Compute

Monday, November 1, 2021

6:36 PM

Doubts:

* While deploying VM in Azure below resources are deployed

Vnet

NSG

Nic, IP address

Disks default std ssd

* Azure Bastion -

Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal. The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network. It provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS. When you connect via Azure Bastion, your virtual machines do not need a public IP address, agent, or special client software.

From <[*https://docs.microsoft.com/en-us/azure/bastion/bastion-overview*](https://docs.microsoft.com/en-us/azure/bastion/bastion-overview)>

* Image G1 and G2: cost is same, diff boot archi - G2 has improved boot and installation time ADE cannot be enabled for G2 [Azure support for generation 2 VMs - Azure Virtual Machines | Microsoft Docs](https://docs.microsoft.com/en-us/azure/virtual-machines/generation-2)
* During restart public IP, temp data reamains but deallocate/stop start will loose IP, temp data
* Stop from Azure portal will be stop and deallocate will not incur any charge for underlying physical h/w as it deallocates from physical machine completely, when it is started it might be in same physical or different physical server all together stop from VM will make status stop which still incur minimum charge for underlying h/w
* Azure CLI is only for Azure, PS is for other products as well.
* SSE
  + SSE with PMK - Service side encrypt with platform managed keys (customer managed keys can also be used)
  + All the data of disks are stored in a storage unit of a Azure data center
  + When sse is enabled all the data at rest is protected. It means, the data that is stored in data center storage unit will be encrypted and stored.
  + When VM tries to access data will be unencrypted and then will be available for a VM.
  + Done by 256 bit AES encryption to managed disks data, os
* IOPS, throughput [AZ-104 Microsoft Azure Administrator Certification 2021 (udemy.com)](https://deloittedevelopment.udemy.com/course/microsoft-certified-azure-administrator/learn/lecture/18109787#questions) measured in MBps
* Add data disk through PS [AZ-104 Microsoft Azure Administrator Certification 2021 (udemy.com)](https://deloittedevelopment.udemy.com/course/microsoft-certified-azure-administrator/learn/lecture/18109787#questions)

$resourcegroup = 'testResourceGroup'

$machinename = 'testVM'

$location = 'East US'

$storageType = 'Standard\_LRS'

$dataDiskName = 'newdisk01'

$dataDiskSize = 20

$datadiskConfig = New-AzDiskConfig -SkuName $storageType -Location $location -CreateOption Empty -DiskSizeGB $dataDiskSize

$dataDisk01 = New-AzDisk -DiskName $dataDiskName -Disk $datadiskConfig -ResourceGroupName $resourcegroup

$vm = Get-AzVM -Name $machinename -ResourceGroupName $resourcegroup

$vm = Add-AzVMDataDisk -VM $vm -Name $dataDiskName -CreateOption Attach -ManagedDiskId $dataDisk01.Id -Lun 1

Update-AzVM -VM $vm -ResourceGroupName $resourcegroup

From <[*https://deloittedevelopment.udemy.com/course/microsoft-certified-azure-administrator/learn/lecture/18109805#questions*](https://deloittedevelopment.udemy.com/course/microsoft-certified-azure-administrator/learn/lecture/18109805#questions)>

* Snapshots are used to take backup of a disk. New disk can be created from a snapshot and can be attached to another VM
* Azure Shared Disks - A disk can be attached/ accessed by multiple VMs. Possible only with premium and ultra.
  + Ideally A disk can only be attached to one VM. But say SQL workload has to be clustered this can be used.
  + Use application cluster to ensure data to be shared by the VMs via shared disk. Ex: services for windows server for a file cluster. It is responsible that data is shared across the m/c
* Managed Vs Unmanaged
  + Managed availability is maintained by Azure cost is applicable for entire size irrespective of consumption.
  + Unmanaged disk needs user to create a storage account , cost is less - only for data consumed. User needs to ensure availability. Std SSD is not supported by unmanaged.
  + A VM cannot have both managed and Unmanaged disks.
* Custom Script Extension for windows:
  + Can be used for VM to download or execute scripts
  + Its idea when u want to deploy custom config for any s/w installations on VM.
  + Scripts can be located on Azure storage account or Github
  + Max time limit 90mins will fail after that.
  + Recommended not to use for reboots bcz it stops working after reboot and remaining script after reboot will not be executed. If it does need reboot then other tools can be used like Desire state config, Chef or puppet
  + Script runs only once.
  + It executes like a local system account.
* Cloud init file - for linux machine packages can be pre installed on new Linux VM. This is more specifically for Linux VM
* Boot diagnostics - VM - BD - serial logs (very useful for Linux VM). To get an idea of what happened during boot time (helpful if any issues)
* Serial console - used to send commands to VM itself. It needs boot diagnostic custom storage account to be used.
* Run in VM portal allows VM agent to let you run the scripts inside VM
* Confidential Computing and Azure Dedicated Host
  + Azure Confidential Computing
  + This is a feature that allows you to isolate sensitive data when it is being processed in the cloud.

* This feature is available for your virtual machines. In Confidential computing , a part of the CPU’s hardware is reserved for the portion of code and data in your application. This portion is known as an enclave.

* There is a special series of virtual machines which support confidential computing. This is the DCsv2-Series

* <https://docs.microsoft.com/en-us/azure/virtual-machines/dcv2-series>

* These series of virtual machines are built on Intel SGX technology for hardware-based enclaves.

* To actually ensure that your code or application runs inside the enclave, you will have to program it accordingly.

* For this you need to use two open-source frameworks

* a) Open Enclave Software Development Kit

<https://github.com/openenclave/openenclave>

* ·b)Confidential Consortium Framework

<https://github.com/Microsoft/CCF>

* Azure Dedicated Hosts
* This service provides physical servers to host virtual machines. The physical server is dedicate to the Azure subscription.

* The benefits of Azure Dedicated Hosts is that no other virtual machines from any other customers would be placed on the physical server.

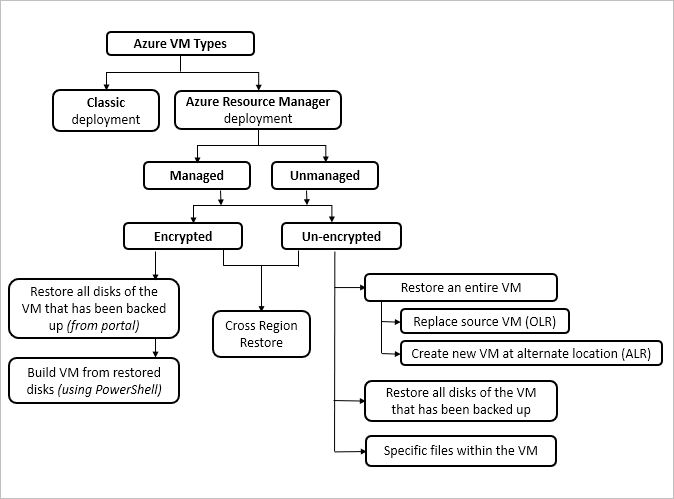
* You can also control the maintenance events that are initiated on the Azure platform.

* Here the users are charged per dedicated host. This is irrespective of the number of virtual machines running on the physical server

* For more information on Azure Dedicated Hosts , you can visit the URL - <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/dedicated-hosts>

* Azure Back UP:

* Recovery service vault has to be in same region. Backups can be scheduled and retention can be mentioned in backup policy, recovery point is created when a backup is taken.
* Recovery is done from specific recovery point it can be file recovery, VM recovery (duplicate), Disk recovery
* Azure backup for virtual machine is a feature that is used to back up the disks allocated to virtual machine. During first backup an extension in installed in OS and is different for Linux and windows.
* This extension takes snapshot of VMs
* For windows based m/c back service works with windows volume shadow copy for application consistent snapshot.
* Linux based with file consistent snapshot
* Diff types of snapshots:
  + Application consistent \_ Backup services captures memory content, pending IO. Whatever the state of VM is taken consistent when backup is restored.
  + File consistent - backup service take snapshot of all files at same time.
  + Crash - consistent - this happens if VM shut down at the time of backup
* Instant restore - for 2 days
* Restore point is already there even before taking backup it is because of instant restore feature
* Instant restore takes the back of snapshot and is in VM itself.
* Backup copies from VM to recovery service vaults.

* 

[About the Azure Virtual Machine restore process - Azure Backup | Microsoft Docs](https://docs.microsoft.com/en-us/azure/backup/about-azure-vm-restore)

* A executable file is downloaded enables a connection bw mount point and recovery point.
* Even if backup data is deleted recovery vault will not be deleted during the retention period. Disable soft delete and then delete recovery vault.
* Recovery vault --> backup items --> Delete
* MARS agent or Recovery service agent or Azure Backup Agent
  + VM contents can also be backed using this agent apart from extension
  + Using extension entire VM is backed up but by this agent a specific file can be selected
  + This can be used for Azure or on prem VMs by installing agent, schedule and recover the data

ASR

* Continuously replicates a VM, when smthng goes wrong can fail over to secondary region and fail back to primary region
* Source region requires a storage account which acts like a cache where the changes on source machine are first stored here before sending to target.
* Replication creates SA in target if the VM is unmanaged and created AV Set/ AZ with same no will be allocated to target VM in the target region. It creates RG, Vnet that the target VM belongs , reside in.
* Retention policy - default, recovery point retention - 24 hrs, app consistent snapshot - 4hrs
  + Site recovery mobility extension is installed on source VM
  + Continuous replication then occurs to cache SA in source region(during this time targt VM is not yet created)
  + Failover can be conducted once the recovery points are at target (app consistent/ crash consistent)

AV SET:

2 + VMs , FD - 3, UD - 20

Aligned - managed

Classic - unmanaged

proximity placement group - allows to group Azure resources physically closer

Existing VM cannot be moved in/out of VM only way is to re create

Delete VMs first and then AVSet if not an error occurs

SLA - 99.95

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/azure>- n njsubscription-service-limits#virtual-machines-limits---azure-resource-manager

VMSS:

This service allows to manage group of identical VMs, can place behind load balancer, No. VMs are increased/ decreased based on demand.

AV Zone:

Each region has multiple zones. each zone is one or more DC

Used in DC failure

SLA 99.99%

AV Zone needs to pay extra cost for commun across VMs - bandwidth comm (this is not in AV Set)

Creating custom image - known as Generalization of VM

Say some app configs are done and an image can be customized from this and VMs can be deployed

From a VM once an image is created that VM cannot be used anymore but the image can be used.

Connect to VM --> c\sys32\sysprep --> Run sysprep (select generalize) shut down --> OK force stop from cloud shell

Proximity placement group:

Normally when multiple VMs or VMs of VMSS are deployed, VMs are placed in diff dc. Sometimes, app/sys want them to stay close physically to reduce latency. This can be done by placing VMs as part of placement group.

Sub -> cost analysis

KV stores keys,certificates,secrets

ADE creates encryption key in Azure KV and uses this to encrypt and decrypt data that is stored in disks attached.

az vm encryption enable -g BackUPRG --name BackUPDemo --disk-encryption-keyvault kvdemoade

WebApp:

When an app is hosted on Azure it can be done in two ways:

1. VMs - IAAS - need to manage under lying infrastructure, used for custom/ vendor based apps
2. Web apps - PAAS - platform managed, provides auto scale - security , Devops - CD

Web app is linked to app service plan. So two resources are created. Depending on app service plan, web app is billed and features are accordingly

[App Service Pricing | Microsoft Azure](https://azure.microsoft.com/en-us/pricing/details/app-service/windows/)

App service plans:

Free, shared, basic, std, premium, isolated.

Free / shared - have CPU limits 60/ 240 accordingly remaining does not have

Deployment slots - Available when std or higher, Adv - diff version of applications can be run on the same web app

like prd slot, stg slot each has its own DNS name

Adv:

U'll have chance to validate all app changes in stg deployment slot

U can then swap prd and stg slot

Downtime is less when new changes are deployed

Easy to roll back changes

Auth / autho - by default it is disabled everybody can use, can be enabled and define settings/rules

Backup - std/ higher

Scale up/down - upgrade/ downgrade the app service plan

Scale in/out - No. compute machines are increased/ decreased

az appservice plan create --name webappplan7000 --resource-group azuredemo --sku B1

az webapp create --name webapp9000 --plan webappplan7000 --resource-group azuredemo

Features like auto scale, deployment slots are available in std and higher

Basic doesn’t have dep slot and scaling is manual

Rules can be defined for auto scale these metrics can be based on other azure resources as well

Cool down period is the time taken to distribute traffic among instances when a new one is created as part of scaling

PAAS service for docker container:

Deploy VM, install docker pull nginx instead u have platform as a service which need not to manage underlying VM

**Azure container**: ensures automatically VM is deployed and run containers

Cannot scale mem CPU assigned to ACS

Container groups: collection of containers, deployed at once on same physical host, shares same life cycle, local n/w storage vol and deployed via RM temp, yml

**Kubernetes:** open source orchestration platform to manage containers

|  |  |
| --- | --- |
| Kubernetes | Azure kubernetes |
| Open source platform to manage containerized apps | Fully managed k8s service on azure |
| Provides DNS name to contianers | Makes it easy to deploy and manage containerized app |
| LB | It helps to remove burden of managing underlying infra for k8s deployment |
| Restart, replace, kill containers |  |
| Helps to store and manage sensitive info like pwds, Oauth, SSH |  |

Containers are run as POD

Nodes are VM on which containers run

Containers are spun on images from Docker hub

To deploy clusters on k8s cluster deployment files .yml are used, app.yml for pods, service.yml for services(service exposes pods to outside world)

AKS Networking:

Containers are deployed to indiviudal container which are deployed on Node(compute instance for hosting POD).

Ips are assigned to pods for inter comm b/w pods. Can be done in two ways:

1. Using Kubenet node gets an IP from Azure Vnet underlying.

PODs receive Ip that are logically different address space to Azure virtual network subnet

NAT is then used

1. Azure container network interface

Every POD gets the Ip address from the Subnet directly but this can cause exhaustion of Ips

If it is CNI need to define address range

AKS Storage:

Similar to VM writing persistent data to disks, storage account AKS can do to Azure premium disks or Azure file share.

Disks are available to only single pod, Azure file share is accessed by multiple nodes, pods.

While creating disk AV Zone need to be checked and make sure of same zone of AKS

Master and Nodes are created in different resource groups

[AZ-104 Microsoft Azure Administrator Certification 2021 (udemy.com)](https://deloittedevelopment.udemy.com/course/microsoft-certified-azure-administrator/learn/lecture/25666974#announcements)

Azure Container registry:

Usually AKS gets images from docket hub but images can be stored/upload and get from company's own/private Azure container registry.

AKS need to authenticate itself to pull images from Azure container registry it is done by Service principle.

When AKS is created, it creates service principle that is attached to cluster it is like having a user in AD and then ensure service principle has authority to download images from Azure container registry.

It has to be in same location as AKS

Diff provisioned iops and max burst iops

retention

ACS/AKS diff

Can multiple containers of diff users run on one VM

Doubts:

Retention defaults and limits

Create webapp

Sample app, publish

App service --> scale up means upgrades app service plan

What about other webapps associated to this app service plan

Bottle neck perf

App logging / app insights diff

Orchestration

Disks shared when scaled?

How to see no. instances running

For portal publish - code/ docker ?

Max no. VMs in AVSet

Rpo

Rto

Change html in source and test failover