
Assignment: Deploying Cloud Services

Course: IN609: Operating System Concepts

Semester 2, 2021 Otago Polytechnic

Name: Anthony Legg_____ **Student ID: 03007276**_____

This assignment is worth 15%, which includes performing the actual assignment including the planning tasks as part of the instructions!

Deadline: Friday, 17 Sep 2021, 11:59pm

Learning Outcomes

- Investigate cloud and Directory Services
- Execute System Administration Tasks in Diverse Platform

Instructions

In this assignment you will be deploying key infrastructure services for a company named ‘ABC International’ for their newly purchased Azure subscription. You have started your new position as a cloud solution engineer and your task is to help ABC International to slowly migrate to Azure. Your manager assigned you a simple task of creating a skeleton network infrastructure (as shown in Figure 1) which will be expanded gradually to replicate the existing on-premises set up.

The tasks you need to complete are specified in the tasks section below. Your instructors have already created a dedicated resource group for you on Azure. You will find this resource group as IN609OE1-
<yourname> which is the other IN609OE resource group beside the IN609OE1 on your Azure portal under the OP Azure subscription. You might have to delete existing resources from this resource group, if you have any. You will need to use only this resource group for this assignment.

You will need to submit screenshots along with command executions of your deployments as a proof of completion of the tasks.

For any queries, you are welcome to consult your instructors. Please note that we may ask questions related to your submissions after you submit just to make sure that you have understood what you have done. Failing to explain what you have done may result in rejection of the submission.

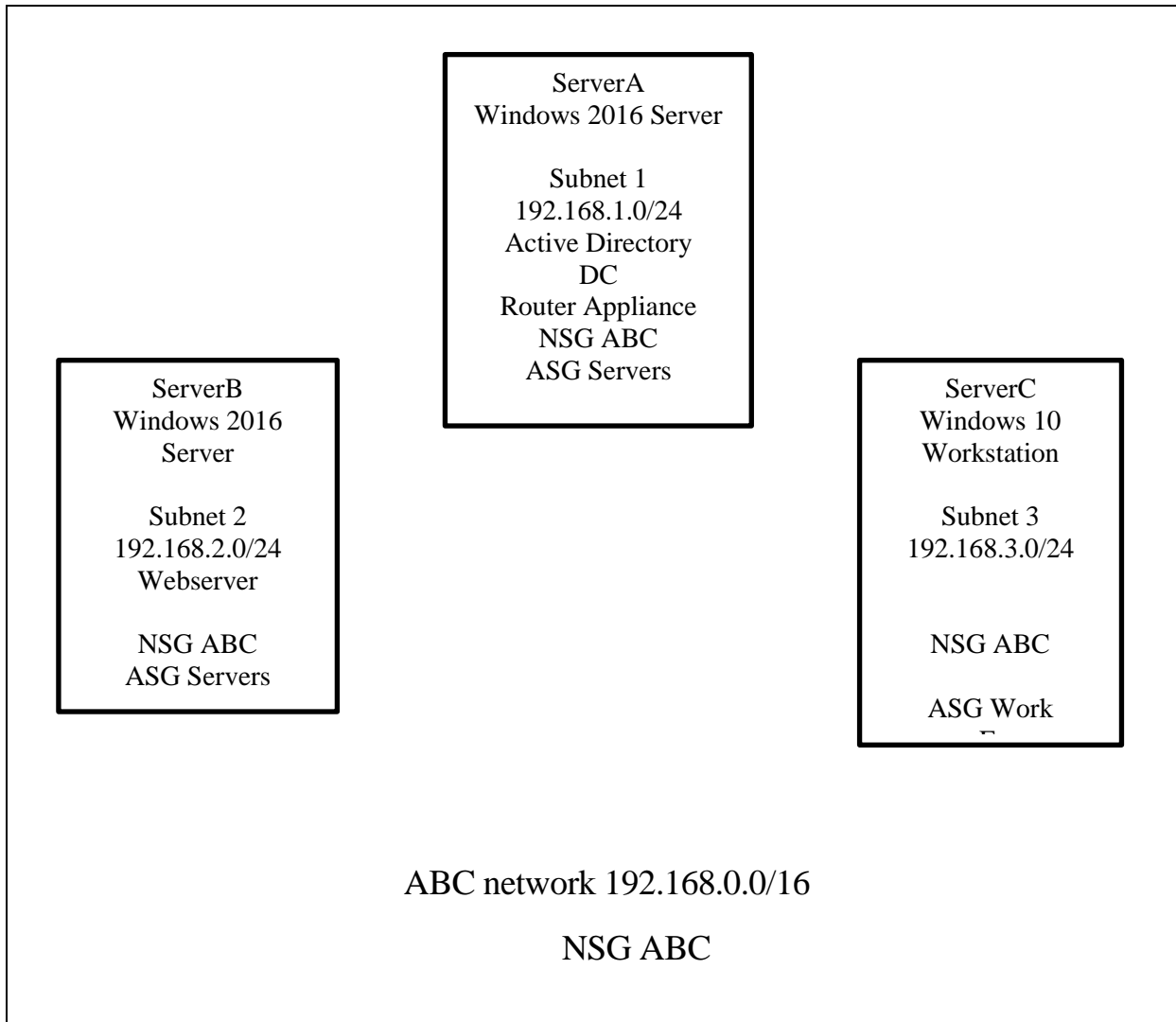


Figure 1: Network Topology

Your tasks will be to do the following:

Task 1: create network topology (2 points)

- a. A virtual network for ABC International vnet<yournetid> with IP Address 192.168.0.0/16

```
# ----- CREATE VIRTUAL NETWORK ----- #  
$vnet = @{  
    Name = 'vnet-leggtc1'  
    ResourceGroupName = 'IN6090E1-LEGGTC1'  
    Location = 'AustraliaEast'  
    AddressPrefix = '192.168.0.0/16'  
}  
$virtualNetwork = New-AzVirtualNetwork @vnet  
$virtualNetwork | Set-AzVirtualNetwork  
  
$Net = $virtualNetwork.Name  
$Loc = $virtualNetwork.Location  
$RGroup = $virtualNetwork.ResourceGroupName
```

Home > IN6090E1-LEGGTC1 > vnet-leggtc1

Virtual network

Search (Ctrl+/) Refresh Move Delete

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Address space

Connected devices

Subnets

DDoS protection

Firewall

Security

Essentials

Resource group (change) : IN6090E1-LEGGTC1

Location : Australia East

Subscription (change) : Azure School of ICT

Subscription ID : ee67cd86-3ab6-4382-81f9-9e62f569ffc6

Tags (change) : Click here to add tags

Address space : 192.168.0.0/16

DNS servers : Multiple

Connected devices

Search connected devices

Device ↑↓	Type ↑↓	IP Address ↑↓	Subnet ↑↓
server-c-vm150	Network interface	192.168.3.4	subnet3
server-b685	Network interface	192.168.2.4	subnet2
server-a265	Network interface	192.168.1.5	subnet1

- b. Subnet subnet1 192.168.1.0/24

Home > Server-A > vnet-leggtc1 > server-a265

server-a265 | IP configurations

Network interface

Search (Ctrl+/) Add Save Discard Refresh

Overview

Activity log

Access control (IAM)

Tags

Settings

IP configurations

DNS servers

Network security group

Properties

IP forwarding settings

IP forwarding : Disabled Enabled

Virtual network : vnet-leggtc1

IP configurations

Subnet * : subnet1 (192.168.1.0/24)

Search IP configurations

Name	IP Version	Type	Private IP address	Public IP address
ipconfig1	IPv4	Primary	192.168.1.5 (Static)	52.237.199.147 (Server-A-ip)

- c. Subnet subnet2 192.168.2.0/24

Home > Server-A > vnet-leggtc1 > server-b685

server-b685 | IP configurations

Network interface

Search (Ctrl+/) << + Add Save Discard Refresh

- Overview
- Activity log
- Access control (IAM)
- Tags

Settings

- IP configurations
- DNS servers
- Network security group
- Properties

IP forwarding settings

IP forwarding

Disabled Enabled

Virtual network

vnet-leggtc1

IP configurations

Subnet *

subnet2 (192.168.2.0/24)

Search IP configurations

Name	IP Version	Type	Private IP address	Public IP address	
ipconfig1	IPv4	Primary	192.168.2.4 (Static)	-	...

d. Subnet subnet3 192.168.3.0/24

Home > vnet-leggtc1 > server-c-vm150

server-c-vm150 | IP configurations

Network interface

Search (Ctrl+/) << + Add Save Discard Refresh

- Overview
- Activity log
- Access control (IAM)
- Tags

Settings

- IP configurations
- DNS servers
- Network security group
- Properties

IP forwarding settings

IP forwarding

Disabled Enabled

Virtual network

vnet-leggtc1

IP configurations

Subnet *

subnet3 (192.168.3.0/24)

Search IP configurations

Name	IP Version	Type	Private IP address	Public IP address	
ipconfig1	IPv4	Primary	192.168.3.4 (Static)	-	...

Submission: command execution/screen shot of created subnets

```

83
84
85 # ----- CREATE A SUBNET THAT HAS THE VIRTUAL NETWORK AS A PARENT ----- #
86 # ----- AND USES THE NEW NETWORK SECURITY GROUP ----- #
87
88 $subnet1 = @{
89     Name = 'subnet1'
90     VirtualNetwork = $virtualNetwork
91     AddressPrefix = '192.168.1.0/24'
92     NetworkSecurityGroup = $NSGABC
93 }
94
95 $subnet2 = @{
96     Name = 'subnet2'
97     VirtualNetwork = $virtualNetwork
98     AddressPrefix = '192.168.2.0/24'
99 }
100
101 $subnet3 = @{
102     Name = 'subnet3'
103     VirtualNetwork = $virtualNetwork
104     AddressPrefix = '192.168.3.0/24'
105 }
106
107 # ----- ADD NEW SUBNET CONFIG TO THE VIRTUAL NETWORK ----- #
108
109 Add-AzVirtualNetworkSubnetConfig @subnet1
110 Add-AzVirtualNetworkSubnetConfig @subnet2
111 Add-AzVirtualNetworkSubnetConfig @subnet3
112
113 $virtualNetwork | Set-AzVirtualNetwork
114
115 $virtualNetwork = Get-AzVirtualNetwork `
116     -Name 'vnet-leggtc1'
117     -ResourceGroupName 'IN6090E1-LEGGTC1'
118

```

Task 2: Create Application Security Groups (ASG) (3 points)

- a. Application security Group 'AsgServers' should have Server A and B.

The screenshot shows the Azure portal interface for a virtual machine named 'Server-A'. The 'Networking' section is active, displaying the network interface 'server-a265'. The IP configuration shows 'ipconfig1 (Primary)' with a public IP of 52.237.199.147 and a private IP of 192.168.1.5. The network interface is connected to the virtual network 'vnet-leggtc1/subnet1'. Under the 'Application security groups' tab, the 'AsgServers' group is listed, and a button 'Configure the application security groups' is visible.

Home > Server-B > server-a265 | Effective security rules

Network interface

Search (Ctrl+/) « Download Refresh

Showing only top 50 security rules in each grid, click Download above to see all.

Associated NSGs: NSG-ABC (Network interface)

Click on a rule row to see the expanded list of prefixes.

NSG-ABC

Inbound rules

Name	Priority	Source	Source Ports	Destination	Destination Ports	Protocol	Access
workstation-web-all	110	0.0.0.0/0,0.0.0.0/0	0-65535	ASGServers	22-22,3389-3389	TCP	Allow
Workstation-RDP-Connections	120	ASGServers	0-65535	ASGWork	3389-3389	TCP	Allow
webserver_block_workstations	140	ASGWork	0-65535	ASGServers	8080-8080	All	Deny
AllowVnetInBound	65000	Virtual network (2 prefixes)	0-65535	Virtual network (2 prefixes)	0-65535	All	Allow
AllowAzureLoadBalancerInBound	65001	Azure load balancer (2 prefixes)	0-65535	0.0.0.0/0,0.0.0.0/0	0-65535	All	Allow
DenyAllInBound	65500	0.0.0.0/0,0.0.0.0/0	0-65535	0.0.0.0/0,0.0.0.0/0	0-65535	All	Deny

Outbound rules

Name	Priority	Source	Source Ports	Destination	Destination Ports	Protocol	Access
Block_Workstation_Webserver_...	150	ASGWork	0-65535	192.168.2.0/24	0-65535	All	Deny
AllowVnetOutBound	65000	Virtual network (2 prefixes)	0-65535	Virtual network (2 prefixes)	0-65535	All	Allow
AllowInternetOutBound	65001	0.0.0.0/0,0.0.0.0/0	0-65535	Internet (257 prefixes)	0-65535	All	Allow
DenyAllOutBound	65500	0.0.0.0/0,0.0.0.0/0	0-65535	0.0.0.0/0,0.0.0.0/0	0-65535	All	Deny

Home > Server-B

Server-B | Networking

Virtual machine

Search (Ctrl+/) « Attach network interface Detach network interface Feedback

server-b685

IP configuration: ipconfig1 (Primary)

Network Interface: server-b685 Effective security rules Troubleshoot VM connection issues Topology

Virtual network/subnet: vnet-leggtc1/subnet2 NIC Public IP: - NIC Private IP: 192.168.2.4 Accelerated networking: Enabled

Inbound port rules Outbound port rules Application security groups Load balancing

ASGServers Configure the application security groups

Home > Server-B > server-b685 | Effective security rules

Network interface

Search (Ctrl+/) « Download Refresh

Showing only top 50 security rules in each grid, click Download above to see all.

Associated NSGs: NSG-ABC (Network interface)

Click on a rule row to see the expanded list of prefixes.

NSG-ABC

Inbound rules

Name	Priority	Source	Source Ports	Destination	Destination Ports	Protocol	Access
workstation-web-all	110	0.0.0.0/0,0.0.0.0/0	0-65535	ASGServers	22-22,3389-3389	TCP	Allow
Workstation-RDP-Connections	120	ASGServers	0-65535	ASGWork	3389-3389	TCP	Allow
webserver_block_workstations	140	ASGWork	0-65535	ASGServers	8080-8080	All	Deny
AllowVnetInBound	65000	Virtual network (2 prefixes)	0-65535	Virtual network (2 prefixes)	0-65535	All	Allow
AllowAzureLoadBalancerInBound	65001	Azure load balancer (2 prefixes)	0-65535	0.0.0.0/0,0.0.0.0/0	0-65535	All	Allow
DenyAllInBound	65500	0.0.0.0/0,0.0.0.0/0	0-65535	0.0.0.0/0,0.0.0.0/0	0-65535	All	Deny

Outbound rules

Name	Priority	Source	Source Ports	Destination	Destination Ports	Protocol	Access
Block_Workstation_Webserver_...	150	ASGWork	0-65535	192.168.2.0/24	0-65535	All	Deny
AllowVnetOutBound	65000	Virtual network (2 prefixes)	0-65535	Virtual network (2 prefixes)	0-65535	All	Allow
AllowInternetOutBound	65001	0.0.0.0/0,0.0.0.0/0	0-65535	Internet (257 prefixes)	0-65535	All	Allow
DenyAllOutBound	65500	0.0.0.0/0,0.0.0.0/0	0-65535	0.0.0.0/0,0.0.0.0/0	0-65535	All	Deny

b. Application security Group 'AsgWork' for workstations.

Home > Server-C-VM

Server-C-VM | Networking

Virtual machine

Search (Ctrl+/) < Attach network interface > Detach network interface < Feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Networking

Connect

Disks

server-c-vm150

IP configuration ⓘ

ipconfig1 (Primary)

Network Interface: server-c-vm150 Effective security rules Troubleshoot VM connection issues Topology ⓘ

Virtual network/subnet: vnet-leggtc1/subnet3 NIC Public IP: - NIC Private IP: 192.168.3.4 Accelerated networking: Disabled

Inbound port rules Outbound port rules Application security groups Load balancing

ASGWork Configure the application security groups

Home > Server-C-VM > server-c-vm150

server-c-vm150 | Effective security rules

Network interface

Search (Ctrl+/) < Download Refresh

Overview

Activity log

Access control (IAM)

Tags

Settings

IP configurations

DNS servers

Network security group

Properties

Locks

Monitoring

Alerts

Metrics

Diagnostic settings

Automation

Tasks (preview)

Export template

Support + troubleshooting

Effective security rules

Effective routes

New Support Request

Showing only top 50 security rules in each grid, click Download above to see all.

Network interface (server-c-vm150)

Associated NSGs ⓘ

NSG-ABC (Network interface)

Click on a rule row to see the expanded list of prefixes.

NSG-ABC

Inbound rules

Name	↑↓	Priority	↑↓	Source	Source Ports	↑↓	Destination	Destination Ports	↑↓	Protocol	↑↓	Access	↑↓
workstation-web-all		110		0.0.0.0/0,0.0.0.0/0	0-65535		ASGServers	22-22,3389-3389		TCP		Allow	
Workstation-RDP-Connections		120		ASGServers	0-65535		ASGWork	3389-3389		TCP		Allow	
webserver_block_workstations		140		ASGWork	0-65535		ASGServers	8080-8080		All		Deny	
AllowVnetInBound		65000		Virtual network (2 prefixes)	0-65535		Virtual network (2 prefixes)	0-65535		All		Allow	
AllowAzureLoadBalancerInBound		65001		Azure load balancer (2 prefixes)	0-65535		0.0.0.0/0,0.0.0.0/0	0-65535		All		Allow	
DenyAllInBound		65500		0.0.0.0/0,0.0.0.0/0	0-65535		0.0.0.0/0,0.0.0.0/0	0-65535		All		Deny	

Outbound rules

Name	↑↓	Priority	↑↓	Source	Source Ports	↑↓	Destination	Destination Ports	↑↓	Protocol	↑↓	Access	↑↓
Block_Workstation_Webserver_...		150		ASGWork	0-65535		192.168.2.0/24	0-65535		All		Deny	
AllowVnetOutBound		65000		Virtual network (2 prefixes)	0-65535		Virtual network (2 prefixes)	0-65535		All		Allow	
AllowInternetOutBound		65001		0.0.0.0/0,0.0.0.0/0	0-65535		Internet (257 prefixes)	0-65535		All		Allow	
DenyAllOutBound		65500		0.0.0.0/0,0.0.0.0/0	0-65535		0.0.0.0/0,0.0.0.0/0	0-65535		All		Deny	

c. Network Security Group NSG-ABC for the organization.

Home >

NSG-ABC

Network security group

Search (Ctrl+/) < Move > Delete Refresh Give feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

Monitoring

Alerts

Diagnostic settings

Logs

NSG flow logs

Automation

Tasks (preview)

Export template

Essentials

Resource group (change) : IN6090E1-LEGGTCT1

Location : Australia East

Subscription (change) : Azure School of ICT

Subscription ID : eee7cd86-3ab6-4382-81f9-9e62f569ffc6

Tags (change) : Click here to add tags

Custom security rules : 3 inbound, 1 outbound

Associated with : 1 subnets, 3 network interfaces

Filter by name Port == all Protocol == all Source == all Destination == all Action == all

Priority ↑↓ Name ↑↓ Port ↑↓ Protocol ↑↓ Source ↑↓ Destination ↑↓ Action ↑↓

Inbound Security Rules

110	workstation-web-all	22,3389	TCP	Any	ASGServers	Allow
120	Workstation-RDP-Connections	3389	TCP	ASGServers	ASGWork	Allow
140	webserver_block_workstations	8080	Any	ASGWork	ASGServers	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Outbound Security Rules

150	Block_Workstation_Webserver_...	Any	Any	ASGWork	192.168.2.0/24	Deny
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Home > NSG-ABC

NSG-ABC | Network interfaces

Network security group

Search (Ctrl+/) Associate Refresh Dissociate

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Search network interfaces

Name ↑↓	Public IP address ↑↓	Private IP address ↑↓	Virtual machine ↑↓
server-a265	52.237.199.147	192.168.1.5	Server-A
server-b685	-	192.168.2.4	Server-B
server-c-vm150	-	192.168.3.4	Server-C-VM

- d. Workstations should not have access to the webserver running on Server B.

Device specifications

Device name: **Server-C-VM**

Processor: Intel(R) Xeon(R) Platinum 8171M CPU @ 2.60GHz

Related settings: [BitLocker settings](#)

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.19042.1237]
(c) Microsoft Corporation. All rights reserved.

C:\Users\leggtc1>ping Server-B

Pinging Server-B.r3rxh15j1utupj4qtbw33lptdg.px.internal.cloudapp.net [192.168.2.4] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\leggtc1>ping Server-A

Pinging Server-A.r3rxh15j1utupj4qtbw33lptdg.px.internal.cloudapp.net [192.168.1.5] with 32 bytes of data:
Reply from 192.168.1.5: bytes=32 time=1ms TTL=128
Reply from 192.168.1.5: bytes=32 time=1ms TTL=128
Reply from 192.168.1.5: bytes=32 time=1ms TTL=128
Reply from 192.168.1.5: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\leggtc1>
```

PC name: **Server-B**

Rename PC

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\leggtc1>ping Server-C-VM

Pinging Server-C-VM.r3rxh15j1utupj4qtbw33lptdg.px.internal.cloudapp.net [192.168.3.4] with 32 bytes of data:
Reply from 192.168.3.4: bytes=32 time=3ms TTL=127
Reply from 192.168.3.4: bytes=32 time=2ms TTL=127
Reply from 192.168.3.4: bytes=32 time=2ms TTL=127
Reply from 192.168.3.4: bytes=32 time=2ms TTL=127

Ping statistics for 192.168.3.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\Users\leggtc1>tracert Server-C-VM

Tracing route to Server-C-VM.r3rxh15j1utupj4qtbw33lptdg.px.internal.cloudapp.net [192.168.3.4]
over a maximum of 30 hops:
  0  <1 ms    *       <1 ms  server-a.internal.cloudapp.net [192.168.1.5]
  1  2 ms     1 ms    4 ms   server-c-vm.internal.cloudapp.net [192.168.3.4]
Trace complete.

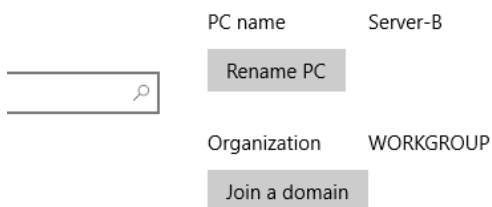
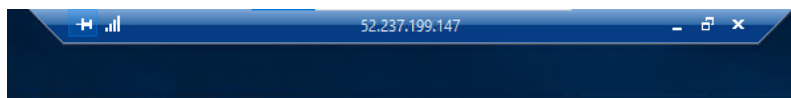
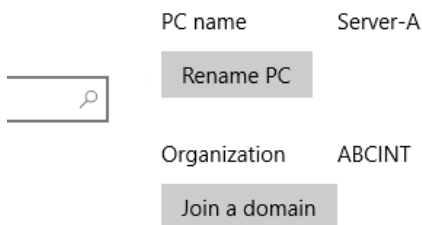
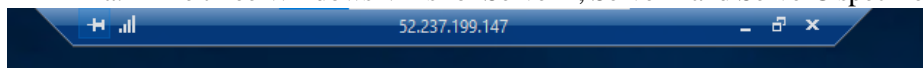
C:\Users\leggtc1>
```


Submission: command execution/screen shot of created security groups

```
0 # ----- THEN CREATE APPLICATION SECURITY GROUP FOR EACH SUBNET ----- #
1
2 $ASGServe = 'ASGServers'
3 $ASGWork = 'ASGwork'
4
5 $AsgServer = New-AzApplicationSecurityGroup `
6     -ResourceGroupName $RGroup
7     -Name $ASGServe
8     -Location $Loc
9
10 $AsgWork = New-AzApplicationSecurityGroup `
11     -ResourceGroupName $RGroup
12     -Name $ASGwork
13     -Location $Loc
14
```

Task 3: Create VMs (3)

- a. The three Windows VMs for ServerA, ServerB and ServerC specified on the Figure 1.



Submission: command execution/screen shot of created VMs

Task 4: Create Routing (3)

- a. You need to create routing to route traffic from ServerB to ServerC via ServerA's router appliance.
- b. Configure appropriate routing rules on the router appliance

Submission: command execution/screen shot of routing table

Home > **ABC-INT-Route** ...
Route table

Search (Ctrl+F) << → Move Delete Refresh Give feedback

Overview

Activity log
Access control (IAM)
Tags
Diagnose and solve problems

Settings

Configuration
Routes
Subnets
Properties
Locks

Monitoring

Alerts
Automation
Tasks (preview)
Export template

Essentials

Resource group (change) : [IN609OE1-LEGGTC1](#) Associations : 2 subnet associations
Location : Australia East
Subscription (change) : [Azure School of ICT](#)
Subscription ID : ee67cd86-3ab6-4382-81f9-9e62f569ffc6
Tags (change) : [Click here to add tags](#)

Routes

Search routes

Name	Address prefix	Next hop type	Next hop IP address
from-server-b	192.168.2.0/24	Virtual appliance	192.168.1.5
from-server-c	192.168.3.0/24	Virtual appliance	192.168.1.5

Subnets

Search subnets

Name	Address range	Virtual network	Security group
subnet2	192.168.2.0/24	vnet-leggtc1	-
subnet3	192.168.3.0/24	vnet-leggtc1	-

Task 5: Active directory Domain service (4)

- ServerA must have active directory domain services enabled.
- ServerB and ServerC must be member of the domain.

I tried to do this using the link provided to a tutorial that was made six years ago. The content was not even slightly helpful. It resulted in the network that was working up to this point to break; Using the information in the link my authentication to the server disappeared.

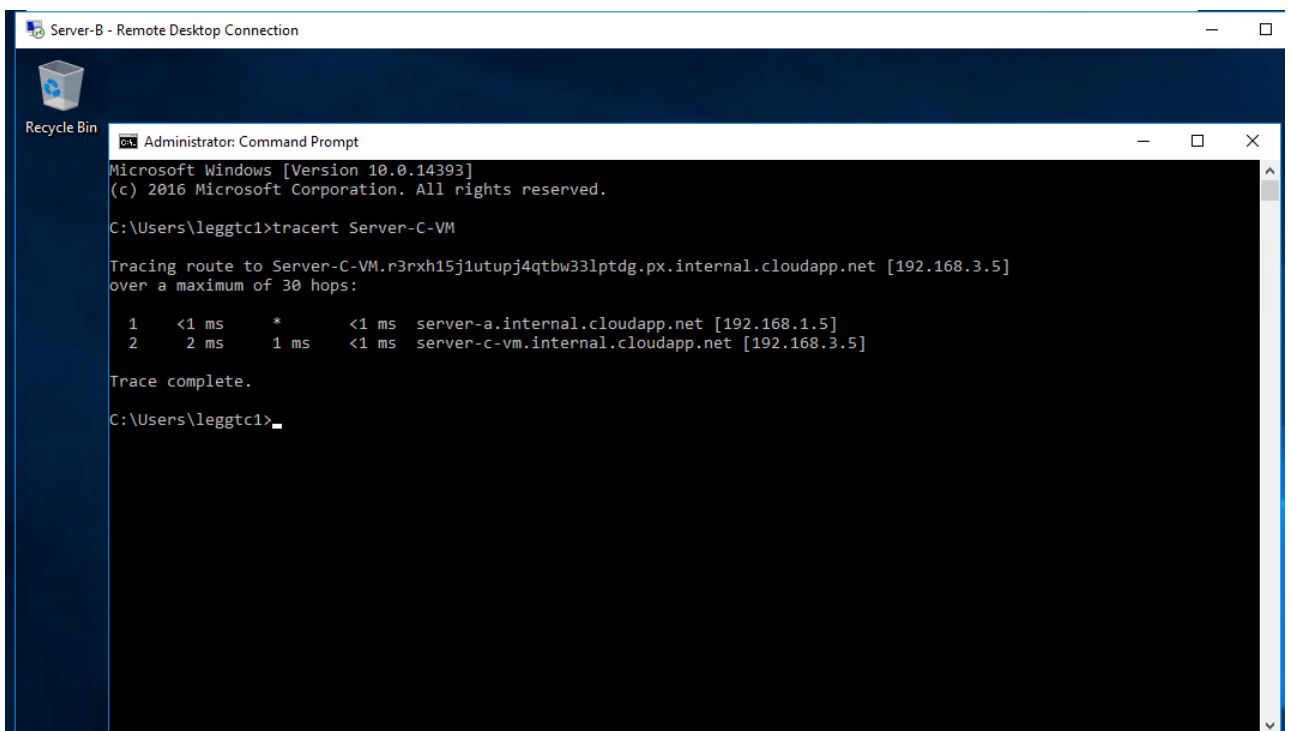
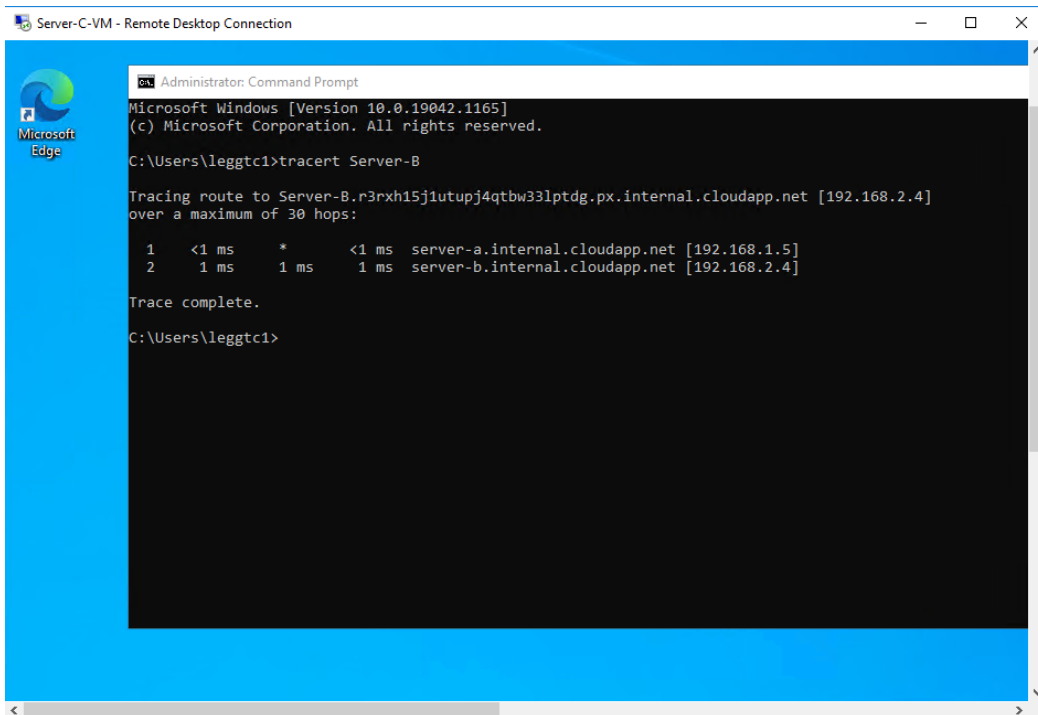
I still have no idea what the hell an active directory even does or why it is needed. Do we need to configure DNS and DHCP?? I have no idea because nothing outside of the completely useless link was provided in class.

Cut my marks if you want, but I did not fail this task because I didn't try. I fail because that's how this assessment has been set up.

Submissions:

- All the commands/scripts for the Tasks.

2. Screenshot of traceroute from ServerB to ServerC and vice versa, This should show the routes traversed.



3. Screen shot of RDP session from ServerB to ServerC and vice versa.
4. Screen shot of ssh session from your local computer to ServerA

-
5. Screen shot of RDP session from your local computer to ServerA on active directory domain.

You will need to include the above in a file and then submit it through Teams-Assignment tab