**Deploy and manage Azure compute resources**

**Azure VM –** Is an IaaS offering,

**Create**

Required: RG, Storage account, Vnet, VNic

Optional: PIP, Data disk

Extensions: Custom script after deployment (diagnostics, etc)

Powershell cmd: New-AzVM

Azure CLI: az vm create

**Moving VM**

Diff subscription – vNet resources must be moved too

VM with integrated keyvault for disk encryption cannot be moved (disable disk encryption first)

VM scalesets with Std LB and std PIP cannot be moved

VM with Az backup must have restore points deleted prior to moving

**Sizing / Resizing**

VM’s will be stopped when resizing

**Redeploying**

Redeploy shutsdown the VM and moves to new node

**Configure VM’s**

**Network**:

VNic – VM’s can have multiple VNic (using Powershell or CLI)

To add Vnic, the VM must be deallocated

Nic can only be assigned to VNet with the same location (only location of net not RG)

Subnet within a VNet

No security boundary between subnet by default  
IP – Private is assigned automatically, Public is optional

Deallocating VM’s will release dynamic public IP

**Data disk**:  
 Can be added on the fly, then manage the disk inside the OS

Type: BLOBS or Snapshots

**Azure Disk encryption**

BitLocker for Windows and DMCrypt for Linux

Full disk encryption of OS and Data disk

Integrated with Azure Keyvault

VM’s must be able to connect to either Azure AD or KeyVault endpoint

Az KeyVault access policy must be enabled for Azure Disk Encryption

(New-AzKeyVault ………… -EnabledForDiskEncryption)

**High Availability and Scalability**

**Availability Zones**

Zones are DC that are on same region but separated physically

Distribute VM’s across an Azure region (1- 3 zones per region)

LB standard is availability zone aware

PIP standard is required

SLA is 99.99% if 2 or more AZ zone VM’s

**Availability Sets –** Groups VM’s to distribute across a single DC

Must be set, during creation. Cannot be added after VM creation.

SLA is 99.95% for VM’s that have two or more instances deployed on same availability sets

**Fault domains –** Server racks in a DC. VM’s in same fault domain share power source and physical network switch

**Update domains –** Individual Servers in the Racks. VM in same update domain will be restarted together during maintenance. Only 1 update domain is restarted at a time.

**Scale Sets –** Group of LB machines

Can scale automatically based on schedule or demand (RULES)

Only pay for the extra instances – no other cost

Can be deployed across Fault and Update domains

**Automate deployment of virtual machines (VMs) by using Azure Resource Manager templates**

**ARM templates –** JSON format (key value pairs) > Submit template to ARM (Azure Resource Manager) > Track deployments.

ARM templates are for CREAITNG as well as UPDATING resources

**Modify existing templates** – Export template under Automation > Select deploy to edit template > Purchase

**Deploy from template**

Create the JSON template or you can download from Azure portal >

Deploy a Custom template in portal > Build your own template in the editor > paste or load file > Create

**Save deployment as an ARM template**

Go to RG or Resource > Choose Export template > Download template

Powershell: Export-AzResourceGroup

**Automate deployment and configuration of VM’s**

**Custom Script Extensions** (Ex. Install IIS) – Settings > Extensions > Custom Script extension

Scripts can be located anywhere as long as VM has access to it

Scripts only run once – Can be added during deployment or post deployment of VM

Scripts are Idempotent

**Configure VHD template** – Managed image or Golden image

Sysprep /generalized the managed image with support up to 20 simultaneous deployments

Capture image, provide name

Choose to delete VM after capture

Provide name of VM

Go to Image > search for the image you have created > Create VM

**Create and configure containers**

**Azure Containers –** Single containers service from Azure

**Create container instances**

On portal > Container instances> Provide basic info > DNS Name label (will append to full FQDN) > Port > Restart policy

Restart policy can only be set during creation/deployment

**Azure Container Groups –** Azure Service for Collection of containers in same host (Like Kubernetes). Only Linux. Deployed via ARM or YAML

Properties that will require Container deletion (redeployment):  
 -OS Type

-CPU, Memory, GPU

-Restart Policy

-Network profile

**Azure Kubernetes Service**

**Create AKS Cluster**

Nodes of same config are grouped into node pools

When you create a cluster, you create a system node pool

AKS cluster must use VM scale sets for the nodes for autoscaling and multiple node pools

All node pools must reside on the same VNet

AKS cluster must use the Standard SKU load balancer to use multiple node pools

Create the cluster then use Kubectl to deploy the app

**AKS Storage**

Volumes – Can use Azure Disk or Azure Files (for multiple clusters, Azure Files is recommended)

Persistent Volumes – Volumes defined and created as part of Pods life cycle

Storage Classes – Define SKU of storage

Persistent Volume claims – Requests either disk or File storage by Storage class

**AKS Scaling**

Manual Scale pods or Nodes –

Pods: kubectl scale –replicas=5 deployment/xxxx

Nodes: az aks scale -resource-group xxxxx … --node-count 3

Auto scale: kubectl autoscale deployment xxxx

Horizontal pod auto-scaler

Cluster auto-scaler

**AKS Networking**

Kubenet

Nodes gets an IP from subnet

Pods gets IP from Kubenet

Routing are configured by Routing Table

Azure CNI

Nodes gets IP from subnet

Pods also gets IP from subnet

Downside, need to consider how many IP for the subnet

**Upgrade an AKS cluster**

Can only upgrade 1 minor version at a time – 1.14.x to 1.15 not 1.14 to 1.16

**Create and configure Azure App Service**

**Azure App Service**

Supports containerization and Docker

Web app and App Service Plan needs to be in the same region

Linux app plan can run Linux apps – Windows App plan can run Windows apps

App cloning is supported for Standard, Premium and Isolated app service plans

Dev/Test

F1 – No feature / Shared infrastructure

D1 – Feature Custom Domains / Shared infra

B1 – Custom domain, Manual Scale up to 3 / not shared anymore

Production

S1 – Custom domain, Auto scale up to 10, Staging slots up to 5, Daily backups (10 times daily), Traffic manager

Pxxx (premium levels) – Auto scale up to 20, Staging up to 20, backups (50 times daily)

**Create**

App Service Plan > Need to choose if Linux or Windows > Pricing Tier

**Scaling – App Service plan**

Scale in/out – adding more instances

Scale up/down – changing the plan

**Secure**

Add SSL certificate

App Service Managed cert and App Service cert meet requirements

Must be exported as a password protected PFX file prior to upload to portal

Must Contain private key at least 2048 bits long

Must Contain all intermediate cert in the cert chain

Authentication

Authenticate users – Built in. App Service > Authorization Settings > Choose Identity Provider

Managed Identity – App Service > Identity > System Assigned/User assigned

Access restriction

Priority Order list of allow/deny (IP, AZ subnets)

Works with all azure app service hosted workloads

Service endpoints must be enabled on network and service side

Encryption using managed keys

Encrypting web apps data requires a storage account and KeyVault

App Service can securely access secrets through managed identity

Revoke a webapp data access by rotating SAS key or removing app access to KeyVault

**Configure App Service**

**Custom Domain Names**

-Must verify ownership by adding a verification ID (drop a txt record)

-Root domain, you add an (A) record (host record) to your domain provider (subdomain is C record)

**AppService Backup (not azure backup)**

Must have Standard, Premium or Isolated App Service Plan

Backs up app configuration, file content, and database content

Manually or schedules

Partial or Full

Backups are visiable on the container page of the storage account (same subscription)

Database Backups max at 10GB (bigger? Use Azure Backup)

TLS enabled azure database MySQL and PostgreSQL are not supported

**Network options for App Service**

VNet integration - Multitenant and App Service Endpoints Configuration for VNet

-VNet integration does not grant inbound private access to app from Vnet

-Requires Standard, Premium, V2, V3 or Elastic premium plan

Hybrid Connections – An Azure Service as well as a Feature of App Service Plan

-Used to access app resources in any network that can make outbound calls to azure port 443

-Each Hybrid conn correlates to single TCP host and port combination (meaning any OS)

-Require basic or higher app service plan

Azure Front Door with WAF

Azure CDN