

5/3/2023

Cloud Computing architecture

Assesment 2



Student: Denis Gori (2010117)
Teacher: Suneth Fernando

Table of Contents

Virtual machines.....	2
Virtual Networks and Network Security Groups.....	4
Additional Exercise	7
Creation Virtual Network	8
Creation Virtual Machines.....	11
Conclusion	21
References.....	21



Virtual machines

Modern cloud computing structures rely heavily on virtual machines (VMs), which provide a practical way of running multiple operating systems and applications on a single physical host. Each VM operates as if it were a separate physical computer, with its own CPU, RAM, and storage capabilities, enabling the deployment of several VMs on a single physical host, resulting in cost savings and better resource utilization. To create a VM, it needs to be allocated access to various resources, such as CPU, RAM, and storage, which are usually provided by the physical host computer and shared among several VMs.

The CPU executes the operating system and application instructions, and each VM is allocated one or more virtual CPUs mapped to actual CPU cores on the host computer, depending on the workload the VM is expected to handle. The operating system and applications store data and instructions that are currently in use in the RAM, and each VM is allocated a certain amount of virtual RAM mapped to actual physical memory on the host system, depending on the workload it is expected to handle. Storage is used to store the VM's operating system, programs, and data, and the files that make up the virtual hard disks are stored on the physical host's storage and associated with the VM.

Once the resources have been allocated, a hypervisor is used to build and operate the VM. A hypervisor is a layer of software that creates a virtualized environment in which multiple VMs can run while abstracting the underlying physical hardware. Type 1 hypervisors, also known as "bare metal" hypervisors, operate directly on the hardware and provide an efficient and secure virtualization environment. Type 2 hypervisors, on the other hand, run on top of an existing operating system and offer a less efficient and less secure virtualization environment.

Virtualization solutions such as VMware vSphere, Microsoft Hyper-V, or KVM can be used to create and manage VMs. The typical stages involved in creating a VM include setting the parameters for the VM, choosing the operating system and applications to be installed, configuring the IP address and network connectivity for the virtual network, creating virtual hard disks and attaching them to the VM, launching the VM, and setting up the software and operating system.

Here are some additional details about virtual machines (VMs) and their use in modern cloud computing structures:

- Virtual machines are a fundamental building block of cloud computing, enabling the efficient sharing and utilization of physical resources among multiple users and applications. By running multiple VMs on a single physical host, cloud providers can achieve economies of scale and offer flexible, on-demand computing resources to their customers.
- Each virtual machine is an isolated and self-contained environment, with its own virtual CPU, RAM, storage, and network interfaces. This allows multiple VMs to coexist on the same physical host without interfering with each other, and enables easy migration and management of VMs across different physical hosts.
- The allocation of CPU, RAM, and storage resources to VMs can be dynamically adjusted based on the workload demand, allowing the cloud provider to optimize resource utilization and minimize wastage. This is typically done through a process called virtual machine placement, which involves selecting the best physical host for each VM based on factors such as resource availability, performance, and cost.
- Virtualization technology has evolved significantly over the past few years, with the emergence of new hypervisor architectures, containerization technologies, and cloud-native platforms. Some of the most popular hypervisor architectures include VMware ESXi, Microsoft Hyper-V, and KVM, while containerization technologies like Docker and Kubernetes offer a lightweight and efficient way of running applications in a virtualized environment.
- Virtual machines can be used for a wide range of purposes, from running legacy applications and operating systems to hosting web servers, databases, and other mission-critical workloads. They can also be used for development and testing, disaster recovery, and other use cases that require flexible and scalable computing resources.
- While virtual machines offer many benefits in terms of efficiency, flexibility, and cost savings, they also introduce some unique challenges and considerations. For example, managing a large number of VMs can be complex and time-consuming, and security and compliance issues can arise when multiple users and applications share the same physical resources. As such, it's important for cloud providers and IT teams to carefully plan and manage their virtualization environments, and to implement appropriate policies and controls to ensure the security and availability of their systems and data.

Virtual Networks and Network Security Groups

Software-defined networks known as virtual networks (vNets) are used in cloud computing to build unique virtualized network environments. These networks provide a way to connect and isolate resources like virtual machines (VMs), containers, and other cloud resources. The virtual switches, routers, and firewalls that connect these resources are under the management of the cloud provider's infrastructure. Regardless of their location or availability zone inside the cloud environment, resources can interact within the same vNet and users can customise their network topology and security regulations.

The key advantage of setting up a vNet is improved security. A virtual network's ability to logically isolate its resources from those of other virtual networks and the internet overall improves security. The management of traffic entering and exiting virtual network resources can be done using network security groups (NSGs). Additionally, hybrid cloud installations can be made by connecting cloud resources to on-premises infrastructure or other cloud environments using virtual networks. In order to scale vNets to meet business requirements, subnets can be added or removed, IP address ranges can be changed, and routing and security configurations can be made.

In cloud computing, NSGs are a crucial part of the network security system. They manage inbound and outbound traffic to and from resources within a virtual network. By developing security policies that may be applied to a virtual machine or a subnet, NSGs offer a method of controlling resource access and traffic flow. Based on source and destination IP addresses, protocols, ports, and traffic direction, these rules can accept or reject traffic. Cloud resources are more secure thanks to NSGs, which lowers the risk of hacker attacks and data breaches. They may also be used to enforce compliance and security standards.

In addition to other network security measures like firewalls or virtual private networks (VPNs), NSGs can be utilised. It is possible to apply different NSGs to different subnets or virtual machines within the same virtual network, allowing security policies to be tailored to apply to certain resources or groups of resources within the virtual network. It is simple to update or modify NSG rules, but security and compliance must be adjusted as necessary.

In conclusion, vNets and NSGs are essential elements of the infrastructure for cloud computing. They offer scalable, flexible, and hybrid cloud deployments while guaranteeing that cloud resources are secure and tailored to the particular requirements of enterprises or organisations. They also give secure and adaptable solutions to connect cloud resources. Cloud architecture can be strengthened even more by combining NSGs with other network security features, which also improve network performance and ensure security compliance. security policy and manage the traffic through it.

An essential part of the cloud computing architecture, virtual networks (vNets) let users build and administer software-defined networks. Users can introduce resources like virtual machines or containers to the subnet ranges by defining a subnet and an IP address space, and these resources can communicate with one another within the same vNet. Virtual switches, routers, and firewalls that are under the management of the cloud provider's infrastructure connect the resources. Users have the ability to create their own private network topology and security policies that can be tailored to match their unique needs.

Security is one of the main benefits of having a virtual network. The logical isolation of resources within a vNet from other virtual networks and the public internet adds another degree of security for cloud resources. Network security groups (NSGs) can be used to regulate traffic entering and departing the virtual network's resources. This lowers the risk of unauthorised access or data breaches and enables users to control access to particular apps or categories of data.

The ability to connect cloud resources to on-premises infrastructure or other cloud environments is another advantage of employing virtual networks. Using a VPN gateway, users can connect their vNet to their on-premises network securely and connect multiple vNets to each other within the same cloud environment or across different cloud environments. By doing this, users can build a hybrid cloud environment that gives them access to cloud computing benefits without giving up control of their on-premises infrastructure.

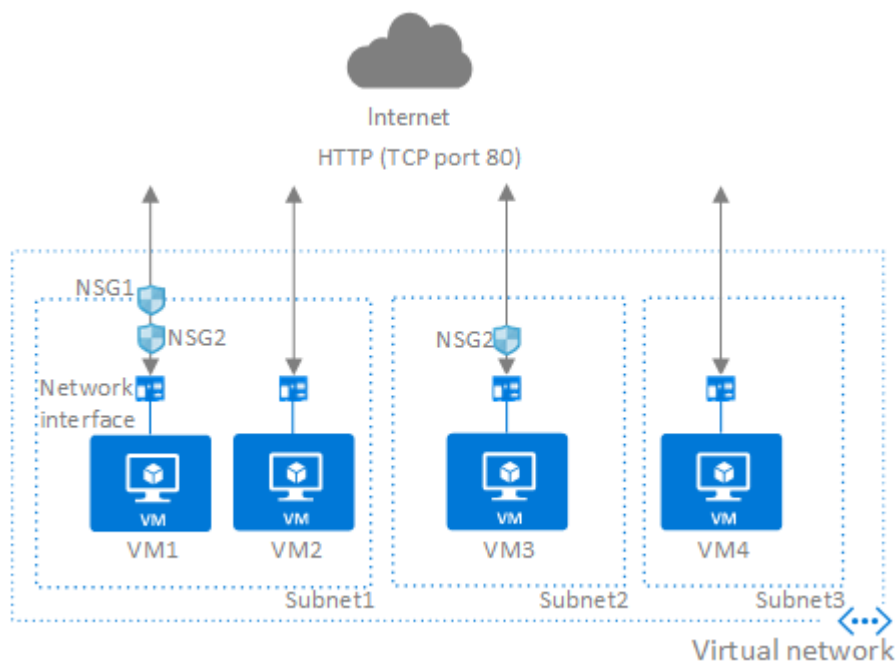
Virtual networks can be scaled to meet a company's or organization's demands. You can change IP address ranges, add or delete subnets, and tweak routing and security settings as necessary. With this flexibility, users can design a network architecture that is both flexible enough to suit changing business needs and optimised for their particular use case.

Here are a few instances where virtual networks have been utilised in various cloud computing scenarios:

- **Development and testing:** To reduce the danger of interference or errors, developers might set up virtual networks to separate their development and testing environments from production settings. Additionally, they can use NSGs to control traffic and guarantee that only essential traffic is permitted to pass between resources.
- **Disaster recovery:** In the event of a disaster, virtual networks can be utilised to replicate essential workloads and resources to a different location. In the event of an outage, this enables speedy recovery and little downtime.
- **Big data and analytics:** To connect big data and analytics applications to data sources, virtual networks can be utilised. This enables quick and safe data processing and analysis.

- Applications with many tiers: Subnets can be utilised to divide application tiers using virtual networks. This makes it possible to handle application traffic more easily and with higher security.

In conclusion, virtual networks are crucial components of cloud architecture because they offer a flexible and safe approach to connect cloud resources. They enable customers to build a scalable, adaptable, and logically segregated network architecture that is compatible with hybrid cloud deployment, guaranteeing that cloud resources are secure and tailored to a company's particular requirements.



Additional Exercise

In this experiment, we'll deploy a virtual network and two virtual computers using Azure. Microsoft's Azure public cloud platform offers a variety of services, such as PaaS, IaaS, and managed database services.

Without the use of actual hardware, we can easily create and manage our virtual machines in the cloud with Azure. This gives us the ability to scale up or down our resources as necessary while also enabling us to quickly and effectively deploy our apps and services.

To get things going, we'll build a virtual network that will support our virtual computers. To separate and safeguard our resources, we can set up our own private IP address space, subnets, and security guidelines. This gives us a network environment that is secure and flexible in which to deploy our applications.

We can deploy our virtual machines inside of our established virtual network. Azure offers a large selection of virtual machine images that we may use to quickly deploy virtual machines that are already configured for various operating systems and applications. As an alternative, we can build our own unique virtual machine images with our own software and settings.

A powerful and adaptable cloud computing solution that enables us to quickly and easily deploy our applications and services while also giving us the scalability and security we need to meet our changing business needs is provided by using Azure to deploy virtual networks and virtual machines.



Creation Virtual Network

When using Azure, you can create a Virtual Network by selecting it from the list of available

Microsoft Azure

Search resources, services, and docs (G+/I)

All services > Virtual networks >

Create virtual network

Basics Security IP addresses Tags Review + create

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation.

[Learn more.](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * Azure for Students

Resource group * (New) myRGVNet

[Create new](#)

Instance details

Virtual network name * vnet1

Region ⓘ * (US) East US

[Deploy to an edge zone](#)

Previous Next Review + create

services.

In this instance, the choice was made to use Azure for Students, and subsequently, a resource group called myRGVNet was created. The virtual network was then given the identifier name of vnet1.

Microsoft A...

Search resources, services, and docs (G+)

2112906@stu
UNIVERSITY OF W

[All services](#) > [Virtual networks](#) >

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 an IP address space

10.0.0.0/16

+ Add a subnet

10.0.0.0 - 10.0.255.255 (65536 addresses)

Subnets	IP address range	Size	NAT gateway
default	10.0.0.0 - 10.0.0.255	/24 (256 addresses)	-

A NAT gateway is recommended for outbound internet access from subnets. Edit the subnet to add a NAT gateway. [Learn more](#)

Previous

Next

Review + create



Following that, there are no modifications made in the security section. As depicted in the provided image, Azure automatically assigns a default IP range.

Microsoft A...

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



21129
UNIVER

[All services](#) > [Virtual networks](#) >

Create virtual network

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

[View automation template](#)

Basics

Subscription	Azure for Students
Resource Group	myRGVNet
Name	vnet1
Region	East US

Security

Azure Bastion	Disabled
Azure Firewall	Disabled
Azure DDoS Network Protection	Disabled

IP addresses

Address space	10.0.0.0/16 (65536 addresses)
Subnet	default (10.0.0.0/24) (256 addresses)

Tags

Previous

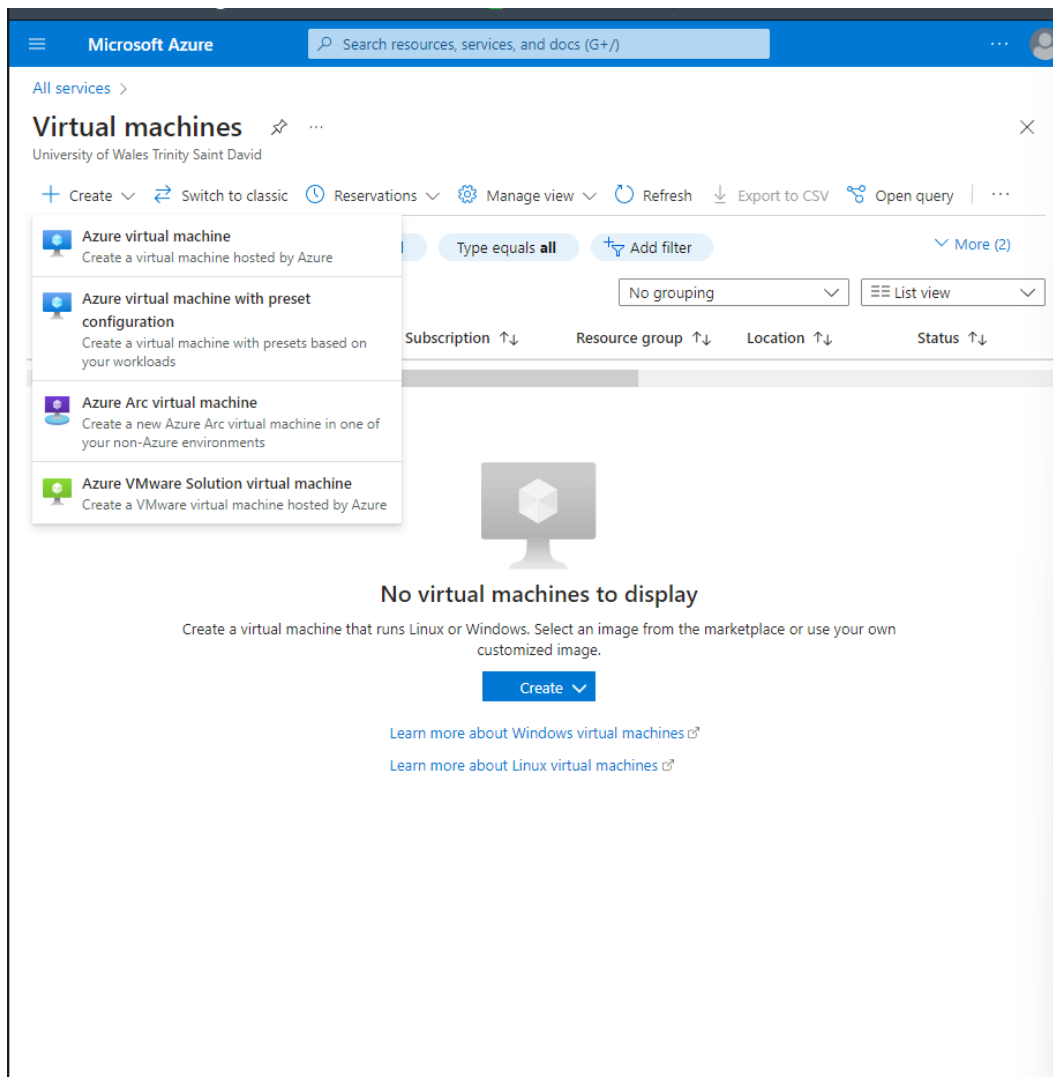
Next

Create

UWISD
London

After verifying that all settings are correct, we can proceed with the creation of the Virtual Network.

Creation Virtual Machines



To create virtual machines in Microsoft Azure, simply click on the virtual machine option and proceed to create as many machines as required. This can be done by selecting the Azure virtual machine option to start the creation process.

All services > Virtual machines >

Create a virtual machine ...

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

i This subscription may not be eligible to deploy VMs of certain sizes in certain regions.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ Azure for Students
Resource group * ⓘ myRGVNet
[Create new](#)

Instance details

Virtual machine name * ⓘ vm1 ✓
Region * ⓘ (US) East US
Availability options ⓘ No infrastructure redundancy required
Security type ⓘ Standard
Image * ⓘ Windows Server 2019 Datacenter - x64 Gen2
[See all images](#) | [Configure VM generation](#)
VM architecture ⓘ
☐ Arm64
☒ x64

For the virtual machine creation process in Microsoft Azure, the first two steps of the virtual network creation are kept the same in the Basics section. The machine is then given a name, such as vm1 for the first one, and the preferred image is chosen, in this case, Windows Server 2019.

Microsoft A...

Search resources, services, and docs (G+)



2112906@student...
UNIVERSITY OF WALES TR

[All services](#) > [Virtual machines](#) >

Create a virtual machine

VM architecture ⓘ

☐ Arm64

☒ x64

 Arm64 is not supported with the selected image.

Run with Azure Spot discount ⓘ

☐

Size * ⓘ

Standard_B1ms - 1 vcpu, 2 GiB memory (US\$17.96/month) ▾

[See all sizes](#)

Administrator account

Username * ⓘ

azureuser ✓

Password * ⓘ

..... ✓

Confirm password * ⓘ

..... ✓

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ

☐ None

☒ Allow selected ports

Select inbound ports *

RDP (3389) ▾

 **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.

Review + create

< Previous

Next : Disks >

 Give fee

London

Next, a username and password are added to enable access to the virtual machine.

Microsoft A...Search resources, services, and docs (G+)

2112906@student.university of wales tr

[All services](#) > [Virtual machines](#) >

Create a virtual machine

BasicsDisksNetworkingManagementMonitoringAdvancedTagsReview + 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 *

(new) vm1-vnet

Create new

Subnet *

(new) default (10.0.0.0/24)

Public IP

(new) vm1-ip

Create new

NIC network security group

None

☒ Basic

Advanced

Public inbound ports *

None

☒ Allow selected ports

Select inbound ports *

RDP (3389)

 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.

Delete public IP and NIC when VM is deleted

☐

Review + create

< Previous

Next : Management >

 Give feedl

Under the Networking section, the virtual network vm1-vnet and subnet default (10.0.0.0/24) were selected, along with the public IP address named vm1-ip.

Microsoft A...

Search resources, services, and docs (G+)

2112906@student.u
UNIVERSITY OF WALES TRI

[All services](#) > [Virtual machines](#) >

Create a virtual machine ...

Validation passed

1 X Standard B1ms
by Microsoft
[Terms of use](#) | [Privacy policy](#)

Subscription credits apply ⓘ
0.0246 USD/hr
[Pricing for other VM sizes](#)

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

You have set RDP port(s) 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 for Students
Resource group	myRGVNet
Virtual machine name	vm1
Region	East US
Availability options	No infrastructure redundancy required
Security type	Standard
Image	Windows Server 2019 Datacenter - Gen2
VM architecture	x64
Size	Standard B1ms (1 vcpu, 2 GiB memory)
Username	azureuser
Public inbound ports	RDP

Create

< Previous

Next >

[Download a template for automation](#)

[Give feed](#)

Once all the settings have been configured, click on the "Review + create" button. Azure will then check if everything is set up correctly and will provide information on whether the virtual machine can be created successfully.

Microsoft A...

Search resources, services, and docs (G+)

2112906@student.U
UNIVERSITY OF WALES TR

[All services](#) > [Virtual machines](#) >

Create a virtual machine

⚠

Changing Basic options may reset selections you have made. Review all options prior to creating the virtual machine.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Azure for Students

Resource group *

myRGVNet

Create new

Instance details

Virtual machine name *

vm2

Region *

(US) East US

Availability options

No infrastructure redundancy required

Security type

Standard

Image *

Windows 10 Pro, version 22H2 - x64 Gen2

See all images | Configure VM generation

VM architecture

Arm64

☒ x64

Arm64 is not supported with the selected image.

Run with Azure Spot discount

☐

Size *

Standard_B1ms - 1 vcpu, 2 GiB memory (US\$15.11/month)

See all sizes

Administrator account

Review + create

< Previous

Next : Disks >

Give feed

This is the process for setting up the second virtual machine, which will be used to establish a connection within the Virtual Network. The settings for this machine are similar to those for the first machine, with the exception of the name of the virtual machine, which is vm2, and the operating system used, which is Windows 10 Pro, as it will be used as a client.

Microsoft A...

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

2112906@student.
UNIVERSITY OF WALES TR

[All services](#) > [Virtual machines](#) >

Create a virtual machine

✓ Validation passed

Basics

Disks

Networking

Management

Monitoring

Advanced

Tags

Review + create

Cost given below is an estimate and not the final price. Please use [Pricing calculator](#) for all your pricing needs.

Price

1 X Standard B1ms
by Microsoft
[Terms of use](#) | [Privacy policy](#)

Subscription credits apply ⓘ
0.0246 USD/hr
[Pricing for other VM sizes](#)

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

⚠ You have set RDP port(s) 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 for Students

Resource group

myRGVNet

Virtual machine name

vm2

Create

< Previous

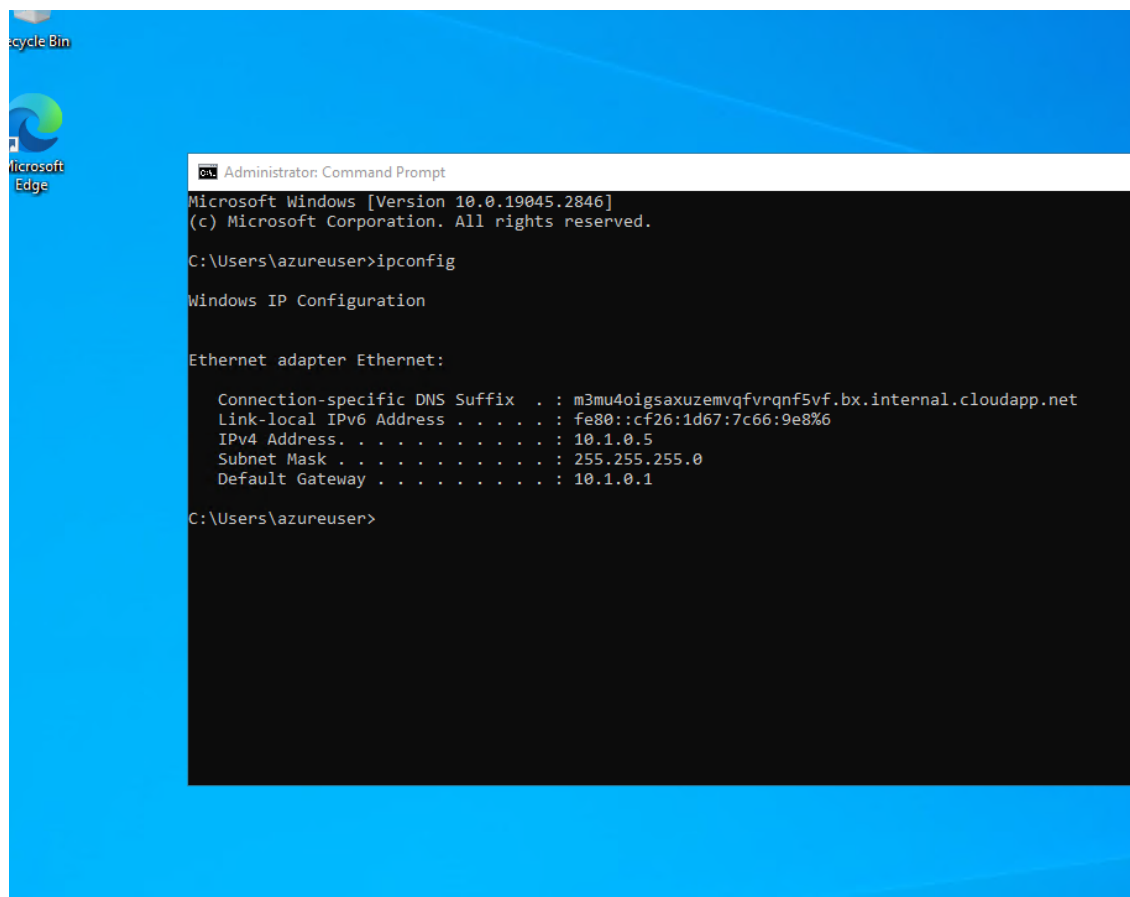
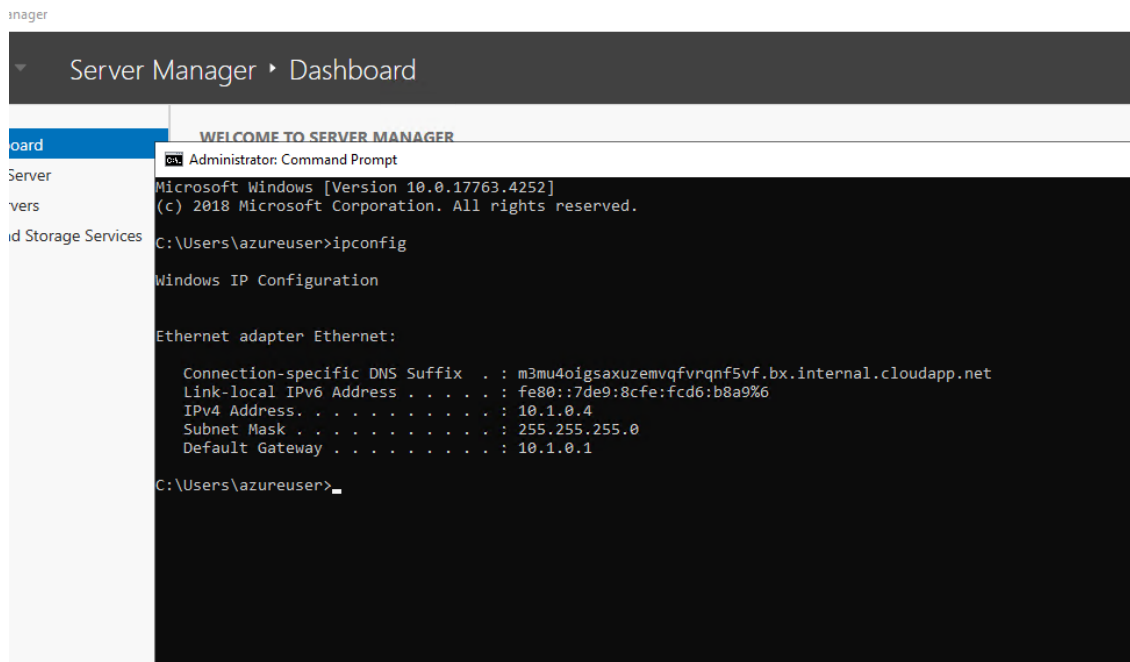
Next >

Download a template for automation

Give feedback

London

To see if Azure allows you to successfully construct the second machine, client, press review and create.



The following images display the default IP addresses assigned to the virtual machines. The first machine, which functions as the server, has been assigned the IP address 10.1.0.4, while the second machine, which serves as the client, has been assigned the IP address 10.1.0.5.

Administrator: Windows PowerShell

Windows PowerShell

Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell <https://aka.ms/pscore6>

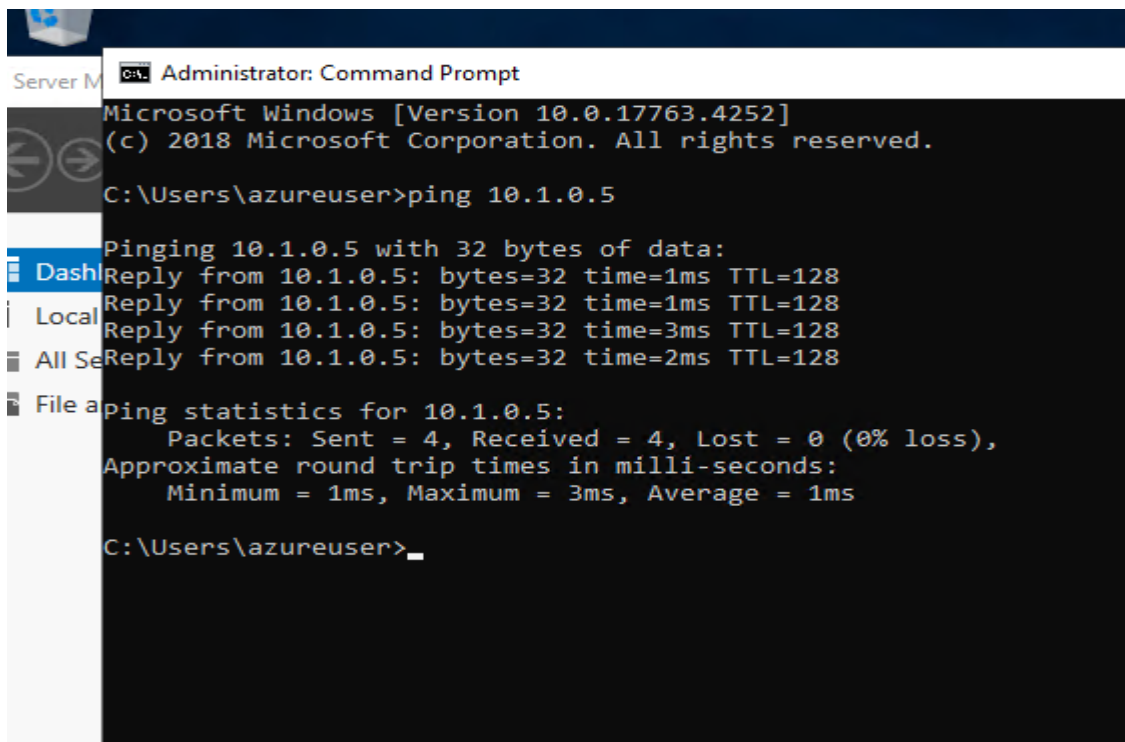
```
PS C:\Users\azureuser> New-NetFirewallRule -DisplayName "Allow ICMPv4-In" -Protocol ICMPv4
```

```
Name                           : {65039308-f549-4ca6-933d-0d87d6d9148a}
DisplayName                     : Allow ICMPv4-In
Description                     :
DisplayGroup                    :
Group                           :
Enabled                         : True
Profile                         : Any
Platform                       : {}
Direction                      : Inbound
Action                          : Allow
EdgeTraversalPolicy             : Block
LooseSourceMapping              : False
LocalOnlyMapping                : False
Owner                           :
PrimaryStatus                   : OK
Status                         : The rule was parsed successfully from the store. (65536)
EnforcementStatus               : NotApplicable
PolicyStoreSource               : PersistentStore
PolicyStoreSourceType           : Local
RemoteDynamicKeywordAddresses  :
```

```
PS C:\Users\azureuser> █
```

London

In this step, we will enable the Internet Control Message Protocol (ICMP) port by typing the command "New-NetFirewallRule -DisplayName "Allow ICMPv4-In" -Protocol ICMPv4" in the PowerShell of the client machine. This will allow inbound connections.



Administrator: Command Prompt

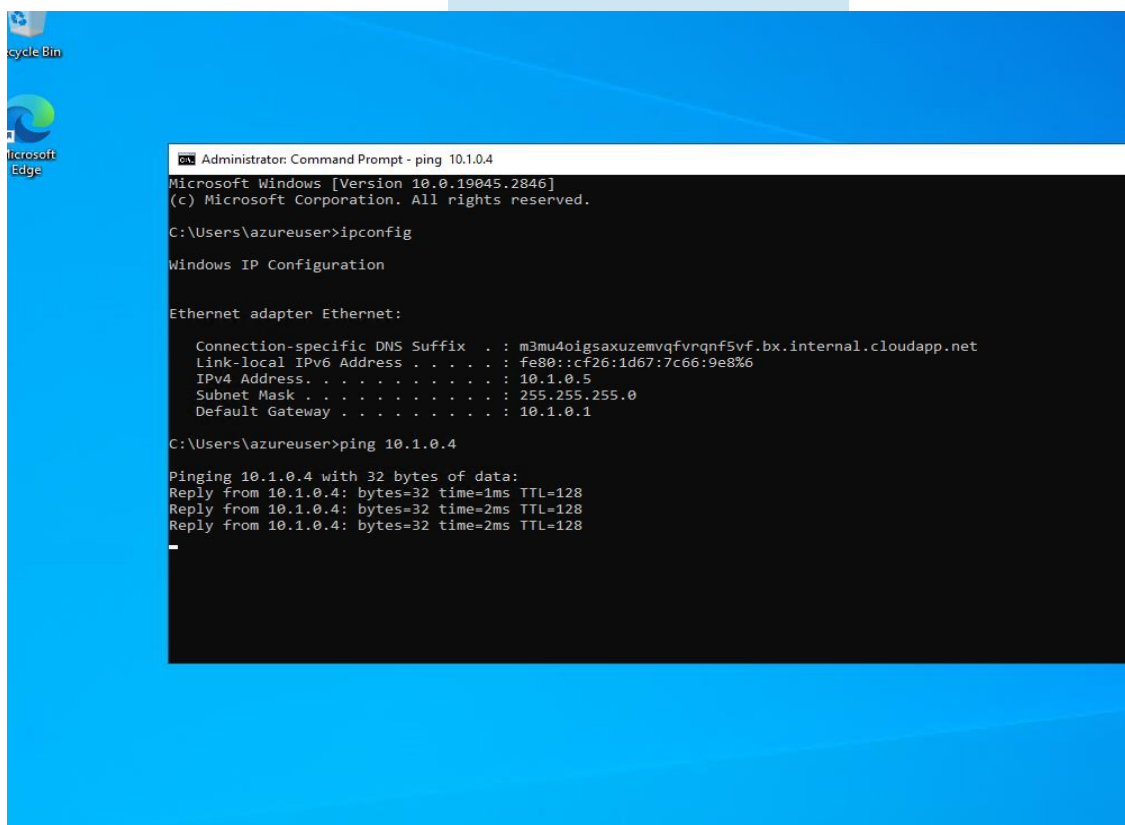
```
Microsoft Windows [Version 10.0.17763.4252]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\azureuser>ping 10.1.0.5

Pinging 10.1.0.5 with 32 bytes of data:
Reply from 10.1.0.5: bytes=32 time=1ms TTL=128
Reply from 10.1.0.5: bytes=32 time=1ms TTL=128
Reply from 10.1.0.5: bytes=32 time=3ms TTL=128
Reply from 10.1.0.5: bytes=32 time=2ms TTL=128

Ping statistics for 10.1.0.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 1ms

C:\Users\azureuser>
```



Administrator: Command Prompt - ping 10.1.0.4

```
Microsoft Windows [Version 10.0.19045.2846]
(c) Microsoft Corporation. All rights reserved.

C:\Users\azureuser>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : m3mu4oigsaxuzemvqfvrqnf5vf.bx.internal.cloudapp.net
    Link-local IPv6 Address . . . . . : fe80::cf26:1d67:7c66:9e8%6
    IPv4 Address. . . . . : 10.1.0.5
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.1.0.1

C:\Users\azureuser>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
Reply from 10.1.0.4: bytes=32 time=2ms TTL=128
Reply from 10.1.0.4: bytes=32 time=2ms TTL=128

C:\Users\azureuser>
```

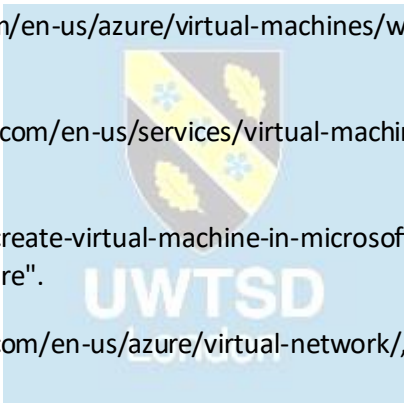
After successfully enabling the ICMP port on the client machine by running the command "New-NetFirewallRule -DisplayName "Allow ICMPv4-In" -Protocol ICMPv4" in PowerShell, both the server and client machines were able to successfully ping themselves.

Conclusion

We learnt how to use Microsoft Azure to deploy a virtual network and two virtual machines in this project. We began by constructing the virtual network and giving it a name, then we created the virtual machines, gave them names, and selected the proper operating systems. We also set up the network settings for the virtual machines, including the virtual network, subnet, and public IP address.

The ICMP protocol was then enabled to accept incoming connections, and the link between the virtual computers was successfully tested. We acquired hands-on experience with the Azure platform and learnt how to put up a basic virtual network infrastructure using virtual machines through this project. Overall, this study lays a solid basis for anyone who want to learn more about cloud computing and virtualization using Microsoft Azure.

References

- 
- [1] M. A. <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/>, "Get started with Azure Virtual Machines".
- [2] b. M. A. <https://azure.microsoft.com/en-us/services/virtual-machines/>, "What is Azure Virtual Machines?".
- [3] b. L. <https://www.lifewire.com/create-virtual-machine-in-microsoft-azure-4164296>, "How to Create a Virtual Machine in Microsoft Azure".
- [4] b. M. A. <https://docs.microsoft.com/en-us/azure/virtual-network/>, "Azure Virtual Network Documentation".
- [5] ". p. f. A. v. m. M. A. <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/best-practices>, "Best practices for Azure virtual machines".