Microsoft Azure (AZURE-Cloud)

1. Network OS
2. Client OS
3. Traditional IT
4. Virtualization
5. On premise
6. Cloud computing
7. On demand service
8. Pay As you Go
9. **Network OS:**

*Windows* : Server 2008, server 2012, server 2016, server 2019, server 2022

*Linux* : Red hat Linux, SUSE Linux

*Processo*r : XEON (24\*7 running)

Uses : web server, mail server, tally server, domain controller, SAP HANA, movie maker, In-house application

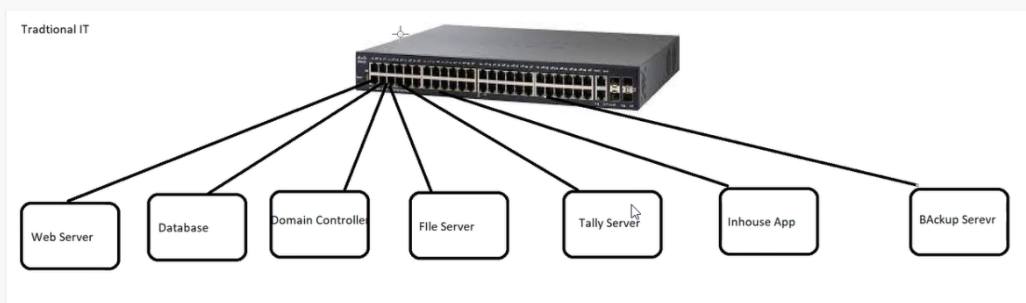
1. **Client OS:**

*Windows* : Windows 7, win8, win 10, win 11

*Linux* : Centos, Ubuntu

*Processor* : Core i3, core i5, core i7

1. **Traditional IT:**



Drawback of Traditional IT: More space consuming, Operation & Maintenance, dust proof environment, 24\*7 Electricity consumption, and 24\*7 Engineer required for O&M, Managers, Disaster Recovery (DR), and Hardware issue.

PDC : Primary Data Center

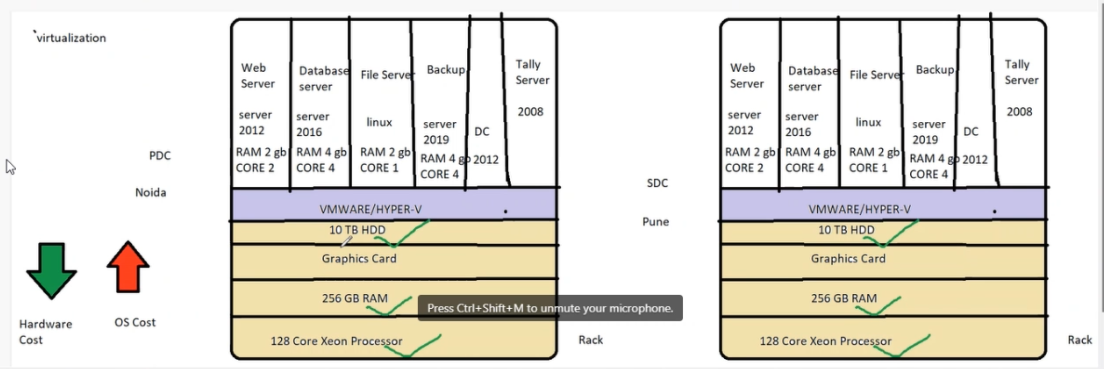
**VPN**

**SDC**

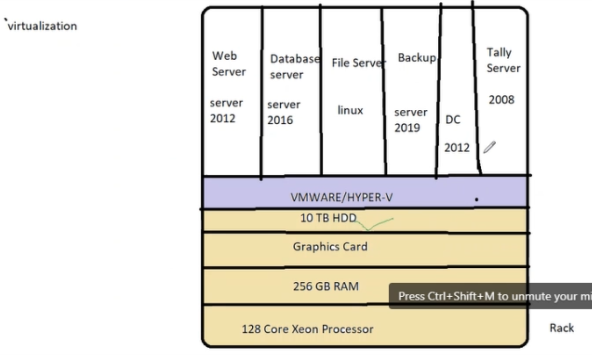
**PDC**

SDC : Secondary Data Center

DR : Disaster recovery



1. **Virtualization:**



1. **On-premise:**

Physical Hardware

1. **Cloud Computing:**
2. **On-Demand Service:**
3. **Pay as you GO**

Ask to client : Working days : - Monday to Friday: Total 22Days

Non-working days : - Saturday & Sunday

Working Hours : - 09:00 am to 07:00 am: Total 220 Hrs. 10Hrs. /Day

Non-working days : - 07:00 pm to 09:00

Public Cloud

Private Cloud

Hybrid Cloud

f

1. Single tenant: Under Armor
2. Reserved Hardware
3. Isolate
4. Costly
5. You can access over the internet

Public Cloud + Private Cloud = Hybrid Cloud

1. Single tenant: HDFC bank
2. Reserved Hardware
3. Isolate
4. Costly
5. You can access within **intranet**

Frontend: Public facing

Backend: Private facing

1. Multitenant ID: HCL, IBM, TCS, Wipro, Flipkart, Startup etc.
2. Shared Hardware
3. Isolate
4. Cheaper
5. You can access over the internet

Frontend: Public facing

Backend: Private facing

Internet: Public (User facing)

Intranet: Private

Hybrid Cloud: Remote user for example (Indian User + Foreign User)

Difference between Traditional Computing & Cloud Computing:

Cloud Computing

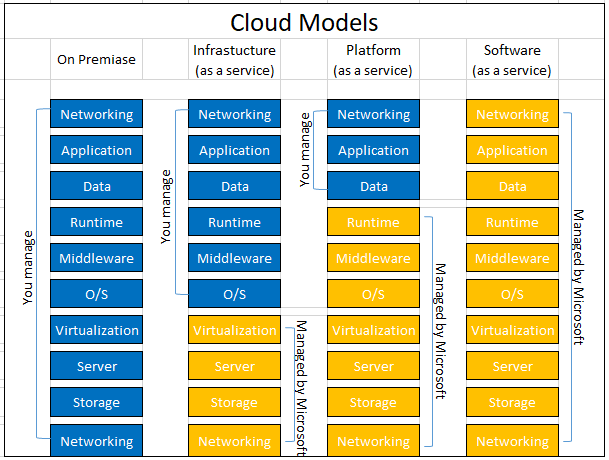
Demand Time

Traditional Computing

Demand Time

Types of Cloud Services:

1. On-premise
2. Infra as a service (IAAS)
3. Platform as a service (PAAS) : Application works like- .net, JAVA, .net, Python, PHP.
4. Software as a service (SAAS) : YouTube, Facebook, Google drive



**Resource Group:** Resource group is like a container.

1. Before creating resource group we need to organize a meeting with the client to understand his requirements.
2. During meeting with the client we need to check the latency of the server regions via azure speed test portal (<http://www.azurespeed.com>).
3. During latency check via portal we must need to choose best server region with low latency.

Processor

RAM

HDD

Graphics card

Power Supply

VM

Backup

Database

VPN

Automation

Etc.

Cabinet CPU

RG: HCL-RG

Region: Central India

1. **IP (Internet Protocol):**

The internet protocol is the network layer communications protocol, which is including the rules of the internet, its port no. 0.

(Each computer can communicate with each other through different IP if IP becomes the same for another computer so it will show “Conflict error” due to this issue both systems will get out from the network, so we can interchange the IP with each other but it can’t be same.).

Switch

Vivek

Dheeraj

Sumit

Rahul

Arun

Amit

172.168.1.1 172.168.1.2 172.168.1.3 172.168.1.4 172.168.1.5 172.168.1.6

**Types of IP:**

**IPv4 (Internet Protocol Version 4):** IPv4 address is having 32 Bits of address, having 4 octets.

4th Octet

8 Bits

3rd Octet

8 Bits

2nd Octet

8 Bits

1st Octet

8 Bits

**. 8 Bits . .**

**(32 bits)**

1. **Class A (By default 8 Bit full):** 1 Cr. Host Approx. (Enterprise Org.) /8

1 1 1 1 1 1 1 1. 0 0 0 0 0 0 0 0. 0 0 0 0 0 0 0 0. 0 0 0 0 0 0 0 0

8 Bits

**128 64 32 16 8 4 2 1**

By default subnet mask: **255.0.0.0**

1. **Class B (By default 16 Bit full):**  65535 Host Approx. (Medium Org.) /16

1 1 1 1 1 1 1 1. 1 1 1 1 1 1 1 1 1. 0 0 0 0 0 0 0 0. 0 0 0 0 0 0 0 0

16 Bits

By default subnet mask: **255.255.0.0**

1. **Class C (By default 24 Bit full):** 256 Host Approx. (Medium Org.)

1 1 1 1 1 1 1 1. 1 1 1 1 1 1 1 1. 1 1 1 1 1 1 1 1. 0 0 0 0 0 0 0 0 /24

24 Bits

By default subnet mask: **255.255.255.0**

**Loopback IP:** this is an ip of network interface card which is use to check its self ping (self-testing). Example: 127.0.0.1 it is a loopback ip.

**Dividing a Big network into a small network is called Subnetting.**

***Formula to make Subnet*:**

**Serial No. Host**

Example of Class C: IPv4…..32 Bit

Building 100 server Host (for Ex.), 100 number comes on 7th serial number

RG Name: HCL-RG

VNET: HCL-VNET01

Address space: 10.10.20.0/24 (24 Bit)

IPv4…. (32 Bit -7 = 25)

Subnet: Infra Subnet

Subnet Range: 10.10.20.0/25 (32-7=25)

**1 2**

**2 4**

**3 8**

**4 16**

**5 32**

**6 64**

**7 128**

**8 256**

**9 512**

**10 1024**

**11 2048**

Example of Class B: IPv4…..32 Bit

Building 1000 server Host (for Ex.), 1000 number comes on 10th serial number

RG Name: IBM-RG

VNET: IMB-VNET01

Address space: 192.168.0.0/16 (16 Bit)

IPv4…. (32 Bit -10 = 22)

Subnet: Web Subnet

Subnet Range: 192.168.0.0/22 (32-10=22)

**12 4096**

**13 8192**

**14 16284**

**15 32768**

**16 65536**

**VNET PEERING:** VNET Peering is working in single region (Example: Central India).

It is use to make the connection between two VM, after peering between both VM they can communicate easily.

**VNET TO VNET VPN:**

1. If two different organization or branch from two different region wants to communicate then they use VPN, data will be send in encryption form via VPN.

IBM

TCS

Public

ISP

I

File server

File server

RG: TCS-RG RG: IMB-RG

Region: Central India Region: Central US

Third party Remote Tools: Third party Remote Tools:

Not

Using

1. Ultra Viewer 1. Ultra Viewer
2. Team Viewer 2. Team Viewer
3. Any Desk 3. Any Desk
4. Amy admin 4. Amy admin

If we are using the third party remote tools:

Data will move into .txt format which is not very safe for the organization, and it will create a compliance issue. Anyone can easily access or hack the organization data. Via this data is exposed publicly, so we do not using these topology in our organization.

***VNET TO VNET VPN: (AZURE to AZURE)***

Using VPN gateway data will be transfer within organization in encrypted format, it’s very safe.

Two protocol is used: **IKEV1 (**128 Bits encryption \*\*\*\*\***) or IKEV2 (**256 Bits encryption \*\*\*\*\***).**

For production environment we are using **IKEV2** **protocol (Internet key enhancement version 2)**.

Tunnel UP Tunnel UP

VPN Gateway

File server

Server 2012

File server

Server 2012

RG: TCS-RG RG: IBM-RG

Region: Central India Region: Central US

***Steps for Both side*:** RG=> VNET=> Subnet=> gateway subnet=> VPN Gateway PIP (Public IP) with using…..=> (take 30-45 min to get provisioned on Azure) => Connection => destination VPN Gateway PIP (public IP) => pre-shared key (Both side will be same for ex: expert@123)

If both side pre-shared key will be same then tunnel will become UP and then both server will able to communicate with each other.

***Steps for VNET to VNET VPN: TWO DIFFERENT REGIONS***

1. RG: TCS-RG > REGION: CENTRAL INDIA > Virtual Network: TCS-VNET01 > ADDRESS SPACE: 172.168.1.0/24 > SUBNET NAME: INFRA-SUBNET > SUBNET RANGE: 172.168.1.0/25 > ADD GATEWAY SUBNET INSIDE SUBNET: TCS-VNET01 >>Subnet >> GATEWAY >> GATEWAY SUBNET >> Save
2. Global search >> VPN Gateway > Create VPN GATEWAY: TCS-VPN-CI-GW01 > REGION: CETNRAL INDIA > select VPN TYPE: ROUTE BASED > SKU: BASIC
3. Public address Name: TCS-VPN-CI-GW01-PIP > (TAKE 45MIN FOR PROVISONING)
4. RG: IMB-RG > REGION: CENTRAL US > Virtual network: IBM-VNET01 > ADDRESS SPACE: 172.168.20.0/24 > SUBNET NAME: INFRA-SUBNET > SUBNET RANGE: 172.168.20.0/25 > ADD GATEWAY SUBNET INSIDE Subnet: IBM-VNET01 >> Subnet >>GATEWAY >> GATEWAY SUBNET >> Save
5. Create VM >> VM NAME: TCS-VM01
6. Global search>> VPN GATEWAY >> Create VPN GATEWAY: IBM-VPN-CUS-GW01 > REGION: CENTRAL US > select VPN TYPE: ROUTE BASED > SKU: BASIC > Public address Name: IBM-VPN-CI-GW01-PIP (*TAKE 45MIN FOR PROVISONING*)
7. Create VM: IBM-VM01
8. Global search : Virtual network gateway >> IBM-VPN-CUS-GW01
9. Connection: add>> NAME: IBM-TO-TCS-VPN-CONNETION >> Connection type: VNET TO VNET >> SECOND VIRTUAL NETWORK GATEWAY >> SELECT >> TCS-VPN-CI-GW01 (select different vpn gateway) >> PRESHARED KEY: expert@123 >> IKE PROTOCOL: IKEv2

1. Global search: Virtual network gateway >> TCS-VPN-CI-GW01
2. Connection: add>> Add Connection >> NAME: TCS-TO-IBM-VPN-CONNETION >> Connection type: VNET TO VNET >> SECOND VIRTUAL NETWORK GATEWAY >> SELECT >> IBM-VPN-CUS-GW01 (select different vpn gateway) >> PRESHARED KEY: expert@123 >> IKE PROTOCOL: IKEv2

IBM-VPN-CUS-GW01 >> download VPN client >> show download folder copy it and paste on desktop >> inside the point folder >> extract here > wondowsAMD64 >> do the right click and run as administrator > yes > win + R = ncpa.cpl >> IBM-VNET01 >> connect

Win + R = %appdata% > Microsoft > network > pbk > rasphone > send to desktop >> desktop: rename as Azure VPN

Create a Folder: Point >> download Makecert.exe application via link >> download vpn & client certificate >> open certificate copy first command and open cmd >> inside cmd go to point folder and paste the copied command >> copy second command and paste>> succeeded message will be show >> now VPN & client certificate has been generated inside point folder.

Win + R = Certmgr.msc >> personal >> certificates >> right click on VPN certificate >> all tasks >> Open >> next with (no, do not export private key) >> Base -64 encoded: next >> Brows >> desktop > select point folder >> next & finish

VPN certificate >> right click and open with notepad > Copy VPN certificate from notepad (Except Begin and end) >> public certificate data > paste the copied certificate >> Name: Sumantra >> save >> Download VPN client >> move this downloaded file towards point folder on desktop >> extract here >> open windows AMD64 >> right click on VPN client setup and run as administrator >> Do you want to install >> yes

To make the connections between two VM>> Virtual network gateway >> IBM-CUS-GW01 >> Connections > add >> Name: IBM-TO-TCS-VPN-CONNECTION >> PSK: EXPERT@123 >> IKEV2 >> OK

Virtual network gateway >> TCS-CI-GW01 >> Connections > add >> Name: TCS-TO-IBM-VPN-CONNECTION >> PSK: EXPERT@123 >> IKEV2 >> OK *Now both private IP will be ping on both VM’s. turn off the firewall connections.*

**Point to Site VPN (P to S):**

For Example: Work from Home, in this scenario Point is remote location (anywhere) and site is organization/company.

Point ---------------------- Remote location

Site ----------------------- organization/Company

Below mentioned topology we can’t use in any organization due to third party remote tools, it will create a compliance issue.

Remote User (Point)

Sachin

Gurugram

Vivek

Pune

ISP

Windows Server 2012

Tally server

Aniket

Dubai

Gaurav

France

Microsoft Azure (Site) TXT format (abcd123)

Not

Using

Third party Remote Tools: Third party Remote Tools:

1. Ultra Viewer 1. Ultra Viewer
2. Team Viewer 2. Team Viewer
3. Any Desk 3. Any Desk
4. Amy admin 4. Amy admin

***Below mentioned topology shall be used for P to S: (eg: Work from Home user)***

Remote User (Point)

Organization(Site)

Rahul

Tally server

Private IP: Enable

Public IP: Disable

Dheeraj

VPN Gateway

Swapnil

Sumit

**SSTP Protocol**

(Secure socket tunneling Protocol)

Root Certificate

Upload, Download VPN client

For example: a work from home user can access the server with the help of VPN.

Download VPN client and install it, using makecert application needs to be generate root certificate, Client certificate.

**Steps for Point to site VPN: steps Ahead from P to P VPN**

1. Virtual network gateway>> IBM>> Address pool: 182.168.200.0/24 choose different ip which is not is being used inside the network
2. Copy VPN certificate from notepad (Except Begin and end) >> public certificate data > paste the copied certificate >> Name: Sumantra >> save >> Download VPN client >> move this downloaded file towards point folder on desktop >> extract here >> open windows AMD64 >> right click on VPN client setup and run as administrator >> Do you want to install >> yes
3. Win + R = ncpa.cpl >> IBM-VNET01 >> Connect >> Connected
4. Win + R =% appdata% >> network >> connections >> rasphone : right click and send to desktop >> Rename as Azure VPN

**Network Security Group (NSG):- Firewall related**

Network security group is working on firewall protection like inbound & outbound rules.

It has two types’ inbound rule and outbound rule.

If we want to enter any organization we will reach first to the receptionist then she will check our authority if we are an authorized person then she will allow going inside otherwise for the unauthorized person she will deny entering the organization, and the same function will go through with NSG.

TCS Noida (For example)

Reception

OFFICE PREMISE

By default allow

By default deny

OUT

IN

*Rules*:

In this inbound rule anyone can take the server on remote from anywhere.

Rule 1 Source: Any Destination: Any Port No: 3389 Port name: RDP Action: Allow

In this inbound rule no one can take the server on remote from anywhere

For Webserver etc.

Rule 2 Source: Any Destination: Any Port No: 3389 Port name: RDP Action: Deny

In this inbound rule any particular user can take the server on remote from anywhere so we need to add his public-IPv4 in the RDP rule.

For example: 47.9.77.255

Rule 3 Source: Public IP Destination: Any Port No: 3389 Port name: RDP Action: Allow

Rule 4 Source: Public IP (M) Destination: Any Port No: 3389 Port name: RDP Action: Allow

In this inbound rule multiple user can take the server on remote from anywhere so we need to add his public-IPv4 using comma in the RDP rule.

For example: 47.9.77.255, 103.89.59.160

Rule 5 Source: Any Destination: Any Port No: 80, 443 Port name: HTTP, HTTPS Action: Deny

In this outbound rule we need to block the internet inside the server desktop

Internet\_block

In this outbound rule we need to allow the internet inside the server desktop

Internet\_unblocked

Rule 6 Source: Any Destination: Any Port No: 80, 443 Port name: HTTP, HTTPS Action: Allow

**Site to Site VPN (S to S): (AZURE to On-premise)**

To make tunnel (for communication) between which is two different organization: Azures clouds to On-premise using site to site VPN.

In site to site VPN two team is involving:

1. On premise team (Organization/Company)
2. Cloud team (Azure)

Local public IP Local subnet range, PSK

Shared

RG VNET Subnet GW Subnet VPN GW Local Network Gateway Local Public IP and local subnet range PSK key: vpn@123

VPN Gateway

On premise Site

(VPN Gateway public ip, VNET, PSK-vpn@123)

Shared

* Before initiating site to site VPN we need to refer below documents via portal which is related with the different firewall guidelines. <https://www.docs.microsoft.com>

***Steps for Site to Site VPN: (For example sonic wall firewall)***

(How to configure VPN between Sonic wall firewall and Microsoft Azure)

1. Login to <https://www.portal.azure.com>
2. Resource Group
3. Vnet
4. Gateway Subnet
5. Public IP
6. Sonic-wall will share his LAN Subnet range and his public IP with the Azure
7. Virtual Network Gateway with PIP …………….(Take 45 min to provisioning)
8. Virtual Network Gateway >> Connection >> Add >> Name: Azure-SNWL >> choose Connection Type >> site to site(IPsec) >> Local network gateway
9. Local network gateway >> Name: SNWL >> ip address (on premise firewall public IP) >> address space >> ip range (on premise address space range)
10. Preshared key (PSk) : vpn@123

We need to share article which is recommended by Microsoft Azure <https://www.portal.azure.com> to on premise firewall engineer.

**Azure Automation: Scheduler** (On demand service pay as you go)

Inside this service, backend servers using scheduler it will be turned off and turned on automatically as per the selected time this is called azure automation. For example, a digital library of a college I need to turn it on from Monday to Friday between 10 am to 05 pm hence we required like “Azure automation” service.

Front end : Public facing applications Backend : Private facing applications

For example: I need to deploy azure automation for a tally server for backend users. These parameters needs to be asked by organization.

Working days : Monday to Friday = 5 days

Non-working days : Saturday & Sunday

Tally server

Working Hours : 09:00 am to 05:00 pm = 10 hours

Buffer time : 05 pm to 07 pm

Non-working hours : 07pm to 09:00 am

Calculation for automation hours : 30days x 08hours = 240 hours Calculation for 24x7 hours: 30days x 24 hr. =720 hours

***Steps for Azure Automation:***

1. Create Resource group
2. Create VNET
3. Create VM
4. Global search: Automation Accounts >> run book >> using graphical power shell import and publish the rule
5. Process automation >> stop and start rule with scheduler time
6. Needs to be set parameter and run setting
7. Azure automation is ready to run.

**Virtual Machine (Theory):**

|  |  |
| --- | --- |
| **Windows** | **Linux** |
| 1. Network OS: server 2012, server 2016, server 2022 2. Client OS: Windows 10 and Windows 11 3. RDP (Remote Desktop Protocol) 4. RDP Port No:3389 5. Windows + R >> mstsc >> IP >> user name and password 6. Gallery Image | 1. Network OS: Red hat Linux and SUSE Linux 2. Client OS: Ubuntu and Centos 3. SSH (Secure Shell) 4. SSH port no: 22 5. Putty download >> IP >> port 22 >> username and password 6. Gallery Image |
| 1. Username : admin, administrator and root | 1. Username : admin, administrator and root |

Username for: during VM building for windows and Linux, we can’t choose admin, administrator and root.

***Steps for VM (Windows and Linux):***

**Widows VM:**

1. Create VM >> crate: RG HCL-RG >> choose region >> HCL-WINDOWSVM01 >>choose image (Widows 2012 R2 datacenter)
2. Set username and password for VM >> Review and create
3. Win + R= mstsc >> paste public IP >> enter username and password >> VM opened

**Linux VM:**

1. Create VM : choose RG: HCL-RG >> choose region >> HCL-LINUXVM01 >> choose image >> Red hat >> select Red hat enterprise Linux 7.8 Gen 1 >> size : standard\_B1s >> Review and create
2. Download and install putty latest version in your laptop
3. Hostname IP >> paste the public IP of VM >> select port 22 >> select SSH
4. Enter Username and password >> VM opened >> ifconfig command to check IP.

**VM Disk:**

1. OS Disk : OS Files max size 2 TB : Chargeable
2. Temp Disk : Testing purpose : Non-Chargeable
3. Data Disk : MAX size 32 TB : Chargeable

Microsoft is recommended that don’t save your personal data inside the temp disk, if you store the data inside the temp disk and server will become reboot then data will be lost and Microsoft will not be responsible for this.

If consumer wants to save your personal data then Microsoft is recommended that needs to attached Data disk and then save your personal data inside the Data disk.

MBR (Master Boot record) : Max 2 TB partition are possible **GPT (Guide partition table)** : Max 32 TB partition are possible

***Steps for DATA Disk addition:***

***Scenario 1:***

1. Create RG >> HCL-RG , Region : Central India >> Create Vnet >> Create VM >> HCL-FILEVM01
2. Disk: Standard HDD >> Create VM >> MSTSC >> Open VM desktop
3. Virtual Machine >> HCL-FILEVM01 >> Disk >> Create attach a new disk >> Disk name: HCL-FILEVM01-DATA-DISK01 (Data disk) >> Storage type: standard HDD >>Size (32 GB to 32767) : 500 GB >> Save
4. LUN (Logical unit Number) :
5. Go to VM desktop : Win+R : diskmgmt.msc >> **Select GPT Option**
6. Disk 2: select and right click >> New simple volume > next > next > finish
7. New volume has been attached with the VM desktop

***Scenario 2:***

1. Go to inside VM: HCL-FILEVM01 >> Disk > Create and attach a new disk (You can add new volume)
2. Global search : Disks >> Create >> disk name : HCL-FILEVM01-DATA-DISK02 (Data disk)
3. Size : change size >> Custom size disk >> Disk SKU: Standard HDD >> select 64 GB (As per requirement) >> ok >> review create
4. Disk has been created but needs to be attached with VM
5. Go to resource >> HCL-FILEVM01 >> Attach existing disk > refresh if option not showing > HCL-FILEVM01-DATA-DISK02 > save
6. Go to VM desktop : Win+R : diskmgmt.msc >> **Select GPT Option**
7. Disk 3 : select and right click >> Go to VM desktop : Win+R : diskmgmt.msc >> **Select GPT Option**
8. Disk 3: select and right click >> New simple volume > next > next > finish (Steps to make partition)
9. Check inside the VM desktop new volume of 64 GB has been attached.

***If disk volume 64 GB has been full then below steps for the Volume increase***

***(Without Downtime): consumer are not giving any downtime***

1. HCLFILEVM01 >> HCL-FILEVM01-DATA-DISK02 >
2. size + performance > Message: changes to the disk size can be made only when the **disk is unattached** or the managing virtual machines are **deallocated**
3. If we are not getting approval from customer side then we go to the disk unattached process
4. HCL-FILEVM01-DATA-DISK02 > click on X (delete the existing disk) > save
5. HCLFILEVM01 >> HCL-FILEVM01-DATA-DISK02 > size + performance > Disk SKU > Standard HDD > select 128 GB > resize
6. Go to VM : HCL-FILEVM01 >> disk >> attached existing disk >> select in Disk name: HCL-FILEVM01-DATA-DISK02 > save
7. Go to VM desktop : Win+R : diskmgmt.msc >> **Select GPT Option**
8. Disk 3: select and right click >> Extend volume > next > finish
9. Disk 3 : Disk volume has been increased as 127 GB

***If disk volume 64 GB has been full then below steps for the Volume increase***

***(With Downtime): consumer are giving any downtime to us***

1. HCLFILEVM01 >> click on Stop (To stop the VM)
2. HCLFILEVM01 >> Disks >> HCL-FILEVM01-DATA-DISK02 >> size + performance >> Disk SKU > Standard HDD > select 1024 GB > resize
3. HCLFILEVM01 >> click to Start (To start the VM)
4. Go to VM desktop : Win+R = diskmgmt.msc >> **Select GPT Option**
5. Disk 3: select and right click >> Extend volume > next > finish
6. Disk 3 : Disk volume has been increased as 127 GB

**Snapshot:**

Snapshot is a process that is used to install all software from the existing VM to the new VMs.

1. Go to VM desktop: WIN + R = appwiz.cpl (program & features) to check program list and in this section we can install and uninstall the applications and software’s. (install some software’s or applications, for example: Chrome, notepad ++)
2. VM: HCLFILEVM01 >> Disk: click on disk name: create snapshot: HCL-FILEVM01-SNAPSHOT01-BASIC-SOFTWARE
3. Storage type : standard HDD > review create
4. HCL-FILEVM01-SNAPSHOT01-BASIC-SOFTWARE >> Create disk >> disk name: HCL-FILEVM02-OS-DISK >> Size: create > disk SKU: standard HDD >> select 128 GB > ok > Review + create
5. HCL-FILEVM02-OS-DISK >> create VM >> VM name: HCL-FILEVM02 >> image : HCL-FILEVM02-OS-DISK-Gen2 >>(It will not asking about username and password because it will be same as previous VM: HCLFILEVM01) >> Next Disk >> next >> create (VM has been build)
6. MSTSC >> copy public IP from VM: HCL-FILEVM02 paste >> username and password will be same which was used in VM: HCLFILEVM01
7. VM desktop opened >> appwiz.cpl >> same applications and software’s are available as present in previous VM.

**Antivirus:**

Inside the VM: HCLFILEVM01 => Extension and application

1. Extension and application >> add >> search >> find the Microsoft antimalware > click and next
2. Don’t need to choose third party antivirus software, only add Microsoft antimalware software
3. VM: HCLFILEVM01 >> copy public IP and access the server VM desktop
4. Search or scroll down and find: System center endpoint protection >> click >> error: your system administrator has restricted access to the app.
5. Open Windows PowerShell : run as administrator >> paste the script command > enter > after this step registry value will become zero 0 ($value =”0”) 
6. Now we can able to open: System center endpoint protection (It is an antimalware).
7. We need to enable System center endpoint protection on each server for server.

***If we forgot the User name and password of the VM.*** Protection

Inside the VM: HCLFILEVM01 => Export template (Inside the Automation section)

1. Export template >> Scroll down and check OSprofile : adminUsername: “fileadmin01”
2. Copy username and go to VM: HCLFILEVM01 >> Reset password >> paste user name and choose password by yourself >> update
3. MSTSC >> copy public IP and access the server VM desktop

IMP Note: Never shut down the server VM desktop directly from the server desktop, charges will be applicable until and unless we will not shut it down from the azure portal: Stop VM = “Stopped deallocated” will be showing then VM will be off.

**Load Balancer**

Load balancer is use to distribute the traffic equally, we are taking example of two VM’s, during maintenance, patch update or due to hardware failure if one VM gets down then all traffic will be shifted towards the second VM with the help of load balancer. Inside the load balancer we are using the Availability sets.

**Availability sets:**

We are using the Availability sets where servers/VM are running in 24\*7 for the critical servers.

Example: web server, data base server,

When we are making a new VM then we need to attach with the availability set with the VM, once we have make the VM then we could not attach the availability set. Minimum two VM’s required when we are going to attach the availability set then it will work.

Inside the availability sets it has two types of Domain……

1. Fault Domain : Hardware Failure : No of Rack [ 0 1 2 ]
2. Update Domain : Patch management : No of VM [ 1 2 3…..20]

We need to choose minimum ……………………………….. : No of fault domains : 2

: No of Update domains : 2

Tower1 Tower2 Tower3

Rack1 Rack2 Rack3

**WEB-VM1**

**WEB-VM1**

**WEB-VM1**

**WEB-VM2**

**WEB-VM2**

**WEB-VM2**

In the above scenario we have choose 3 Racks and two VM’s, if any rack or any VM will gets down due to patch update/during maintenance/during dust clearance, then traffic will move towards the another VM, Hence applications/ server will be in UP stage.

Microsoft is providing 99.95% SLA (Service level agreement)

Architecture of Public load balancer:

HCL-RG

PUBLIC LOAD BALANCER

Load Balancer

BACKEND POOL

HCL-WEB02

HCL-WEB01

AVAILABILITY SET

HCL-FRONTEND-SUBNET

HCL-VNET01

***Steps for Availability set and Public load balancer:***

1. RG :FLIPKART-RG >> Region :Central India >> VNET :FLIPKART-VNET01 >> Address space: 10.0.0.0/24 >> FLIPKART-FRONTEND-SUBNET >> 10.0.0.0/24
2. Global search :Availability sets >> create >> Name :FLIPKART-WEB-AVSET >> Fault domains : select 2 >> Update domain :select 2 >> Review and create
3. Create VM: **FLIP-WEB01** >> Availability option :select availability sets >> availability set : select existing FLIPKART-WEB-AVSET >> Disk: Standard HDD >> Select VNET in Networking >> Select inbound ports : select HTTP(80), HTTPS(443) & RDP(3389) >> Create
4. Create VM: **FLIP-WEB02** >> Availability option :select availability sets >> availability set : select existing FLIPKART-WEB-AVSET >> Disk: Standard HDD >> Select VNET in Networking >> Select inbound ports : select HTTP(80), HTTPS(443) & RDP(3389) >> Create
5. VM: FLIP-**WEB01** >> Win + R = mstsc >> Open VM desktop >> open server manager >> IE >> off >> manage >> add roles and features >> next >> select Role based and feature based installation >> next >> select web server(IIS) (Internet information service) >> next >> Install
6. VM: FLIP-**WEB02** >> Win + R = mstsc >> Open VM desktop >> open server manager >> IE >> off >> manage >> add roles and features >> next >> select Role based and feature based installation >> next >> select web server(IIS) (Internet information service) >> next >> Install
7. FLIP-WEB01 desktop **:**Go to google.com and search >> HTML template download >> select klassy café and download >> extract to all >> klassy-café >> templatemo\_558\_klassy\_cafe >> cut this folder>> go to C drive >> inetpub >> wwwroot >> paste this folder (templatemo\_558\_klassy\_cafe)
8. Do this steps for both VM (Step 7)
9. VM desktop :FLIP-WEB01 >> Win + R= inetmgr >> select :FLIP-WEB01 and extract for more option >> site : right click >> add website >> site name: flipkart >> select : C drive >> inetpub > wwwroot > select folder : templatemo\_558\_klassy\_cafe >ok > IP address: select private IP (10.0.0.4) > type: HTTP > ok
10. Right click on flipkart or select: brows (10.0.0.4.80(http) > click > now website is running via IP
11. FLIP-WEB02 desktop >> win down arrow >> internet information service > no > select :FLIP-WEB01 and extract for more option >> site : right click >> add website >> site name: flipkart >> select : C drive >> inetpub > wwwroot > select folder : templatemo\_558\_klassy\_cafe >ok > IP address: select private IP (10.0.0.4) > type: HTTP > ok
12. Right click on flipkart or select: brows (10.0.0.4.80(http) > click > now website is running via IP

Now I need to access this website publicly

1. Load balancer >> select Load balancer >> create >> RG: select FLIPKART-RG >> Name: FLIPKART-PUBLIC-LBN >> sku : Basic (for practice) >> type : public
2. SKU: 1. Standard : Payed : we can run HTTP, HTTPS websites : will get SLA

2. Gateway : Within organization through VPN gateway

3. Basic : Free : we can’t run HTTPS websites : will not get SLA

1. Frontend IP configuration : add >> Name : FLIPKART-FRONTEND-PIP >> Choose IPv6 >> public IP address : Name : FLIPKART-FRONTEND-PIP >> Assignment : Static > ok
2. Backend pool >> add >> FLIPKART-FRONTEND-PIP >> select virtual network: FLIPKART-VNET01 >> associated to : select virtual machines >> IPv4 >> add >> select all, both virtual machined >> add >> select all VM’s >> add
3. Inbound rule >> add load balancing rule >> FLIPKART-LBN-RULE >> IPv4 >> frontend IP address >> select FLIPKART-FRONTEND-PIP >> select FLIPKART BACKENDPOOL >> Protocol : TCP >> port : 80 >> backend port : 80 >> health probe: create new >> Name : FLIPKART-FRONTEND-PIP >> protocol : HTTP > Port : 80 >> interval : 5 seconds >> unhealthy threshold : 2 >> ok
4. Review + create >> create
5. FLIPKART-PUBLIC-PIP >> frontend IP configuration : copy the public IP and pate on browser >> now we are able to access the website publicly

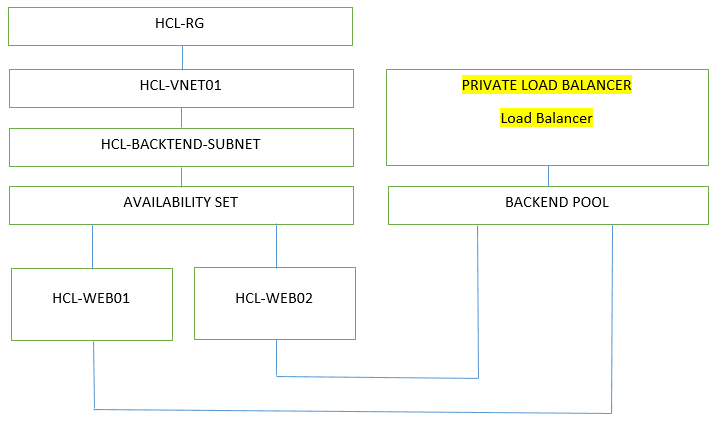
For domain creation:

1. Godaddy.com >> primes.xyz >> search >> select cheaper domain >> pay and purchase >> no thanks >> no domain protection >> continue to cart >> select for one year >> continue with Google >> Gmail id : sign in >> pay >> Verify the email
2. Accounts >> my products >> domains : DNS >> copy primes.xyz
3. FLIP-WEB01 desktop >> Win + R= inetmgr >> FLIP-WEB01 >> flipkart >> right click >> edit bindings >> select > edit > Hostname : primes.xyz >> ok
4. FLIP-WEB01 desktop >> Win + R= inetmgr >> FLIP-WEB01 >> flipkart >> right click >> edit bindings >> select > edit > Hostname : primes.xyz >> ok

Site will not be accessible through IP publicly because DNS entry is pending in Godaddy website

1. Accounts >> my products >> domains : DNS >> add >> type : A >> value : paste IP of load balancer >> TTL : ½ hour >> Name : primes.xyz >> add record >> yes: save >> success
2. DNS Checker search in browser >> type domain name and search >> when domain name will propagate for all country then website will be accessible (primes.xyz).

Architecture of Private load balancer:



HDFC BANK NOIDA

JUMP SERVER

***Steps for Private Load Balancer:***

1. Create RG: HDFC-BANK-RG >> India Region >> VNET: HDFC-BANK-VNET01 >> IP address: 10.0.0.0/24 >> subnet name : HDFC-BANK-BACKENDSUBNET01 >> range: 10.0.0.0/25 >> add
2. Global search : availability sets >> create >> Name: HDFC-BANK-AVSET >> region : Central India >> fault domains : select 2 >> update domain : select 2 >> review create
3. VM : **HDFC-P-WEB01** >> Availability option : Availability set >> Availability set : HDFC-BANK-AVSET >> disk: standard HDD >> select inbound ports : HTTP(80), HTTPS (443), RDP (3389)
4. VM : **HDFC-P-WEB02** >> Availability option : Availability set >> Availability set : HDFC-BANK-AVSET >> disk: standard HDD >> select inbound ports : HTTP(80), HTTPS (443), RDP (3389)
5. HDFC-P-WEB01 >> Win + R = mstsc >> Open VM desktop >> open server manager >> IE >> off >> manage >> add roles and features >> next >> select Role based and feature based installation >> next >> select web server(IIS) (Internet information service) >> next >> Install
6. HDFC-P-WEB02 >> Win + R = mstsc >> Open VM desktop >> open server manager >> IE >> off >> manage >> add roles and features >> next >> select Role based and feature based installation >> next >> select web server(IIS) (Internet information service) >> next >> Install
7. HDFC-P-WEB01 Desktop >> Go to google.com and search >> HTML template download >> select klassy café and download >> extract to all >> klassy-café >> templatemo\_558\_klassy\_cafe >> Rename as Bank >> cut this folder>> go to C drive >> inetpub >> wwwroot >> paste this folder (Bank)
8. VM desktop : HDFC-P-WEB01 >> Win + R= inetmgr >> select :HDFC-P-WEB01 and extract for more option >> site : right click >> add website >> site name: hdfc >> select : C drive >> inetpub > wwwroot > select folder : Bank > ok > IP address: select private IP (10.0.0.5) > type: HTTP > ok
9. Right click on hdfc or select: brows (10.0.0.5.80(http) > click > now website is running via IP
10. VM desktop : HDFC-P-WEB02 >> Win + R= inetmgr >> select :HDFC-P-WEB01 and extract for more option >> site : right click >> add website >> site name: hdfc >> select : C drive >> inetpub > wwwroot > select folder : Bank > ok > IP address: select private IP (10.0.0.5) > type: HTTP > ok
11. Right click on hdfc or select: brows (10.0.0.5.80(http) > click > now website is running via IP

Now we need to create one more VM which is called Jump server it could be only use as a private server.

1. VM: create >> VM name : HDFC-JUMP01 >> Disk : Standard HDD >> review create

**Create Load balancer:**

1. Load balancer : create >> Name: HDFC-PRIVATE-LBN01 >> SKU : Basic >> type : internal
2. Add Frontend IP configuration >> Name : HDFC-FRONTEND-IP >> Subnet : select VNET >> assignment : Static >> IP address : 10.0.0.10 >> ok
3. Backend pools : Add >> Name : HDFC-BACKENDENDPOOL >> subnet >> Associated to : Virtual machine >> IPv4 >> VM : add >> select HDFC-P-WEB01 & HDFC-P-WEB02 don’t select jump server >> add >> select all >> add
4. Inbound rule : add >> Name : HDFC-LBN-RULE >> IPv4 >> Frontend IP : select HDFC-FRONTEND-IP (10.0.0.10) >> Backend pool >> HDFC-BACKENDPOOL >> Protocol : TCP >> Port : 80 >> Backend port : 80 >> health probe >> Name: HDFC-LBN-HEALTHPROBE >> Protocol : HTTP >> interval : 5 seconds > unhealthy threshold : 2 > ok >> review create
5. HDFC-PRIVATE-LBN01 >> Frontend IP configuration >> copy ip address
6. With this private IP we can’t access the bank website right now.
7. VM: HDFC-JUMP01 >> access HDFC-JUMP01 desktop
8. VM: HDFC-P-WEB01 >> Networking > network interface : select and click >> IP configuration >> select and open IP config1 > public IP address : disable
9. VM: HDFC-P-WEB02 >> Networking > network interface : select and click >> IP configuration >> select and open IP config1 > public IP address : disassociate > save
10. VM: HDFC-JUMP01 >> access HDFC-JUMP01 desktop >> open server manger >> local server >> IE off >> open browser >> type the IP of Load balancer (10.0.0.10).

Now the bank employee can access the website through the load balancer IP via Jump server. Bank employees does not have the access of the web server01&02 both only application team is having those access.

BANK

AZURE

Bank Emp.1

HDFC-WEB01

**LOAD BALANCER**

Bank Emp.2

HDFC-WEB02

**VPN**

Bank Emp.3

JUMP SERVER

**IIS SERVER MIGRATION**

(IIS: Internet server migration)

With the help of IIS server migration, we can migrate complete data (Applications, websites, etc.) from the old version to the latest version which is present in the existing VM desktop. For the server migration, we are using *Web Deployment 3.0 tool*.

Web Deploy 3.0 Web Deploy 3.0

Export file package Import file package

Azure

SERVER 2012

IIS

FLIPKART

IIS WEB SERVER

Server 2012

On-Premise

ISP

Jio

Airtel

Year 2019 Year 2022

Xeon Processor 11th Generation

(Old generation) (New Generation)

In the above mentioned scenario if On-premise server is connected with the two ISP’s if they both get down then server will not be isolated because Microsoft Azure is providing free internet to their server.

***Steps for IIS Server Migration:***

1. RG: ONPREMISE >> Region: Central India
2. RG: Azure >> Region: Central India
3. VM >> Name : ONPREMISE-VM >> User name: onpremiseadmin01 >> Disk: Standard HDD
4. VM >> Name : AZURE-WEB-VM01 >> User name: azurewebadmin01 >> Disk: Standard HDD
5. VM Desktop: ONPREMISE-VM >> open server manager >> IE >> off >> manage >> add roles and features >> next >> select Role based and feature based installation >> next >> select web server(IIS) (Internet information service) >> next >> Install
6. ONPREMISE-VM desktop >>Go to google.com and search >> HTML template download >> select klassy café and download >> extract to all >> klassy-café >> templatemo\_558\_klassy\_cafe >> Rename as Bank >> cut this folder>> go to C drive >> inetpub >> wwwroot >> paste this folder
7. ONPREMISE-VM desktop >> Win + R= inetmgr >> select :HDFC-P-WEB01 and extract for more option >> site : right click >> add website >> site name: klassy-cafe >> select : C drive >> inetpub > wwwroot > select folder : Bank > ok > IP address: select private IP (10.0.0.4) > type: HTTP > ok
8. Right click on klassy-cafe or select: brows (10.0.0.4.80(http) > click > now website is running via IP
9. Copy Web Deploy tool 3.0 and paste on ONPREMISE-VM desktop >> run
10. ONPREMISE-VM desktop >> Win + R= inetmgr >> select : ONPREMISE-VM and extract for more option >> site : klassy-café >> right click >> deploy : Export application > next > brows : choose path in desktop folder > Name: migration\_web\_export > save > next > the package was created successfully > finish

>>>>> Copy migration folder & web deploy 3.0 application

1. VM Desktop: AZURE-WEB-VM01 >> open server manager >> IE >> off >> manage >> add roles and features >> next >> select Role based and feature based installation >> next >> select web server(IIS) (Internet information service) >> next >> Install
2. Paste on Desktop: AZURE-WEB-VM01 >> migration folder & web deploy 3.0 application
3. Install web deploy 3.0
4. Copy migration folder and paste inside inetpub folder (wwwroot) don’t extract this folder
5. AZURE-WEB-VM01 desktop >> Win + R= inetmgr >> select: AZURE-WEB-VM01 and extract for more option >> site: and right click >> deploy > import server or site package > brows: C drive: inetpub: wwwroot: select migration\_web\_export > next > finish.
6. Right click on klassy-cafe or select: brows (10.0.0.4.80(http) > click > now website is running via IP

Now complete package has been migrated successfully from On-premise to Azure.

**TRAFFIC MANAGER**

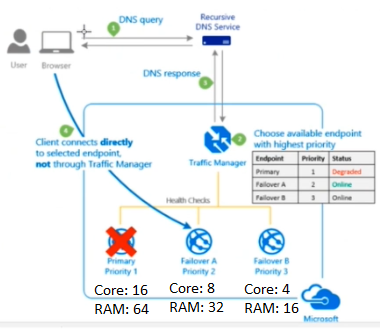
Traffic manager is use to Distribute the Tracing inside the Geographic location, it is also works like disaster recovery. IT is a part of a Load balancer.

We can see below mentioned diagram traffic manager is distributing traffic for both region (Central India & Central US). If one region is gets down due to some disaster then traffic manager will move the traffic towards the second region. Then user will go through the traffic manager and traffic manager will give a path of the second region.

Both region is called endpoint. Traffic manager is having **3 different routing method**.

Routing Methods:

1. Priority Traffic-Routing Method
2. Weighted Traffic-Routing Method
3. Performance Traffic-Routing Method
4. Priority Traffic-Routing Method:



Inside the priority routing method, it has 3 different priorities with different Core and RAM sizes.

When we type any website inside the browser (For example www.flipkat.com) the request will go to the DNS server first then it will transfer towards the traffic manager then the traffic manager will checking server’s health of the lower value like priority 1 and then it will route the traffic towards the priority 1, if during health check of priority one is found that it is in downstage then traffic manager will route the traffic towards the second priority by checking its health.

Configuring the Endpoints:

With the Azure resource manager you configure the endpoint priority specially using the priority property of each endpoint. **This property is a value between 1 and 1000 lower value represent a higher priority**. Endpoints can’t share priority values.

**DNS**

The Domain Name System (**DNS**) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com.

**Root Server**

**Hidden dot**

WWW.FLIPKART.COM.

**TLD .COM .IN .UK .GOV.IN .CO.IN .PK .AC.IN**

**TLD (Top Level Domain)**

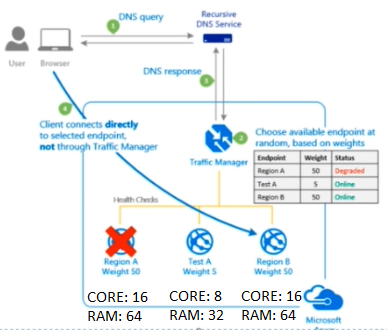
**Domain Name**

**Hostname**

**HOSTNAME + DOMAIN NAME = FQDN**

**FULLY QAULIFIED DOMAIN NAME**

1. Weighted Traffic-Routing Method:

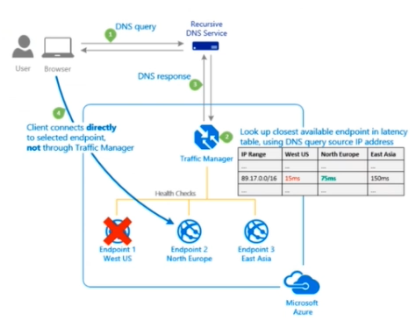


When we search any website in the browser then request will go to DNS server and then it will forwards towards the Traffic Manager and then Traffic manager will distribute the traffic (50%-50%) towards the both server which have same weight, 50% traffic will move to the weight 50 and rest 50% traffic will move to the second weight 50. Traffic will balanced.

If Region A will gets down during any disaster then Traffic Manager will move the Traffic towards region B, if region B will get down then traffic will move towards the weight 5.

1. Performance Traffic-Routing Method:

It is more popular method which is use in production environment which works on **Lower latency**.



When we search any website (for example <http://www.underarmour.com>) in the browser then request will go to DNS server and then it will forwards towards the Traffic Manager and then Traffic manager will check where user is present if user is in India then Traffic manager will transfer the traffic towards the Asia region. If user is present in the Canada or US then Traffic manager will move the traffic towards the US region. If user is present in the France then Traffic manager will transfer the traffic towards the North Europe.

It means Traffic manager is checking that user is present on which location and then it will move the traffic towards its nearby reason then **website will be more responsive**.

***Steps for Performance Traffic-Routing Method:***

1. Create VM 1: RG: UNDER-ARMOUR-RG-INDIA >> VM Name: UA-WEB01-CI > region : Central India > User name: webadmin01 > inbound port rule > HTTP,HTTPS,RDP
2. Create VM 2: RG: UNDER-ARMOUR-RG-CUS >> VM Name: UA-WEB01-CUS > region : Central US > user name: webadmin01 > inbound port rule > HTTP,HTTPS,RDP
3. Login both VM desktop and install IIS rule
4. Go to VM Desktop 1: C Drive > inetpub > wwwroot > double click on : iis-85 >> type INDIA
5. Go to VM Desktop 1: C Drive > inetpub > wwwroot > double click on : iis-85 >> type SCUS
6. Load Balancer : Traffic Manager >> create > Name: underarmour > routing method : performance > RG: UNDER-ARMOUR-RG-INDIA > Create
7. Load Balancer : Traffic Manager >> underarmour >> configuration
8. Load Balancer : Traffic Manager >> Endpoint > add > target source : Public IP Address > choose one IP >> Error : No DNS name is configured
9. VM 1: UA-WEB01-CI > click on public IP > DNS Name: Indians > dynamic > save
10. VM 1: UA-WEB01-CUS > click on public IP > DNS Name: usdns > dynamic > save
11. Load Balancer : Traffic Manager >> Endpoint > add > Name: India > target source : Public IP Address > choose IP of India VM : UA-WEB01-CI (20.9.3.39 for example) > add
12. Load Balancer : Traffic Manager >> Endpoint > add > Name: US > target source : Public IP Address > choose IP of India VM : UA-WEB01-CUS (40.3.5.49 for example) > add
13. Load Balancer: Traffic Manager >> Overview > Copy DNS name: https…….

Now website is running and inside the website India region is showing

If we shutdown India Vm or due to any disaster VM1 is stopped then Traffic manager will move the traffic towards the US region and then inside the website US region will show. It is taking 60 second time.

**AZURE STORAGE**

Microsoft Azure storage is a Microsoft-managed cloud service that provides storage that is highly available, **secure, durable, scalable, and redundant**. We are using Azure storage so that any malware or any virus can’t attack the data.

Azure storage consists of three data services: Blob storage, File storage, and Queue storage.

Container (Folder)

Blob Storage

Azure Storage

**Blob storage:**

Azure Blob storage is a service for storing large amounts of unstructured object data, such as text or binary data, that can be accessed from anywhere in the world via HTTP or HTTPS. You can use Blob storage to expose data publicly to the world, or to store application data privately.

**Containers: (Folder)**

A container organizes a set of blobs, similar to a directory in a file system. A storage accounts can includes an unlimited numbers of containers, and a container can store an unlimited number of blobs.

Blob Storage Max size : **500 TB**

Block Blob Max size : **4.7TB**

**Page Blob:**

Page Blob store random access file up to **8 TB** in size. Page blobs store virtual hard drive (VHD).

Azure storage offers different access tiers, which allow you to store Blob object data in the most **Cost-effective manner.**

The available access tiers includes:

1. **Hot** – The cheapest to access, but the most expensive to store.

When we mark the storage or the blob files as Hot it means we want these files **frequently accessible**. The data stored in these types of storage are always readily available. In case these files are not being accessed frequently you may end up paying more than expected for the files that are not been accessed as much as it should.

DATA ACCESS

DATA STORAGE

Chargeable No charge

* Access Frequency – High
* Storage Cost – Higher
* Access Cost – Lower

1. **COOL** – Medium Price storage, but expensive to access.

We are taking about those files or storage that are **not accessed frequently**. Let’s taken an example of a file that summaries your system performance once a month and store it. These type of files you want to access once a while. With this type of storage you pay slightly less for storing but pay more for retrieving the files.

For Example: we are using COOL storage for the Performance & Increment related which are accessible in yearly only.

DATA STORAGE

DATA ACCESS

Downloading

No Charge Chargeable

* Access Frequency – Low
* Storage Cost – Lower
* Access Cost – Higher

**AZURE FILE SHARE**

Azure files offers fully managed file shares in the cloud that are accessible via the industry standard **server massage block (SMB) protocol** (also known as common Internet file system or CIFS). **SMB Port No. 445**

Max size : **5 TB**

ONPREMISE server Infrastructure

Router

**FILE SERVER**

**SERVER 2019**

**SALES**

**HR**

**IT**

In the above On-premise server infrastructure all users are connected with the File server via the router and switches, but due to any disaster or cable issue, router failure, switch failure all users will be disconnected with the server and our data will be lost. So that we are not using such type of topology. We are using Azure file share service to avoid this.

User B

User C

User D

User A

FILE SHARE MAX 5 TB

AZURE STORAGE

**SMB Port No. 445**

* **Enable**

ISP (SMB Port No. 445 Enable)

Storage Replication:

1. LRS (Locally Redundant Storage): It is working in the single region. In the LR storage data will be in 3 copies with 3 different Rack/Tower, due to DR (disaster recovery) 1st copy is become down then Microsoft automatically maintaining the 3 copies and along with copy 2 & copy 3, if DR is coming whole region then Microsoft Azure will not be responsible for the SLA (Service level Agreement).

2nd Copy

Rack/Tower 2

3rd Copy

Rack/Tower 3

1st Copy

Rack/Tower 1

Single Region: Central India

1. GRS (Globally Redundant Storage): It is working in the dual region, in the GR Storage data will be available in 6 copies, 3 copies in primary region and 3 copies in secondary region.

If Tower 1 has been demolished due to some reason then tower 2 and tower 3 will be up and data will be high level available, if DR (Disaster Recovery) is coming to whole primary region then data will be high level available to the second Region. Always 6 copies will be available at any cost Microsoft Azure will make it that after any tower down, until and unless both regions will not be getting down.

Microsoft Azure is providing **99.95% SLA** for the GR storage.

Tower1 Tower 2 Tower 3 Tower 1 Tower 2 Tower 3

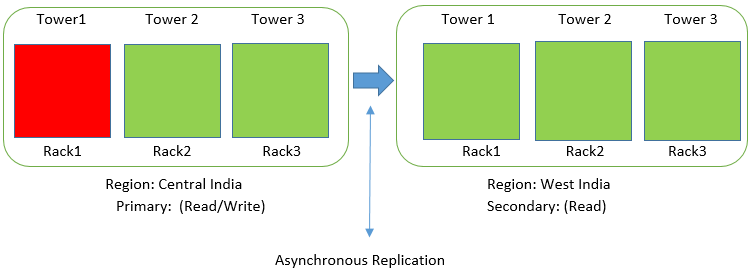
Rack1 Rack2 Rack3 Rack1 Rack2 Rack3

Region: Central India Region: West India Primary: (Read/Write) Secondary: (No Read/No Wr.)

Asynchronous Replication

|  |  |  |
| --- | --- | --- |
| LRS | GRS | RAGRS |
| 5 Rs. | 10 Rs. | 15 Rs. |

1. RAGRS (Read Access Geo Redundant Storage): It is too much expensive, inside the production Environment generally we are not using this type of storage.



1. ZRS (Zone-Redundant Storage): It is working in Same Region. Very big drawback is that if you choose the option of ZRS then you can never convert it into the LRS & GRS storage options.
2. GZRS (Geo-Zone-Redundant Storage): It is working in different Region. It will make total 12 copies 6 copies in the primary region and 6 copies in the secondary region.

***Steps for LRS (Locally Redundant Storage):***

<https://azure.microsoft.com/en-in/features/storage-explorer/>

1. Create RG: IBM-RG > Region: Central India
2. Storage Account > Create >> Storage account name: ibmstorage01 >> Performance: Standard >> Premium account type: page blob >> Redundancy: LRS > Review create
3. Go to the browser and type: Microsoft Azure storage Explorer >> select Windows : Download & Install this tool
4. Storage Account > ibmstorage01 > we can upload data directly from here but we did not providing direct azure access to client so we are giving access on Azure storage Explorer
5. Microsoft Azure storage Explorer: Open this application > for login this application we need to go to the
6. Storage Account > ibmstorage01 >> access key: copy account name and paste on application >> copy key > paste on account key option inside application. >> storage domain: Azure > next > connect
7. Microsoft Azure storage Explorer : IBM-STORAGE > Blob container: right click > create Blob container(folder) : HR-DATA >

Now whatever we creating and saving the data all will be showing inside the storage: ibmstorage01

1. ibmstorage01 > File share : Name > hrfileshare > Tier: Hot > create

Note: To make the file share enable SMB Protocol must be enabled by the ISP provider on port No.445 otherwise data will not be shared.

1. ibmstorage01 > File share > hrfileshare: Connect > copy script for the Windows OS > open PowerShell: run as administrator > paste the command >> credential added successfully.

Now storage disk will be shown inside this PC section.

1. If I want to change the disk size: ibmstorage01 > File share > hrfileshare > Edit quota
2. Configuration: Large file share: Enable then we can share 5-100 TB

**Interview Question:** If a customer has the LRS storage in the primary region which has 100 GB of data, and now the consumer wants to convert LRS to GRS storage then what can be possible?

**Answer:** Yes! We can convert from LRS to GRS storage but Microsoft will charge only the first time to transfer your 100 GB data into the second region after that only a service charge will be applied.

----------------------------------------------------------------------------------------------------------------------------------------

**AZURE BACKUP**

*In* ***On premise*** *we storing backup inside pendirve, External HDD, NAS shortage, SAN storage*.

*But in the Microsoft Azure we are storing data inside* ***Recovery Service Vault.***

MARS BACKUP

(MICROSOFT AZURE RECOVERY SERVICE BACKUP)

FILE AND FOLDER

Internet

On premise

Windows 2016

On premise

Windows 10

Recovery service vault

Data Restore

In the above Azure Backup scenario, it will take Backup through **MARS BACKUP (Microsoft Azure Backup Service Backup)**, it is taking only the Files and Folder level Backup from the on premise client OS or Network Operating system. It is not taking whole operating system backup.

We need to install **MARS Agent**, with the help of MARS agent data will be uploaded to Recovery service Vault. If you want to restore the Data from Recovery service Vault then it could be possible through MARS Agent software.

**Azure IAAS Backup**

With help of Azure IAAS Backup we can take the complete Virtual Machine level Backup.

INTERNET

Recovery Service Vault

LINUX

WINDOWS

(Full VM level Backup)

***Steps for Azure IAAS Backup:***

1. RG: TCS-RG > Region: Central India > Create
2. VM: TCS-TALLYVM01 > tallyadmin01 > RDP(3389) > standard HDD > Create
3. Global search: Recovery Service Vaults > create > vault name: TCS-BACKUP-VAULT > create
4. VM Desktop: TCS-TALLYVM01 > create a folder on desktop: test > inside test folder create a txt file > test1: type Azure > save
5. Recovery Service Vaults > TCS-BACKUP-VAULT > Properties > Backup configuration : Update > select : LRS (Locally-redundant storage) > save
6. TCS-BACKUP-VAULT > Backup: select where is your workload running: Azure > what do you want to backup: Virtual Machine > Backup -------
7. Configure Backup: create a new backup policies > policies Name: tally-backup-policies > select Indian time zone > Frequency: Daily, Select time > retention range : check all boxes > ok > add > select VM > ok > enable backup
8. VM: TCS-TALLYVM01 > Backup : click Backup now (for instant backup if required)

This backup process will takes too much time: Transfer data to vault: In progress.

***Steps for Azure On premise MARS Backup:***

1. Global search: Recovery Service Vaults > TCS-BACKUP-VAULT > backup > where is your workload is running: select On-premises > what do you want to backup: select File and folders > prepare
2. Download agent for the windows server or windows client : Download and install
3. Download vault credential to register the server : tick checkbox > Download
4. Open Microsoft Azure Backup application : Open > Register server > next > brows select file key > next > Generate passphrase key > Brows and save the passphrase key on desktop > register > yes

If you lost your passphrase key then there is no chance to restore the backup files again, so save it in one drive or email or any secure location.

1. Desktop: save a txt file: name test write inside 1 > save
2. Start items to backup: we can choose whole drive otherwise we can choose any selected files or folders.
3. select test file > ok > next > choose backup timing on day format > next > select retention policies (30 Days, 8 weeks, 12 months, 5 years) we can choose also modify option> next > Online (Transfer over the network) > finish

If I want to store the backup on my own computer then:

1. Microsoft Azure Backup > recover data (**Backup restore drill**)> this server > next > individual file and folder > next > select the volume and date time : C drive and select date time > Mount

Now the Backup drive has been created inside the Computer:

1. Go to this PC > drive is visible > inside the drive all data is available which we had taken as backup file.

If we wants to take the backup again of the latest files and folder then we need to **unmount** the drive first:

1. Microsoft Azure Backup > Backup Now > select current date and time > recover data (**Backup restore drill**) > this server > next > individual file and folder > next > select the volume and date time: C drive and select date time > Mount.

If we want to **Restore VM Backup** (**Backup restore drill**) then create a new RG inside the Azure

1. Storage Account : Create > create RG: RESTORE-BACKUP-DRILL-RG > Storage account name: backupstorage01 > region : Central India > Redundancy: LRS > create
2. VM: TCS-TALLYVM01 > Backup > Restore VM > Select restore point > Recovery point showing >ok > VM name: restore-VM > RG: select RESTORE-BACKUP-DRILL-RG > staging location: select backupstorage01 > restore (Now VM backup restoration process has been start)
3. VM: restore-VM > access through the public IP user name and password must be same.

Process to enable security PIN inside the Recovery service vault: if anyone wants to delete your backup data the

1. Global search: Recovery service vault > properties > security PIN : generate
2. Microsoft Azure backup application > Schedule backup >Stop using the backup schedule and delete all the stored backups : then it will ask the PIN
3. SO anyone can’t delete data without entering PIN
4. If Backup has been detected by mistake then you can restore backup within 14 days.

Steps for How to delete the Backup:

1. Delete the backup from Microsoft Azure backup application > Schedule backup > Stop
2. VM: TCS-TALLYVM01 > Backup > Stop Backup > delete backup data > type of backup: TCS-TALLYVM01 > Region: I couldn’t support > comment : Testing > Stop backup
3. Global search: Recovery service vault > TCS-BACKUP-VAULT > Backup policies > delete all policies
4. Backup items: Azure backup agent > delete
5. RG: TCS-RG > Delete all resource from this RG
6. TCS-RECOERY-VAULT: it will be deleted after 14 Days but no charge will be applicable after deleting above all.

**Retention Policies:**

For Example if choose **retention policies** of 30 Days, or 8 weeks or 12 Months then it will save the threshold values only not more than this. For example Daily Backup if we have make the retention policies of 30 days then it will store only 30 recovery point only not 31, it will delete previous file on more than 30 recovery point. So only 30 recovery point will be stored.

* Daily Backup : 30 days
* Weekly Backup : 8 weeks
* Monthly Backup : 12 months
* Yearly Backup : 5 Years

If we are taking Azure **IAAS Backup** or **MARS Backup** then:

* First time Backup: Full Backup

For Example, we want to take an **IAAS backup** or **MARS Backup** of a file server that has 100GB of data choosing retention policies for 30 Days.

* 1st JAN – Fist time backup: full backup 100 GB.
* 2nd JAN – Second time backup: 100 GB uploaded + **10 GB incremental data** = 110 GB data

(10 GB is become the **incremental data**, it will only storing incremental data day by day.)

* 3rd JAN – Third time backup: 110 GB uploaded + **20 GB incremental data =** 130 GB data

We have choose only 30 Days of retention policies then on next month more than 30 Recovery point:

* 1st FEB – On 1st FEB recovery point of 1st JAN will be remove automatically
* 2nd FEB - On 2nd FEB recovery point of 2nd JAN will be remove automatically

For Example, we want to take an **IAAS backup** or **MARS Backup** of a file server that has 100GB of data choosing retention policies for 8 weeks.

* It has a total of 8 recovery points, during 9th week it will delete previous recovery points.
* From January to February it has a total of 8 recovery points then on the 1st week of March it will delete automatically the copy of 1st week of January and this process will be followed.

|  |  |  |
| --- | --- | --- |
| JANUARY | FEBRUARY | MARCH |
| 1 recovery point | 1 recovery point | 1 recovery point |
| 2 recovery point | 2 recovery point | 2 recovery point |
| 3 recovery point | 3 recovery point | 3 recovery point |
| 4 recovery point | 4 recovery point | 4 recovery point |

For Yearly Backup:

* It is use for the ISO audit purpose, ISO audit is conducted by the third party agencies (KPMG, DELLOYET).
* In the yearly backup, backup will be done only **once in a year**.

**Azure SQL Administration**

**(How to create database & How to access database)**

Azure SQL (Sequel) is a **relational database** which is use to resolve the query.

Example of relational database: on YouTube if we search about news then it will showing all data related with the news word.

***Steps for Azure SQL Administration:***

1. Google: Azure sql dtu (**Data Transaction Unit**) calculator: <https://dtucalculator.azurewebsites.net> >> Download command line utility > make DTU named folder and save inside
2. Sql-performon-cl > Extract here > exe file (open with notepad) > add key value: 3600 change it for 48 hours (172800) > add key (csv path): remove temp > save
3. Right click on script: run as administration > load capturing started > cntrl + C = stop (Now log has been captured inside the C drive in the form of CSV file)
4. <https://dtucalculator.azurewebsites.net> > upload CSV file and calculate: choose file: select CSV file > Standard-S1 series will be show.
5. Create RG: UA-RG > create
6. SQL database: create > database name: uadb01 > server: create new: server name: uadbserver01 > location: select region: CI > use SQL authentication > server admin login: dbadmin01 > PW > ok
7. Compute+ storage: configure database > service tier: select DTU: but for practical choose: Basic > apply
8. <https://aka.ms/ssmsfullsetup> > **download SQL server management studio** (it use to take the remote of the SQL server) > download & install: open
9. uadb01: overview > click on server name > copy server name > paste in SSMS application > authentication: SQL server authentication > login: dbadmin01 > pw > connect > error msg show
10. uadb01: overview > set server firewall > public network access: selected networks > firewall rule: add your client IPv4 address > save
11. SQL server management studio > connect > authentication: SQL server authentication > login: dbadmin01 > pw > connect > usb0> tables > we can create a new table > save

Now we need to configure its backup

1. uadb01: overview > click on server name > uadbserver01 > backups > retention policies > tick checkbox of database : configure policies > select long term retention > select 8 weeks, 12 months, 5 years > apply
2. uadb01: overview > click on server name > uadbserver01 > restore > point in time > database name: uadb02\_2022-07-31-backup > review + create
3. SQL server management studio > detach database and login again > login: dbadmin01 > pw > connect > now two servers are showing.

**Onprem Microsoft SQL to Azure SQL Database migration**

***Steps:***

1. RG: IBM-RG, Region: Central India
2. VM: ONPREMISE-DB > Images: see all images : Databases : select SQL server 2016 SP2 standard on windows server 2016 SP2 standard on windows server 2016 -x64Gen 1 > size : **D series : D4ds\_v4 -4 vcpus, 16 GiB** > username: onpremdb01 > disk: standard SSD > create
3. Onpremise VM Desktop: ONPREMISE-DB > server manager : IE off > Internet Explorer > download chrome > open DTU calculator (<https://dtucalculator.azurewebsites.net/>) > download command line utility > copy utility file and paste inside C drive: inside DTU folder > extract: SqlDtuPerformance.exe : open with notepad > value: replace 3600 to 172800 > value : remove temp and save inside C diver only
4. SqlDtuPerformon : run as administration > control + c to stop the operation > open <https://dtucalculator.azurewebsites.net/> > upload csv file : calculate > SQL workload will show standard S-7 so need to create S-7 in target site
5. VM Desktop: Go to windows start : open Microsoft SQL server management studio > server type : database engine > server name: ONPREM-DB > windows authentication > connect > create new database > testdb01 : create new table: testtable01 > create notepad file and save
6. SQL database: create RG: IBM-CLOUD-RG > Database name: ibmclouddb01 > server: create new: ibmcloudserver01 > location: central India > use SQL authentication > server admin login: clouddbadmin01 > pw > ok > workload environment > Development > compute + storage: configure database : to check and know S-7 workload open azure pricing calculator: <https://azure.microsoft.com/en-in/pricing/calculator/> > search Azure SQL database: select DTU in purchase model > service tier: Standard > performance level: select **S7: 800 DTUs**
7. SQL database: compute + storage: configure database: select 800 DTUs but for practical environment we need to choose Basic(for less demanding workloads) > review create
8. SQL database: ibmclouddb01: set server firewall > add your client IPv4 address > we need to attach our VM public IP so open duplicate tab and open VM: ONPREM-DB-PIP > copy public IP > ibmclouddb01: set server firewall > add a firewall rule: paste public IP of VM in start IP and end IP: rule name: ONPREM-DB > ok > save
9. Onpremise VM Desktop: ONPREMISE-DB > Microsoft SQL server management studio > disconnect > connect: Database engine: server name: ibmclouddbserver01.database.windows.net > Authentication: SQL server authentication > username: clouddbadmin01 > pw > connect > error: sign in (ip not allowed)
10. Copy public IP from Onprem VM > SQL Database > set firewall > add a firewall rule: paste public IP of VM in start IP and end IP: rule name: ONPREM-DB-PIP > ok > save
11. Onpremise VM Desktop: ONPREMISE-DB > Microsoft server management studio > disconnect > connect: Database engine: server name: ibmclouddbserver01.database.windows.net > Authentication: SQL server authentication > username: clouddbadmin01 > pw > connect
12. Onpremise VM Desktop: Search in chrome: <https://dotnet.microsoft.com/en-us/download/dotnet-framework/net48> > install > **download .NET Framework 4.8 runtime > Database migration assistant (DMA)** **Version5.6** > <https://www.microsoft.com/en-us/download/details.aspx?id=53595> > download > Install > reboot now
13. Onpremise VM Desktop: ONPREMISE-DB > install database migration assistant (DMA) Version5.6 > open DMA application > + new > project type: select Assessment > project name: ibmmigration assessment > source server type: SQL Server > target server type: Azure SQL Database > create > next > Server name: ONPREMISE-DB (cmd: hostname: ONPREMISE-DB) > Authentication type: Windows Authentication > connect > select ONPREM-DB & testdb01 > add > start assessment > check compatibility issues > msg will be shown: **There are no compatibility issue with the database**. > save assessment > close

We will share assessment report to the customer then consumer will check there are no compatibility issue then he will allow to do the migration. If any issue is persist with the database then we will provide them to resolve it.

1. Open database migration assistant (DMA) application > project type: Migration > Project name: Onprem-to-azure-dB-migration > source server type: SQL Server > target server type: Azure SQL Database > migration scope: Schema and data > create > source Server name: ONPREM-DB > windows authentication > tick on: Encrypt connection & windows authentication > connect > tick testdb01 > connect to target server: server name: (copy from SQL database from azure portal) ibmclouddbserver01.database.windows.net > Authentication type: SQL Server authentication > username: clouddbadmin01 > pw > tick on both connection properties > connect > generate SQL script> deploy schema > **Migrate data**
2. Start Migration (Migration has been started it will takes too much time in the organization) > successful
3. SQL management studio inside VM desktop > connect > Migrated Database will be shown

**AZURE to AZURE DR MIGRATION**

***Steps:***

1. 1ST RG: FLIPKART-RG > Region: Central India > Crete > VNET: FLIPKART-VNET01 > address space: 10.0.0.0/24 > subnet: FLIP-WEB-SUBNET > subnet range: 10.0.0.0/25
2. VM: FLIP-WEB01 > windows 2012R2 > size: B1s > username: webadmin01 > disk: standard HDD > create
3. VM Desktop: FLIP-WEB01 > create a new folder: create a test notepad and save

We need to create the **replication** of this VM in the paired region (Central India to South India)

1. 2ND RG: FLIPKART-RG-SOUTHINDIA > region: south India
2. Global search: Recovery service vault: create: RG: FLIPKART-RG-SOUTHINDIA > name: FLIPKART-RSV-SOUTHINDIA > review create
3. Recovery service vault: FLIPKART-RSV-SOUTHINDIA > properties: storage replication type: Backup Configuration: LRS > save > overview: site recovery
4. VM: FLIP-WEB01 > disaster recovery: Target region: south India > next > select source and destination, Availability: single instance > next > start replication
5. Recovery service vault: FLIPKART-RSV-SOUTHINDIA > site recovery > Enable site recovery > enable replication > source location: central India > resource group: FLIPKART-RG > next > tick on VM: FLIP-WEB01 > target location: South India > customize > target resource group: FLIPKART-RG-SOUTHINDIA > target virtual network: by default (FLIPKART-VNET01-asr) > ok >> enable replication

Replication creation will takes 35 minutes of time, for the replicationwe are using Agent version**: 9.50**

1. VM: FLIP-WEB01 > disaster recovery > replication health: Healthy will show & Status: Protected > last successful test failover: never performed successfully

Test Failover: During Failover case same VM will be created inside Azure Site Recovery (ASR), this process is called **Test DR DRILL,** After doing this steps consumer will giving a signoff for the cleanup, during this process no impact will be on production environment no services will be down

1. Recovery service vault: FLIPKART-RSV-SOUTHINDIA > site recovery > click on 1 Healthy > status healthy & protected must be shown > Failover health: warning
2. VM: FLIP-WEB01 > disaster recovery > Test failover > from central India to south India > select Azure virtual network: FLIPKART-VNET01-asr > ok

Now new virtual machine has been create named as FLIP-WEB01-test in the south India region

1. VM: FLIP-WEB01-test > Public IP address: public IP is not attached so we need to attach this.
2. VM: FLIP-WEB01-test > networking > click on Network interface > IP configuration > click on IPv4 > Public IP associate: associate > Public IP address: create new: SOUTH-PIP, Dynamic > ok > save
3. VM Desktop: FLIP-WEB01-test > all data are the same as we saved inside FLIP-WEB01
4. Recovery service vault: FLIPKART-RSV-SOUTHINDIA > site recovery: click on healthy: status: cleanup test failover pending
5. Recovery service vault: FLIPKART-RSV-SOUTHINDIA > site recovery: click on healthy: FLIP-WEB01 > Cleanup test failover > notes: testing done > click on testing is complete delete the test failover > ok

Now the Test VM has been deleted, we will do further Failover process

1. Recovery service vault: FLIPKART-RSV-SOUTHINDIA > site recovery: click on healthy: FLIP-WEB01 > Failover > ok

Now VM has been created named as FLIP-WEB01 in south India region

1. VM: FLIP-WEB01 Region: south India > networking > click on Network interface > IP configuration > click on IPv4 > Public IP associate: associate > Public IP address: create new: SOUTH-PIP, Dynamic > ok > save
2. VM Desktop: FLIP-WEB01 > all data will be shown which saved inside the central India VM

Recovery service vault

Web server

Azure site recovery (ASR)

1. Failover
2. Test Failover
3. Clean-up

Replication enabled

**AWS to Azure Migration (Azure Migrate)**

***Steps:***

1. Infra is running on AWS we need to migrate on Azure.
2. Create 1st VM > Login AWS account <https://aws.amazon.com> >> choose region: US East (N. Virginia) >> EC2 Dashboard >> Instances (Running): Launch Instances > Name: CONFIGURATION SERVER (This is a replication server which helps to migrate the server, it requires 8 core 16 GB) >> application and image: select windows >> select Microsoft windows server 2016 Base >> Instance type: t2.2xlarge (8 core 16 GB) >> key pair: create new key pair: WIN-KEY > create key pair Configure + storage : 650GiB > launch instance
3. Instances: select VM: connect: RDP client: download remote desktop file >> Get password: Brows > select WIN-KEY > Decrypt password >copy & paste password on RDP >> VM Desktop
4. Create 2nd VM: Windows server 2016 R2 Base, 2 core 4GB >> choose same IP & its subnet range as 1St VM >> connect VM
5. Time Zone must be same of both VM desktop so set both server time zone same and firewall must be off of both server >> IE must be off for both server
6. Install IIS rule in HCL-WEB server >> download Google chrome: /download HTML templates: paste inside C-Drive : inetpubmgr: wwwroot >> paste the extracted file.>> Win+R= inetmgr.msc >> add website
7. Win+R= cmd : ipconfig: copy ip address of configuration server & WEB server and paste on notepad

We need to check connectivity of both server via Ping command

1. Win+R= cmd: ping (ip of different server) do this step for both server >> result not ping
2. Inside AWS required to Traffic Allow: select server: Security > security group: select: edit inbound rule >> Type: select All traffic (0.0.0.0/0 means all traffic has been allowed) > save rule > outbound is already allowed by default >>>>> do these step for both server.
3. Win+R= cmd: ping (ip of different server) do this step for both server >> now both server is pingable.
4. VM Desktop: WIN+X= cmd (admin) > net user administrator test@123456 (Now password has been reset successfully) password must be same for both VM so do this steps for both VM. Access both VM via new credentials

Go to Azure portal and create the New RG

1. HCL-PROD-CI-RG > Region: Central India > VNET create: HCL-PROD-CI-VNET01 > IP range: 172.168.1.0/24 > subnet: HCL-PROD-SUBNET , 172.168.1.0/25 > Create
2. Azure migrate: Discover Assess and migrate > create project: RG:HCL-MIGRATION-PROJECT-RG > project: HCL-MIGRATION-PROJECT01 > geography: India > connectivity method: public endpoint > create
3. Azure migrate: servers, database and web app >> Click on HCL-MIGRATION-PROJECT01 >> migration tool >> click on discover option > select Physical or other (AWS, GCP, XEN, etc.) >> target region: Central India > tick on the confirm checkbox >> create resource.
4. Global search: Azure migrate: Discover: are your machine virtualized: select physical or other (AWS, GCP, XEN, etc.) >> select install a replication appliance >> right click on Download: copy link >> Go to appliance server desktop: paste the link and download the file
5. Rename the server desktop name: this PC: properties: computer name: change setting: APPLIANCE: ok > restart
6. Global search: Azure migrate: Discover: Download: and paste on Appliance server desktop:
7. Global search: Recovery service vault: HCL-MIGRATION-PROJECT01: properties > LRS > save
8. Appliance server desktop: Install downloaded file:Install Microsoft Azure recovery service > finish > copy passphrase key or take screenshot > Desktop: click on CSP config > add account > friendly name: APPLIANCE01, User name: administrator > pw: test@123456 > Vault registration: Brows key which was saved in download folder > register > DRA Registration succeeded.
9. Global search: Azure migrate: Discover: physical or other (AWS, GCP, XEN, etc.) > install a replication appliance > select configuration server: APPLIANCE > finalize registration > Registration finalized
10. Appliance server desktop: Win+R = %programdata% > Microsoft Azure site recovery > private > copy connection passphrase > paste on server desktop > open with notepad > copy passphrase key from notepad
11. Appliance server desktop: Win+R = %programdata% > ASR > home > svsystem > pushinstallsvc > repository > copy Microsoft-ASR\_UA\_windows application (Mobility agent) > paste on desktop
12. copy private ip 172.31.10.40 from Appliance server Go to web server: Win+R = \\172.31.10.40\c$ > username: administrator, pw: test@123456 >>> users > administrator > desktop > copy configuration passphrase & copy Microsoft-ASR\_UA\_windows application (Mobility agent) > paste on desktop > right click on mobility agent application run as administrator > install mobility service > it will takes time
13. Proceed to configuration > paste ip of configuration server >> configuration server passphrase: copy passphrase from notepad and paste > configuration server port: 443 >> Register > finish
14. Global search: Azure Migrate: Discover: server: migration toot >> Replication >> /what do you want to migrate: Servers or VM >> what do you want to migrate to: Azure VM > continue >> Are your machine virtualized: physical or other (AWS, GCP, XEN, etc.) >> on-premise appliance: APPLIANCE >> next >> No I’ll specify the migration setting manually >> tick on private server ip >> next >>
15. Target setting: Subscription >> HCL-PROD-CI-RG >> Virtual network: HCL-PROD-CI-VNET01 >> Subnet: HCL-PROD-SUBNET >> next >> choose D2as\_V4 2 core 8GB RAM >> next >> VM name: HCL-WEB02 >> Choose disk: Standard HDD >> next >> Replicate >> replication done
16. Recovery service vault: HCL-MIGRATION-PROJECT01 >> Overview >> Site recovery: Healthy >> Test failover > from: APPLIANCE >> To: Microsoft Azure >> Azure virtual network: HCL-PROD-CI-VNET01 >> OK
17. HCL-WEB002-Test >> networking >> Network interface: IP Configuration: Public IP associate: Public IP address: create new: HCL-INFRA-PIP: Static >> ok >> save
18. VM Desktop:HCL-WEB002-Test >> user name: administrator >> pw: test@123456 > check your all application is running then
19. Recovery service vault: HCL-MIGRATION-PROJECT01 >> Overview >> Site recovery: Healthy >> Cleanup Test failover > Note: Testing Done signoff from the application team >> tick on testing is done >> ok
20. VM: The virtual machine resource was not found
21. Global search: Azure migrate: Discover: Migration tool >> refresh >> Migrate >> shutdown: No >> select VM >> Migrate
22. HCL-WEB002 >> networking >> Network interface: IP Configuration: Public IP associate: Public IP address: create new: HCL-INFRA-PIP: Static >> ok >> save
23. VM Desktop:HCL-WEB002 >> user name: administrator >> pw: test@123456 > check your VM has been migrated successfully and all application is running well
24. HCL-PROD-CI-VNET01 >> Subnet: Name: HCL-APPGW01 >> IP: 172.168.1.128/27 >> save
25. Load Balancer: create: RG: HCL-PROD-CI-RG >> Application Gateway: HCL-APPLICATION-GW01 >> Tier: standard V2 >> Enable auto-scaling: No >> Instance count: 1 >> HTTP2: Disable >> choose VNET: HCL-PROD-CI-VNET01 >> choose subnet: HCL-APPGW01 >> Next frontend >> Public IP: add new: Name: HCL-APPGW01-PIP >> Next >> Add a backend pool: HCL-WEB-BACKENDPOOL >> Virtual machine & its IP >> add >> next
26. Add a routing rule >> /rule name: HCL-WEB-ROUTINGRULE >> priority: 1 >> User name: HCL-WEB-LISTNER >> Frontend IP: Public >> Protocol: HTTP >> port: 80 >> listener type: choose Basic (but during production site we need to choose Multi site: Hostname: thechetan.xyz)
27. Backend target: choose HCL-WEB-BACKENDPOOL >> backend target: add new: Backend setting name: HCL-WEB-BACKEND-TARGET >> HTTP >> Request time out: 60 sec >> add >> next >> review create >> create

Server 2012

MS SQL server

Server 2012

Web server

Server 2016

Configuration server Appliance

8 Core

16 GB RAM

OS Disk size: 80 GB



**Azure Monitoring**

1. Create VM: HCL-WEB01 >> (During VM creation) Management: Boot Diagnostic: Enable with managed storage account (recommended) > Enable OS diagnostic: Tick on checkbox (It Diagnostic OS level means it provides a notification if OS will be corrupt) >> Review + Create
2. VM Desktop: HCL-WEB01 >> Metrics >> Inside the metrics we can check the RAM and memory utilization on daily and monthly basis.
3. Metrics >> Share >> Download to Excel
4. For the CPU utilization: Metrics >> select percentage CPU
5. We can reshape the Processor & RAM size >>> VM: Size >> we can change the size

*How to configure the Alerts*

We are going to set alerts for the CPU utilization, alert will send to Email ID

1. VM: Alerts >> create >> alert rule >> select percentage CPU >> Threshold value: 75% >> Aggregation granularity (Period) >> set 1 Minutes >> Frequency of evaluation: every 1 Minutes >> done
2. Next action >> create action group: Action group name: HCL-TALLYVM01-CPU-ALERT >> Display name: HCL-TALLYVM01 >> Notification type: Email/SMS/message/push/voice >> choose Email: [sumantra93@outlook.com](mailto:sumantra93@outlook.com) >> Name: Sumantra >>>> we can choose multiple email ID >> create
3. Next >> Details: severity: 0-criticle >> alert rule name: CPU alert threshold value 75 >> same copy and paste in the description >> create
4. VM Desktop: HCL-TALLYVM01 >> Download Google chrome >> Heavy Load: <https://www.jam-software.com> >> download and run >> now CPU utilization will become 100% then alert will fire within one minute and notification will be send via the mail ID
5. VM: Boot diagnostics >> Time and date will be shown
6. VM: Resource Heath: we can check our service is available or not available
7. Monitor: Service health >> all service center is healthy if any location get down then it will show as a red
8. Monitor: Service health >> create service health alert: select services >> choose region where data center is running of the customer: Central India for example >> select action group: create action group: action group name >> service health alert >> next >> enter email ID for the notification >> Notification type: Email/SMS/ message/ push/ voice >> choose Email: [sumantra93@outlook.com](mailto:sumantra93@outlook.com) >> Name: Sumantra >>>> we can choose multiple email ID
9. Alert rule name: Service health issue >> paste in description >> create alert rule

**Azure Pricing Calculator**

With the help of Azure pricing calculator we are calculating the estimated amount for the Network creation.

<https://azure.microsoft.com/en-us/pricing/calculator/>

1. We want to create a Tally server then >> virtual machine option >> HCL-TALLYVM01 (220 HRS) >> Region: Central India >> choose OS and it Instance >> choose No of virtual machine count and fill the 220 hrs. >> choose tier: Standard HDD >> Disk Size: S10: 128 GB >> Disk: 1
2. If servers are running (24\*7) then don’t choose Pay as you go option this will be costly for the consumer then choose 1Year(R1) or 3Year(R3) subscription which will be discounted for the consumer.
3. HCL-APP-HYBRID : OS >> Azure Hybrid benefit (If windows license are present in the on-premise) >> Managed disk: Standard HDD

If we wants to attach Data Disk then Go to Storage Accounts option

1. Storage Accounts: HCL-APP01-DATA-DISK01 >> Type: Manage Disks >> Tier: premium SSD >> choose disk size
2. Storage Accounts: Type: Block Blob Storage >> Tier: Standard >> Access Tier: Hot or Cool >> capacity in GB: choose >>
3. For the Linux VM Cost: Operating system: Linux >> Type: Ubuntu or Red Hat (Ubuntu is cheaper and Open source but Red Hat is costly but it provides the support from the Red Hat team)
4. VPN Gateway: type: VPN Gateways: HCL-VPN-GW01 >> choose Gateway type: Basic >> choose Gateway Hours
5. With the VPN Gateway public IP will be included so search IP: IP address >> HCL-VPN-GW01-PIP
6. Azure Backup: Region: Central India >> Type: choose (Azure VM, Onpremise, and SQL etc.) >> Protected Instance Calculation >> 1-50 GB Price will be 399 Rs but above 50 GB price will be 799 Rs.
7. Azure SQL Database: Region >> Backup storage tier: LRS or GRS >> purchase model: DTU >> Retention policies: Weekly backup, monthly backup, yearly backup
8. Azure Migrate: There is no charge to use Azure Migrate
9. Load Balancing: >> Basic load balancer is free of charge >>
10. Load Balancing: Standard Load balancing >> choose number of load balancing rule >> Data proceed: 0 >> set IP cost >> type: Standard >> Choose static or Dynamic IP count
11. Bandwidth >> Data transfer type: Inter Region >> source region: Central India >> Destination region: South India >> Outbound data Transfer will be free up to 5GB in each Zone above this it will be chargeable 6 Rs/GB.

For the Estimate go to down side and click on Export to get the estimated amount in the form of Excel sheet

**Azure Active Directory (Azure AD)**

1. Azure Active Directory (Azure AD): Add domain: Enter domain name and also allow its DNS into Godaddy portal >> now domain name is registered and verified
2. cloudblogger.in : add custom domain (ibm.com or ril.com or hcl.com): cloudblogger.in >> add domain
3. Azure Active Directory >> Users >> New user: create new user >> User name: sumantra.upadhyay >> Name: First name, Last name >> Password: Auto-generated password > copy this password > Usage location: India > Job title: cloud engineer > Department: cloud delivery > company name: cloud blogger > manager: enter manager email ID >> create
4. Copy user email id and go to > <www.portal.azure.com> > login with the copied mail id >> PW: auto generated > login and change password > Microsoft Authenticator (It is use for the MFA multi factor authenticator)> next > Download Microsoft authenticator application in that phone for which you are creating the account > scan QR code in the Microsoft authenticator application > next > Done > Authentication successful.
5. Sign out account and login again > Now two factor authentication has been created (1st authentication is User ID and PW & 2nd authentication is Microsoft authenticator application )

Now David can’t do anything on the Azure portal he don’t have any rights

1. Go to <http://www.portal.azure.com> > create RG: CLOUDBLOGER-RG > VNET: CLOUDBLOGGER-VNET01 > address space: 10.0.0.0/24 > subnet name: CLOUDBLOGGER-INFRA-SUBNET > address range: 10.0.0.0/26 > add > create
2. VM: CB-TALLYVM01 > User name: tallyadmin01 > standard HDD > Networking > NIC > None > create

We need to add one more subnet inside the VM Using Bastion service (security service)

1. Virtual Network: Bastion > create Azure Bastion using defaults > Virtual Network: Subnet > created
2. VM: CB-TALLYVM01 > dissociate its public IP
3. VM: CB-TALLYVM01 > overview > connect > Bastion > Username: tallyadmin01 > PW: admin@123456 > connect

On this VM we wants to give permission to the David only for Read only.

1. VM: Access control (IAM): add: add role assignment: Reader (Read only permission) > next select member: User, group or service principal > select David name > Review + assign
2. Sign out David Azure account then signing IN with two factor authenticator > now only Virtual machines are showing inside the David Azure account no resource are showing. Also it can’t stop the VM, So it’s only read only permission.

On this VM we wants to give permission to Read/Write (Pay as you go sub) on the David account.

1. Azure Active Directory > User: New User: create: Sumantra > copy auto generated PW > create
2. [www.portal.azure.com](file:///E:\AZURE\www.portal.azure.com) > Login with [Sumantra@cloudblogger.in](mailto:Sumantra@cloudblogger.in) > change PW > scan QR code on Microsoft Authenticator application > Login complete
3. I want to give the permission of Pay-as-you-go subscription > global search: subscription > Pay-as-you-go > Access control (IAM) > add: add role assignment: Contributor (Read/Write permission) > next select member: User, group or service principal > select Sumantra name > Review + assign
4. Signin: [www.portal.azure.com](file:///E:\AZURE\www.portal.azure.com) > Login with [Sumantra@cloudblogger.in](mailto:Sumantra@cloudblogger.in) > username: tallyadmin01 > pw: admin@123456 > connect > give permission on app > Login complete (Its working like RDP on web browser)

Create SQL Database

1. Database name: cloudbloggerdb01 > server: create > cloudbloggerdbserver01 > authentication: Use SQL server authentication > server admin login: dbadmin01 > choose: LRS > service + compute: DTU: Basic > Apply
2. Set server firewall: choose selected network > add your client IPV4 address (this my laptop public IP) > save
3. Open Microsoft SQL Server Management studio on laptop > Login with SQL authentication

I want to make more secure this SQL server then

1. SQL Database: click on Database: click on server name: Azure Active Directory >> set admin > select user (Sumantra) > save
2. copy mail ID of added user and login Microsoft SQL Server Management studio on laptop > connect database > Authentication: Azure Active Directory Universal with MFA > user name: Email ID (sumantra@cloudblogger.in) > connect > PW > Opened

To Activate MFA for Database access

1. sign out from browser > Azure Active Directory: User > select user: per user MFA: select user: Enable > Enable multi factor authenticator
2. Login again: Microsoft SQL Server Management studio on laptop > Login with [Sumantra@cloudblogger.in](mailto:Sumantra@cloudblogger.in) > username: tallyadmin01 > pw: admin@123456 > connect > give permission on app > Login complete
3. Now database has been access with MFA

We can access whole resource from our Email ID in our Laptop

1. Laptop Setting Option > Accounts > Access Work or School > connect > click on Join this Device to Azure Active Directory > Login with the mail ID > now restart the Laptop

Role base

MFA

Bastion

**Interview**

1. Introduction
2. What are you doing on daily basis activity (Which task you performing)
3. What is your roll and responsibility
4. If you are working before 2015 then--- (Local IT Operations)

Answer: Sir we was updating windows patch before updating this we are checking CMD>> Winver command to check version of the windows (Search Microsoft patch catalog in Google: <https://www.catalog.update.microsoft.com/Home.aspx>) >> Laptop: search windows update: you will see the KB number (KB5016688) >> copy KB number and paste on patch catalog site and downloading the latest patch file. We was taking downtime to patch update

1. Print spooler services are going to stop then user can’t take print so we are correct those service Services > Print spooler > stop > start
2. <https://www.manageengine.com/products/desktop-central/> > with the help of this we was updating windows patch > software deployment in user computer > IT Asset management > remote control (we was deleting the temp file, prefetch file in user computer)
3. OS image and deployment <https://www.pendrivelinux.com/yumi-multiboot-usb-creator/> >> we was making bootable pen drive with ISO file

Daily Routine Activity in Azure

1. In our official ID we are getting contributor access on multiple customer subscription level.
2. We are checking all number of servers is in proper running condition, in Azure to Azure DR replication is proper or not, backup’s recovery point is making on daily basis or not, VPN tunnel is working properly or not, VNET peering is connected or not,
3. Activity log (VM: Activity log) we are checking that some have made the changes or not
4. We are also checking Alerts: CPU utilization, memory utilization

Q. What are doing on delivery, or what kind of environment you building?

1. Our sales team is taking projects and we are giving the demo to the client, we were pitching customer on cloud, before the demo we are doing transitioning (we are asking them what king of servers are running in your organization, asking about Network OS & Client OS, any virtualization are you using or still not then we are asking about his working hours and NON working hours, which database servers you are working asking about database version, asking about backup, recovery point, are any remote user is present, how much VPN is connected) through this we are giving them a demo session on our official ID we are making VM all services client is using same services we are making on Azure portal and showing them.

2. After knowing his requirement we was making the BOM (Bill of material) in pricing calculator and sharing to our sales team then after the approval as per BOM we are creating the environment.

Q. Which king of environment you have build?

1. Windows server, Linux servers, VPN’s, Production environment, staging environment, UAT env Production (Live server), Staging (Application team/DB team the was doing testing), UAT (Users are testing the environment)

In our organization we are performing quarterly Backup Drill for backup & DR drill in 6 months,

Test DR Drill (we were showing to customer that your primary data center is good and secondary data center server we are doing UP, then we was doing Test restore drill firstly we are going to UP database server once it is done then we are doing UP to app server then testing team and application was performing their testing after that we are performing cleanup process firstly to app server then the database server).

Scenario Based Question

Q. for any customer if we are building an environment then what kind of approach we have?

A. Sir firstly we are checking that customer is working in which country, then we are checking latency and in top thee result we are choosing the cheaper region after that we are building the environment.

Q. Our user in unable to access inside the Point to site VPN?

A. We are troubleshooting, firstly we are updating our windows, patch update, Win+R= devmgmt.msc > Network adapter > WAN Miniport (IKEV2) > update driver

Q. In our server Database server/ file server/ SQL server / App server, we don’t expose our data publicly, then we want to block the internet?

A. Sir in our type of sensitive servers we are making the outbound rule inside the rule we are blocking port not 83, 443, then internet is completely blocked inside the server.

Q. We want to make site to site VPN?

A. Same steps we are using as a VNET to VNET VPN, after that we need to communicate between Azure firewall to Onpremise firewall, We are checking that Onpremise firewall is matching the Azure VPN parameter or not, also we are checking that Onpremise OS version is supporting as per Azure parameters or not, and they are using which company’s firewall after that >> we are creating Globle search: Local network gateway > we are choosing site to site VPN option and adding their Public IP and their subnet range. Also we are sharing to Onpremise engineer to our public IP and local range of VPN gateway and the range of VNET then our tunnel is become UP.

Q. What kind of troubleshooting you have done in site to site VPN?

A. sir we have found during the tunnel was down then our customer was changed PSK (pre shared key) after addition of the correct PSK tunnel is become UP.

VM related Scenario Based Question

**Q.** This our VM server and I was unable to access the VM server then how you will troublshoot?

A. Sir we are checking first that our VM is in which state (running or stop-deallocated), then we are checking our VM is pingable on VPN connection or not, NSG port is allowed or not, NSG source allowed or denied,

Q. VM is in running but it is not pingable?

A. sir we are checking Network interface may be user can change the IP inside, then we detached network interface and attaching new Network interface, then server will be accessible.

Q. Still VM is not accessible?

A. Sir then we redeploy the server, server will be migrated to Microsoft secondary server

A. Sir then we are restoring the backup’s on all recovery points.

A. Sir we will resetting the passwords.

A. Sir we will change the Private IP of VM.

A. Sir then we will use the Azure Bastion service, and through the browser server will be accessible.

Q. Suppose I have chosen 1 TB HDD and my data is only 100 GB, so can I change my network storage disk?

A. No sir once we have chosen then size then we will be unable to reduce the disk size, we can increase the disk size but not decrease?

Or I can attach a new disk, I will copy and paste the data from existing disk, after that we can detached previous disk.

Q. Are you recommending a third party antivirus?

A. No sir, this is not the best approach to install the third party antivirus, best practice is we need to choose Microsoft antimalware which is highly secure this is the product of microsoft. When we are using a third party antivirus after ending subscription 1 Y, it will create a virus inside the system.

Q. If I have chosen the D series VM then SAP HANA server will works on that?

A. No sir D series VM is not certified VM for the SAP HANA server, we will use the M series VM.

Q. Inside the Load balancer what kind of issue you have faced?

A. Inside the Load balancer, if we are using the standard load balancer then public IP will standard otherwise VM will not be added in the backend pool, if we are using the basic load balancer then we need to choose basic public IP then we can add the VM inside the backend pool.