

### 31) 24 August 2024 – AzureBastionAndVMForeach

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

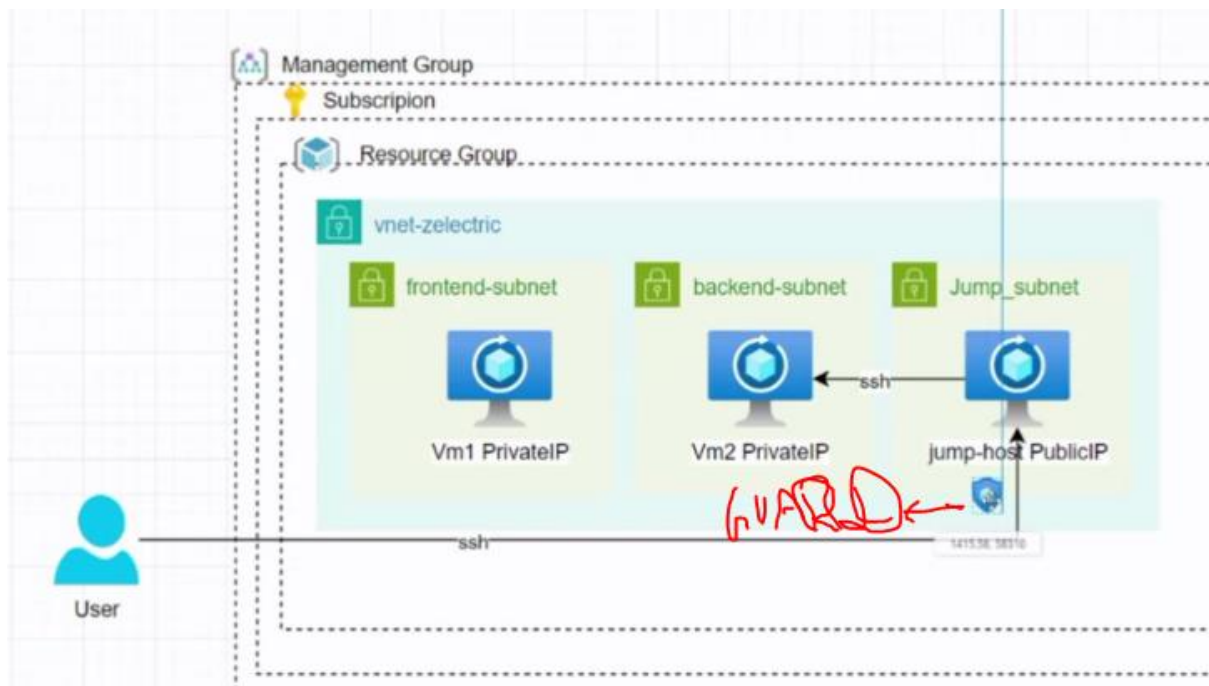
1)



+++++

#### 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

Help me create a low cost VM   Help me create a VM optimized for high availability   Help me choose the right VM size for my workload

When creating a virtual machine, a network interface will be created for you.

Virtual network \*    
 [Create new](#)

Subnet \*    
 [Manage subnet configuration](#)

Public IP    
 [Create new](#)

NIC network security group ☐ None

2) Make boot diagnostic disable

**Diagnostics**

Boot diagnostics ☐ Enable with managed storage account (recommended)   
 ☐ Enable with custom storage account   
 ☒ **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

The screenshot shows the Microsoft Azure portal interface. On the left, the 'Subnets' option under the 'vnetsoni' virtual network is selected. The main pane displays the 'Add a subnet' dialog. In this dialog, the 'Subnet purpose' is set to 'Create Bastion' (highlighted with a red circle), and the 'Name' is 'AzureBastionSubnet'. The 'Add' button at the bottom is also highlighted with a red circle. The background shows the Azure portal navigation pane with 'Subnets' selected.

Microsoft Azure Upgrade Search resources, services, and docs (G+/I) Copilot

## Create a Bastion

Availability zone ⓘ None

Tier \* ⓘ Standard

Instance count \* ⓘ 2

Configure virtual networks

Virtual network \* ⓘ vnetsoni  
[Create new](#)

Subnet \* ⓘ AzureBastionSubnet (10.0.1.0/26)  
[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+/I)

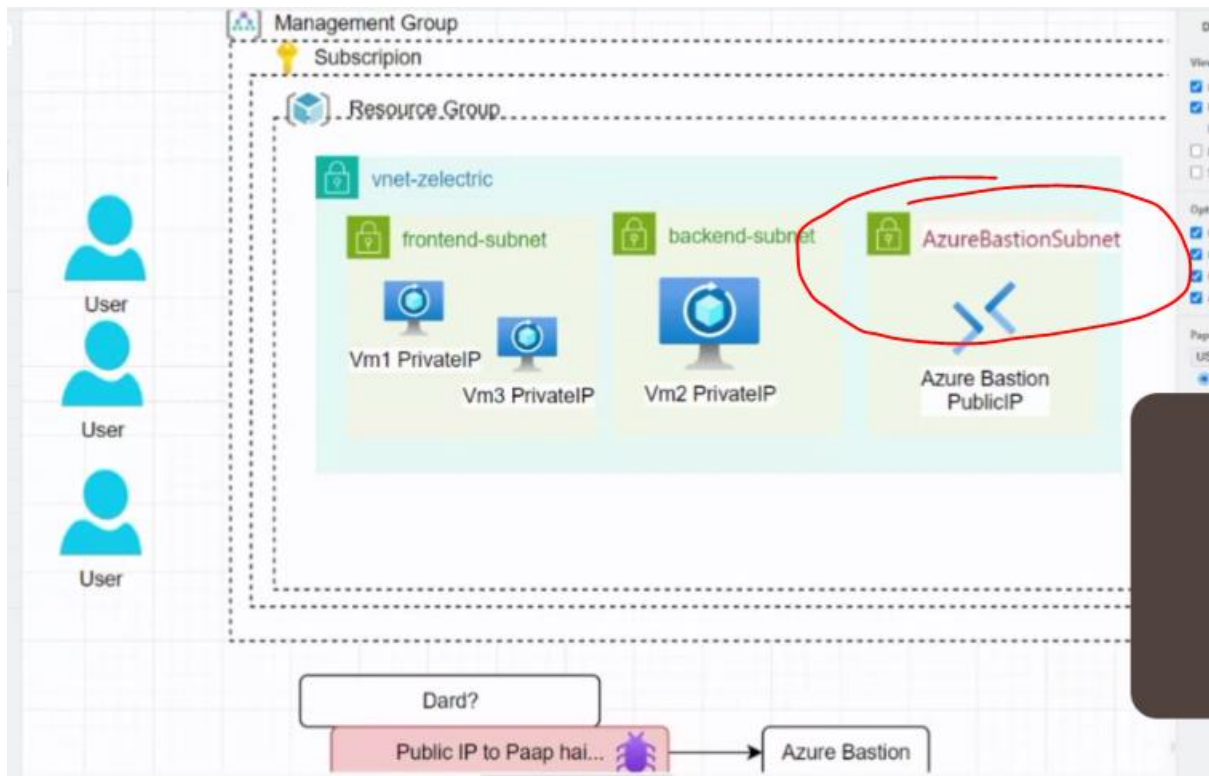
## Create a Bastion

Basics Advanced Tags Review + create

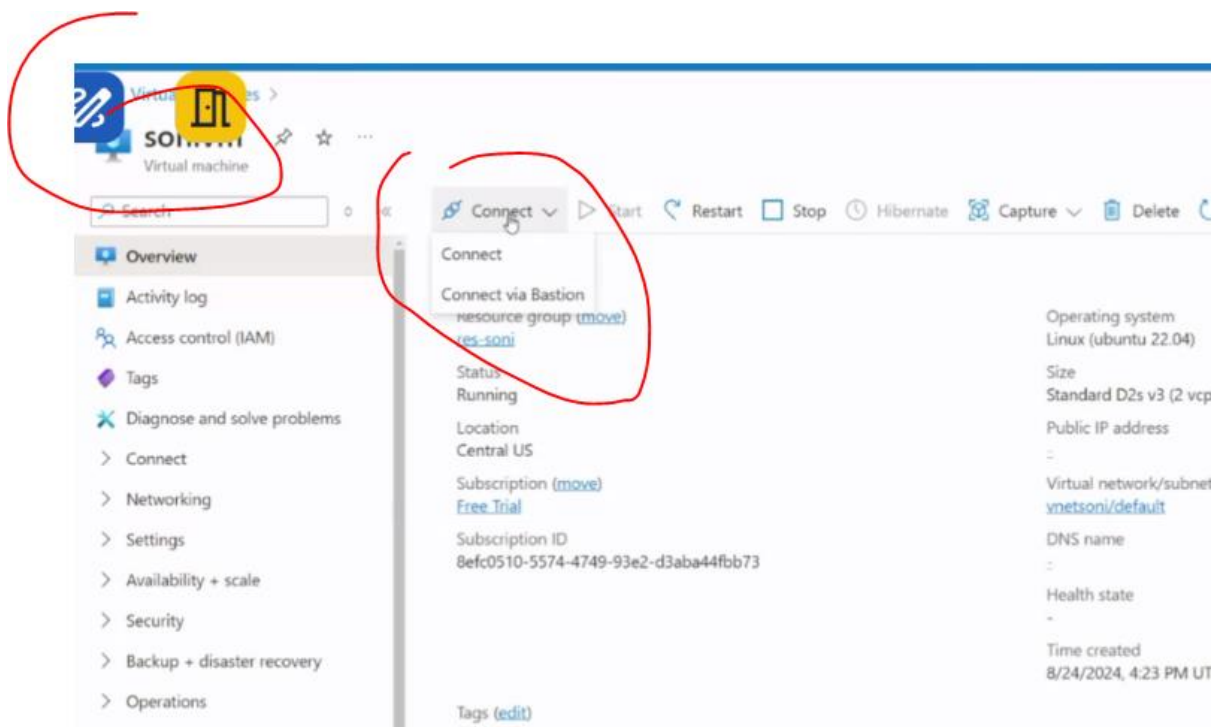
Bastion Features

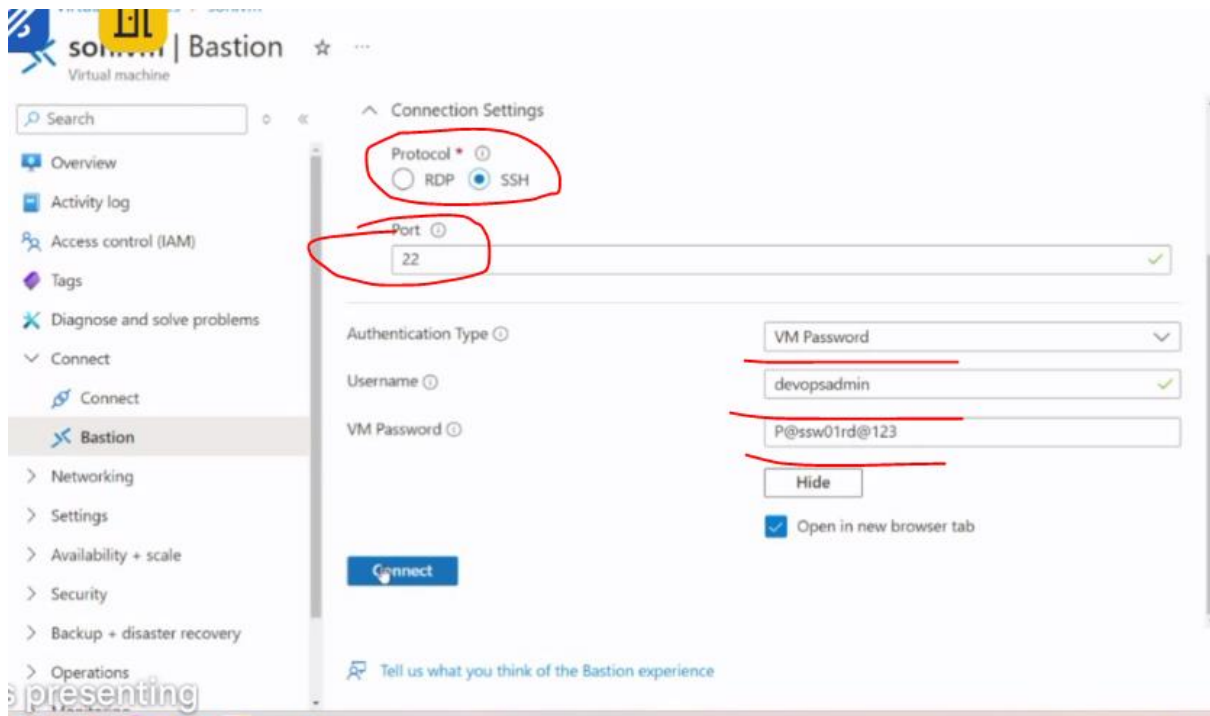
Bastion allows web based RDP access to your vnet VM. [Learn more](#)

- ☒ 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”





A popup blocker is preventing new window from opening. Please allow popups and retry.

+++++

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

```
main.tf ...\azurerm_Virtual_Machine X main.tf ...\azurerm_Virtual_Netw
Modules > azurerm_Virtual_Machine > main.tf > resource "azurerm_li
1 #####publicip
2 resource "azurerm_public_ip" "pip" {
3   name           = "pubip_dev1"
4   resource_group_name = "rgdev1"
5   location        = "centralindia"
6   allocation_method = "Static"
7 }
8
```

```
#####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

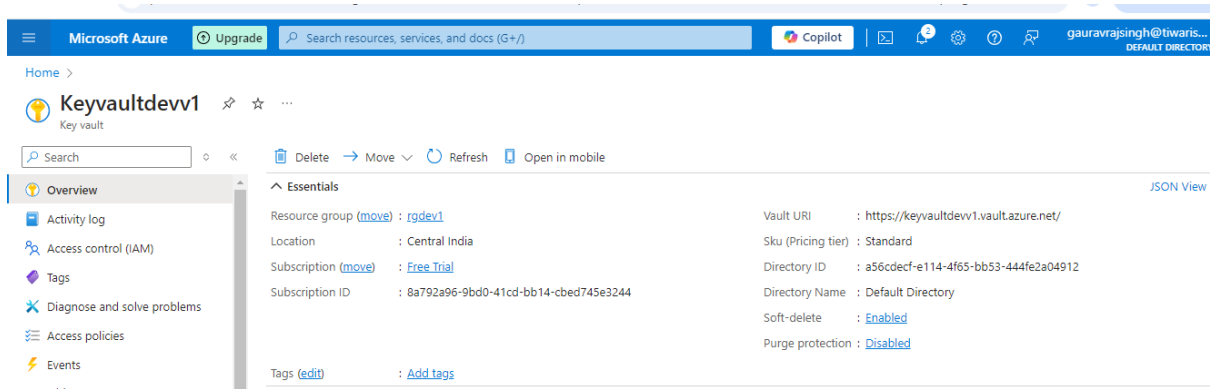
```
disable_password_authentication = false
network_interface_ids          = [azurerm_network_interface.nic[each.key].id]
```

+++++

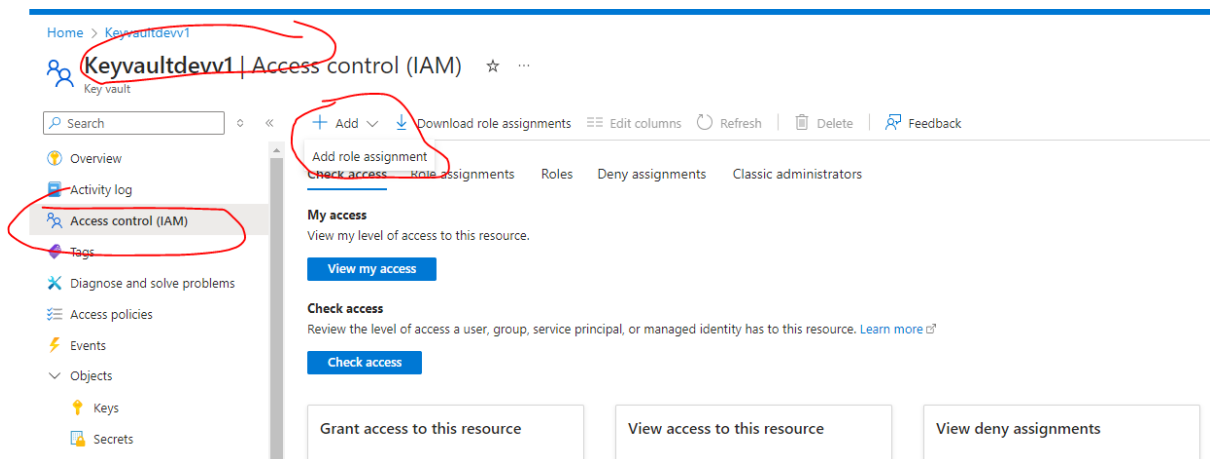
## AGENDA – CREATE KEY VAULT ON PORTAL

1) Create keyvault

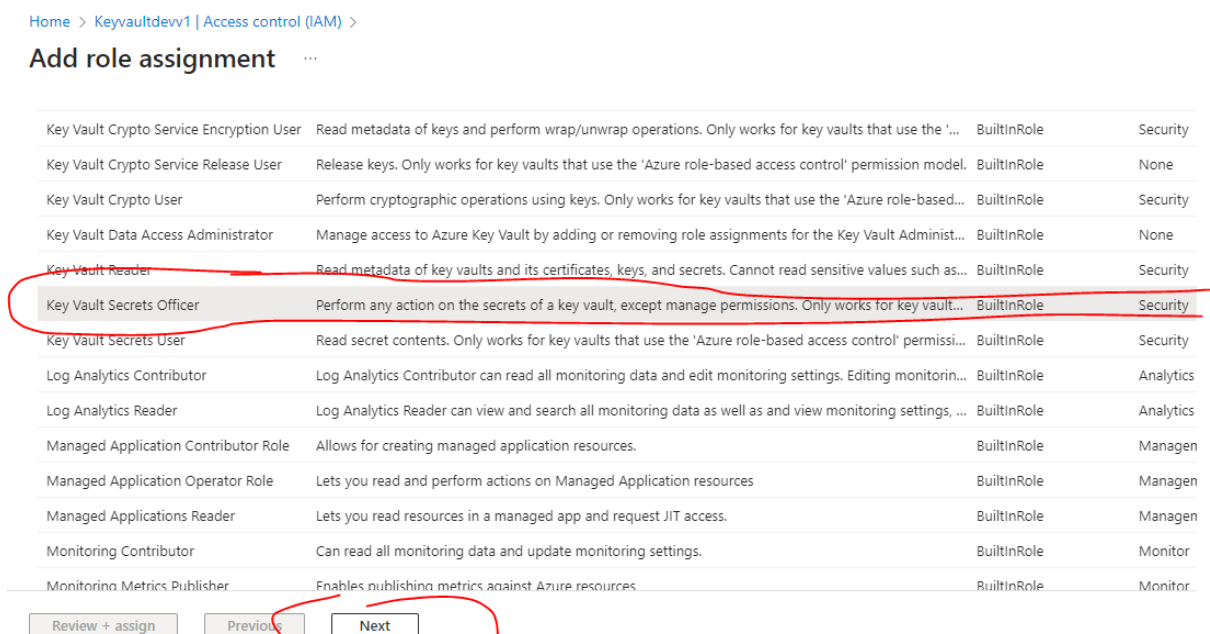




## 2) To create secret. Firstly provide access



## 3) Now give below role access





## Add role assignment

Role **Members** Conditions Review + assign

**Selected role** Key Vault Secrets Officer

**Assign access to** ☒ User, group, or service principal  
☐ Managed identity

**Members** + Select members

Name	Object ID	Type
gaurav raj singh	8cbd37a2-ffb8-4882-bdb3-e7aa80bdf5a7	User

**Description** Optional

Review + assign

Previous

Next

## AGENDA – CREATE SECRET

1)

Home > Keyvaultdevv1

### Keyvaultdevv1 | Secrets

Key vault

Search

Generate/Import Refresh Restore Backup View sample code Manage deleted secrets

Name	Type	Status
There are no secrets available.		

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Access policies
- Events
- Objects
  - Keys
  - Secrets**

i) Create for vmusername

Home > Keyvaultdevv1 | Secrets >

## Create a secret

Upload options: Manual

Name \* ①: vmusername

Secret value \* ①: .....

Content type (optional):

Set activation date ①: ☐

Set expiration date ①: ☐

Enabled: Yes No

Tags: 0 tags

Create Cancel

Secret value = adminuser

ii) Create for vmpassword

Home > Keyvaultdevv1 | Secrets >

## Create a secret

Upload options: Manual

Name \* ①: vmpassword

Secret value \* ①: .....

Content type (optional):

Set activation date ①: ☐

Set expiration date ①: ☐

Enabled: Yes No

Tags: 0 tags

Create Cancel

Secret value = mom6daD?

Home > Keyvaultdevv1

Keyvaultdevv1 | Secrets ☆ ...

Key vault

Search

Generate/Import Refresh Restore Backup View sample code Manage deleted secrets

The secret 'vmpassword' has been successfully created.

Name	Type	Status	Expiration date
vmpassword		✓ Enabled	
vmusername		✓ Enabled	

+++++

+++++

### 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