Microsoft Azure Exam for AZ – 300 & 301

Deploy & Configure Infrastructure

Agenda
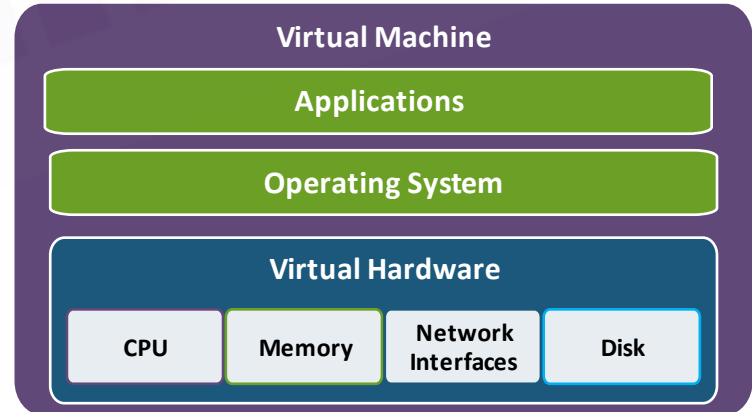
- ❏ Virtual Machine

- ❏ Automating Deployments of VMs

- ❏ Azure PowerShell

- ❏ Azure Monitoring

Virtual Machine

What Is a Virtual Machine?

❑ A virtual machine is a computer file, typically called an image, which behaves like an actual computer.

❑ In other words, it is like creating a computer within a computer.

❑ It runs in Windows/Linux, much like any other program, giving the end user the same experience on a virtual machine as they would have on the host operating system itself.

❑ For servers, the multiple operating systems run side by side with a piece of software called a hypervisor to manage them.

❑ Each virtual machine provides its own virtual hardware, including CPUs, memory, hard drives, network interfaces, and other devices.

❑ The virtual hardware is then mapped to the real hardware on the physical machine.

Virtual Machine

Applications

Operating System

Virtual Hardware

| CPU | Memory | Network Interfaces | Disk |

What Is Azure Virtual Machine?

❏Azure Virtual Machine (VM) is one of several types of on-demand, scalable computing resources that Azure offers.

When you run Azure VMs, you pay for the compute time on a per-minute basis.

The price for VMs is calculated based on their size, the operating system, and any licensed software installed.

Therefore, to avoid the corresponding charges whenever you are not using it, you should change its state to **Stopped** (Deallocated).

Azure VM: Classic and ARM

❑ The Azure classic deployment model was originally referred to as the Service Management model.

❑ This model served as the primary method of deploying and managing Azure services until the introduction of Azure Resource Manager (ARM).

❑ You can provision Azure VMs by using either the classic or the Azure Resource Manager deployment model.

❑ In comparison to the classic deployment model, the capabilities of Azure Resource Manager offer significant changes to the implementation and management of Azure VMs, including:

Support for up to three fault domains in an availability set. The classic deployment model supports two fault domains in an availability set.

Integration of the Azure Key Vault with Azure VMs to help secure secret information such as administrative passwords. Azure Key Vault also facilitates platform-based encryption of VM disks.

Azure VM: Sizing

❏ In Azure, you select from a range of predefined configuration options that correspond to different VM sizes.

❏ The VM size determines characteristics such as the number and speed of its processors, amount of memory, maximum number of network adapters or data disks you can attach to it, and maximum size of a temporary disk.

| General purpose VM	Compute optimized VM	Memory optimized VM	Storage optimized VM	GPU optimized VM
• General purpose VM sizes provide balanced CPU-to-memory ratio.	• Compute optimized VM sizes have a high CPU-to-memory ratio.	• Memory optimized VM sizes offer a high memory-to-CPU ratio.	• Storage optimized VM sizes offer high disk throughput and IO.	• GPU optimized VM sizes are for heavy graphic rendering and video editing.

Azure VM: ACU

❑ ACU stands for Azure Compute Unit.

❑ This is a measurement created by Microsoft to provide a way to more accurately compare the vCPU performance (or the Virtual CPU Compute Performance) across Azure VM Instance sizes.

❑ Using the Azure Compute Unit measurement, you will be able to identify which VM size will fulfill your cloud compute performance requirements.

❑ It is based on A0 (extra small) having a value of 50.

  ❑ A VM with an ACU of 100 has twice the compute of a VM with an ACU of 50.

  ❑ A VM with an ACU of 200 would be twice that of a VM with an ACU of 100 and so on.

Azure VM:
Disks
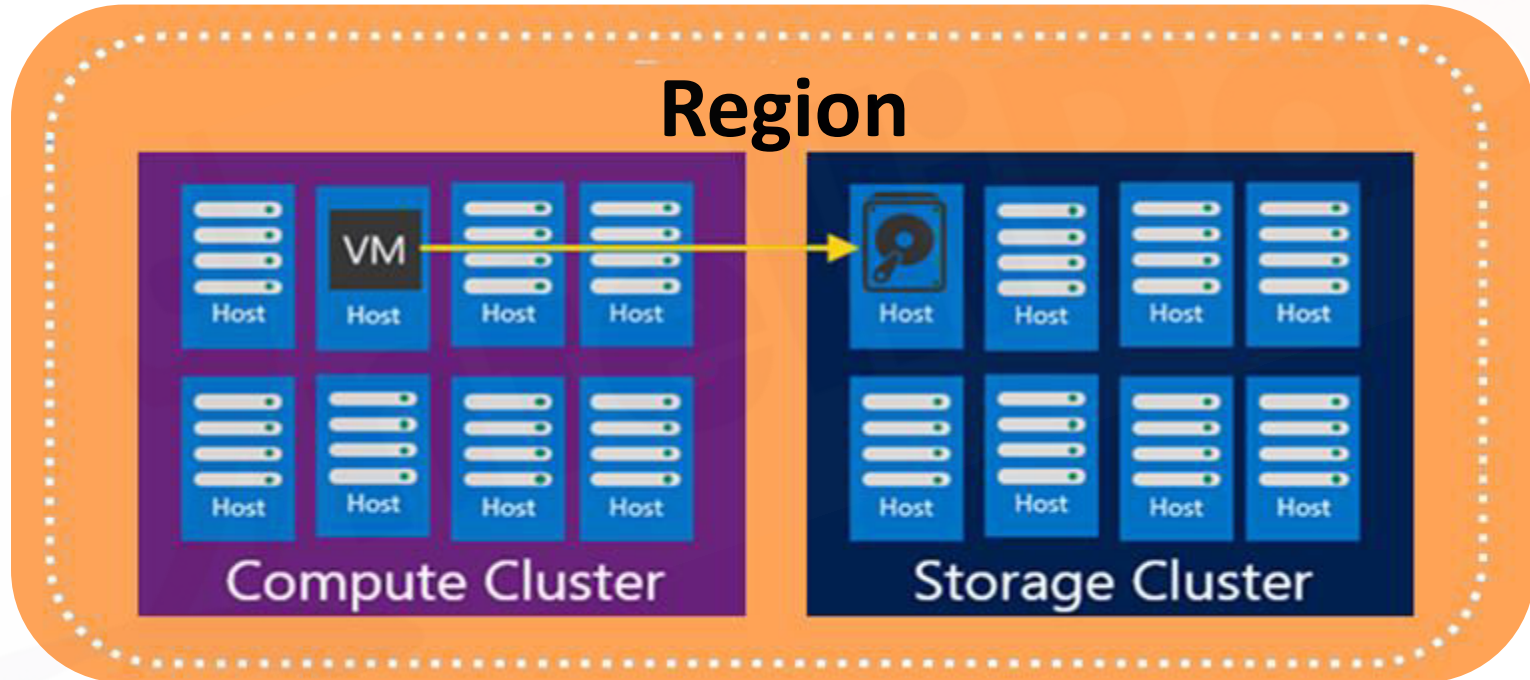
Azure VM:
Disks

❑ Disks that you attach to Azure VMs are stored as Virtual Hard Disk (VHD) files within an Azure storage account.

❑ Azure Disks are designed for 99.999% availability.

❑ You have three replicas of your data that enables high durability.

❑ Azure Disks have consistently delivered enterprise-grade durability, with an industry-leading 0% annualized failure rate.

❑ There are two performance tiers for storage you can choose from when creating your:

- Standard Storage is backed by HDDs.

Standard Storage

- Premium Storage is backed by SSDs and delivers high-performance, low-latency disk support for VMs running IO-intensive workloads.
- Premium offers a higher pricing level.

Premium Storage

Azure VM:
Standard Vs. Premium Disks

Category	Azure Premium Disk	Azure Standard Disk
Disk Type	Solid State Drives (SSDs)	Hard Disk Drives (HDDs)
Overview	SSD-based high-performance, low-latency disk support for VMs running IO-intensive workloads or hosting mission critical production environment	HDD-based cost-effective disk support for Dev/Test VM scenarios
Scenario	Production and performance sensitive workloads	Dev/Test, non-critical, infrequent access
Disk Type	Managed disks only	Unmanaged and managed disks
Max. Throughput per Disk	250 MB/s	60 MB/s
Max. IOPS per Disk	7500 IOPS	500 IOPS

Azure VM: Disks Storage

❑ Virtual machines in Azure use disks as a place to store an operating system, applications, and data.

❑ The operating system disk is created from an image, and both the operating system disk and the image are virtual hard disks (VHDs) stored in an Azure storage account.

❑ All Azure virtual machines have at least two disks:

- Operating system disk

- Temporary disk

❑ The temporary storage provided with each VM has no extra cost associated with it for storage space as well as for transactions.

❑ If the data on the temporary drive is lost, when you resize the VM, shutdown or restart your VM moved to a different host server.

❑ During a standard reboot of the VM, the data on the temporary drive should persist.

Azure VM:

Disks Used by VMs

Azure VM supports three types of disks:

Operating system disk
- One per VM
- It is labeled as, C: drive for Windows and /dev/sda for Linux by default
- This disk has a maximum capacity of 2048 gigabytes (GB)

Temporary disk
- One per VM
- The size varies depending on the tier size used
- Provides a temporary, non-persistent storage
- It is labeled as, D: drive for Windows and /dev/sdb for Linux

Data disk
- Maximum number of disks is determined by the size of the VM
- Each data disk has a maximum capacity of 4095 GB
- Provides a persistent storage for applications and data

The operating system and data disks are implemented as **blob storage in a storage account.**

The temporary disk is implemented as **local storage on the host where the VM is running.**

Azure VM:
Unmanaged Vs. Managed Disks

Unmanaged Disks

- You must create Azure storage accounts where Azure VM disks will reside.
- The maximum number of Azure storage accounts per region is limited to 200.
- When using standard storage with unmanaged disks, you pay only for the space you use.

Managed Disks

- The Azure platform controls the placement of VM disk files.
- The limit on the number of storage accounts no longer applies; there is a limit of 10,000 managed disks per region.
- With managed disks, you pay for the full capacity of a disk, regardless of the disk space that is in use.

Azure VM: Images

❑ You can use images to create Azure virtual machines.

❑ You can capture images from on-premises virtual machines, or you can use pre-built images from the Azure Marketplace.

❑ The Marketplace contains basic operating-system images and images that are built to provide a specific purpose.

❑ The Marketplace contains hundreds of images in the following categories:

Microsoft Windows Server	Linux Distributions	Database Servers	Application Servers

Azure VM:
Image Type

❑ VHD files in an Azure storage account represent one of two object types:

Images	Disks

❑ Images serve as templates from which you can create new disks during the provisioning of new virtual machines.

❑ There are two types of images:

Operating System Images	VM Images
• Represent a single disk containing a generalized installation of the Windows or Linux operating system.	• Refer to an image that contains all disks attached to a VM during its capture.

Azure VM: Custom Image

❑ You can reuse Azure virtual machines that you configure to deploy images as new Azure virtual machines.

❑ This process saves time when you are configuring new virtual machines by reusing a configuration that exists already within an Azure virtual machine.

❑ To create an image of a virtual machine, you need to:

▪ Generalize the Windows VM using Sysprep

  o Sysprep removes all your personal account information, among other things, and prepares the machine to be used as an image.

Azure VM: Resource Group

❑ All resources in your group should share the same life cycle. You deploy, update, and delete them together.

❑ Each resource can only exist in one resource group.

❑ You can add or remove a resource to or from a resource group at any time.

❑ You can move a resource from one resource group to another group.

❑ A resource group can contain resources that reside in different regions.

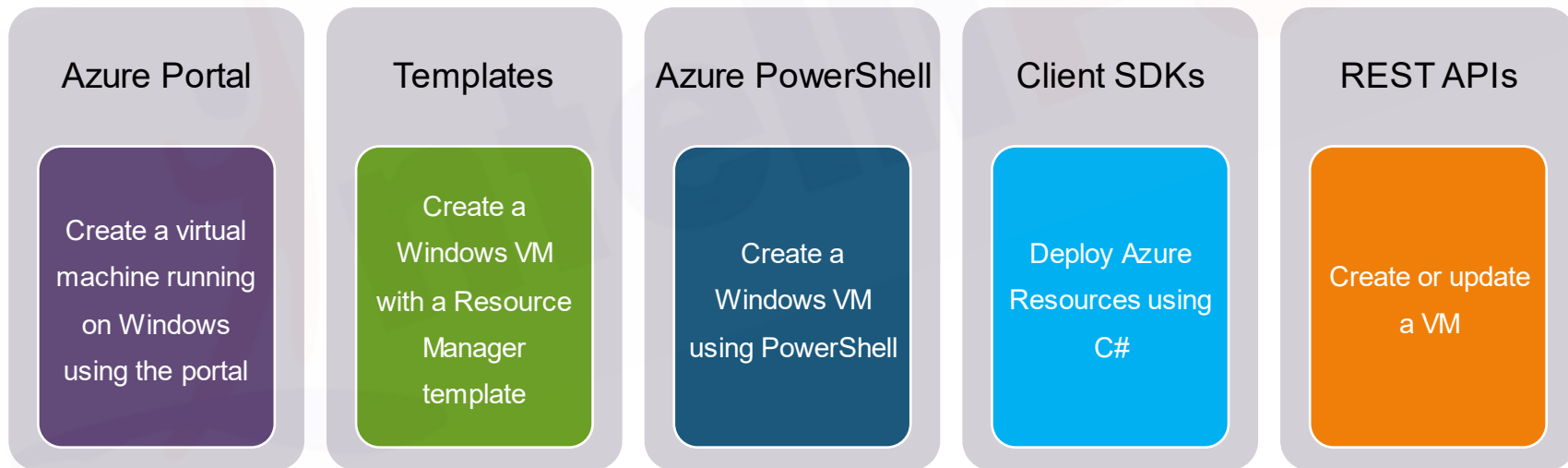❑A resource group can be used to scope access control for administrative actions.

A resource can interact with resources in other resource groups.

When creating a resource group, you need to provide a location for that resource group.

Azure VM:

How Do I Create My First VM?

❑ You have several choices for creating your VM.

❑ The choice that you make depends on the environment you are in.

Azure Portal	Templates	Azure PowerShell	Client SDKs	REST APIs
Create a virtual machine running on Windows using the portal	Create a Windows VM with a Resource Manager template	Create a Windows VM using PowerShell	Deploy Azure Resources using C#	Create or update a VM

Azure VM:
Network Interfaces

❑ A network interface (NIC) is the interconnection between a VM and a virtual network (VNet).

❑ A VM must have at least one NIC but can have more than one, depending on the size of the VM you create.

❑ Each NIC attached to a VM must exist in the same location and subscription as the VM.

❑ You can change the subnet a VM is connected to after it's created, but you cannot change the VNet.

❑ You can assign these types of IP addresses to an NIC in Azure:

Public IP addresses

Private IP addresses

Azure VM:
Network Security Groups

❑ A network security group (NSG) contains a list of access control list (ACL) rules that allow or deny network traffic to subnets, NICs, or both.

❑ NSGs can be associated with either subnets or individual NICs connected to a subnet.

❑ When an NSG is associated with a subnet, ACL rules apply to all VMs in that subnet.

❑ In addition, traffic to an individual NIC can be restricted by associating an NSG directly to an NIC.

❑ NSGs contain two sets of rules: inbound and outbound.

❑ The priority for a rule must be unique within each set.

❑ Each rule has properties of protocol, source and destination port ranges, address prefixes, direction of traffic, priority, and access type.

Azure VM: Resizing

❏ One of the great benefits of Azure VMs is the ability to change the size of your VM based on resources.

❏ Consider the following, when planning to resize virtual machines:

  ❏ The region in which your VM is deployed. Different VM sizes require different physical hardware.

  ❏ In some instances, an Azure region may not contain the hardware required to support the desired VM size.

❏ If the VM size you desire to use is not available in your current region, then your options are either to wait for the size to become available in the region or to move the VM, and possibly other services, to a new region.

Azure VM: Snapshots

❑ A managed snapshot is a read-only full copy of a managed disk which is stored as a standard managed disk.

❑ With snapshots, you can back up your managed disks at any point in time.

❑ These snapshots exist independent of the source disk and can be used to create new managed disks.

❑ They are billed based on the used size.

For example, if you create a snapshot of a managed disk with provisioned capacity of 64 GB and actual used data size of 10 GB, the snapshot will be billed only for the used data size of 10 GB.

Azure VM:
Converting Disk Storage

❑ It allows you to easily switch between two options with minimal downtime based on your performance needs.

❑ This capability is not available for unmanaged disks.

Managed disks offer two storage options

Premium (SSD-based)

Standard (HDD-based)
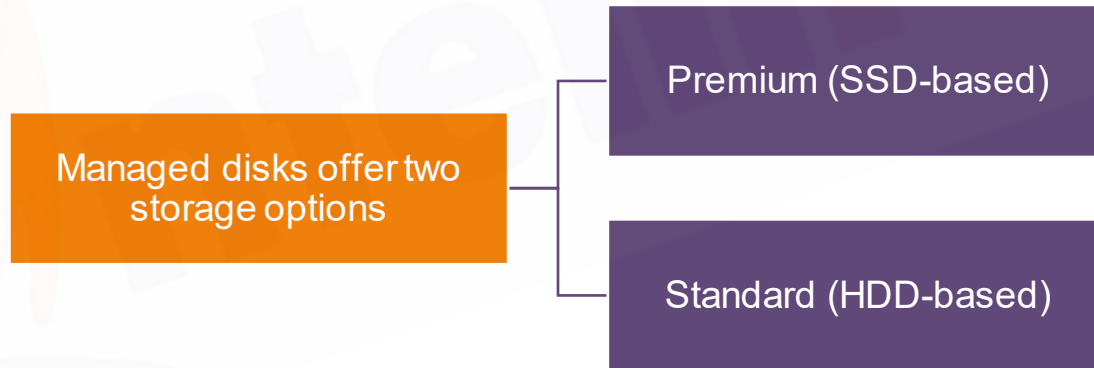
Automating the Deployment of VMs

Automating the Deployment of VMs

❑   For updating a resource in an ARM template, you can use the following **GitHub** link:

https://github.com/mspnp/template-examples

Create a Windows VM from a specialized disk by using PowerShell

Before you begin

❑ To use PowerShell, make sure that you have the latest version of the AzureRM.Compute PowerShell module.

```
PowerShell                                          Copy

Install-Module AzureRM -RequiredVersion 6.0.0
```

Option 1:
• Use an existing disk

Option 2:
• Upload a specialized VHD, upload the VHD to your storage account, and create a managed disk from the VHD

Option 3:
• Copy an existing Azure VM and create a new disk from the snapshot, then **create** the new VM with the subnet and virtual network, security group, public IP address, etc. Next step is to select the name, size, and OS, and now you're good to go

Automating the Deployment of VMs

Create a Windows virtual machine from a Resource Manager template

Launch the Azure Cloud Shell

Create a resource group; all resources must be deployed in a resource group	Get a list of available locations where resources can be created	Create the resource group in the location that you select. This example shows the creation of a resource group named **myResourceGroup** in the **West US** location

Create files

In this step, you create a template file that deploys the resources and a parameters file that supplies parameter values to the template. You also create an authorization file that is used to perform ARM operations	Create a file named *CreateVMTemplate.json* and add your JSON code to it. Replace the value of *domainNameLabel* with your own unique name	Create a file named *Parameters.json* and add this JSON code to it	Create a new storage account and container	Upload the files to the storage account

Then simply create the resource by deploying the template

Automating the Deployment of VMs: Downloading the Template for a VM

Download the template using the portal

Log in to the Azure portal	From the left menu, select **Virtual Machines**	Select a virtual machine from the list	Select **Automation script**	Select **Download** from the menu at the top and save the .zip file to your local computer

Open the .zip file and **Extract** the files to a folder. The **.zip file** contains:

- **deploy.ps1**
- **deploy.sh**
- **deployer.rb**
- **DeploymentHelper.cs**
- **parameters.json**
- **template.json**

The template.json file is the template.

Automating the Deployment of VMs: Downloading the Template for a VM

Download the template using PowerShell

You can also download the .json template file using the Export-AzureRMResourceGroup cmdlet. You can use the -path parameter to provide the filename and path for the .json file.

```
Export-AzureRmResourceGroup -ResourceGroupName "myResourceGroup" -Path "C:\users\public\downloads"
```

Automating the Deployment of VMs: Windows VM Using Azure Portal

Create a Virtual Machine

1.Choose **Create** a resource from the upper left-hand corner of the Azure portal	In the search box above the list of Azure Marketplace resources, search for and select Windows Server 2016 Datacenter, and then choose **Create**	In the Basics tab, under Project details, make sure the correct subscription is selected and then choose **Create** new resource group. Type *myResourceGroup* for the name	Under **Instance details**, type *myVM* for the **Virtual machine name** and choose *East US* for your **Location**. Leave the other defaults

Under **Administrator account**, provide a username, such as *azureuser* and a password. The password must be at least 12 characters long	Under **Inbound port rules**, choose **Allow selected ports** and then select **RDP (3389)** and **HTTP** from the drop-down	Leave the remaining defaults and then select the **Review + create** button at the bottom of the page

Connect to virtual machine and then install the web server and view the IIS welcome page.
After this, clean up the resources

Automating the Deployment of VMs: Linux VM Using Azure Portal

Create SSH key pair

Open a bash shell and use SSH-keygen to create an SSH key pair. If you don't have a bash shell on your local computer, you can use the Azure Cloud Shell

`ssh-keygen -t rsa -b 2048`

This command generates public and private keys with the default name of *id_rsa* in the *~/.ssh* directory. The command returns the full path to the public key. Use the path to the public key to display its contents with *cat*

`cat ~/.ssh/id_rsa.pub`

Save the output of this command. You will need it when configuring your administrator account to log in to your VM

If you create your SSH key pair using the Cloud Shell, it will be stored in an Azure File Share that is automatically mounted by the Cloud Shell. Don't delete this file share or storage account until you retrieve your keys, otherwise you will lose access to the VM

After this, simply sign in to the Azure portal, create the VM following the previous steps, connect to the VM by creating SSH connection, install the web server, and view the web server in action

Then clean up the resources

Azure VM: Pricing

Pay-as-you-go

- Pay for compute capacity per second

- Increase or decrease compute capacity on demand

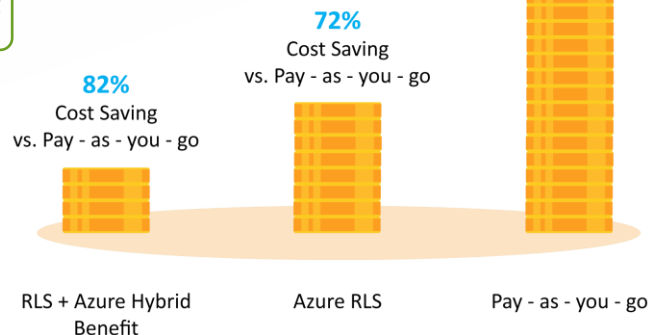- Start or stop at any time and only pay for what you use

Reserved Virtual Machine Instances

- Advanced purchase for one or three years in a specified region

- You get up to 72% price savings compared to the pay-as-you-go pricing

Azure Hybrid

- Use your on-premises Windows Server licenses to save big on Azure, while you just pay for base compute costs

82%
Cost Saving
vs. Pay - as - you - go

72%
Cost Saving
vs. Pay - as - you - go

RLS + Azure Hybrid Benefit

Azure RLS

Pay - as - you - go

Hands-on

Hands-on

- ❑ Create a virtual machine
    - ❑ Connect the virtual machine
    - ❑ Install a web server
- ❑ Create a customized OS image
    - ❑ Launch a new VM using the customized image
- ❑ Convert the dynamic IP address to static IP address
- ❑ Create an additional NIC
    - ❑ Assign the second NIC to the VM
- ❑ Create and manage VM disks
- ❑ Create a snapshot of the disk
- ❑ Resize a virtual machine
- ❑ Delete a resource group
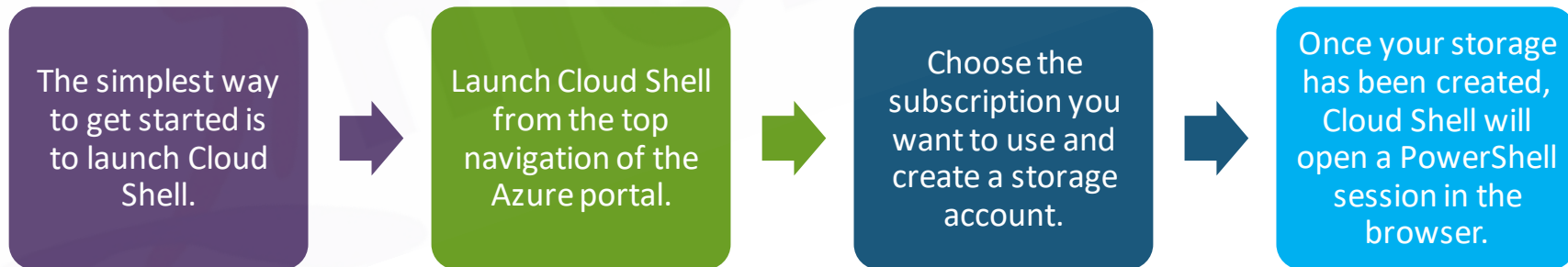
Azure PowerShell

What Is Azure PowerShell?

❑ Azure PowerShell provides a set of cmdlets that use the ARM model for

managing your Azure resources.

❑ You can use it in your browser with Azure Cloud Shell, or you can install it

on your local machine and use it in any PowerShell session.

❑ Use the Cloud Shell to run the Azure PowerShell in your browser,

or install it on own computer.

Azure PowerShell: Cloud Shell

❑ Azure PowerShell is designed for managing and administering Azure resources from the command line and for building automation scripts that work against the ARM.

❑ You can use it in your browser with Azure Cloud Shell, or you can install it on your local machine and use it in any PowerShell session.

❑ **Connect**

| The simplest way to get started is to launch Cloud Shell. | → | Launch Cloud Shell from the top navigation of the Azure portal. | → | Choose the subscription you want to use and create a storage account. | → | Once your storage has been created, Cloud Shell will open a PowerShell session in the browser. |

Hands-on

Azure PowerShell:

Creating a Resource Group

❑ Create a resource group named "MyResourceGroup" in the "westeurope" region of Azure

❑ To do so, type the following command:

New-AzureRmResourceGroup -Name 'myResourceGroup' -Location 'westeurope'

```
PowerShell

New-AzureRmResourceGroup -Name 'myResourceGroup' -Location 'westeurope'
```

```
Output

ResourceGroupName : myResourceGroup
Location          : westeurope
ProvisioningState : Succeeded
Tags              :
ResourceId        : /subscriptions/XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX/resourceGroups/myResourceGroup
```

Azure PowerShell:
Creating Network Resources

First, we need to create a subnet configuration to be used with the virtual network creation process.

We also create a public IP address so that we can connect to this VM.

We create a network security group to secure access to the public address.

Finally, we create the virtual NIC using all of the previous resources.

```powershell
PowerShell

# Variables for common values
$resourceGroup = "myResourceGroup"
$location = "westeurope"
$vmName = "myWindowsVM"

# Create a subnet configuration
$subnetConfig = New-AzureRmVirtualNetworkSubnetConfig -Name mySubnet1 -AddressPrefix 192.168.1.0/24

# Create a virtual network
$vnet = New-AzureRmVirtualNetwork -ResourceGroupName $resourceGroup -Location $location `
    -Name MYvNET1 -AddressPrefix 192.168.0.0/16 -Subnet $subnetConfig

# Create a public IP address and specify a DNS name
$publicIp = New-AzureRmPublicIpAddress -ResourceGroupName $resourceGroup -Location $location `
    -Name "mypublicdns$(Get-Random)" -AllocationMethod Static -IdleTimeoutInMinutes 4
$publicIp | Select-Object Name,IpAddress

# Create an inbound network security group rule for port 3389
$nsgRuleRDP = New-AzureRmNetworkSecurityRuleConfig -Name myNetworkSecurityGroupRuleRDP  -Protocol Tcp `
    -Direction Inbound -Priority 1000 -SourceAddressPrefix * -SourcePortRange * -DestinationAddressPrefix * `
    -DestinationPortRange 3389 -Access Allow

# Create a network security group
$nsg = New-AzureRmNetworkSecurityGroup -ResourceGroupName $resourceGroup -Location $location `
    -Name myNetworkSecurityGroup1 -SecurityRules $nsgRuleRDP

# Create a virtual network card and associate with public IP address and NSG
$nic = New-AzureRmNetworkInterface -Name myNic1 -ResourceGroupName $resourceGroup -Location $location `
    -SubnetId $vnet.Subnets[0].Id -PublicIpAddressId $publicIp.Id -NetworkSecurityGroupId $nsg.Id
```

Azure PowerShell:
Creating a Virtual Machine

❑ First, we need a set of credentials for the OS.

```
PowerShell

# Create user object
$cred = Get-Credential -Message "Enter a username and password for the virtual machine."
```

❑ Now that we have the required resources, we can create the VM.

❑ For this step, we create a VM configuration object; then, we use the configuration to create the VM.

```
PowerShell

# Create a virtual machine configuration
$vmConfig = New-AzureRmVMConfig -VMName $vmName -VMSize Standard_D1 |
    Set-AzureRmVMOperatingSystem -Windows -ComputerName $vmName -Credential $cred |
    Set-AzureRmVMSourceImage -PublisherName MicrosoftWindowsServer -Offer WindowsServer -Skus 2016-Datacenter -Vers
    Add-AzureRmVMNetworkInterface -Id $nic.Id

# Create a virtual machine
New-AzureRmVM -ResourceGroupName $resourceGroup -Location $location -VM $vmConfig
```

Azure PowerShell: Samples

Azure Virtual Machine PowerShell samples

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/powershell-samples?toc=%2Fpowershell%2Fazure%25%2Ftoc.json

Azure PowerShell:
Tutorial

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/tutorial-manage-vm

Azure Monitoring

What Is Azure Monitoring?

❑ Azure Monitor is the platform service that provides a single source for monitoring Azure resources.

❑ Azure Monitor provides base-level infrastructure metrics and logs for most services in Microsoft Azure.

❑ Azure Monitor makes metrics available for many Azure resources.

❑ These metrics convey the performance and health of those resources.

❑ In many cases, metric values can point to something being wrong with a resource.

❑ You can create metric alerts to monitor abnormal behavior and be notified if it occurs.

Azure Monitoring: Monitoring Azure Environment

There are a range of tools for monitoring that works together to offer comprehensive monitoring and includes:

Azure Monitor

- It gives you access to performance metrics and events that describe the operation of the Azure infrastructure.

Application Insights

- It is an Azure service that offers application performance monitoring and user analytics.

Log Analytics

- It provides rich tools to analyze data across sources, allows complex queries across all logs, and can proactively alert us on specified conditions.
- You can even collect custom data into its central repository so that you can query and visualize it.

Azure Monitoring: Metrics

❑ Azure Monitor enables you to consume telemetry to get into the performance and health of your workloads.

❑ The most important type of Azure telemetry data is metrics (also called performance counters).

❑ Metrics are a valuable source of telemetry and enable you to do the following tasks:

Track the performance of your resource	Get notified of an issue that impacts the performance of your resource	Configure automated actions, such as autoscaling a resource or firing a runbook	Perform advanced analytics or reporting on performance or usage trends of your resource	Archive the performance or health history of your resource for compliance or auditing purposes

Azure Monitoring: Characteristics of Metrics

Metrics have the following characteristics:

✔ All metrics have one-minute frequency.

✔ You receive a metric value every minute from your resource, giving you near real-time visibility.

✔ Metrics are available immediately.

✔ You can access 30 days of history for each metric.

✔ Some metrics can have name–value pair attributes called dimensions.

✔ These enable you to further segment and explore a metric in a more meaningful way.

Azure Monitoring: Alerts

❑ Alerts offer a method of monitoring in Azure that allows you to configure conditions over data and become notified when the conditions match the latest monitoring data.

❑ Azure uses the following terms to describe alerts and their functions:

Alert	Active	Resolved	Notification	Action
• A definition of criteria (one or more rules or conditions) that becomes activated when met	• The state when the criteria defined by an alert are met	• The state when the criteria defined by an alert are no longer met after previously having been met	• The action taken based on an alert becoming active	• A specific call sent to a receiver of a notification (e.g., emailing an address or posting to a webhook URL). Notifications can usually trigger multiple actions

Azure Monitoring: Activity Log

❑ The Azure Activity Log provides insights into subscription-level events that have occurred in Azure.

❑ This includes a range of data, from Azure Resource Manager operational data to updates on Service Health events.

❑ Using the Activity Log, you can determine the 'what, who, and when' for any write operations in your subscription.

❑ You can retrieve events from your Activity Log using the Azure portal, CLI, PowerShell cmdlets, and Azure Monitor REST API.

❑ You can use the activity logs to find an error when troubleshooting or to monitor how a user in your organization modified a resource.

❑ Activity Logs are retained for 90 days.

❑ You can query for any range of dates, as long as the starting date is not more than 90 days in the past.

Azure Monitoring: Diagnostic Logs

❑ Azure resource-level diagnostic logs are logs emitted by a resource that provide rich, frequent data about the operation of that resource.

❑ Resource-level diagnostic logs differ from the Activity Log.

<table>
<tr>
<td>The Activity Log provides insights into the operations that were performed on resources in your subscription using Resource Manager, for example, creating a virtual machine or deleting a logic app.</td>
<td>While the Activity Log is a subscription-level log, resource-level diagnostic logs provide insights into operations that were performed within that resource itself, for example, getting a secret from a Key Vault.</td>
</tr>
</table>

❑ Resource-level diagnostic logs also differ from guest OS-level diagnostic logs.

❑ Guest OS-level diagnostic logs are those collected by an agent running inside of a virtual machine or other supported resource types.

Azure Monitoring: Action Groups

❑ You can configure a list of actions with action groups.

❑ These groups can be used when you define activity log alerts.

❑ These groups can then be reused by each activity log alert you define, ensuring that the same actions are taken each time the activity log alert is triggered.

❑ An action group can have up to 10 of each action type.

❑ Each action is made up of the following properties:

Name	Action type	Details
• A unique identifier within the action group	• Send an SMS, send an email, call a webhook, send data to an ITSM tool, call an Azure app, or run an Automation runbook	• The corresponding phone number, email address, webhook URI, or ITSM connection details

Azure Monitoring: Service Health Notification

❑ Service health notifications are published by Azure and contain information about resources.

❑ Service health notifications can be informational or actionable, depending on the class.

❑ There are various classes of service health notifications:

Action required	Assisted recovery	Incident	Maintenance	Information	Security
• Azure might notice something unusual happening on your account and work with you to remedy this	• An event has occurred, and engineers have confirmed that you are still experiencing the impact. Azure engineering needs to work with you directly to restore your services to full health	• An event that impacts service is currently affecting one or more resources in your subscription	• A planned maintenance activity might that impact one or more resources under your subscription	• Potential optimizations that might help improve your resource use	• Urgent security-related information regarding your solutions that run on Azure

Azure Monitoring: SMS Alert

❑ Action groups enable you to configure a list of receivers.

❑ These groups can then be leveraged when defining activity log alerts, ensuring that a particular action group is notified when the activity log alert is triggered.

❑ One of the alerting mechanisms supported is SMS; the alerts support bi-directional communication.

❑ A user can respond to an alert to:

Unsubscribe from alerts	Re-subscribe to alerts	Request help
• A user can unsubscribe from all SMS alerts for all action groups or a singular action group.	• A user can re-subscribe to all SMS alerts for all action groups or a singular action group.	• A user can ask for more information on the SMS.

Hands-on

Hands-on

- ❏ Configure Monitoring

- ❏ Configure an Alert

- ❏ Get a Notification

- ❏ Review the Activity Log

- ❏ Review the Diagnostic Log

QUIZ

Quiz 1

Which service in Azure is used to manage resources in Azure?

| A | Application Insights |

| B | Azure Resource Manager |

| C | Azure Portal |

| D | Log Analytics |

Answer 1

Which service in Azure is used to manage resources in Azure?

A	Application Insights
B	Azure Resource Manager
C	Azure Portal
D	Log Analytics

Quiz 2

What are Virtual Machine scale sets in Azure?

A Azure compute resource that can be used to deploy and manage a set of identical VMs.

B Azure compute resource that can be used for deploying and manage the new VMs created

C Azure compute resource that can be used for deploying and manage the already existing VMs

D Azure compute resource which is used for scaling up and down the instances based on the requirements

Answer 2

What are Virtual Machine scale sets in Azure?

A   Azure compute resource that can be used to deploy and manage a set of identical VMs.

B   Azure compute resource that can be used for deploying and manage the new VMs created

C   Azure compute resource that can be used for deploying and manage the already existing VMs

D   Azure compute resource which is used for scaling up and down the instances based on the requirements

Quiz 3

Can we add the existing VM to an Availability Set?

A Yes

B No

Answer 3

Can we add the existing VM to an Availability Set?

A Yes

B No

Quiz 4

How much storage can you use with a Virtual Machine?

A	10GB

B	1GB

C	100MB

D	1TB

Answer 4

How much storage can you use with a Virtual Machine?

A	10GB

B	1GB

C	100MB

D	1TB

Quiz 5

Which is the right command to create a VM in Azure CLI?

A   az vm create ` --resource-group myResourceGroup ` --name myVM --image win2016datacenter ` --admin-username azureuser ` --admin-password myPassword12

B   az create vm ` --name myVM --image win2016datacenter ` --admin-username azureuser ` --admin-password myPassword12

C   az vm `--resource-group myResourceGroup ` --name myVM --image win2016datacenter

D   **vm create ` --resource-group myResourceGroup ` --name myVM --image win2016datacenter ` --admin-username azureuser ` --admin-password myPassword12**

Answer 5

Which is the right command to create a VM in Azure CLI?

A
az vm create ` --resource-group myResourceGroup ` --name myVM --image win2016datacenter ` --admin-username azureuser ` --admin-password myPassword12

B
az create vm ` --name myVM --image win2016datacenter ` --admin-username azureuser ` --admin-password myPassword12

C
az vm `--resource-group myResourceGroup ` --name myVM --image win2016datacenter

D
vm create ` --resource-group myResourceGroup ` --name myVM --image win2016datacenter ` --admin-username azureuser ` --admin-password myPassword12

Quiz 6

What do we use in order to Automate the deployment of VM?

A   Azure VM

B   Azure Blob Storage

C   Azure PowerShell

D   **Azure CloudShell**

Answer 6

What do we use in order to Automate the deployment of VM?

A   Azure VM

B   Azure Blob Storage

C   Azure PowerShell

D   **Azure CloudShell**

Quiz 7

IntelliPaat

Which template we used to create a Windows Virtual Machine?

A	Azure Powershell Template

B	Azure Content delivery Template

C	Azure Site Recovery Template

D	Azure Resource Manager Template

Answer 7

Which template we used to create a Windows Virtual Machine?

A	Azure Powershell Template

B	Azure Content delivery Template

C	Azure Site Recovery Template

D	Azure Resource Manager Template

India: +91-7847955955

US: 1-800-216-8930 (TOLL FREE)

sales@intellipaat.com

24/7 Chat with Our Course Advisor