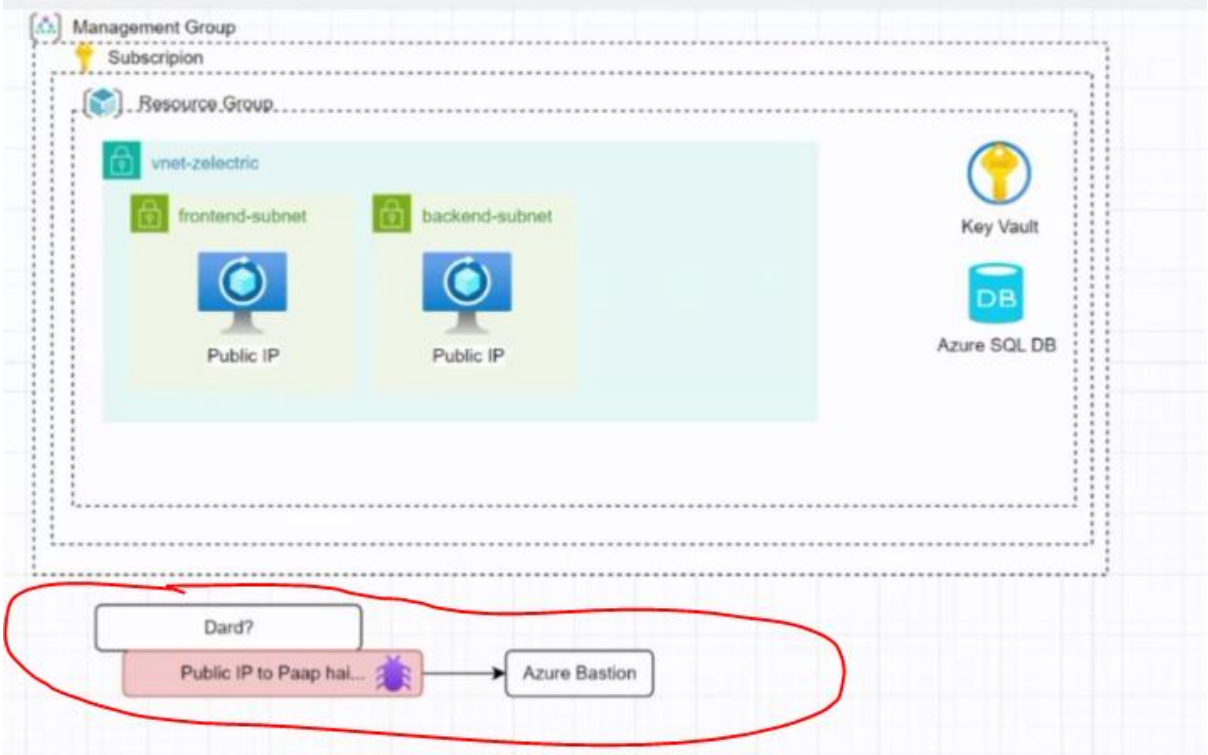
31) 24 August 2024 – AzureBastionAndVMForeach

AGENDA – HOW TO USE AND ACCESS AZURE BASTION & PUT FOR EACH LOOP IN THE CODE AND MAKE 2 VMS

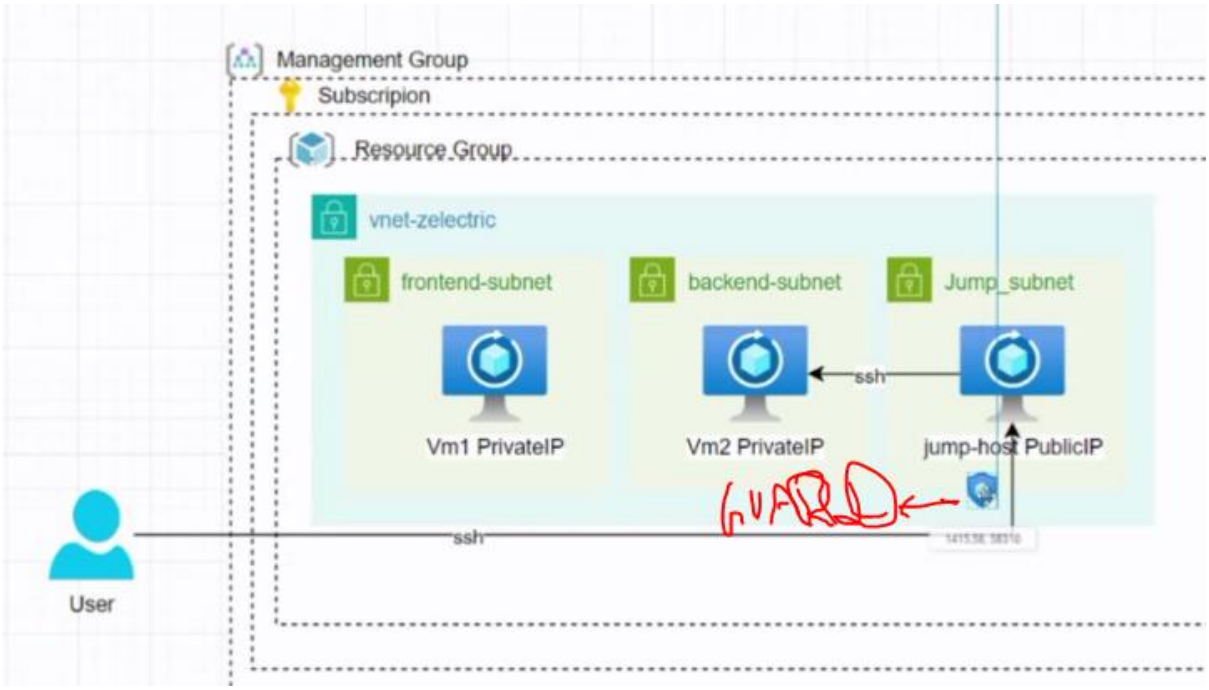
1)



++

AGENDA - JUMP SUBNET/ JUMP HOST

1) Jump server has public IP which has guard into it to disallow unknowns to enter in network.



++

AGENDA – AZURE BASTION

1) Now instead of jump server we will put azure bastion because jump server has limitations for number of VMs connected through it.

2) Azure bastion has also public ip assigned to it

3) TLS – It means https i.e. green lock

4)

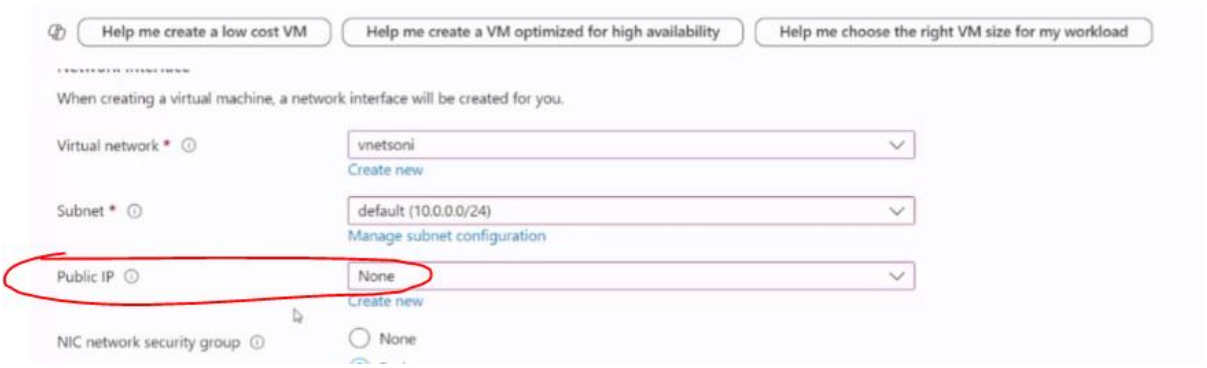
- Required inbound ports:
  - For Windows VMs: RDP (3389)
  - For Linux VMs: SSH (22)

5) An azure bastion fitted in one vnet can access vms of that particular network only. But it cannot access vms of another vnet. For that vnet peering is required.

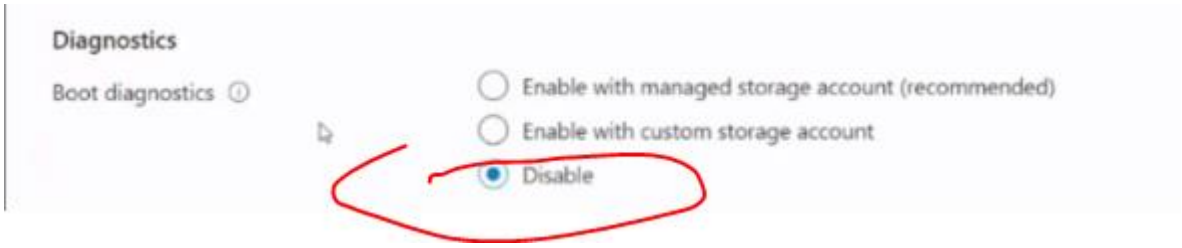
++

AGENDA – VIRTUAL MACHINE

1) Create virtual machine that has no public key below



2) Make boot diagnostic disable



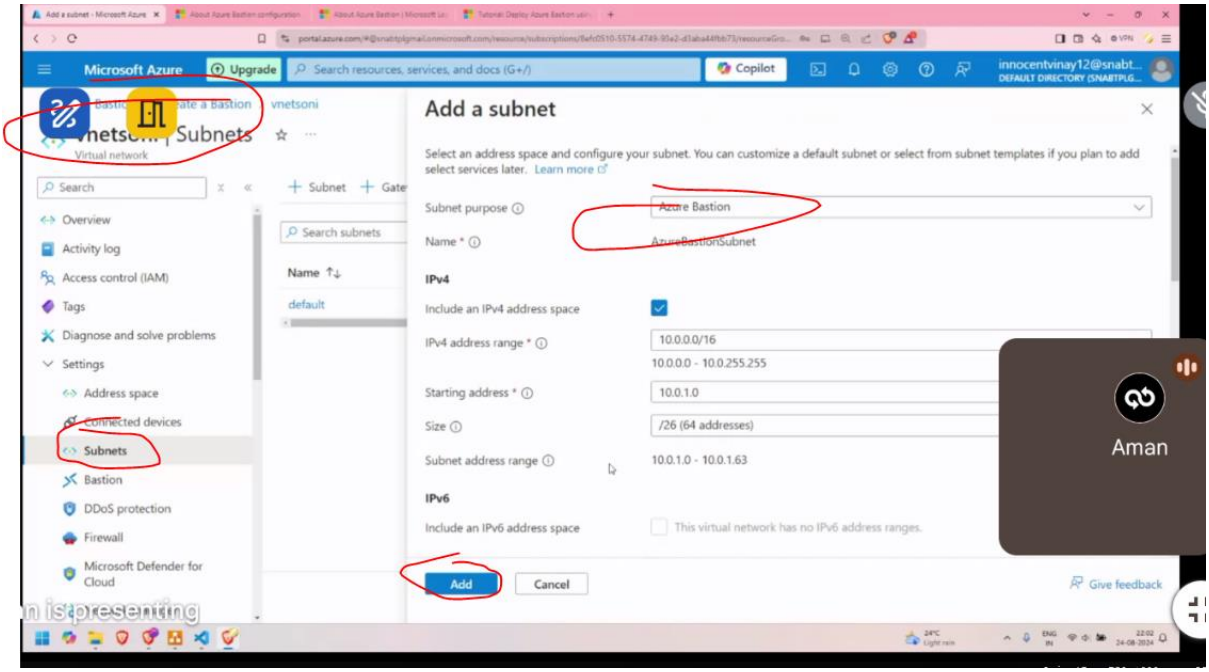
++

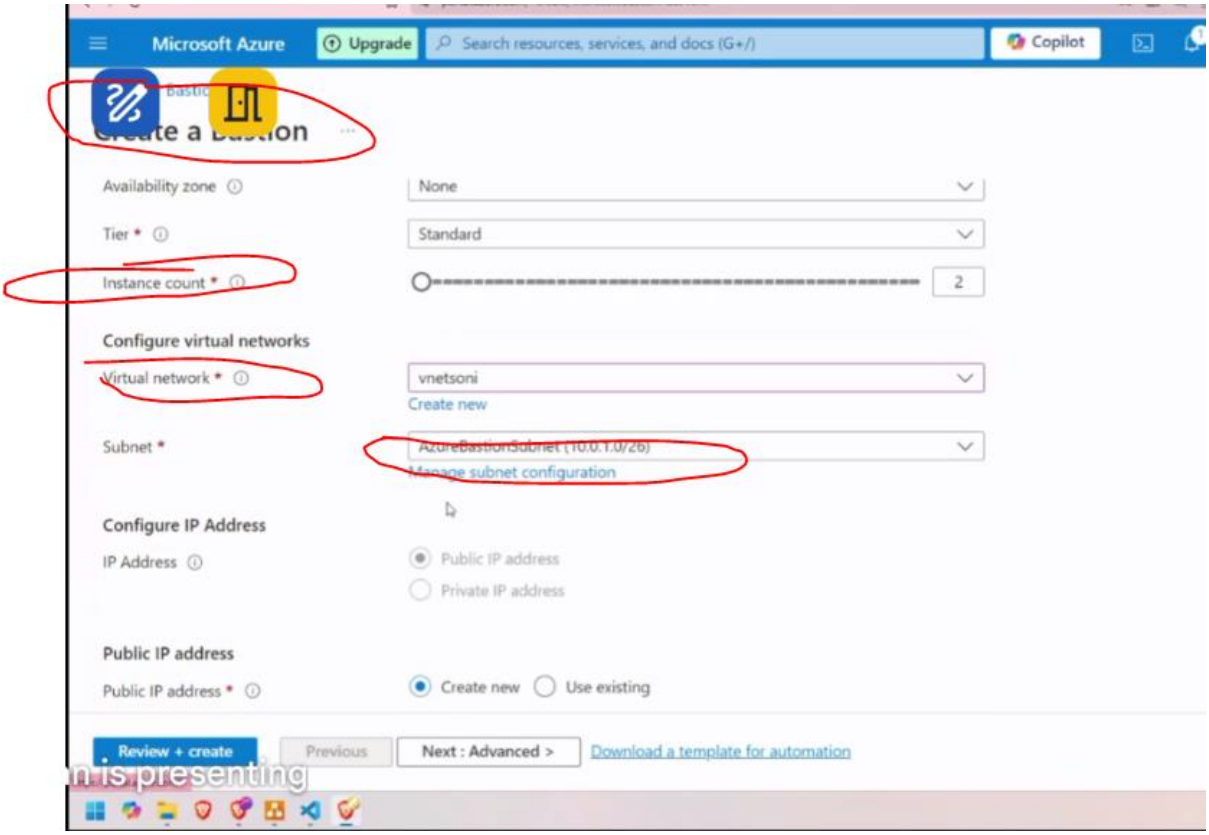
AGENDA – CREATE BASTION IN VNET ON PORTAL

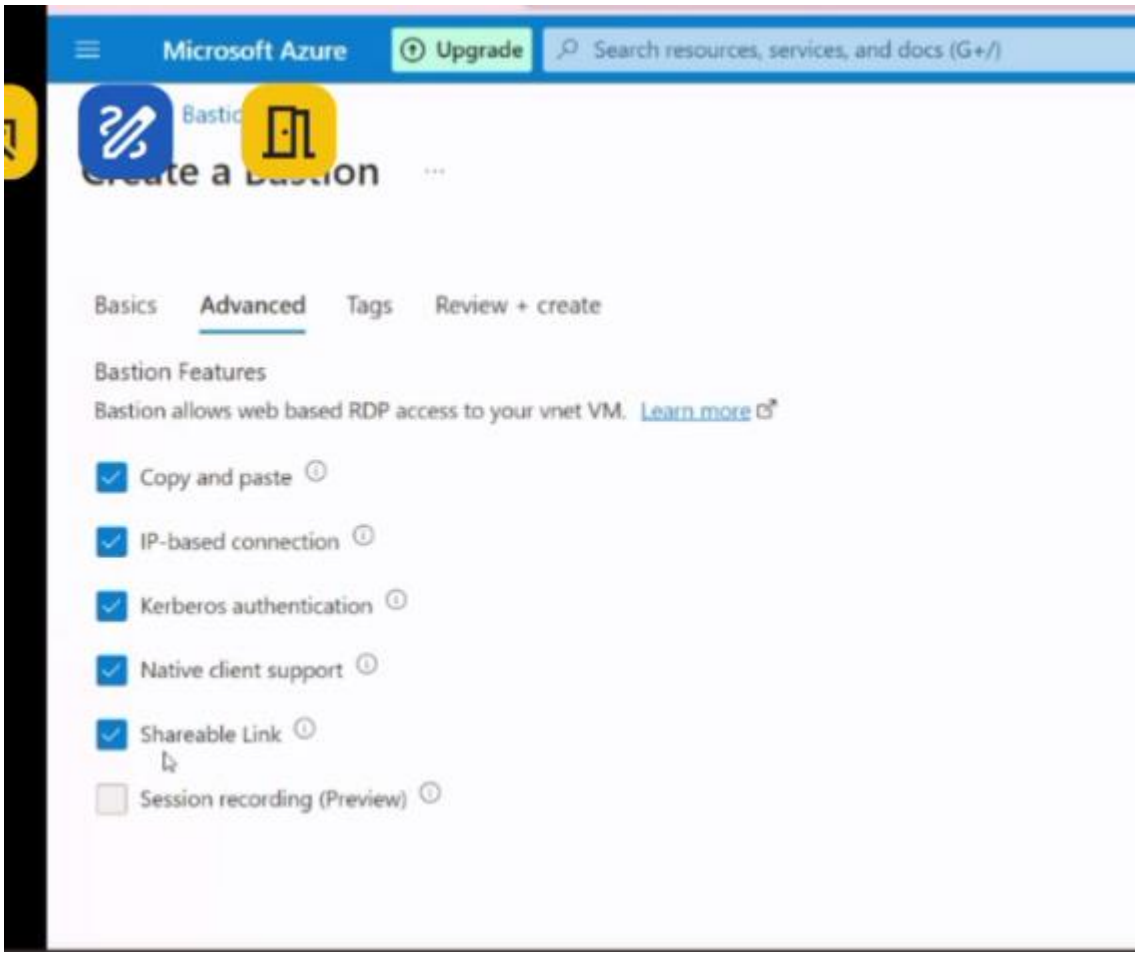
1) Go to vnet page

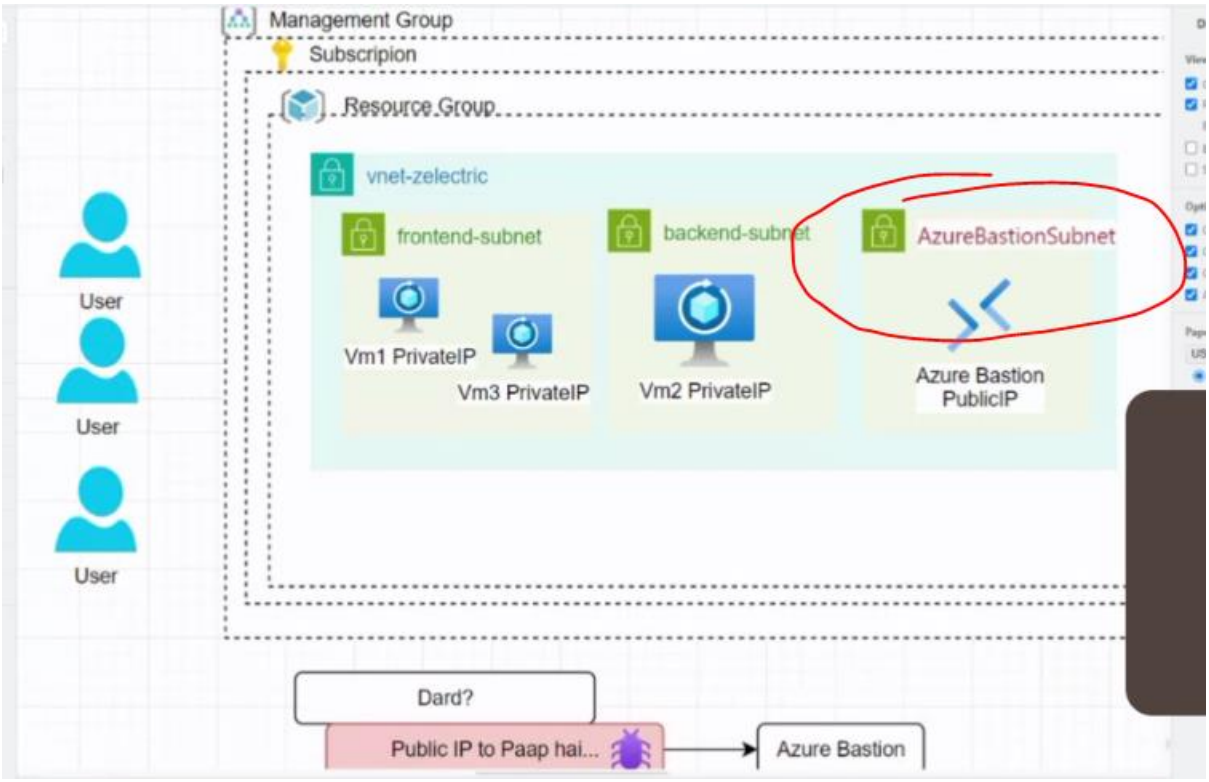
2) Select subnets -> Add a subnet

3) Default name is azure bastion subnet -> add

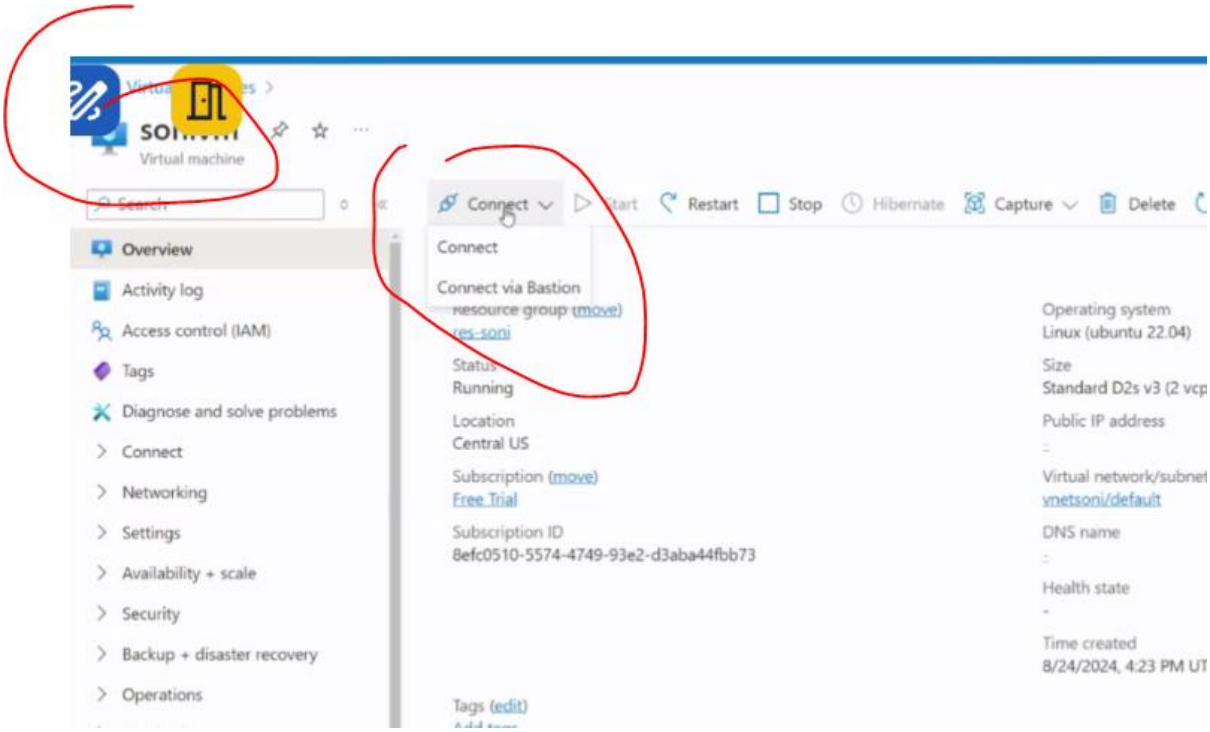


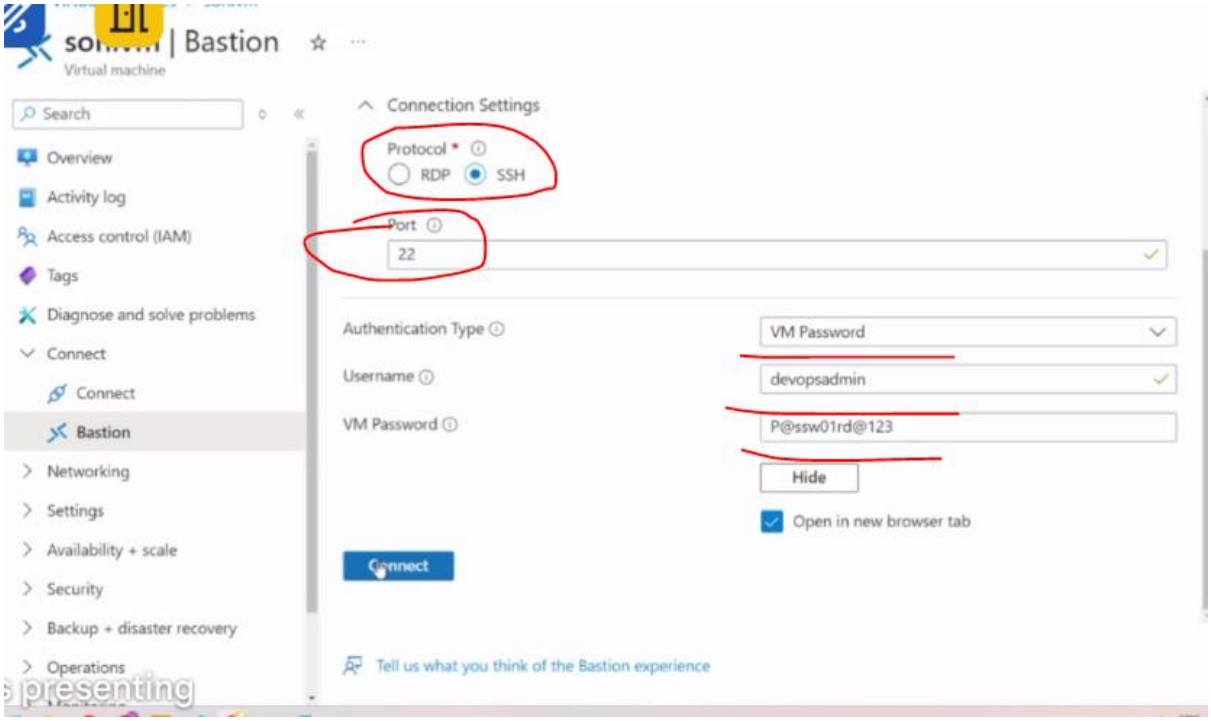

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Availability zone
None
Tier *
Standard
Instance count *
2
Configure virtual networks
Virtual network *
vnetsoni
Create new
Subnet *
Manage subnet configuration
Configure IP Address
IP Address
Public IP address
Private IP address
Public IP address
Public IP address *
Create new
Use existing
Review + create
Previous
Next : Advanced >
Download a template for automation


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Basics
Advanced
Tags
Review + create
Bastion Features
Bastion allows web based RDP access to your vnet VM.
Learn more
Copy and paste
IP-based connection
Kerberos authentication
Native client support
Shareable Link
Session recording (Preview)



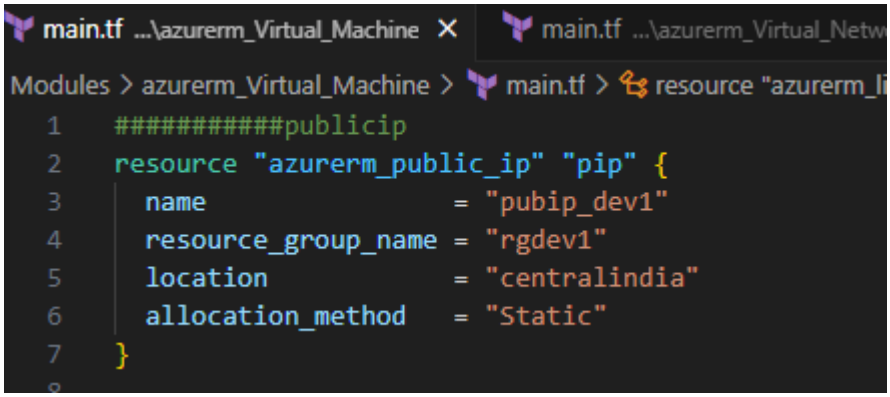
4) Now to connect bastion go to vm and select “Connect via bastion”





++

1) Now in code of VM, remove below public ip code as we have set up or created bastion



```
##############nic
resource "azurerm_network_interface" "nic" {
  name                = "Virtual_nic"
  location            = "centralindia"
  resource_group_name = "rgdev1"

  ip_configuration {
    name                          = "nic_ip1"
    subnet_id                     = data.azurerm_subnet.frontend_subnet.id
    private_ip_address_allocation = "Dynamic"
    public_ip_address_id          = azurerm_public_ip.pip.id
  }
}
```

2) Bring subnet data block in vm code

3) For subnet_id use each.key to map subnet_id as per vms respectively like for

Frontend subnet = vm1

Backend subnet = vm2

```
ip_configuration {
  name                          = "nic_ip1"
  subnet_id                     = data.azurerm_subnet.subnets[each.key].id
  private_ip_address_allocation = "Dynamic"
}
```

4) We can use same each.key concept for vm's id and password as well, as we had used for subnet case

```
admin_username                  = data.azurerm_key_vault_secret.kvsecret_username.value
admin_password                  = data.azurerm_key_vault_secret.kvsecret_password.value
```

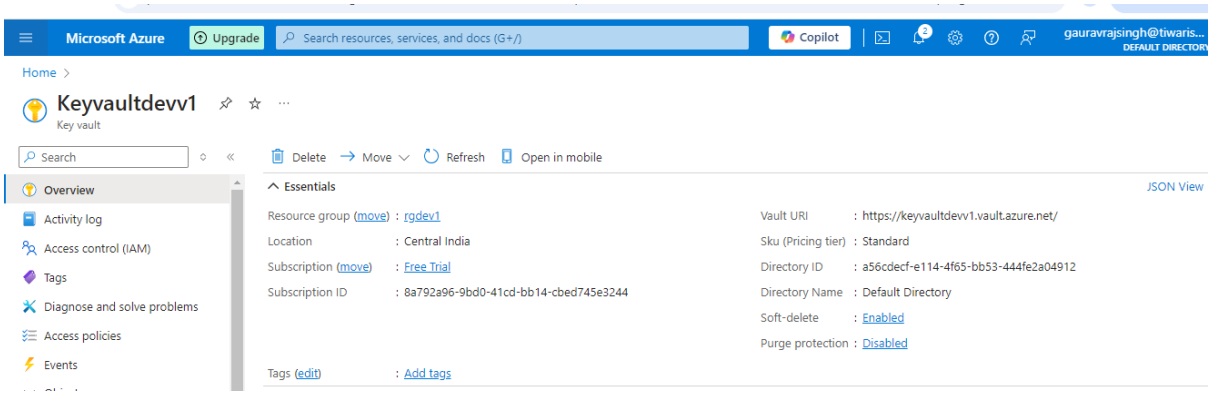
5) Use each.key concept for below network_interface_ids also

```
network_interface_ids           = [azurerm_network_interface.nic[each.key].id]
```

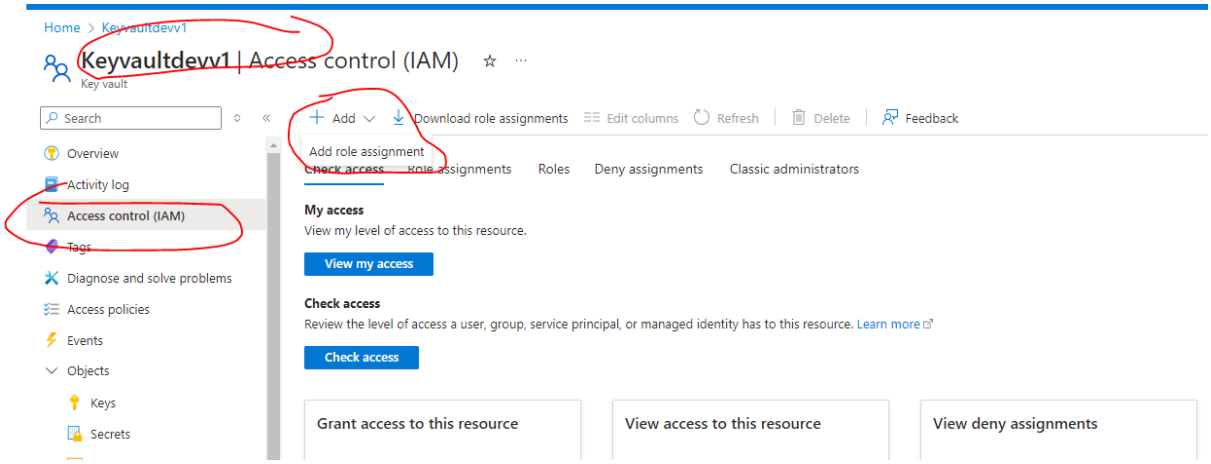
++

AGENDA – CREATE KEY VAULT ON PORTAL

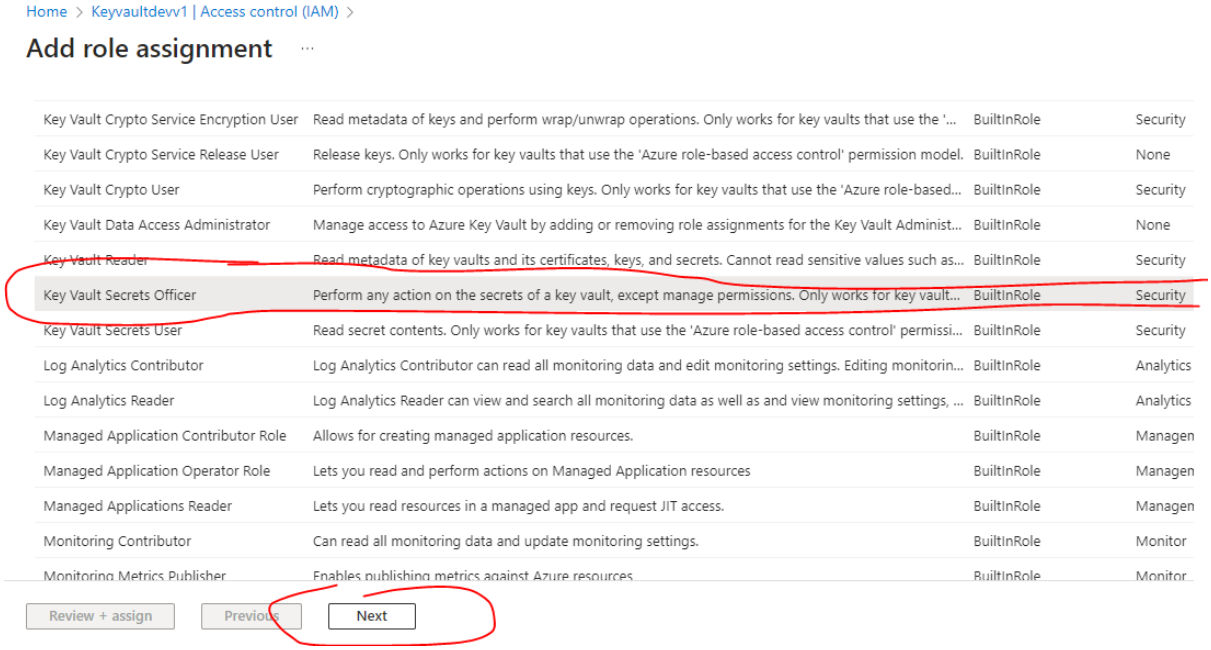
1) Create keyvault

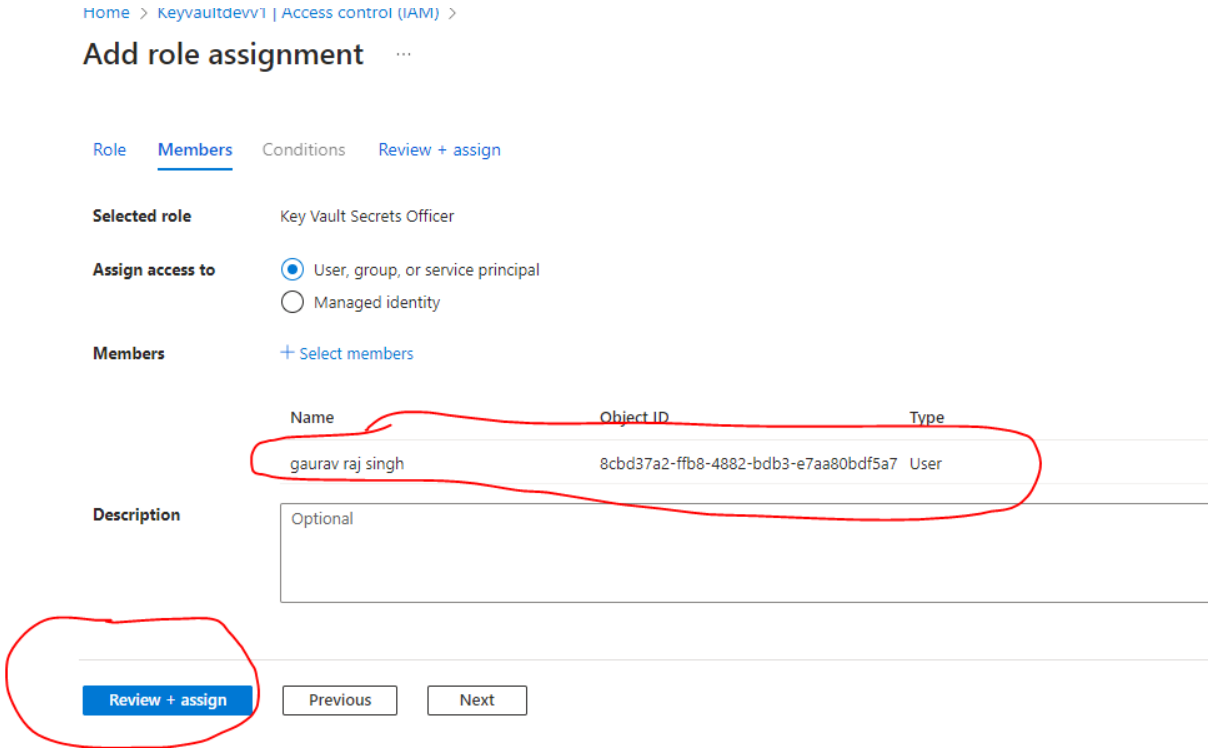


2) To create secret. Firstly provide access



3) Now give below role access

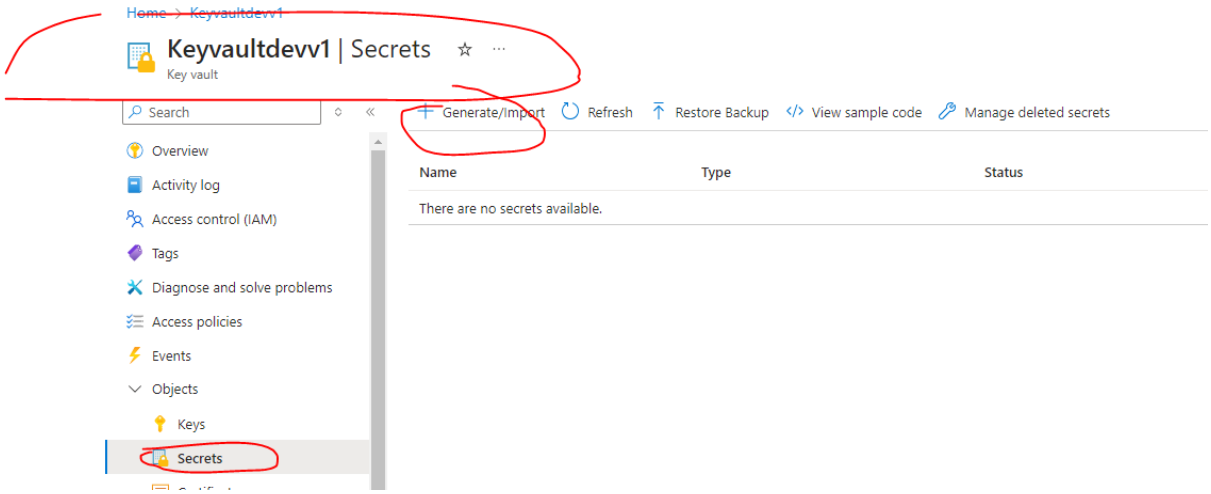




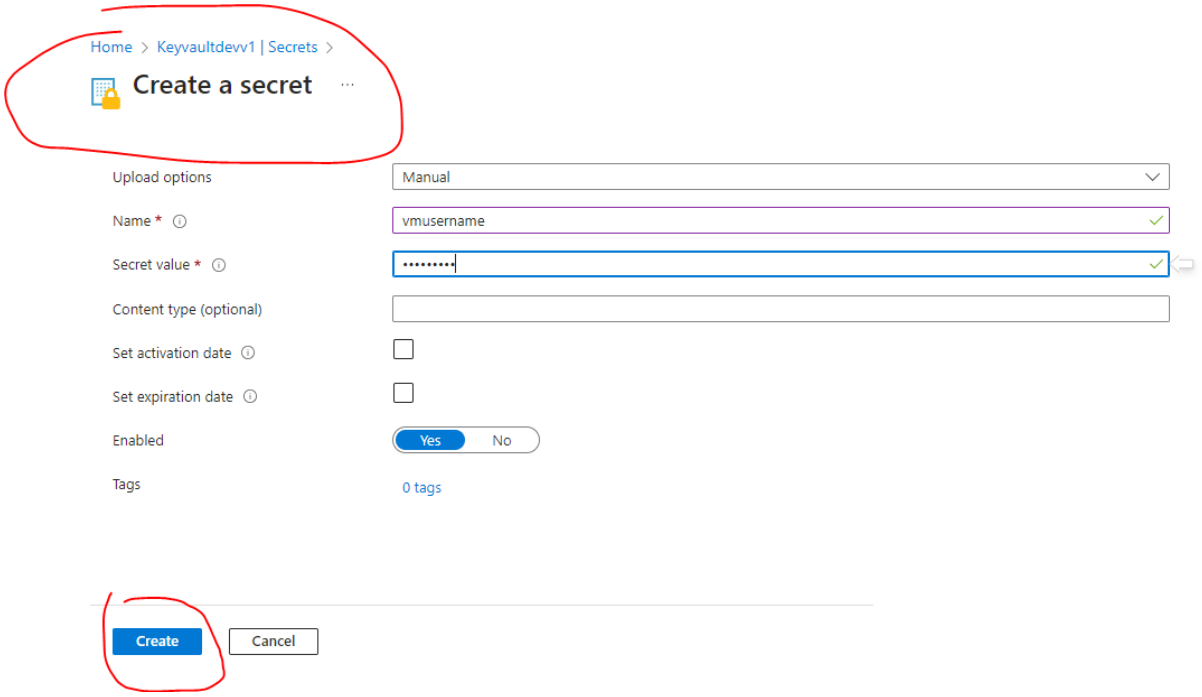
++

AGENDA – CREATE SECRET

1)

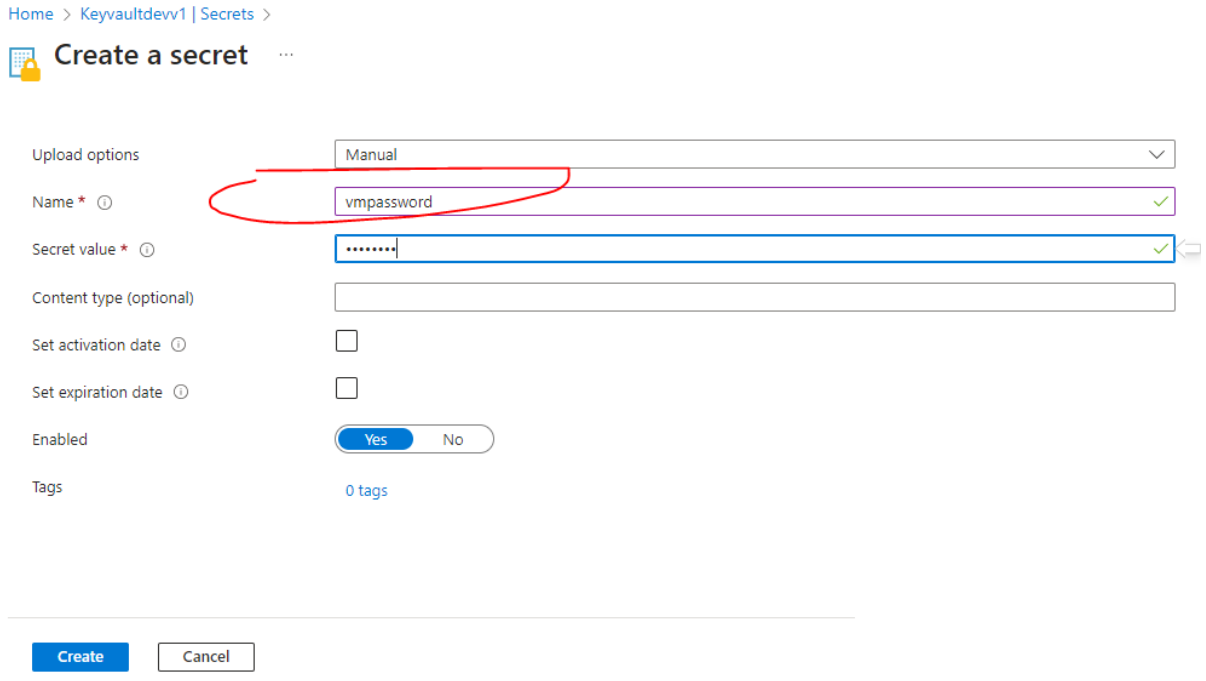


i) Create for vmusername

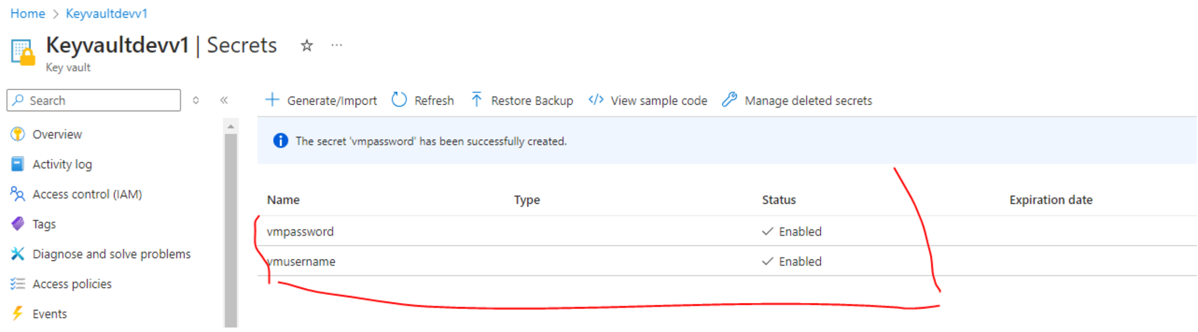


Secret value = adminuser

ii) Create for vmpassword



Secret value = mom6daD?



Assignment

Make with foreach + map of object

1) 1 folder of bastion

2) 1 folder of keyvault

Both should be in child as well as in module