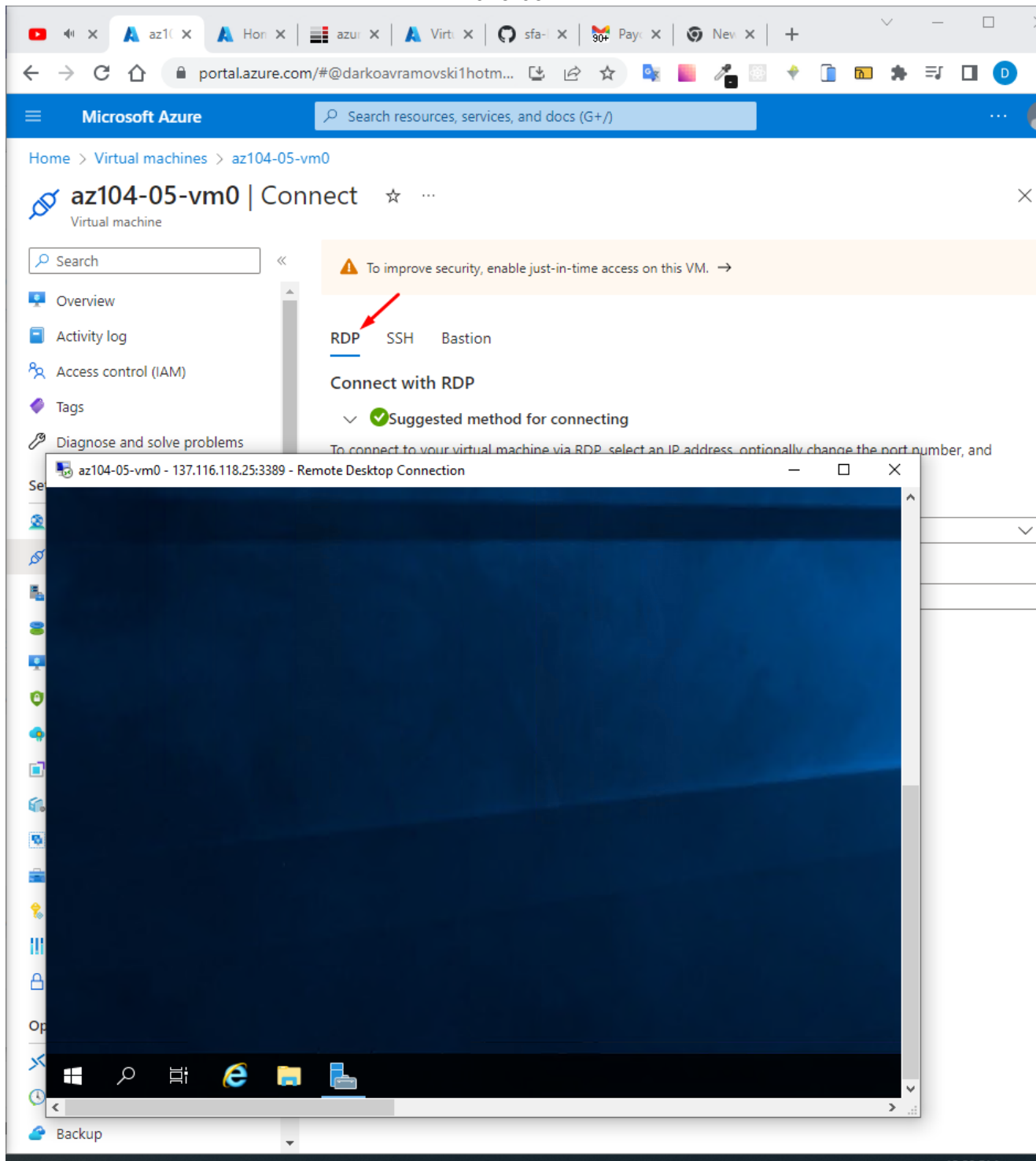
☐ Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network

Add

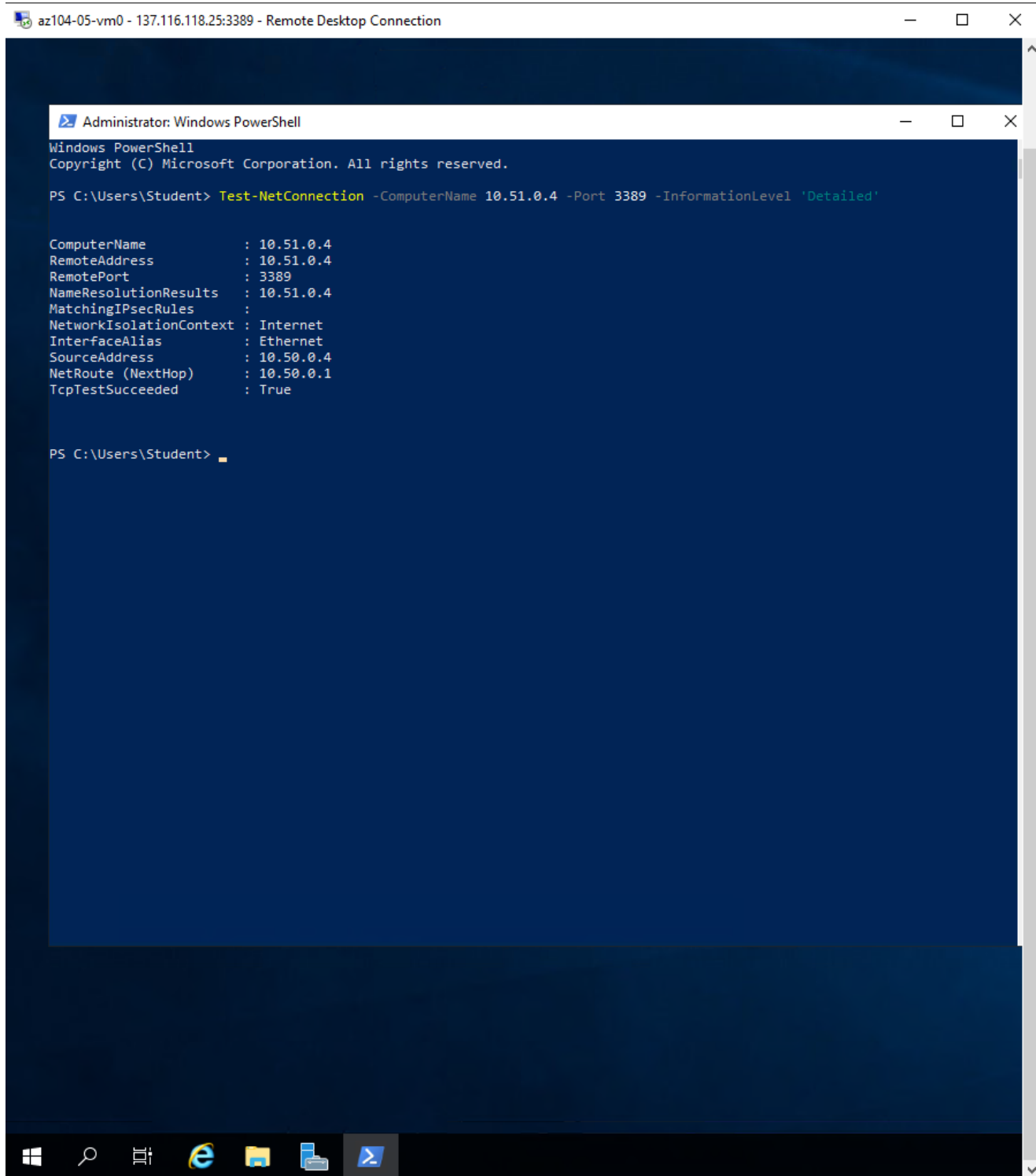
Repeat this step with virtual networka - az104-05-vnet2

Next open VM az104-05-vm0 and connect with RDP



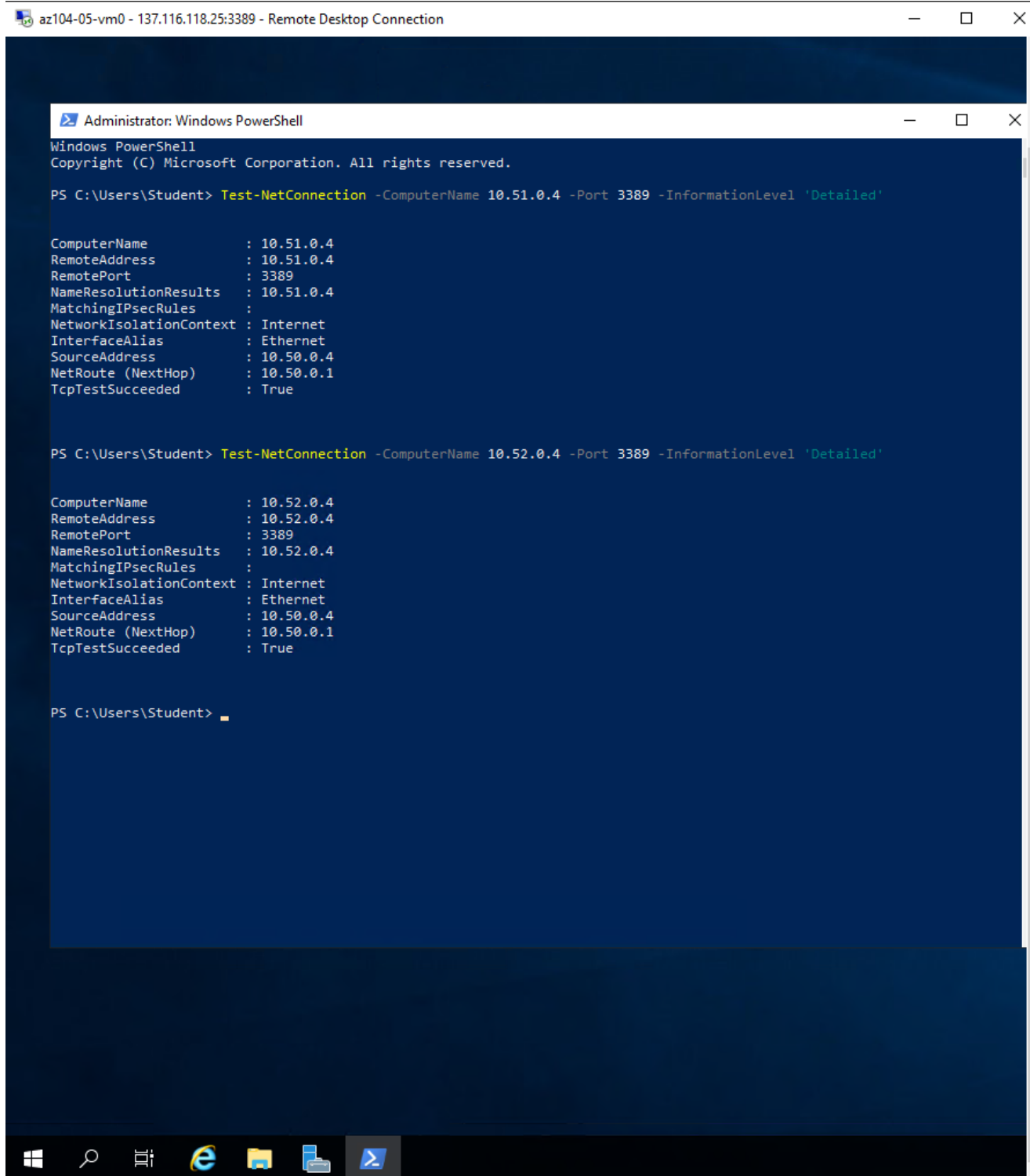
Open powershell run the following to test connectivity to az104-05-vm1

```
Test-NetConnection -ComputerName 10.51.0.4 -Port 3389 -InformationLevel 'Detailed'
```

In the Windows PowerShell console window, run the following to test connectivity to az104-05-vm2

```
Test-NetConnection -ComputerName 10.52.0.4 -Port 3389 -InformationLevel 'Detailed'
```



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Student> Test-NetConnection -ComputerName 10.51.0.4 -Port 3389 -InformationLevel 'Detailed'

ComputerName           : 10.51.0.4
RemoteAddress           : 10.51.0.4
RemotePort              : 3389
NameResolutionResults   : 10.51.0.4
MatchingIPsecRules      :
NetworkIsolationContext : Internet
InterfaceAlias           : Ethernet
SourceAddress           : 10.50.0.4
NetRoute (NextHop)      : 10.50.0.1
TcpTestSucceeded        : True

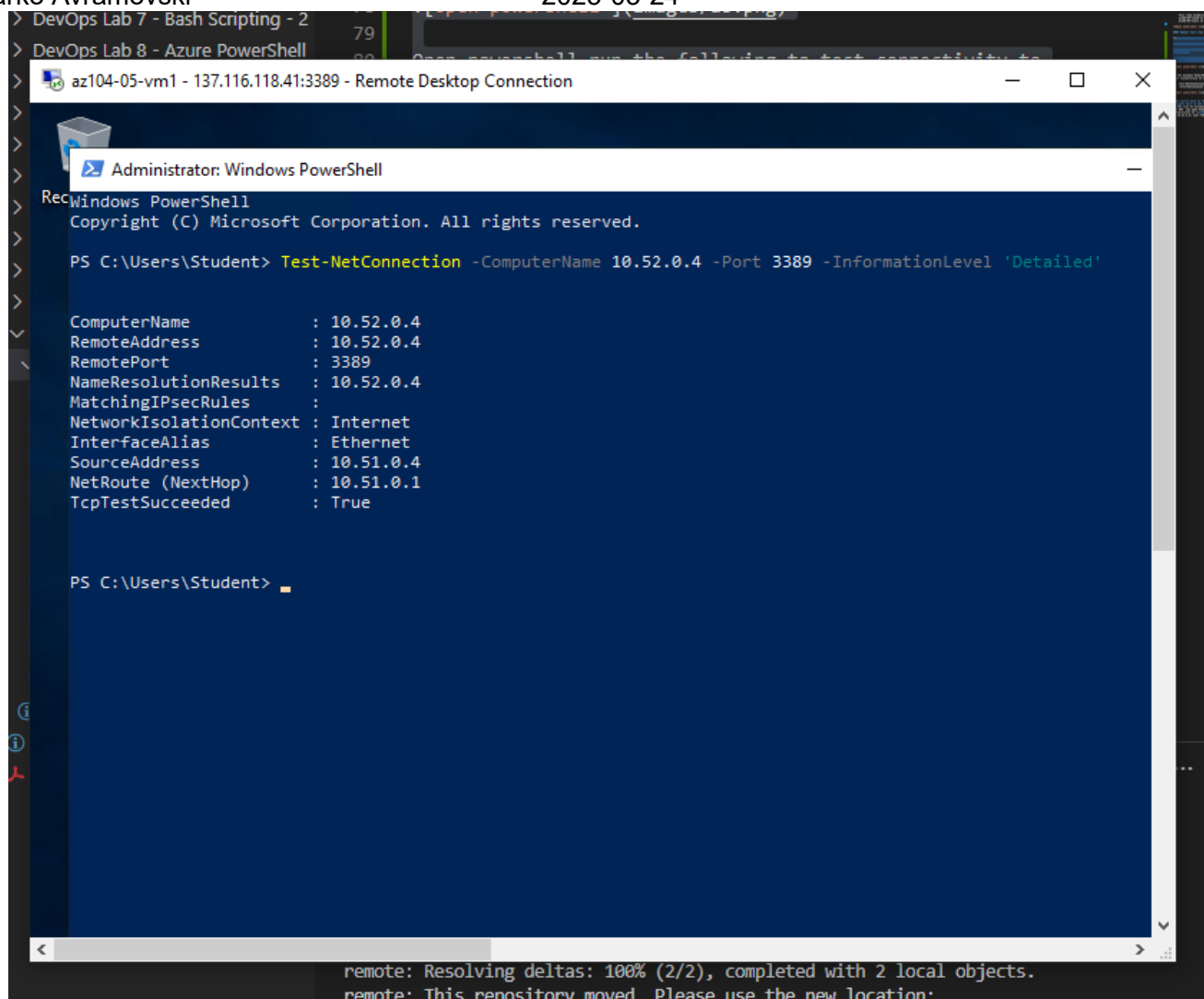
PS C:\Users\Student> Test-NetConnection -ComputerName 10.52.0.4 -Port 3389 -InformationLevel 'Detailed'

ComputerName           : 10.52.0.4
RemoteAddress           : 10.52.0.4
RemotePort              : 3389
NameResolutionResults   : 10.52.0.4
MatchingIPsecRules      :
NetworkIsolationContext : Internet
InterfaceAlias           : Ethernet
SourceAddress           : 10.50.0.4
NetRoute (NextHop)      : 10.50.0.1
TcpTestSucceeded        : True

PS C:\Users\Student>
```

Switch back to the Azure portal on your lab computer and navigate back to the Virtual machines blade.

In the list of virtual machines, click **az104-05-vm1**. and connect via RDP and open PowerShell as admin, run the command to test connectivity to **az104-05-vm2** (which has the private IP address of 10.52.0.4) over TCP port 3389:



```
DevOps Lab 7 - Bash Scripting - 2
DevOps Lab 8 - Azure PowerShell
az104-05-vm1 - 137.116.118.41:3389 - Remote Desktop Connection

Administrator: Windows PowerShell

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Student> Test-NetConnection -ComputerName 10.52.0.4 -Port 3389 -InformationLevel 'Detailed'

ComputerName           : 10.52.0.4
RemoteAddress           : 10.52.0.4
RemotePort              : 3389
NameResolutionResults   : 10.52.0.4
MatchingIPsecRules      :
NetworkIsolationContext : Internet
InterfaceAlias          : Ethernet
SourceAddress           : 10.51.0.4
NetRoute (NextHop)      : 10.51.0.1
TcpTestSucceeded        : True

PS C:\Users\Student>
```

remote: Resolving deltas: 100% (2/2), completed with 2 local objects.
remote: This repository moved. Please use the new location: