#SNPIM-120478 : **Eriez: Find the Alternative Way to Login into the Eriez Servers as we decomminsoed the N-able**

Servers on Nable

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Eriez Manufacturing Company. | | | | |
| Name | Network Address | Device Class | License Mode | Virtual network/subnet |
| AP-BACK02 | 10.1.0.13 | Servers - Windows | Professional | EriezVirtualNetwork/default |
| AP-DC01 | 10.1.0.5 | Servers - Windows | Professional | EriezVirtualNetwork/default |
| AP-SYNC01 | 10.1.0.9 | Servers - Windows | Professional | EriezVirtualNetwork/default |
| AP-SYNC02 | 10.1.0.10 | Servers - Windows | Professional | EriezVirtualNetwork/default |
| APBACK01 | 10.1.0.11 | Servers - Windows | Professional | EriezVirtualNetwork/default |
| EriezAzureDFS | 10.1.0.14 | Servers - Windows | Professional | EriezVirtualNetwork/default |
| Sonic FIrewall | 192.168.0.7 | Switch/Router | Essential | Note- this Physical device has no Monitoring configured. |

Other devices on same Virtual network/subnet

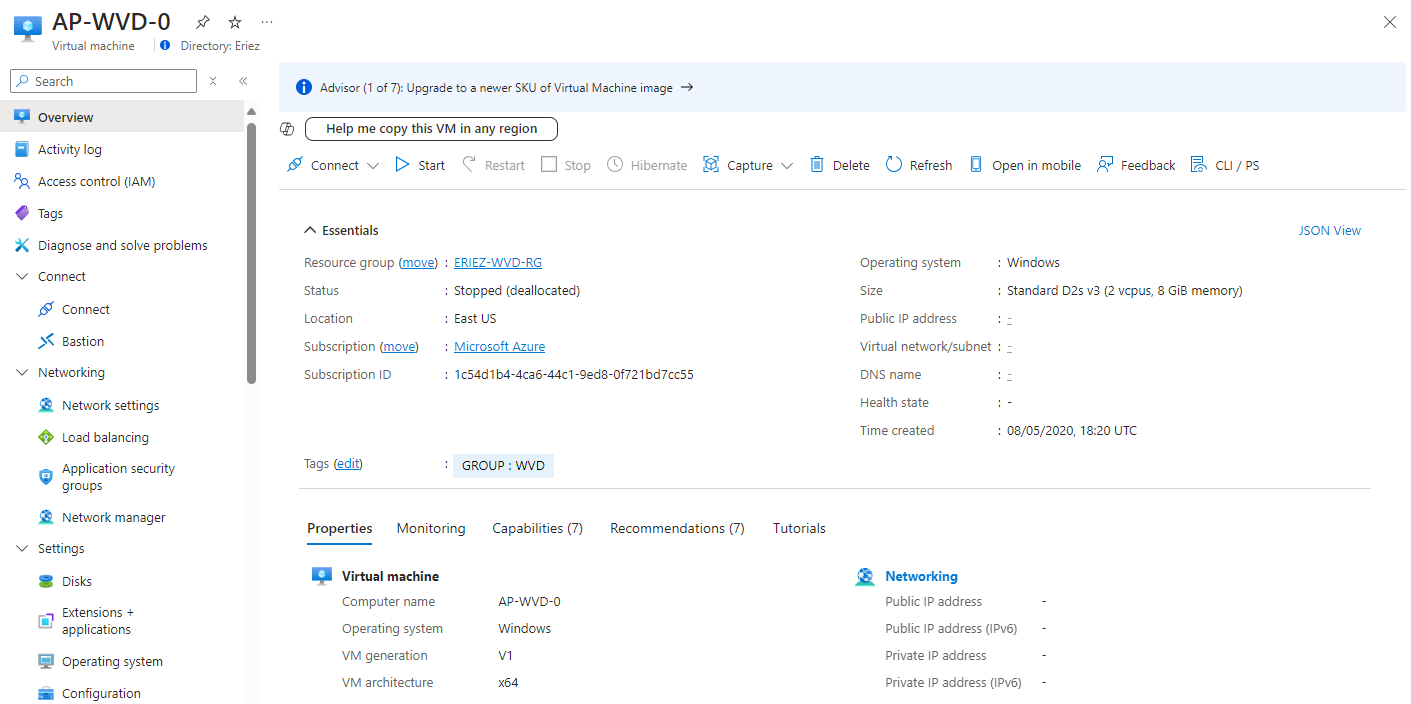
|  |  |  |
| --- | --- | --- |
| Server | Network interface | IP Address |
| AP-NESSUS01 | ap-nessus01347 | 10.1.0.4 |
| AP-ORCH02 | ap-orch02151\_z1 | 10.1.0.16 |
| AP-Scan01 | ap-scan01404\_z1 | 10.1.0.12 |
| NIC not associated to VM | apdb01546 | 10.1.0.7 |

Next Action Plan- remove Nable agent from servers.

Account used by SNP- ERIEZUSA\snp

Eriez AVD assigned to SNP.

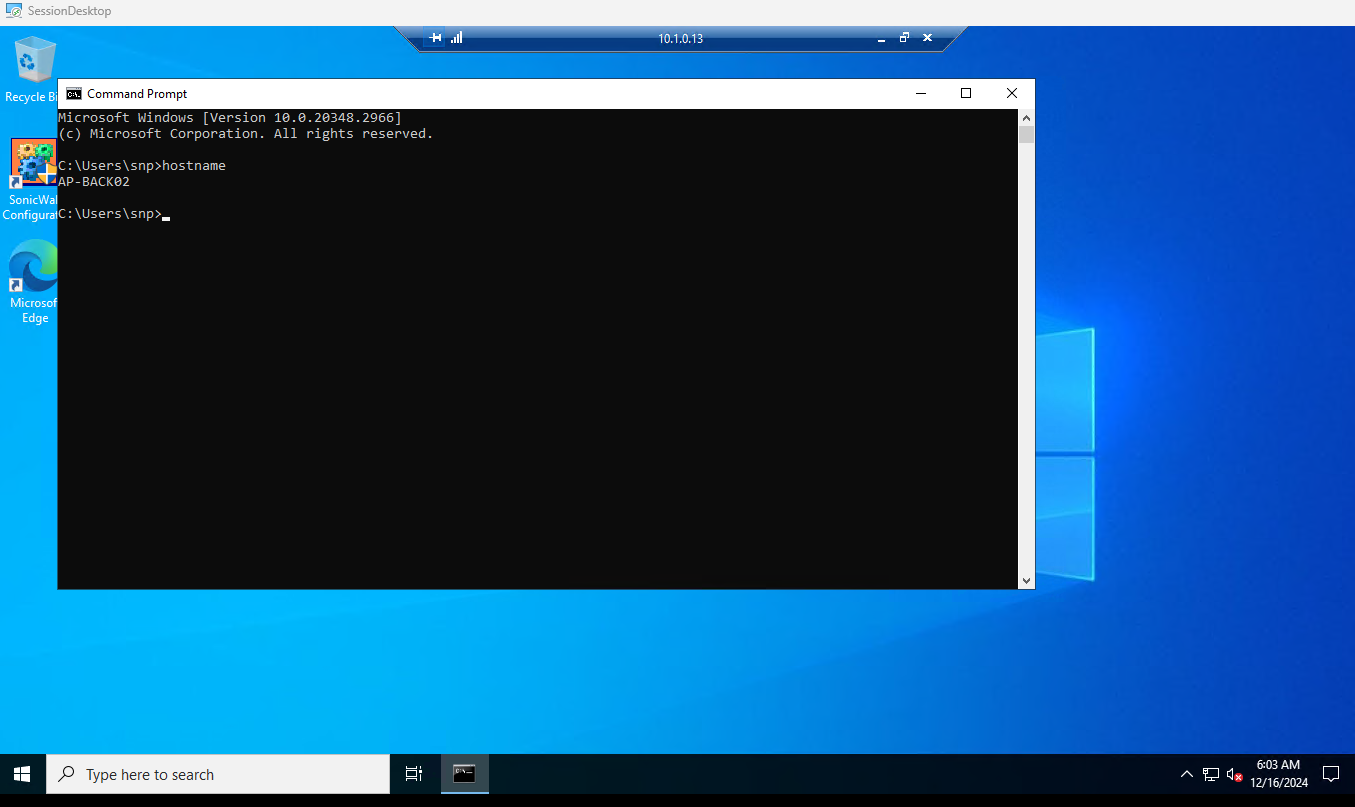
[AP-WVD-0.EriezUSA.net](https://portal.azure.com/)



Existing Network–

[EriezVirtualNetwork/WVDSubnet](https://portal.azure.com/#blade/HubsExtension/ResourceMenuBlade/id/%2Fsubscriptions%2F1c54d1b4-4ca6-44c1-9ed8-0f721bd7cc55%2FresourceGroups%2FEriezHybridRG%2Fproviders%2FMicrosoft.Network%2FvirtualNetworks%2FEriezVirtualNetwork)

Able to take rdp to servers from AVD.



The subnet associated with servers which we need to connect is “default” subnet. And the subnet associated with a NSG called “Production\_NSG”.

A screenshot of a computer

Description automatically generated

The NSG allow Inbound traffic from VNET.

A screenshot of a computer

Description automatically generated

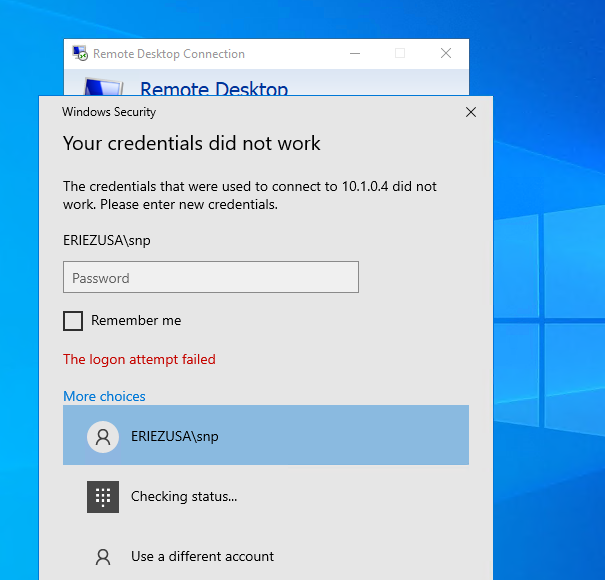
As you are looking into more security and not allowing the rdp to all vms. We will follow below steps-

* .Next plan of action create a ASG assign servers need to connect from AVD.
* Block VNET default inbound rule.
* Create a new security rule to allow traffic from AVD to ASG

Additionally traffic is block to other servers and we are using SNP account which has very limited permissions to connect to limited servers.

A screenshot of a computer

Description automatically generated



Client is using AVD for different purpose. so, alternative was looking for bastion.

Targeted to create bastion to have connection to other servers.

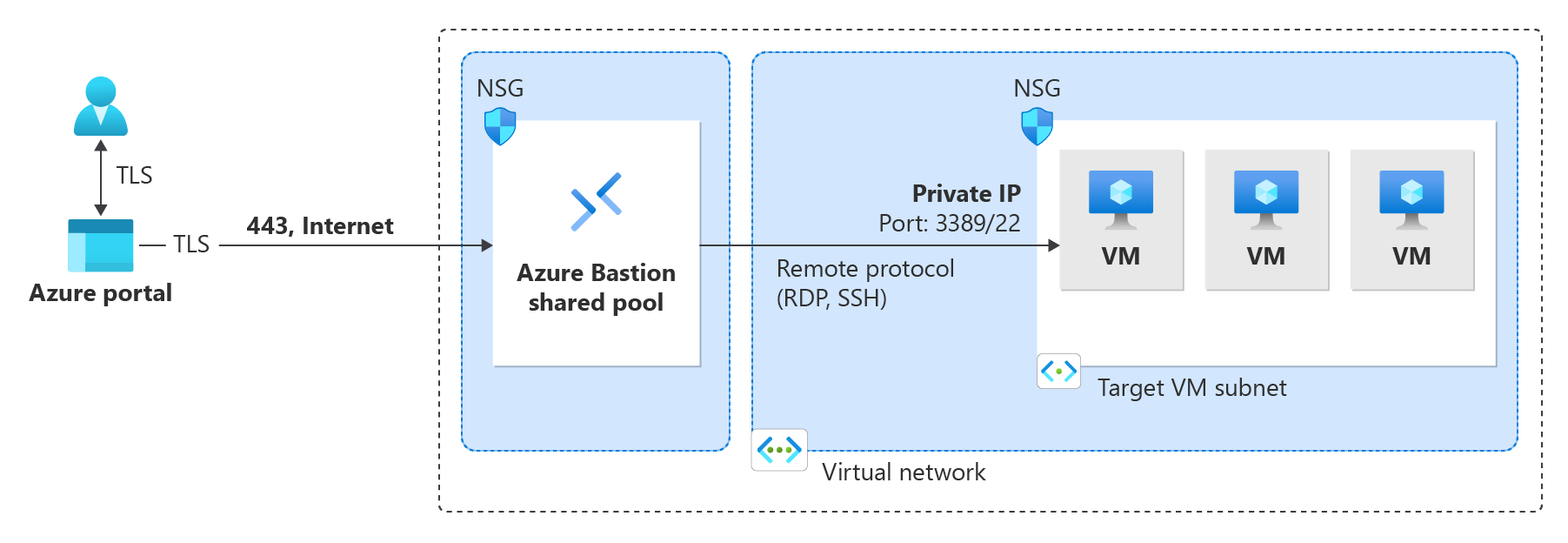
1. Difference between basic and standard bastion versions.

* **Instances**:
  + **Basic**: Comes with two instances by default.
  + **Standard**: Allows you to specify the number of instances, starting with a minimum of two
* **Features**:
  + **Basic**: Provides essential features for secure RDP/SSH connectivity to your virtual machines without needing a public IP address
  + **Standard**: Includes all Basic features plus additional capabilities like auto-scaling, support for multiple virtual networks, and enhanced security features
* **Pricing**:
  + **Basic**: Generally more cost-effective, priced at around $0.19 per hour
  + **Standard**: Slightly more expensive, priced at around $0.29 per hour

When Azure Bastion Basic SKU mentions "comes with two instances by default," it means that the Bastion deployment will automatically create and use two instances for handling connections. This setup ensures redundancy and availability.

These two instances are not a limit on the number of connections but rather the number of Bastion hosts running to manage the connections. You can have multiple users connecting to your virtual machines through these two instances simultaneously

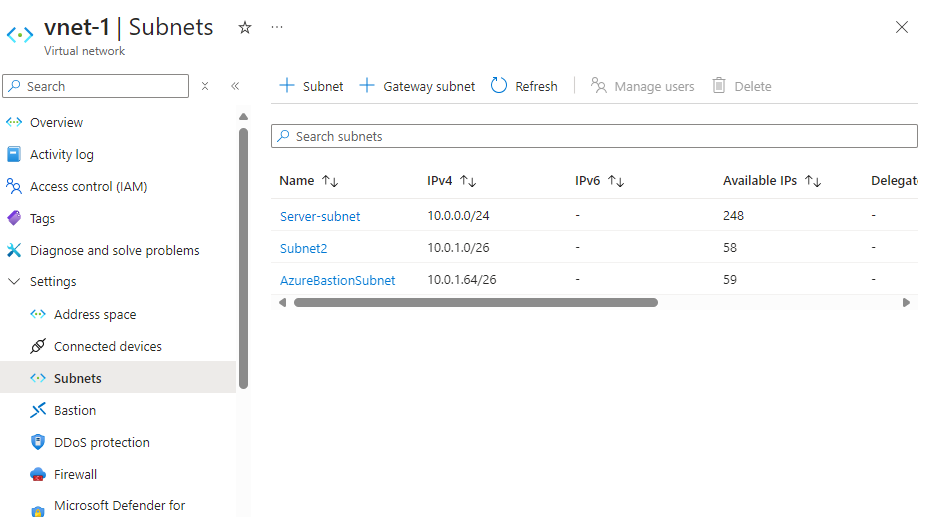
Bastion diagram-



**Monthly cost- 146.78 USD**

Deployment any working-

1. Deploy Bastion subnet



1. Deploy bastion

A white screen with text

Description automatically generated with medium confidence

Connect to vm using bastion.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Connect to vm in different subnet.

A screenshot of a computer

Description automatically generated

A black background with a black square

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated

A black screen with a black background

Description automatically generated

Sessions-

A close-up of a white background

Description automatically generated

Block other subnet vm connections.

Note- if we access servers on client environment by using bastion. This blocking traffic is totally optional. Because SNP user account has access to very limited servers. If we try to access other servers by using the same credentials login failed.

A screenshot of a computer

Description automatically generated

NSG applied on other subnets to archive same.

Subnet associated

A screenshot of a computer

Description automatically generated

Traffic block rule

A screenshot of a computer

Description automatically generated

Blocking traffic proof.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Vm in same subnet but not added in ASG

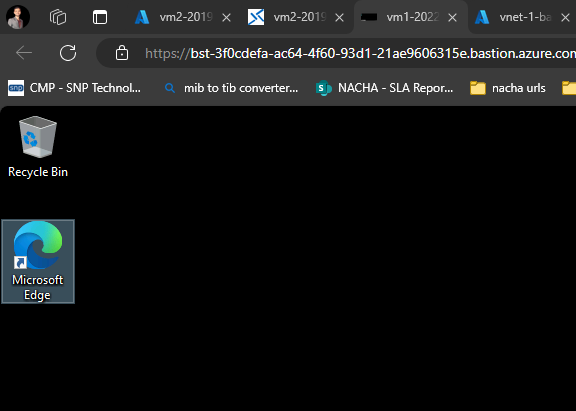
A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Servers in allowed subnet and added to ASG



A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Diagram-

A computer screen shot of a diagram

Description automatically generated

Have a separate RG for the new resource.

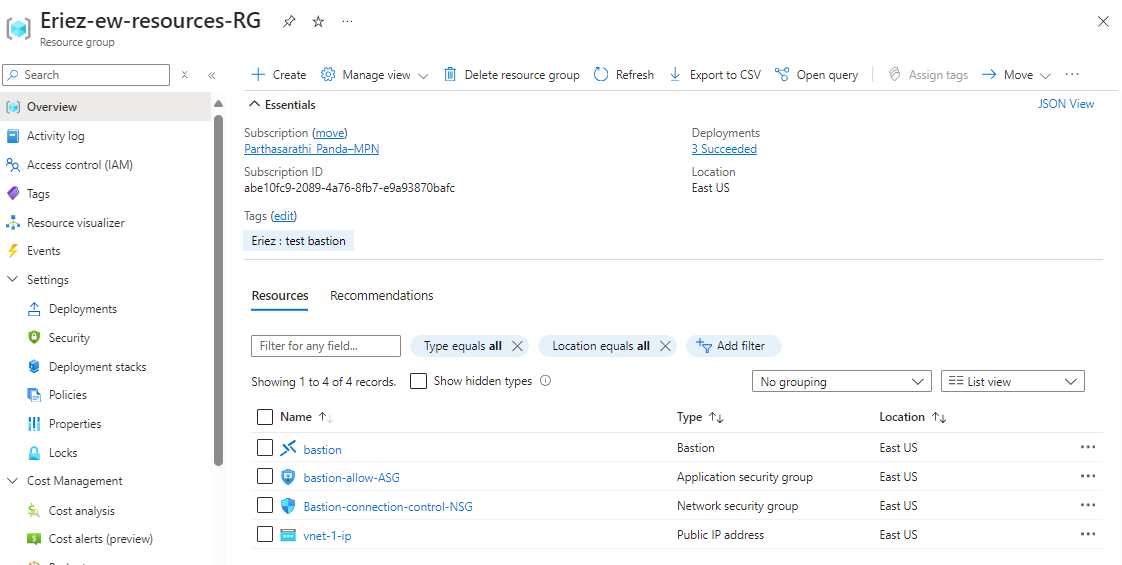
A screenshot of a computer

Description automatically generated

Create bastion for the targeted Vnet on new Subnet. (subnet will get create on the vnet RG)

Also create NSG ASG on new RG.

Those all does not even depend on VNET and Subnet.



A screenshot of a computer

Description automatically generated

Do required config for NSG and ASG

It works.

Note- make sure of other dependencies suh as if client is using any other jump server that must have allowed rule.

Best to go with don’t block all traffic block only rdp traffic on vnt. That will have less impact.

Block rule should have highest priority number hence lowest priority so other rules can easily override that.

Allow load balancer if have any dependency.

Ref image-

A screenshot of a computer

Description automatically generated

Mistake-

If you attach subnet to any of the NSG, previously attached NSG will be detached.

1 subnet can not be associated to 2 NSG.

Due to this the sub net was only attached to my configured NSG and got detached from actual one in which application, load balancer and different ports are enabled. So it’s impacted on application as well as on server RDP.

Hence, we need to assign NSG on those subnet which already don’t have and for rest which all have attache to any of the NSG need to made change on existing.

The diagram and the method I suggested previously can be best if subnet’s don’t have any assigned NSG. But in real time the subnet’s will have NSG for diff port it’s best to update there.

Mistake- don’t block vnet communication that will impact on AVD servers. Because AVD we connect 1 from another.

Block rdp from bastion and allow from bastion. So, only the bastion will take place default vnet communication will not impact.

Ref img-

