Azure Virtual Machine

Ranjit Karni

VPark Innovations

Ranjit.balu@gmail.com

Ph.No: 9676976662

Agenda

1. Azure VM Disk Types
2. Standard VS Premium Storage Disks
3. Managed Vs Unmanaged Disks
4. Public IP Address Notes
5. Planning for High Availability
6. VM Deployment Methods
7. Best Practices to Keep in Mind
8. Azure Disaster Recovery as a Service (DRaaS)
9. Azure Disk Encryption

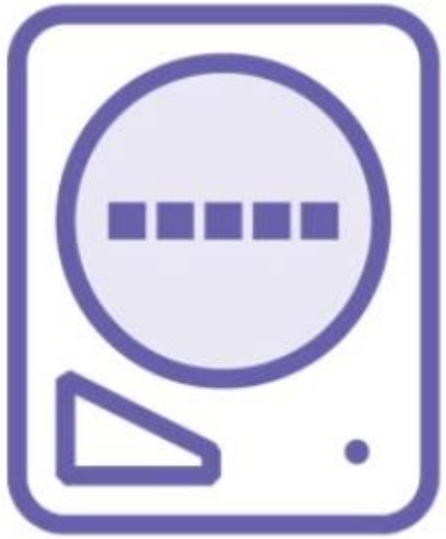
Azure VM Disk Types

OS Disk

Generation 1 .VHD

Registered as SATA drive

Max capacity 2 TB



Data Disk

dependent on VM instance size

Registered as SCSI disk

Max capacity 4 TB

Temporary Disk

D: or /dev/sdb1

Bound to the hardware host

Do not store permanent data!

Standard VS Premium Storage Disks

Standard Disks	Premium Disks
Backed by cost-effective HDDs	Backed by high-speed SSDs
Several replication options	IOPS values are predictable, expected performance levels
Standard SSD (Preview) available for managed disks only (for dev/test/entry level production applications)	Pre-pay for all storage used (fixed disk sizes
Standard storage provides maximum IOPS values for each VHD	P10, 128 GB, 500 IOPS, 50 MB/sec

Unmanaged Disks

- Disk created and managed by customer. You need to create page Blob storage for storing VHD.

- Storage Account is limited to 20000 IOPS

- Since there is limit with 20000 IOPS in a storage account, we can't keep more than 40 VM's in a single storage account. Every VM supports maximum 500 IOPS. We cannot have more than 40 VMs in a storage account.

- Use TRIM with unmanaged standard disks. TRIM discards unused blocks on the disk so you are only billed for storage that you are actually using:

    - Open a command prompt on your Windows VM and type:

    fsutil behavior query DisableDeleteNotify

    - If the command returns 0, TRIM is enabled correctly.

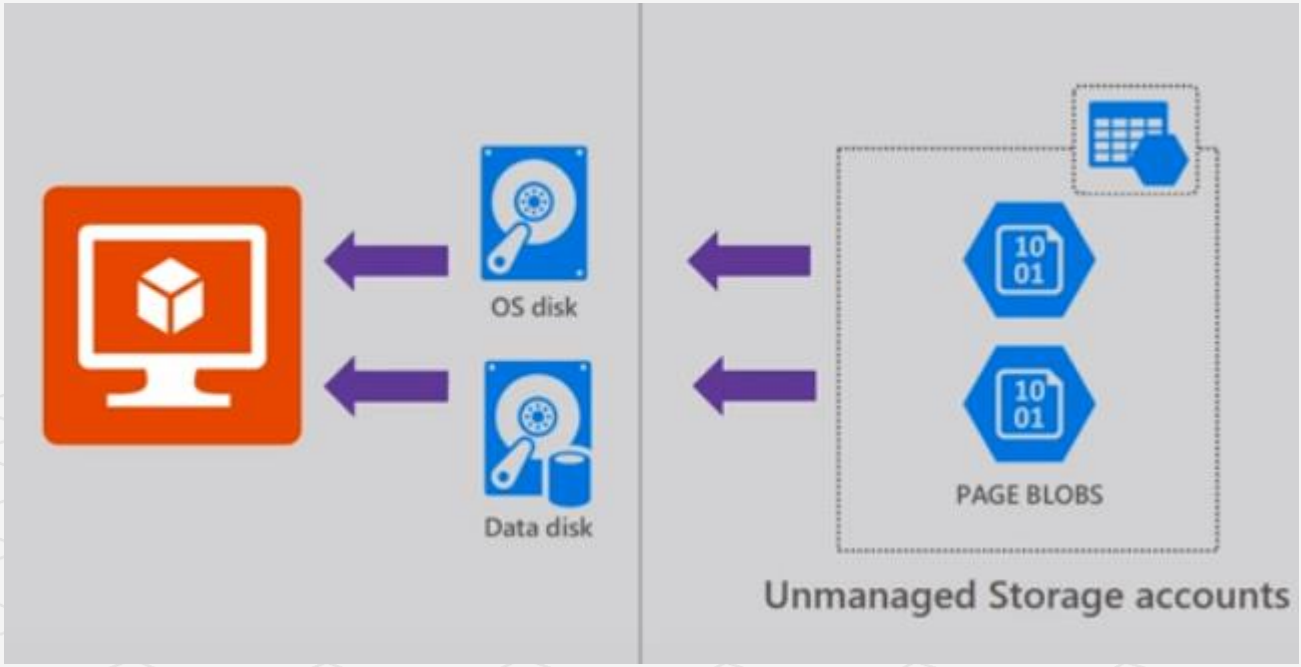
    - If it returns 1, run the following command to enable TRIM:

    fsutil behavior set DisableDeleteNotify 0

- Sparse Storage (Standard) – only pay for actual data than a disk size

- You can create upto 250 storage accounts

-



Managed Disks

- Simple: No need to select a storage account and Microsoft does it under the hood

- Granular access control: You can have granular level access with Azure Role Based Access Control (RBAC).

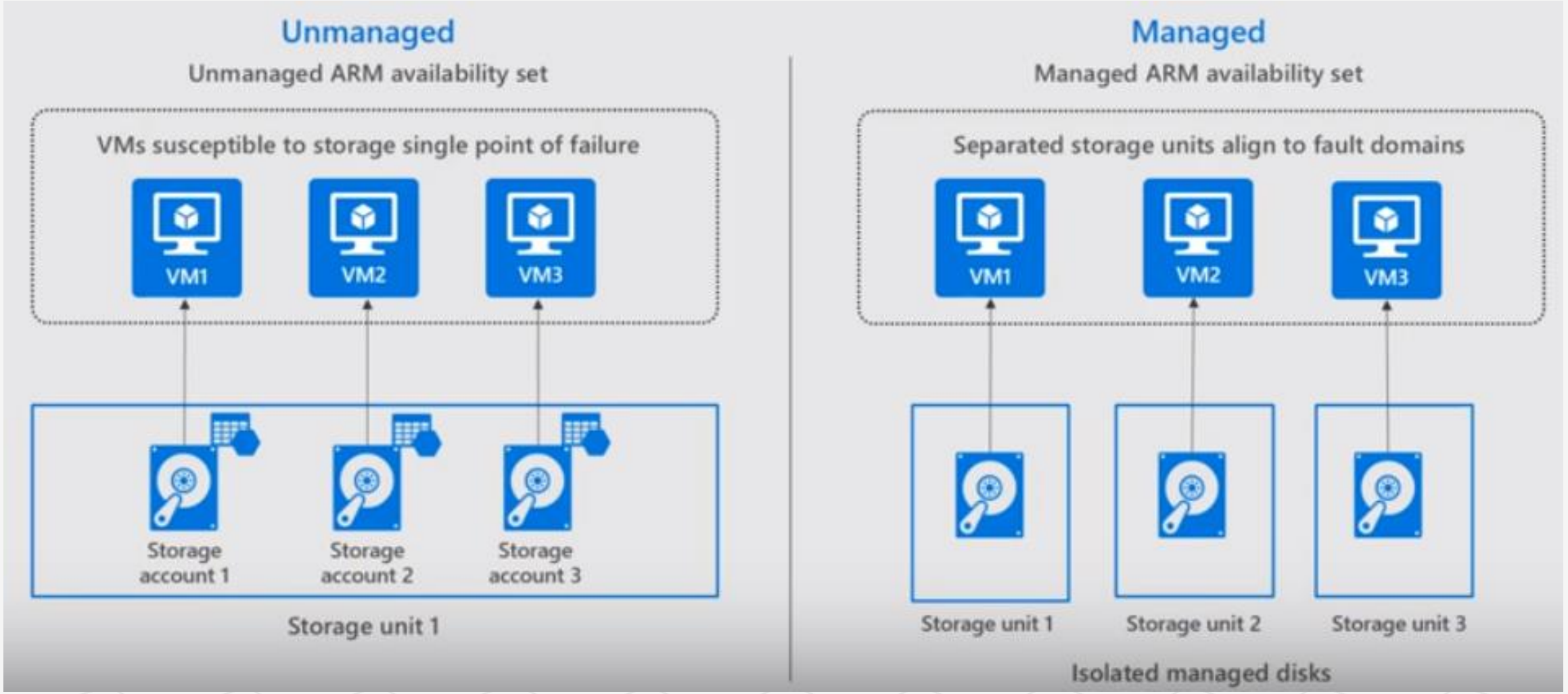
- Better Performance: No need to worry about Storage account limits

- Big Scale: It supports up to 20,000 disks per region per subscription. i.e. 10,000 standard and 10,000 premium storage disks

- Migration from unmanaged to managed disk can be done by ConvertTo-AzureRmVMManaged Disk powershell command.

- Managed Disk pricing details : https://azure.microsoft.com/en-in/pricing/details/managed-disks/

Major Difference between Unmanaged and Managed Disks



Managed Vs Unmanaged Disks

Unmanaged Disks

Original method to store VM VHDs

VHDs stored as page blobs in an Azure storage account

Maximum 256 TB of storage per VM

You need to manage standard or premium storage account availability

20,000 IOPS limit across all VM disks in a standard storage account

Managed Disks

Azure manages the disks, so you don't have to worry about storage account-level IOPS restrictions

Pre-pay for disk size (no need for SA)

S10, 128 GB, 500 IOPS, 60 MB/sec

Supports Standard and Premium SSD and Standard HDD

LRS replication only for Premium managed disks

Managed Disks and UnManaged Disks

- Use Managed Disk for all the production IaaS workloads

- Use Managed Disks with Availability Set

- Not all Azure services support managed disk yet (like Azure Site Recovery)

- Some partner solutions still require unmanaged disk

- Migration to managed disk can be done by **ConvertTo-AzureRmVMManagedDisk**

Public IP Address Notes

- Do we really need IP Address?
    - Consider Azure Load Balancer
- Public IPV4 addresses can be associated with:
    - VM vNICs, Public Load Balancers, VPN Gateways and Application Gateways

Basic SKU

- Open by default

Static and dynamic allocation

Standard SKU

- Secure by default (NSG)
- Static allocation only
- Availability Zone aware

Planning for High Availability

- Availability Set
    - Fault Domain
    - Update Domain
- Availability Zone

Availability Set

- Logical Grouping Capability

- Azure ensures that the VMs you place within an Availability Set run across multiple physical servers, compute racks, storage units and network switches.

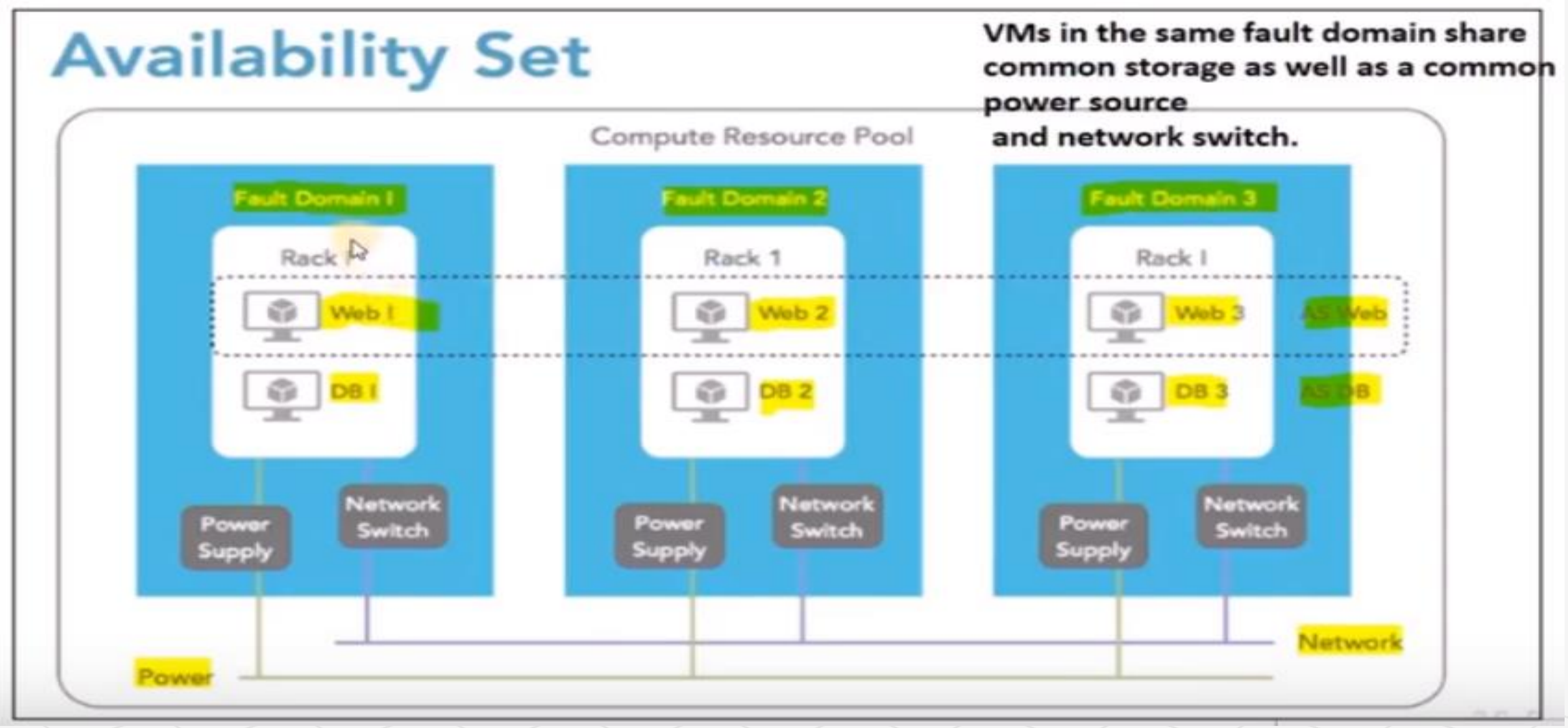
- VMs are spread across fault and update domains

- 99.95% SLA from Microsoft (Excluding Premium Storage)

- Group similar VM together; ex SQL Server in one AS, Web Server in another availability set.

- Can only have VM in one availability Set

Availability Set



Fault Domain

- Is a physical unit of failure

- Infrastructure of each Azure DC is divided into multiple sections which are treated as fault domains

- Designed in such a way that a failure of 1 FD is extremely unlikely to affect any other FD

- VMs in the same **fault domain** share common storage as well as a common power source and network switch

Update Domain

- logical boundary that controls how Microsoft will deploy planned maintenance

- Microsoft will only perform planned maintenance on one update domain at a time. There will be several update domains within a fault domain

- Is a group of VMs and underlying physical hardware that can be rebooted at the same time

- Logical unit of deployment does not exist physically

- Used for patching

- Only one update domain is updated at a time

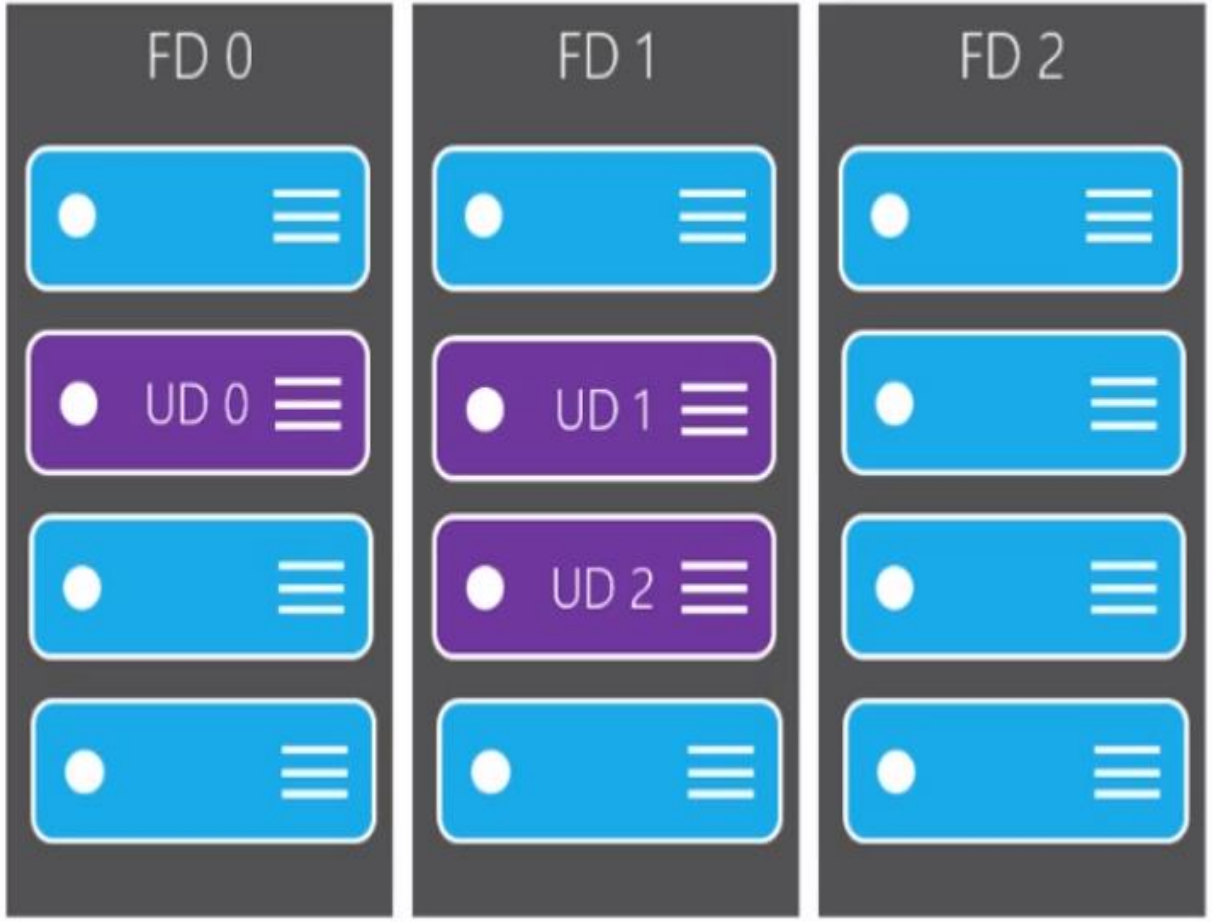
- VM within that UD will reboot together

- VM is assigned to update domain automatically, when you put your VM into availability set.

Availability Set

Fault domains are VMs that share the same power source and switch

3 fault domains available



Update domains are VMs that share the same hardware host

5-20 update domains available

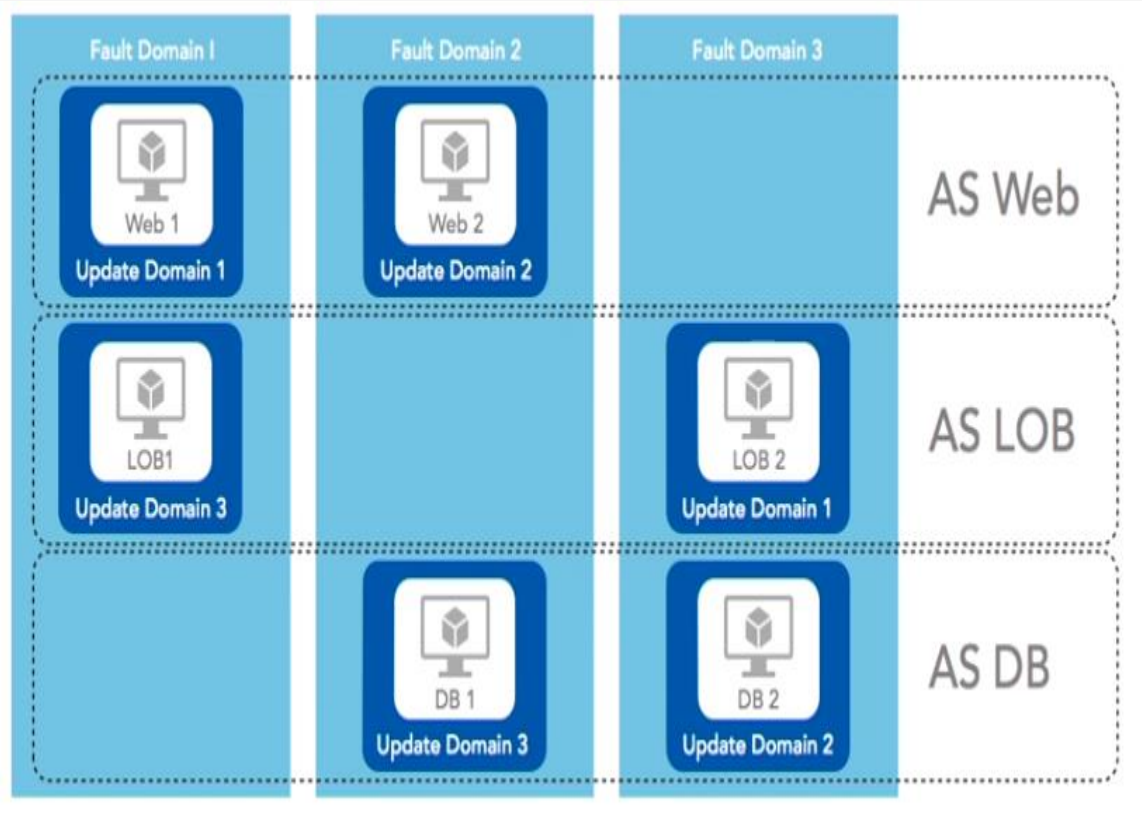
ARM with 2 Fault Domains

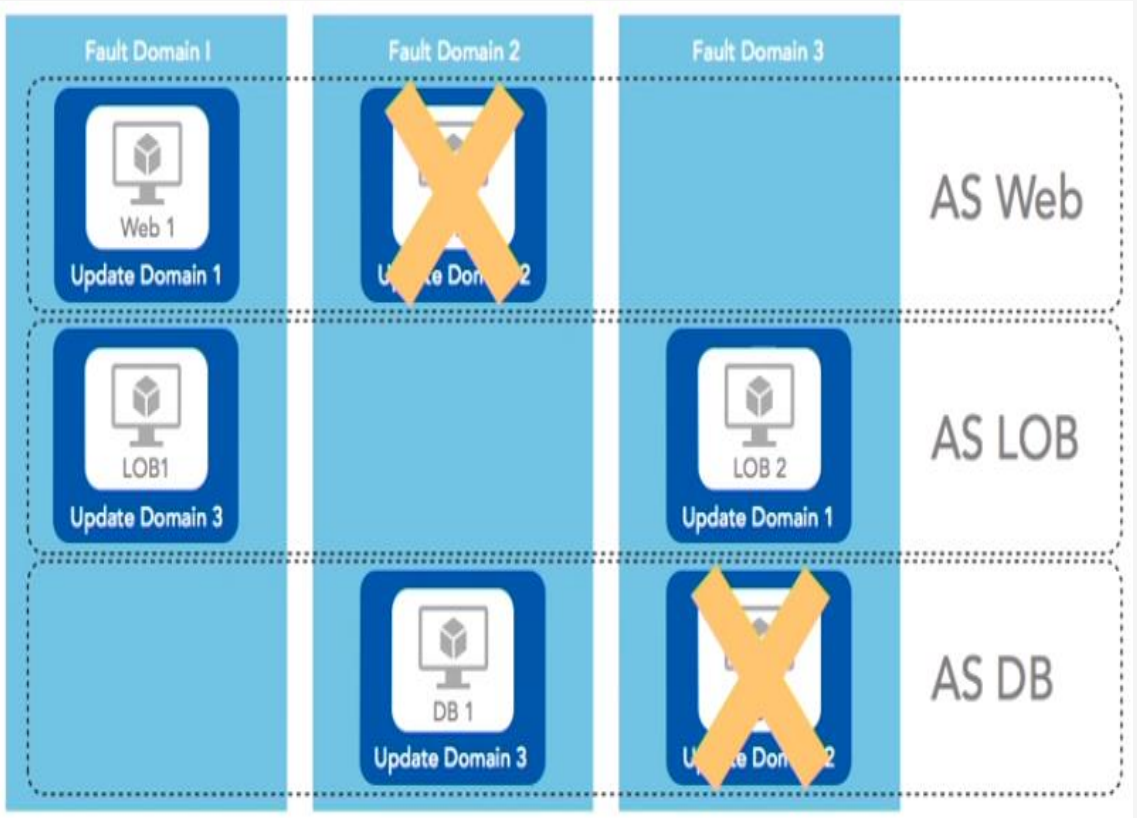
VM	Update Domain	Fault Domain
VM1	0	0
VM2	1	1
VM3	2	0
VM4	3	1
VM5	4	0

ARM with 3 Fault Domains

VM	Update Domain	Fault Domain
VM1	0	0
VM2	1	1
VM3	2	2
VM4	3	0
VM5	4	1

Putting All Together





Microsoft Best Practices for Availability Set

- Group two or more similar virtual machines in an availability set

- The virtual machines needs to be created in the resource group as the availability set

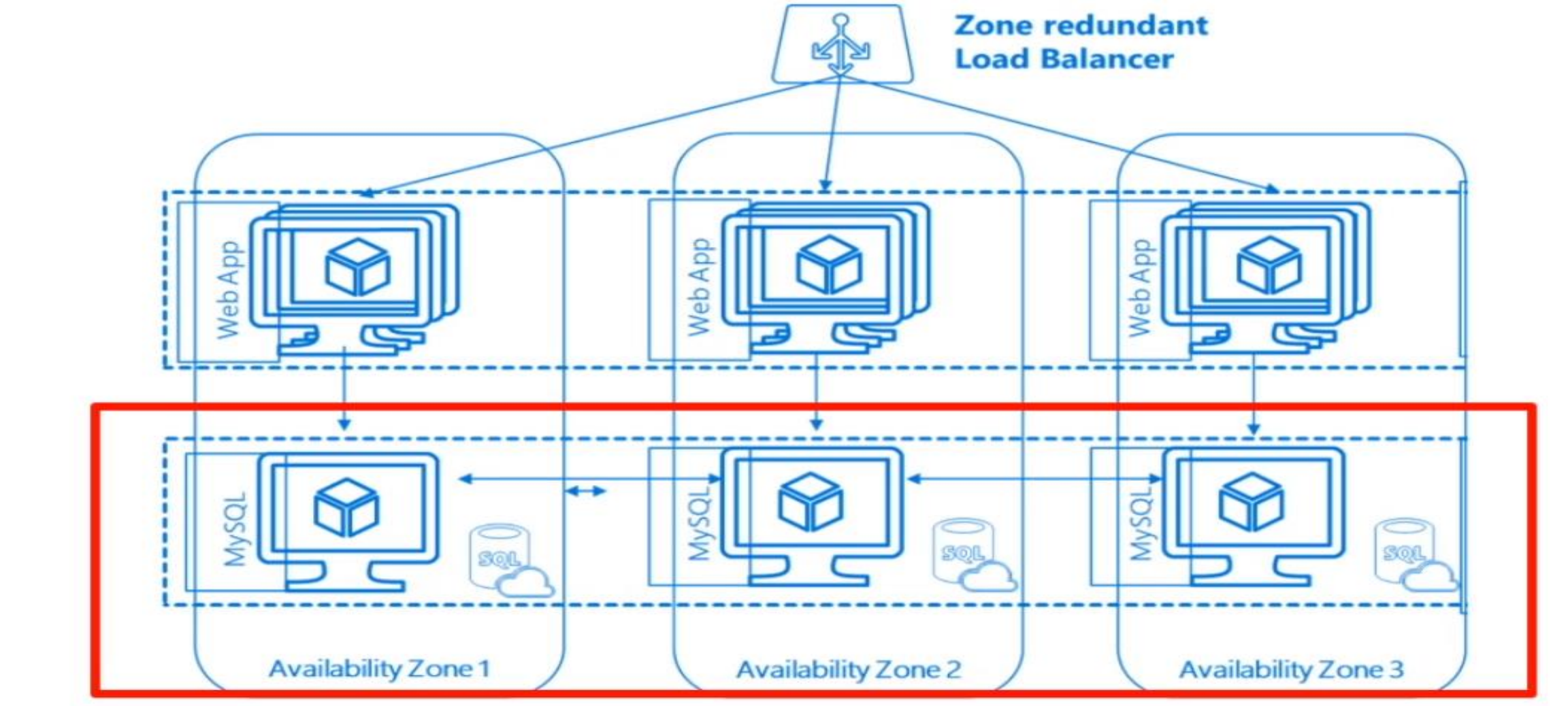
- Can only have virtual machines in one availability set

- Determine the number of availability sets needed based on roles and tiers and you need to do this step before provisioning virtual machines because you can only assign the availability set during the creation of virtual machine.

- Create separate storage accounts for each virtual machine

- Consider your naming conventions (Recommend to keep the logical and descriptive names)

Availability Zone



VM Deployment Methods

- Azure Portal
- Azure Powershell
- Azure CLI
- ARM Templates
- Azure SDK
- Cloud Shell

Best Practices to Keep in Mind

- Virtual Network
    - Create before deployment
- Availability Set
    - Associate during deployment
- Naming Convention
    - Develop and use one
- NSG
    - Create before deployment
- Deployment Script

    0 Save it

Azure Disaster Recovery as a Service (DRaaS)

Azure Backup

Policy-based backup and restore

"Born in the cloud" VMs

On-premises VMs (Hyper-v,

Azure Site Recovery

Hybrid VM replication solution

Fail over application to the cloud or secondary datacenter

Azure Disk Encryption (ADE)

- Azure Disk Encryption

  Windows VM: Bit-Locker

  Linux VM: DM-Crypt

- ADE Requirement

  - Basic Tier VMs are not supported for ADE. **Please choose Standard Tier VMs**.

  - **Azure Key Vault:** ADE required that yours key vault and VMs reside in the same Azure region and subscription

  - **Boot Volume:** ADE must be turned on before Data Volume ADE can be turned on.

  - Azure Disk Encryption is supported on the following:

    - Windows Server Versions: Windows Server 2008 R2, Windows Server 2012, Windows 2012 R2 and Windows server 2016
    - Windows Client Versions: Windows 8 client, Windows 10 client
    -Linux: RHEL, CentOS, OpenSuse, SLES

  - The **Storage account** to store the encrypted OS VHD and the VM must be created in the same resource group and location

Azure Disk Encryption (ADE)

- To enable disk encryption for Windows and Linux VMs, do the following:
    - Opt in to enabling disk encryption via the Azure Disk Encryption Resource Manager Template

Steps to enable ADE on an existing running Windows VM with help of ARM Template

- Have a Standard tier VM provisioned with a data disk attached to it

- Register an Azure AD Application through portal with following details:
    - User friendly App name
    - **Sign-on URL**
    - **App ID URL**

- Next create an **Azure Key Vault (AKV)** to store BitLocker Keys

- Assign following permissions on AKV to Application registered in Step2
    - **Enable AKV to be used for disk encryption**
    - **Key Permission → User Cryptographic Operations, Wrap Key**
    - **Secreat Permissions → Under Secret Management Operations, SET**

- **Finally, deploy the ADE ARM template from Github and fill out following details:**

https://github.com/Azure/azure-quickstart-templates/tree/master/201-encrypt-running-windows-vm-without-aad

Questions?

Ranjit Karni

Vpark Innovations

Ranjit.balu@gmail.com

Ph No: +91-9676976662