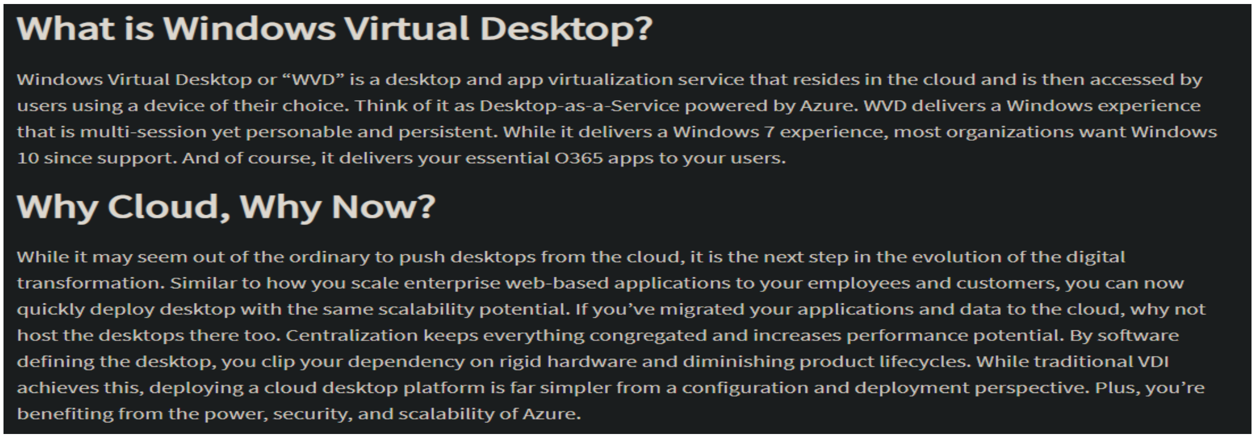
Setup Windows Virtual Desktop in Azure – Part 1

In this post, I will go through various steps to setup, configure and deploy virtual desktops in cloud using Azure and On Premises AD.

PART 1:

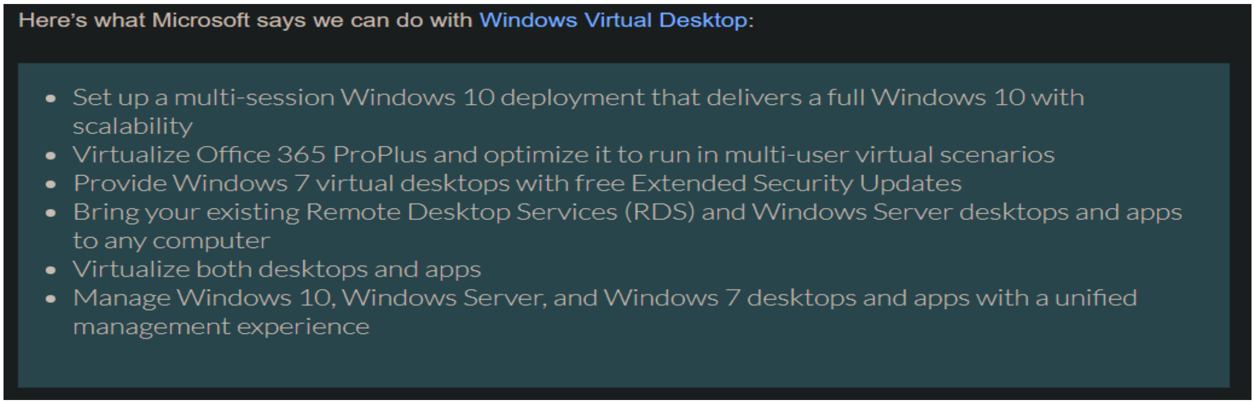


What is Windows Virtual Desktop?

Windows Virtual Desktop or "WVD" is a desktop and app virtualization service that resides in the cloud and is then accessed by users using a device of their choice. Think of it as Desktop-as-a-Service powered by Azure. WVD delivers a Windows experience that is multi-session yet personable and persistent. While it delivers a Windows 7 experience, most organizations want Windows 10 since support. And of course, it delivers your essential O365 apps to your users.

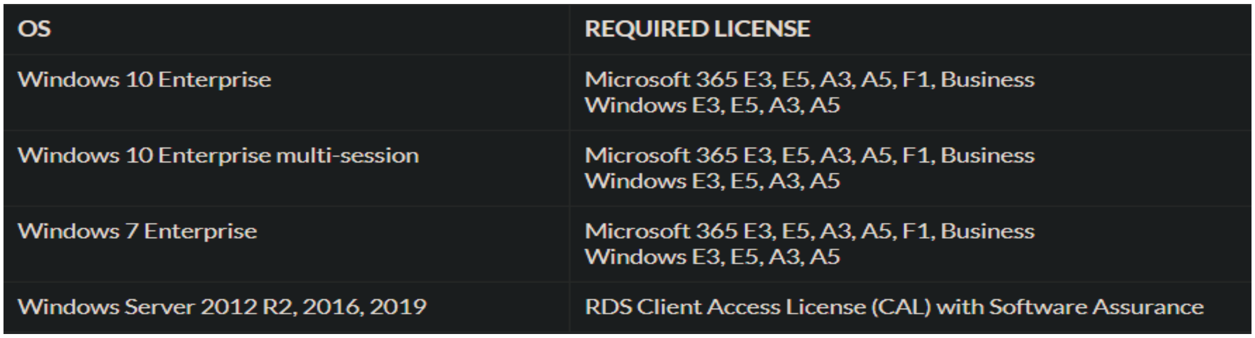
Why Cloud, Why Now?

While it may seem out of the ordinary to push desktops from the cloud, it is the next step in the evolution of the digital transformation. Similar to how you scale enterprise web-based applications to your employees and customers, you can now quickly deploy desktop with the same scalability potential. If you've migrated your applications and data to the cloud, why not host the desktops there too. Centralization keeps everything congregated and increases performance potential. By software defining the desktop, you clip your dependency on rigid hardware and diminishing product lifecycles. While traditional VDI achieves this, deploying a cloud desktop platform is far simpler from a configuration and deployment perspective. Plus, you're benefiting from the power, security, and scalability of Azure.

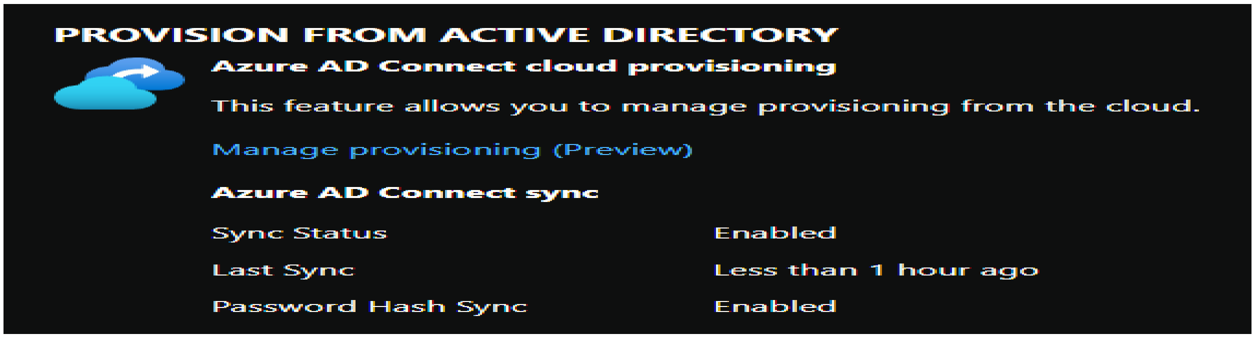


Here's what Microsoft says we can do with Windows Virtual Desktop:

- Set up a multi-session Windows 10 deployment that delivers a full Windows 10 with scalability
- Virtualize Office 365 ProPlus and optimize it to run in multi-user virtual scenarios
- Provide Windows 7 virtual desktops with free Extended Security Updates
- Bring your existing Remote Desktop Services (RDS) and Windows Server desktops and apps to any computer
- Virtualize both desktops and apps
- Manage Windows 10, Windows Server, and Windows 7 desktops and apps with a unified management experience



OS	REQUIRED LICENSE
Windows 10 Enterprise	Microsoft 365 E3, E5, A3, A5, F1, Business Windows E3, E5, A3, A5
Windows 10 Enterprise multi-session	Microsoft 365 E3, E5, A3, A5, F1, Business Windows E3, E5, A3, A5
Windows 7 Enterprise	Microsoft 365 E3, E5, A3, A5, F1, Business Windows E3, E5, A3, A5
Windows Server 2012 R2, 2016, 2019	RDS Client Access License (CAL) with Software Assurance



PROVISION FROM ACTIVE DIRECTORY

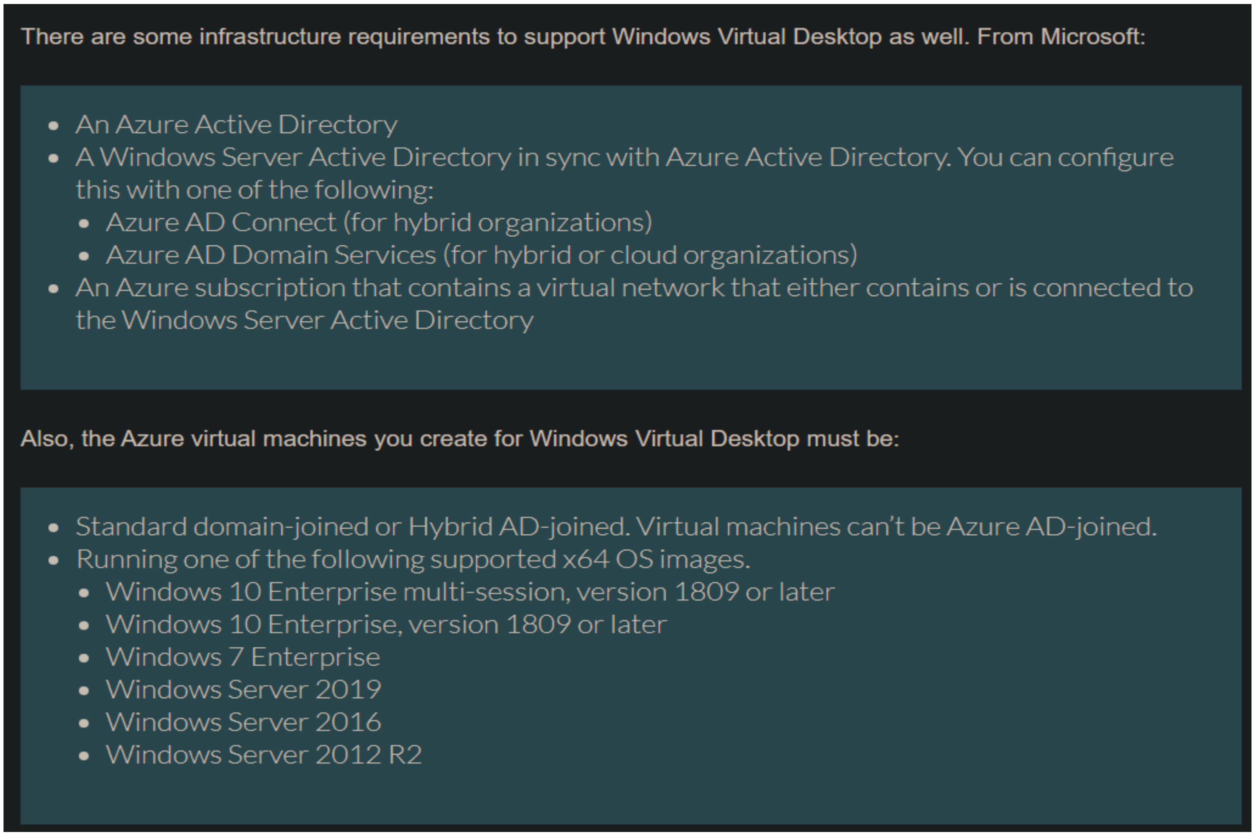
Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

Manage provisioning (Preview)

Azure AD Connect sync

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled

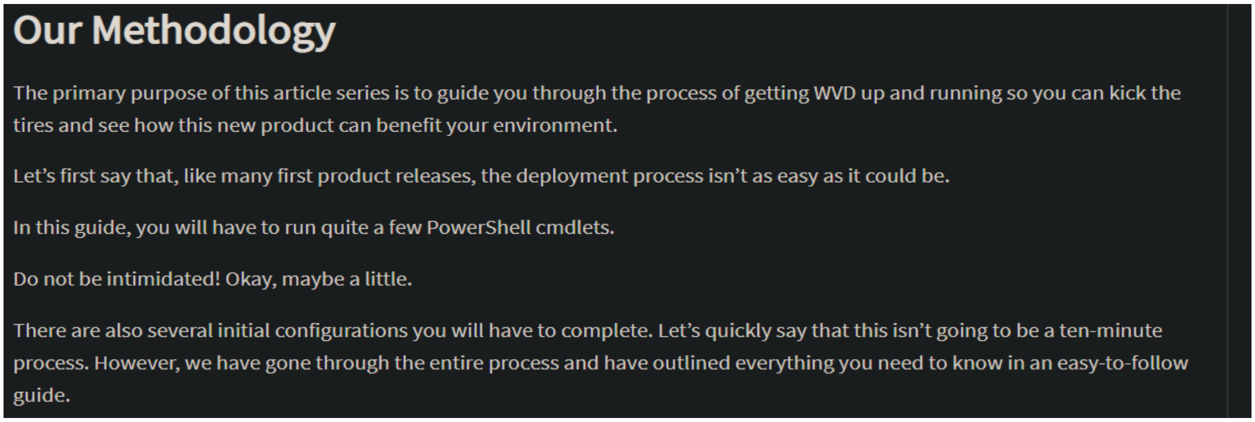


There are some infrastructure requirements to support Windows Virtual Desktop as well. From Microsoft:

- An Azure Active Directory
- A Windows Server Active Directory in sync with Azure Active Directory. You can configure this with one of the following:
  - Azure AD Connect (for hybrid organizations)
  - Azure AD Domain Services (for hybrid or cloud organizations)
- An Azure subscription that contains a virtual network that either contains or is connected to the Windows Server Active Directory

Also, the Azure virtual machines you create for Windows Virtual Desktop must be:

- Standard domain-joined or Hybrid AD-joined. Virtual machines can't be Azure AD-joined.
- Running one of the following supported x64 OS images.
  - Windows 10 Enterprise multi-session, version 1809 or later
  - Windows 10 Enterprise, version 1809 or later
  - Windows 7 Enterprise
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2



Our Methodology

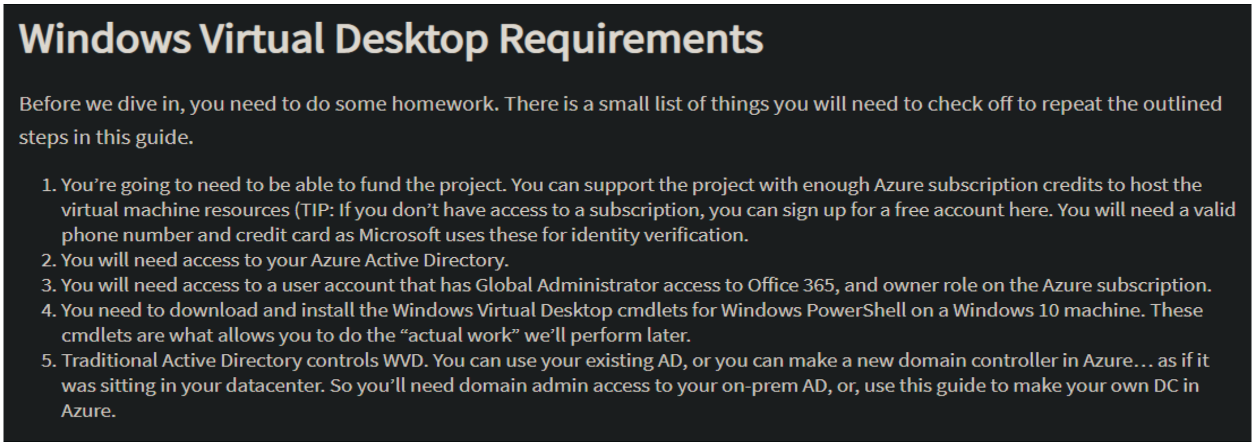
The primary purpose of this article series is to guide you through the process of getting WVD up and running so you can kick the tires and see how this new product can benefit your environment.

Let's first say that, like many first product releases, the deployment process isn't as easy as it could be.

In this guide, you will have to run quite a few PowerShell cmdlets.

Do not be intimidated! Okay, maybe a little.

There are also several initial configurations you will have to complete. Let's quickly say that this isn't going to be a ten-minute process. However, we have gone through the entire process and have outlined everything you need to know in an easy-to-follow guide.



Windows Virtual Desktop Requirements

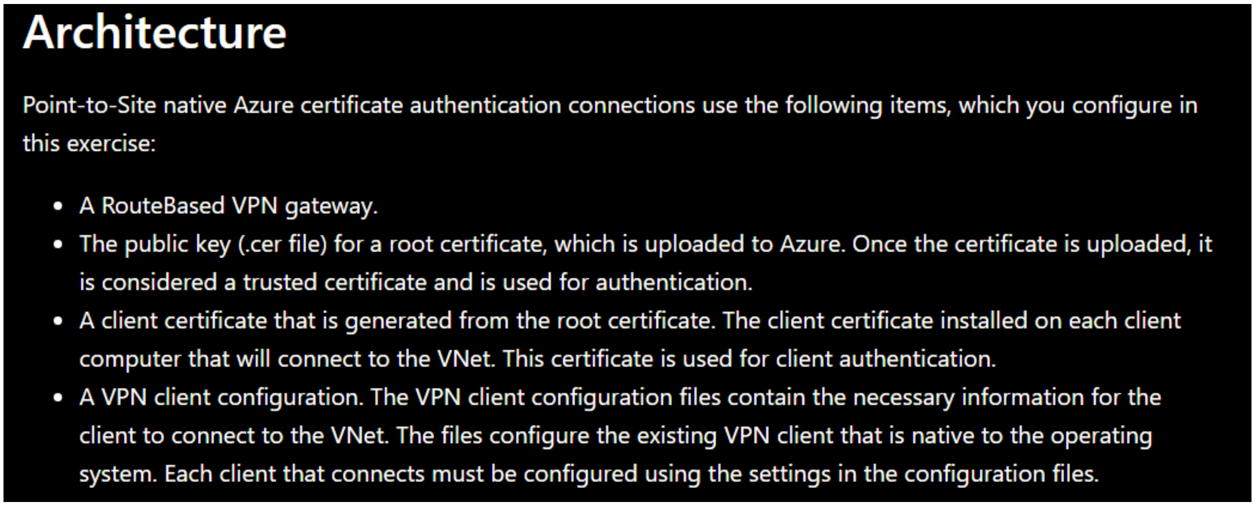
Before we dive in, you need to do some homework. There is a small list of things you will need to check off to repeat the outlined steps in this guide.

1. You're going to need to be able to fund the project. You can support the project with enough Azure subscription credits to host the virtual machine resources (TIP: If you don't have access to a subscription, you can sign up for a free account here. You will need a valid phone number and credit card as Microsoft uses these for identity verification.
2. You will need access to your Azure Active Directory.
3. You will need access to a user account that has Global Administrator access to Office 365, and owner role on the Azure subscription.
4. You need to download and install the Windows Virtual Desktop cmdlets for Windows PowerShell on a Windows 10 machine. These cmdlets are what allows you to do the "actual work" we'll perform later.
5. Traditional Active Directory controls WVD. You can use your existing AD, or you can make a new domain controller in Azure… as if it was sitting in your datacenter. So you'll need domain admin access to your on-prem AD, or, use this guide to make your own DC in Azure.

I have completed step 1, 2 and 3. Will cover step 4 below. I will be using on premise workstation to access Azure portal.

This will be my P2S Network for Azure. I followed this document to create - https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal

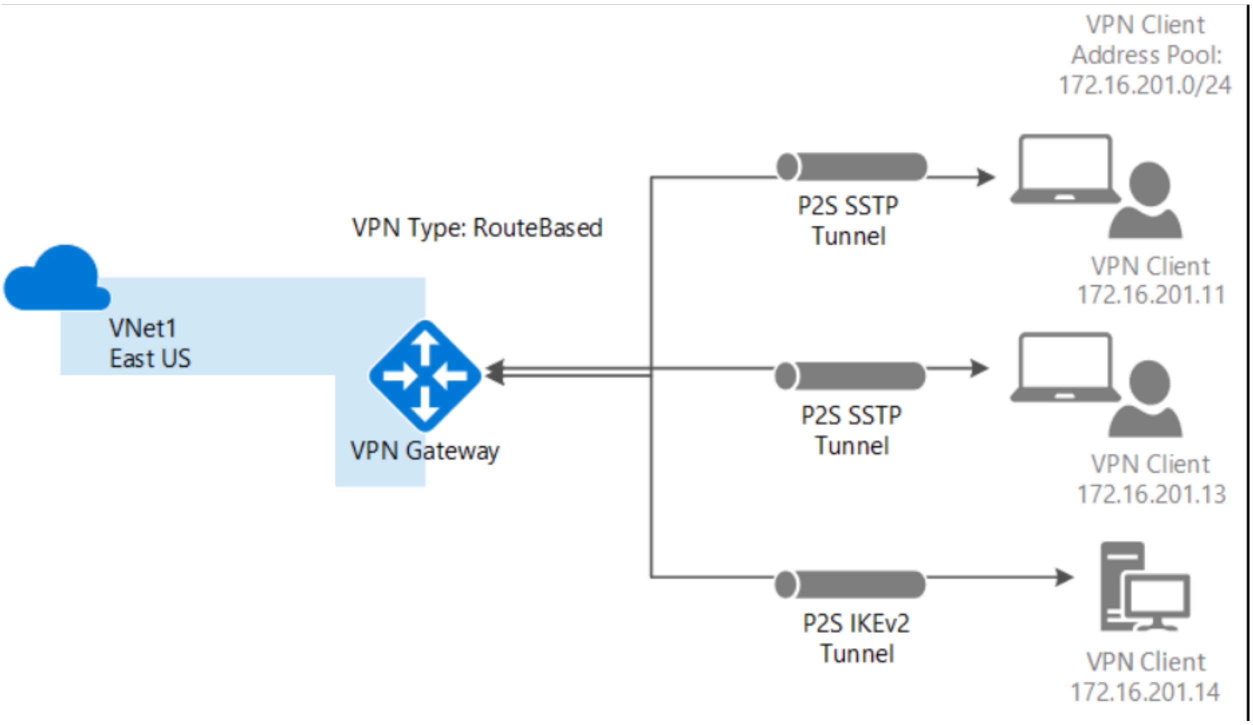
You can also use P2S instead of a Site-to-Site VPN when you have only a few clients that need to connect to a VNet. Point-to-Site connections do not require a VPN device or a public-facing IP address. P2S creates the VPN connection over either SSTP (Secure Socket Tunneling Protocol).

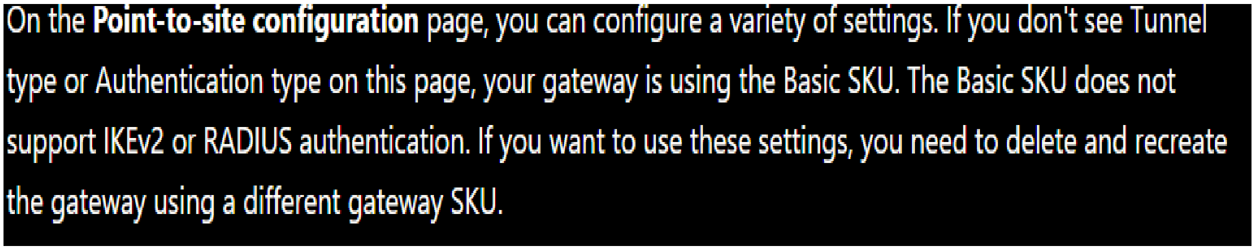


Architecture

Point-to-Site native Azure certificate authentication connections use the following items, which you configure in this exercise:

- A RouteBased VPN gateway.
- The public key (.cer file) for a root certificate, which is uploaded to Azure. Once the certificate is uploaded, it is considered a trusted certificate and is used for authentication.
- A client certificate that is generated from the root certificate. The client certificate installed on each client computer that will connect to the VNet. This certificate is used for client authentication.
- A VPN client configuration. The VPN client configuration files contain the necessary information for the client to connect to the VNet. The files configure the existing VPN client that is native to the operating system. Each client that connects must be configured using the settings in the configuration files.



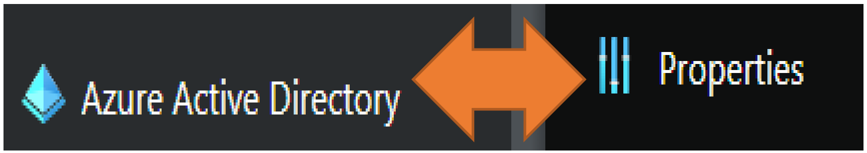


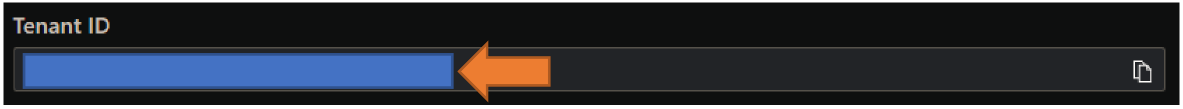
On the **Point-to-site configuration** page, you can configure a variety of settings. If you don't see Tunnel type or Authentication type on this page, your gateway is using the Basic SKU. The Basic SKU does not support IKEv2 or RADIUS authentication. If you want to use these settings, you need to delete and recreate the gateway using a different gateway SKU.

PART 2:

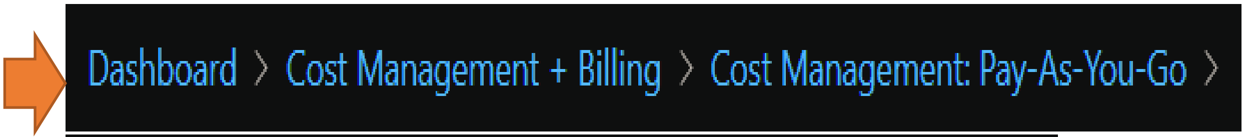
Before we login to below URL, we need to have this information ready from Azure Portal.

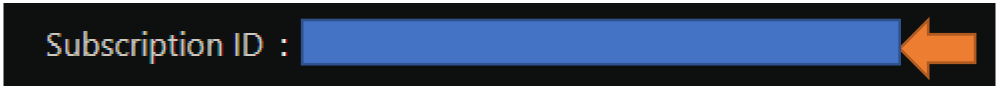
1. Azure Active Directory Tenant ID



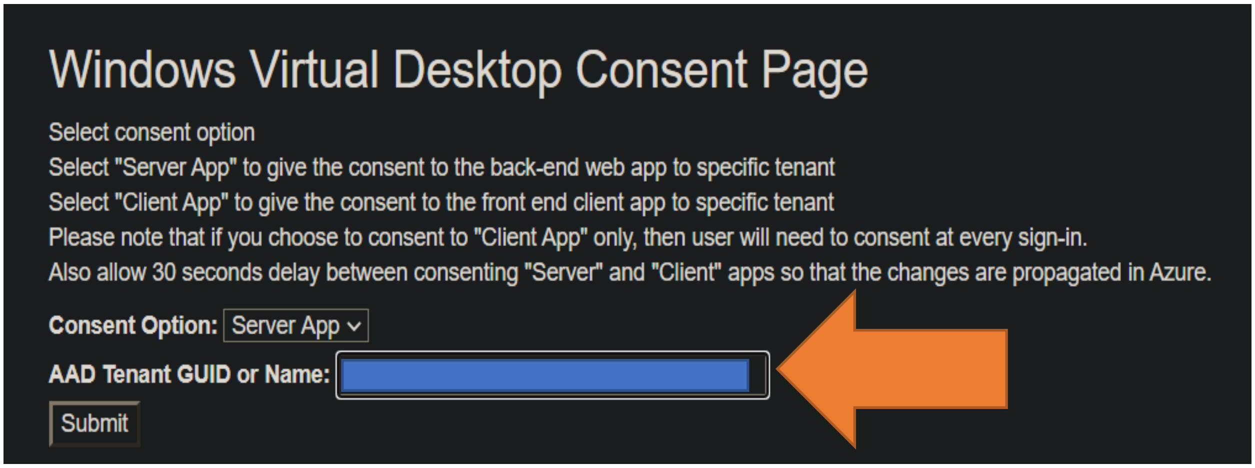

Tenant ID [redacted]

2. Azure Subscription ID


Dashboard > Cost Management + Billing > Cost Management: Pay-As-You-Go >


Subscription ID : [redacted]

Login to this URL https://rdweb.wvd.microsoft.com/

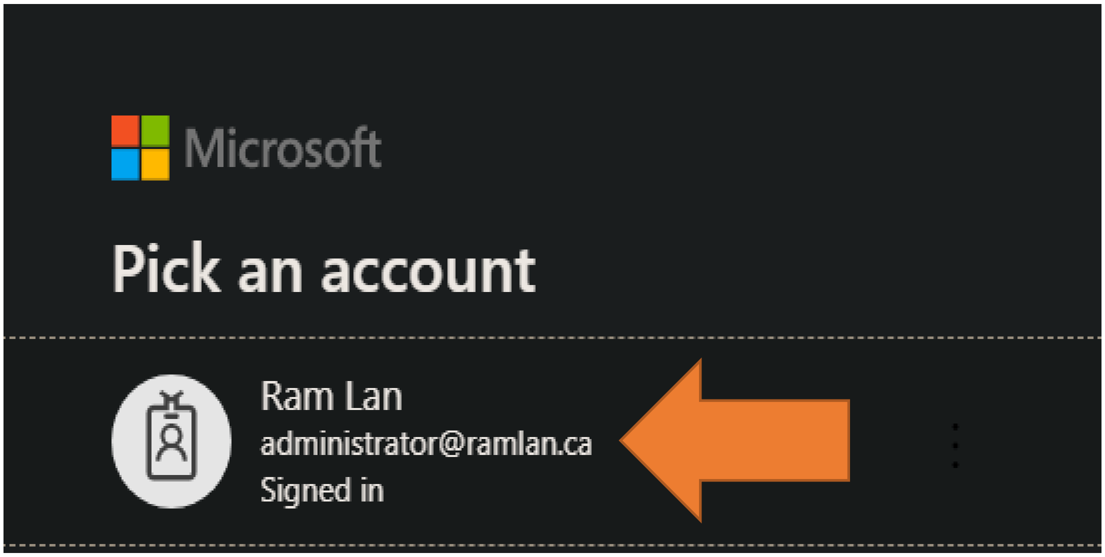


Windows Virtual Desktop Consent Page

Select consent option
Select "Server App" to give the consent to the back-end web app to specific tenant
Select "Client App" to give the consent to the front end client app to specific tenant
Please note that if you choose to consent to "Client App" only, then user will need to consent at every sign-in.
Also allow 30 seconds delay between consenting "Server" and "Client" apps so that the changes are propagated in Azure.

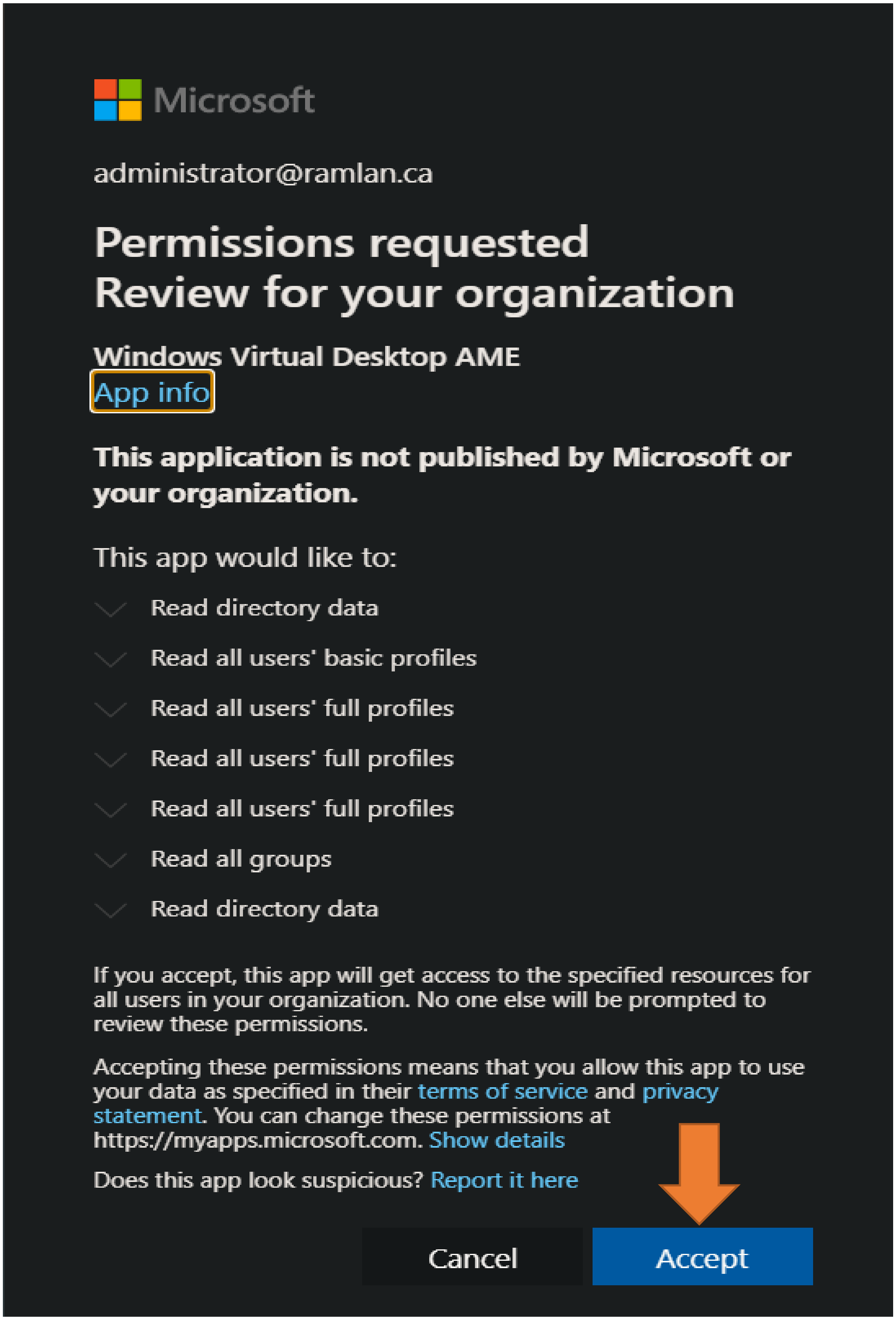
Consent Option: Server App

AAD Tenant GUID or Name: [redacted]



Pick an account

Ram Lan
administrator@ramlan.ca
Signed in



administrator@ramlan.ca

Permissions requested
Review for your organization

Windows Virtual Desktop AME
App info

This application is not published by Microsoft or your organization.

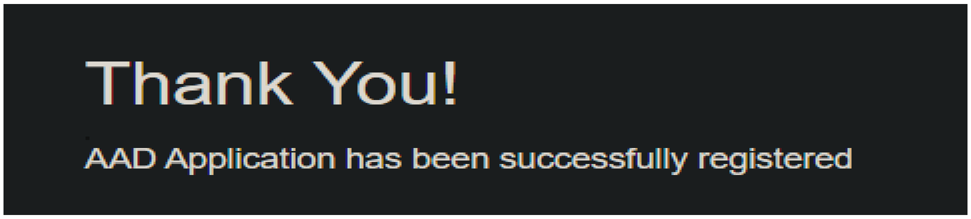
This app would like to:

- Read directory data
- Read all users' basic profiles
- Read all users' full profiles
- Read all users' full profiles
- Read all users' full profiles
- Read all groups
- Read directory data

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

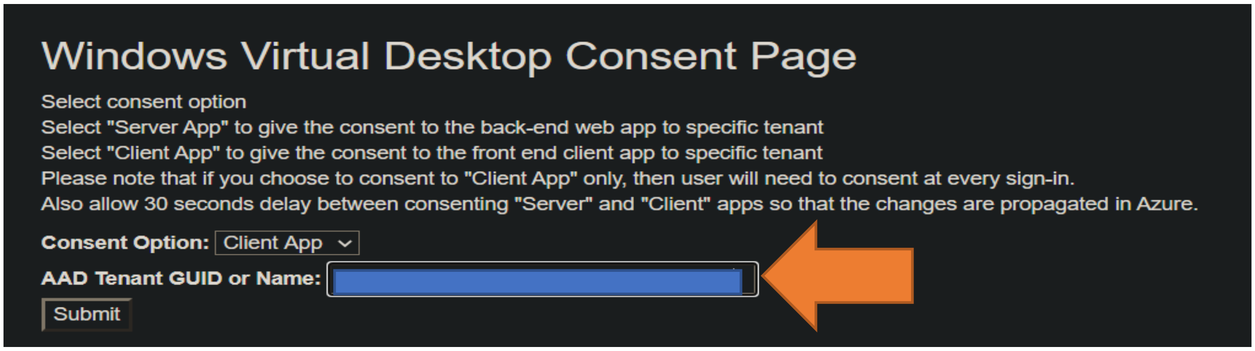
Does this app look suspicious? Report it here



Thank You!

AAD Application has been successfully registered

Repeat same again & select Client App this time. Login to this URL https://rdweb.wvd.microsoft.com/

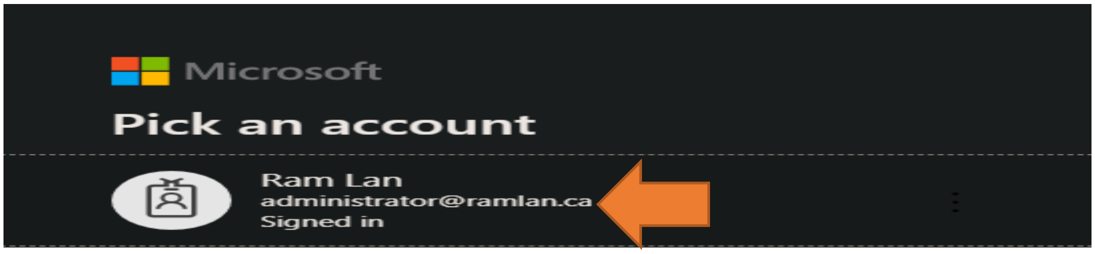


Windows Virtual Desktop Consent Page

Select consent option
Select "Server App" to give the consent to the back-end web app to specific tenant
Select "Client App" to give the consent to the front end client app to specific tenant
Please note that if you choose to consent to "Client App" only, then user will need to consent at every sign-in.
Also allow 30 seconds delay between consenting "Server" and "Client" apps so that the changes are propagated in Azure.

Consent Option: Client App

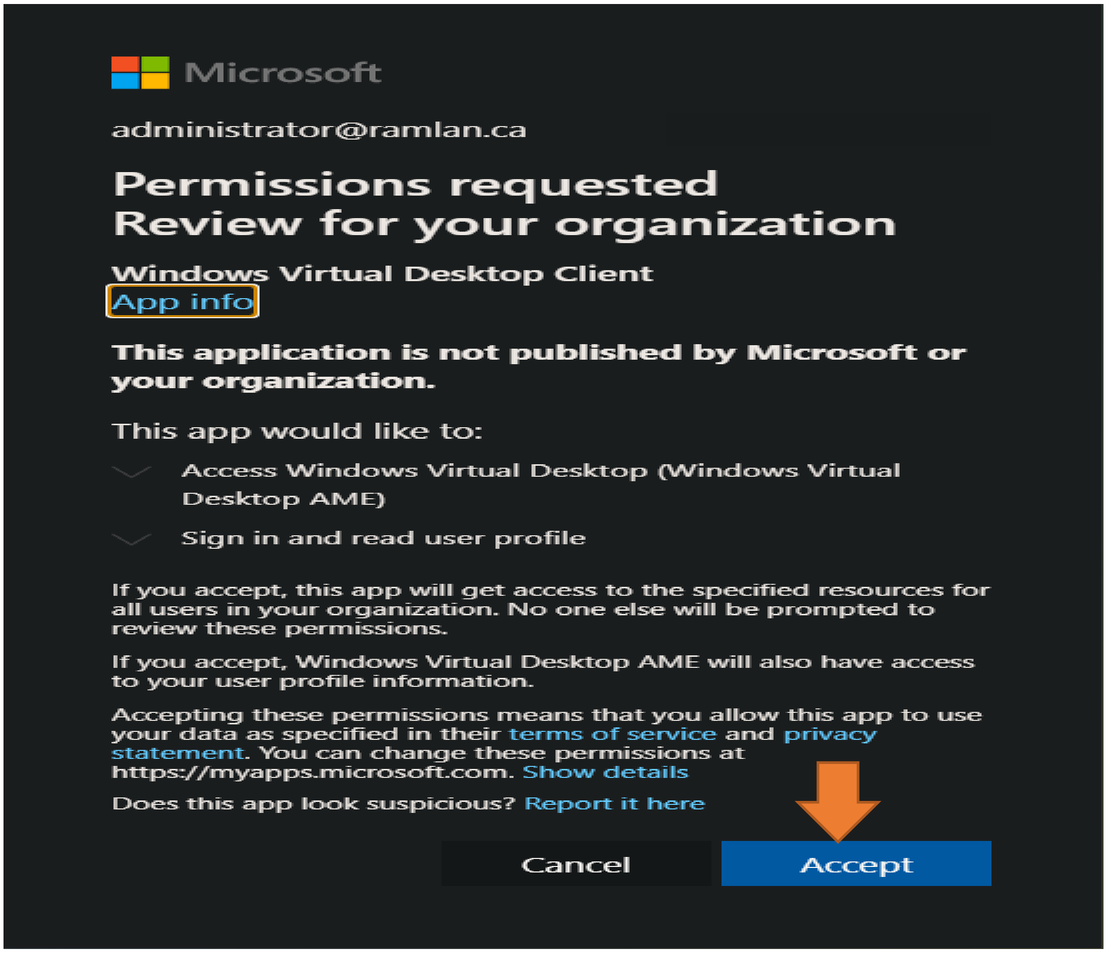
AAD Tenant GUID or Name: [redacted]



Microsoft

Pick an account

Ram Lan
administrator@ramlan.ca
Signed in



Microsoft

administrator@ramlan.ca

Permissions requested
Review for your organization

Windows Virtual Desktop Client
App info

This application is not published by Microsoft or your organization.

This app would like to:

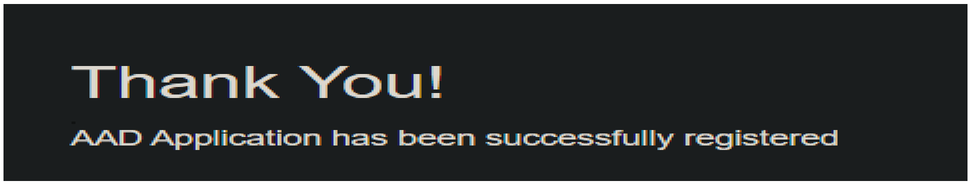
- Access Windows Virtual Desktop (Windows Virtual Desktop AME)
- Sign in and read user profile

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

If you accept, Windows Virtual Desktop AME will also have access to your user profile information.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

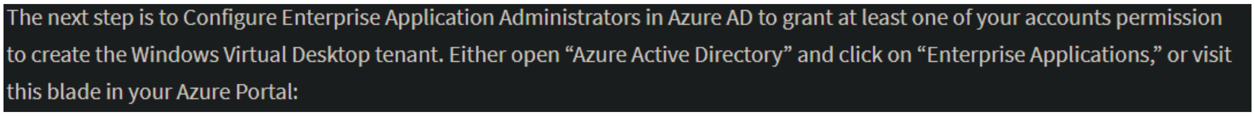


Thank You!

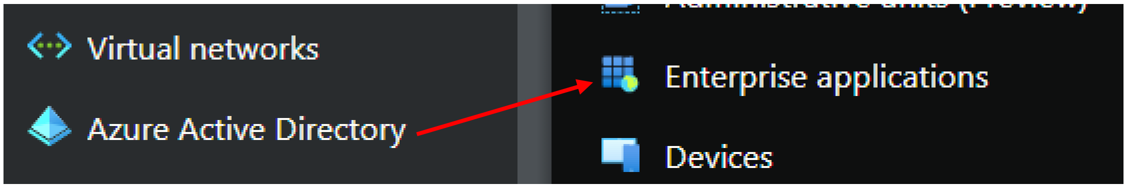
AAD Application has been successfully registered

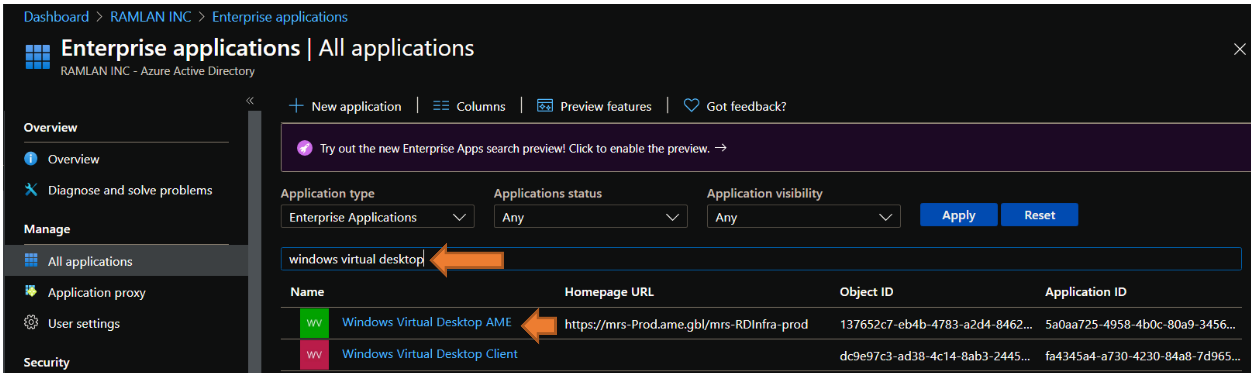
PART 3:

Assign Permissions to users in Azure Portal



The next step is to Configure Enterprise Application Administrators in Azure AD to grant at least one of your accounts permission to create the Windows Virtual Desktop tenant. Either open “Azure Active Directory” and click on “Enterprise Applications,” or visit this blade in your Azure Portal:





Enterprise applications | All applications

RAMLAN INC - Azure Active Directory

Try out the new Enterprise Apps search preview! Click to enable the preview. →

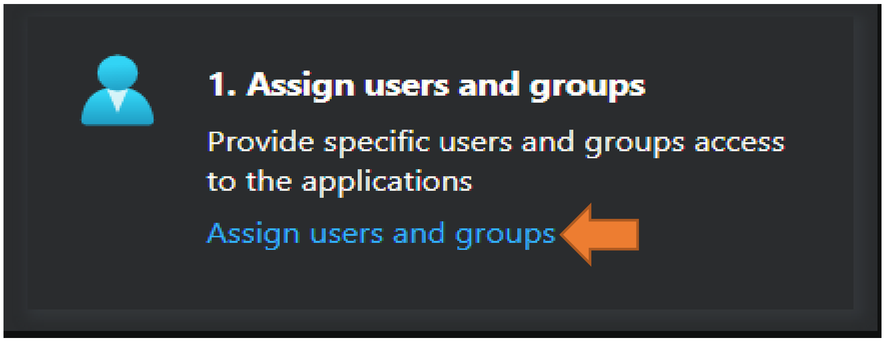
Application type: Enterprise Applications

Applications status: Any

Application visibility: Any

windows virtual desktop

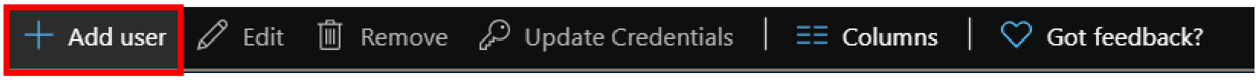
Name	Homepage URL	Object ID	Application ID
WV Windows Virtual Desktop AME	https://mrs-Prod.ame.gbl/mrs-RDInfra-prod	137652c7-eb4b-4783-a2d4-8462...	5a0aa725-4958-4b0c-80a9-3456...
WV Windows Virtual Desktop Client		dc9e97c3-ad38-4c14-8ab3-2445...	fa4345a4-a730-4230-84a8-7d965...

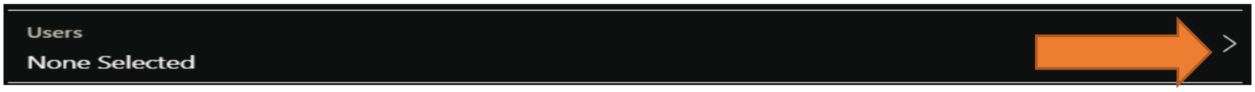


1. Assign users and groups

Provide specific users and groups access to the applications

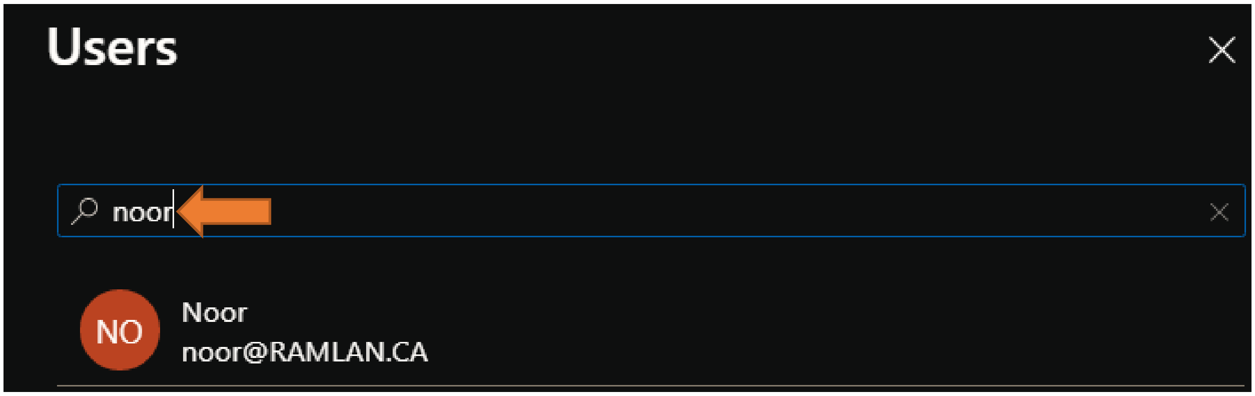
Assign users and groups





Users

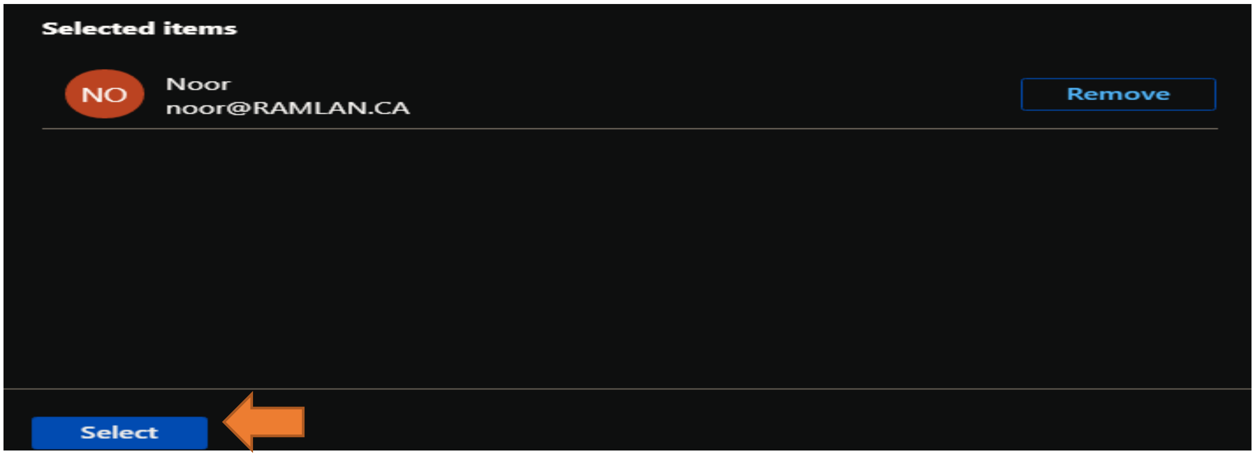
None Selected



Users

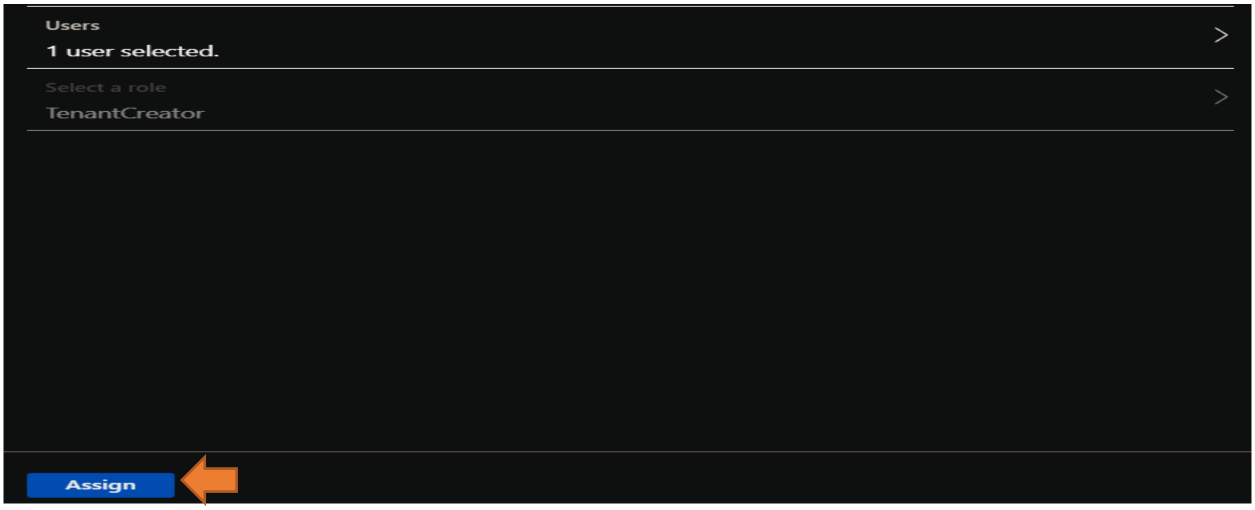
noor

NO Noor
noor@RAMLAN.CA



Selected items

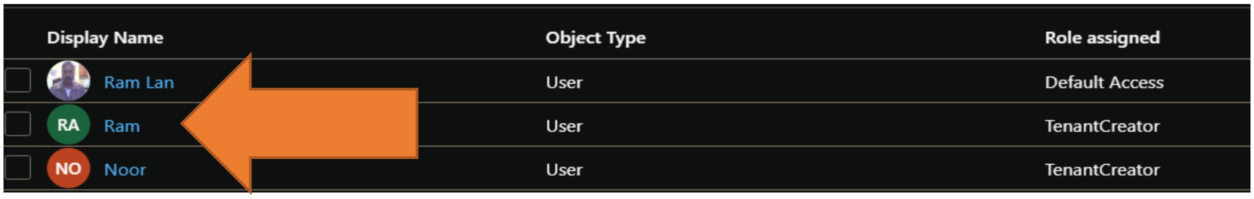
NO Noor
noor@RAMLAN.CA



Users
1 user selected.

Select a role
TenantCreator

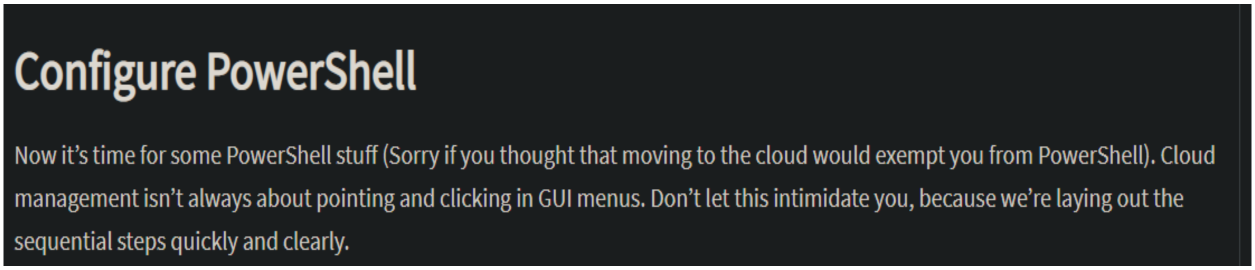
Now we have list of users for TenantCreator Role.



Display Name	Object Type	Role assigned
□ Ram Lan	User	Default Access
□ RA Ram	User	TenantCreator
□ NO Noor	User	TenantCreator

PART 4:

Now we can do the stuff on a workstation using PowerShell. For this exercise, I will be doing it on Windows Server 2019 machine instead of Windows 10 workstation.



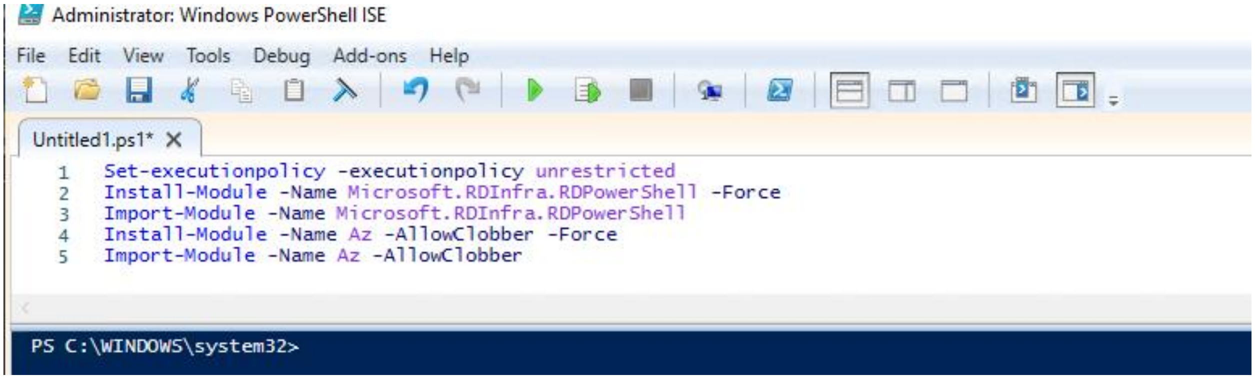
Configure PowerShell

Now it’s time for some PowerShell stuff (Sorry if you thought that moving to the cloud would exempt you from PowerShell). Cloud management isn’t always about pointing and clicking in GUI menus. Don’t let this intimidate you, because we’re laying out the sequential steps quickly and clearly.

The required commands are here - https://docs.microsoft.com/en-us/powershell/windows-virtual-desktop/overview

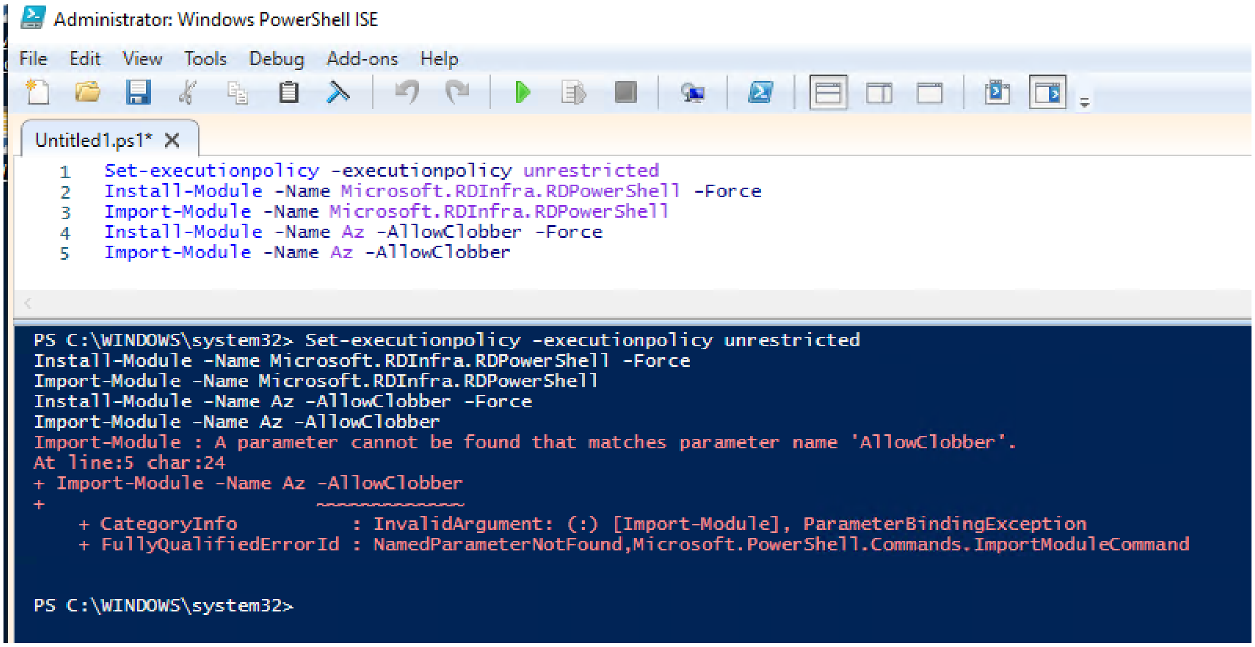
Run these commands. Open PowerShell ISE as Administrator

Set-executionpolicy -executionpolicy unrestricted
Install-Module -Name Microsoft.RDInfra.RDPowerShell -Force
Import-Module -Name Microsoft.RDInfra.RDPowerShell
Install-Module -Name Az -AllowClobber -Force
Import-Module -Name Az -AllowClobber


Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1*

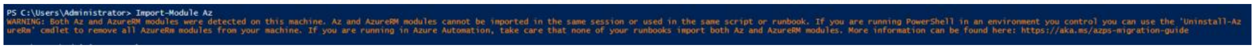
```
Set-executionpolicy -executionpolicy unrestricted
Install-Module -Name Microsoft.RDInfra.RDPowerShell -Force
Import-Module -Name Microsoft.RDInfra.RDPowerShell
Install-Module -Name Az -AllowClobber -Force
Import-Module -Name Az -AllowClobber
```

```
PS C:\WINDOWS\system32>
```

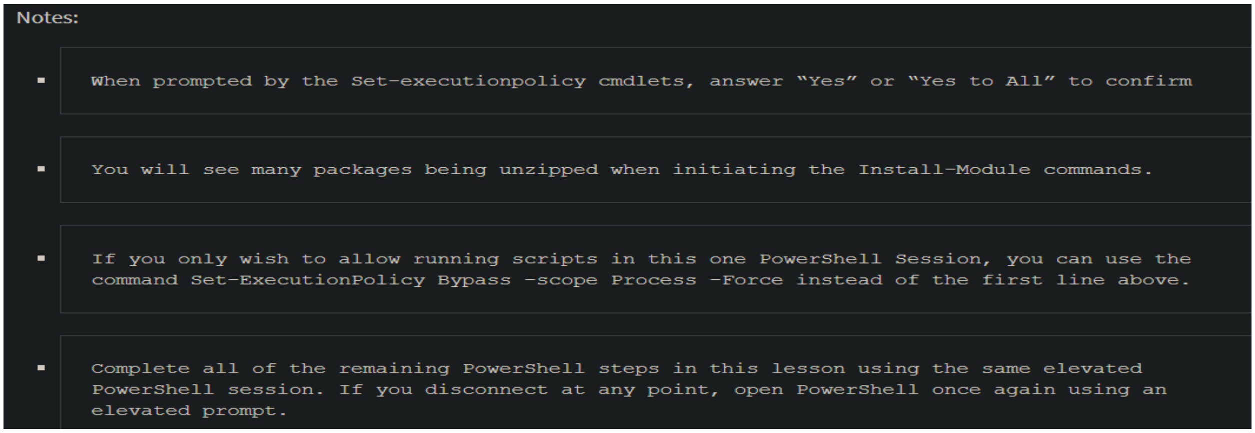

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1*

```
Set-executionpolicy -executionpolicy unrestricted
Install-Module -Name Microsoft.RDInfra.RDPowerShell -Force
Import-Module -Name Microsoft.RDInfra.RDPowerShell
Install-Module -Name Az -AllowClobber -Force
Import-Module -Name Az -AllowClobber
```

```
PS C:\WINDOWS\system32> Set-executionpolicy -executionpolicy unrestricted
Install-Module -Name Microsoft.RDInfra.RDPowerShell -Force
Import-Module -Name Microsoft.RDInfra.RDPowerShell
Install-Module -Name Az -AllowClobber -Force
Import-Module -Name Az -AllowClobber
Import-Module : A parameter cannot be found that matches parameter name 'AllowClobber'.
At line:5 char:24
+ Import-Module -Name Az -AllowClobber
+                        ~~~~~~~~~~~~~
    + CategoryInfo          : InvalidArgument: (:) [Import-Module], ParameterBindingException
    + FullyQualifiedErrorId : NamedParameterNotFound,Microsoft.PowerShell.Commands.ImportModuleCommand


PS C:\WINDOWS\system32>
```



```
PS C:\Users\Administrator> Import-Module Az
WARNING: Both Az and AzureRM modules were detected on this machine. Az and AzureRM modules cannot be imported in the same session or used in the same script or runbook. If you are running PowerShell in an environment you control you can use the 'Uninstall-Az
ureRm' cmdlet to remove all AzureRm modules from your machine. If you are running in Azure Automation, take care that none of your runbooks import both Az and AzureRM modules. More information can be found here: https://aka.ms/azps-migration-guide
```



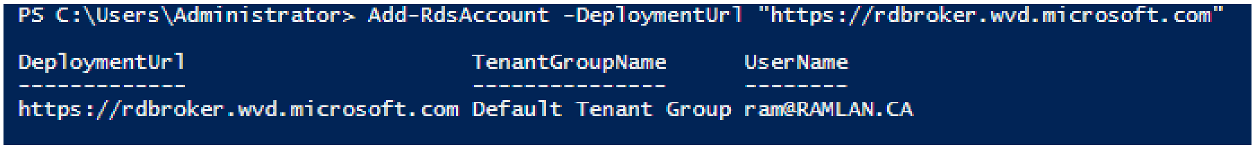
Notes:

- When prompted by the Set-executionpolicy cmdlets, answer “Yes” or “Yes to All” to confirm
- You will see many packages being unzipped when initiating the Install-Module commands.
- If you only wish to allow running scripts in this one PowerShell Session, you can use the command Set-ExecutionPolicy Bypass -scope Process -Force instead of the first line above.
- Complete all of the remaining PowerShell steps in this lesson using the same elevated PowerShell session. If you disconnect at any point, open PowerShell once again using an elevated prompt.

Now we will connect to Azure through PowerShell

Add-RdsAccount -DeploymentUrl https://rdbroker.wvd.microsoft.com

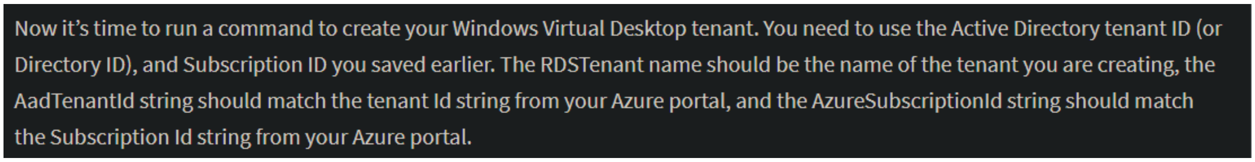
Enter your TenantCreator account and password to login to Azure



```
PS C:\Users\Administrator> Add-RdsAccount -DeploymentUrl "https://rdbroker.wvd.microsoft.com"

DeploymentUrl                     TenantGroupName      UserName
-------------                     ---------------      --------
https://rdbroker.wvd.microsoft.com Default Tenant Group ram@RAMLAN.CA
```

PART 5:

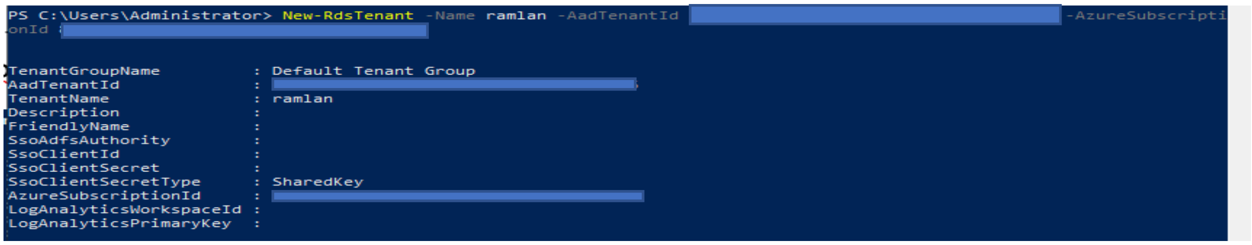
Setup Windows Virtual Desktop Tenant and RDS Owner



Now it's time to run a command to create your Windows Virtual Desktop tenant. You need to use the Active Directory tenant ID (or Directory ID), and Subscription ID you saved earlier. The RDSTenant name should be the name of the tenant you are creating, the AadTenantId string should match the tenant Id string from your Azure portal, and the AzureSubscriptionId string should match the Subscription Id string from your Azure portal.

Run this command

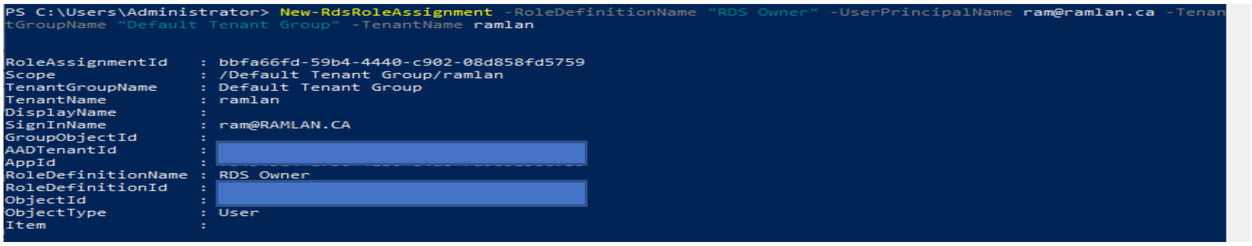
New-RdsTenant -Name ramlan -AadTenantId [redacted] -AzureSubscriptionId [redacted]



```
PS C:\Users\Administrator> New-RdsTenant -Name ramlan -AadTenantId [redacted] -AzureSubscripti
onId [redacted]

TenantGroupName           : Default Tenant Group
AadTenantId               : [redacted]
TenantName                : ramlan
Description               :
FriendlyName              :
SsoAdfsAuthority          :
SsoClientId               :
SsoClientSecret           :
SsoClientSecretType       : SharedKey
AzureSubscriptionId       : [redacted]
LogAnalyticsWorkspaceId :
LogAnalyticsPrimaryKey    :
```

Run this command

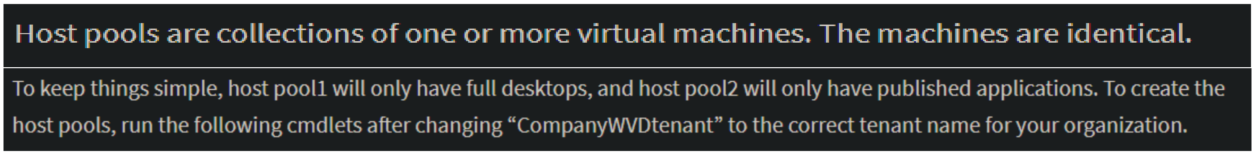
New-RdsRoleAssignment -RoleDefinitionName "RDS Owner" -UserPrincipalName ram@ramlan.ca -TenantGroupName "Default Tenant Group" -TenantName ramlan



```
PS C:\Users\Administrator> New-RdsRoleAssignment -RoleDefinitionName "RDS Owner" -UserPrincipalName ram@ramlan.ca -Tenan
tGroupName "Default Tenant Group" -TenantName ramlan

RoleAssignmentId    : bbfa66fd-59b4-4440-c902-08d858fd5759
Scope               : /Default Tenant Group/ramlan
TenantGroupName     : Default Tenant Group
TenantName          : ramlan
DisplayName         :
SignInName          : ram@RAMLAN.CA
GroupObjectId       :
AADTenantId         : [redacted]
AppId               :
RoleDefinitionName  : RDS Owner
RoleDefinitionId    : [redacted]
ObjectId            :
ObjectType          : User
Item                :
```

PART 6:

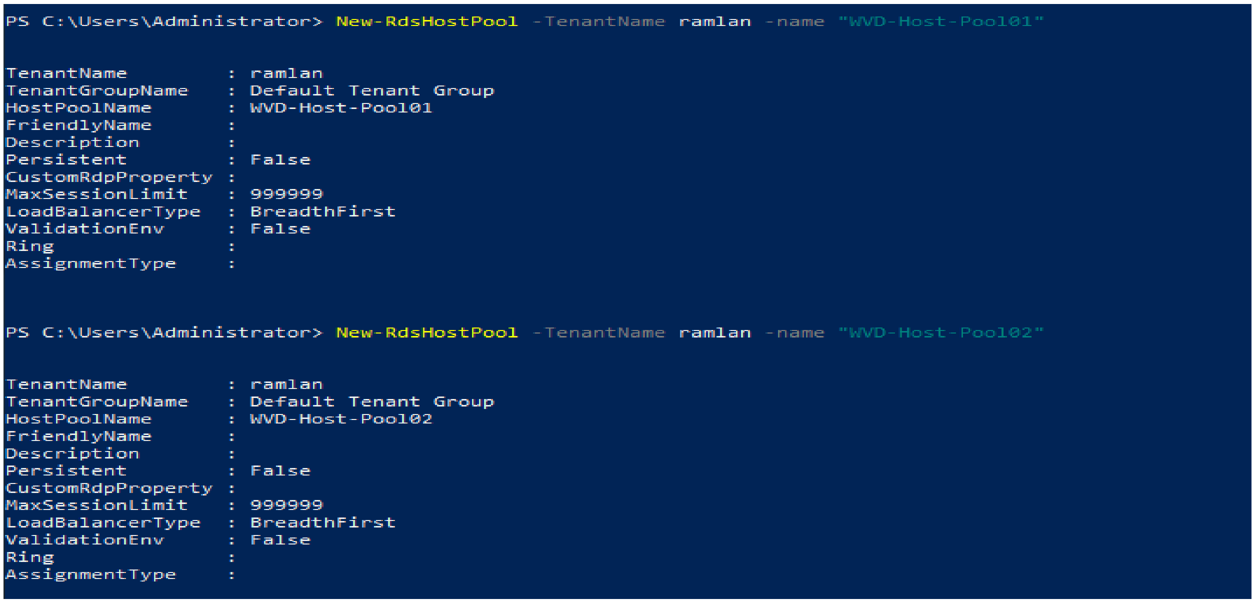
Creating Host Pools



Host pools are collections of one or more virtual machines. The machines are identical.

To keep things simple, host pool1 will only have full desktops, and host pool2 will only have published applications. To create the host pools, run the following cmdlets after changing "CompanyWVDtenant" to the correct tenant name for your organization.

New-RdsHostPool -TenantName ramlan -name "WVD-Host-Pool01"
New-RdsHostPool -TenantName ramlan -name "WVD-Host-Pool02"

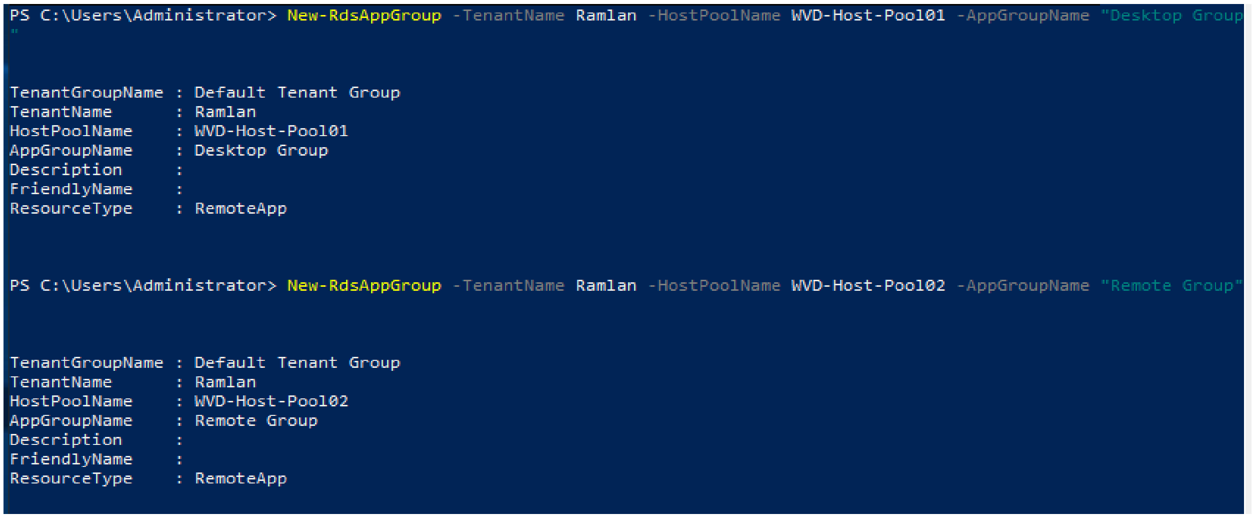


```
PS C:\Users\Administrator> New-RdsHostPool -TenantName ramlan -name "WVD-Host-Pool01"

TenantName          : ramlan
TenantGroupName     : Default Tenant Group
HostPoolName        : WVD-Host-Pool01
FriendlyName        :
Description         :
Persistent          : False
CustomRdpProperty   :
MaxSessionLimit     : 999999
LoadBalancerType    : BreadthFirst
ValidationEnv       : False
Ring                :
AssignmentType      :


PS C:\Users\Administrator> New-RdsHostPool -TenantName ramlan -name "WVD-Host-Pool02"

TenantName          : ramlan
TenantGroupName     : Default Tenant Group
HostPoolName        : WVD-Host-Pool02
FriendlyName        :
Description         :
Persistent          : False
CustomRdpProperty   :
MaxSessionLimit     : 999999
LoadBalancerType    : BreadthFirst
ValidationEnv       : False
Ring                :
AssignmentType      :
```

Part 7:

Create Desktop and Remote Groups

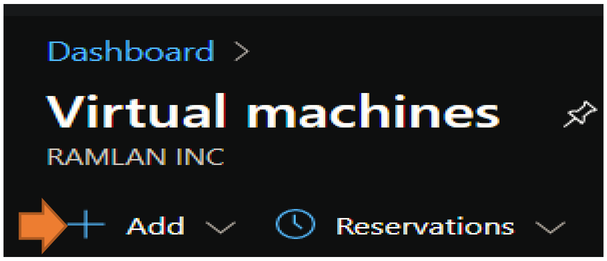
New-RdsAppGroup -TenantName ramlan -HostPoolName WVD-Host-Pool01 -AppGroupName "Desktop Group"
New-RdsAppGroup -TenantName ramlan -HostPoolName WVD-Host-Pool02 -AppGroupName "Remote Group"

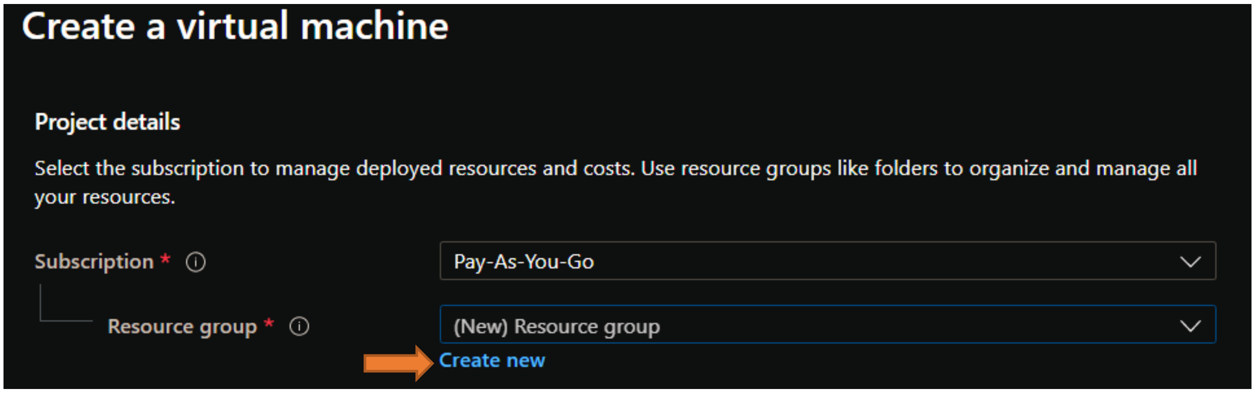


```
PS C:\Users\Administrator> New-RdsAppGroup -TenantName Ramlan -HostPoolName WVD-Host-Pool01 -AppGroupName "Desktop Group
"

TenantGroupName : Default Tenant Group
TenantName      : Ramlan
HostPoolName    : WVD-Host-Pool01
AppGroupName    : Desktop Group
Description     :
FriendlyName    :
ResourceType    : RemoteApp


PS C:\Users\Administrator> New-RdsAppGroup -TenantName Ramlan -HostPoolName WVD-Host-Pool02 -AppGroupName "Remote Group"

TenantGroupName : Default Tenant Group
TenantName      : Ramlan
HostPoolName    : WVD-Host-Pool02
AppGroupName    : Remote Group
Description     :
FriendlyName    :
ResourceType    : RemoteApp
```

PART 8:

Create Virtual Machine – For Domain Controller in Azure





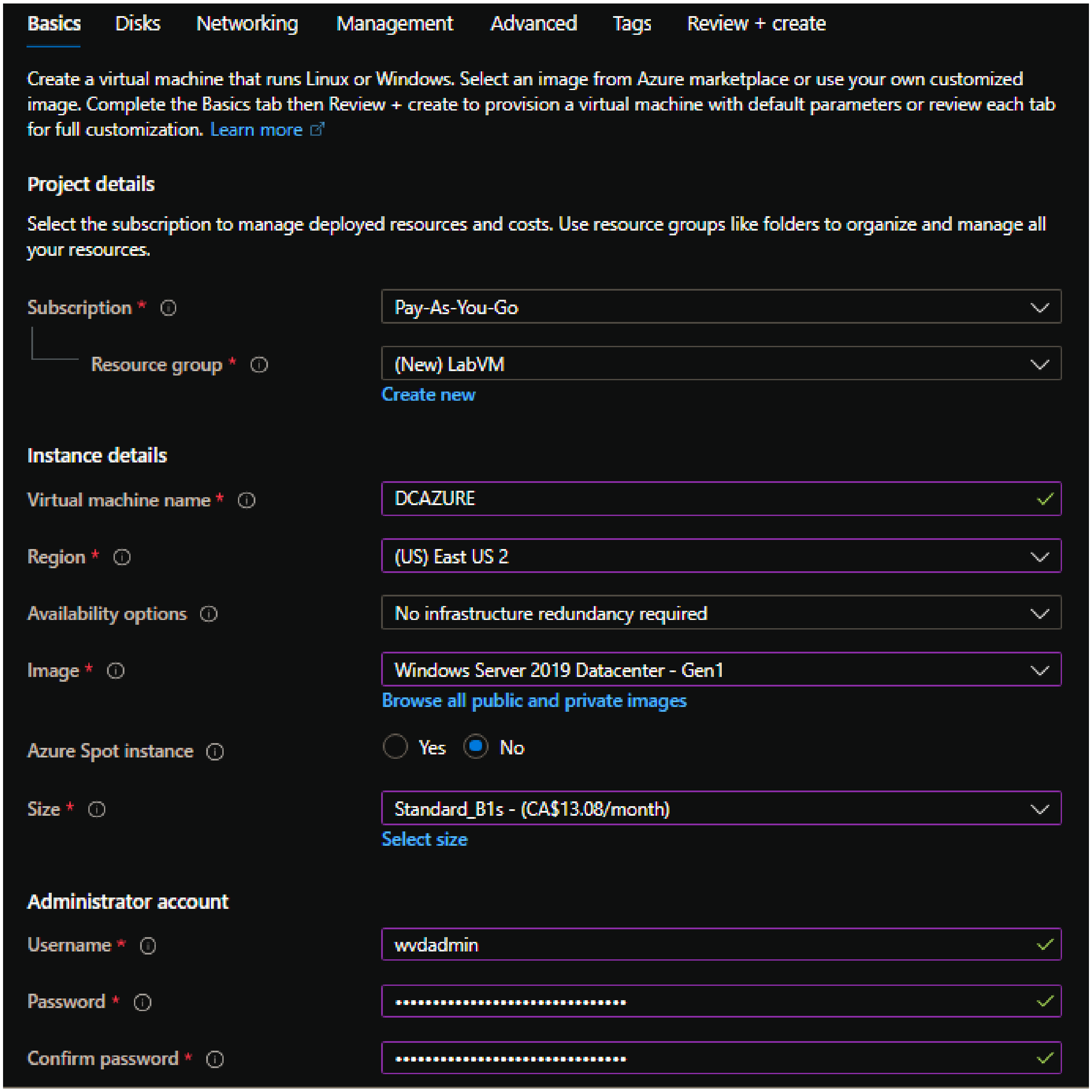
Create a virtual machine

Project details

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

Subscription * ⓘ Pay-As-You-Go

Resource group * ⓘ (New) Resource group



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

Project details

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

Subscription * ⓘ Pay-As-You-Go

Resource group * ⓘ (New) LabVM

Instance details

Virtual machine name * ⓘ DCAZURE ✓

Region * ⓘ (US) East US 2

Availability options ⓘ No infrastructure redundancy required

Image * ⓘ Windows Server 2019 Datacenter - Gen1

Azure Spot instance ⓘ ○ Yes ● No

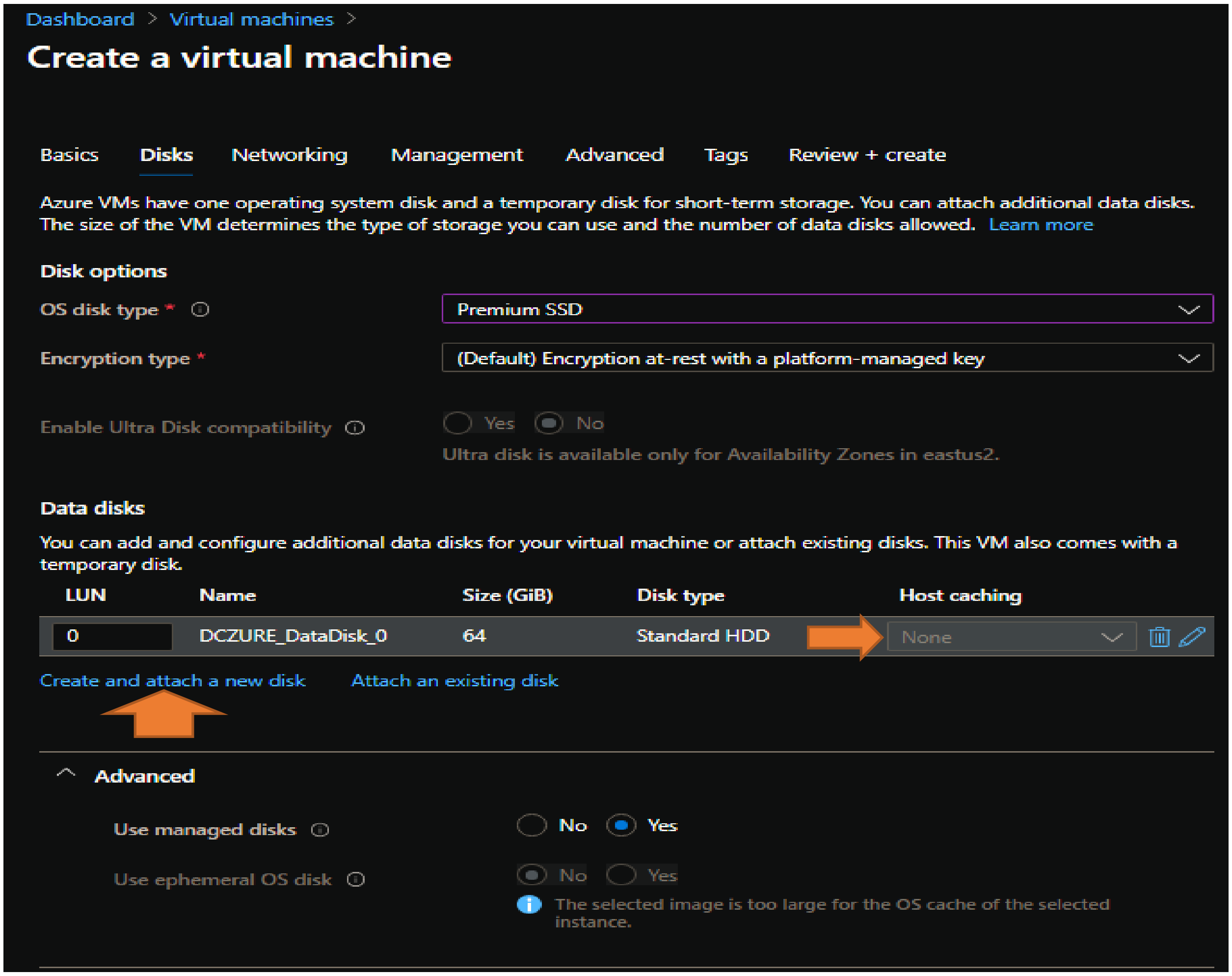
Size * ⓘ Standard_B1s - (CA$13.08/month)

Administrator account

Username * ⓘ wvdadmin ✓

Password * ⓘ •••••••••••••••••••••••••••••••• ✓

Confirm password * ⓘ •••••••••••••••••••••••••••••••• ✓



Dashboard > Virtual machines >

Create a virtual machine

Basics | Disks | Networking | Management | Advanced | Tags | Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. Learn more

Disk options

OS disk type * ⓘ: Premium SSD

Encryption type *: (Default) Encryption at-rest with a platform-managed key

Enable Ultra Disk compatibility ⓘ: ○ Yes ● No

Ultra disk is available only for Availability Zones in eastus2.

Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching
0	DCZURE_DataDisk_0	64	Standard HDD	None

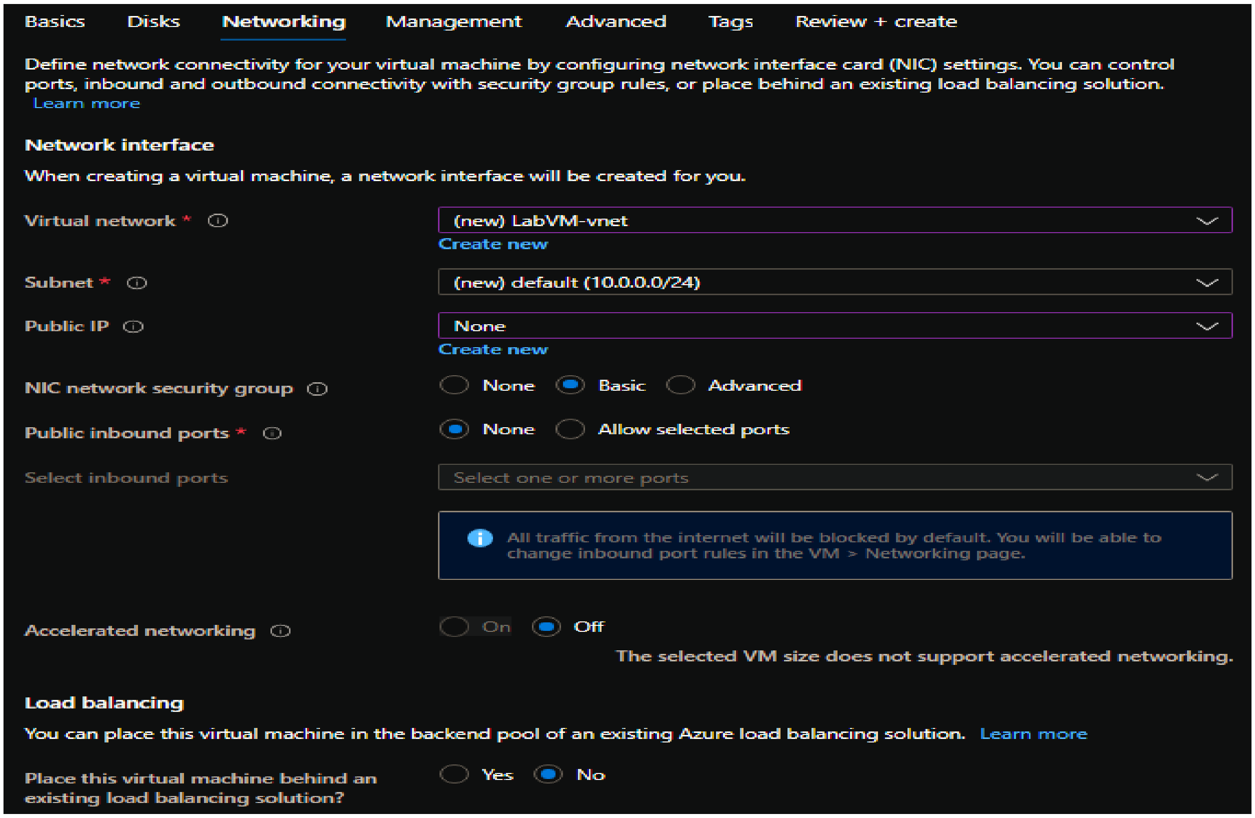
Create and attach a new disk   Attach an existing disk

Advanced

Use managed disks ⓘ: ○ No ● Yes

Use ephemeral OS disk ⓘ: ● No ○ Yes

ⓘ The selected image is too large for the OS cache of the selected instance.



Basics | Disks | Networking | Management | 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 * ⓘ: (new) LabVM-vnet
Create new

Subnet * ⓘ: (new) default (10.0.0.0/24)

Public IP ⓘ: None
Create new

NIC network security group ⓘ: ○ None ● Basic ○ Advanced

Public inbound ports * ⓘ: ● None ○ Allow selected ports

Select inbound ports: Select one or more ports

ⓘ All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

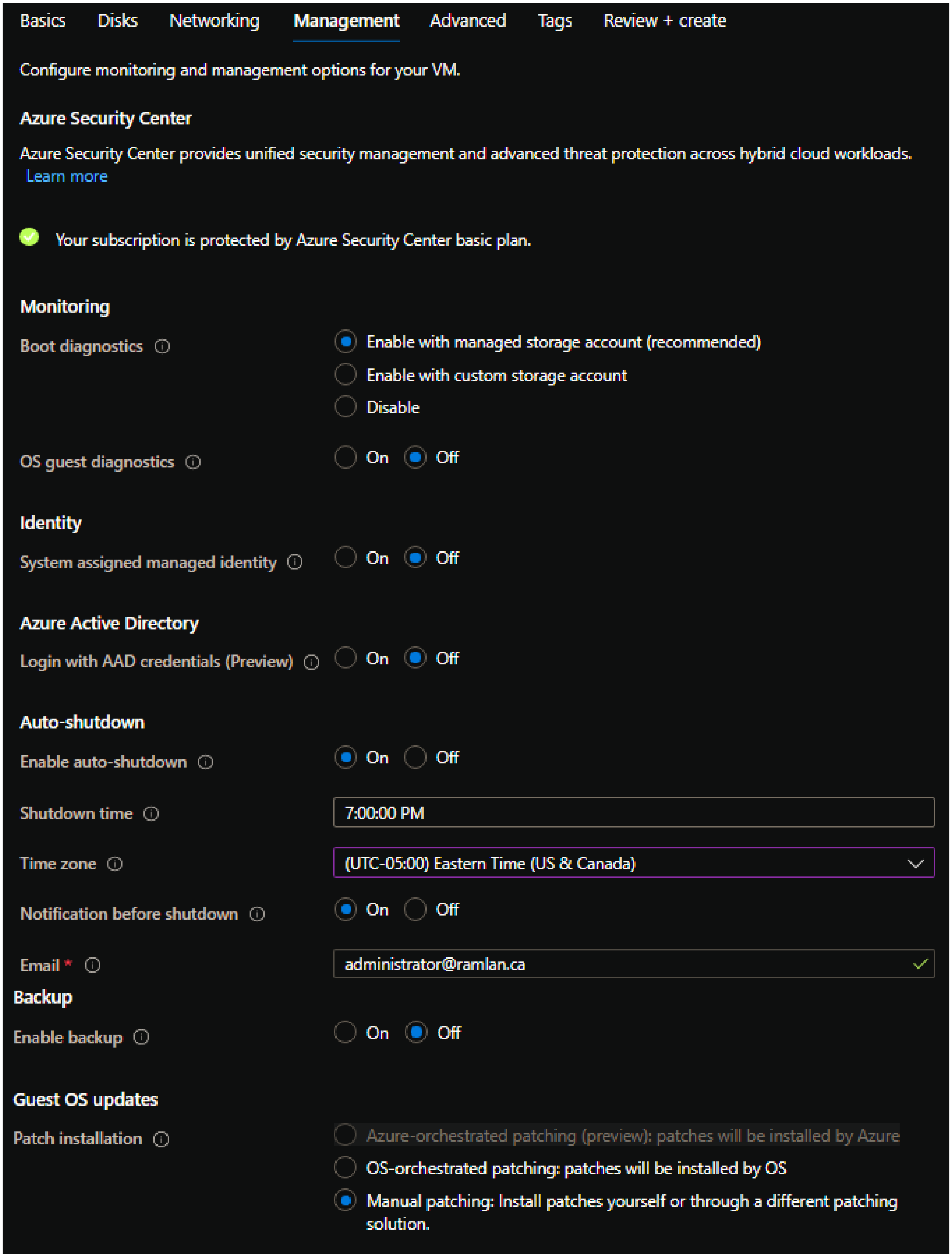
Accelerated networking ⓘ: ○ On ● Off

The selected VM size does not support accelerated networking.

Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more

Place this virtual machine behind an existing load balancing solution? ○ Yes ● No



Configure monitoring and management options for your VM.

Azure Security Center

Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads. Learn more

✓ Your subscription is protected by Azure Security Center basic plan.

Monitoring

Boot diagnostics ⓘ
● Enable with managed storage account (recommended)
○ Enable with custom storage account
○ Disable

OS guest diagnostics ⓘ ○ On ● Off

Identity

System assigned managed identity ⓘ ○ On ● Off

Azure Active Directory

Login with AAD credentials (Preview) ⓘ ○ On ● Off

Auto-shutdown

Enable auto-shutdown ⓘ ● On ○ Off

Shutdown time ⓘ 7:00:00 PM

Time zone ⓘ (UTC-05:00) Eastern Time (US & Canada)

Notification before shutdown ⓘ ● On ○ Off

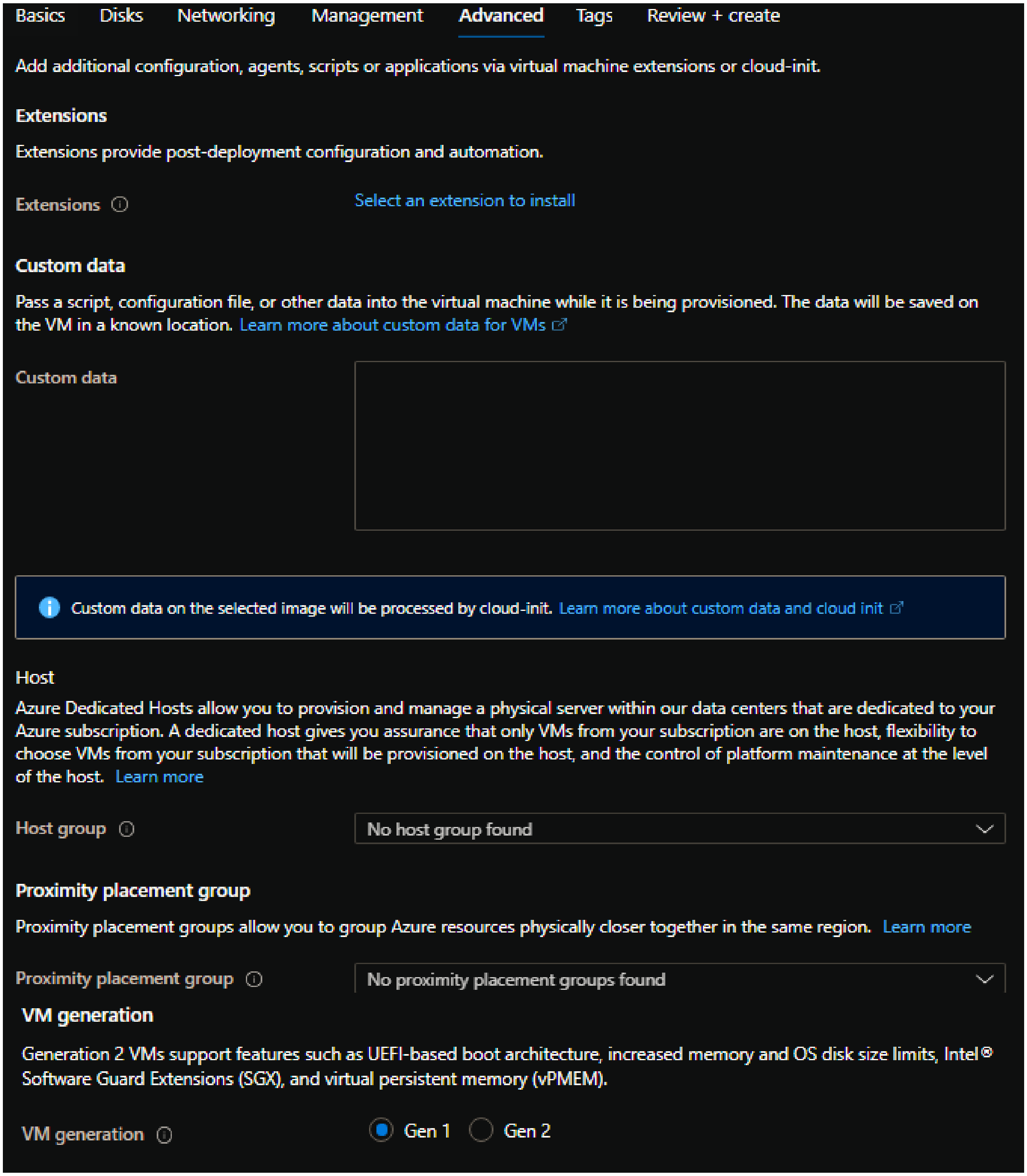
Email * ⓘ administrator@ramlan.ca ✓

Backup

Enable backup ⓘ ○ On ● Off

Guest OS updates

Patch installation ⓘ
○ Azure-orchestrated patching (preview): patches will be installed by Azure
○ OS-orchestrated patching: patches will be installed by OS
● Manual patching: Install patches yourself or through a different patching solution.



Add additional configuration, agents, scripts or applications via virtual machine extensions or cloud-init.

Extensions

Extensions provide post-deployment configuration and automation.

Extensions ⓘ Select an extension to install

Custom data

Pass a script, configuration file, or other data into the virtual machine while it is being provisioned. The data will be saved on the VM in a known location. Learn more about custom data for VMs

Custom data

ⓘ Custom data on the selected image will be processed by cloud-init. Learn more about custom data and cloud init

Host

Azure Dedicated Hosts allow you to provision and manage a physical server within our data centers that are dedicated to your Azure subscription. A dedicated host gives you assurance that only VMs from your subscription are on the host, flexibility to choose VMs from your subscription that will be provisioned on the host, and the control of platform maintenance at the level of the host. Learn more

Host group ⓘ No host group found

Proximity placement group

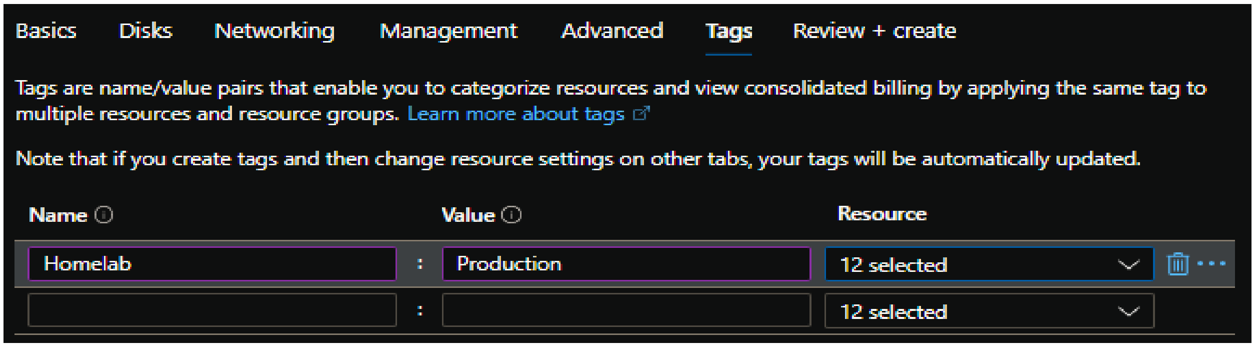
Proximity placement groups allow you to group Azure resources physically closer together in the same region. Learn more

Proximity placement group ⓘ No proximity placement groups found

VM generation

Generation 2 VMs support features such as UEFI-based boot architecture, increased memory and OS disk size limits, Intel® Software Guard Extensions (SGX), and virtual persistent memory (vPMEM).

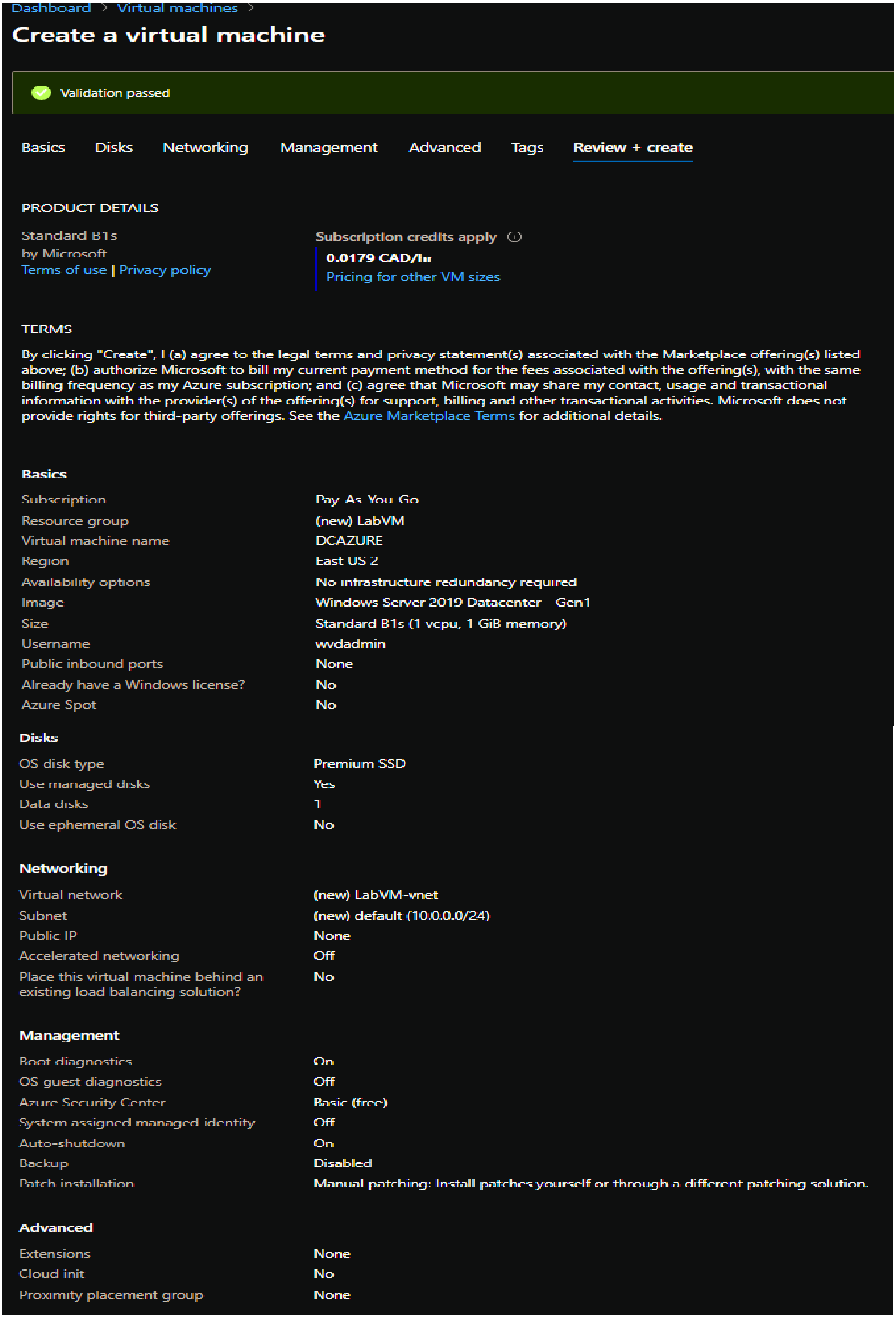
VM generation ⓘ ● Gen 1 ○ Gen 2



Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Learn more about tags

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name ⓘ		Value ⓘ	Resource
Homelab	:	Production	12 selected
	:		12 selected



Dashboard > Virtual machines >

Create a virtual machine

✓ Validation passed

PRODUCT DETAILS

Standard B1s
by Microsoft
Terms of use | Privacy policy

Subscription credits apply ⓘ
0.0179 CAD/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.

Basics

Subscription	Pay-As-You-Go
Resource group	(new) LabVM
Virtual machine name	DCAZURE
Region	East US 2
Availability options	No infrastructure redundancy required
Image	Windows Server 2019 Datacenter - Gen1
Size	Standard B1s (1 vcpu, 1 GiB memory)
Username	wvdadmin
Public inbound ports	None
Already have a Windows license?	No
Azure Spot	No

Disks

OS disk type	Premium SSD
Use managed disks	Yes
Data disks	1
Use ephemeral OS disk	No

Networking

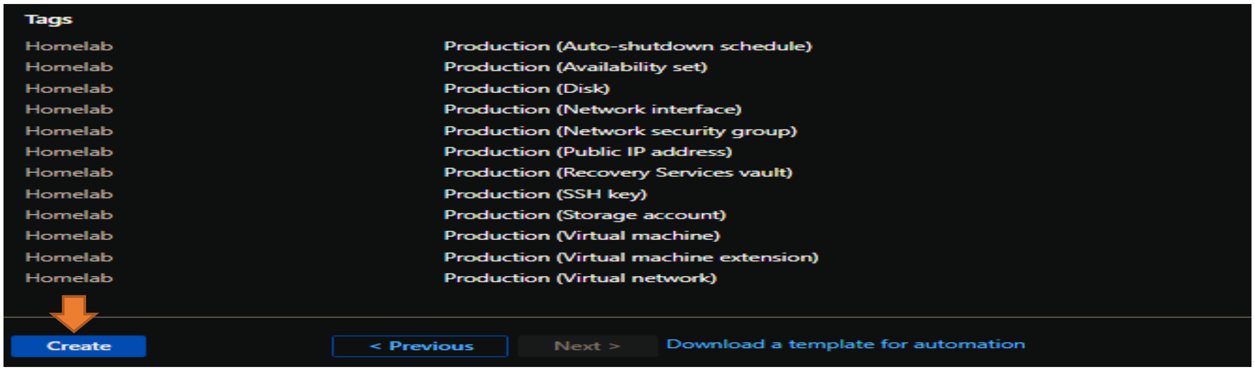
Virtual network	(new) LabVM-vnet
Subnet	(new) default (10.0.0.0/24)
Public IP	None
Accelerated networking	Off
Place this virtual machine behind an existing load balancing solution?	No

Management

Boot diagnostics	On
OS guest diagnostics	Off
Azure Security Center	Basic (free)
System assigned managed identity	Off
Auto-shutdown	On
Backup	Disabled
Patch installation	Manual patching: Install patches yourself or through a different patching solution.

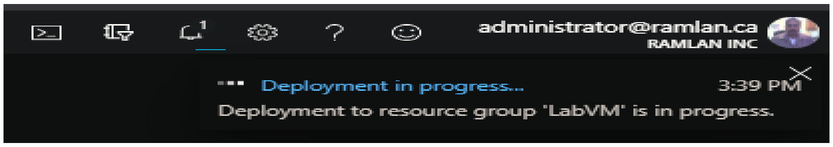
Advanced

Extensions	None
Cloud init	No
Proximity placement group	None



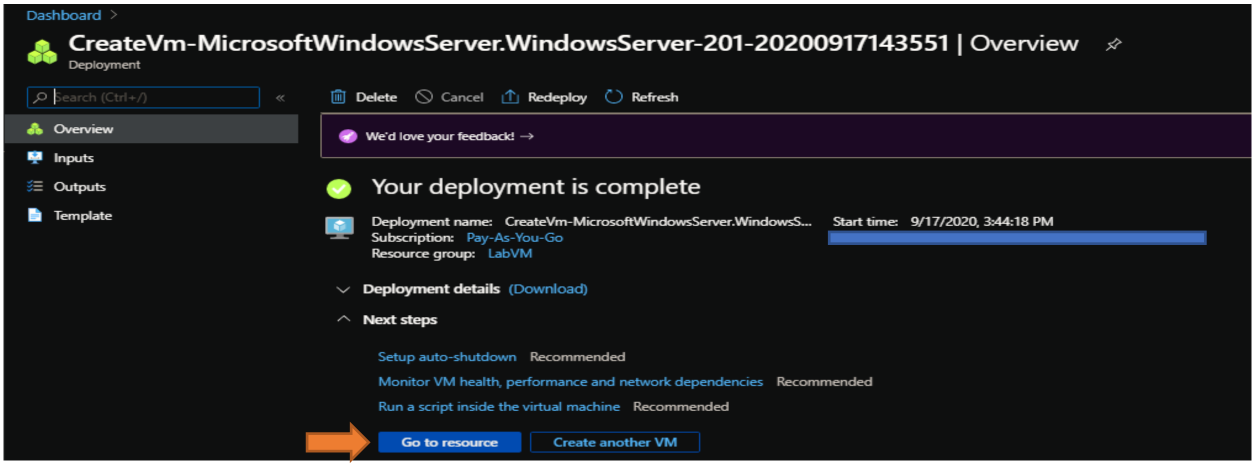
Tags

Homelab	Production (Auto-shutdown schedule)
Homelab	Production (Availability set)
Homelab	Production (Disk)
Homelab	Production (Network interface)
Homelab	Production (Network security group)
Homelab	Production (Public IP address)
Homelab	Production (Recovery Services vault)
Homelab	Production (SSH key)
Homelab	Production (Storage account)
Homelab	Production (Virtual machine)
Homelab	Production (Virtual machine extension)
Homelab	Production (Virtual network)



Deployment in progress... 3:39 PM

Deployment to resource group 'LabVM' is in progress.



CreateVm-MicrosoftWindowsServer.WindowsServer-201-20200917143551 | Overview

Deployment

Your deployment is complete

Deployment name: CreateVm-MicrosoftWindowsServer.WindowsS...
Start time: 9/17/2020, 3:44:18 PM [redacted]
Subscription: Pay-As-You-Go
Resource group: LabVM

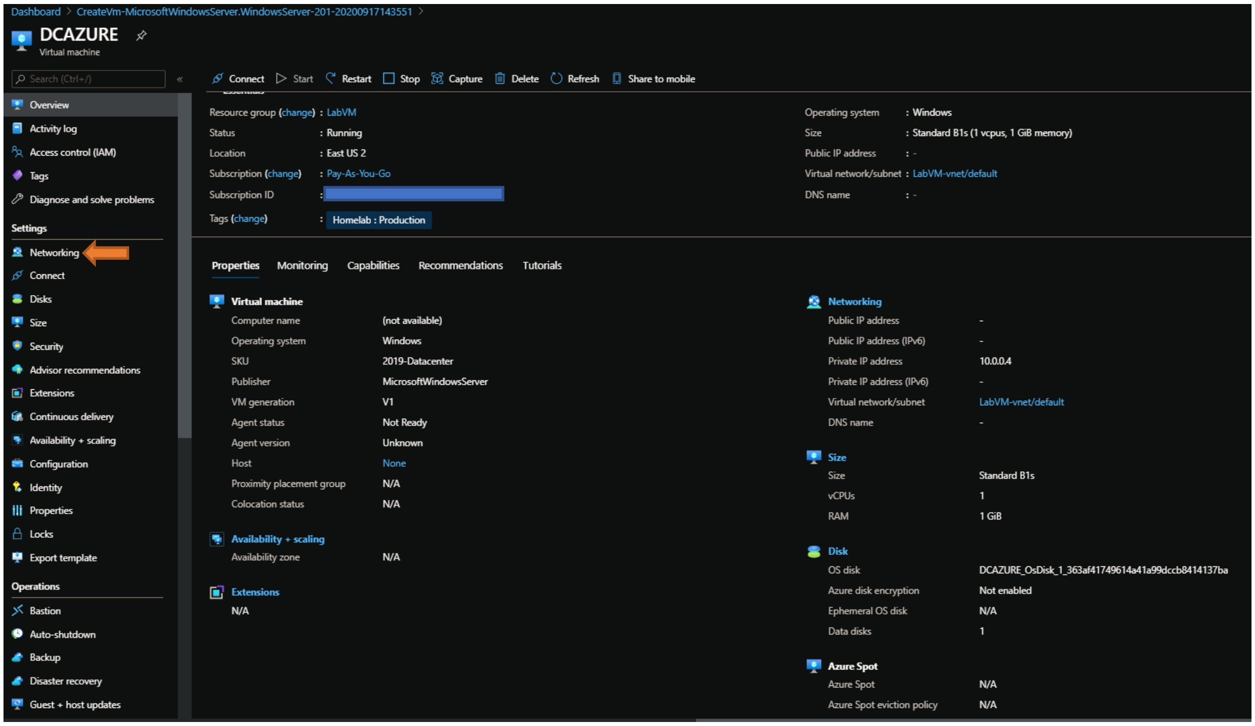
Deployment details (Download)

Next steps

Setup auto-shutdown Recommended

Monitor VM health, performance and network dependencies Recommended

Run a script inside the virtual machine Recommended



DCAZURE

Virtual machine

Resource group (change) : LabVM
Status : Running
Location : East US 2
Subscription (change) : Pay-As-You-Go
Subscription ID : [redacted]
Tags (change) : Homelab : Production

Operating system : Windows
Size : Standard B1s (1 vcpus, 1 GiB memory)
Public IP address : -
Virtual network/subnet : LabVM-vnet/default
DNS name : -

Virtual machine

Computer name	(not available)
Operating system	Windows
SKU	2019-Datacenter
Publisher	MicrosoftWindowsServer
VM generation	V1
Agent status	Not Ready
Agent version	Unknown
Host	None
Proximity placement group	N/A
Colocation status	N/A

Availability + scaling

Availability zone	N/A

Extensions

N/A

Networking

Public IP address	-
Public IP address (IPv6)	-
Private IP address	10.0.0.4
Private IP address (IPv6)	-
Virtual network/subnet	LabVM-vnet/default
DNS name	-

Size

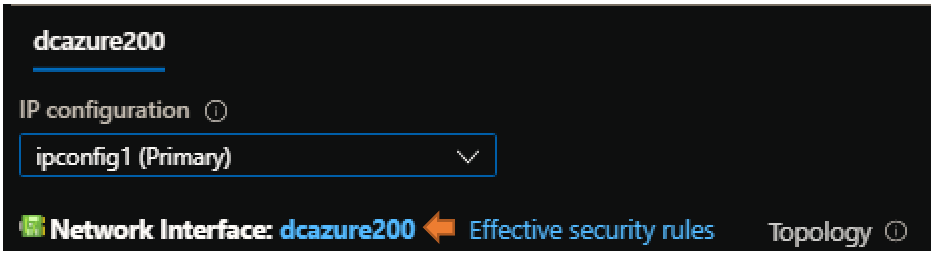
Size	Standard B1s
vCPUs	1
RAM	1 GiB

Disk

OS disk	DCAZURE_OsDisk_1_363af41749614a41a99dccb8414137ba
Azure disk encryption	Not enabled
Ephemeral OS disk	N/A
Data disks	1

Azure Spot

Azure Spot	N/A
Azure Spot eviction policy	N/A

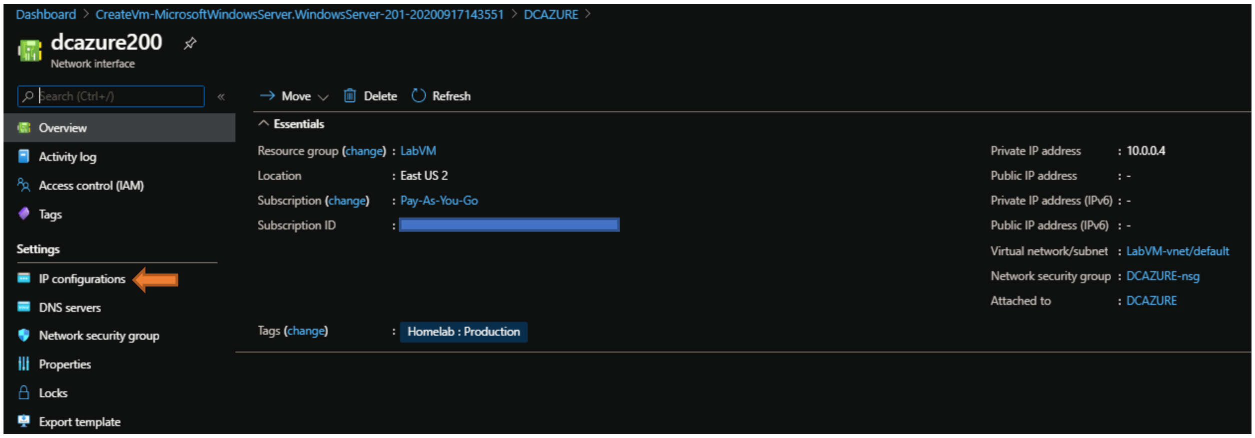


dcazure200

IP configuration ⓘ

ipconfig1 (Primary)

Network Interface: dcazure200



Dashboard > CreateVm-MicrosoftWindowsServer.WindowsServer-201-20200917143551 > DCAZURE >

dcazure200

Network interface

Resource group (change) : LabVM

Location : East US 2

Subscription (change) : Pay-As-You-Go

Subscription ID : [redacted]

Tags (change) : Homelab : Production

Private IP address : 10.0.0.4

Public IP address : -

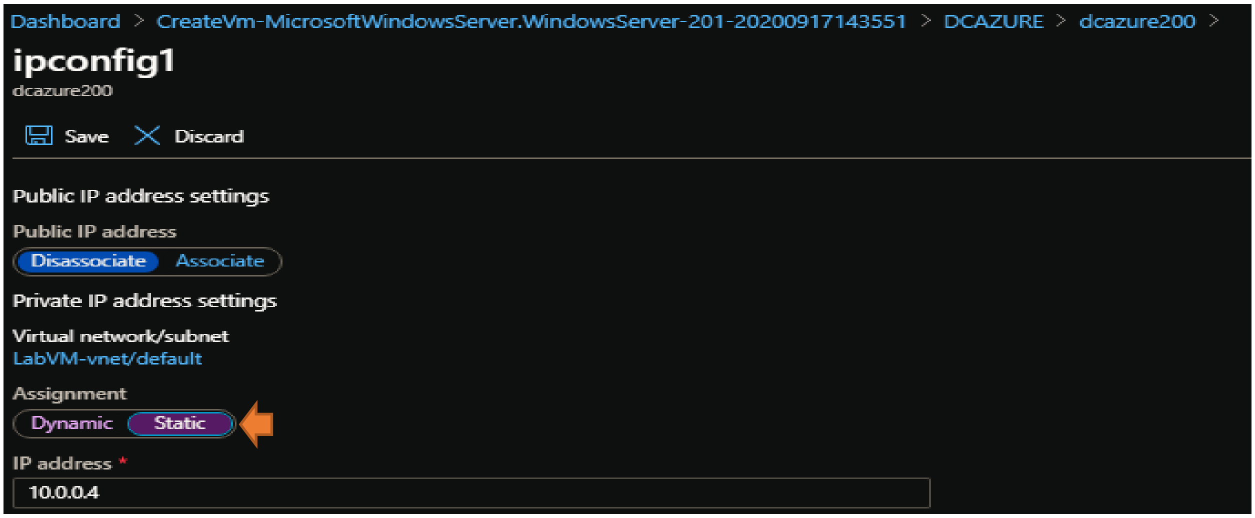
Private IP address (IPv6) : -

Public IP address (IPv6) : -

Virtual network/subnet : LabVM-vnet/default

Network security group : DCAZURE-nsg

Attached to : DCAZURE



Dashboard > CreateVm-MicrosoftWindowsServer.WindowsServer-201-20200917143551 > DCAZURE > dcazure200 >

ipconfig1

dcazure200

Public IP address settings

Public IP address

Disassociate | Associate

Private IP address settings

Virtual network/subnet

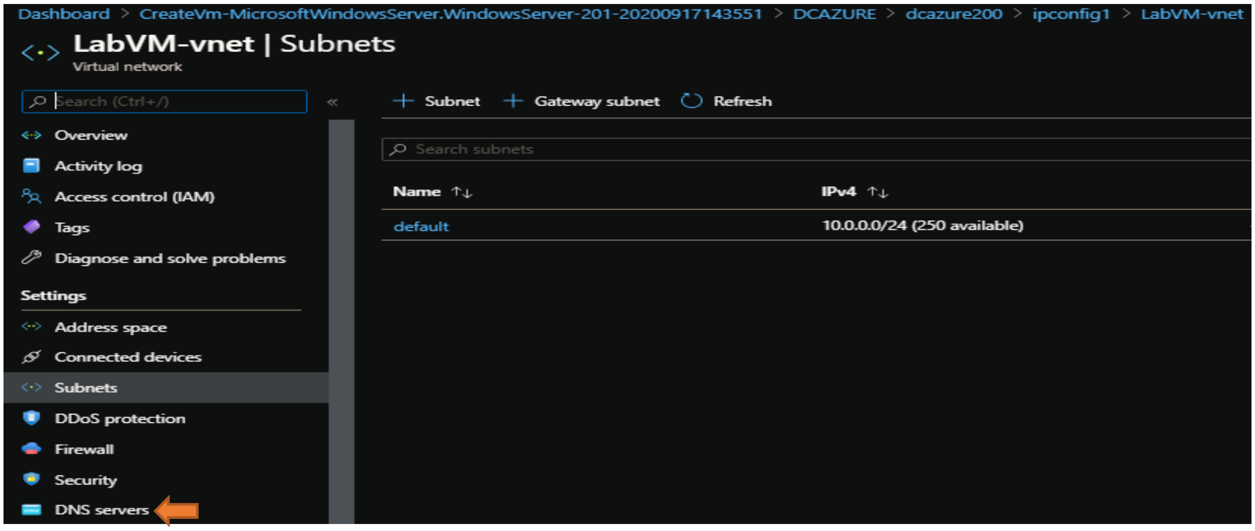
LabVM-vnet/default

Assignment

Dynamic | Static

IP address *

10.0.0.4



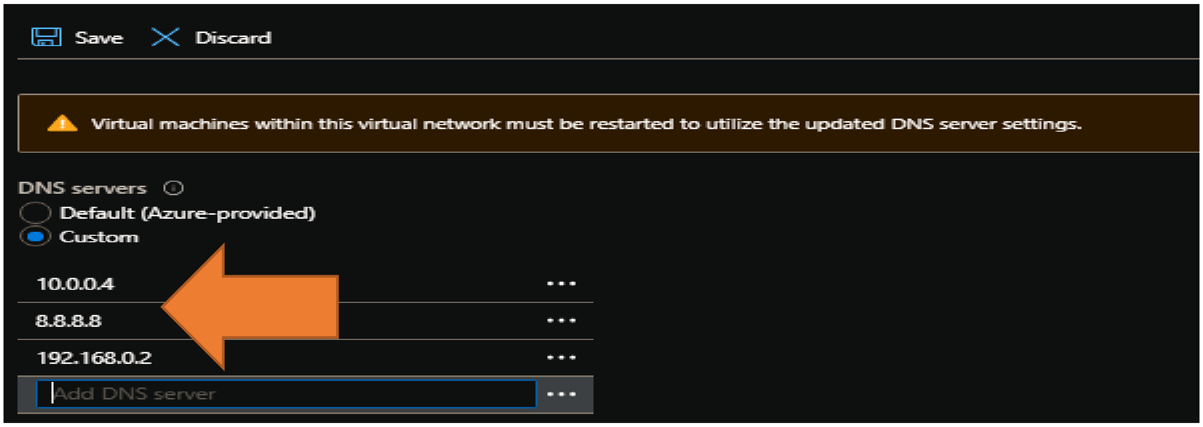
Dashboard > CreateVm-MicrosoftWindowsServer.WindowsServer-201-20200917143551 > DCAZURE > dcazure200 > ipconfig1 > LabVM-vnet

LabVM-vnet | Subnets

Virtual network

Name ↑↓	IPv4 ↑↓
default	10.0.0.0/24 (250 available)

The address 10.0.0.4 will be our DCAZURE, 8.8.8.8 is Google DNS & 192.168.0.2 is On Premise DNS



Virtual machines within this virtual network must be restarted to utilize the updated DNS server settings.

DNS servers

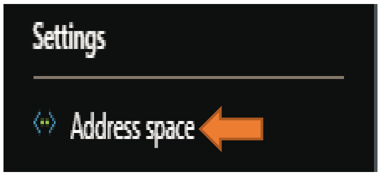
○ Default (Azure-provided)

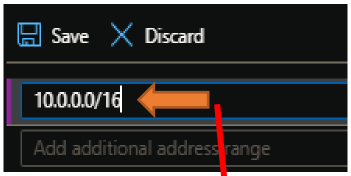
● Custom

10.0.0.4

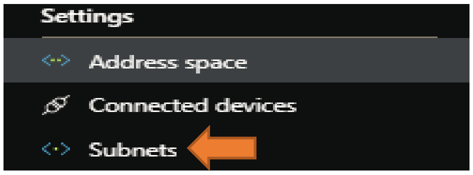
8.8.8.8

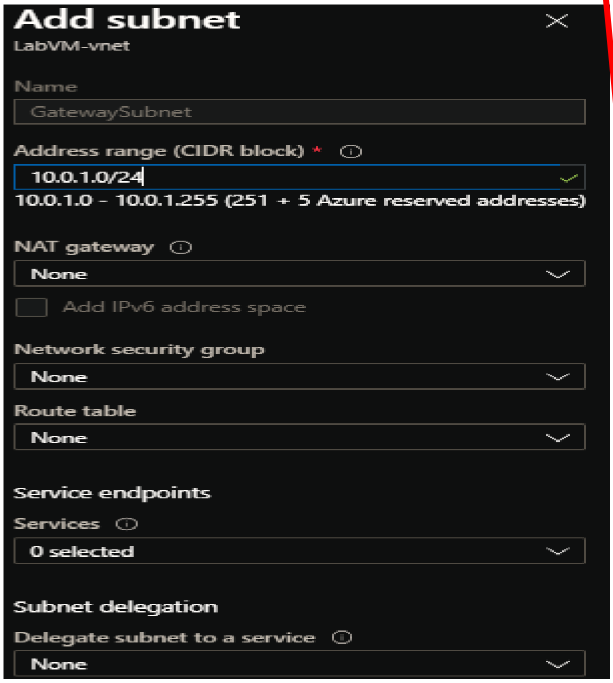
192.168.0.2





10.0.0.0/16





Add subnet

LabVM-vnet

Name: GatewaySubnet

Address range (CIDR block) *: 10.0.1.0/24

10.0.1.0 - 10.0.1.255 (251 + 5 Azure reserved addresses)

NAT gateway: None

□ Add IPv6 address space

Network security group: None

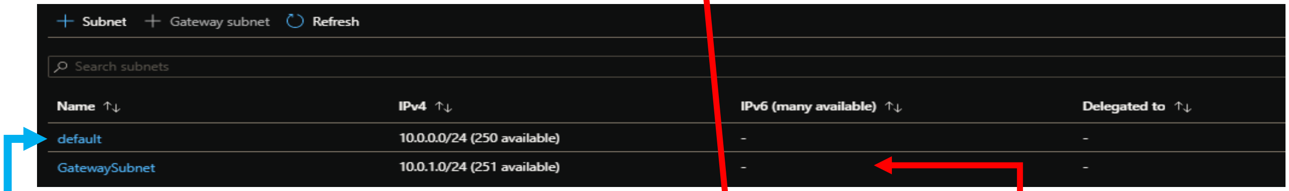
Route table: None

Service endpoints

Services: 0 selected

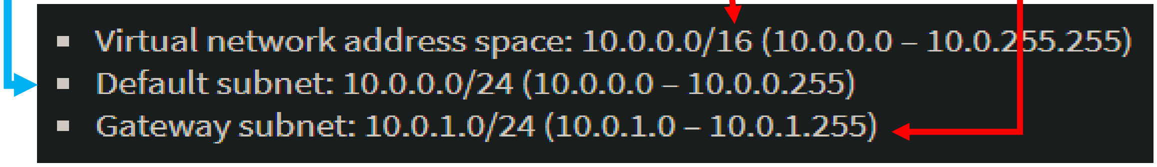
Subnet delegation

Delegate subnet to a service: None



Name ↑↓	IPv4 ↑↓	IPv6 (many available) ↑↓	Delegated to ↑↓
default	10.0.0.0/24 (250 available)	-	-
GatewaySubnet	10.0.1.0/24 (251 available)	-	-

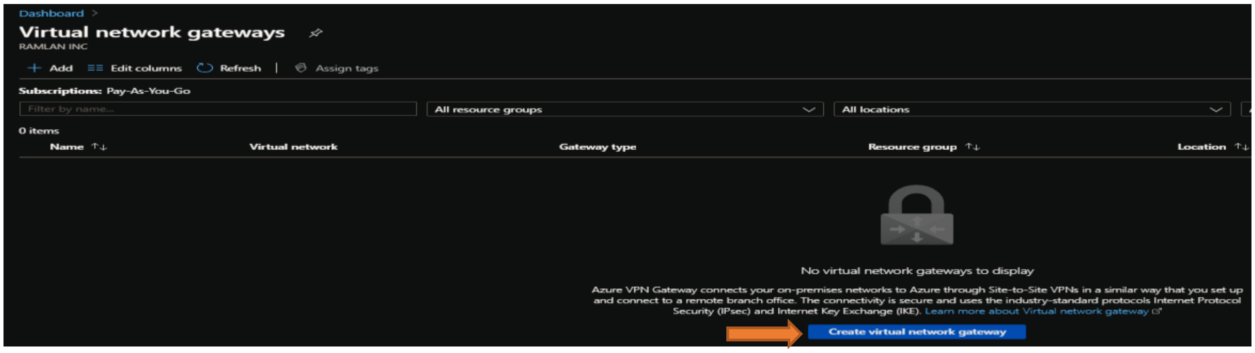
This will be out network configuration in Cloud Azure



- Virtual network address space: 10.0.0.0/16 (10.0.0.0 – 10.0.255.255)
- Default subnet: 10.0.0.0/24 (10.0.0.0 – 10.0.0.255)
- Gateway subnet: 10.0.1.0/24 (10.0.1.0 – 10.0.1.255)

PART 9:

VPN Configuration – P2S - First, we need to set up a Point to Site VPN connection so we can manage the VM(s) without having to enable RDP over the public internet. To do this, first, use the "Search" in the Azure portal to search for "virtual network gateway," then click on "Virtual network gateways" found in the results. Next, click on "Add" or "Create a virtual network gateway" to continue.



Virtual network gateways
RAMLAN INC

Subscriptions: Pay-As-You-Go

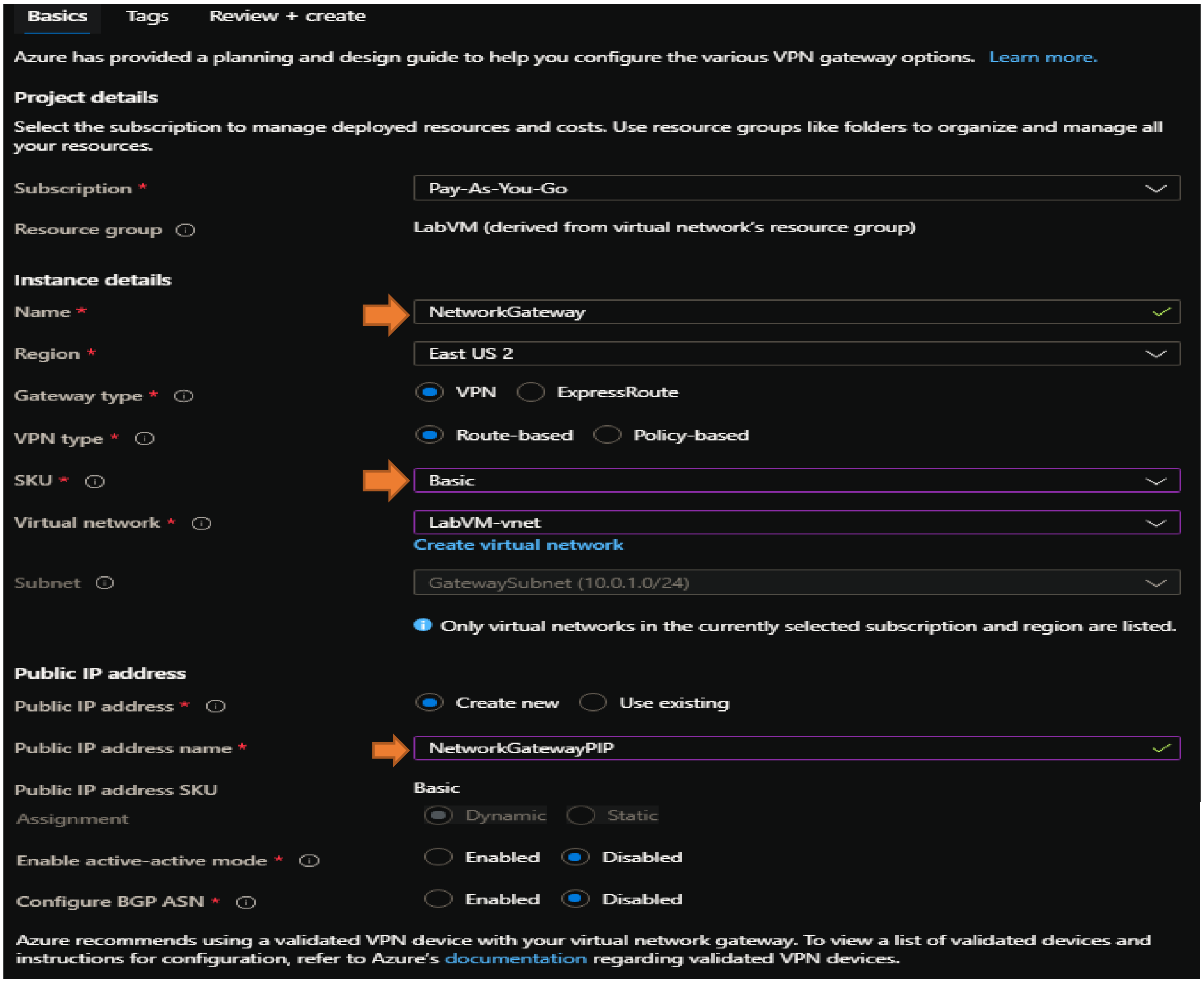
Filter by name... | All resource groups | All locations

0 items

Name ↑↓	Virtual network	Gateway type	Resource group ↑↓	Location ↑↓

No virtual network gateways to display

Azure VPN Gateway connects your on-premises networks to Azure through Site-to-Site VPNs in a similar way that you set up and connect to a remote branch office. The connectivity is secure and uses the industry-standard protocols Internet Protocol Security (IPsec) and Internet Key Exchange (IKE). Learn more about Virtual network gateway



Azure has provided a planning and design guide to help you configure the various VPN gateway options. 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 *	Pay-As-You-Go
Resource group ⓘ	LabVM (derived from virtual network's resource group)

Instance details

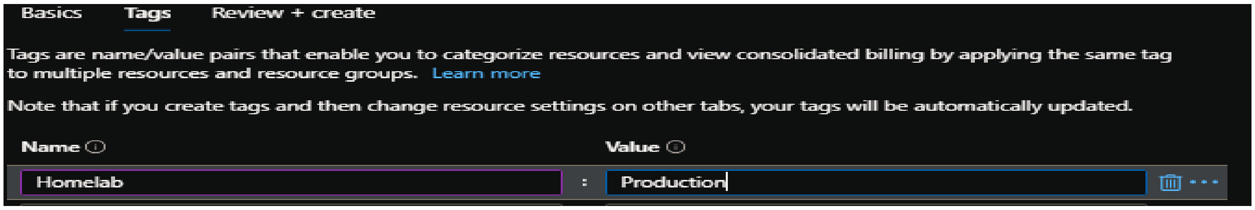
Name *	NetworkGateway ✓
Region *	East US 2
Gateway type * ⓘ	● VPN ○ ExpressRoute
VPN type * ⓘ	● Route-based ○ Policy-based
SKU * ⓘ	Basic
Virtual network * ⓘ	LabVM-vnet Create virtual network
Subnet ⓘ	GatewaySubnet (10.0.1.0/24)

ⓘ Only virtual networks in the currently selected subscription and region are listed.

Public IP address

Public IP address * ⓘ	● Create new ○ Use existing
Public IP address name *	NetworkGatewayPIP ✓
Public IP address SKU	Basic
Assignment	● Dynamic ○ Static
Enable active-active mode * ⓘ	○ Enabled ● Disabled
Configure BGP ASN * ⓘ	○ Enabled ● Disabled

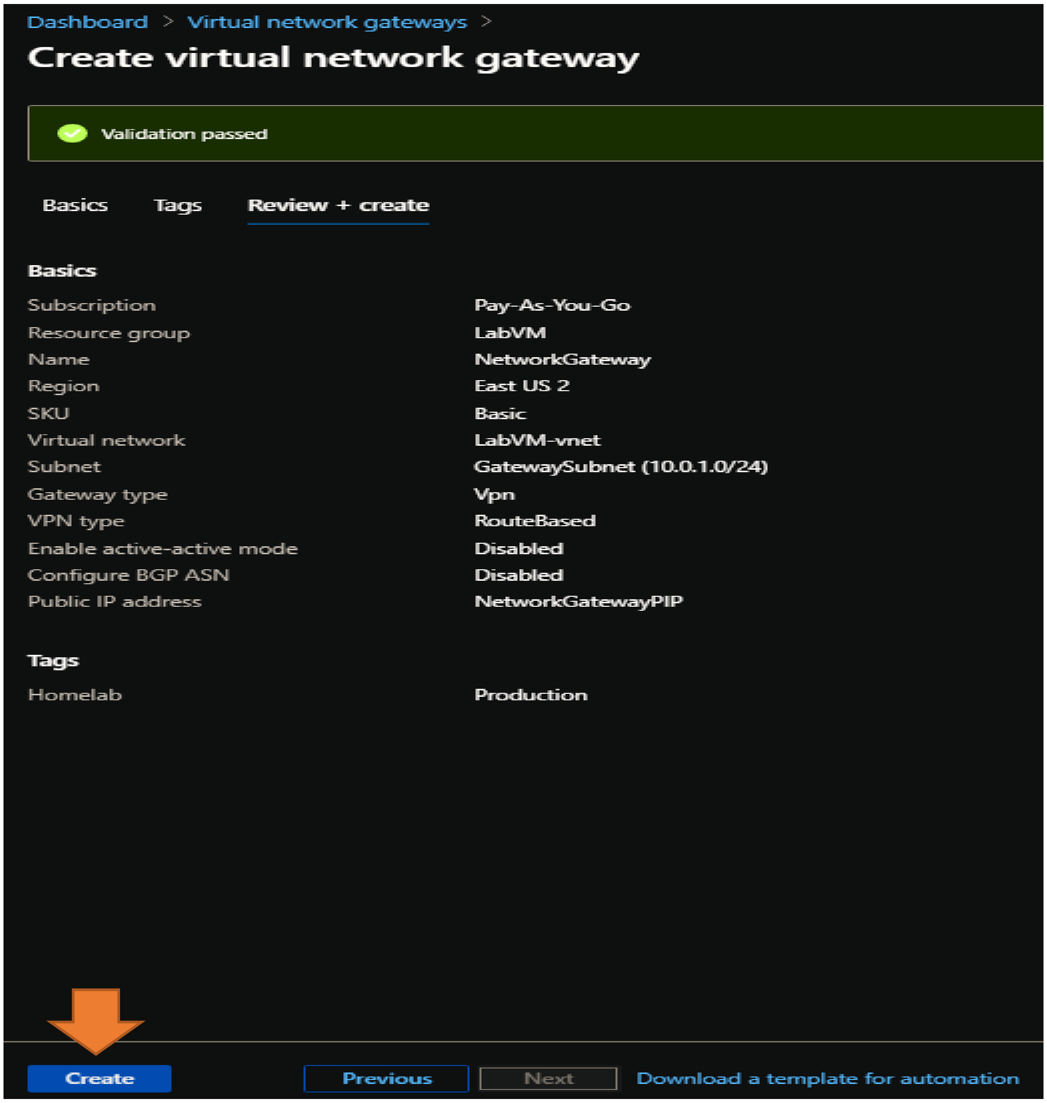
Azure recommends using a validated VPN device with your virtual network gateway. To view a list of validated devices and instructions for configuration, refer to Azure's documentation regarding validated VPN devices.



Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Learn more

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name ⓘ		Value ⓘ
Homelab	:	Production



Create virtual network gateway

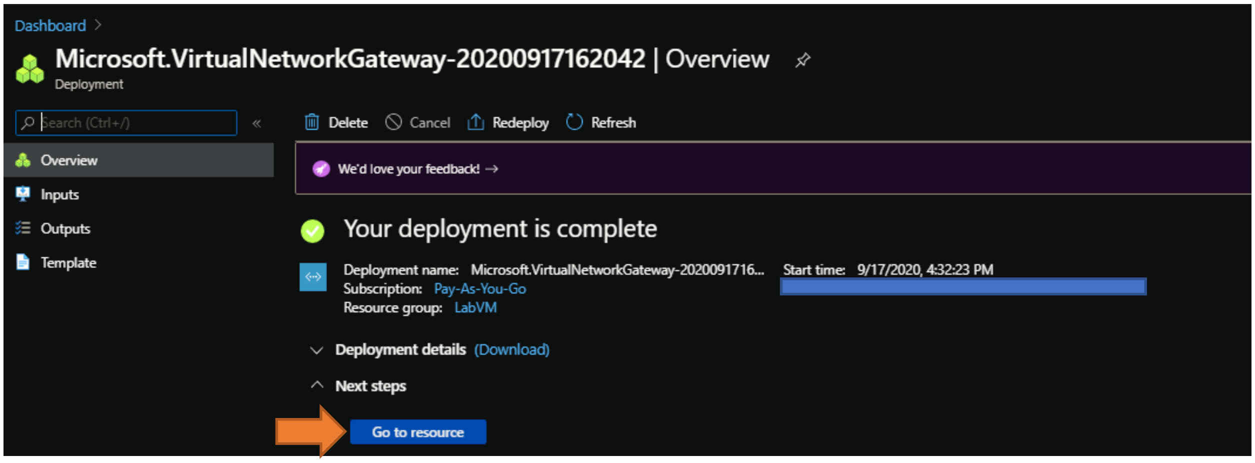
✓ Validation passed

Basics

Subscription	Pay-As-You-Go
Resource group	LabVM
Name	NetworkGateway
Region	East US 2
SKU	Basic
Virtual network	LabVM-vnet
Subnet	GatewaySubnet (10.0.1.0/24)
Gateway type	Vpn
VPN type	RouteBased
Enable active-active mode	Disabled
Configure BGP ASN	Disabled
Public IP address	NetworkGatewayPIP

Tags

Homelab	Production



Microsoft.VirtualNetworkGateway-20200917162042 | Overview

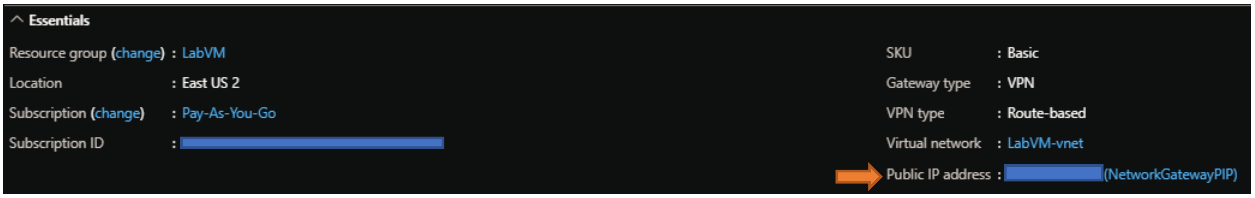
Deployment

✓ Your deployment is complete

Deployment name: Microsoft.VirtualNetworkGateway-2020091716... Start time: 9/17/2020, 4:32:23 PM
[redacted]
Subscription: Pay-As-You-Go
Resource group: LabVM

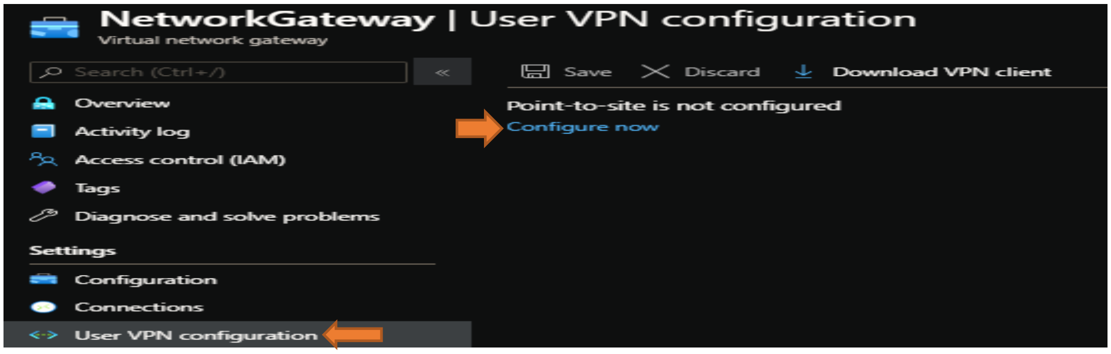
Deployment details (Download)

Next steps

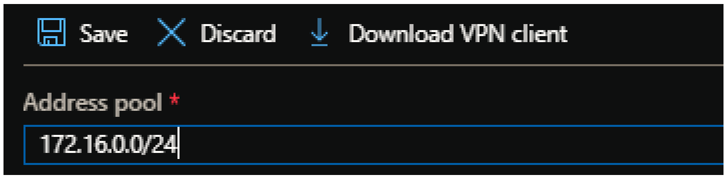

Essentials

Resource group (change)	: LabVM	SKU	: Basic
Location	: East US 2	Gateway type	: VPN
Subscription (change)	: Pay-As-You-Go	VPN type	: Route-based
Subscription ID	: [redacted]	Virtual network	: LabVM-vnet
		Public IP address	: [redacted] (NetworkGatewayPIP)

Once the deployment is successful, click on the “Go to resource” button if available, if not then select “All resources” from the left column in the portal and then click on the network gateway name you created in the previous step. If you have many resources, it may help to use the filter.

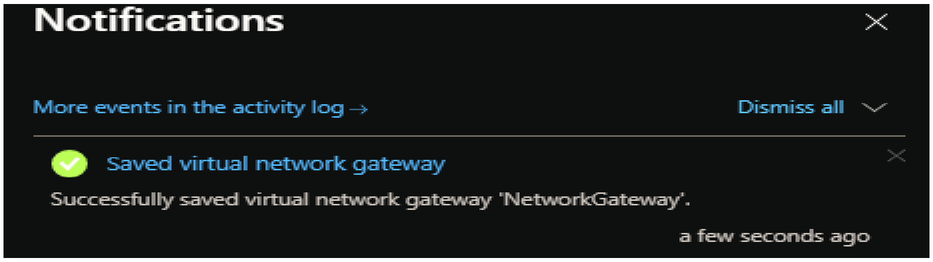


Point-to-site is not configured



Address pool * 172.16.0.0/24

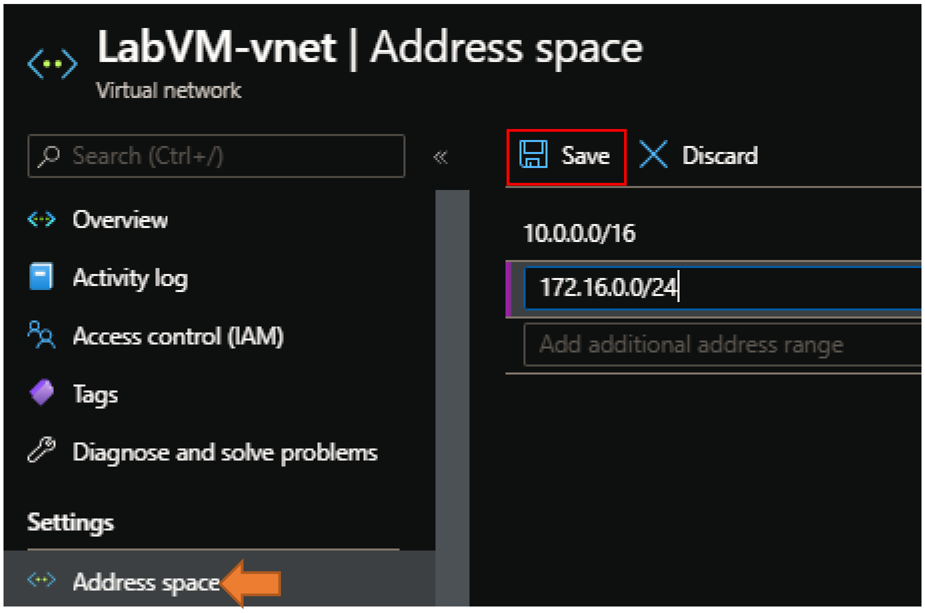
For the “Address Pool” enter any private internet range (i.e., 172.16.0.0/24) that is not present in your Azure Virtual Network range (if you followed my steps correctly, then do not use anything within 10.0.0.0/16 (10.0.0.0 – 10.0.255.255), then click “Save.” Regardless of which network address, remember to go back to your Virtual Network and add it in as an additional address space. You may want to draw out your IP configuration on paper to get a mental picture of how it is all connected.



Saved virtual network gateway

Successfully saved virtual network gateway 'NetworkGateway'.

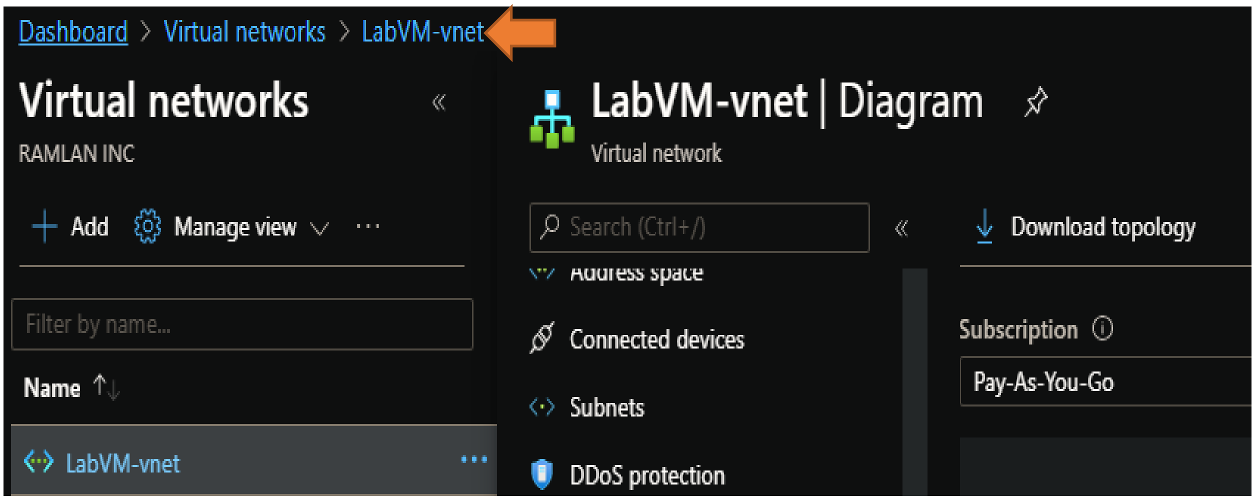
a few seconds ago

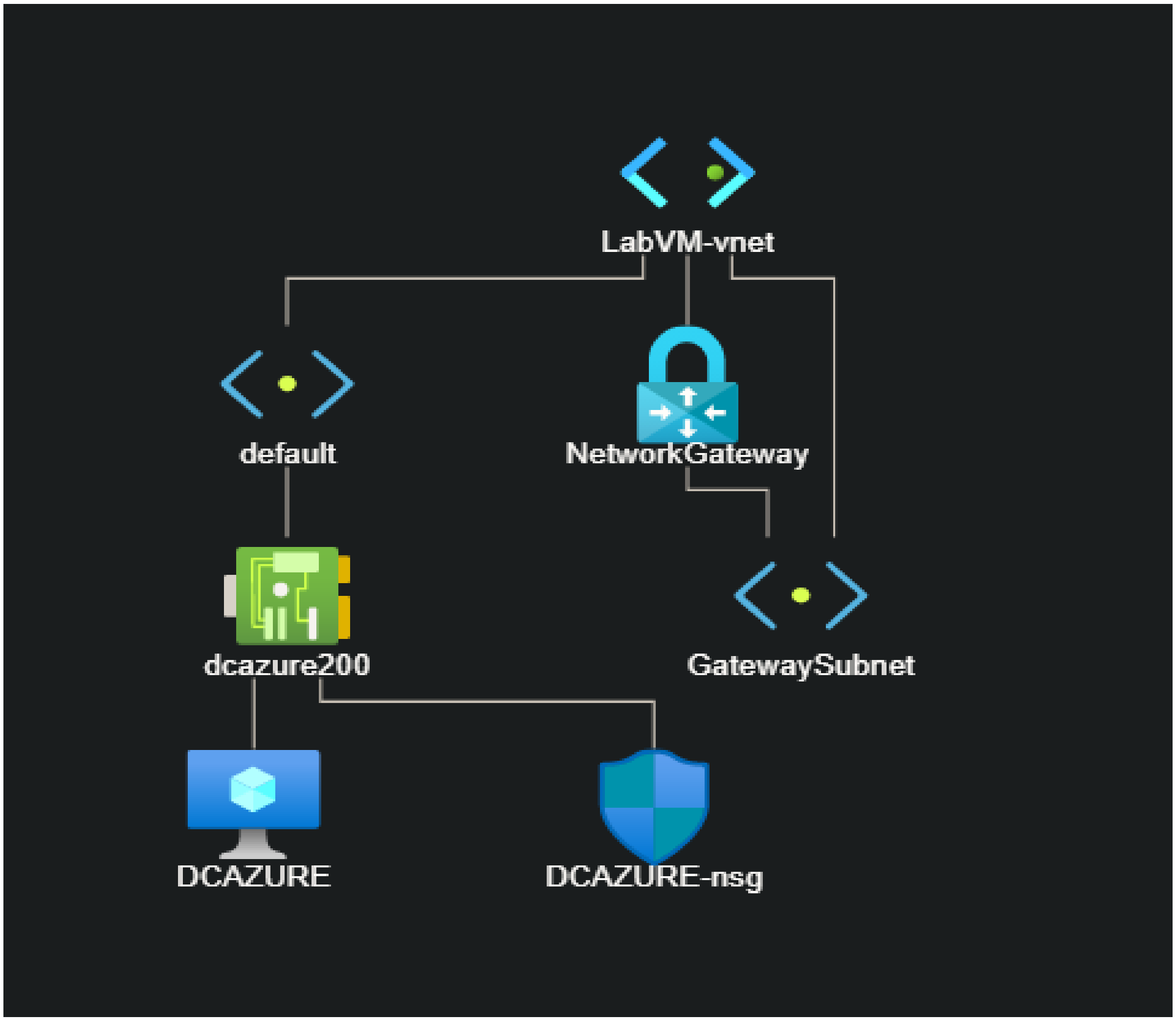


10.0.0.0/16

172.16.0.0/24

Below is our P2S network diagram. I downloaded this from Azure Portal after the configuration.



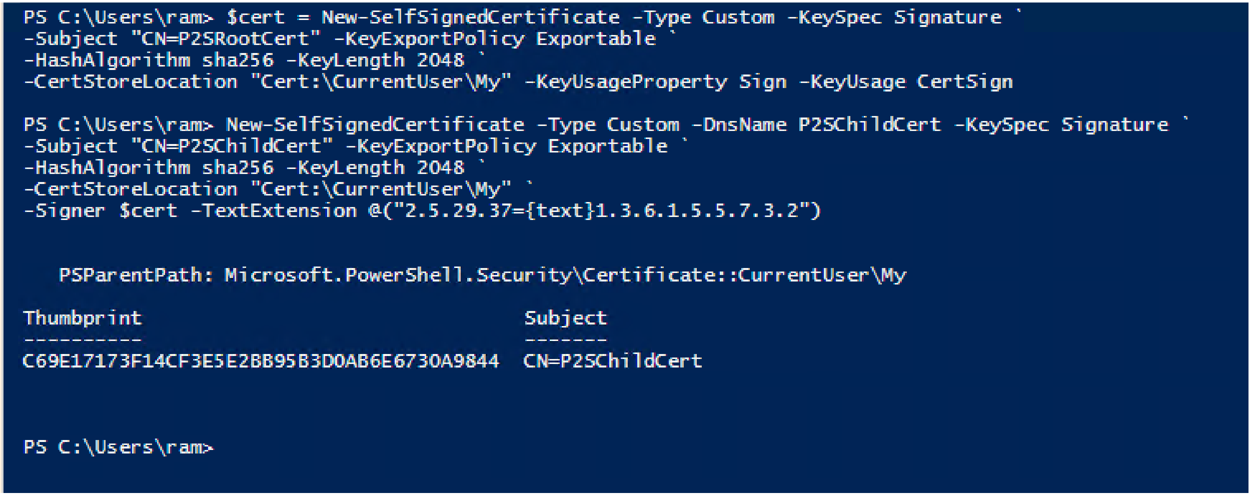


Root and Child Certificates – You can get the script from here - https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-certificates-point-to-site

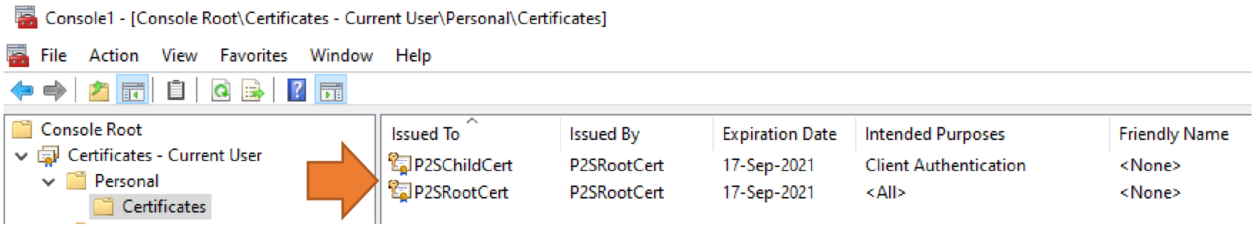
Open PowerShell ISE as Administrator and run these commands

$cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature \`
-Subject "CN=**P2SRootCert**" -KeyExportPolicy Exportable \`
-HashAlgorithm sha256 -KeyLength 2048 \`
-CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -KeyUsage CertSign

New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec Signature \`
-Subject "CN=**P2SChildCert**" -KeyExportPolicy Exportable \`
-HashAlgorithm sha256 -KeyLength 2048 \`
-CertStoreLocation "Cert:\CurrentUser\My" \`
-Signer $cert -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2")



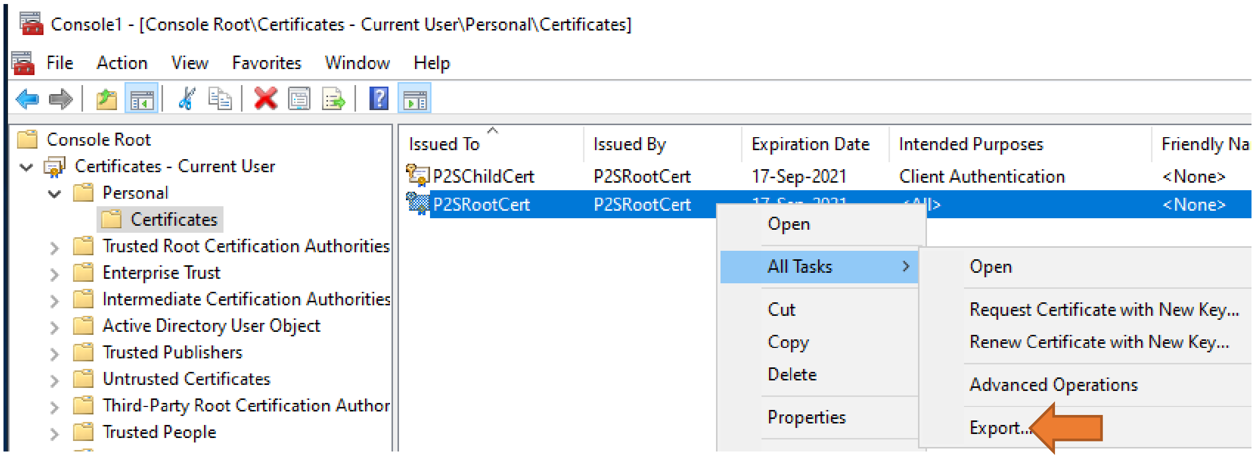
```
PS C:\Users\ram> $cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature `
-Subject "CN=P2SRootCert" -KeyExportPolicy Exportable `
-HashAlgorithm sha256 -KeyLength 2048 `
-CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -KeyUsage CertSign

PS C:\Users\ram> New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec Signature `
-Subject "CN=P2SChildCert" -KeyExportPolicy Exportable `
-HashAlgorithm sha256 -KeyLength 2048 `
-CertStoreLocation "Cert:\CurrentUser\My" `
-Signer $cert -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2")


   PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\My

Thumbprint                                Subject
----------                                -------
C69E17173F14CF3E5E2BB95B3D0AB6E6730A9844  CN=P2SChildCert


PS C:\Users\ram>
```



Console1 - [Console Root\Certificates - Current User\Personal\Certificates]

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
P2SChildCert	P2SRootCert	17-Sep-2021	Client Authentication	<None>
P2SRootCert	P2SRootCert	17-Sep-2021	<All>	<None>

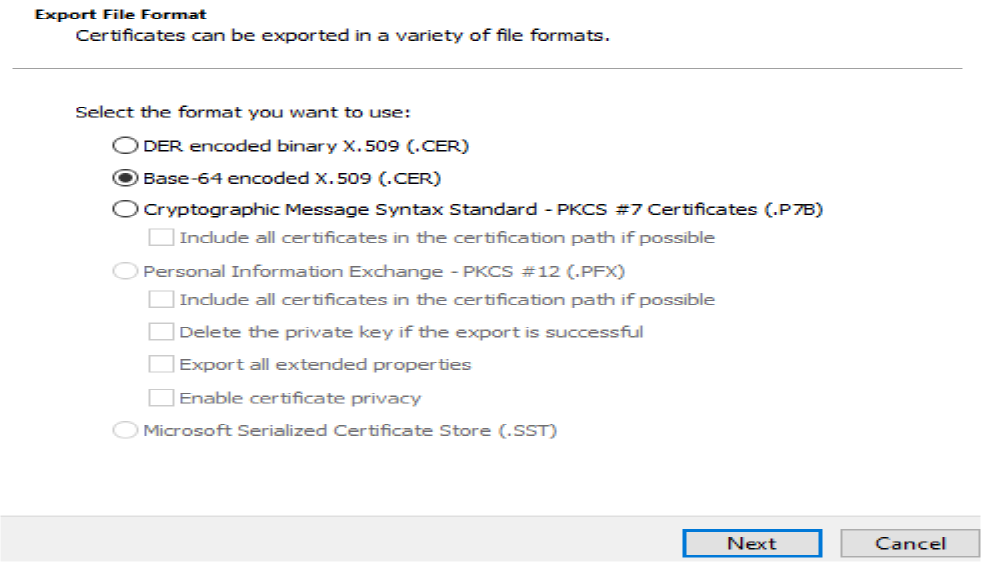
Now we will export P2SRootCert and use the CSR into Azure VPN Address Pool 172.16.0.0/24



Console1 - [Console Root\Certificates - Current User\Personal\Certificates]

File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Author
Trusted People
Open
All Tasks
Cut
Copy
Delete
Properties
Open
Request Certificate with New Key...
Renew Certificate with New Key...
Advanced Operations
Export...

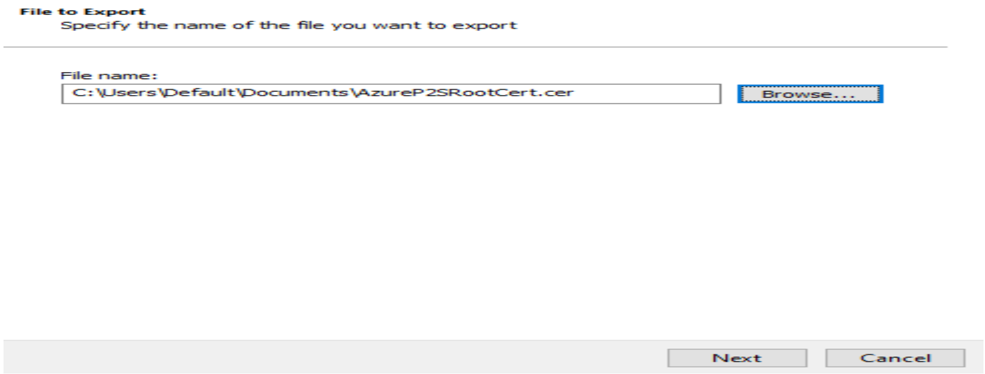
Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Na
P2SChildCert	P2SRootCert	17-Sep-2021	Client Authentication	<None>
P2SRootCert	P2SRootCert	17-Sep-2021	<All>	<None>



Export File Format
Certificates can be exported in a variety of file formats.

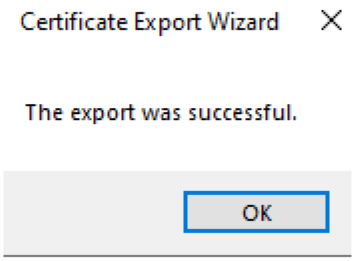
Select the format you want to use:

- ○ DER encoded binary X.509 (.CER)
- ● Base-64 encoded X.509 (.CER)
- ○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  - □ Include all certificates in the certification path if possible
- ○ Personal Information Exchange - PKCS #12 (.PFX)
  - □ Include all certificates in the certification path if possible
  - □ Delete the private key if the export is successful
  - □ Export all extended properties
  - □ Enable certificate privacy
- ○ Microsoft Serialized Certificate Store (.SST)



File to Export
Specify the name of the file you want to export

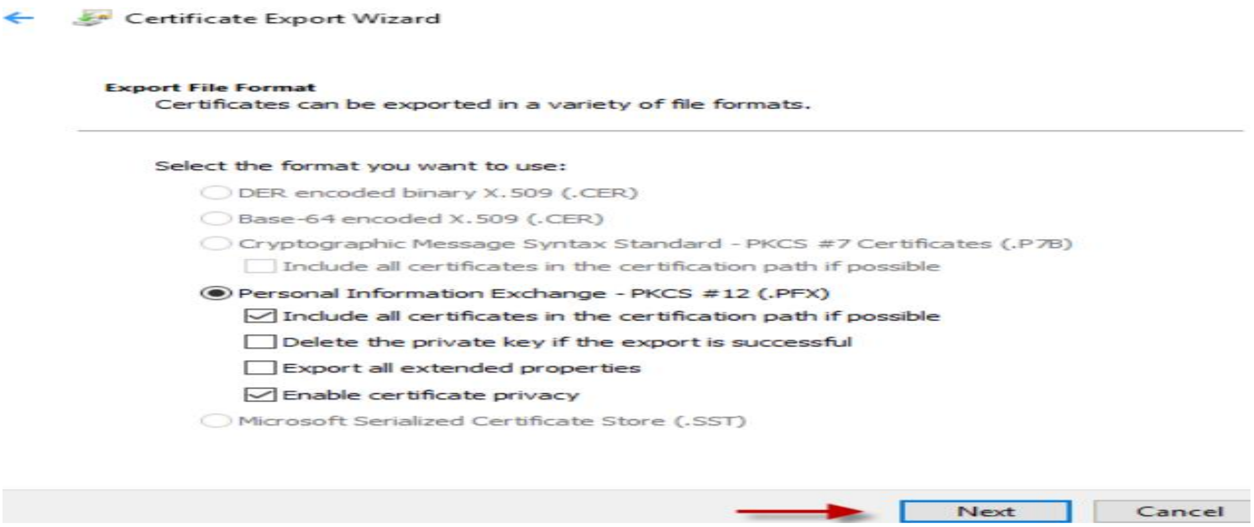
File name:
C:\Users\Default\Documents\AzureP2SRootCert.cer



Certificate Export Wizard

The export was successful.

Export Point to Site Client Certificate

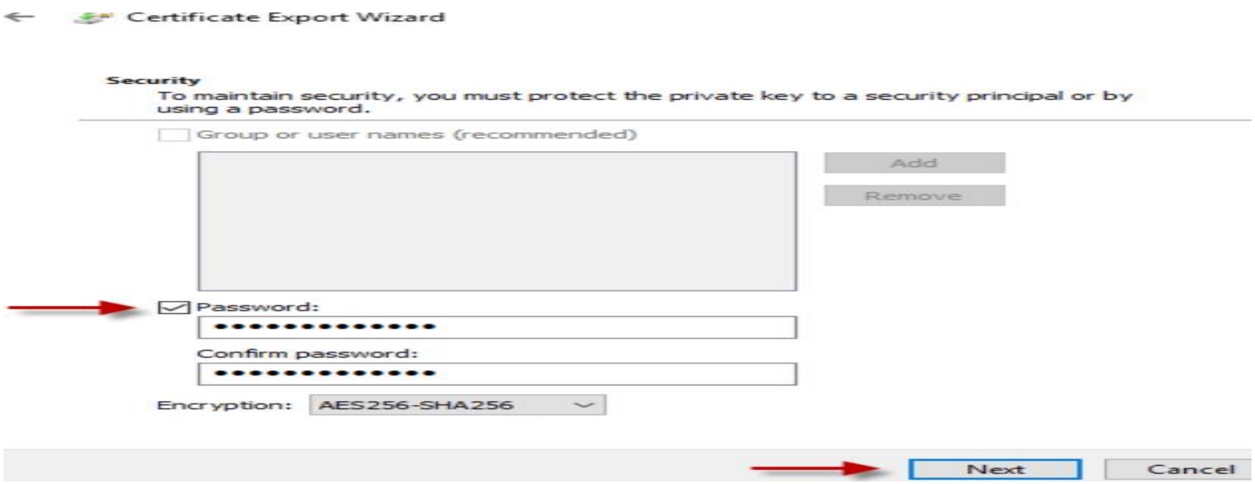


Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

- ○ DER encoded binary X.509 (.CER)
- ○ Base-64 encoded X.509 (.CER)
- ○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  - □ Include all certificates in the certification path if possible
- ● Personal Information Exchange - PKCS #12 (.PFX)
  - ☑ Include all certificates in the certification path if possible
  - □ Delete the private key if the export is successful
  - □ Export all extended properties
  - ☑ Enable certificate privacy
- ○ Microsoft Serialized Certificate Store (.SST)



Certificate Export Wizard

Security

To maintain security, you must protect the private key to a security principal or by using a password.

□ Group or user names (recommended)

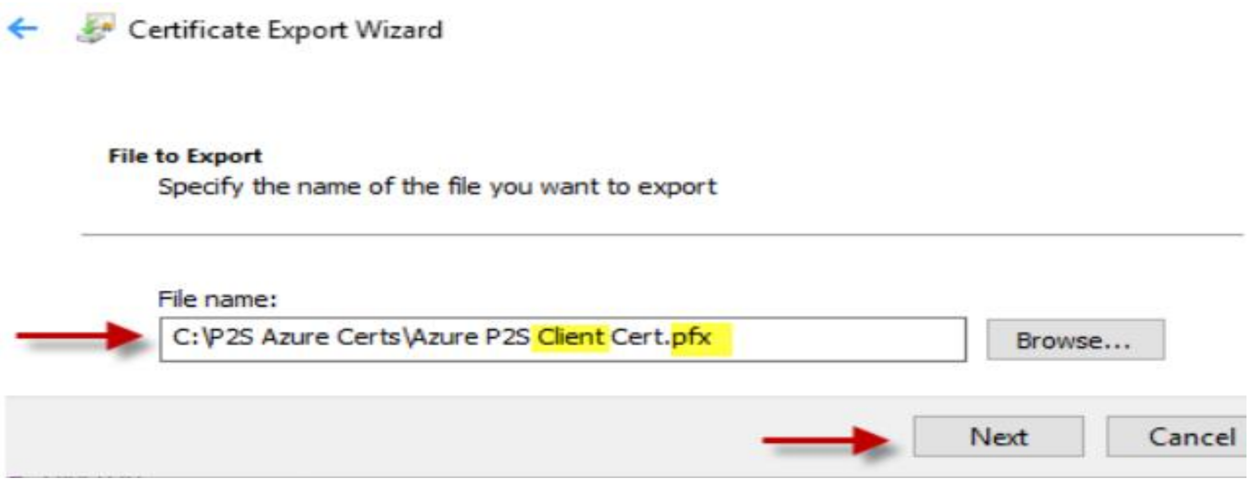
☑ Password:

••••••••••••••

Confirm password:

••••••••••••••

Encryption: AES256-SHA256



Certificate Export Wizard

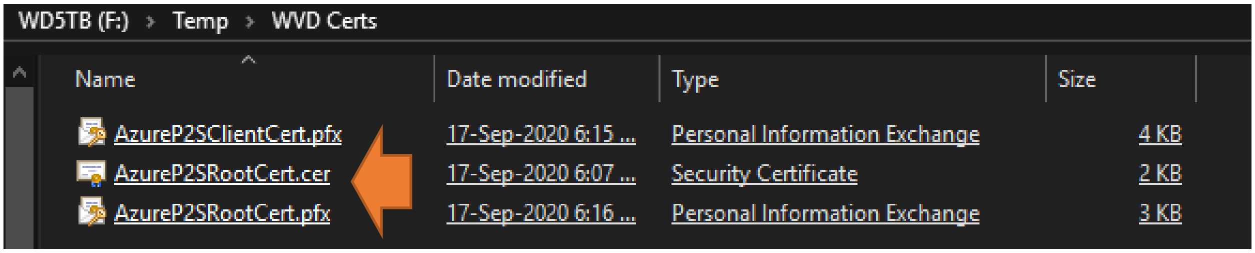
File to Export

Specify the name of the file you want to export

File name:

C:\P2S Azure Certs\Azure P2S Client Cert.pfx

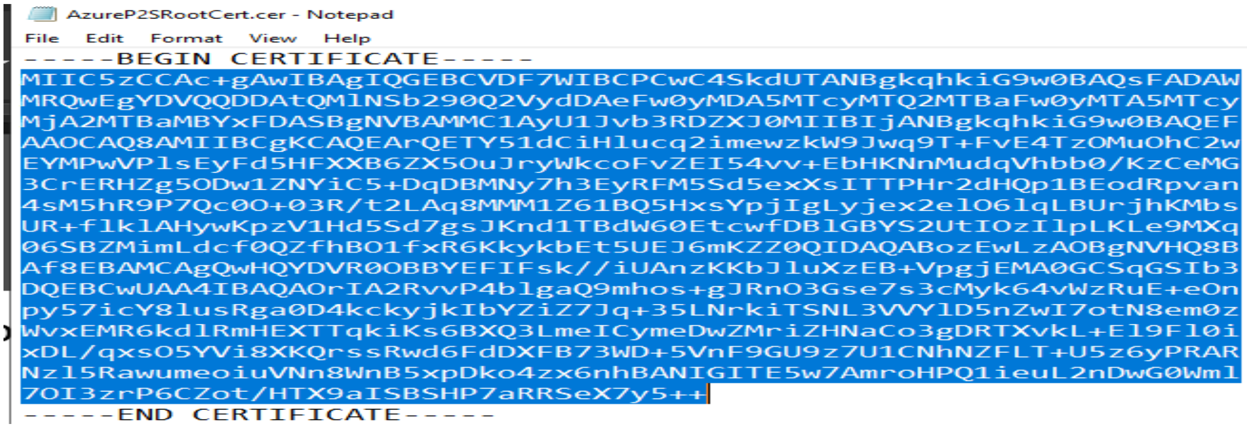
Do the same for P2SRoot Certificate as well. When all export done you should have this



WD5TB (F:) › Temp › WVD Certs

Name	Date modified	Type	Size
AzureP2SClientCert.pfx	17-Sep-2020 6:15 ...	Personal Information Exchange	4 KB
AzureP2SRootCert.cer	17-Sep-2020 6:07 ...	Security Certificate	2 KB
AzureP2SRootCert.pfx	17-Sep-2020 6:16 ...	Personal Information Exchange	3 KB

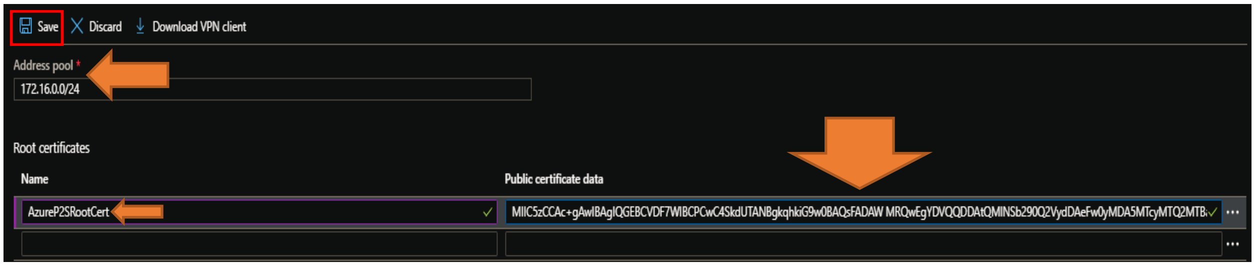
Open AzureP2SRootCert.cer in notepad – Select highlighted range - Copy



AzureP2SRootCert.cer - Notepad

```
-----BEGIN CERTIFICATE-----
MIIC5zCCAc+gAwIBAgIQGEBCVDF7WIBCPCwC4SkdUTANBgkqhkiG9w0BAQsFADAW
MRQwEgYDVQQDDAtQMlNSb290Q2VydDAeFw0yMDA5MTcyMTQ2MTBaFw0yMTA5MTcy
MjA2MTBaMBYxFDASBgNVBAMMC1AyU1Jvb3RDZXJ0MIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEArQETY51dCiHlucq2imewzkW9Jwq9T+FvE4TzOMuOhC2w
EYMPwVPlsEyFd5HFXXB6ZX5OuJryWkcoFvZEI54vv+EbHKNnMudqVhbb0/KzCeMG
3CrERHZg5ODw1ZNYiC5+DqDBMNy7h3EyRFM5Sd5exXsITTPHr2dHQp1BEodRpvan
4sM5hR9P7Qc0O+03R/t2LAq8MMM1Z61BQ5HxsYpjIgLyjex2el06lqLBUrjhKMbs
UR+flklAHywKpzV1Hd5Sd7gsJKnd1TBdW60EtcwfDBlGBYS2UtIOzIlpLKLe9MXq
06SBZMimLdcf0QZfhBO1fxR6KkykbEt5UEJ6mKZZ0QIDAQABozEwLzAOBgNVHQ8B
Af8EBAMCAgQwHQYDVR0OBBYEFIFsk//iUAnzKKbJluXzEB+VpgjEMA0GCSqGSIb3
DQEBCwUAA4IBAQAOrIA2RvvP4blgaQ9mhos+gJRnO3Gse7s3cMyk64vWzRuE+eOn
py57icY8lusRga0D4kckyjkIbYZiZ7Jq+35LNrkiTSNL3VVYlD5nZwI7otN8em0z
WvxEMR6kdlRmHEXTTqkiKs6BXQ3LmeICymeDwZMriZHNaCo3gDRTXvkL+El9Fl0i
xDL/qxsO5YVi8XKQrssRwd6FdDXFB73WD+5VnF9GU9z7U1CNhNZFLT+U5z6yPRAR
Nzl5RawumeoiuVNn8WnB5xpDko4zx6nhBANIGITE5w7AmroHPQ1ieuL2nDwG0Wml
7OI3zrP6CZot/HTX9aISBSHP7aRRSeX7y5++
-----END CERTIFICATE-----
```

Go to Azure Portal at below location and paste under Public Certificate Data & Click Save

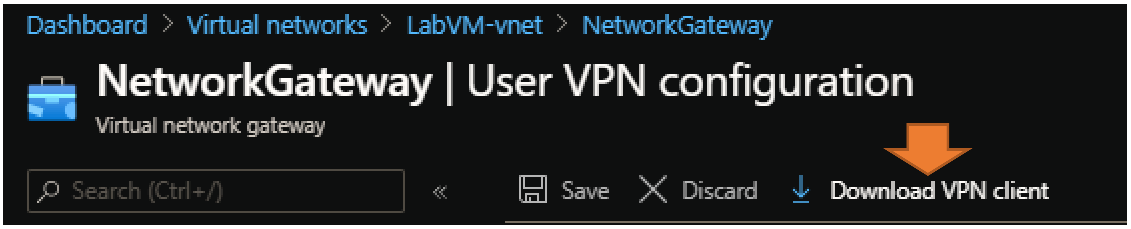


Address pool *
172.16.0.0/24

Root certificates

Name	Public certificate data
AzureP2SRootCert	MIIC5zCCAc+gAwIBAgIQGEBCVDF7WIBCPCwC4SkdUTANBgkqhkiG9w0BAQsFADAW MRQwEgYDVQQDDAtQMINSb290Q2VydDAeFw0yMDA5MTcyMTQ2MTB

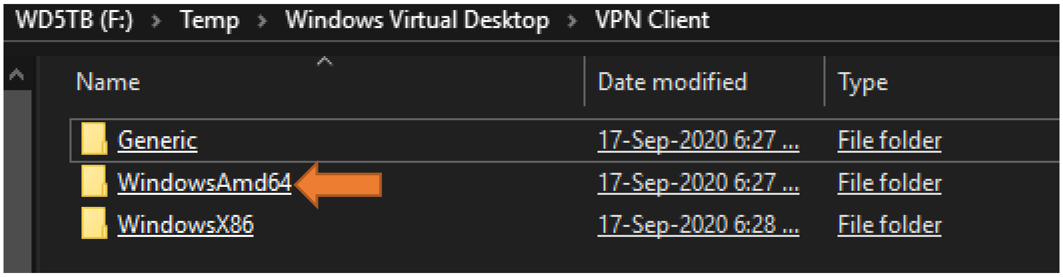
Download VPN Client



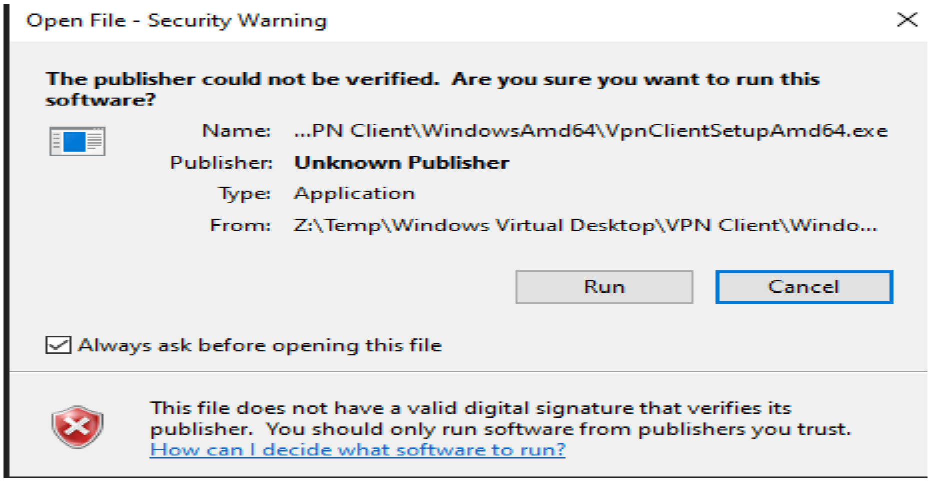
NetworkGateway | User VPN configuration

Virtual network gateway

After download – extract and install vpn client x64 on workstation



Name	Date modified	Type
Generic	17-Sep-2020 6:27 ...	File folder
WindowsAmd64	17-Sep-2020 6:27 ...	File folder
WindowsX86	17-Sep-2020 6:28 ...	File folder

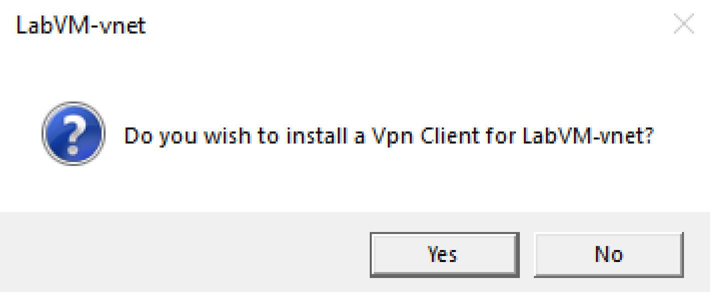

Open File - Security Warning

The publisher could not be verified. Are you sure you want to run this software?

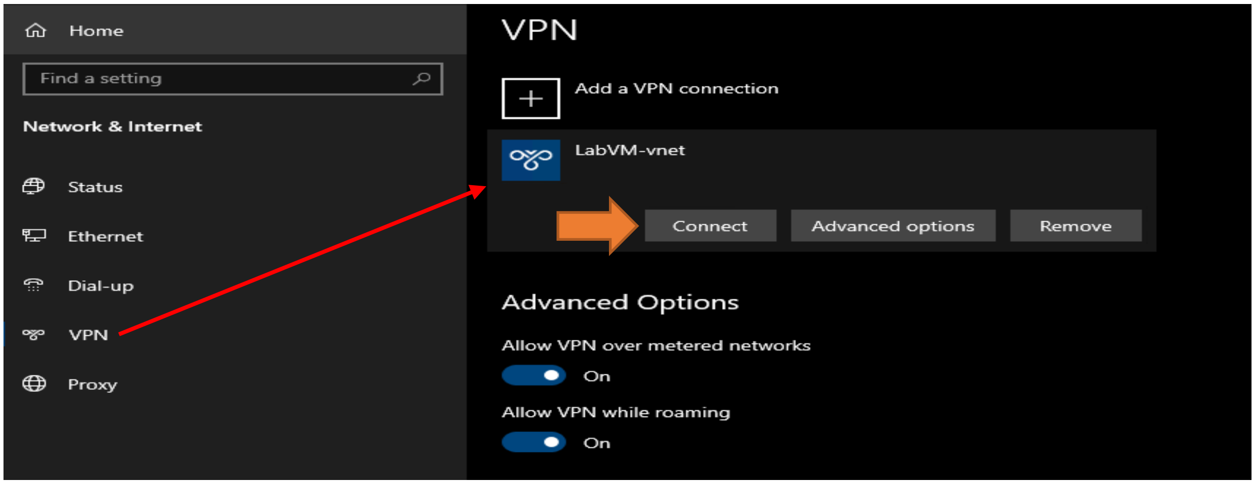
Name: ...PN Client\WindowsAmd64\VpnClientSetupAmd64.exe
Publisher: **Unknown Publisher**
Type: Application
From: Z:\Temp\Windows Virtual Desktop\VPN Client\Windo...

☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.
How can I decide what software to run?

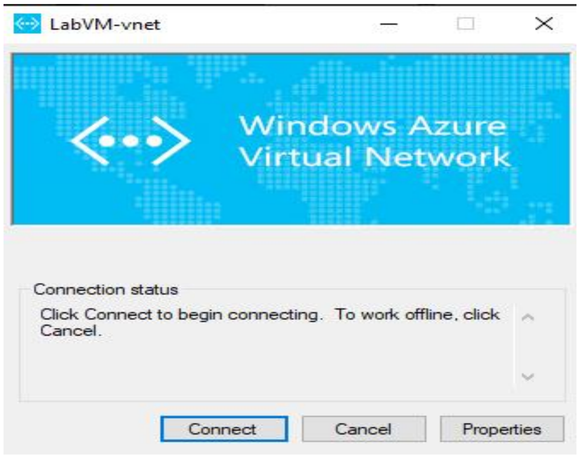

LabVM-vnet

Do you wish to install a Vpn Client for LabVM-vnet?



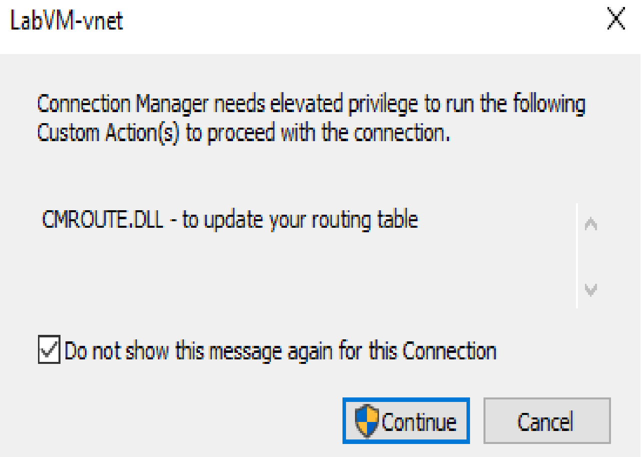
Allow VPN over metered networks: On

Allow VPN while roaming: On



Connection status

Click Connect to begin connecting. To work offline, click Cancel.

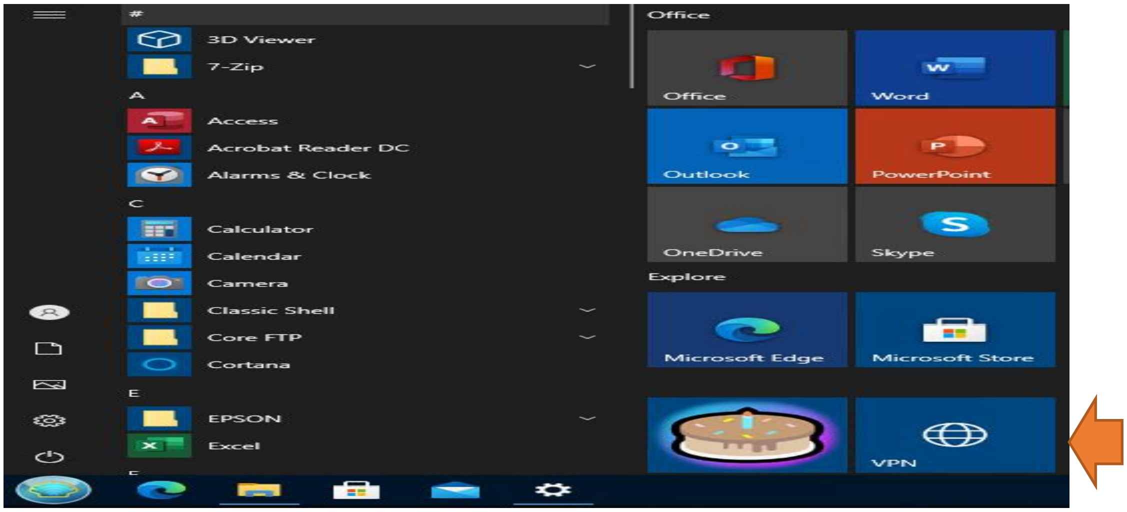


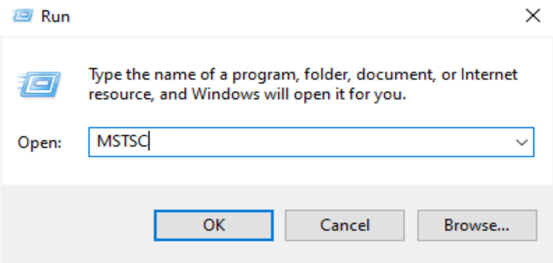
Connection Manager needs elevated privilege to run the following Custom Action(s) to proceed with the connection.

CMROUTE.DLL - to update your routing table

☑ Do not show this message again for this Connection

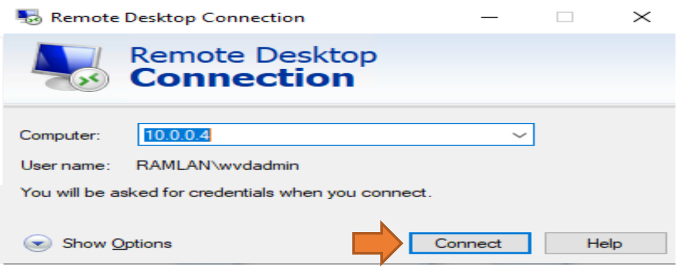
Add VPN connection to Start button





Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

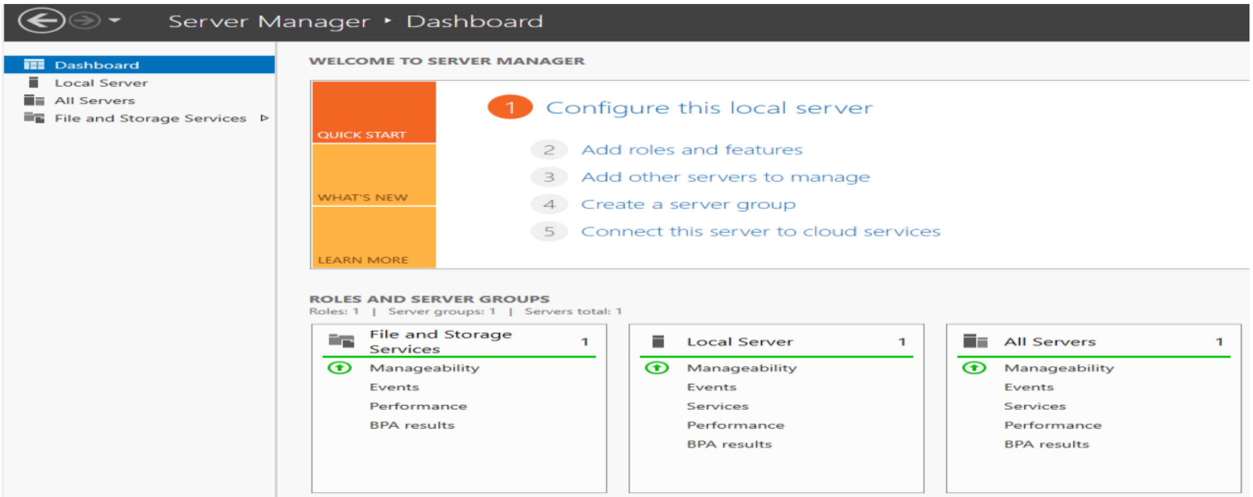
Open: MSTSC

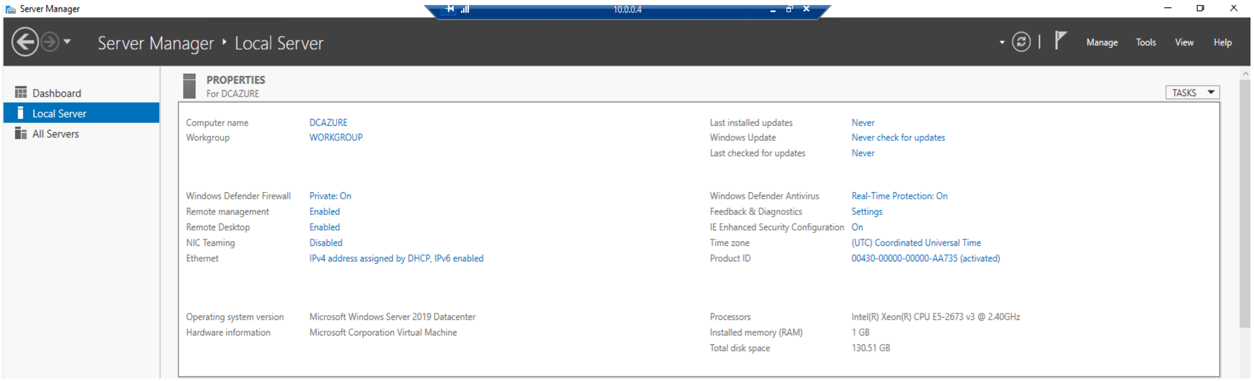


Computer: 10.0.0.4

User name: RAMLAN\wvdadmin

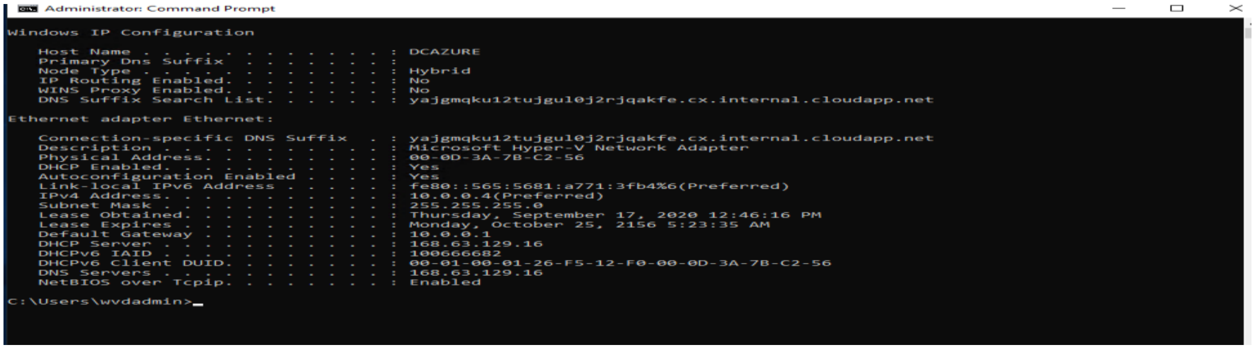
You will be asked for credentials when you connect.



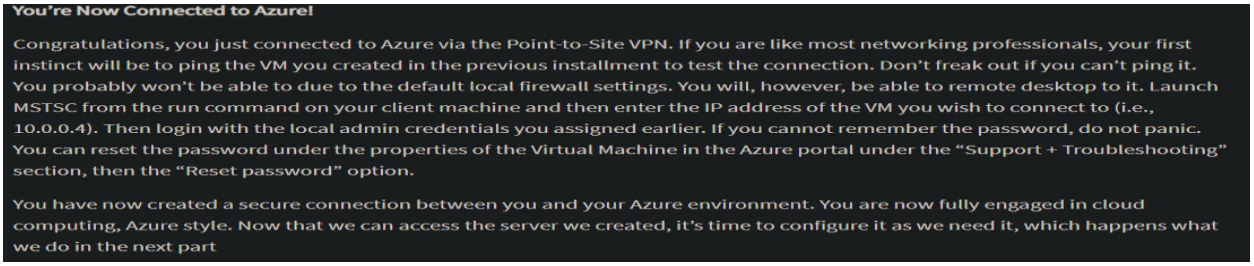


PROPERTIES
For DCAZURE

Computer name	DCAZURE	Last installed updates	Never
Workgroup	WORKGROUP	Windows Update	Never check for updates
		Last checked for updates	Never
Windows Defender Firewall	Private: On	Windows Defender Antivirus	Real-Time Protection: On
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Enabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC) Coordinated Universal Time
Ethernet	IPv4 address assigned by DHCP, IPv6 enabled	Product ID	00430-00000-00000-AA735 (activated)
Operating system version	Microsoft Windows Server 2019 Datacenter	Processors	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz
Hardware information	Microsoft Corporation Virtual Machine	Installed memory (RAM)	1 GB
		Total disk space	130.51 GB



```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : DCAZURE
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : yajgmqku12tujgul0j2rjqakfe.cx.internal.cloudapp.net

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : yajgmqku12tujgul0j2rjqakfe.cx.internal.cloudapp.net
   Description . . . . . . . . . . . : Microsoft Hyper-V Network Adapter
   Physical Address. . . . . . . . . : 00-0D-3A-7B-C2-56
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::565:5681:a771:3fb4%6(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.0.0.4(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, September 17, 2020 12:46:16 PM
   Lease Expires . . . . . . . . . . : Monday, October 25, 2156 5:23:35 AM
   Default Gateway . . . . . . . . . : 10.0.0.1
   DHCP Server . . . . . . . . . . . : 168.63.129.16
   DHCPv6 IAID . . . . . . . . . . . : 100666682
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-F5-12-F0-00-0D-3A-7B-C2-56
   DNS Servers . . . . . . . . . . . : 168.63.129.16
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\wvdadmin>_
```



You're Now Connected to Azure!

Congratulations, you just connected to Azure via the Point-to-Site VPN. If you are like most networking professionals, your first instinct will be to ping the VM you created in the previous installment to test the connection. Don't freak out if you can't ping it. You probably won't be able to due to the default local firewall settings. You will, however, be able to remote desktop to it. Launch MSTSC from the run command on your client machine and then enter the IP address of the VM you wish to connect to (i.e., 10.0.0.4). Then login with the local admin credentials you assigned earlier. If you cannot remember the password, do not panic. You can reset the password under the properties of the Virtual Machine in the Azure portal under the "Support + Troubleshooting" section, then the "Reset password" option.

You have now created a secure connection between you and your Azure environment. You are now fully engaged in cloud computing, Azure style. Now that we can access the server we created, it's time to configure it as we need it, which happens what we do in the next part

This concludes Part 1. In Part 2, I will connect to DCAZURE and install ADDS role and setup Domain Controller. After that we will complete Windows Virtual Desktop Pool and test WVD.

Thanks

Ram Lan
17th Sep 2020