

MiVoice MX-ONE
MX-ONE Azure Installation
Document
Release 7.4
November 15, 2021



Notice

The information contained in this document is believed to be accurate in all respects but is not warranted by **Mitel Networks™ Corporation (MITEL®)**. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: <http://www.mitel.com/trademarks>.

®, ™ Trademark of Mitel Networks Corporation
© Copyright 2021, Mitel Networks Corporation
All rights reserved

Contents

Chapter: 1	Introduction	1
Chapter: 2	Prerequisites	2
	MX-ONE Prerequisites	2
	MX-ONE Image for Azure	2
	Azure Prerequisites	2
Chapter: 3	Network Topology	4
Chapter: 4	Azure Environment Preparation	5
	Resource Groups	5
	Upload the Image to Azure from your Local Computer or Network Path	5
	Example of Uploading an MX-ONE VHD Image to Azure	6
	Create an Image Snapshot	7
	Create a Disk	8
Chapter: 5	Create the MX-ONE VM and Additional Setup	10
	Create the MX-ONE VM using the Disk	10
	Setup Static IP Addresses to be Used in MX-ONE VM	13
	Allow ICMP, SSH and HTTPS access to Service Node IP address	16
	Test the Connectivity	19
Chapter: 6	Deploy MX-ONE by Accessing VM via Serial Console	21
Chapter: 7	Deployment of MX-ONE in Azure HCI Stack Setup	23
	Introduction	23
	Prerequisites	23
	Installation Procedure	23
Chapter: 8	Good to know / limitations	31

Chapter: 9	Acronyms, Abbreviations and Glossary	32
Chapter: 10	References	34

Introduction

This installation document describes how you can deploy MX-ONE in the Microsoft Azure environment.

Prerequisites

In this document, not all the steps/instructions are described, so it is assumed:

- The Azure environment and Azure accounts setup is available.
- Engineer/technician has good knowledge of cloud technologies, specially, Microsoft Azure.
- The MX-ONE deployment in Azure is approved by the customer IT or equivalent department.
- The connectivity between Azure and the customer premises is active and it supports real time applications, for example, the connectivity must to have a low latency.

MX-ONE Prerequisites

- MX-ONE is properly dimensioned according to MX-ONE documentation.
- The MX-ONE licenses are active.
- An MX-ONE image for Azure is available.
- The TCP/UDP/SCTP ports required by MX-ONE are properly configured in the enterprise customer firewall. For additional information, refer *MiVoice MX-ONE System Planning - Description, chapter IP Protocols and Ports*.
- NTP and DNS are configured.
- It is highly recommended that HTTPS and SIP/TLS protocols are used in the Azure setup.

MX-ONE Image for Azure

- For MiVoice MX-ONE to be deployed in Azure, an MX-ONE VHD image is required.
- Azure requires fixed size images, so, the current MX-ONE VHD image size is 100 GB.
- The MX-ONE Azure image is based on Hyper-V, in a zip format around 6.5 GB. An example of zip filename is `Azure_Image-MX-ONE_7.3.sp0.hf0.rcX.zip`.
- Download the latest available image from the appropriate repository and store it in a drive in the local network to transfer it to Azure. Since the image is in compressed zip format, you must uncompress it before transferring it to Azure.

Azure Prerequisites

- Azure subscription and accounts should be active, for example, the engineer, who is configuring the MX-ONE system, shall be able to access Azure portal and has the proper rights to setup the environment.
- The virtual machines sizes are selected.
- Connectivity between the enterprise customer and Azure should be up and running, for example, Azure ExpressRoute.
- Resource groups, Vnet (Virtual Network), Subnets, Gateway Subnet, Availability and Azure Dedicated Hosts, etc are created and designated to MX-ONE deployment.

- NTP and DNS are configured and accessible from Azure, so the MX-ONE installation can access it during the installation process.

Network Topology

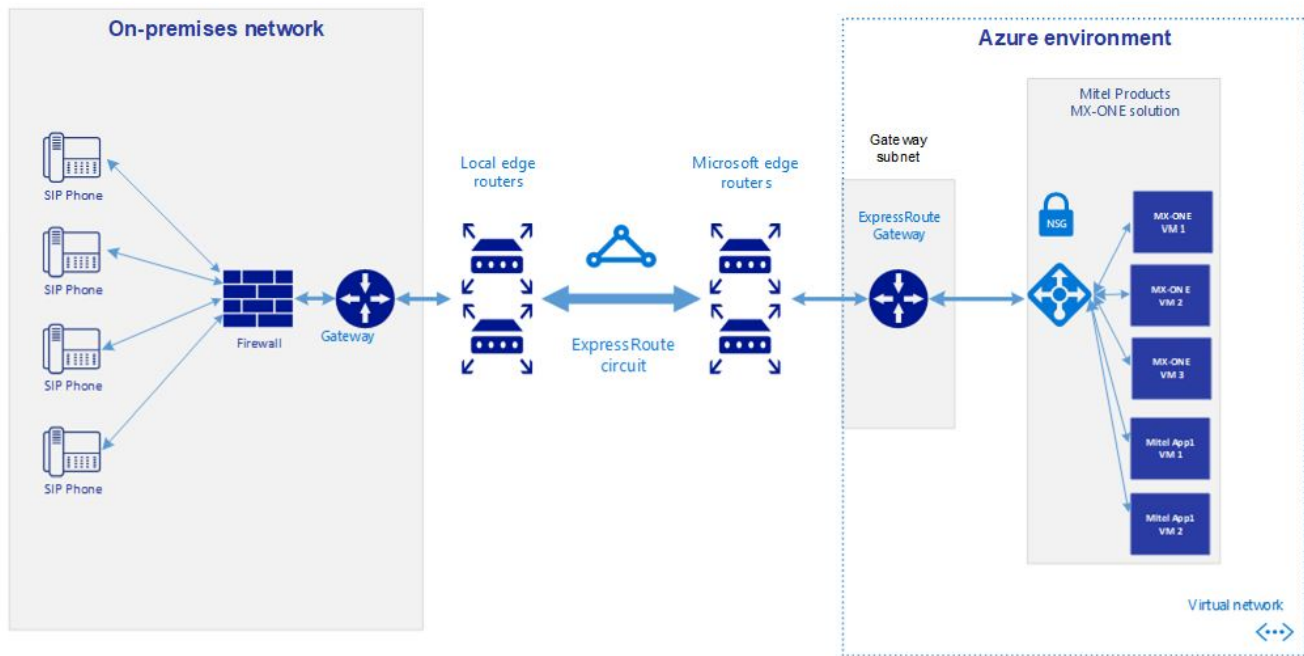
The following figure shows the recommended topology between the enterprise site and the Azure environment. Azure offers different connectivity possibilities, but Mitel recommends Azure ExpressRoute, because it offers lower latency.

A firewall is recommended to be added in the LAN (on-premises side). It is also recommended that only MX-ONE traffic is allowed in the setup.

Mitel never recommends that MX-ONE is placed directly to Internet, so MX-ONE shall not be facing Internet without proper Firewall or SBC in front on it.

Normally, the networks to be used in this solution shall be defined by the Enterprise IT team, so it is recommended that the partner have a discussion with the IT team before starting to plan the MX-ONE installation.

Figure 3.1: Network Topology



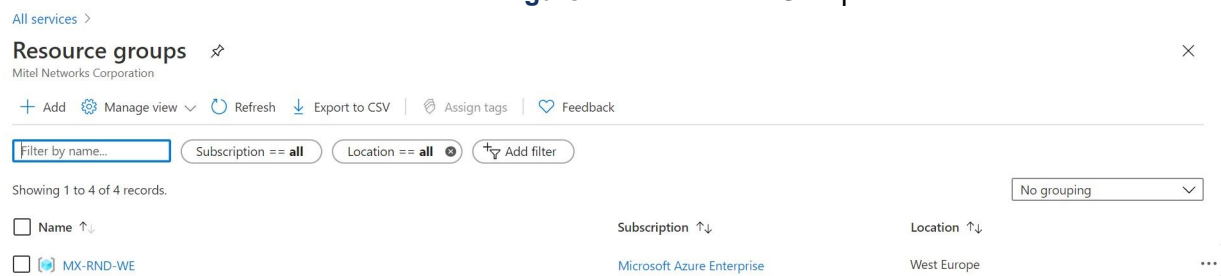
Azure Environment Preparation

The Azure environment needs to be prepared before you upload an MX-ONE image. The items described in the next sections are the minimum for the system to work and it is assumed the Azure environment was properly defined in advance.

Resource Groups

1. Login in Azure portal.
2. Create Resource Groups, if they are not already available to be used by the MX-ONE system. A Resource Group is required to upload the MX-ONE vhd image to the disk in Azure.
3. Go to Resource Groups and create a new group.
4. In the following figure, the Resource Groups called **MX-RND-WE** is already created.

Figure 4.1: Resource Group



Upload the Image to Azure from your Local Computer or Network Path

There are different ways of uploading an image to Azure, choose one of the available options:

- Powershell
- Azure GUI
- Storage Explorer

For more information, see *Choose an Azure solution for data transfer*, <https://docs.microsoft.com/en-us/azure/storage/common/storage-choose-data-transfer-solution> ().

In this document powershell is used to upload the MX-ONE image.

The vhd file is uploaded to Azure using the AzCopy tool via powershell.

Check the prerequisites in the Azure article, [Upload a vhd to Azure using Azure PowerShell](#).

After the prerequisites are in place, go to powershell in your computer and follow the steps in the article above.

Example of Uploading an MX-ONE VHD Image to Azure

The following steps shows an example of uploading an MX-ONE vhd image using the Azure article "Upload a vhd to Azure using PowerShell".

This process only needs to be done once per deployment, since a snapshot of the image can be created and it can be reused to deploy the whole MX-ONE system regardless of the number of MX-ONE servers.

The MX-ONE image in the example is called `MX-ONE_7.3.sp0.hf0.rc4.vhd` and it located in the network drive **Z**, the resource group is called **MX-RND-WE** and the disk name is called **mxonedisk73-disk1**.

Always check the Microsoft Azure documentation for the latest commands.

1. Execute the following commands:

- a. `$vhdSizeBytes = (Get-Item Z:\Azure_Image-MX-ONE_7.3.sp0.hf0.rc4\MX-ONE_7.3.sp0.hf0.rc4\MX-ONE_7.3.sp0.hf0.rc4.vhd).Length`
- b. `$diskconfig = New-AzDiskConfig -SkuName 'Standard_LRS' -OsType 'Linux' -UploadSizeInBytes $vhdSizeBytes -Location 'West Europe' -CreateOption 'Upload'`
- c. `New-AzDisk -ResourceGroupName 'MX-RND-WE' -DiskName 'mxonedisk73-disk1' -Disk $diskconfig`

The figure below shows the result of the commands.

```
PS C:\WINDOWS\system32> $vhdSizeBytes = (Get-Item Z:\Azure_Image-MX-ONE_7.3.sp0.hf0.rc4\MX-ONE_7.3.sp0.hf0.rc4\MX-ONE_7.3.sp0.hf0.rc4.vhd).Length
PS C:\WINDOWS\system32> $diskconfig = New-AzDiskConfig -SkuName 'Standard_LRS' -OsType 'Linux' -UploadSizeInBytes $vhdSizeBytes -Location 'West Europe' -CreateOption 'Upload'
PS C:\WINDOWS\system32> New-AzDisk -ResourceGroupName 'MX-RND-WE' -DiskName 'mxonedisk73-disk1' -Disk $diskconfig

ResourceGroupName : MX-RND-WE
ManagedBy        :
Sku               : Microsoft.Azure.Management.Compute.Models.DiskSku
Zones             :
TimeCreated       : 2020-03-26 16:54:23
OsType            : Linux
HyperVGeneration :
CreationData      : Microsoft.Azure.Management.Compute.Models.CreationData
DiskSizeGB        :
DiskSizeBytes     :
UniqueId          :
EncryptionSettingsCollection :
ProvisioningState  : Succeeded
DiskIOPSReadWrite : 500
DiskMBpsReadWrite : 60
DiskState          : ReadyToUpload
Encryption         : Microsoft.Azure.Management.Compute.Models.Encryption
Id                : /subscriptions/.../resourceGroups/MX-RND-WE/providers/Microsoft.Compute/disks/mxonedisk73-disk1
Name              : mxonedisk73-disk1
Type              : Microsoft.Compute/disks
Location          : westeurope
Tags              : {}
```

2. Execute the following commands:

- a. `$diskSas = Grant-AzDiskAccess -ResourceGroupName 'MX-RND-WE' -DiskName 'mxonedisk73-disk1' -DurationInSecond 86400 -Access 'Write'`
- b. `$disk = Get-AzDisk -ResourceGroupName 'MX-RND-WE' -DiskName 'mxonedisk73-disk1'`

```
PS C:\WINDOWS\system32> $diskSas = Grant-AzDiskAccess -ResourceGroupName 'MX-RND-WE' -DiskName 'mxonedisk73-disk1' -DurationInSecond 86400 -Access 'Write'
PS C:\WINDOWS\system32> $disk = Get-AzDisk -ResourceGroupName 'MX-RND-WE' -DiskName 'mxonedisk73-disk1'
```

- c. `.\azcopy.exe copy "Z:\Azure_Image-MX-ONE_7.3.sp0.hf0.rc4\MX-ONE_7.3.sp0.hf0.rc4\MX-ONE_7.3.sp0.hf0.rc4.vhd" $diskSas.AccessSAS --blob-type PageBlob`

The transfer of the files takes some time. Please wait until it is completed. In the example below it took 160 minutes.

```
PS C:\Azure_tools\azcopy_windows_amd64_10.3.4> .\azcopy.exe copy "2:\Azure_Image-MX-ONE_7.3.sp0.hf0.rc4\MX-ONE_7.3.sp0.hf0.rc4\MX-ONE_7.3.sp0.hf0.rc4.vhd" $diskSas.
AccessSAS --blob-type PageBlob
INFO: Scanning...

Job 70516f55-0e05-e143-6c99-799f3430d454 has started
Log file is located at: C:\Azure_tools\azcopy\70516f55-0e05-e143-6c99-799f3430d454.log

100.0 %, 0 Done, 0 Failed, 1 Pending, 0 Skipped, 1 Total,

Job 70516f55-0e05-e143-6c99-799f3430d454 summary
Elapsed Time (Minutes): 160.4862
Total Number Of Transfers: 1
Number of Transfers Completed: 1
Number of Transfers Failed: 0
Number of Transfers Skipped: 0
TotalBytesTransferred: 107374182912
Final Job Status: Completed

PS C:\Azure_tools\azcopy_windows_amd64_10.3.4>
```

3. `Revoke-AzDiskAccess -ResourceGroupName 'MX-RND-WE' -DiskName 'mxone-disk73-disk1'`

```
PS C:\Azure_tools\azcopy_windows_amd64_10.3.4> Revoke-AzDiskAccess -ResourceGroupName 'MX-RND-WE' -DiskName 'mxonedisk73-disk1'

Name       : 01d57d92-ed7c-41f6-98c3-b9b59e49c1ce
StartTime  : 2020-03-26 21:49:18
EndTime    : 2020-03-26 21:49:50
Status     : Succeeded
Error      :
```

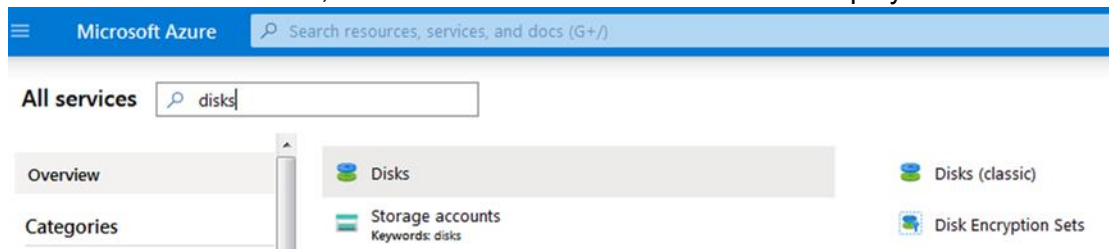
Now the image is uploaded in Azure.

Create an Image Snapshot

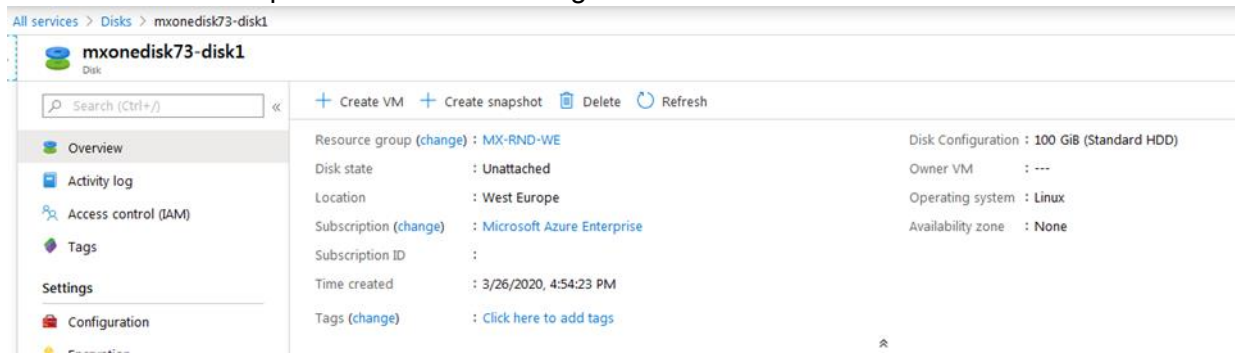
In the Azure portal and create a snapshot of the MX-ONE uploaded image, if needed. The snapshot can be used to create MX-ONE virtual machines when it is needed. So, it simplifies and speeds up the deployment when many MX-ONE servers need to be deployed, because the image is uploaded once.

To create the MX-ONE image snapshot:

1. In the Azure portal, left menu, select **All services**.
2. In the All services search box, enter disks and then select **Disks** to display the list of available disks.



3. Select the disk and upload the MX-ONE image.



4. Follow the steps 4 to 8 in the **Copy a disk** section in the article **Create a VM from a VHD by using the Azure portal** (link below) to create the snapshot.

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/create-vm-specialized-portal>.

Create a Disk

1. Follows the steps 9 to 17 in the following article to create the disk to be used in the Virtual Machine. The recommended disk is Premium (SSD).

[Create a VM from a VHD by using the Azure portal](#)

Figure 4.2: Manage Disks

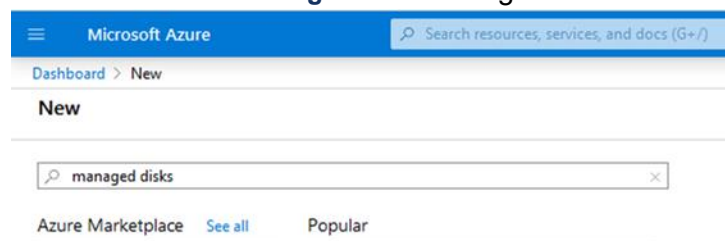


Figure 4.3: Create Manage Disk

Dashboard > New > Marketplace > Managed Disks > Create managed disk

Create managed disk

Basics Encryption Tags Review + create

Select the disk type and size needed for your workload. Azure Disks are designed for 99.999% availability. Azure Managed Disks encrypt your data at rest, by default, using Storage Service Encryption. [Learn more about disks.](#)

Project details

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

Subscription *

Resource group * [Create new](#)

Disk details

Disk name *

Region *

Availability zone

Source type *

*Source snapshot

Size * Premium SSD [Change size](#)

Select a disk size

Browse available disk sizes and their features.

Storage type

Size	Disk tier	Max IOPS	Max throughput
4 GiB	P1	120	25
8 GiB	P2	120	25
16 GiB	P3	120	25
32 GiB	P4	120	25
64 GiB	P6	240	50
128 GiB	P10	500	100
256 GiB	P15	1100	125
512 GiB	P20	2300	150
1024 GiB	P30	5000	200
2048 GiB	P40	7500	250
4096 GiB	P50	7500	250
8192 GiB	P60	16000	500
16384 GiB	P70	18000	750
32767 GiB	P80	20000	900

Create a custom size

Enter the size of the disk you would like to create. You will be charged the same rate for your provisioned disk, regardless of how much of the disk space is being used. For example, a 200 GiB disk is provisioned on a 256 GiB disk, so you would be billed for the 256 GiB provisioned.

Custom disk size (GiB) *

- If more than one MX-ONE server (Service Node, Database, Provisioning Manager and Media Server) is required, use the snapshot to create the required number of disks. To do it, repeat steps 9 to 17 for each MX-ONE server.

Refer [Create a VM from a VHD by using the Azure portal.](#)

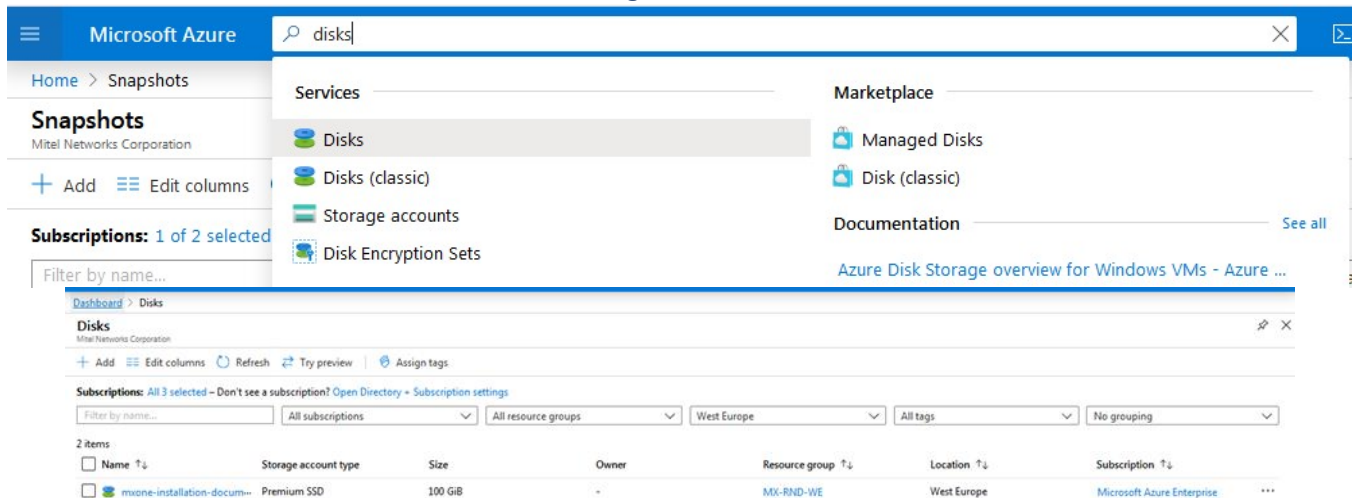
Create the MX-ONE VM and Additional Setup

To create a VM instance of MX-ONE setup and for the additional setups required in MX-ONE Azure deployment, see the instructions in the following sections.

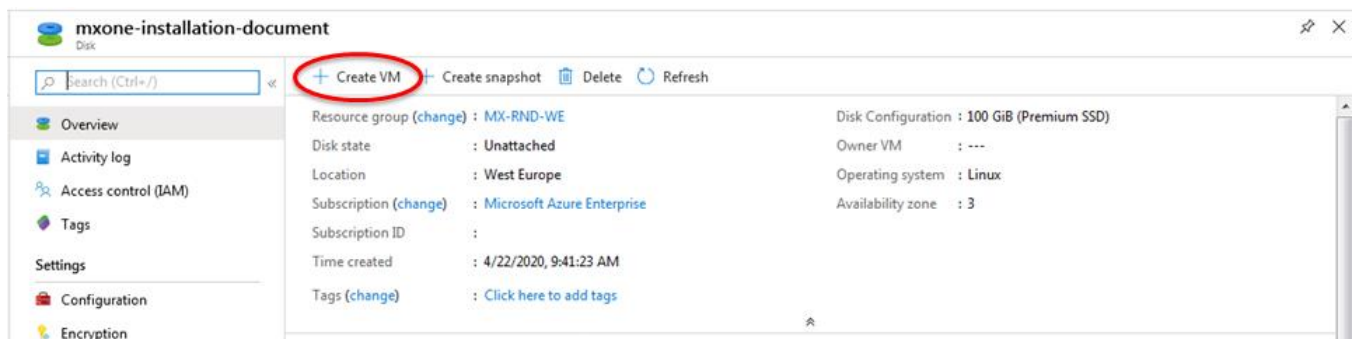
Create the MX-ONE VM using the Disk

1. Search by disks.

Figure 5.1: Disk Search



2. Select the disk that you created in the previous step and then click **Create VM**.



3. Follow the steps shown in the GUI or follow the steps in the Create a VM from a disk in the article [Create a VM from a VHD by using the Azure portal](#).
4. Adjust the VM size according to the MX-ONE system size. The *MX-ONE Virtualization and IOPS Disk and Network bandwidth requirements* documents are valid to Azure and cloud deployments. The recommended Virtual Machines sizes are to be used with MX-ONE 7.3 and later are:
 - Minimum: Family D2s-64s v3 latest generation.
 - D4s_v3 /D4_v3 (4 vCPU(s), 16 GB RAM) or equivalent *
 - D8s_v3 /D8_v3 (8 vCPU(s), 32 GB RAM) or equivalent *

- Other suitable family is Fsv2-series.
 - F4s_v2 (4 vCPU(s), 8 GB RAM) or equivalent *
 - F8s_v2 (8 vCPU(s), 16 GB RAM) or equivalent *

* The size of the virtual machines needs to be defined by the number of SIP users, the MX-ONE application and total number of users in the database used in the virtual machine.

- Note that when deploying MX-ONE in Azure, the MX-ONE redundancy options are not available. To have availability in MX-ONE system, the Azure built-in resources must be used. The resources are for example Availability and Azure Dedicated Hosts.
 - Availability, [Availability options for virtual machines in Azure](#)
 - Azure Dedicated Hosts, [Azure Groups, hosts, and VMs](#)
- Select the availability options and availability zone required by the customer who will use MX-ONE.
- Under Advanced selected Host group if Azure Dedicated Hosts are available in the customer Azure subscription.

Dashboard > Disks > mxone-installation-document > Create a virtual machine

Create a virtual machine

Basics Disks Networking Management Advanced Tags Review + create

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

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

Subscription: Microsoft Azure Enterprise ()
Resource group: MX-RND-WE [Create new](#)

Instance details

Virtual machine name: mxone-azure-installation-document ✓

Region: (Europe) West Europe

Availability options: Availability zone

Availability zone: 3

Image: mxone-installation-document [Browse all public and private images](#)

Azure Spot instance: ☐ Yes ☒ No

Size: Standard D4s v3
4 vcpus, 16 GiB memory (€ /month)
[Change size](#)

[Review + create](#) < Previous Next: Disks >

- In the networking tab select the appropriate subnet.

Dashboard > Disks > mxone-installation-document > Create a virtual machine

Create a virtual machine

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 * [Create new](#)

Subnet * [Create new](#)

Public IP [Create new](#)

NIC network security group ☐ None ☒ Basic ☐ Advanced

Public inbound ports * ☒ None ☐ Allow selected ports

Select inbound ports

Accelerated networking ☐ On ☒ Off

The selected image 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](#)

[Review + create](#) < Previous Next : Management >

9. Setup the other options.

10. Click **Review + create**.

Dashboard > Disks > mxone-installation-document > Create a virtual machine

Create a virtual machine

✓ Validation passed

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

mxone-installation-document **Standard D4s v3**
Image 4 vcpus, 16 GiB memory

Basics

Subscription Microsoft Azure Enterprise

Resource group MX-RND-WE

Virtual machine name mxone-azure-installation-document

Region West Europe

Availability options Availability zone

Availability zone 3

Authentication type SSH public key

Key pair name None

Public inbound ports None

Azure Spot No

Disks

OS disk type Premium SSD

Use managed disks Yes

Use ephemeral OS disk No

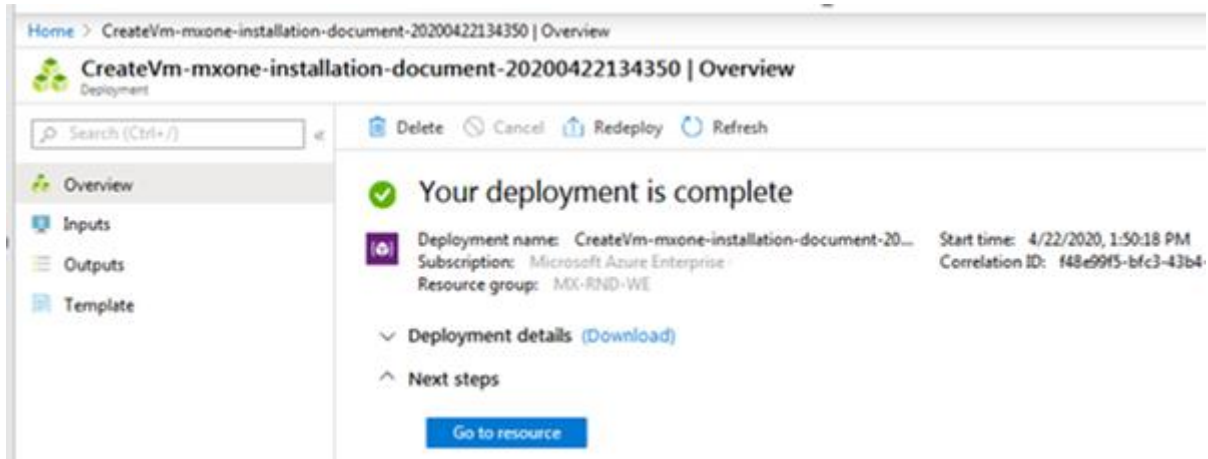
Networking

Virtual network (new) MX-RND-WE-vnet

Subnet (new) default (10.0.1.0/24)

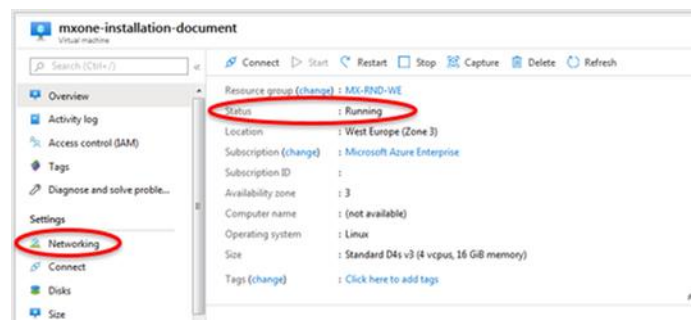
[Create](#) < Previous Next > [Download a template for automation](#)

11. If the information is correct, click **Create** and wait the VM to be created.

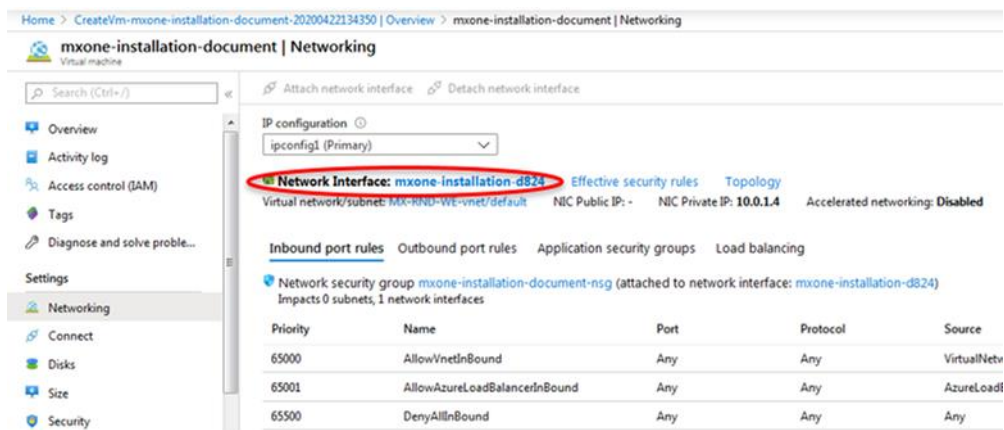


Setup Static IP Addresses to be Used in MX-ONE VM

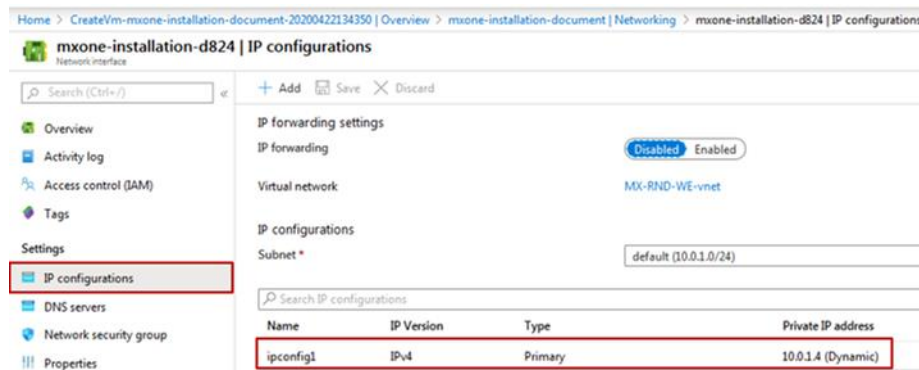
1. When the VM is up and running, go to the VM page and access the networking under the Settings session.



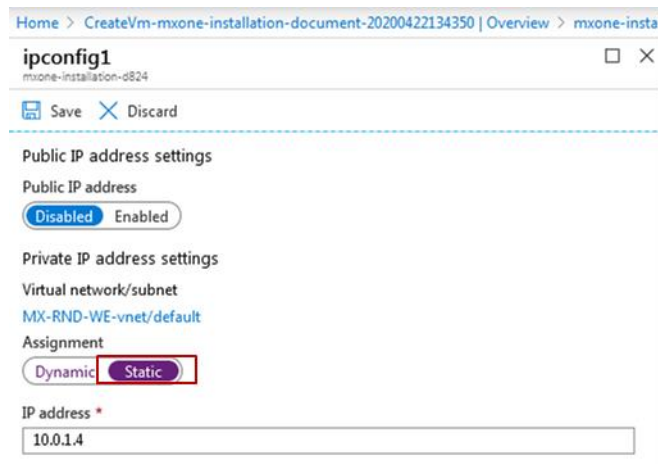
2. Then click **Network Interface**.



3. In the Network Interface, then click **IP Configuration** under **Settings** and then **ipconfig1**.



4. Change the IP address from Dynamic to Static.



Wait until the setup is completed.

5. Now, a secondary private IP address needs to be created to be used for the MX-ONE database.

NOTE: This setup is important, because it will reserve this IP address and it will not be dynamic allocated by Azure when a new VM is created.

6. Go back to the previous page and click **Add**.
7. Add name for the IP configuration and the static IP address.

Home > CreateVm-mxone-installation-document-20200422134350 | Overview > mxone-installation-document | Networking

Add IP configuration

mxone-installation-d824

Name *
ipconfig2-db ✓

Type
Primary Secondary

Primary IP configuration already exists

Private IP address settings

Allocation
Dynamic Static

IP address *
10.0.1.5 ✓

Public IP address
Disabled Enabled

8. When the IP address is added, the result is shown in the following figure.

mxone-installation-d824 | IP configurations

Network interface

Search (Ctrl+F)

+ Add Save Discard

IP forwarding settings

IP forwarding Disabled Enabled

Virtual network MX-RND-WE-vnet

IP configurations

Subnet * default (10.0.1.0/24)

Search IP configurations

Name	IP Version	Type	Private IP address
ipconfig1	IPv4	Primary	10.0.1.4 (Static)
ipconfig2-db	IPv4	Secondary	10.0.1.5 (Static)

NOTE: The Public IP address is not required for MX-ONE deployment as the system shall be using Express Route connectivity between the enterprise network and Azure.

Allow ICMP, SSH and HTTPS access to Service Node IP address

Azure blocks incoming traffic, so to be able to access the MX-ONE VM via SSH after the initial setup, the following needs to be done.

1. Go to **Networking** and click **Add inbound rule**.

The screenshot shows the Azure portal interface for a network interface. The 'Inbound port rules' tab is selected. A blue button labeled 'Add inbound port rule' is highlighted with a red box. Below the button, a table lists existing rules:

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

2. Add the SSH rule with the proper information of the network, so that your local computer can access the MX-ONE in Azure. The below is just an example.

NOTE: It is a best practice to define the specific network in the Source IP Addresses/CIDR ranges.

Add inbound security rule ×

srv1 mitel.com-nsg

Basic

Source * ⓘ

IP Addresses

Source IP addresses/CIDR ranges * ⓘ

10.0.1.0/24 ✓

Source port ranges * ⓘ

*

Destination * ⓘ

IP Addresses

Destination IP addresses/CIDR ranges * ⓘ

10.0.1.0/24 ✓

Destination port ranges * ⓘ

22 ✓

Protocol *

Any TCP UDP ICMP

Action *

Allow Deny

Priority * ⓘ

100

Name *

SSH

Description

Add

3. MX-ONE requires ICMP in the subnet during installation and for some functions, so an ICMP rule needs to be added.

Add inbound security rule
mxone-installation-document-nag

Basic

Source * ⓘ
IP Addresses

Source IP addresses/CIDR ranges * ⓘ
10.0.1.0/24 ✓

Source port ranges * ⓘ
*

Destination * ⓘ
IP Addresses

Destination IP addresses/CIDR ranges * ⓘ
10.0.1.0/24 ✓

Destination port ranges * ⓘ
* ✓

Protocol *
Any TCP UDP **ICMP**

Action *
Allow Deny

Priority * ⓘ
100

Name *
ICMP ✓

Description
ICMP - Traffic ✓

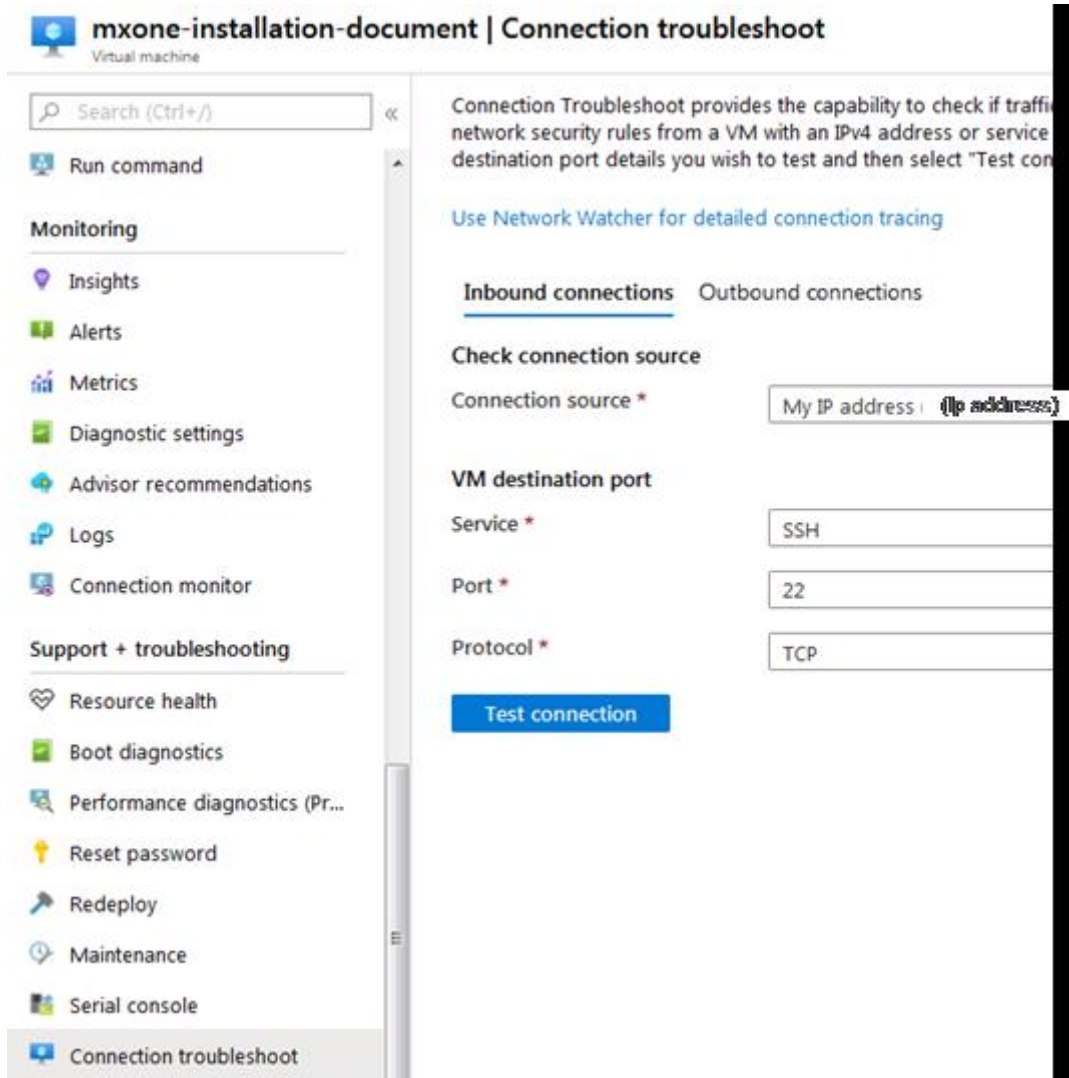
Add

4. Repeat the same procedure to create rules for HTTPS (PM and SNM) and SIP/TLS (5061) SIP/VDP (22226) and SIP/XML (22223).

NOTE: Any type of traffic that needs to be directed to MX-ONE or any application in Azure requires a rule. This is not covered in this document, so for additional information regarding MX-ONE TCP/UDP/SCTP ports read the MX-ONE document called “MiVoice MX-ONE System Planning – Description”, chapter 13 IP Protocols and Ports.

Test the Connectivity

1. Go to **Support + troubleshooting** and select **Connection troubleshoot** and then test the connectivity between your local network and the VM in Azure.



2. After the successful test, the Azure will be ready. Now, install MX-ONE.

Inbound connections Outbound connections

Check connection source

Connection source *

VM destination port

Service *

Port *

Protocol *

Test connection

✓ Network connectivity allowed

Deploy MX-ONE by Accessing VM via Serial Console

NOTE: The serial console is located under the VM, Support + troubleshooting.

1. Click on the serial console and wait the MX-ONE prompt.

The screenshot shows the 'mxone-installation-document | Serial console' window. The left sidebar contains a navigation menu with options like 'Run command', 'Monitoring', 'Alerts', 'Metrics', 'Diagnostic settings', 'Advisor recommendations', 'Logs', 'Connection monitor', 'Support + troubleshooting', 'Resource health', 'Boot diagnostics', 'Performance diagnostics (Pr...', 'Reset password', 'Redeploy', 'Maintenance', 'Serial console' (selected), 'Connection troubleshoot', and 'New support request'. The main area displays a list of boot messages with status icons (OK, U) and a login prompt at the bottom:

```

A OK U Started wicked network nanny service.
      Starting wicked managed network interfaces...
A OK U Started Load kdump kernel early on startup.
A OK U Started wicked managed network interfaces.
A OK U Reached target Network.
      Starting OpenSSH Daemon...
      Starting Open-iSCSI...
      Starting NTP Server Daemon...
      Starting Load kdump kernel and initrd...
A OK U Reached target Network is Online.
      Starting Hyper-V KVP Daemon...
A OK U Started Hyper-V KVP Daemon.
A OK U Started Open-iSCSI.
      Starting Login and scanning of iSCSI devices...
A OK U Reached target Remote File Systems (Pre).
A OK U Started Login and scanning of iSCSI devices.
A OK U Reached target Remote File Systems.
      Starting Permit User Sessions...
      Starting Write information about system start to syslog log...
A OK U Started NTP Server Daemon.
A OK U Reached target System Time Synchronized.
A OK U Started Discard unused blocks once a week.
A OK U Started Daily rotation of log files.
A OK U Reached target Timers.
      Starting Postfix Mail Transport Agent...
      Starting Discard unused blocks on filesystems from /etc/etab...
      Starting Rotate log files...
A OK U Started Permit User Sessions.
      Starting Terminate Plymouth Boot Screen...
      Starting Hold until boot process finishes up...

Welcome to SUSE Linux Enterprise Server 12 SP5 (x86_64) - Kernel 4.12.14-122.12-default (ttyS0).

linux-7ug6 login: root
Password:
linux-7ug6:~ # net_setup
  
```

2. Follow the normal MX-ONE setup described in MX-ONE CPI.

The screenshot shows the 'mxone-installation-document | Serial console' window. The left sidebar is the same as in the previous image. The main area displays the 'MX-ONE Telephony System Setup, Version:7.3.0.0.4' header and a dialog box titled 'MX-ONE Initial Setup'.

```

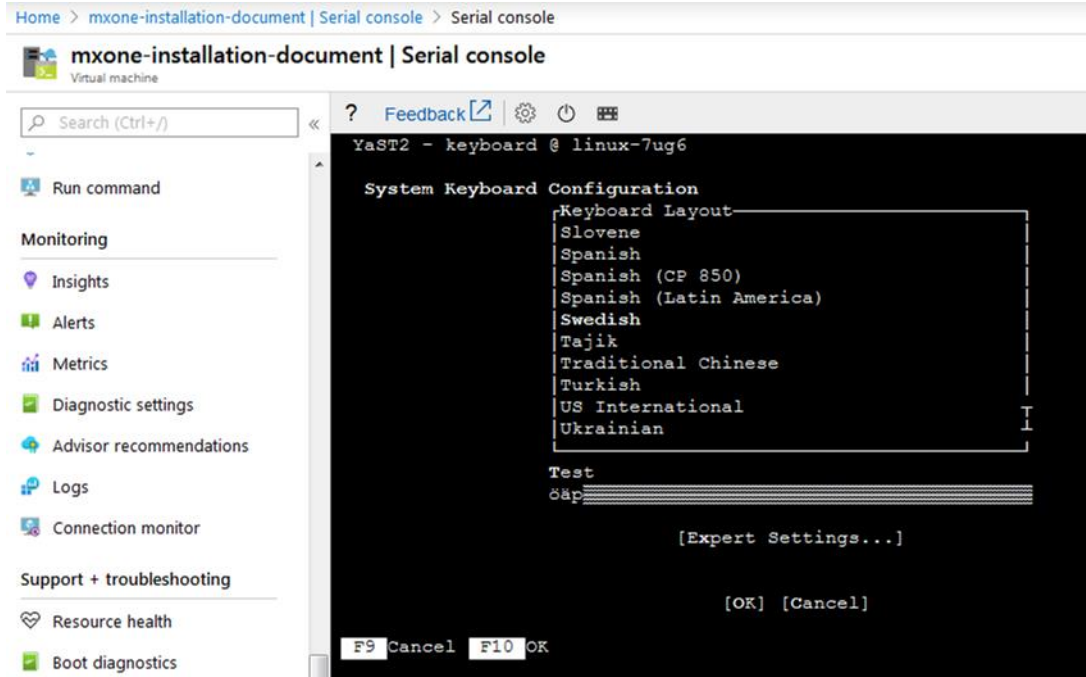
MX-ONE Telephony System Setup, Version:7.3.0.0.4

MX-ONE Initial Setup
Welcome to MX-ONE Telephony System Setup

You have to configure your server before starting
the Telephony System.
Do you want to configure your server now?

< Yes > < No >
  
```

NOTE: The contrast in the net_setup (Yast2) is not optimal, it is the SLES behavior when console is used. So, in the initial setup, after the correct setting is done, use F10 to select OK instead of tab.



NOTE: During the initial installation, the test of default gateway will fail, because Azure does not have a formal default gateway. So, when setup shows the question below, type **Yes**.



3. Complete the remaining setup.

When the initial setup is done, you have the possibility to access the system via SSH and finish the MX-ONE setup from there.

4. Complete the system setup as a normal MX-ONE deployment.

Deployment of MX-ONE in Azure HCI Stack Setup

Introduction

Azure Stack HCI is hyper-converged cluster solution that allows its users to run their virtualized Windows and Linux workloads running in a hybrid environment. Azure Stack HCI allows a hybrid approach integrated with native Azure capabilities such as cloud-based monitoring, site recovery, backup, Azure Monitor, and Azure Security Center.

In addition, this chapter covers how to deploy MX-ONE in Azure Stack HCI.

Prerequisites

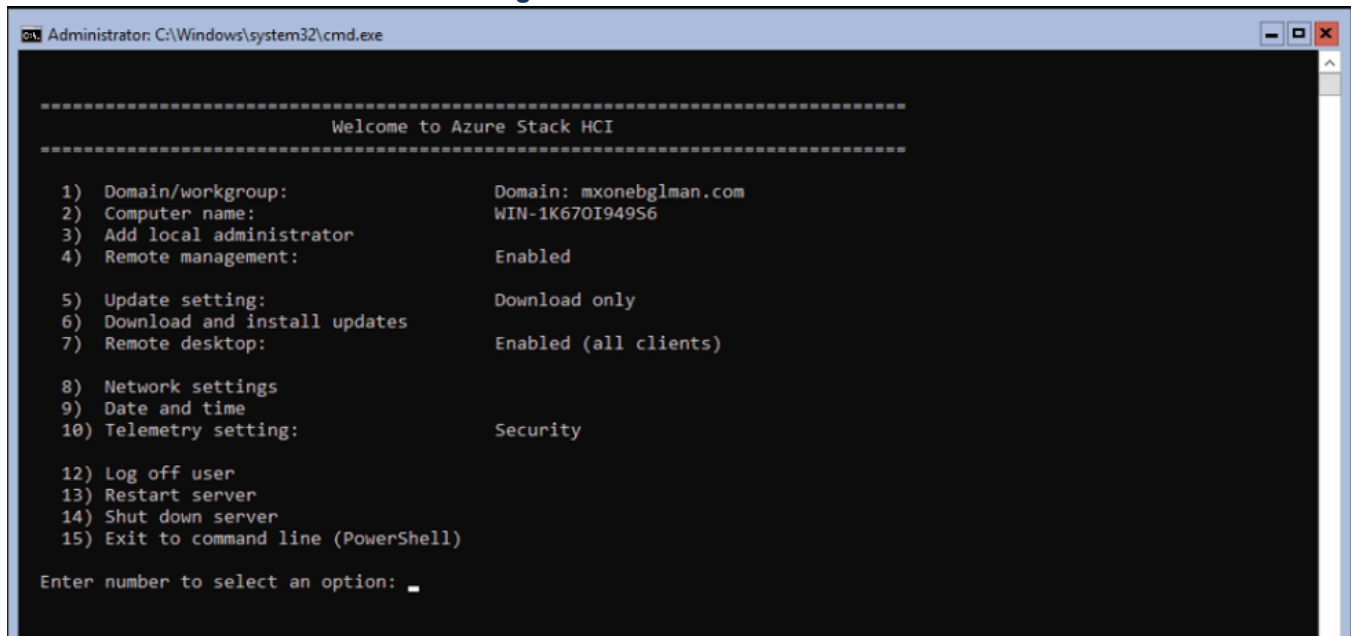
Before you deploy the Azure Stack HCI operating system, you must have the following requisites:

- DELL-440 (Hardware)
- RAM: 32 GB
- Hard Drive: 1 TB
- 2019 Win Server for Management (Windows Admin Center)

Installation Procedure

1. Download the Azure Stack HCI.
<https://azure.microsoft.com/en-us/products/azure-stack/hci/hci-download/>
2. Make a bootable pendrive for Azure Stack HCI.
3. Download the Windows 2019 driver or download Windows Server 2019.
4. Make a bootable pendrive for 2019 or keep the download drivers in pendrive.
5. Connect the Azure Stack HCI (bootable) pendrive to Dell 440 and boot it from USB stick.
6. After booting, connect the 2019 bootable iso pendrive or provide the path for drivers (2019) and enter the password when it prompts.
7. After installation, you will get the following Azure Stack HCI window.

Figure 7.1: Welcome to Azure Stack HCI



8. Enter the number to select an option when system prompts.
9. Press the key 8 and add the IP Address and DNS Server details on both Network Interface Card (NIC).
10. Enter the domain details.
11. Enable Remote desktop.
12. Install Windows Admin Centre on WIN 2019 (different server) and add this on same domain as Azure Stack HCI.
13. Login on Windows Admin Centre and add the Azure Stack HCI system.
14. Go to **Windows Admin Center > Roles & Feature > add roles** (such as Hyper -V Network controller, and so on).
15. Login on Powershell and ping the gateway and domain.
16. Disable the Windows firewall if not reachable as mentioned in the following screen.

Figure 7.2: Disable of Windows Firewall

```
netsh advfirewall set currentprofile state off  
  
netsh advfirewall set domainprofile state off  
  
netsh advfirewall set privateprofile state off  
  
netsh advfirewall set publicprofile state off  
  
netsh advfirewall set allprofiles state off
```

<https://www.windows-commandline.com/enable-disable-firewall-command-line/>

17. Restart the system.

18. Go to **Windows Admin Center**> **Virtual switches** as shown in the following screen.

Figure 7.3: Virtual Switches

Windows Admin Center | Server Manager

WIN-1K67OI949S6

Tools

Virtual switches

Name	Network adapter	Switch type	Shared with management OS
Test-External	Broadcom NetXtreme Gigabit Ethernet	External	Yes
Test-Internal		Internal	Yes

Settings for Test-Internal

General

Switch name: Test-Internal

Notes:

Switch type: Internal

Settings for Test-External

General

Switch name: Test-External

Notes:

Switch type: External

Network adapters:

Name	Description	IP Addresses	Connection state	Link Speed	MAC Address
NIC1	Broadcom NetXtreme Gigabit Ethernet		Connected	1 Gbps	4C-D9-8F-A7-C9-B1
NIC2	Broadcom NetXtreme Gigabit Ethernet #2	10.211.80.81/24	Connected	1 Gbps	4C-D9-8F-A7-C9-B2

The server may lose its network connection while the changes are applied. This may affect any network operations in progress, including this management session. These changes also may overwrite some static changes. If that happens, you must reapply the static changes to restore network connectivity.

Allow management OS to share this network adapter ☒

19. Add Virtual **Switch type** (both **Internal** and **External** switch types).
20. Select the **NIC1** IP address.

```

Administrator: C:\Windows\system32\cmd.exe

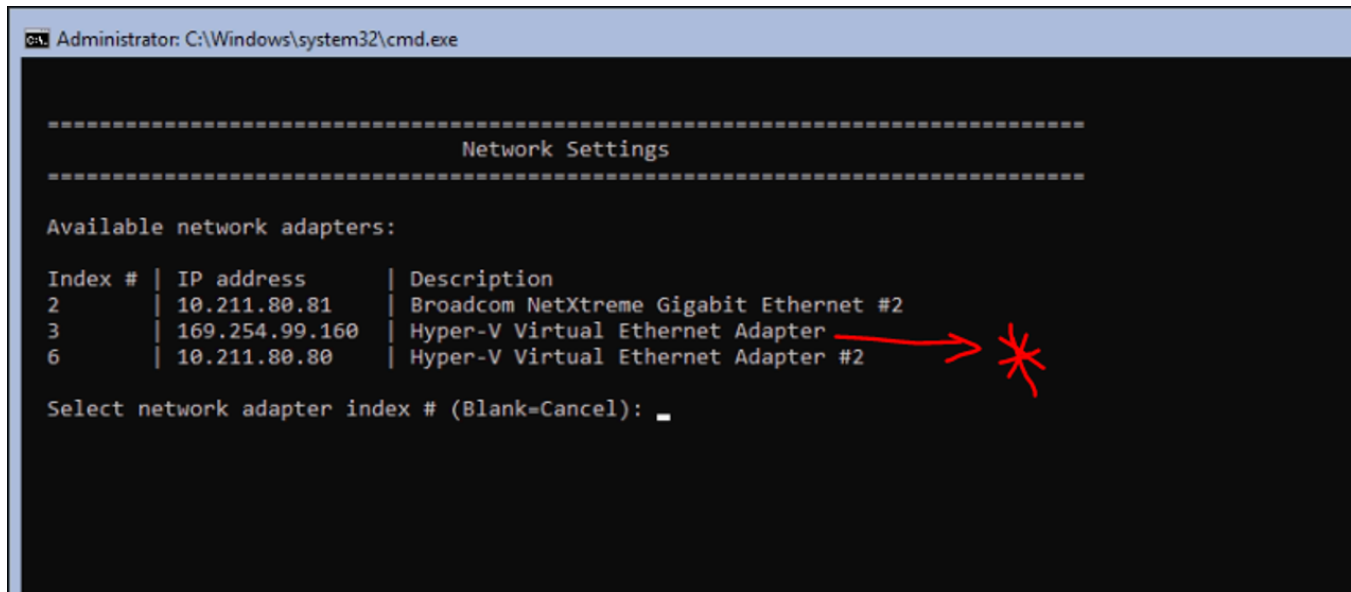
=====
Network Settings
=====

Available network adapters:

Index # | IP address      | Description
-----|-----|-----
2       | 10.211.80.81    | Broadcom NetXtreme Gigabit Ethernet #2
3       | 169.254.99.160 | Hyper-V Virtual Ethernet Adapter
6       | 10.211.80.80    | Hyper-V Virtual Ethernet Adapter #2

Select network adapter index # (Blank=Cancel):

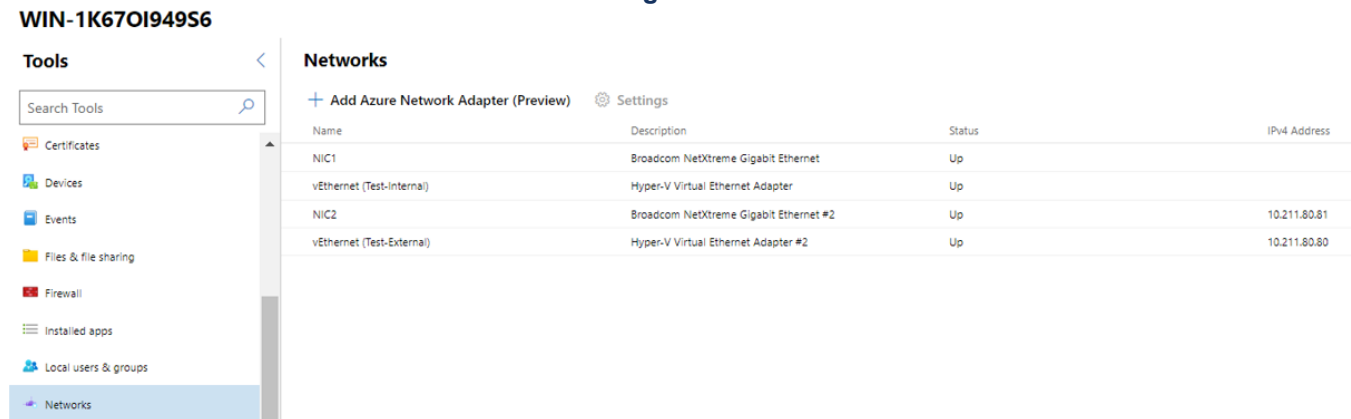
```



NOTE: For Internal switch, it is not compulsory to change the IP address.

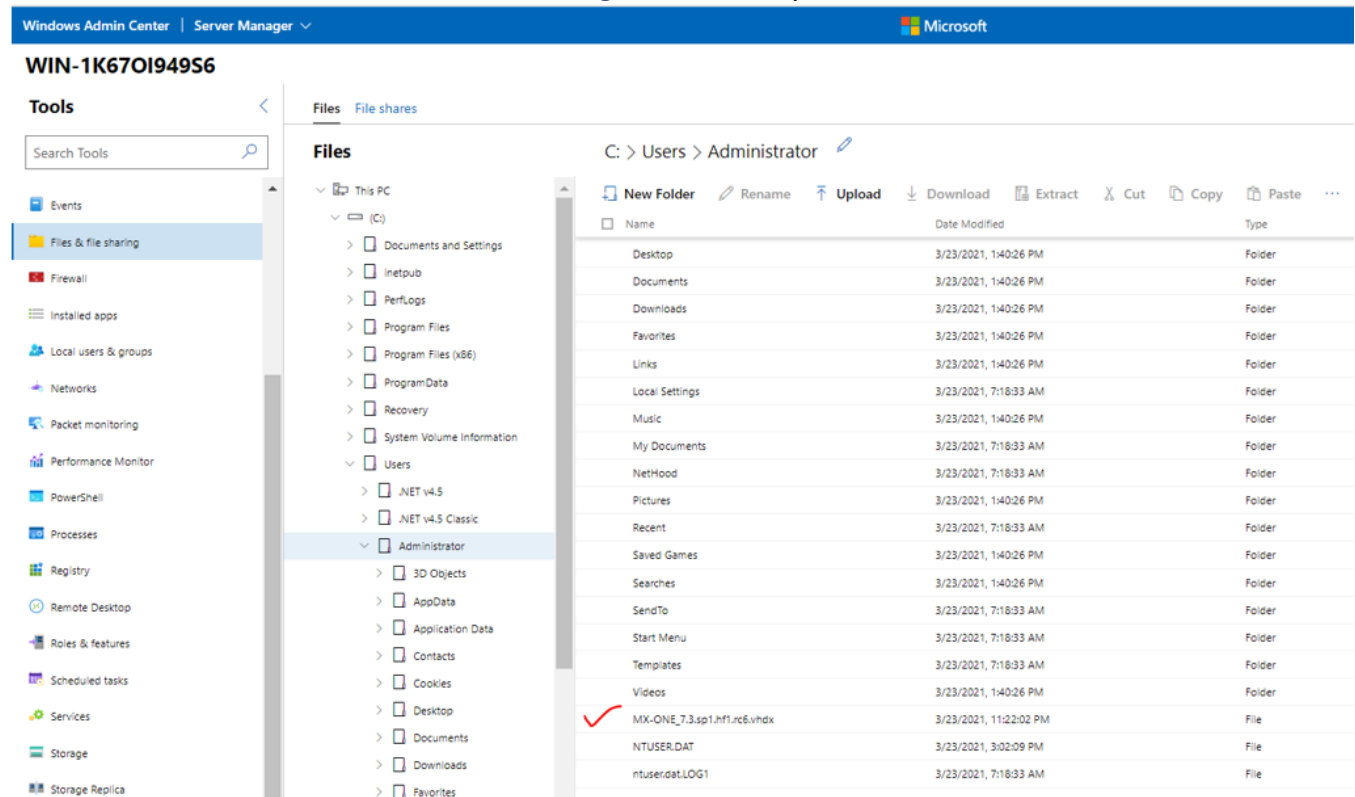
21. Go to **Windows Admin Center** > **Networks**.

Figure 7.4: Networks



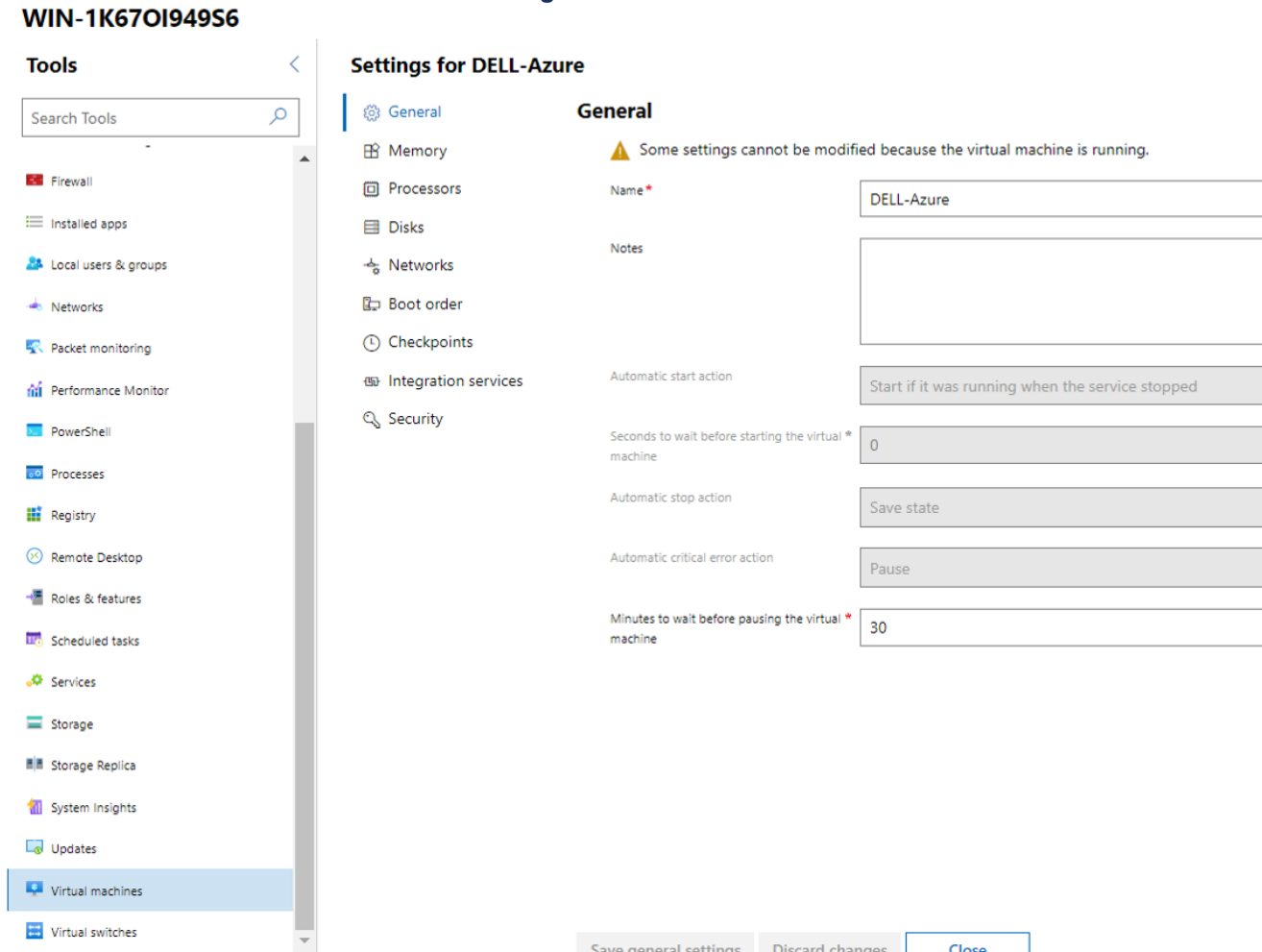
22. Go to **Windows Admin Center** > **Files & file sharing** > select the path where you want to upload the .vhdx file (for example: C:>Users\Administrators).

Figure 7.5: File Upload Path



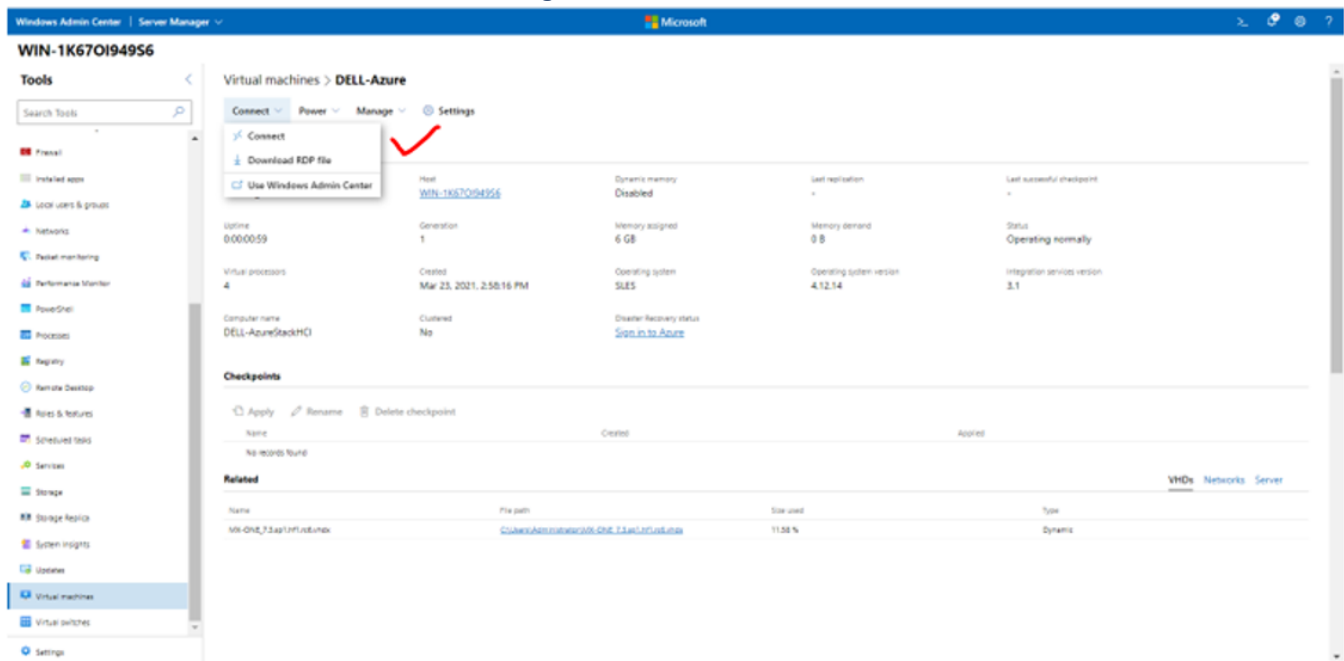
23. Go to Windows Admin Center> Virtual Machines> add a new virtual machine.

Figure 7.6: Add Virtual Machine



24. Enter the required details for Azure **Memory**, **Processors**, **Disks**, and **Networks**.
25. Power on the Virtual machine and select **Connect** option to connect the virtual machine (rdp/connect/Windows Admin Centre).

Figure 7.7: Virtual Machine Connect



26. Install the MX-ONE (with same domain as in Azure Stack HCI and Windows Admin Center) on Remote Desktop Protocol (RDP).

Good to know / limitations

- The default gateway validation will fail during the installation.
- When using the Azure console, the contrast in the net_setup (Yast2) is not optimal. This is a SLES behavior when console is used.

Acronyms, Abbreviations and Glossary

DNS

Domain Name System

GUI

Graphical User Interface

HTTPS

Hypertext Transfer Protocol Secure

ICMP

Internet Control Message Protocol

IT

Information Technology

NTP

Network Time Protocol

SBC

Session Border Controller

SCTP

Stream Control Transmission Protocol

SIP

Session Initiation Protocol

SSD

Solid-State drive

SSH

Secure Shell

TCP

Transport Control Protocol

TLS

Transport Layer Security

UDP

User Data Protocol

VHD

Virtual Hard Disk

Vnet

Virtual Network

XML

Extensible Markup Language

References

- General Azure documentation page: <https://docs.microsoft.com/en-us/azure/?product=featured>
- Choose an Azure solution for data transfer: <https://docs.microsoft.com/en-us/azure/storage/common/storage-choose-data-transfer-solution>
- Upload a vhd to Azure using Azure PowerShell: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disks-upload-vhd-to-managed-disk-powershell>
- Create a VM from a VHD by using the Azure portal: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/create-vm-specialized-portal>
- Availability: <https://docs.microsoft.com/en-us/azure/virtual-machines/linux/availability>
- Azure Dedicated Hosts: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/dedicated-hosts#groups-hosts-and-vm>
- Azure networking services overview: <https://docs.microsoft.com/en-us/azure/networking/networking-overview>
- Virtual Network documentation: <https://docs.microsoft.com/en-us/azure/virtual-network/>
- ExpressRoute overview: <https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction> and <https://docs.microsoft.com/en-us/azure/expressroute/>
- Designing for high availability with ExpressRoute: <https://docs.microsoft.com/en-us/azure/expressroute/designing-for-high-availability-with-expressroute>
- ExpressRoute FAQ: <https://docs.microsoft.com/en-us/azure/expressroute/expressroute-faqs>
- Virtual Hard Disk: [https://docs.microsoft.com/en-us/previous-versions/windows/desktop/legacy/dd323654\(v%3Dvs.85\)](https://docs.microsoft.com/en-us/previous-versions/windows/desktop/legacy/dd323654(v%3Dvs.85))

