

Branden Solomon
5/7/25
Professor Francis
CTEC 475

Capstone Module 6

1. Create two VPCs with one subnet each, either in the same cloud platform or in two different cloud platforms. (Your instructor might require that you use the same cloud platform for this project or two cloud platforms—check with your instructor for specific requirements.) Make sure both subnets have access to the Internet. For example, in AWS, you'll need to add an Internet gateway to each subnet and add an Internet route to each subnet's route table.

The screenshot shows the Microsoft Azure portal interface for creating a new virtual network. The top navigation bar includes 'Microsoft Azure', 'Search resources, services, and docs (G+)', 'Copilot', and a user account 'SOLOMONB0509@stud... BOWIE STATE'. The main title is 'Create virtual network' with a '... more' link. Below it, tabs for 'Basics', 'Security', 'IP addresses' (which is selected), 'Tags', and 'Review + create' are visible. A note says 'Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. Learn more'.

IP addresses section:

- Subnet purpose: Default
- Name: Web-VNet
- Include an IPv4 address space: checked
- IPv4 address range: 192.16.0.0/24 (192.16.0.0 - 192.16.0.255)
- Starting address: 192.16.0.0
- Size: /24 (256 addresses)
- Subnet address range: 192.16.0.0 - 192.16.0.255

IPv6 section:

- Include an IPv6 address space: unchecked (checkbox is grayed out)
- This virtual network has no IPv6 address ranges.

Private subnet section:

- Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. [Learn more](#).

Security section:

- Simplify internet access for virtual machines by using a network address translation gateway. Filter subnet traffic using a network security group. [Learn more](#).
- NAT gateway: None

Buttons at the bottom include 'Previous', 'Next', 'Review + create' (highlighted in blue), 'Save', 'Cancel', and 'Give feedback'.

Basics tab (bottom of page):

- Subscription: Azure for Students
- Resource Group: Web-VNet
- Name: Web-VNet
- Region: East US

Security tab:

- Azure Bastion: Disabled
- Azure Firewall: Disabled
- Azure DDoS Network Protection: Disabled

IP addresses tab:

- Address space: 192.16.0.0/24 (256 addresses)
- Subnet: Web-VNet (192.16.0.0/24) (256 addresses)

Tags tab:

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

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

192.16.1.0/24	<input type="button" value="Delete address space"/>
192.16.1.0	/24
192.16.1.0 - 192.16.1.255	256 addresses

Subnets IP address range Size NAT gateway

default	192.16.1.0 - 192.16.1.255	/24 (256 addresses)	-	<input type="button"/>
---------	---------------------------	---------------------	---	------------------------

Add IPv4 address space

The entered IPv4 address range may not work correctly. It is recommended to use an address range that is not globally routable, such as 172.16.0.0/12, or a range defined in RFC 1918 and RFC 6598. [Learn more ↗](#)

Edit subnet

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. [Learn more ↗](#)

Subnet purpose Default Name * DB-VNet

IPv4

Include an IPv4 address space

IPv4 address range 192.16.1.0/24 192.16.1.0 - 192.16.1.255

Starting address * 192.16.1.0 /24 (256 addresses)

Size Subnet address range 192.16.1.0 - 192.16.1.255

IPv6

Include an IPv6 address space This virtual network has no IPv6 address ranges.

Private subnet

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. [Learn more ↗](#)

Enable private subnet (no default outbound access)

Security

Simplify internet access for virtual machines by using a network address translation gateway. Filter subnet traffic using a network security group. [Learn more ↗](#)

NAT gateway None Create new

Save **Cancel** **Give feedback**

Create virtual network

Basics Security IP addresses Tags Review + create

[View automation template](#)

Basics

Subscription Azure for Students
 Resource Group DB-VNet
 Name DB-VNet
 Region East US

Security

Azure Bastion Disabled
 Azure Firewall Disabled
 Azure DDoS Network Protection Disabled

IP addresses

Address space 192.16.1.0/24 (256 addresses)
 Subnet DB-VNet (192.16.1.0/24) (256 addresses)

Tags

Save **Cancel** **Give feedback**

2. Create a VM instance in each subnet. Make sure each VM receives a public IP address. What public IP address is assigned to your VMs?

Microsoft Azure

Home > Web-VNet | Network settings > web-vnet57_z1

web-vnet57_z1 | IP configurations

Network Interface

Search Refresh

Overview Activity log Access control (IAM) Tags Resource visualizer Settings IP configurations DNS servers Network security group Properties Locks Monitoring Automation Help

IP Settings

Enable IP forwarding:

Virtual network: Web-VNet

Gateway load balancer: None

Subnet: Web-VNet (192.16.0.0/24) 250 free IP addresses 250 free IP addresses

Note: Private and public IP addresses can be assigned to a virtual machine's network interface controller. You can add as many private and public IPv4 addresses as necessary to a network interface, within the limits listed in the Azure limits article. [Learn more](#)

Add Make primary Delete

Name	IP Version	Type	Private IP Address	Public IP Address
ipconfig1	IPv4	Primary	192.16.0.4 (Dynamic)	52.224.242.242 (Web-VNet-ip)

Microsoft Azure

Home > Compute infrastructure | Virtual machines >

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*: DB-VNet

Subnet*: DB-VNet (192.16.1.0/24)

Public IP: (new) DB-VNet-ip

NIC network security group: None Basic Advanced

Public inbound ports*: None Allow selected ports

Select inbound ports*: SSH (22)

Warning: 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.

Deletes public IP and NIC when VM is deallocated

< Previous Next : Management > Review + create

Give feedback

3. Configure security rules that allow ICMP traffic from any source to your target VM so you can confirm the target VM will respond successfully to pings. Get a working ping from your local computer to your target VM before proceeding.

Microsoft Azure

Home > Network security groups >

Network security group

Bowie State

+ Create Manage view ...

Filter for any field...

Name: Web-VNet-nsg

Web-VNet-nsg Network security group

Search Move Delete Refresh Give feedback

Overview

Essentials

Resource group (move) : Web-VNet
Location : East US
Subscription (move) : Azure for Students
Subscription ID : 090f47b7-a8e7-44f5-a691-ac73987dc0a9
Tags (edit) : Add tags

Custom security rules : 2 inbound, 1 outbound
Associated with : 0 subnets, 1 network interfaces

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

Monitoring

Alerts

Diagnostic settings

Logs

NSG flow logs

Automation

Help

Inbound Security Rules

Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑	Destination ↑	Action ↑
300	SSH	22	TCP	Any	Any	Allow
330	AllowAnyCustomAnyIn...	Any	ICMP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInB...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Outbound Security Rules

Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑	Destination ↑	Action ↑
320	AllowAnyCustomAnyOutbo...	Any	ICMP	Any	Any	Allow
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Add or remove favorites by pressing Ctrl + Shift + F

Microsoft Azure

Home > Network security groups >

Network security group

Bowie State

+ Create Manage view ...

Filter for any field...

Name: DB-VNet-nsg

DB-VNet-nsg Network security group

Search Move Delete Refresh Give feedback

Overview

Essentials

Resource group (move) : DB-VNet
Location : East US
Subscription (move) : Azure for Students
Subscription ID : 090f47b7-a8e7-44f5-a691-ac73987dc0a9
Tags (edit) : Add tags

Custom security rules : 2 inbound, 1 outbound
Associated with : 0 subnets, 1 network interfaces

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

Monitoring

Alerts

Diagnostic settings

Logs

NSG flow logs

Automation

Help

Inbound Security Rules

Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑	Destination ↑	Action ↑
300	SSH	22	TCP	Any	Any	Allow
310	AllowAnyCustomAnyIn...	Any	ICMP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInB...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Outbound Security Rules

Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑	Destination ↑	Action ↑
320	AllowAnyCustomAnyOutbo...	Any	ICMP	Any	Any	Allow
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Add or remove favorites by pressing Ctrl + Shift + F

4. Configure security rules that allow SSH or RDP connections to your source VM. Remote into the source VM.

Microsoft Azure

Home > Network security groups > DB-VNet-nsg

Network security group

DB-VNet-nsg | Inbound security rules

Created security rule
Successfully created security rule 'Allow-RDP'.

Priority	Name	Port	Protocol	Source	Destination	Action
300	SSH	22	TCP	Any	Any	Allow
310	AllowAnyCustomAnyIn...	Any	ICMP	Any	Any	Allow
330	Allow-SSH	22	TCP	Any	Any	Allow
340	Allow-RDP	3389	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancer...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Add or remove favorites by pressing Ctrl + Shift + F4

Microsoft Azure

Home > Network security groups > Web-VNet-nsg

Network security group

Web-VNet-nsg | Inbound security rules

Created security rule
Successfully created security rule 'Allow-RDP'.

Priority	Name	Port	Protocol	Source	Destination	Action
300	SSH	22	TCP	Any	Any	Allow
330	AllowAnyCustomAnyIn...	Any	ICMP	Any	Any	Allow
340	Allow-SSH	22	TCP	Any	Any	Allow
350	Allow-RDP	3389	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancer...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Add or remove favorites by pressing Ctrl + Shift + F4

5. Configure security rules that only allow ICMP traffic from your source VM to your target VM. What rules did you add? What effect do you expect each rule to have on traffic to and from each VM?

Microsoft Azure

Home > Network security groups > DB-VNet-nsg

Network security group

Bowie State

+ Create Manage view ...

DB-VNet-nsg | Inbound security rules

Search Add Hide default rules Refresh Delete Give feedback

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Resource visualizer Settings Inbound security rules Outbound security rules Network interfaces Subnets Properties Locks Monitoring Automation Help

Filter by name Priority ↑ Name ↑ Port ↑ Protocol ↑ Source ↑ Destination ↑ Action ↑

Priority	Name	Port	Protocol	Source	Destination	Action
300	SSH	22	TCP	Any	Any	Allow
330	Allow-SSH	22	TCP	Any	Any	Allow
340	Allow-RDP	3389	TCP	Any	Any	Allow
350	Allow-Web-VM	Any	ICMP	71.127.41.163	192.16.1.0	Allow
65000	AllowVnetInbound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInbound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInbound	Any	Any	Any	Any	Deny

Add or remove favorites by pressing Ctrl+Shift+F1+F2

< Page 1 of 1 >

Microsoft Azure

Home > Network security groups > Web-VNet-nsg

Network security group

Bowie State

+ Create Manage view ...

Web-VNet-nsg | Inbound security rules

Search Add Hide default rules Refresh Delete Give feedback

Updated security rule: Successfully saved security rule 'Allow-DB-VM.'

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Resource visualizer Settings Inbound security rules Outbound security rules Network interfaces Subnets Properties Locks Monitoring Automation Help

Filter by name Priority ↑ Name ↑ Port ↑ Protocol ↑ Source ↑ Destination ↑ Action ↑

Priority	Name	Port	Protocol	Source	Destination	Action
300	SSH	22	TCP	Any	Any	Allow
340	Allow-SSH	22	TCP	Any	Any	Allow
350	Allow-RDP	3389	TCP	Any	Any	Allow
360	Allow-DB-VM	Any	ICMP	71.127.41.163	192.16.1.0	Allow
65000	AllowVnetInbound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInbound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInbound	Any	Any	Any	Any	Deny

Add or remove favorites by pressing Ctrl+Shift+F1+F2

< Page 1 of 1 >

6. Run a ping from the source VM to the target VM that shows ICMP traffic is reaching the target VM. Take a screenshot showing the output; include this visual with your answers to this project's questions.

Azure Search resources, services, and docs (Ctrl+F)

Administrator: 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:\WINDOWS\system32> ping 192.16.0.0

Pinging 192.16.0.0 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.16.0.0:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PS C:\WINDOWS\system32> ping 192.16.1.0

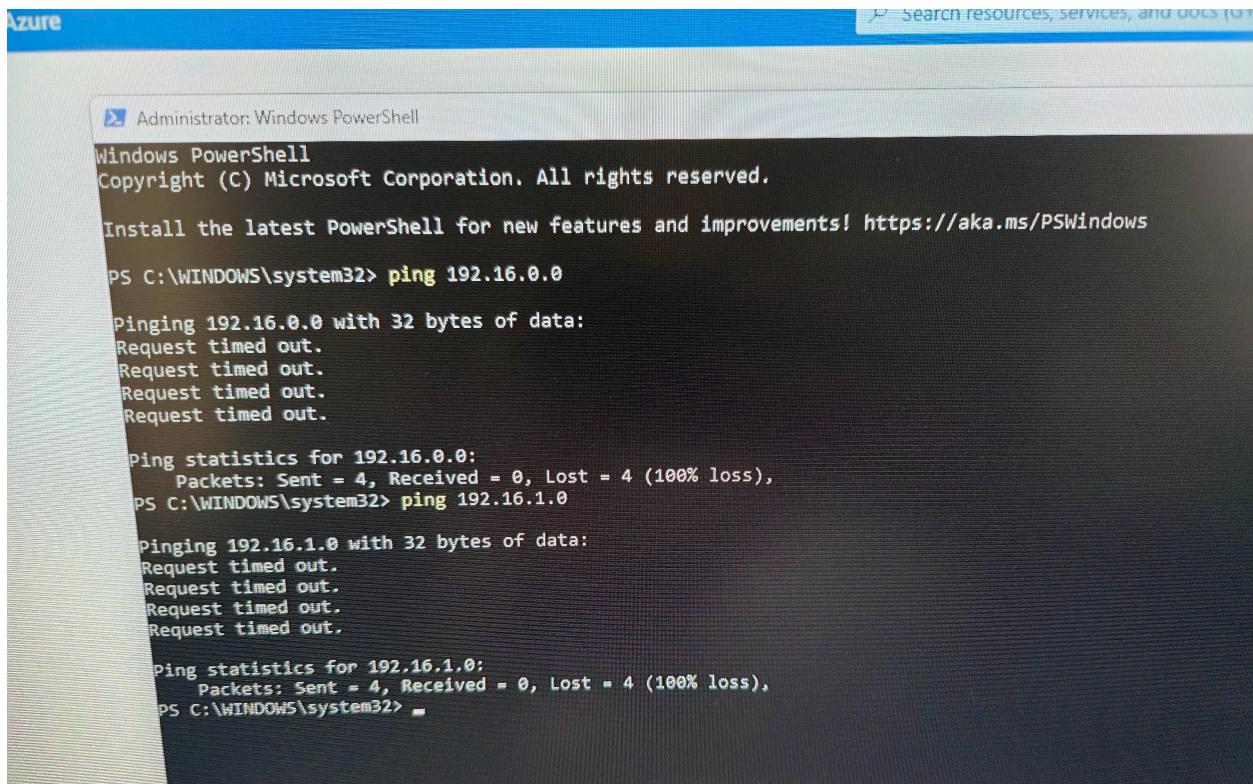
Pinging 192.16.1.0 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.16.1.0:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PS C:\WINDOWS\system32> -

Web-VNet Virtual machine
web-vnet57_z1 Network interface
Web-VNet Resource group
DB-VNet Virtual network

7. Run a ping from your local computer to your target VM that shows ICMP traffic from other sources cannot reach the target VM. Take a screenshot showing the output; include this visual with your answers to this project's questions.



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

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

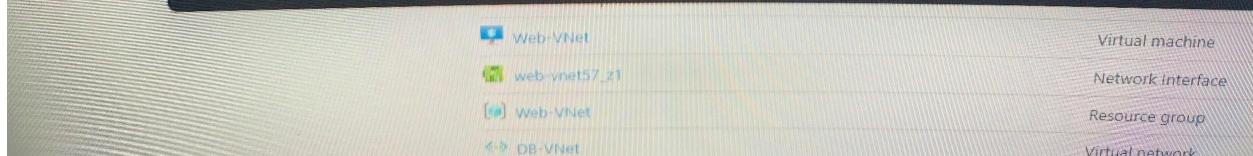
PS C:\WINDOWS\system32> ping 192.16.0.0

Pinging 192.16.0.0 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

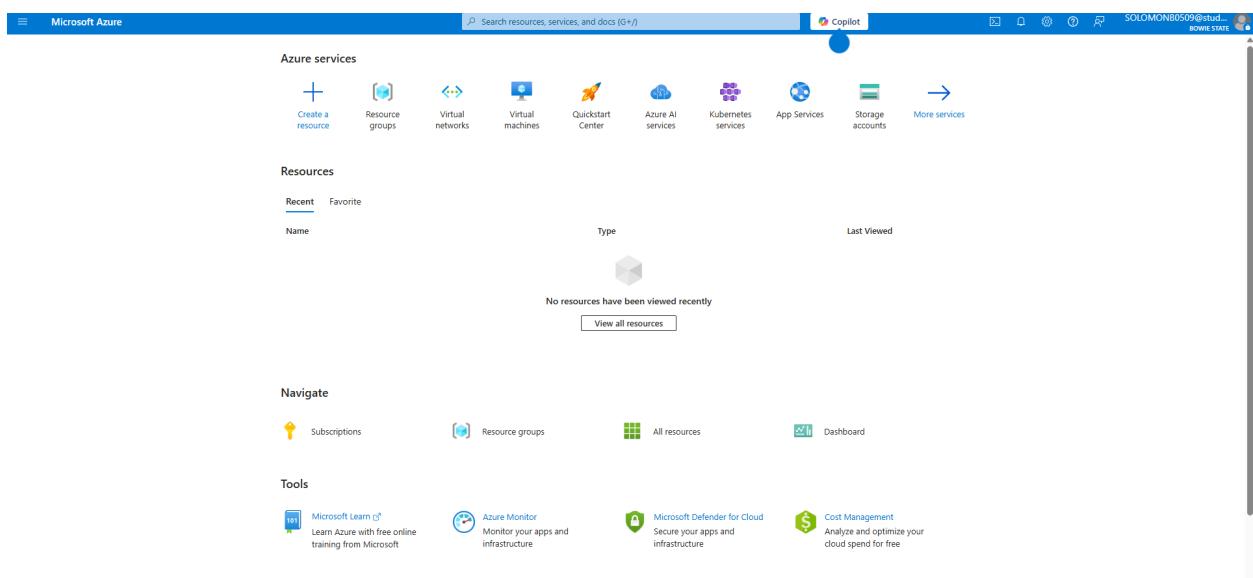
Ping statistics for 192.16.0.0:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\WINDOWS\system32> ping 192.16.1.0

Pinging 192.16.1.0 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.16.1.0:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\WINDOWS\system32> -
```



8. Delete all resources created in this Capstone project. Check through your account to confirm that all related resources have been deleted.



The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with 'Microsoft Azure', a search bar, and user information. Below it is the 'Azure services' section with icons for creating resources, resource groups, virtual networks, virtual machines, Quickstart Center, Azure AI services, Kubernetes services, App Services, storage accounts, and more services. The main area is titled 'Resources' with tabs for 'Recent' (which is selected) and 'Favorite'. It includes filters for 'Name', 'Type', and 'Last Viewed'. A message says 'No resources have been viewed recently' with a 'View all resources' button. Below this is a 'Navigate' section with links to 'Subscriptions', 'Resource groups', 'All resources', and 'Dashboard'. The 'Tools' section contains links to 'Microsoft Learn', 'Azure Monitor', 'Microsoft Defender for Cloud', and 'Cost Management'.