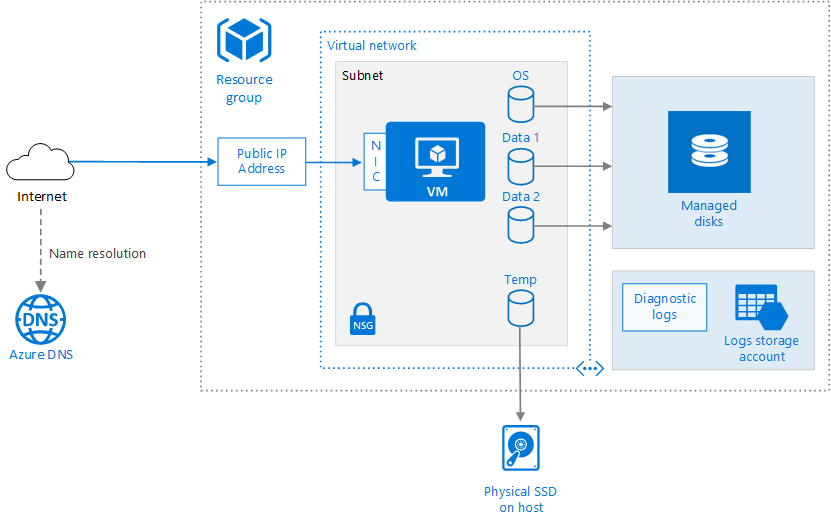
**Agenda:** **Azure Virtual Machine**

* Introduction
* Create a Windows Virtual Machine using Portal / PowerShell / ARM Templates
* Deploy popular application frameworks by using Azure Resource Manager templates
* Virtual Machine Disk
* Convert Unmanaged Disk to Managed Disk
* Generalizing VM and Capture VM Images
* Upload an on-premise VHD to Storage Account and attach to VM as Data Disk
* Working with Disk Snapshot
* VM Disk Types
* VM Sizes in Azure
* Configuring VM Disk Encryption
* Perform configuration management
* Virtual Machine Scale Sets

**Virtual Machine Introduction**



Different ways to create a Windows VM with Azure Resource Manager (ARM)

1. Azure Portal
2. Azure PowerShell
3. Azure CLI
4. ARM Template

**Creating a VM using Azure portal:**

The Management Portal provides many **images** and scripting tools that help you to create new virtual machines in Azure. The template images that are available in the portal are created and fully supported by either Microsoft or an authorized third-party.

Provisioning VMs to Azure requires planning. Before you create a single VM be sure you have thought about the following:

* Start with the network
* Name the VM
* Decide the location for the VM
* Determine the size of the VM
* Understanding the pricing model
* Storage for the VM
* Select an operating system

**Walkthrough:**

1. Azure portal 🡪 On the Hub menu, click New 🡪 Compute 🡪 Windows Server 2016 Datacenter.

Note: To find additional images, click **Marketplace** and then search or filter for available items.

1. On the **Windows Server 2012 R2 Datacenter** page, under **Select a deployment model** = **Resource Manager** 🡪 **Create**.
2. **Create virtual machine** blade 🡪
   * **Basics 🡪 provide values for Name, Username and Password, Resource Group 🡪 OK**
   * **Size** 🡪 Select an appropriate virtual machine size for your needs. Note that Azure recommends certain sizes automatically depending on the image you choose.
   * **Settings** to see storage and networking settings for the new virtual machine. For a first virtual machine you can generally accept the default settings.
   * Click **Summary** to review your configuration choices.
3. Click Create

**Generation1 vs Generation2 VM**

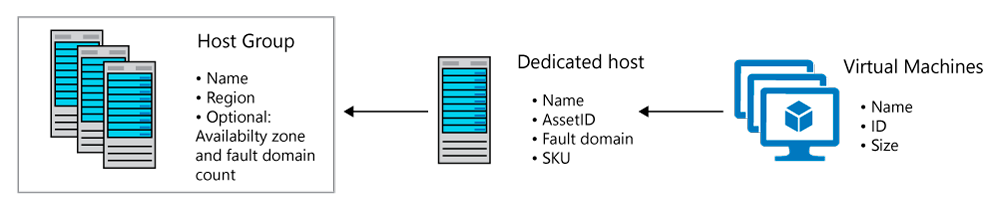
<https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/plan/should-i-create-a-generation-1-or-2-virtual-machine-in-hyper-v>

**Azure Dedicated Hosts**

* Implement hardware isolation at the physical server level.
* Control impact of maintenance events initiated by the Azure platform.

**To deploy highly available VMs to dedicated hosts:**

* Create one or more host groups
* Create one or more hosts in each group
* Create a VM on each host



**Quotas**

* Limit vCPUs for dedicated hosts per region
* Support quota increase

**Pricing**

* Per dedicated host (regardless of the number of deployed VMs)
* Based on VM family, type, and region.

**Shebang Script to Install NGINX on Ubuntu**

#!/bin/bash

wget http://nginx.org/keys/nginx\_signing.key

apt-key add nginx\_signing.key

apt-get update

apt-get install nginx -y

systemctl start nginx

**Virtual Machine Disk Types**

1. **Premium SSD**: Azure Premium Storage delivers **high-performance, low-latency** disk support for virtual machines (VMs) with **input/output (I/O)-intensive** workloads. Best suitable to run performance-intensive workloads in applications like Dynamics CRM, Exchange Server, SAP, SharePoint, SQL Server, Oracle, Redis, which require **consistent** high performance and low latency.
2. **Standard SSD**: A **cost-effective** storage option optimized for workloads that need **consistent performance** at **lower IOPS** levels. Standard SSDs deliver **better** **availability**, **consistency**, **reliability** and **latency** compared to HDD Disks, and are suitable for Web servers, low IOPS application servers, lightly used enterprise applications, and Dev/Test workloads.
3. **Standard HDD:** For development and testing purpose. Also can be used for Backup.

Just like any other computer, virtual machines in Azure uses disks as a place to store an operating system, applications, and data.

**All Azure virtual machines have following disks:**

1. Operating System Disk
2. Temporary Disk.
3. Optional: One or more data disks.

#### Machine generated alternative text: Overview of virtual machine disksr(Contents can be¡est)Data disksIC:\Oper.?’iq Syst.m1D:\Diskrary diskF:\ etc.An:. L

**Steps to Add a Disk to VM:**

### Demo-vm 🡪 Disks 🡪 click **Create and attach a new disk**

### Name: 01-DATADISK1

### Type: HDD

### Size (GiB): 32

### Location: <Select your storage account>

### Host caching: Read/write

### Save

### A screenshot of a computer Description automatically generated

## **Initialize a new data disk**

1. RDP to **Demo=vm** 🡪 Windows Start 🡪 Search **Run** 🡪 **diskmgmt.msc** (Disk Management snap-in).
2. Disk Management will recognize that you have a new, un-initialized disk and the Initialize Disk window will pop up.
3. Make sure the new disk is selected and click **OK** to initialize it.
4. The new disk will now appear as **unallocated**. Right-click anywhere on the disk and select **New simple volume**. The **New Simple Volume Wizard** will start.
5. Go through the wizard, keeping all of the defaults, when you are done select **Finish**.
6. Close Disk Management.
7. ~~You will get a pop-up that you need to format the new disk before you can use it. Click~~ **~~Format disk~~**~~.~~
8. ~~In the~~ **~~Format new disk~~** ~~dialog, check the settings and then click~~ **~~Start~~**~~.~~
9. ~~You will get a warning that formatting the disks will erase all of the data, click~~ **~~OK~~**~~.~~
10. ~~When the format is complete, click~~ **~~OK~~**~~.~~
11. **Go to Windows Explorer 🡪 Verify that a new Drive Letter is created**

### **Configuring VM Disk Encryption**

* You need to demonstrate to your trading partners that data stored on your Azure VMs cannot be accessed by unauthorized users, devices, or applications.

#### **Key management:** In Azure, your encryption keys can be **managed by Microsoft or the customer**. Often the demand for customer-managed keys comes from organizations that need to demonstrate compliance with HIPAA, or other regulations. Such compliance may require that access to keys is logged, and that regular key changes are made and recorded.

#### **Azure disk encryption technologies**

The main encryption-based disk protection technologies for Azure VMs are

##### **Storage Service Encryption (SSE)**

##### Azure Storage Service Encryption (SSE) is an encryption service built into Azure used to **protect data at rest**.

##### It cannot be disabled.

##### The Azure storage platform automatically encrypts data before it's stored to several storage services, including Azure Managed Disks.

##### Encryption is enabled by default using **256-bit AES** encryption, and is managed by **the storage account administrator**.

##### There is be **no noticeable performance impact** on the VM disk IO when using SSE.

To use Customer Managed Key for Encryption: **Select the Disk 🡪 Encryption 🡪 Provide reference of Key from KeyVault**

Note:

* Please grant **get, wrap** and **unwrap** key permissions to **disk encryption set** 'MyDemo-encryptionSet'
* The key vault 'dssdemo-keyValult' used for disk encryption set 'MyDemo-encryptionSet' must have **purge protection enabled**.

##### **Azure Disk Encryption (ADE)**

* **Azure Disk Encryption** is a capability built into the Azure platform that allows you to **encrypt file system of volumes** residing on Windows and Linux virtual machine disks.

##### Azure Disk Encryption (ADE) is **managed by the VM owner**. **VMs boot under customer-controlled keys and policies.**

##### Bring your own encryption (BYOE) and bring your own key (BYOK) scenarios, in which the customers use their own encryption keys and store them in an **Azure key vault.**

##### It controls the encryption of Windows and Linux VM-controlled disks, using **BitLocker** on Windows VMs and **DM-Crypt** on Linux VMs.

* ADE makes use of VM operating system tools (BitLocker and DM-Crypt), so the VM itself has to **do some work** when encryption or decryption on VM disks is being performed. The impact of this additional VM CPU activity is typically **negligible**, except in certain situations. For instance, if you have a **CPU-intensive application**, there may be a case for leaving the OS disk **unencrypted** to **maximize performance**. In a situation such as this, you can store application data on a separate **encrypted data disk**, getting you the performance you need without compromising security.
* ADE is required for VMs backed up to the Recovery Vault.

**Step1: Create a Key Vault Resource**

1. Search Key vault 🡪 +Create
2. Basics Tab

A screenshot of a computer screen

Description automatically generated

1. Access configuration Tab

A screenshot of a computer

Description automatically generated

1. Review + Create 🡪 create
2. **OPTIONAL**: Select **Sandeep-Demo-keyvault** 🡪 Access control (IAM) 🡪 + Add 🡪 Add role assignment
   * Select **Key Vault Administrator** 🡪 Next

A screenshot of a computer

Description automatically generated

* + + Select members 🡪 search your <Username> 🡪 Select 🡪 Select

A screenshot of a computer

Description automatically generated

* + Review + assign

**Step2: Encrypting Disk using ADE**

The first time you encrypt a Windows VM, you can choose to encrypt either all disks or the OS disk only. On some Linux distributions, only the data disks may be encrypted. To be eligible for encryption, your Windows disks must be formatted as NTFS volumes.

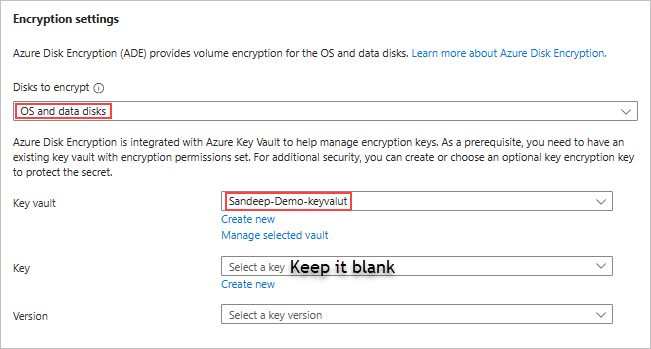
1. Verify that the disk is only SSE with PMK

Demo-vm 🡪 Disks

A screenshot of a computer

Description automatically generated

1. Demo-vm 🡪 Disks 🡪 **Additional Settings**



1. Verify that the disk is encrypted: Demo-vm 🡪 Disks 🡪

A screenshot of a computer

Description automatically generated

## **Working with Disk Snapshot**

### Snapshot can be created from Managed Disk and after creating the snapshot we can delete the managed disk and as snapshot can exist without Managed disk it is called as **Independent Snapshot**

### **Benefits of Snapshot**

### Snapshot can be copied onto another storage account in a different region.

### Using Snapshot, we can restore our VM to a **Point-In-Time** by creating a Managed Disk from snapshot.

### 

### **Create Snapshot**

### Search Disks 🡪 Select OS Disk 🡪 **+ Create snapshot**

### A screenshot of a project Description automatically generated

### Review + Create 🡪 Create

### **Create a New Managed Disk from the snapshot**

### Select **Demo-vm-os-disk-shaphot** 🡪 + Create disk

### Disk name = Demo2-vm-os-disk

### Availability Zone = No infrastructure redundancy required

### Size = 128 GB / P10

### Review + create 🡪 Create

### A screenshot of a computer Description automatically generated

### **Use the Managed Disk to create a new VM if its an OS Disk.**

### Select Demo2-vm-os-disk 🡪 + Create VM

### Virtual machine name = Demo2-vm

### Licensing = Windows-Server

### Review + Create 🡪 Create

### **OR If the Managed disk is Data Disk, then attach to an existing VM.**

**Capture VM Images**

You can create your own custom virtual machine image in one of two ways:

1. If you're building an image from scratch by using Hyper-V, you first create a blank virtual disk, and then create a virtual machine with this disk. When you start the virtual machine, you install the operating system and any other additional software from source disks (typically DVDs) and other packages.
2. If you're customizing an image from Azure Marketplace, you build a virtual machine by using an existing image. The image provides the operating system and base functionality. You add your own software, operating system updates, and other packages as required.

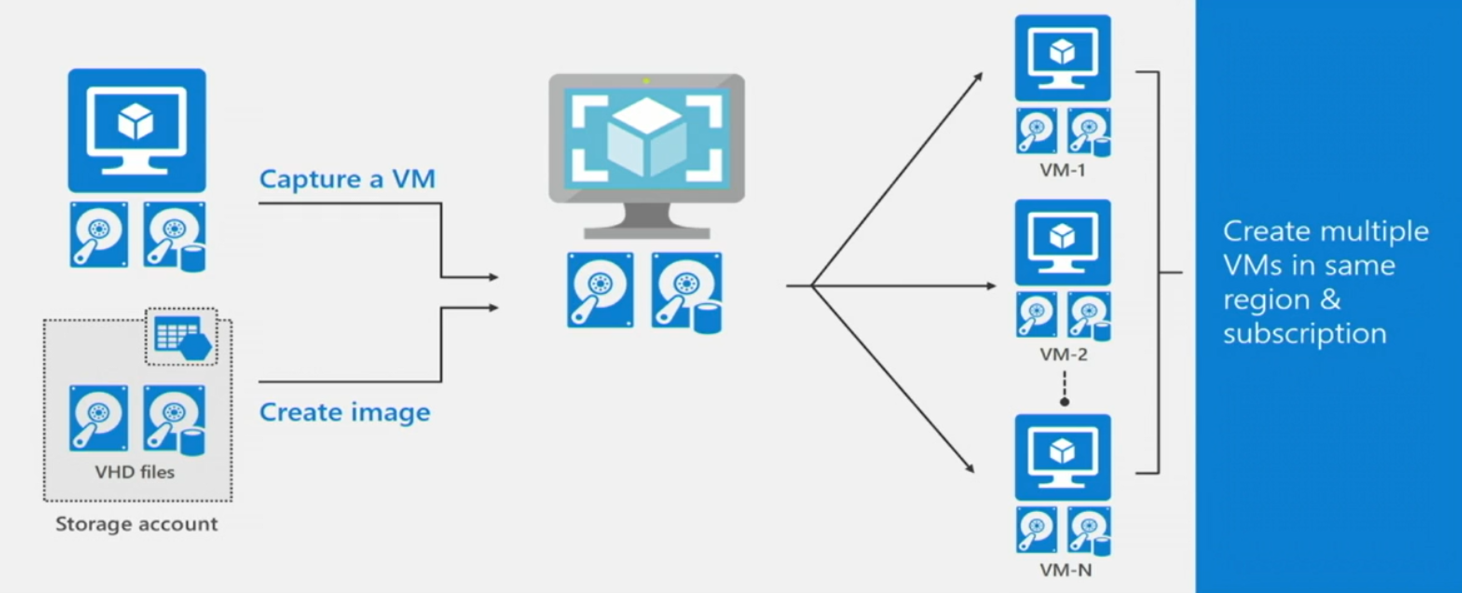
**What is a specialized virtual image?**

* A specialized virtual image is a copy of a live virtual machine after it has reached a specific state. For example, a specialized image might contain a copy of the configured operating system, software, user accounts, databases, connection information, and other data for your system.
* You can use a specialized virtual image as a backup of your system at a particular point in time. If you need to recover after a catastrophic failure, or you need to roll back the virtual machine, you can restore your virtual machine from this image.
* If you use a specialized image to create a new virtual machine, the new virtual machine will retain all of the data from the image. That data includes the host name, user accounts, and other settings.

**What is a generalized image?**

You want to turn the VM you have created into a template from which you can stamp out new cloned instances of the VM, each of them unique with respect to certain settings in the operating system. For example, to scale out a cluster, you add new instances of the template VMs, each of them similarly config­ured but uniquely identified. In this case, each instance has its own identity and is therefore slightly different. In fact, when you create VMs from images available in the Market­place, you utilize generalized images.

**Sysprep** is a process that you could run into a windows installation that will reset the installation of the system and will provide an “**out of the box experience**” by removing all personal data and resetting several components including RDP u/p or hostname.



**Step1: If ADE is enabled on the OS or Data Disk, disable the same.**

1. Demo-vm 🡪 Extension 🡪 uninstall **Azure Disk Encryption extension.**
2. RDP to VM 🡪 Search BitLocker and Disable Encryption

**Step2: Generalize the VM**

1. RDP into VM 🡪 Open Command prompt and execute the following commands
   * **Delelete folder c:\windows\Panther**
   * cd %windir%\system32\sysprep
   * sysprep.exe /oobe /generalize /shutdown
2. Next you need to set the status of the virtual machine to Generalized. Note that you will need to do this because the generalization step above (sysprep) does not do it in a way that Azure can understand.

Open Cloud Shell and execute the following command to Generalize the VM

* + Set-AzVm -ResourceGroupName Demo-rg -Name Demo-vm -Generalized

### **Step3: Capture a MANAGED Image in the Portal**

### Azure Portal 🡪 Select the VM 🡪 **Capture**

### Share image to Azure compute gallery = Yes

### **Check** Automatically delete this virtual machine after creating the image

### Target Azure compute gallery = Create new 🡪 DemoGallery 🡪 OK

### Target VM image definition = Create new 🡪

### DemoImage 🡪 OK

### Publisher = Sandeep

### Offer = Standard

### SKU = Basic

### OK

### A screenshot of a computer Description automatically generated

### Version number = 1.0.0

### A screenshot of a computer Description automatically generated

### Review + Create 🡪 Create

**Step4: Use the Managed Image to Create a New VM**

1. Select the New Image Created 🡪 Create VM

**Configuration Management using VM Extensions**

Microsoft offers a number of different methods that simplify and enhance management of both Windows and Linux operating systems hosted on Azure virtual machines.

In general, you can categorize management options for Azure VMs depending on the operating system support they provide.

Windows Management Options

* + RDP (Remote Desktop)

Linux Management Option

* + SSH (Secure Shell)

Cross Platform management options

* + Azure PowerShell
  + Azure CLI
  + **VM Agent and VM Extensions**

**VM Agents:**

* The VM Agent is a set of lightweight software components running within the operating system of an Azure VM. Their primary purpose is to load additional programs and services known as **VM Extensions**.
* The Azure VM agent is **pre-installed** on **Azure Marketplace** images and can be installed on supported operating systems.
* If the agent is not installed at provisioning time, or if you have migrated a **virtual hard disk from on-premises**, you can manually install the agent on these virtual machines by downloading and installing the agent from Microsoft at <http://go.microsoft.com/fwlink/?LinkID=394789&clcid=0x409>

**VM Extensions:**

* Azure virtual machine extensions are **small applications** that provide **post-deployment configuration** and automation tasks on Azure virtual machines. For example, if a virtual machine requires software installation, anti-virus protection, or Docker configuration, a VM extension can be used to complete these tasks.
* Extensions can be bundled with a new virtual machine deployment or run against any existing system.
* There are many Available VM extensions and some which are popular are:
  1. Access Extension
  2. Custom Script Extension
  3. Desired State Configuration
  4. Disk Encryption Extension.
  5. Backup Extension
  6. SqlServerExtension
  7. DiagnosticsExtension
* Azure VM extensions can be run by using
  1. Azure portal.
  2. PowerShell
  3. Azure CLI
  4. Azure Resource Manager templates

To see a list of al VM extensions, run the following PowerShell commands.

get-command Set-Az\*Extension\* -Module Az.Compute

**VM Access Extension:**

* Currently, the extension can only be enabled using the **Set-AzureVMAccessExtension** cmdlet.
* This cmdlet can reset the local administrator name, password, and also enable Remote Desktop access if it is accidently disabled.
* This extension does not work against Active Directory domain accounts or on domain controllers.

Set-AzVMAccessExtension -Name "DemoAE" -ResourceGroupName $rgName -Location $location -VMName $vmName -TypeHandlerVersion "2.0" -Credential (get-credential)

**Custom Script Extension:**

* The Custom Script Extension **downloads and executes** scripts on Azure virtual machines.
* The most common use of Custom Script extension involves applying **custom configuration settings** during VM provisioning.
* This extension is also useful for **stopping a VM** or **software installation**, or any other configuration / management task.
* Scripts can be downloaded from either **Azure Storage or GitHub**, or provided to the Azure portal at extension run time.
* The Custom Script Extension for Windows requires that the target virtual machine is connected to the internet.

**CLI Command** to download and execute a PowerShell script that **installs IIS** and configures a basic home page.

**az vm extension set \**

**--resource-group Demo-rg\**

**--vm-name Demo2-vm \**

**--name CustomScriptExtension \**

**--publisher Microsoft.Compute \**

**--settings '{"fileUris":["https://raw.githubusercontent.com/MicrosoftDocs/mslearn-welcome-to-azure/master/configure-iis.ps1"]}' \**

**--protected-settings '{"commandToExecute": "powershell -ExecutionPolicy Unrestricted -File configure-iis.ps1"}'**

**Configure Nginx on your VM**

az vm extension set \

--resource-group [sandbox resource group name] \

--vm-name my-vm \

--name customScript \

--publisher Microsoft.Azure.Extensions \

--version 2.1 \

--settings '{"fileUris":["https://raw.githubusercontent.com/MicrosoftDocs/mslearn-welcome-to-azure/master/configure-nginx.sh"]}' \

--protected-settings '{"commandToExecute": "./configure-nginx.sh"}'

**Virtual Machine Scale Sets**

* A VM scale set consists of a **group** of automatically provisioned Windows or Linux virtual machines that share **identical configurations** and deliver the same functionality to support a service or application.
* With a VM scale set, it is possible to have the number of virtual machines **increase or decrease**, adjusting dynamically to changes in demand for the service or application. To implement on demand autoscaling, you combine VM Scale Sets with Azure Insights **Autoscale**.
* With scale sets, all VM instances are created from the **same base OS image and configuration**. This approach lets you easily manage hundreds of VMs without additional configuration tasks or network management.
* It's easier to **build large-scale services** targeting big compute, big data, and containerized workloads.

#### **General guidance**

* You can create both Linux and Windows VM Scale Sets from the Azure Portal. These scale sets are automatically created with **load balancer NAT rules** to enable SSH or RDP connections.
* With un-managed disk, Max VM = 100 and with Managed Disk it can go upto 1000 VMs
* If you create and upload your own custom VM images, the limit is 300 VM instances.
* When you increase the number of virtual machines in a scale set, VMs are balanced across **update and fault domains** to ensure, maximum availability. Similarly, when you scale in, VMs are removed with maximum availability in mind.
* You can set the maximum, minimum and default number of VMs, and define triggers – action rules based on resource consumption.