Surviving a Ransomware Attack with Azure Site Recovery

Volume 1

By Microsoft MVP's:

Dave Kawula Cristal Kawula

Emile Cabot Cary Sun

John O'Neill Sr - rMVP

PUBLISHED BY

MVPDays Publishing
http://www.mvpdays.com

ISBN: TBD

Warning and Disclaimer

Every effort has been made to make this manual as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity concerning any loss or damages arising from the information contained in this book.

Feedback Information

We’d like to hear from you! If you have any comments about how we could improve the quality of this book, please don’t hesitate to contact us by visiting www.checkyourlogs.net or sending an email to dave@mvpdays.com.

Foreword by

Acknowledgments

From Dave

Cristal, you are my rock and my source of inspiration. For the past 20 + years you have been there with me every step of the way. Not only are you the "BEST Wife" in the world you are my partner in crime. Christian, Trinity, Keira, Serena, Mickaila, Mackenzie, and Rycker, you kids, are so patient with your dear old dad when he locks himself away in the office for yet another book. Taking the time to watch you grow in life, sports, and become little leaders of this new world is incredible to watch.

Thank you, Mom and Dad, (Frank and Audry) and my brother Joe. You got me started in this crazy IT world when I was so young. Brother, you mentored me along the way both coaching me in hockey and helping me learn what you knew about PCs and Servers. I'll never forget us as teenage kids working the IT Support contract for the local municipal government. Remember dad had to drive us to site because you weren't old enough to drive ourselves yet. A great career starts with the support of your family, and I'm so lucky because I have all the support one could ever want.

Last but not least, the MVPDays volunteers, you have donated your time and expertise and helped us run the event in over 20 cities across North America. Our latest journey has us expanding the conference worldwide as a virtual conference. For those of you that will read this book, your potential is limitless just expand your horizons, and you never know where life will take you.

About the Authors

Dave Kawula – Microsoft MVP

Dave is a Microsoft Most Valuable Professional (MVP) with over 20 years of experience in the IT industry. His background includes data communications networks within multi-server environments, and he has led architecture teams for virtualization, System Center, Exchange, Active Directory, and Internet gateways. Very active within the Microsoft technical and consulting teams, Dave has provided deep-dive technical knowledge and subject matter expertise on various System Center and operating system topics.

Dave is well-known in the community as an evangelist for Microsoft, 1E, and Veeam technologies. Locating Dave is easy as he speaks at several conferences and sessions each year, including TechEd, Ignite, MVP Days Community Roadshow, and VeeamOn.

Recently Dave has been honored to take on the role of Conference Co-Chair of TechMentor with fellow MVP Sami Laiho. The lineup of speakers and attendees that have been to this conference over the past 20 years is fantastic. Come down to Redmond or Orlando in 2018, and you can meet him in person. Checkout his speaking site at www.davekawula.com

He recently tied for 1st place out of 1800 speakers at the Microsoft Ignite Conference in Orlando.

As the founder and Managing Principal Consultant at TriCon Elite Consulting, Dave is a leading technology expert for both local customers and large international enterprises, providing optimal guidance and methodologies to achieve and maintain an efficient infrastructure.

BLOG: www.checkyourlogs.net

Twitter: @DaveKawula

Cristal Kawula – Microsoft MVP

Cristal Kawula is the co-founder of MVPDays Community Roadshow and #MVPHour live Twitter Chat. She was also a member of the Technical Advisory board and is the President of TriCon Elite Consulting. Cristal is also only the 2nd Woman in the world to receive the prestigious Veeam Vanguard award.

Cristal can be found speaking at Microsoft Ignite, MVPDays, and other local user groups. She is extremely active in the community and has recently helped publish a book for other Women MVP's called Voices from the Data Platform.

This year at Microsoft Ignite she lead community meetups for various topics such as Women in IT, Parenting in IT, Diversity in Tech, and becoming a Community Rockstar.

BLOG: http://www.checkyourlogs.net

Twitter: @supercristal1

Emile Cabot – Microsoft MVP

Emile started in the industry during the mid-90s working at an ISP and designing celebrity web sites. He has a strong operational background specializing in Systems Management and collaboration solutions and has spent many years performing infrastructure analyses and solution implementations for organizations ranging from 20 to over 200,000 employees. Coupling his wealth of experience with a small partner network, Emile works very closely with TriCon Elite, 1E, and Veeam to deliver low-cost solutions with minimal infrastructure requirements.

He actively volunteers as a member of the Canadian Ski Patrol, providing over 250 hours each year for first aid services and public education at Castle Mountain Resort and in the community.

BLOG: http://www.checkyourlogs.net

Twitter: @ecabot

Cary Sun – Microsoft MVP

Cary Sun is CISCO CERTIFIED INTERNETWORK EXPERT (CCIE No.4531) and MCSE, MCIPT, Citrix CCA with over twenty years in the planning, design, and implementation of network technologies and Management and system integration. Background includes hands-on experience with multi-platform, all LAN/WAN topologies, network administration, E-mail and Internet systems, security products, PCs and Servers environment. Expertise is analyzing user's needs and coordinating system designs from concept through implementation. Exceptional analysis, organization, communication, and interpersonal skills. Demonstrated ability to work independently or as an integral part of a team to achieve objectives and goals. Specialties: CCIE /CCNA / MCSE / MCITP / MCTS / MCSA / Solution Expert / CCA

Cary's is a very active blogger at checkyourlogs.net and always available online for questions from the community. He passion for technology is contagious, and he makes everyone around him better at what they do.

Blog:http://www.checkyourlogs.net

Twitter:@SifuSun

John O'Neill Sr – Re-Connect Microsoft MVP

Contents

Introduction

MVPDays Online

The purpose of this book is to showcase the fantastic expertise of our guest speakers of MVPDays Online. They have so much passion, expertise, and expert knowledge that it only seemed fitting to write it down in a book.

MVPDays was founded by Cristal and Dave Kawula back in 2013. It started as a simple idea; "There's got to be a good way for Microsoft MVPs to reach the IT community and share their vast knowledge and experience in a fun and engaging way" I mean, what is the point in recognizing these bright and inspiring individuals, and not leveraging them to inspire the community that they are a part of.

We often get asked the question "Who should attend MVPDays"?

Anyone that has an interest in technology is eager to learn and wants to meet other like-minded individuals. This Roadshow is not just for Microsoft MVP's it is for anyone in the IT Community.

Make sure you check out the MVPDays website at www.mvpdays.com. You never know maybe the roadshow will be coming to a city near you.

The goal of this particular book is to show you how to survive a Ransomware Attack using Azure Site Recovery. Each chapter is broken down into a unique tip, and we hope you find some immense value in what we have written.

Sample Files

All sample files for this book can be downloaded from www.checkyourlogs.net and https://github.com/dkawula/Surviving-a-Ransomware-Attack-Using-Azure-Site-Recovery

Additional Resources

In addition to all the tips and tricks provided in this book, you can find extra resources like articles and video recordings on our blog http://www.checkyourlogs.net

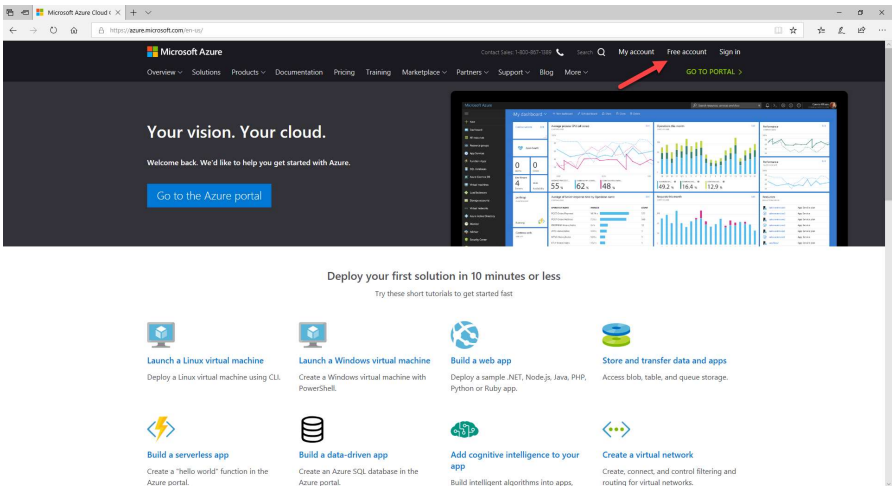
Chapter 1

Setting up your Azure Subscription from Scratch

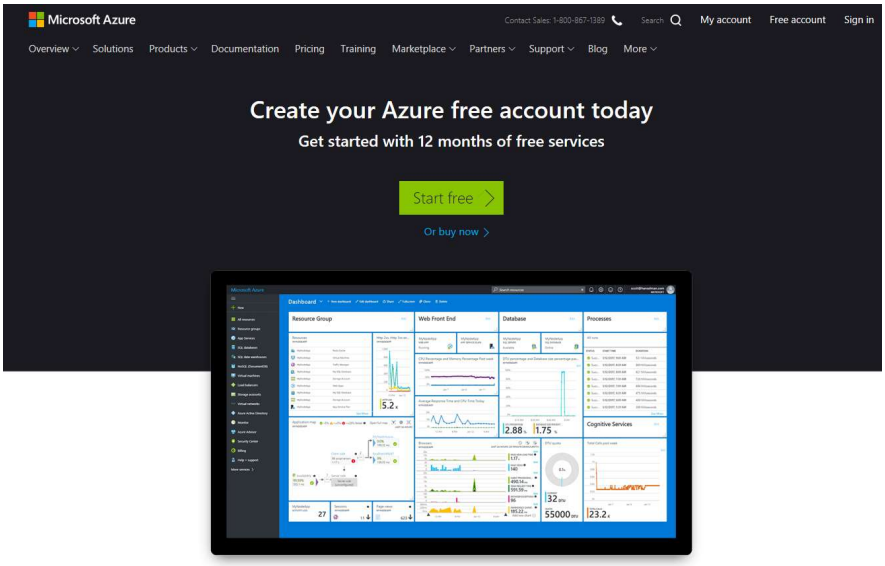
As we know, there are lots of features in Microsoft Azure, to use those features, you need to create a Microsoft Azure account, it's straightforward to create, also you will get $200 credits at the first month.

If you are a newcomer on Microsoft Azure, no worry, I am going to show you how to create Azure free account with $200 credit today, follow the steps as below.

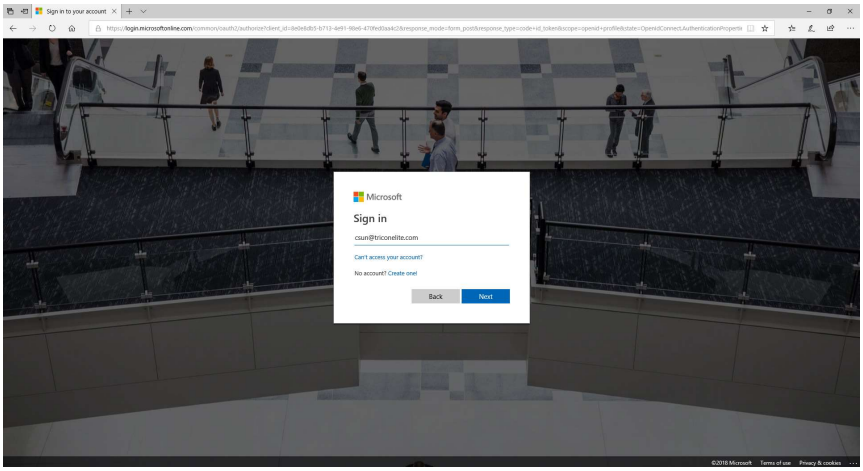
1. Go to https://www.azure.com and then click Free account.



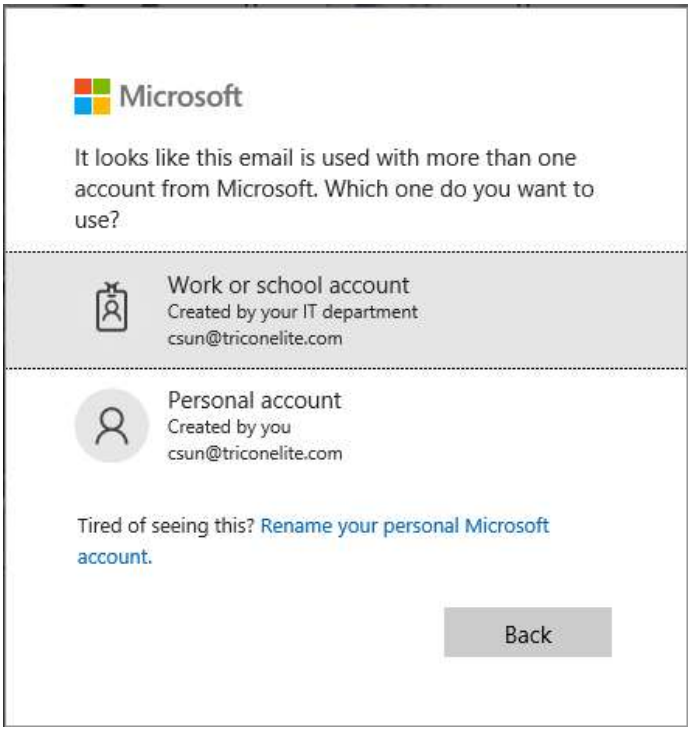
2. On the free account page, click Start free.



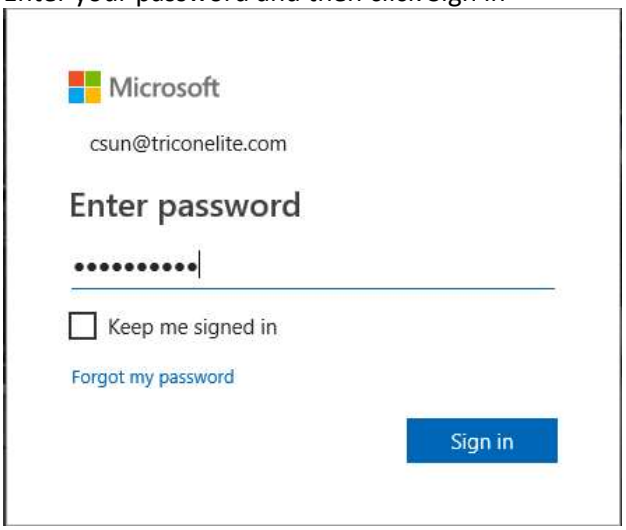
3. If you have an account with Microsoft already (e.g., office 365, outlookf.com ….), enter your email address and then click Next. If you don't have Microsoft account, please click Crete one.



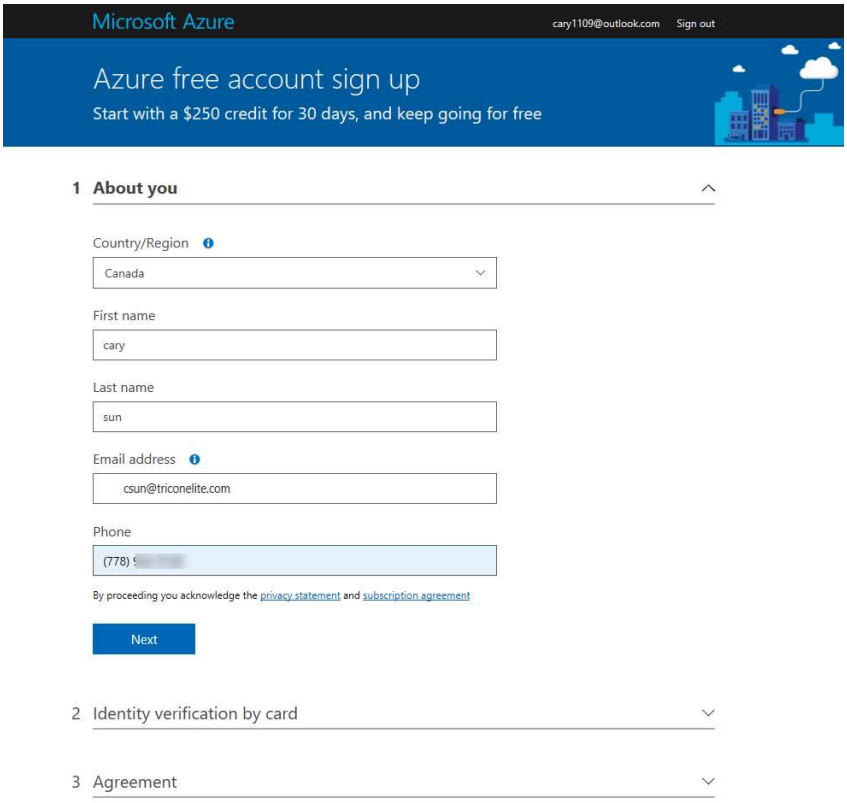
4. If your email address is used with more than on account from Microsoft, you need to select which account do you want to use.



5. Enter your password and then click Sign in

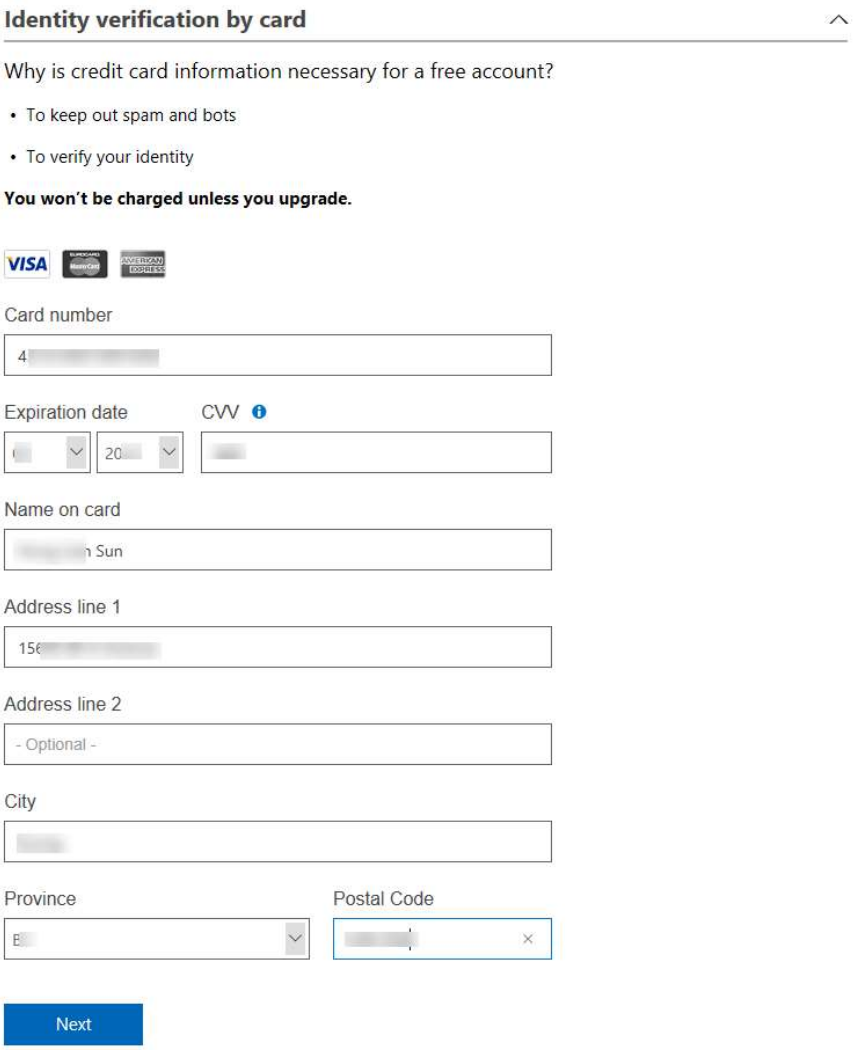


6. On the About you page, enter your personal information and then click Next.



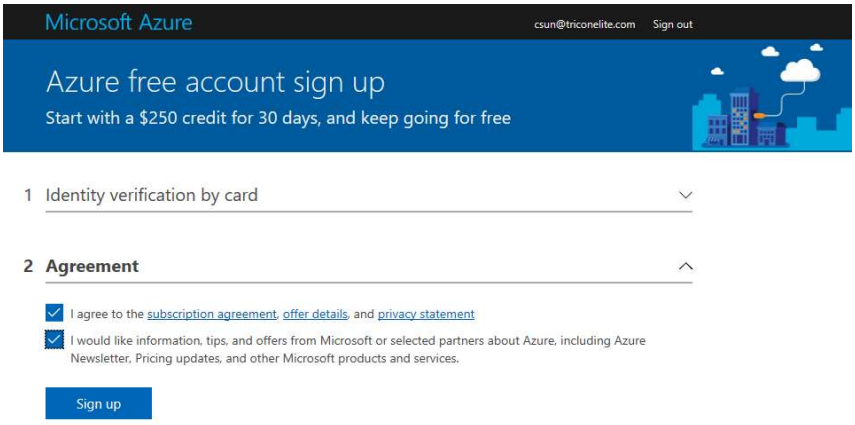
7. On the Identity verification by card page, you need to enter your credit card information and then click Next. Don't worry, Microsoft won't charge you until you upgrade your free

account to pay as you go or others account type.

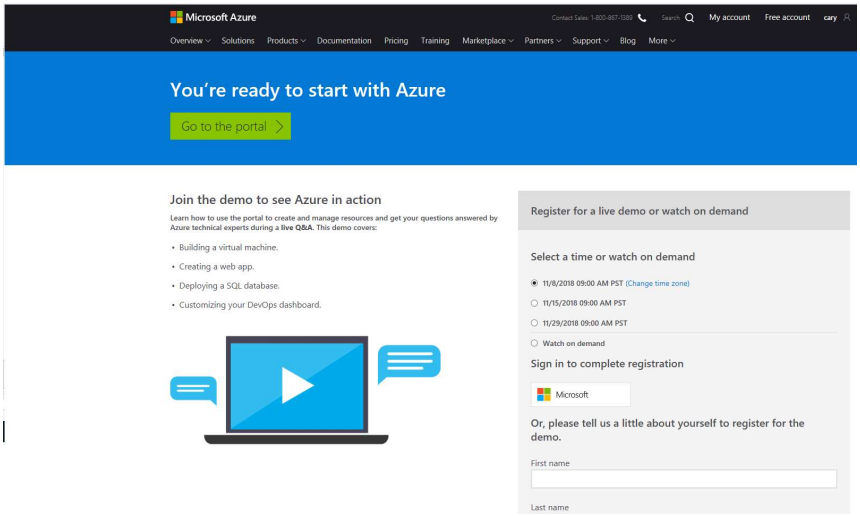


8. On the Agreement page, select I agree to the subscription agreement, offer details, and privacy statement and I would like information, tips, and offers from Microsoft or selected partners about Azure, including Azure Newsletter, Pricing updates, and other

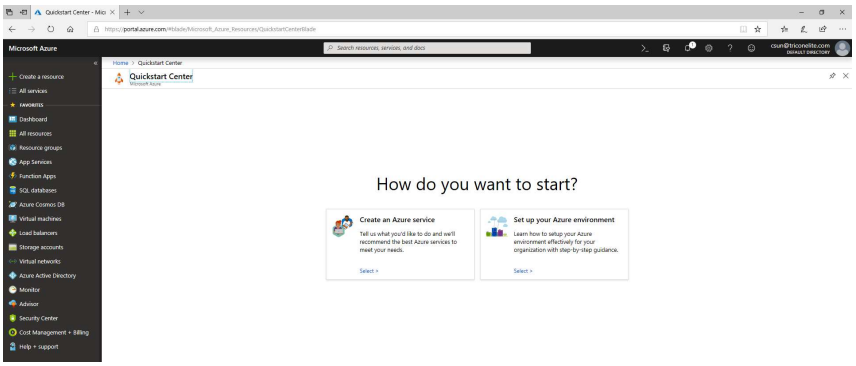
Microsoft products and services, and then click Sign up.



9. Congratulation! You're ready to start with Azure and get $250 create for free. You need to click Go to the portal and enjoy Azure features there.



10. That's it you have now successfully setup your first Azure Tenant and have access to the Azure Portal.


Microsoft Azure
Create a resource
All services
FAVORITES
Dashboard
All resources
Resource groups
App Services
Function Apps
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security Center
Cost Management + Billing
Help + support
Home > Quickstart Center
Quickstart Center
Microsoft Azure
How do you want to start?
Create an Azure service
Tell us what you'd like to do and we'll recommend the best Azure services to meet your needs.
Select >
Set up your Azure environment
Learn how to setup your Azure environment effectively for your organization with step-by-step guidance.
Select >

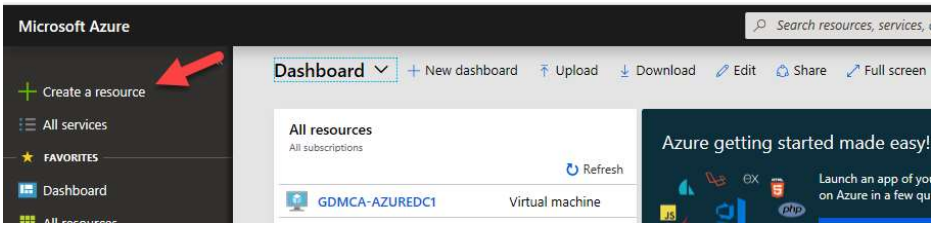
Chapter 2

Building a Hyper-V Nested VM with Multiple Public IP Addresses in Azure

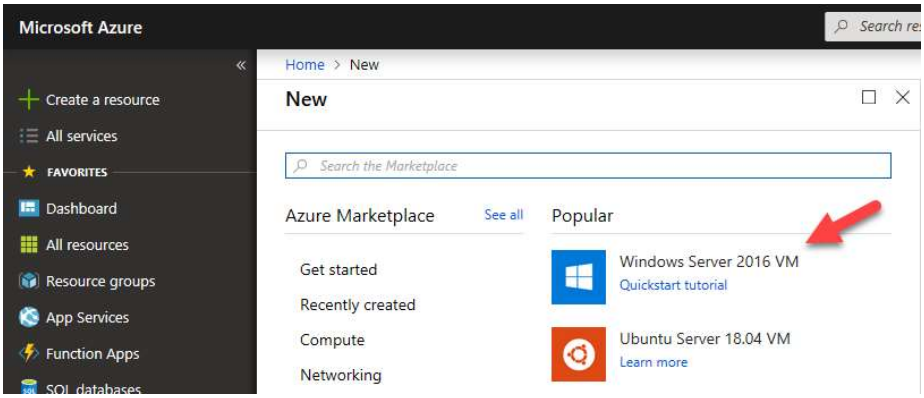
In this chapter, we are going to show you how to build a Hyper-V nested VM with multiple public IP addresses. In this lab configuration, you only need to pay Microsoft for one Hyper-V host (VM) with storage and public IP addresses. After it is configured, you can install a firewall, create VMs, a load balancer, configure customer routing, port forwarding and so on. These scenarios can be used to build up real-world labs for Test, Development, or even proof of concepts.

Building a Windows Server 2016 Virtual Machine

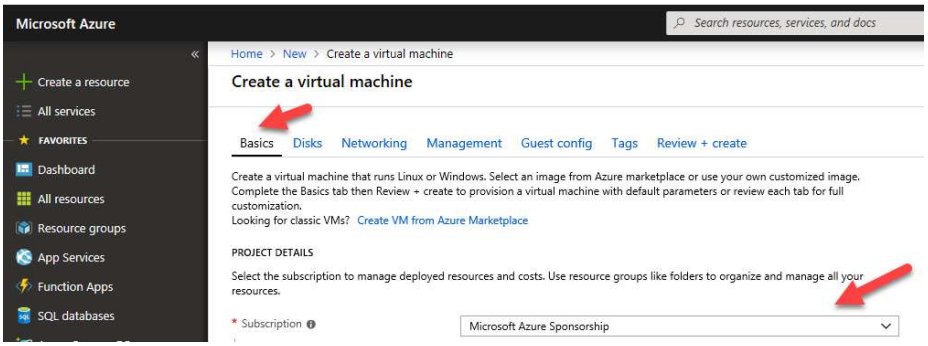
1. Logon to your Microsoft Azure Account and select Create a resource.



2. On the New page, select Windows Server 2016 VM

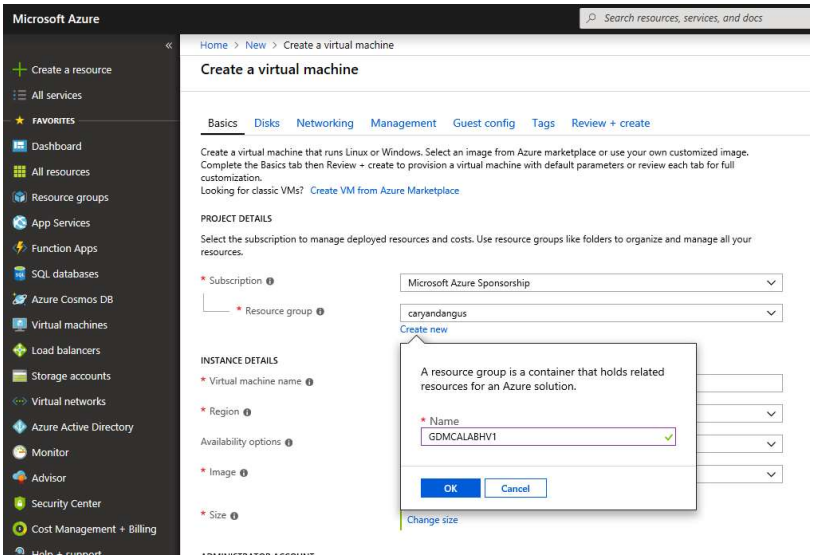


3. On the Create a virtual machine page, click Basics and select your Azure Subscription to pay for this virtual machine.



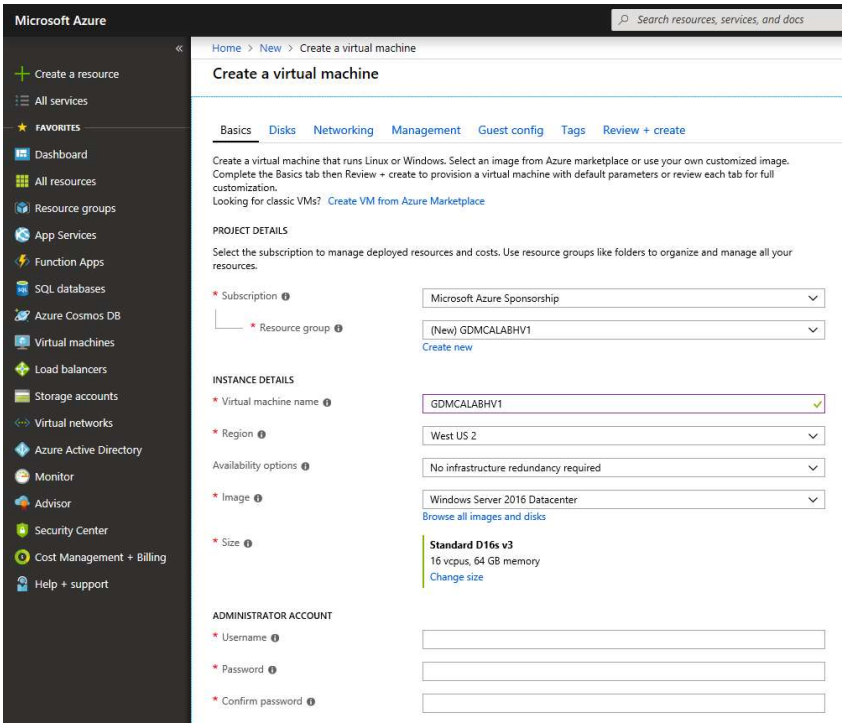
4. Select Create new under the Resource group and enter resource group name, I will recommend it as your virtual machine name, because it will easy to maintain your

resources, and then click OK.

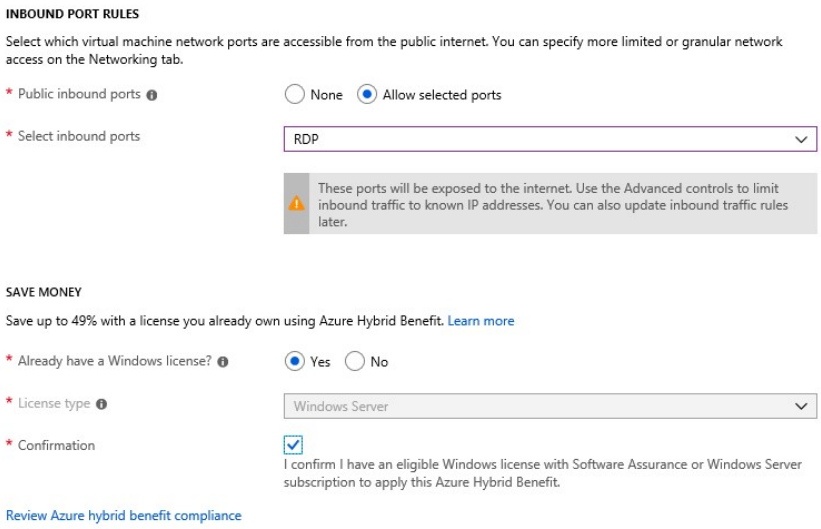


5. **Virtual Machine Name**: Enter Virtual Machine Name as your resource group name.
   Region: Select Region for the virtual machine. For my case, I am using West US 2.
   Availability options: keep the default setting
   Image: select Windows Server 2016 Datacenter
   Size: click change size and select the Dv3 and Ev3 VM sizes. Because we need to enable nested virtualization.
   Username: Enter login user name
   Password: Enter login password

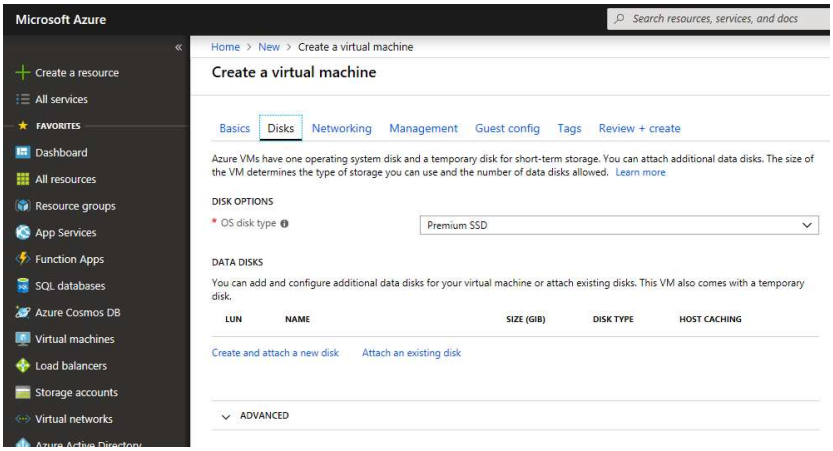
Confirm password: Reenter login password



Public inbound ports: Select Allow selected ports.
Select inbound ports: Select RDP (3389)
Already have a Windows license: Select Yes if you have a license already.
Confirmation: select I confirm I have an eligible Windows license with Software Assurance or Windows Server subscription to apply for this Azure Hybrid Benefit.

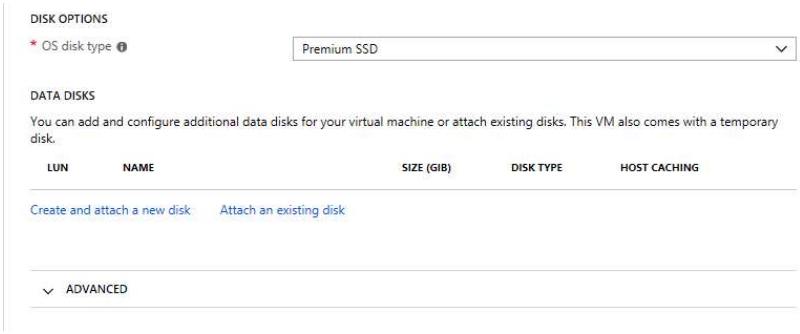


6. On the Create a Virtual Machine page, click Disks.

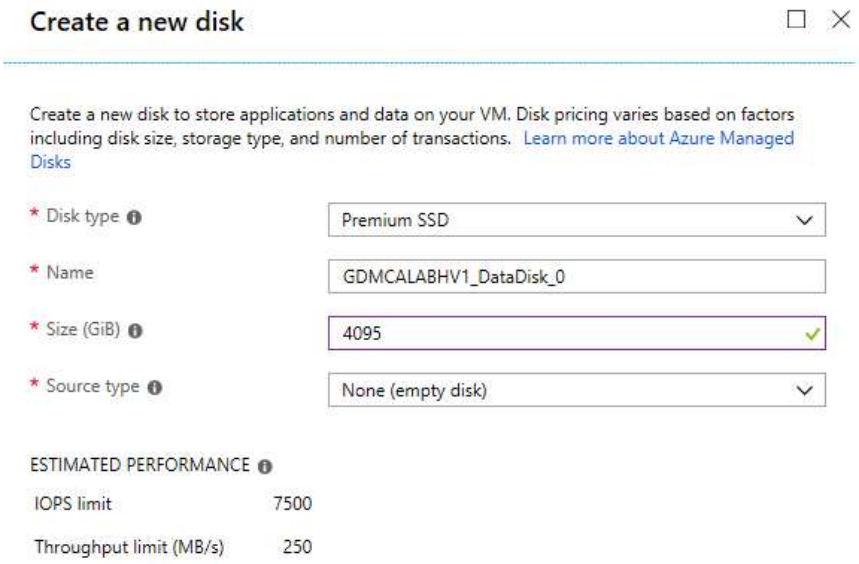


OS disk type: Select Premium SSD

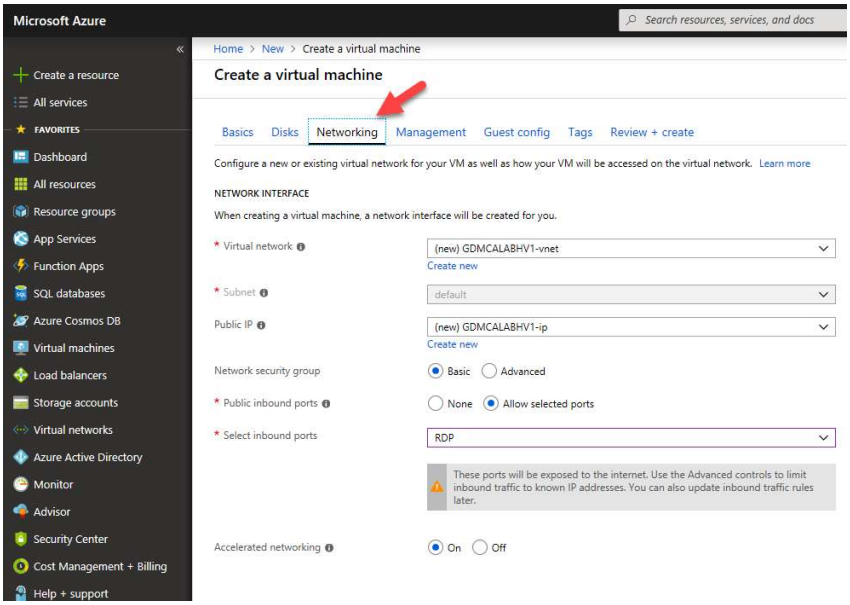
DATA DISKS: Select Create and attach a new disk (this storage space is for your nested VMs)



7. On the Create a new disk page, settings as follow and then click OK.
   Disk type: Select Premium SSD
   Name: keep the default name
   Size(**GiB**): 4095
   Source type: None



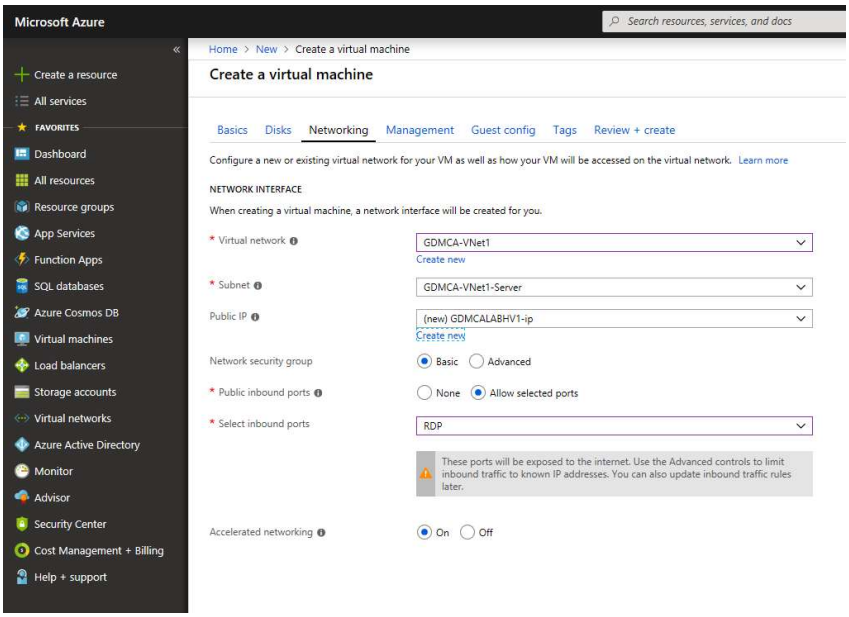
8. On the Create a virtual machine page, click Networking.



Virtual network: Select vnet if you have existing vnet if not, you can keep the default settings.

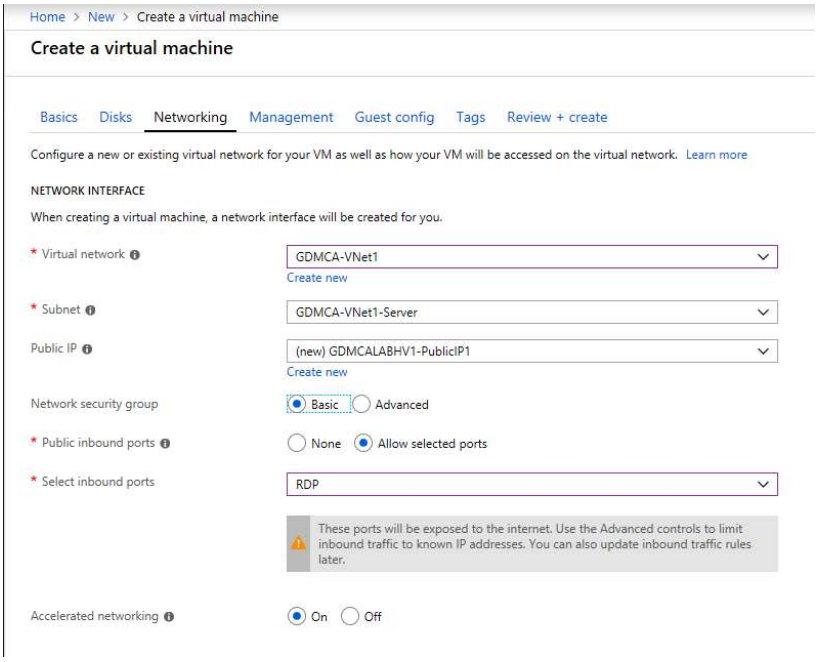
Subnet: Select subnet name if you have an existing subnet; if not, you can keep the default settings.

Public IP: click Create new

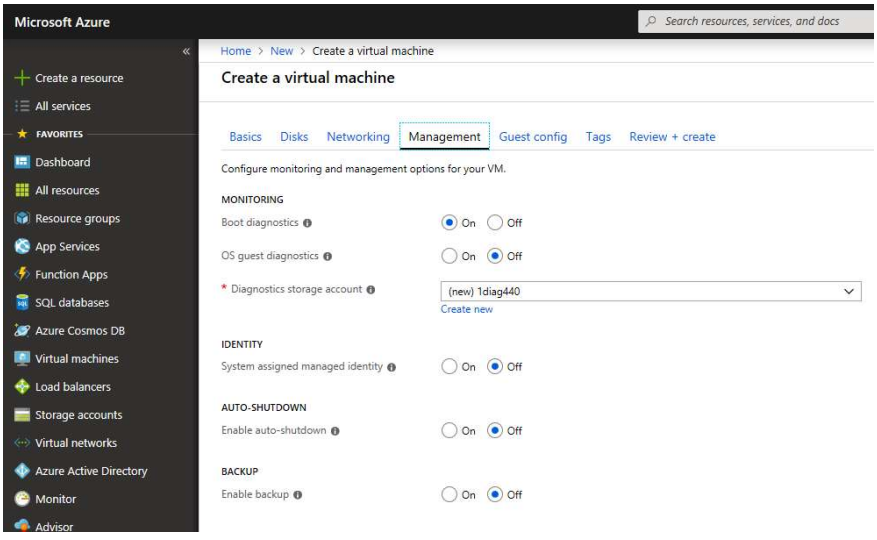


9. On the Create Public IP address page, the settings are as follows
   Name: Enter the Public IP address name.
   SKU: Basic
   Assignment: Static
10. To complete Networking settings as follow:
    Network security group: Basic
    Public inbound ports: Allow selected ports
    Select inbound ports: RDP

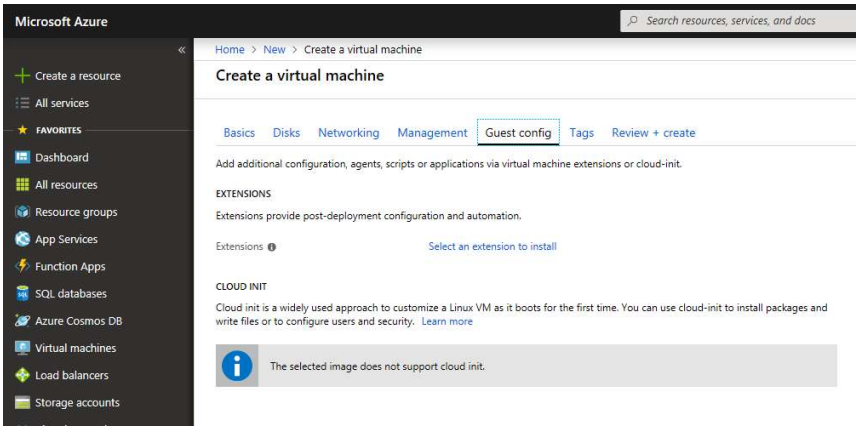
Accelerated networking: On



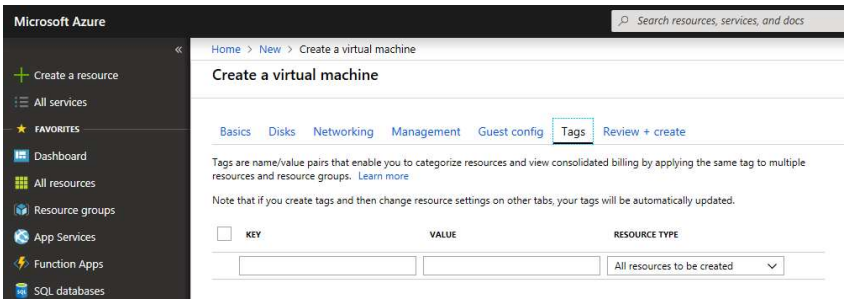
1. On the Create a virtual machine page, click Management and keep the settings as default.



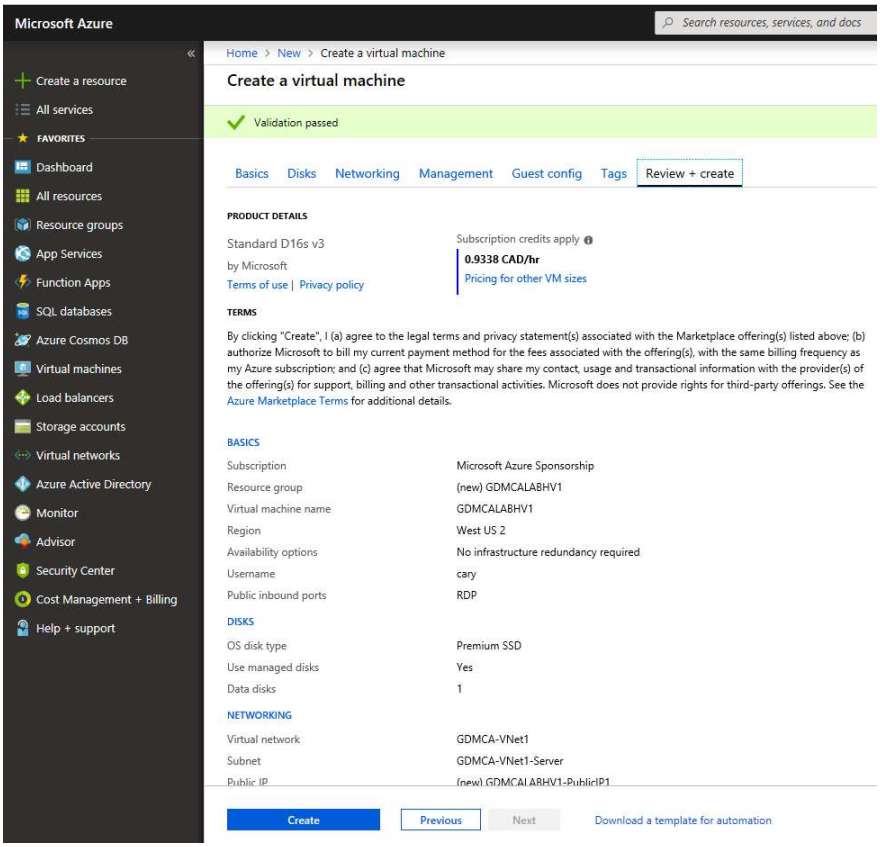
11. On the Create a virtual machine page, click Guest config and keep the settings as default.



12. On the Create a virtual machine page, click Tags and keep the settings as default.

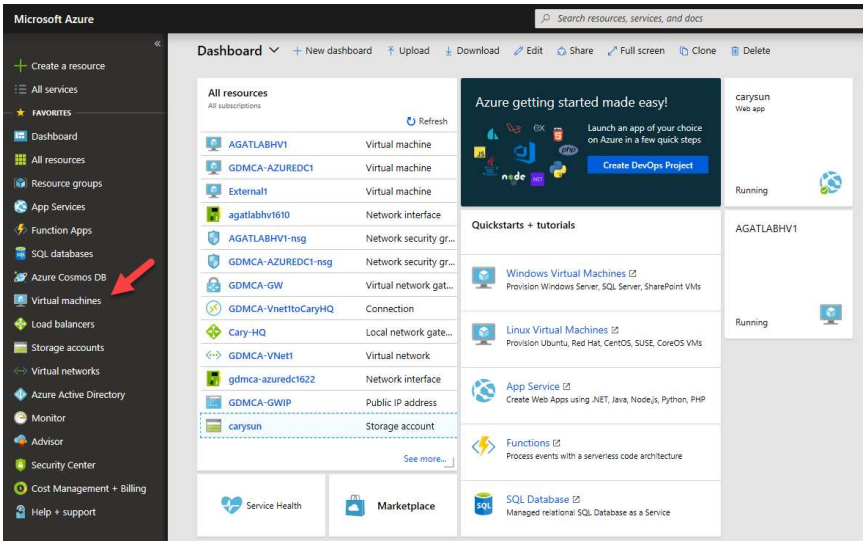


13. On the Create a virtual machine page, click Review + create and make sure Validation passed and then click Create.

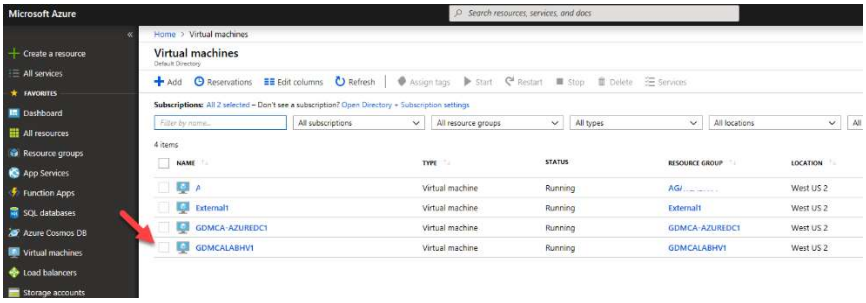


Creating Multiple Internal and External IP's for the Lab

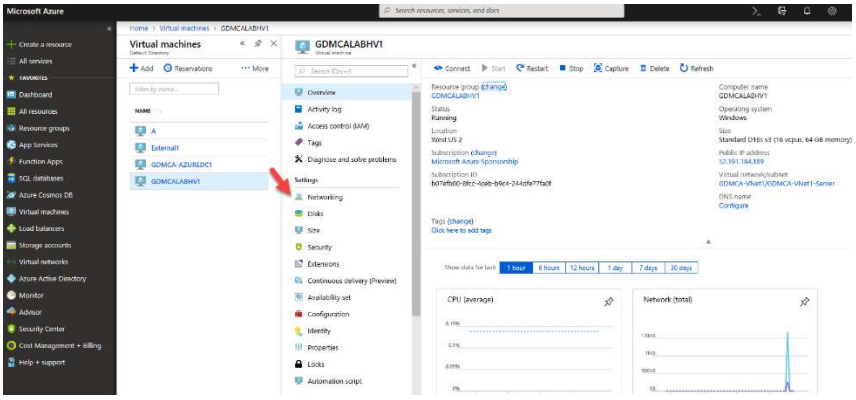
1. On the Microsoft Azure portal page, select Virtual machines.



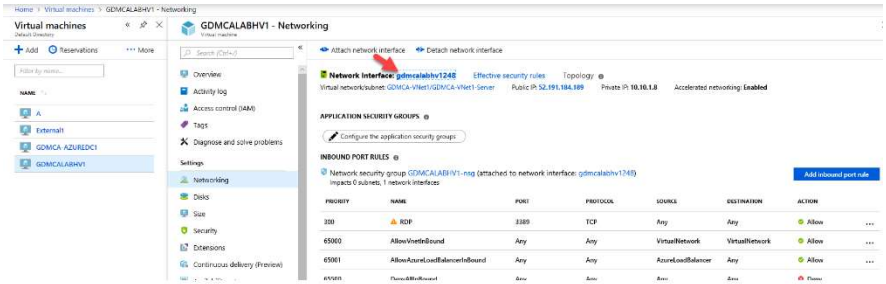
2. On the Virtual machines page, click GDMCALABHV1.



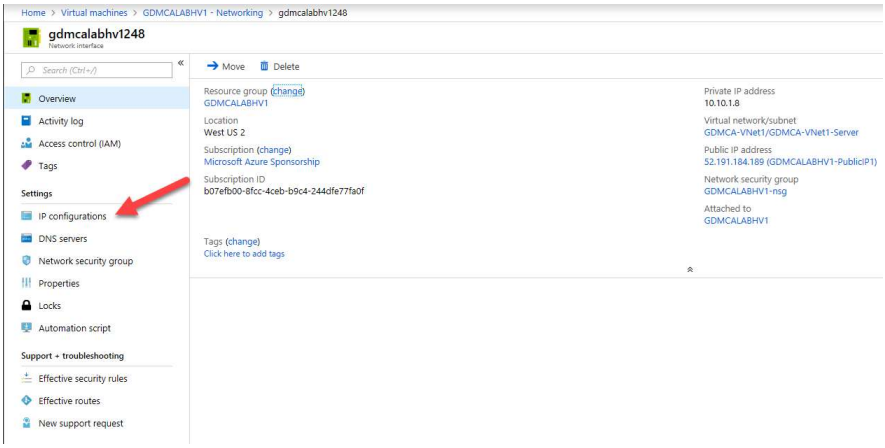
3. On the GDMCALABHV1page, select Networking.



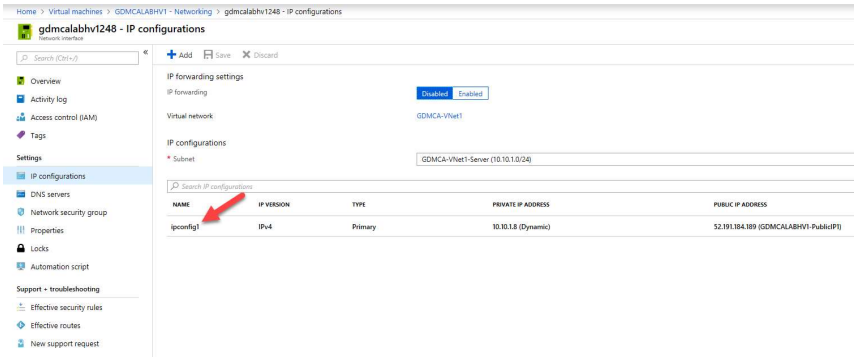
4. On the GDMCALABHV1-Networking page, select Network Interface: gdmcalabhv1238.



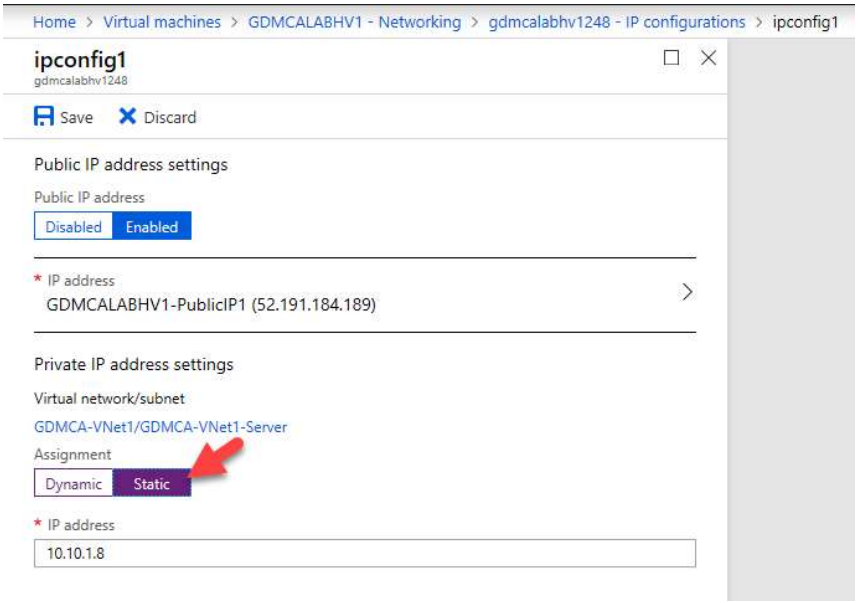
5. On the Network Interface page, select IP configurations.



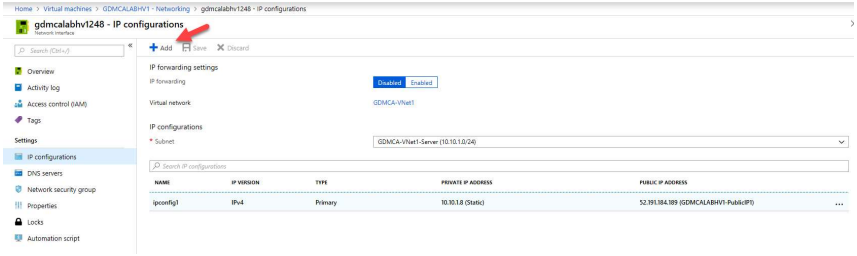
6. On the IP configurations page, select ipconfig1.



7. Change assignment setting from Dynamic to Static, and then click Save.



8. Go back to the IP configurations page, click Add.



9. On the Add IP configuration page, settings as follow and then click OK.

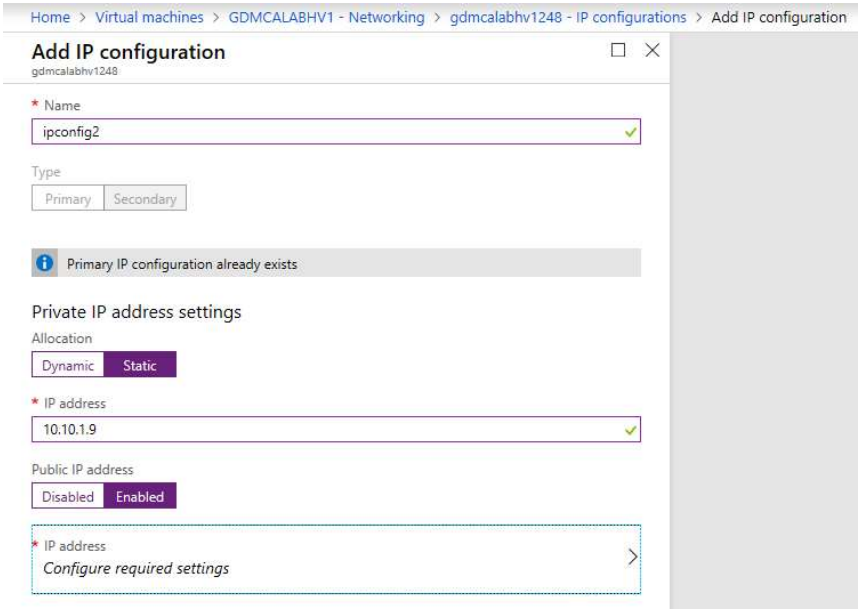
Name: ipconfig2

Private IP address Allocation: Static

IP address: 10.10.1.9

Public IP address: Enable

IP address: click configure required settings

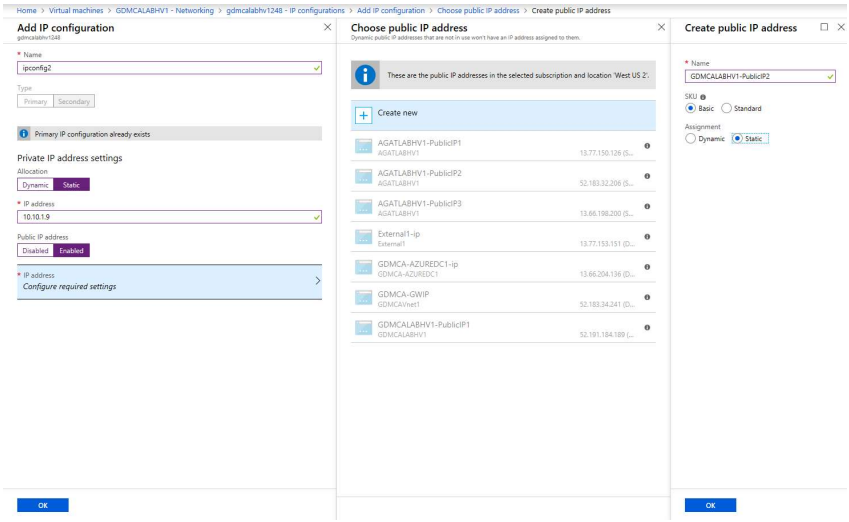


10. Choose public IP address: Create new

    Name: Enter name for Public IP

    SKU: Basic

Assignment: Static and then click OK

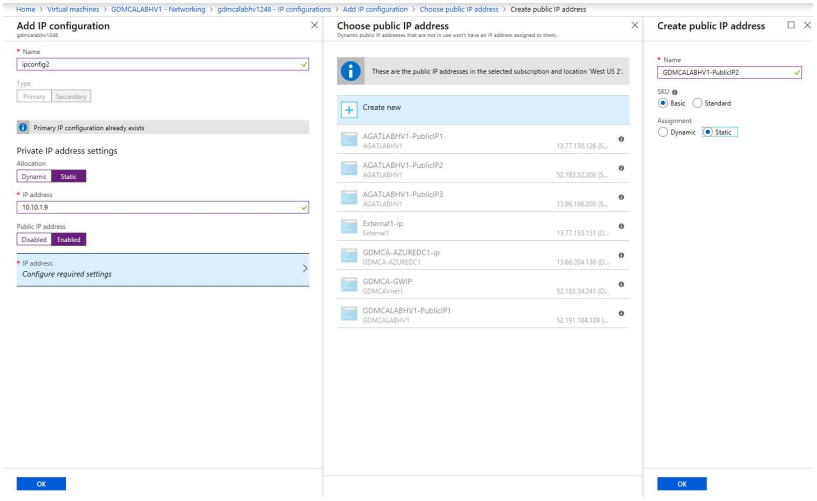


Choose public IP address: Create new

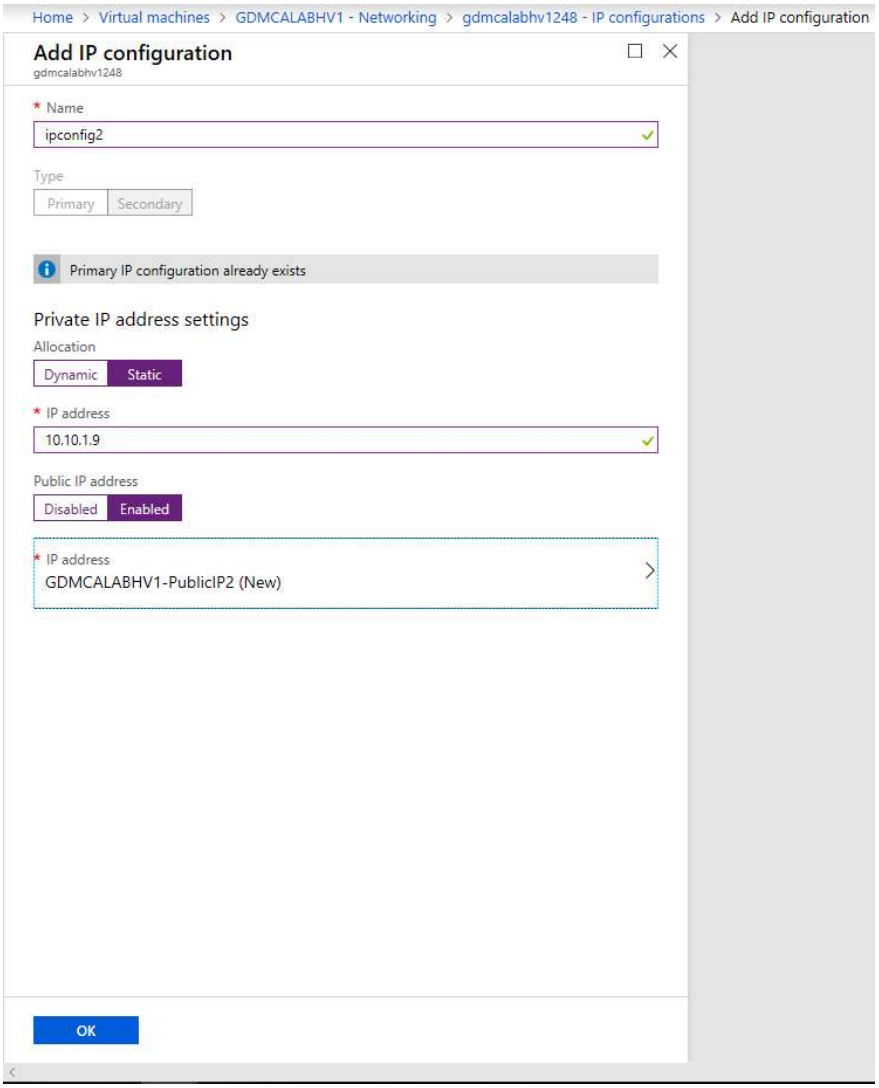
Name: Enter name for Public IP

SKU: Basic

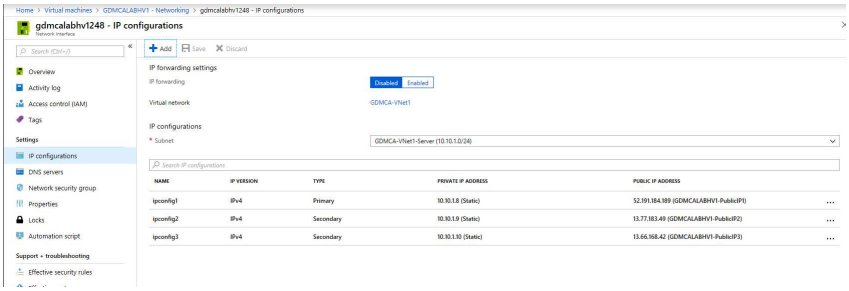
Assignment: Static and then click OK



11. On the Add IP configuration page, click OK.

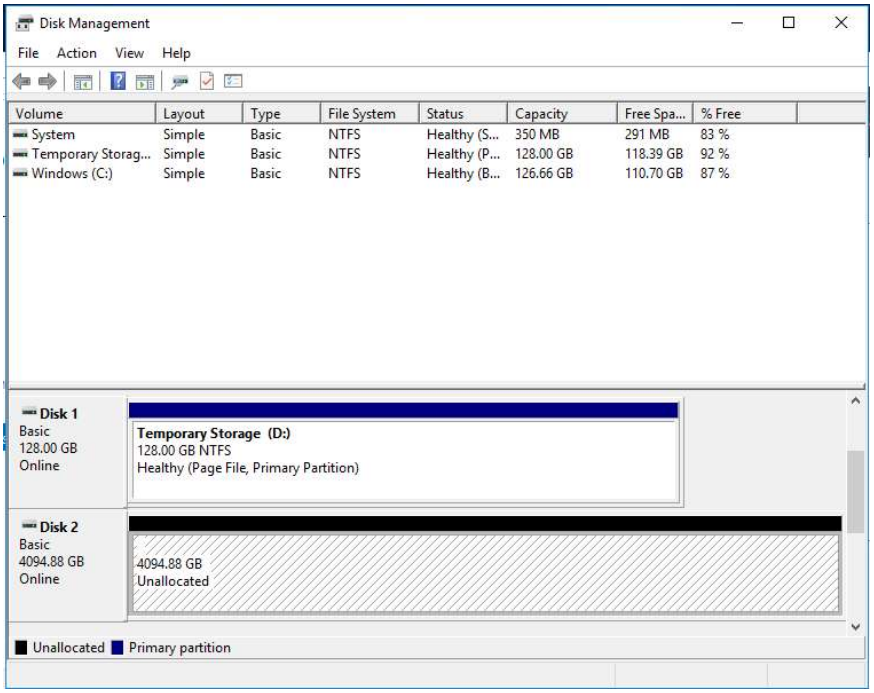


12. Repeat Add IP configurations steps If you need more public IP addresses.

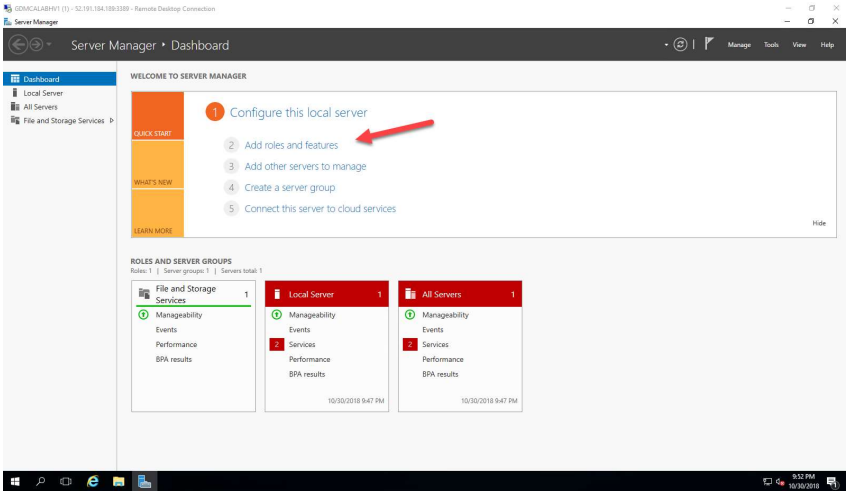


Enable Hyper-V in the LAB Virtual Machine

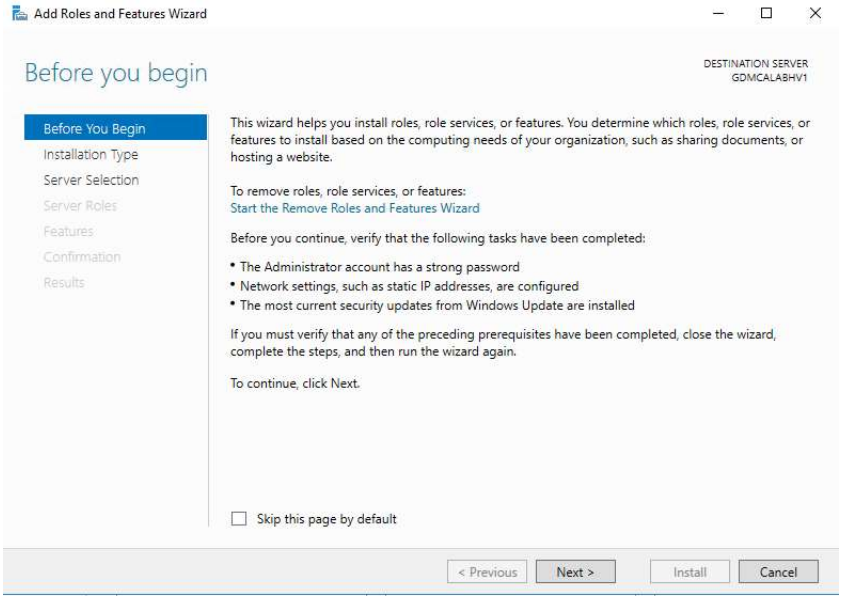
1. Start Azure virtual machine and log in.
2. Open Disk Management to partition and format for your new 4TB storage space. (Use ReFS + 64 KB Block Size.)



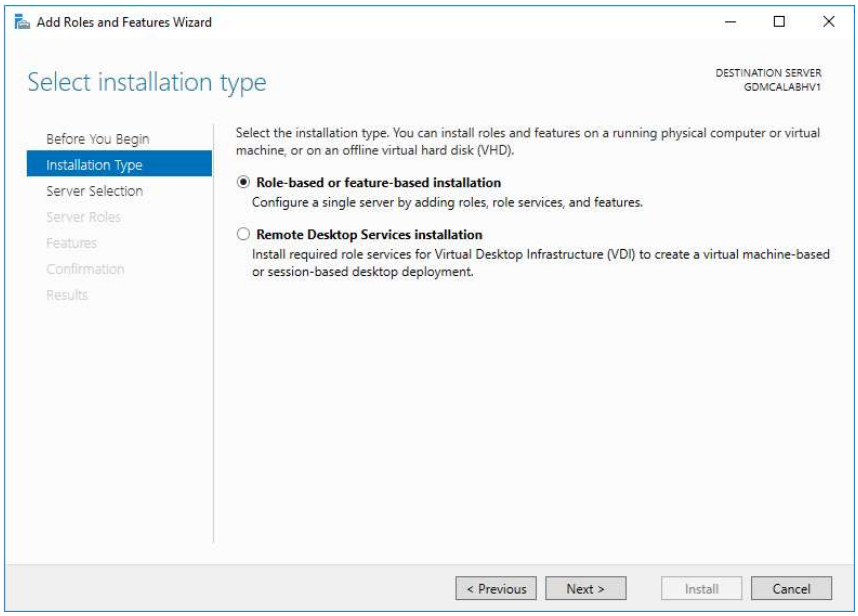
3. On the Server Manager Dashboard, click Add roles and feature.



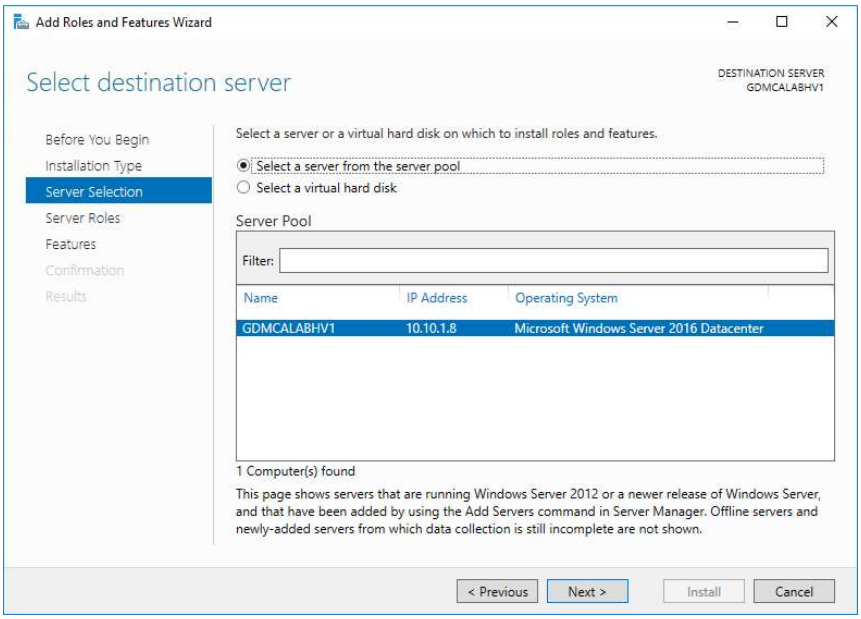
4. On the Before you begin page, click Next.



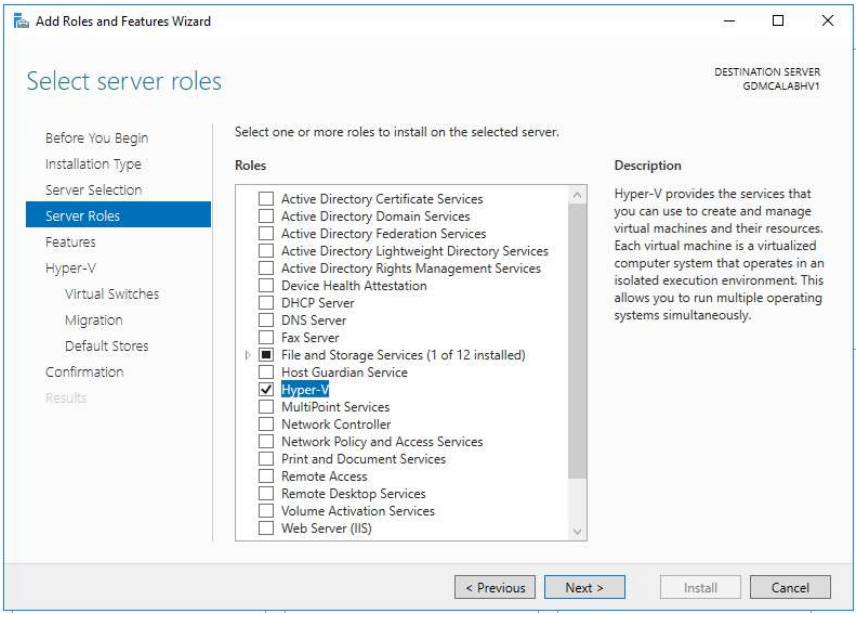
5. On the Select installation type, select Role-based or feature-based installation and then click Next.



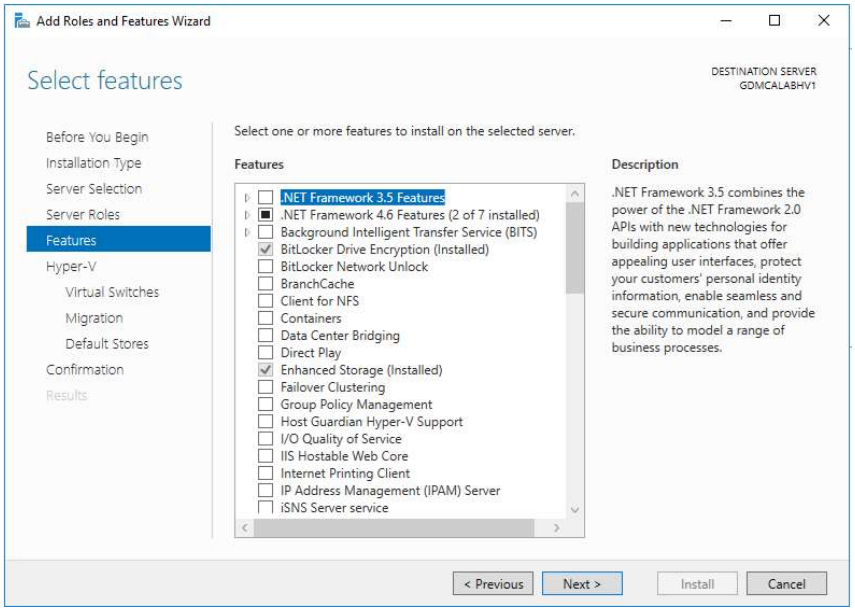
6. On the Select destination server page, click Next.



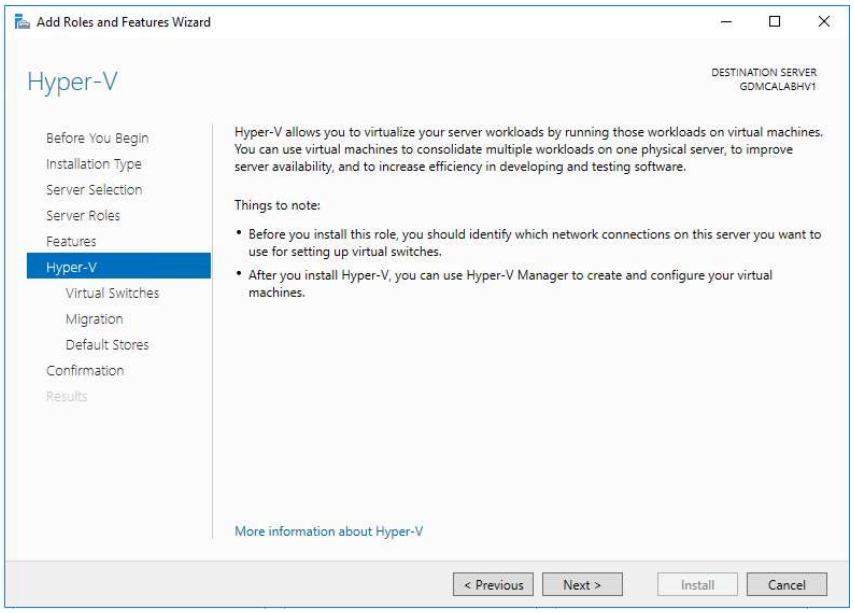
7. On the Select server roles page, select Hyper-V, click Add Features and then click Next.



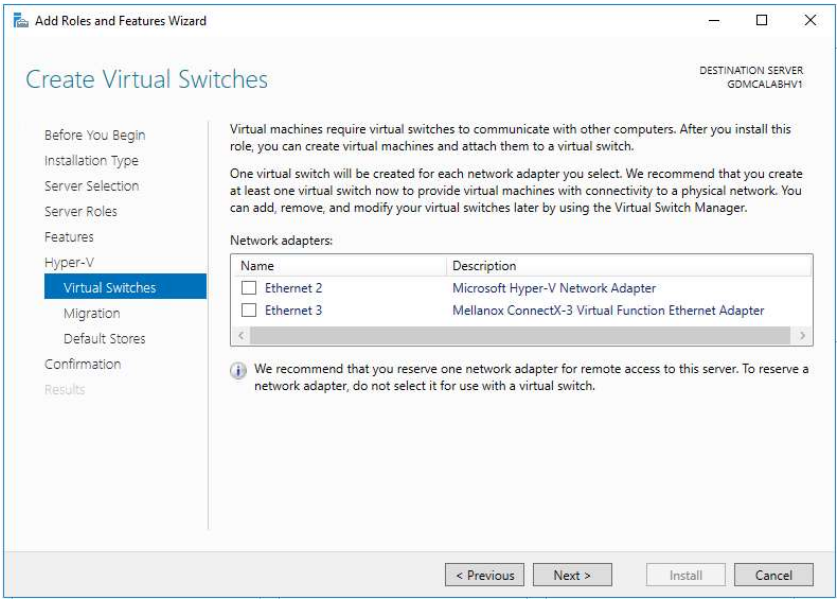
8. On the Select features page, click Next.



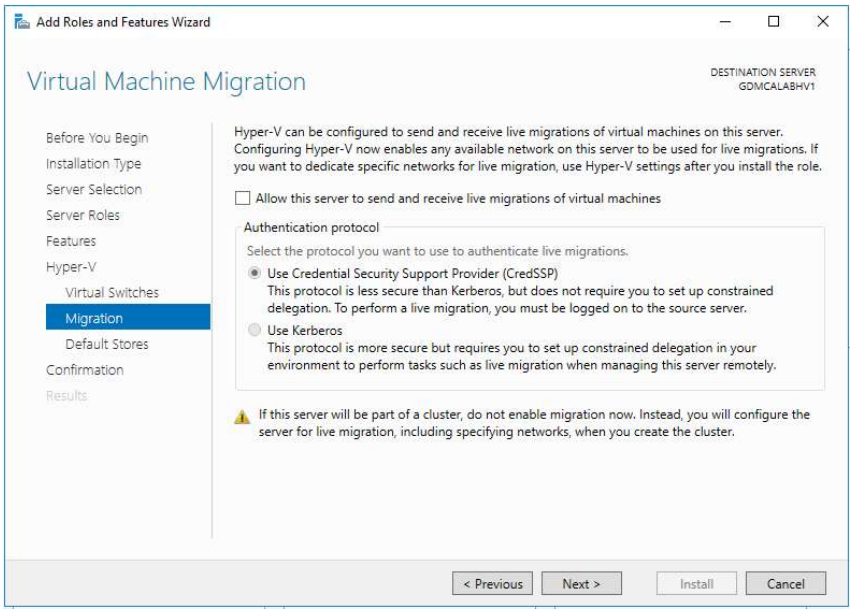
9. On the Hyper-V page, click Next.



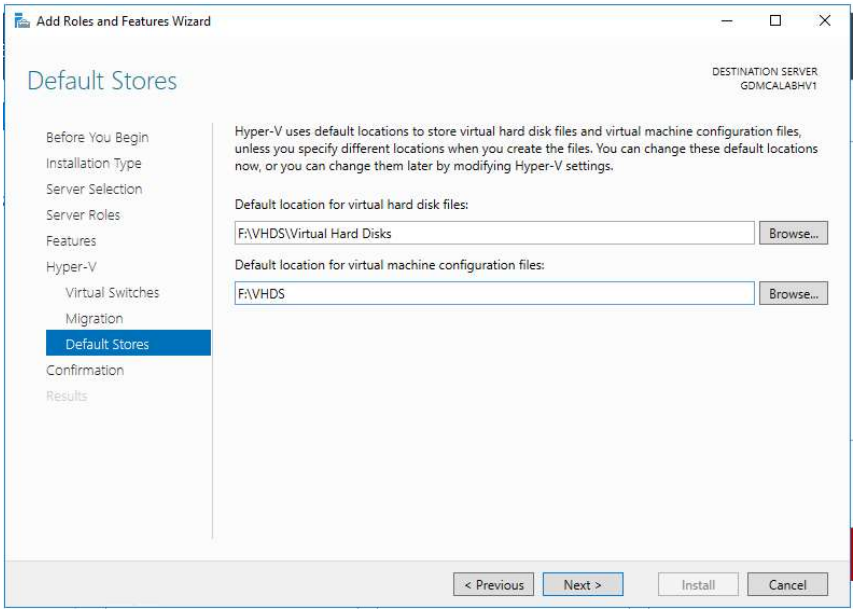
10. On the Create Virtual Switches page, don't select any interface and click Next.



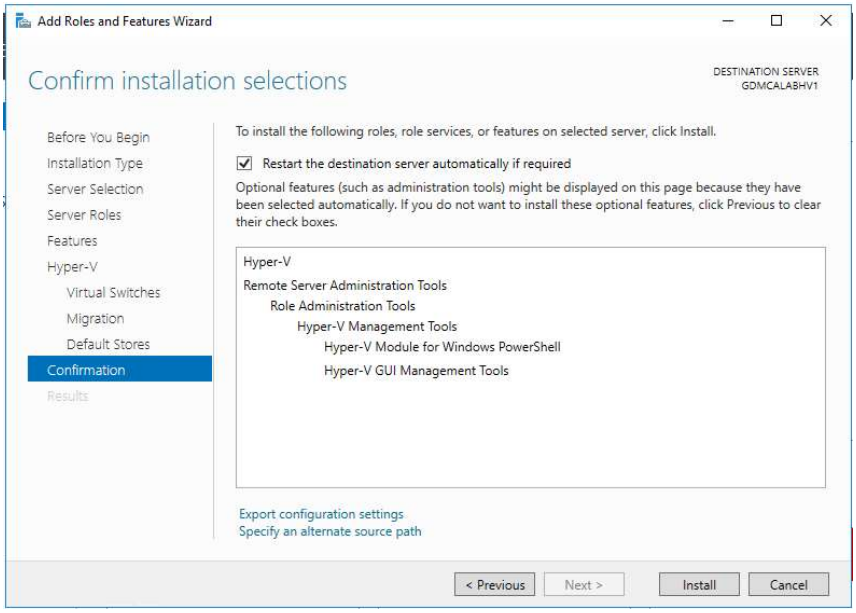
11. One the Virtual Migration page, click Next.



12. On the Default Stores page, you can change the default location to your new 4TB storage space and then click Next.

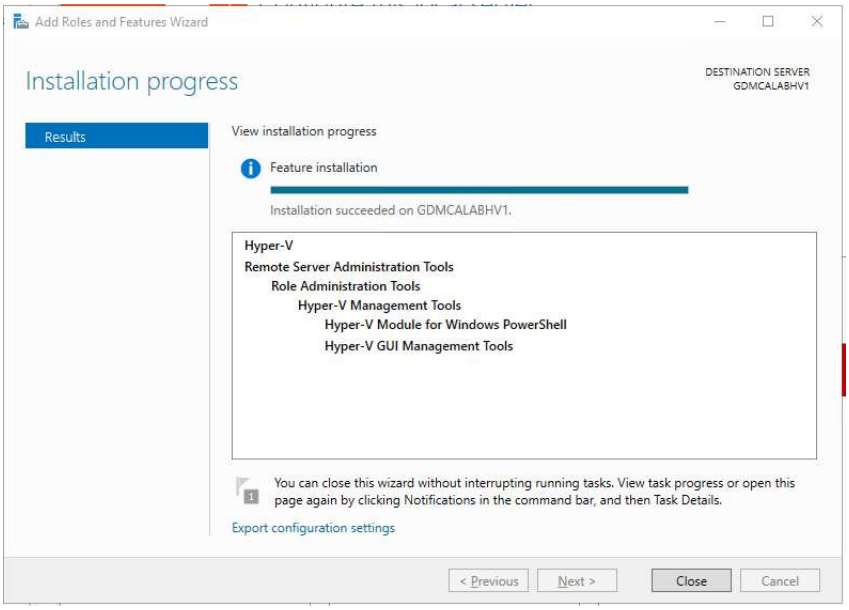


13. On the Confirm installation selections page, select Restart the destination server automatically if required and then click install.



14. Login to Azure Virtual machine after it restarted.

15. On the installation progress page, click Close.



Configuring NAT Networking with one Public IP Address

To configure NAT Networking, we need to create an Internal Virtual Switch for nested guest VMs. In general, there are two options for networking with nested virtual machines, MAC Address Spoofing, and NAT networking. Unfortunately, MAC Address Spoofing is not possible in a public cloud environment. So, If you are using an Azure virtual machine network interface as your Hyper-V external virtual switch and have assigned it to nested guest VMS, the guest VMs won't be able to access the Internet. At this point, we have no choice, but to use NAT networking.

The steps below show how to configure a NetNat Virtual Switch with a single Public IP Address.

1. We can create an internal virtual switch and create NAT rules via Powershell cmdlet as follow:

```
NNew-VMSwitch -Name "NATNetwork" -SwitchType Internal
Get-NetAdapter
New-NetIPAddress -IPAddress 192.168.100.1 -PrefixLength 24 -
InterfaceIndex 14
New-NetNat -Name "NATNetwork" -InternalIPInterfaceAddressPrefix
192.168.100.0/24
```