**[keep similar password ]**

**LAB 1**

1. Login in “Azure Portal” ==🡺 enter credentials
2. After login=🡺 search “Microsoft Entra ID”
3. Click on user to perform various tasks like
4. To create new user
5. Create bulk user (by uploading X-l sheet i.e by updating data”)
6. MFA (multi factor authorization)-🡪 enable so that owner can make contributor
7. Assigned roles🡪add assignment -🡪global administrator
8. Check by login in another window that MAF applied to another account is working or not {by creating user in that} =🡺if not working refresh the root admin account
9. We can apply MFA(multi factor authentication) to one or more user by enabling the MFA \\ open mfa select the user🡺at right side click enable

**LAB 2**

1. Create resource group
2. Create VN( virtual network)🡺 by selecting the resource group created
3. Create a virtual machine 🡺 security standard, select the image eg: window22,

Save the username and password and its public ip

1. Window +r (mstsc)🡪insert public IP, username from notepad, password from notepad
2. Open server manager( wait few minutes to load all the servers and features)🡺click “Add roles and features” 🡺3times “next” 🡺select “Active directory domain services” 🡺next🡺click “add features” 🡺next🡺checkmark the re-start option 🡺click “install”
3. As installation complete 🡺click the notification 🡺click “Promote the server to a domain controller “
4. Click “Add a new forest”🡺click “next” 🡺give password🡺 give a domain name eg: xyz.com 🡺 The NetBIOS domain name is default 🡺 next🡺install
5. Go to tolls select the option to create organizational unit 🡺 create different user 🡺 create a group🡺 add users in group unit by following steps:
6. Select the group🡺properties🡺member🡺add🡺advanced🡺find now🡺select the users to be add in group 🡺apply🡺OK
7. Select group 🡺properties🡺member of 🡺add🡺advanced🡺find now🡺select enterprise admin 🡺ok
8. Download “Azure AD connect”🡺put the id of the email where the organizational administrator is selected 🡺and put its password 🡺next id of enterprise user id and its password 🡺rest steps are as usual 🡺Data will be sync

**Lab 3 (Azure power shell) to paste 🡺ctrl+shift+v**

(MANAGE AZURE RESOURCES WITH POWERSHELL)

Azure CLI Commands...

1= Create New user

az ad user create --display-name hari --password yahoo@123 --user-principal-name hari@priya150@outlook.onmicrosoft.com

2= User Delete

az ad user delete --id 85a48abc-832d-4abd-a776-b45cfb6242af

3= Create Azure AD group

az ad group create --display-name hariomsales --mail-nickname hariomsales

4= Add user in group

az ad group member add --group hariomsales -memberid

5= Group delete

az ad group delete

az ad group delete --groupsales

6= Create resource group

az group create -l Westus -n DeepakRG

az group list --output table

7= Delete resource group

az group delete --name DeepakRG --yes --no-wait

**LAB 4 [Implement virtual network 🡺login with rdp is denied i.e no inbound and outbound traffic is allowed]**

1. Create a resource group
2. Create a virtual machine [assign a subnet over it]
3. Create a Network security group
4. Create a virtual machine🡺 go to disk (just aside of create)🡺go to networking🡺select “Advanced” in NIC network security group 🡺 select the security group create in Configure security group🡺 click “review and create”

Now we can’t login from the RDP: to do so follow the following steps

1.go to NSG🡺select inbound security rules🡺click “Add”🡺 service “RDP”🡺Action “Allow” 🡺click “Add”

Now we can easily allow to access through RDP

**Notes: What is APIPA and why it is used?**

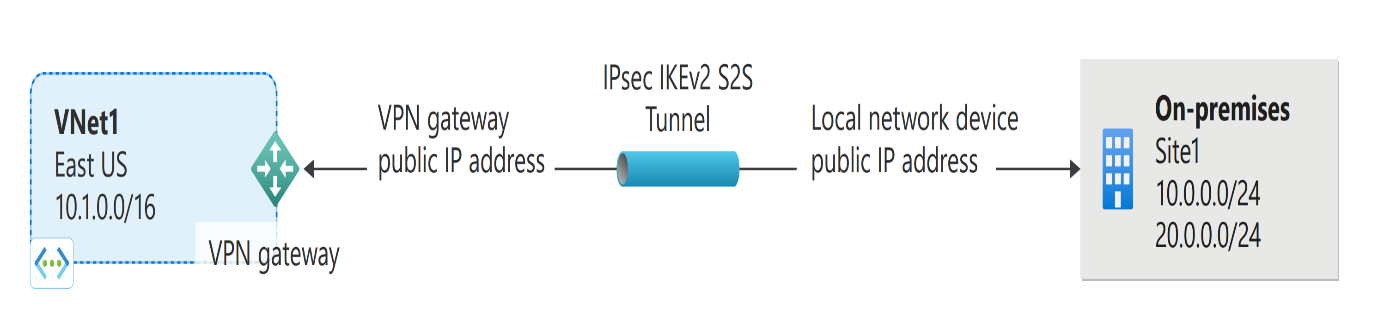
**Automatic Private IP Addressing (APIPA) refers to a feature implemented in the Microsoft Windows operating system that allows devices to automatically assign IP addresses to themselves when they cannot get an IP address from a Dynamic Host Configuration Protocol (DHCP) server.**

**Range: 169.254.0.0 to 169.254.255.255**

**Loop back Nesting: To check your LAN card whether it is working or not**

**Range: 127.0.0.0 to 127.255.255.255**

**LAB-5 To create VPN( Intersite connectivity) 🡺connectivity between sites**



**Why use VPN Gateway?**

Send encrypted traffic between an Azure virtual network and on-premises locations over the public Internet. You can do this by using the following types of connections:

1. **Site-to-site connection:** A cross-premises IPsec/IKE VPN tunnel connection between the VPN gateway and an on-premises VPN device.
2. **Point-to-site connection:** VPN over OpenVPN, IKEv2, or SSTP. This type of connection lets you connect to your virtual network from a remote location, such as from a conference or from home.

Send encrypted traffic between virtual networks. You can do this by using the following types of connections:

1. **VNet-to-VNet:** An IPsec/IKE VPN tunnel connection between the VPN gateway and another Azure VPN gateway that uses a *VNet-to-VNet* connection type. This connection type is designed specifically for VNet-to-VNet connections.
2. **Site-to-site connection:** An IPsec/IKE VPN tunnel connection between the VPN gateway and another Azure VPN gateway. This type of connection, when used in the VNet-to-VNet architecture, uses the *Site-to-site (IPsec)* connection type, which allows cross-premises connections to the gateway in addition connections between VPN gateways.

Configure a site-to-site VPN as a secure failover path for [ExpressRoute](https://learn.microsoft.com/en-us/azure/expressroute/expressroute-introduction). You can do this by using:

1. **ExpressRoute + VPN Gateway:** A combination of ExpressRoute + VPN Gateway connections (coexisting connections).

Use site-to-site VPNs to connect to sites that aren't connected through [ExpressRoute](https://learn.microsoft.com/en-us/azure/expressroute/expressroute-introduction). You can do this with:

1. **ExpressRoute + VPN Gateway:** A combination of ExpressRoute + VPN Gateway connections (coexisting connections).

Step:1. Create two resource group R1(Central India) & R2 (South India)

Step:2 **Create Virtual network VN1 (Central India)**

I.P: 10.0.0.0/16 to 10.0.1.0/24 🡺Create 🡺after creation add Gateway (subnet) 🡺10.0.2.0 /24 (in subnet)

VN2 (South India)

Step: 3 Create VPN Gateway

**Create Virtual network VN2 (South India)**

I.P: 192.168.0.0/16 to 192.168.100.0/24

Step:4 Create two Virtual Machine VM1 & VM2 (Select requirement as per the needs)

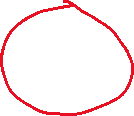
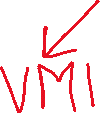
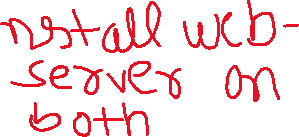
Step:5 Now in Virtual Machine (VM2 i.e in resource group we not created VPN) perform steps:

* 1.Login in RDP(window +R then mstsc)🡺Download the certificate🡺 Run the Child & Root in power-shell.
* Window + R🡺 certmgr.msc🡺 personel 🡺select child cert🡺 All task🡺export 🡺next(few times) 🡺Yes, export the private key🡺make a password for security 🡺Browse to save the export of child certificate 🡺ok (The export was successful)
* select root cert🡺 All task🡺export 🡺next(few times) 🡺No, don’t export the private key🡺select (Base-64 encoded x.509(.cer)make a password for security 🡺Browse to save the export of child certificate 🡺ok (The export was successful )

Step:6 Open the VPN created in VM1 🡺select peer to peer connection 🡺configure🡺 paste the Resource address of VN2 in Address pool, IKEV2 and open VPN(SSL) in tunnel type, Azure certificate in Authentication type 🡺 Give name to VPN and paste the root cert that is exported by opening it on notepad 🡺Save it 🡺 download VPN Client 🡺copy it and paste it on VM2 and INSTALL WINDOWMD64🡺(window +R 🡺 ncpa.cpl ) then connect it

LAB-6 (Traffic management using load balancer)





***Create a load balancer (provide the frontend configuration and backend-pools (vm1 and vm2)🡺assign health probe to load balancer 🡺add load balancing rules 🡺open frontend configuration and use url to check the load on which server***

LAB-7 Storage account in a specific region

* Create a Resource group
* Create a virtual network
* Create a storage account 🡺go to blob service 🡺enable “Blob anonymous access”
* Go to storage account and upload content by creating a container (Publically i.e anonymous read access only)
* Go to container created from settings/data storage of storage account ( click on context menu(^…) and generate SAS and check the SAS token and check the stored data from url and copy the TOKEN
* Create a virtual machine 🡺login 🡺download azure explorer-cloud storage management for windows 🡺install 🡺select “attach to resource” 🡺select “storage account or services” 🡺 go to storage account select the “generate key” from Security+networking 🡺copy the connection string and paste it on vm login 🡺 connect

LAB-8 Mange Virtual Machine

* **Ports 20 and 21:** File Transfer Protocol (FTP). FTP is for transferring files between a client and a server.
* **Port 22:** Secure Shell (SSH). SSH is one of many [tunneling](https://www.cloudflare.com/learning/network-layer/what-is-tunneling/) protocols that create secure network connections.
* [Port 25](https://www.cloudflare.com/learning/email-security/smtp-port-25-587/): Historically, [Simple Mail Transfer Protocol (SMTP)](https://www.cloudflare.com/learning/email-security/what-is-smtp/). SMTP is used for [email](https://www.cloudflare.com/learning/email-security/what-is-email/).
* **Port 53:** [Domain Name System (DNS)](https://www.cloudflare.com/learning/dns/what-is-dns/). DNS is an essential process for the modern Internet; it matches human-readable [domain names](https://www.cloudflare.com/learning/dns/glossary/what-is-a-domain-name/) to machine-readable IP addresses, enabling users to load websites and applications without memorizing a long list of IP addresses.
* **Port 80:** Hypertext Transfer Protocol (HTTP). HTTP is the protocol that makes the World Wide Web possible.
* **Port 123:** [Network Time Protocol (NTP)](https://blog.cloudflare.com/secure-time/). NTP allows computer clocks to sync with each other, a process that is essential for [encryption](https://www.cloudflare.com/learning/ssl/what-is-encryption/).
* **Port 179:** [Border Gateway Protocol (BGP)](https://www.cloudflare.com/learning/security/glossary/what-is-bgp/). BGP is essential for establishing efficient routes between the large networks that make up the Internet (these large networks are called [autonomous systems](https://www.cloudflare.com/learning/network-layer/what-is-an-autonomous-system/)). Autonomous systems use BGP to broadcast which IP addresses they control.
* **Port 443:** [HTTP Secure (HTTPS)](https://www.cloudflare.com/learning/ssl/what-is-https/). HTTPS is the secure and encrypted version of HTTP. All HTTPS web traffic goes to port 443. Network services that use HTTPS for encryption, such as [DNS over HTTPS](https://www.cloudflare.com/learning/dns/dns-over-tls/), also connect at this port.
* **Port 500:** Internet Security Association and Key Management Protocol (ISAKMP), which is part of the process of setting up secure [IPsec](https://www.cloudflare.com/learning/network-layer/what-is-ipsec/) connections.
* **Port 587:** Modern, secure SMTP that uses encryption.
* **Port 3389:** [Remote Desktop Protocol](https://www.cloudflare.com/learning/access-management/what-is-the-remote-desktop-protocol/) (RDP). RDP enables users to remotely connect to their desktop computers from another device.
* The Internet Assigned Numbers Authority (IANA) maintains the [full list](https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml) of port numbers and protocols assigned to them.
* PING stands for Packet InterNet Groper in computer networking field. It is a computer network administration software utility used to test the network connectivity between two systems. These systems may be any type of normal personal computer, Server, Switch, Router or Gateway.

**STEPS**

* 1 = create a resource
* 2= create a vnet.
* 3= create a virtual machine 2k16 (with overview) and add HTTP and RDP
* 4=Login vm
* 5= Diskmgmt.msc (check disks i.e how much extra disk is attached if not then go to created vm and its setting add disk and then again check )
* 6=Go to portal – VM- Disk- add and also add it to Diskmgmt.msc.
* 7= Install web server
* 8=go to local disk c –inetpub – wwwroot – its image – change – check from url
* 9= Go to vm(portal)- capture (option is given in VM nav bar it will be a image of VM which we have created and whose innet pub we changed)🡺also select option delete VM when it is created
* 10= fill the details.
* 11=create
* 12= Delete Vm.(or automatically it will be deleted if option is selected)
* 13= Create a vm – select “see all images” just at below where we select the 0.S – shared image – select – fill creds.- create
* (will download same as the image we captured already)

**LAB-9 Serverless Computing**

**Lab a. Implementing Web app**

**Crete a Resource group 🡺App service(search)🡺create a web app 🡺select/create a resource group🡺runtime stack 🡺select region 🡺create 🡺manage deployment form app**

**Lab b. Creating container Instance**

**Create 🡺enable port (443 for https)🡺copy “fQDN” or Public IP**

**Lab c. Creating container app 🡺create by selecting basic details 🡺see the deployment by application url**

**LAB-10 Files & Folder Backup**

* Create resource group
* Create a virtual network
* Create a virtual machine (2k16)
* Create storage account
* Create recovery service vault
* Go to resource – create a backup – Azure VM
* Go to vm –add disk –
* Create a folder with some files –add roles –web server
* Go to recovery service vault –backup item-start backup with date
* Go to backup
* On primes
* Files and folder –prepare infrastructure- download two files
* Copy both and paste on login vm
* Install setup
* Proceed to register
* Add data in it and exit
* Delete data –go to portal-backup item-and restore data
* Delete vm and backup item – restore vm.

**LAB -11 Monitoring and Review**

* Create a resource group
* Create a virtual network
* Create a virtual machine
* Go to monitor 🡺 select “VM Insights” 🡺 configure VM insights 🡺enable VM
* Create alert rules🡺 select the resource group selected 🡺select signal (delete VM status)🡺alert rule 🡺 create action group ( for notification on Mail or phone no.)