# Install on Azure without CMS

*For supported software information, click here.*

This article describes how to install, or instantiate, a Versa branch device on Microsoft Azure without creating a cloud management system (CMS) connector between Versa Director and the Versa Operating System TM (VOS TM) device. To perform this installation, you upload the VOS software image to the Azure portal, and then you create an Azure active directory application for the software.

Note that the procedure described in Install on Azure, in which you establish a CMS connector between Versa Director and the VOS device in Azure, is the preferred method to install Azure in a Versa branch. However, when you are not able to perform the regular installation, for example, if Versa Director is not connected to the internet, you can follow the installation procedures in this article.

To install a Versa branch device on Azure without creating a CMS connector, you do the following:

- Create a Versa image in Azure.
- Create a Versa VM.
- Add availability sets in Azure (optional).
- Peer Versa VNFs to an Azure virtual router BGP endpoint.
- Deploy dual Versa VNFs in Azure.

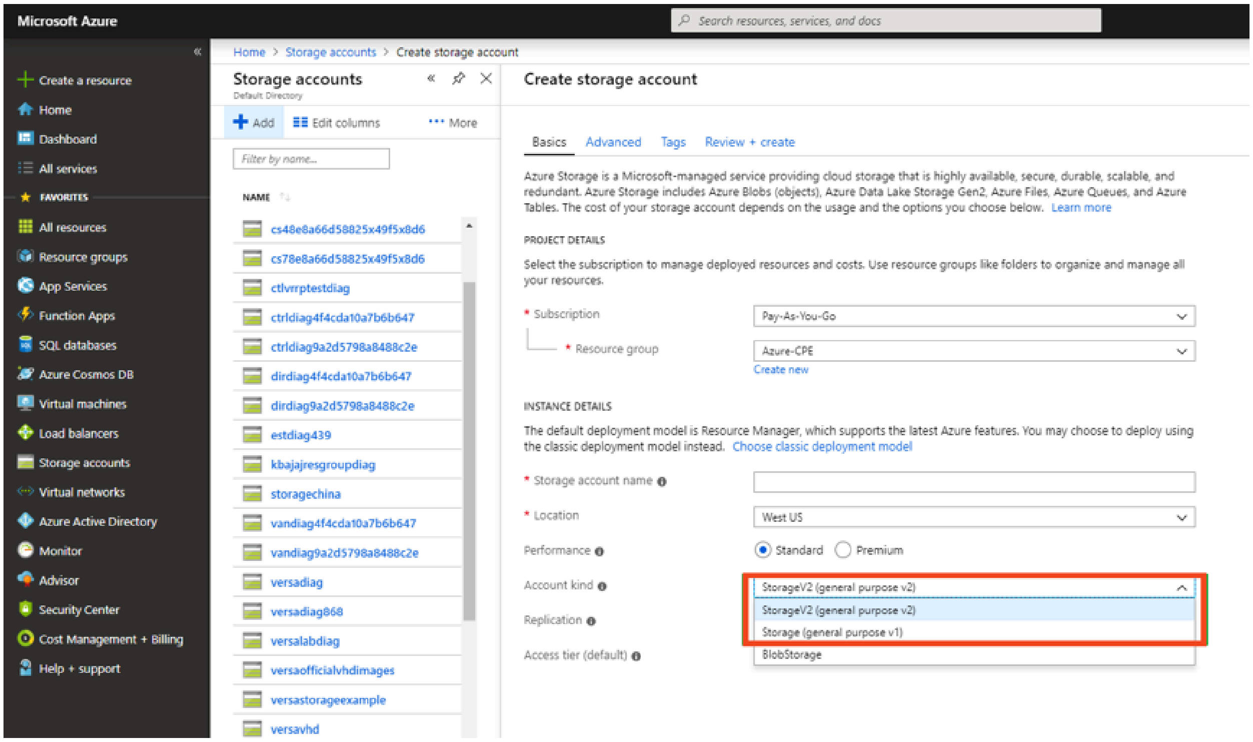
## Create a Versa Image in Azure

For VOS Releases 21.1.0 and earlier, you must manually create a VOS images in Azure. For VOS Releases 21.1.0 and later, the images are available in Microsoft Azure Marketplace, and you can skip this section.

Before you create a Versa image, create an Azure blog storage account and then request that Versa Networks Customer Support move the desired .vhd image (for example, 20.2.vhd for Release 20.2) to the blob account.

To create a blob storage account:

1. In Azure, navigate to Storage Accounts and click + Add. The Create storage account window displays.



Create storage account

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. Learn more

PROJECT DETAILS

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

* Subscription: Pay-As-You-Go

* Resource group: Azure-CPE

Create new

INSTANCE DETAILS

The default deployment model is Resource Manager, which supports the latest Azure features. You may choose to deploy using the classic deployment model instead. Choose classic deployment model

* Storage account name:

* Location: West US

Performance: ● Standard ○ Premium

Account kind: StorageV2 (general purpose v2)

StorageV2 (general purpose v2)
Storage (general purpose v1)
BlobStorage

Replication

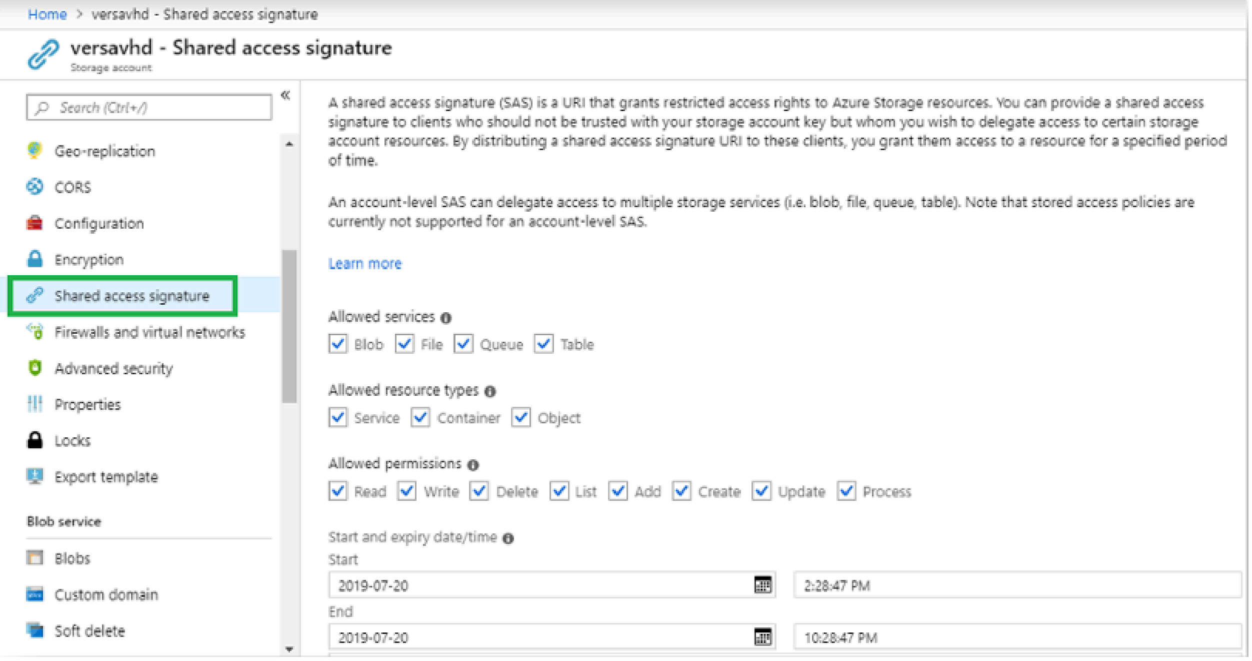
Access tier (default)

a. Select the Basics tab, and in the Account Kind field, select Storage v2.

b. In the Location field, ensure that you create the storage account in the region where you are deploying the Versa VNF.

c. Enter other required information.

2. Navigate to the storage account you created in Step 1 (here, versavhd), and in the left menu bar, select Shared Access Signature.



versavhd - Shared access signature

A shared access signature (SAS) is a URI that grants restricted access rights to Azure Storage resources. You can provide a shared access signature to clients who should not be trusted with your storage account key but whom you wish to delegate access to certain storage account resources. By distributing a shared access signature URI to these clients, you grant them access to a resource for a specified period of time.

An account-level SAS can delegate access to multiple storage services (i.e. blob, file, queue, table). Note that stored access policies are currently not supported for an account-level SAS.

Learn more

Allowed services

☑ Blob ☑ File ☑ Queue ☑ Table

Allowed resource types

☑ Service ☑ Container ☑ Object

Allowed permissions

☑ Read ☑ Write ☑ Delete ☑ List ☑ Add ☑ Create ☑ Update ☑ Process

Start and expiry date/time

Start: 2019-07-20 2:28:47 PM

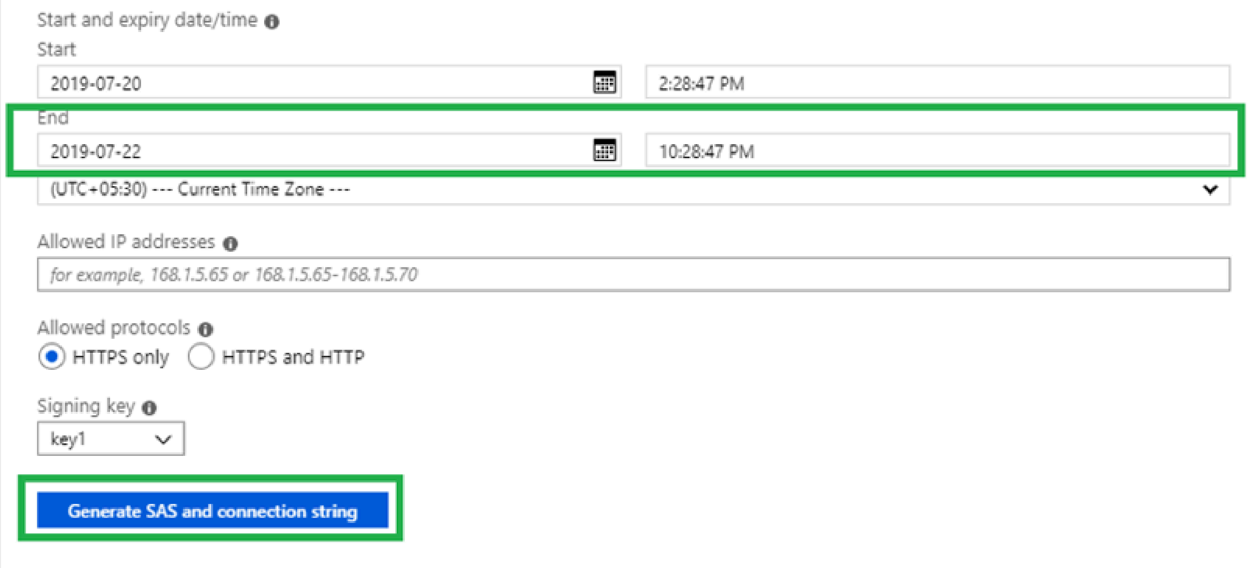
End: 2019-07-20 10:28:47 PM

a. In the Allow Services, Allowed Resource Types, and Allowed Permissions group of fields, click all the options.

b. In the Start field, select a date that is earlier than the current date and select a time that is at least 15 to 30 minutes before the current time, as recommended by Microsoft.

c. In the End field, select an end date that is a day or two after the current date.

d. Click Generate SAS and Connection String.



Start and expiry date/time

Start: 2019-07-20 2:28:47 PM

End: 2019-07-22 10:28:47 PM

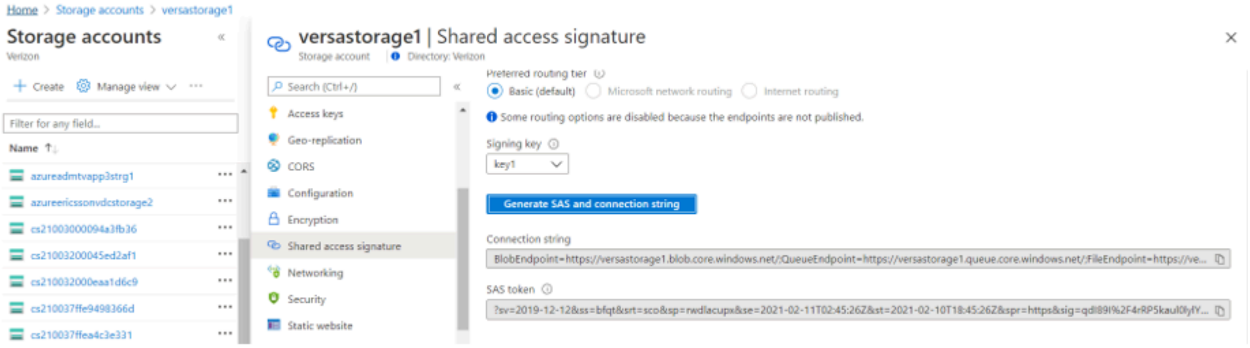
(UTC+05:30) --- Current Time Zone ---

Allowed IP addresses: *for example, 168.1.5.65 or 168.1.5.65-168.1.5.70*

Allowed protocols: ● HTTPS only ○ HTTPS and HTTP

Signing key: key1

e. Save the generated SAS token to a notepad.



Home > Storage accounts > versastorage1

Preferred routing tier: ● Basic (default) ○ Microsoft network routing ○ Internet routing

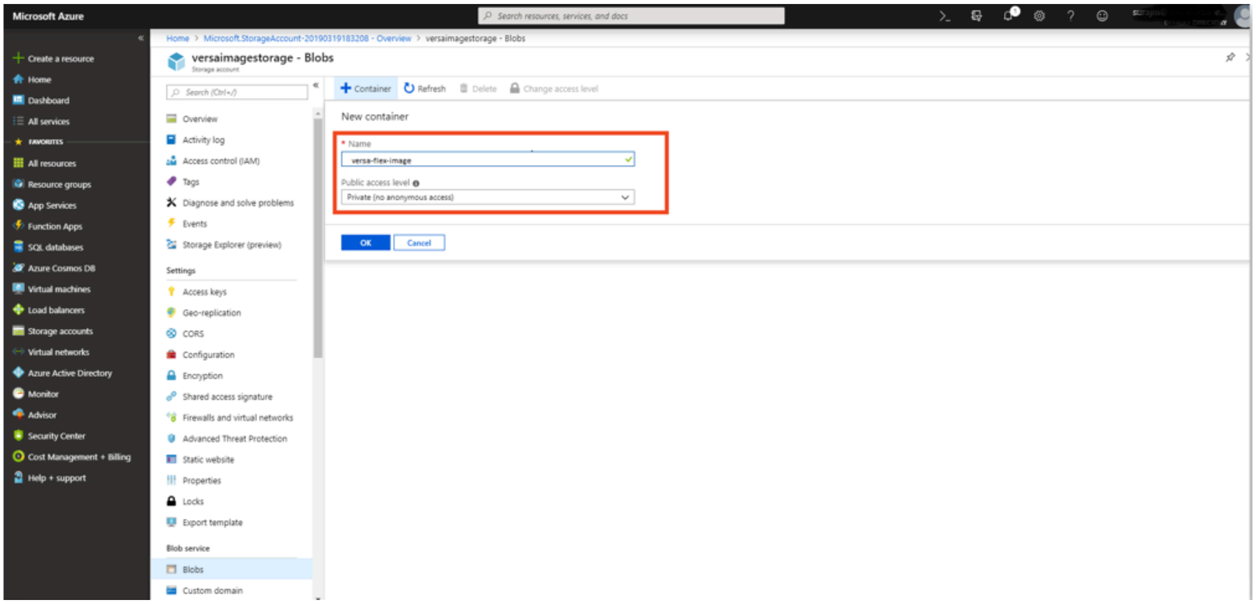
Some routing options are disabled because the endpoints are not published.

Signing key: key1

Connection string: BlobEndpoint=https://versastorage1.blob.core.windows.net/;QueueEndpoint=https://versastorage1.queue.core.windows.net/;FileEndpoint=https://ve...

SAS token: ?sv=2019-12-12&ss=bfqt&srt=sco&sp=rwdlacupx&se=2021-02-11T02:45:26Z&st=2021-02-10T18:45:26Z&spr=https&sig=qdl89I%2F4rRP5kaul0lylY...

3. In your storage account, navigate to Blobs, and then click + Container to create a blobs container. The New container window displays.

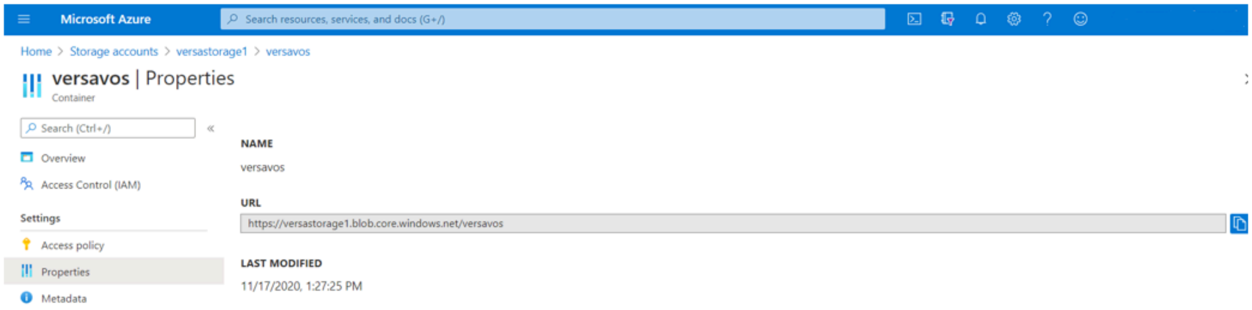


New container

* Name: versa-flex-image

Public access level: Private (no anonymous access)

4. In the Name field, enter a name for the container to use as reference for the image.
5. Configure the appropriate access level rights as shown in the following image, and then click OK.
6. Share the blob URL (displayed in the Properties section of the blob account) and the SAS token for the storage account (displayed in the shared access signature section) with Versa Networks Customer Support so that they can copy the .vhd image to the storage blob account.

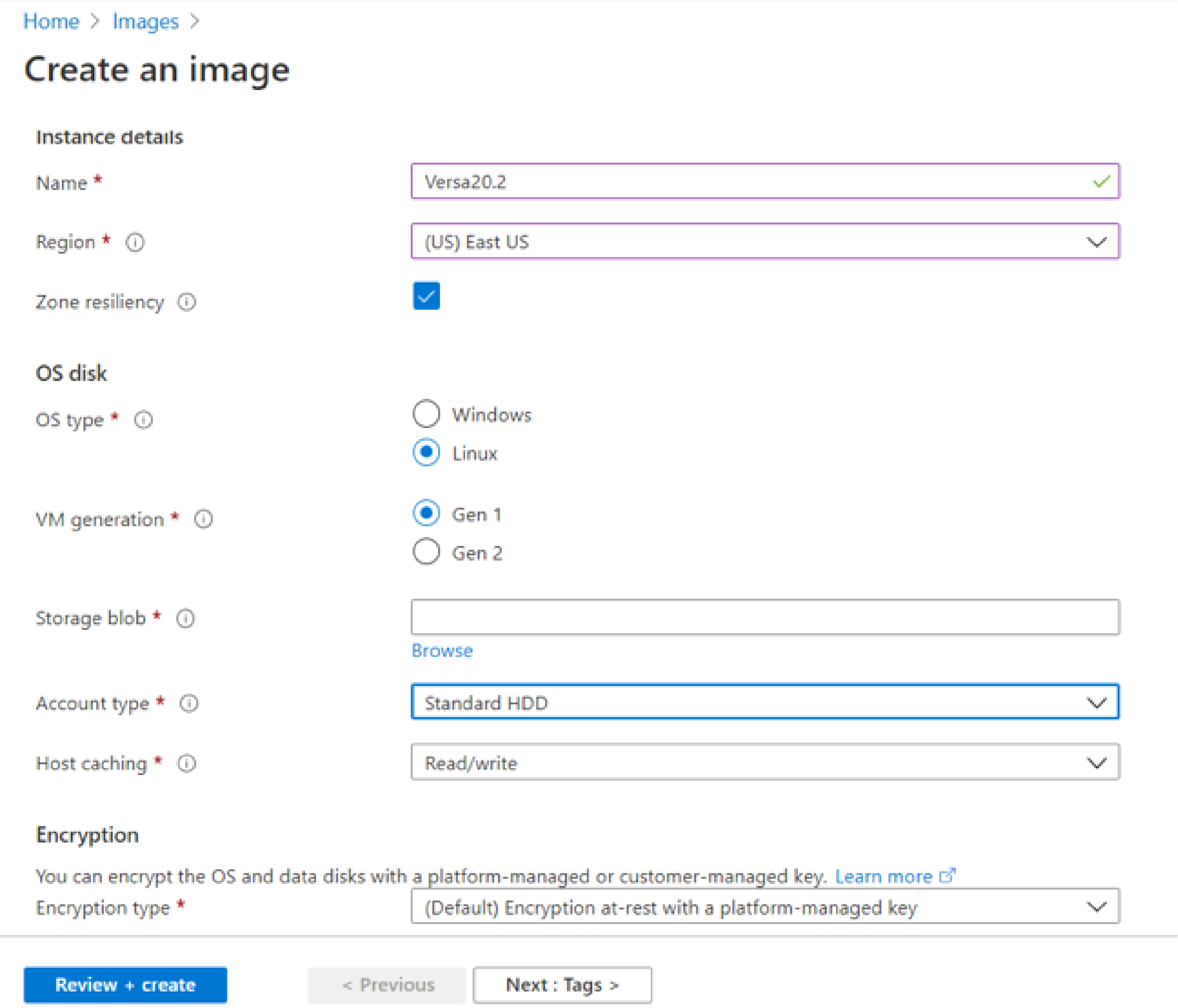


NAME
versavos

URL
https://versastorage1.blob.core.windows.net/versavos

LAST MODIFIED
11/17/2020, 1:27:25 PM

7. After Versa Networks Customer Support has transfered the .vhd file, create an image in Azure Avere for the .vhd file. To do this, in Azure, navigate to Images and then click +Create. The Create an Image screen displays.



Home > Images >

Create an image

Instance details

Name * Versa20.2

Region * (US) East US

Zone resiliency ☑

OS disk

OS type * ○ Windows ● Linux

VM generation * ● Gen 1 ○ Gen 2

Storage blob *

Browse

Account type * Standard HDD

Host caching * Read/write

Encryption

You can encrypt the OS and data disks with a platform-managed or customer-managed key. Learn more

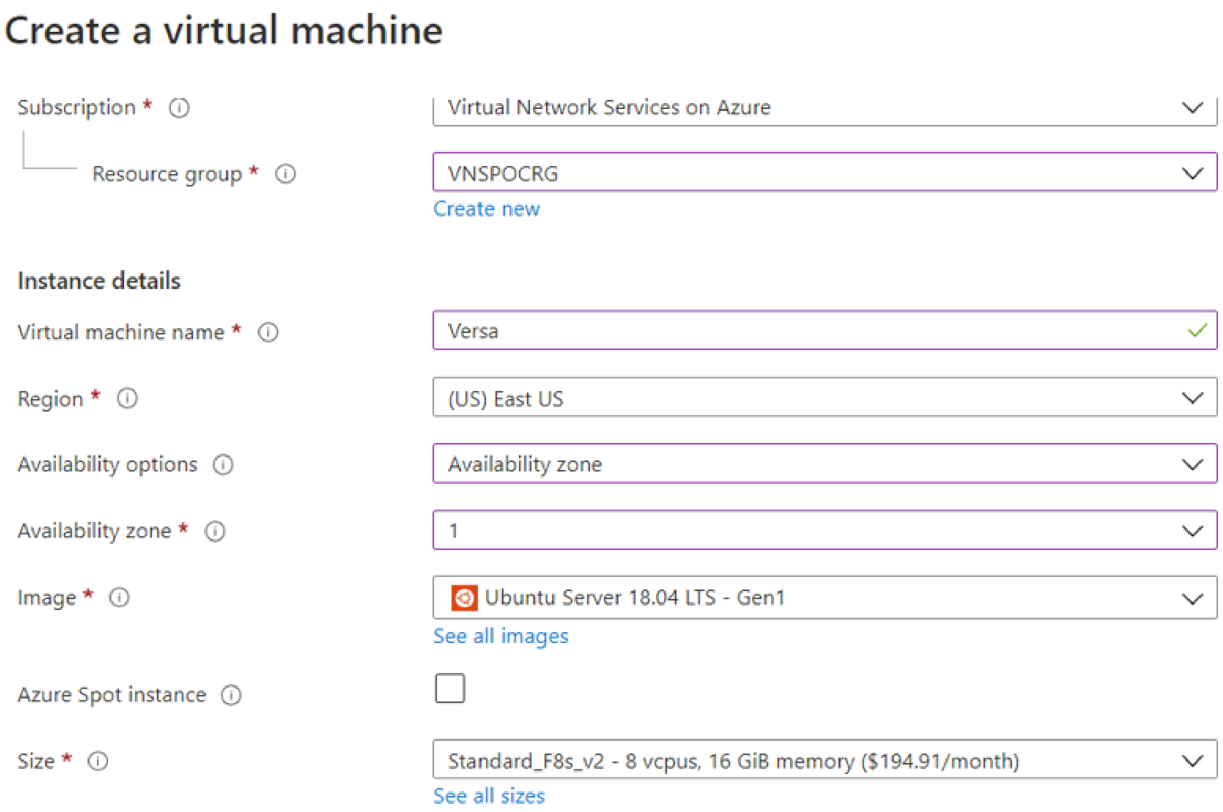
Encryption type * (Default) Encryption at-rest with a platform-managed key

8. In the Storage Blob field, click Browse and select the .vhd file transferred by Versa Networks Customer Support.
9. Enter any other required information.
10. Click Review + Create to create the Versa image.

## Create a Versa VM

Next, create a virtual machine (VM) for the Versa VNF:

1. In Azure, navigate to Virtual Machines, and then click + Add. The Create a Virtual Machine screen displays. Enter information for the following fields.



Create a virtual machine

Subscription * ⓘ Virtual Network Services on Azure

Resource group * ⓘ VNSPOCRG

Create new

Instance details

Virtual machine name * ⓘ Versa ✓

Region * ⓘ (US) East US

Availability options ⓘ Availability zone

Availability zone * ⓘ 1

Image * ⓘ Ubuntu Server 18.04 LTS - Gen1

See all images

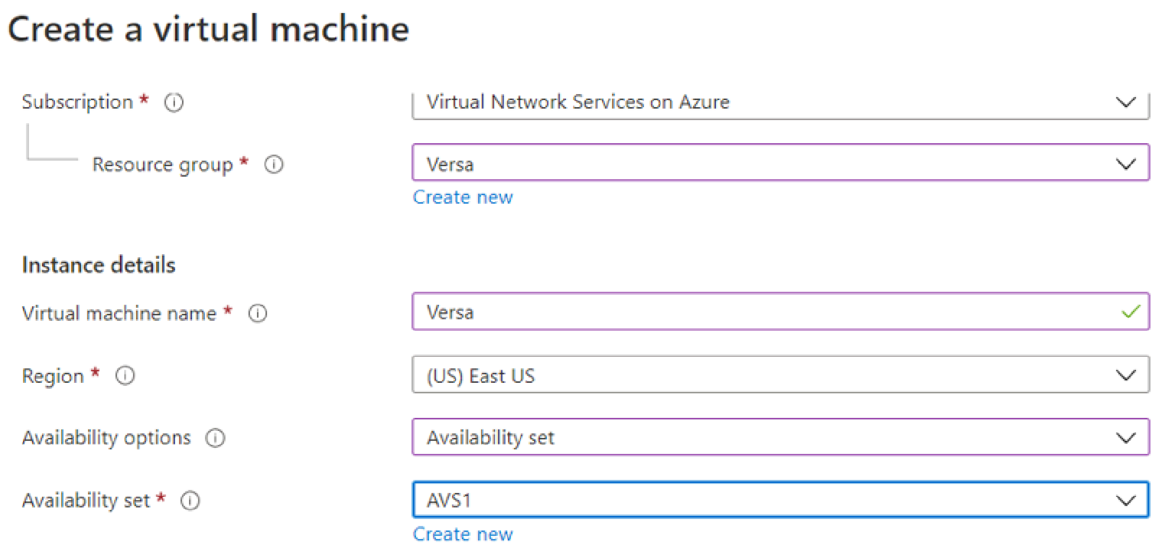
Azure Spot instance ⓘ □

Size * ⓘ Standard_F8s_v2 - 8 vcpus, 16 GiB memory ($194.91/month)

See all sizes

| Field | Description |
|---|---|
| Resource Group | Select the resource group. |
| Virtual Machine Name | Select a name for the Versa VNF. |
| Region | Select the region in which to deploy the Versa VNF. |
| Availability Options | To deploy the Versa VNF in a specific Availably Zone within a region, select Availability Zone. |
| Availability Zone | Select the zone, as shown in the screenshot in Step 1. |

2. For high availability (HA), you can deploy a second Versa VNF in a different zone for geodiversity. If geodiversity HA is not required for a dual Versa VNF deployment, you can deploy multiple Versa VNFs in the same Availability Set, as shown in the following screenshot. For more information, see Add Availability Sets in Azure, below.



Create a virtual machine

Subscription * : Virtual Network Services on Azure

Resource group * : Versa

Create new

Instance details

Virtual machine name * : Versa

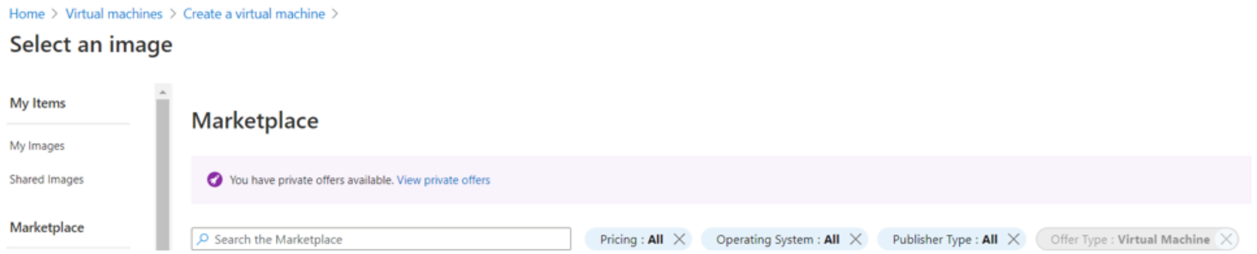
Region * : (US) East US

Availability options : Availability set

Availability set * : AVS1

Create new

3. In the Image field, click See All Images. Then, select My Images and select the image you created in [Create a Versa Image in Azure](), above.



Home > Virtual machines > Create a virtual machine >

Select an image

My Items

My Images

Shared Images

Marketplace

Marketplace

You have private offers available. View private offers

Search the Marketplace

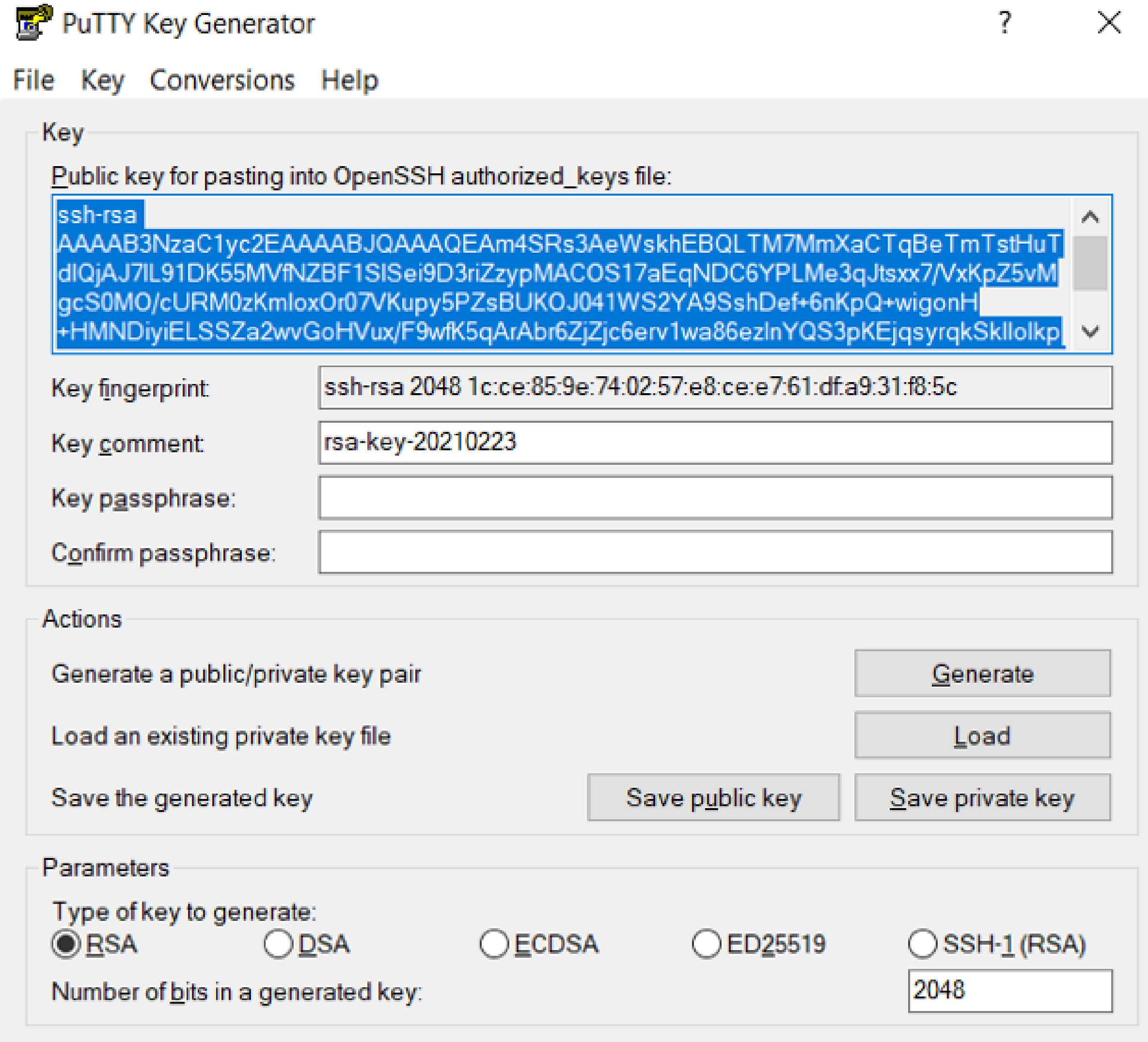
Pricing : All

Operating System : All

Publisher Type : All

Offer Type : Virtual Machine

4. In the Size field, select the appropriate size for the Versa VNF (here, Standard F8s_v2). To view all available sizes, click See All Sizes.
5. Create an SSH key pair to allow SSH connections to the management port. There are multiple options for creating an SSH key pair. The following example shows using PuTTYgen in Windows OS. Select RSA 2048, and then generate the private key.



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEAm4SRs3AeWskhEBQLTM7MmXaCTqBeTmTstHuT
dlQjAJ7IL91DK55MVfNZBF1SISei9D3riZzypMACOS17aEqNDC6YPLMe3qJtsxx7/VxKpZ5vM
gcS0MO/cURM0zKmloxOr07VKupy5PZsBUKOJ041WS2YA9SshDef+6nKpQ+wigonH
+HMNDiyiELSSZa2wvGoHVux/F9wfK5qArAbr6ZjZjc6erv1wa86ezlnYQS3pKEjqsyrqkSkllolkp
```

Key fingerprint: ssh-rsa 2048 1c:ce:85:9e:74:02:57:e8:ce:e7:61:df:a9:31:f8:5c

Key comment: rsa-key-20210223

Key passphrase:

Confirm passphrase:

Generate a public/private key pair

Load an existing private key file

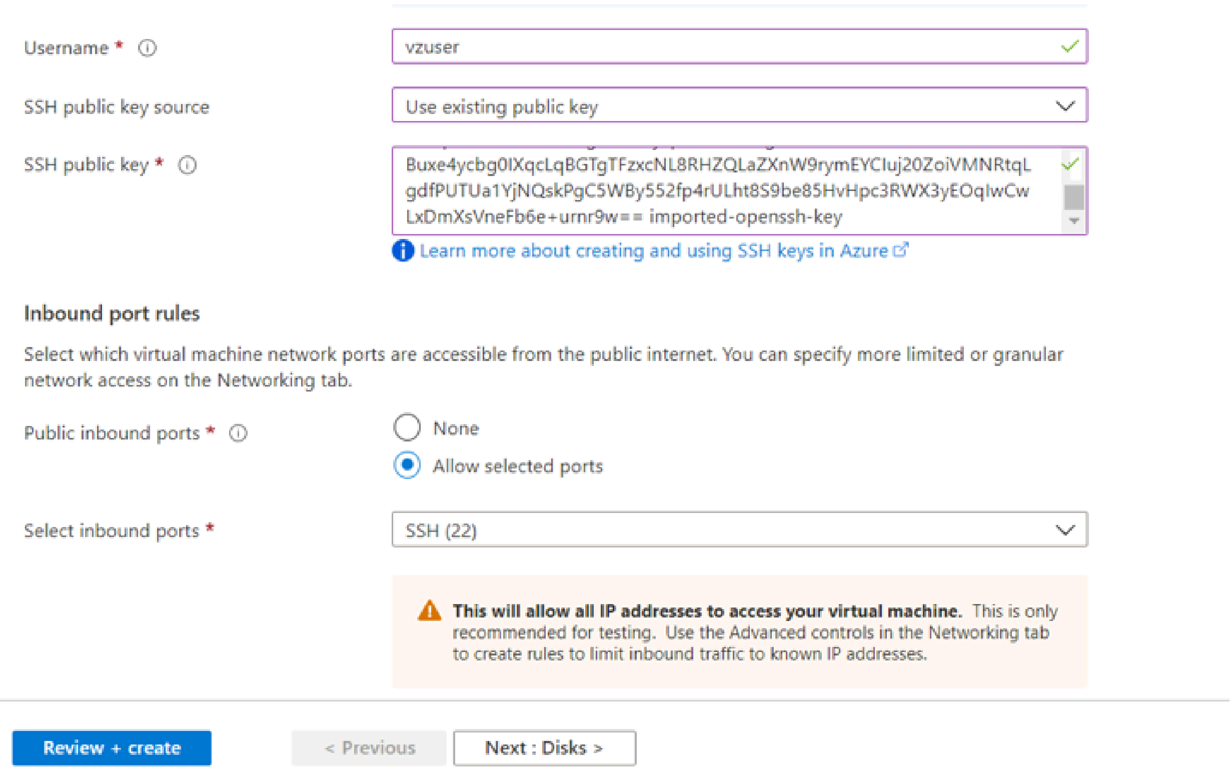
Save the generated key

Type of key to generate:

● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

6. Save the private key to your desktop, and save the public key to a notepad.
7. To enter the public key in the Azure VM, select Use Existing Public Key in the SSH Public Key Source field.
8. In the SSH Public Key field, enter the public key you saved in Step 6. The inbound port rules allow only SSH, as shown in the following screenshot.



Username * ⓘ vzuser ✓

SSH public key source: Use existing public key

SSH public key * ⓘ

```
Buxe4ycbg0IXqcLqBGTgTFzxcNL8RHZQLaZXnW9rymEYCIuj20ZoiVMNRtqL
gdfPUTUa1YjNQskPgC5WBy552fp4rULht8S9be85HvHpc3RWX3yEOqIwCw
LxDmXsVneFb6e+urnr9w== imported-openssh-key
```

Learn more about creating and using SSH keys in Azure

**Inbound port rules**

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ

○ None

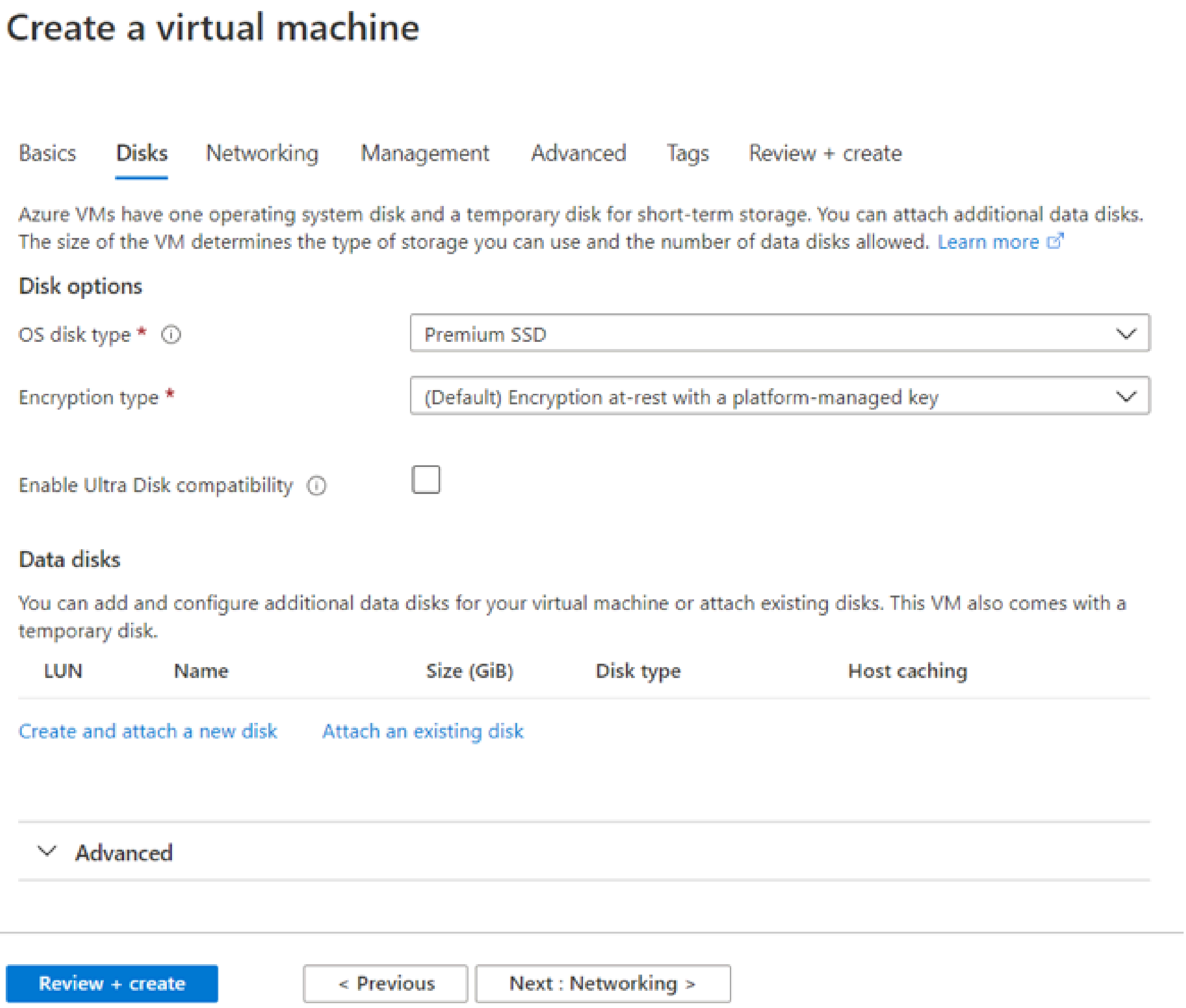
● Allow selected ports

Select inbound ports * SSH (22)

**This will allow all IP addresses to access your virtual machine.** This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Note that if you ssh to the VM from a Linux machine instead of selecting Use Existing Public Key and generating a key pair on your own, you can select Generate New Key Pair. Doing this automatically places the public key in the VM, and you can download the .pem file after you create the VM. You can then use the .pem file from a Linux machine to ssh to the VM.

9. Click Next: Disks >. The Disks tab displays. On this tab, use the default values.



Create a virtual machine

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. Learn more

Disk options

OS disk type * : Premium SSD

Encryption type * : (Default) Encryption at-rest with a platform-managed key

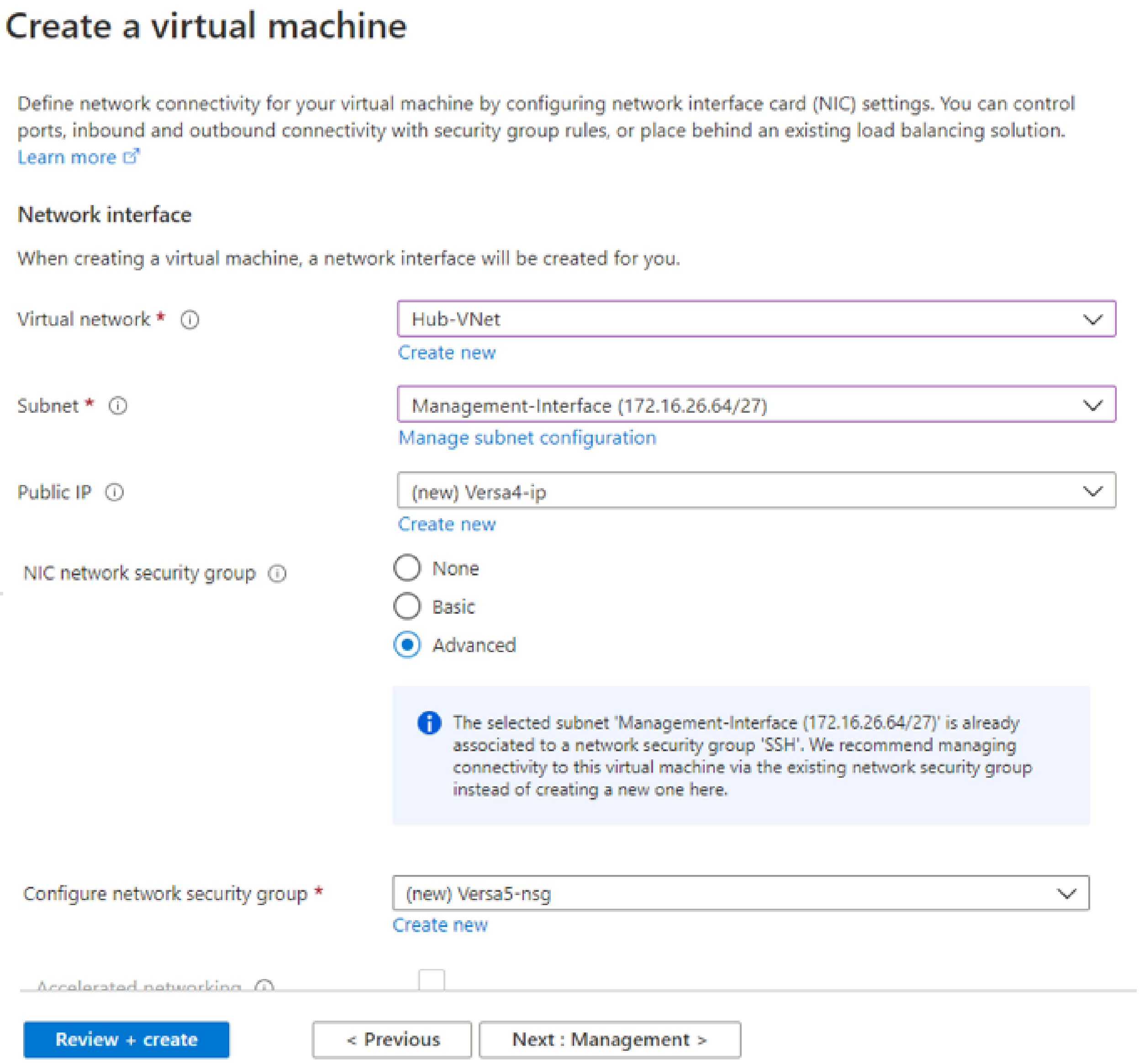
Enable Ultra Disk compatibility ☐

Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

| LUN | Name | Size (GiB) | Disk type | Host caching |
|---|---|---|---|---|

10. Click Next Networking >. The Networking tab displays. Enter information for the following fields.



Create a virtual machine

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. Learn more

Network interface

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

Virtual network * : Hub-VNet

Create new

Subnet * : Management-Interface (172.16.26.64/27)

Manage subnet configuration

Public IP : (new) Versa4-ip

Create new

NIC network security group:

○ None

○ Basic

● Advanced

The selected subnet 'Management-Interface (172.16.26.64/27)' is already associated to a network security group 'SSH'. We recommend managing connectivity to this virtual machine via the existing network security group instead of creating a new one here.

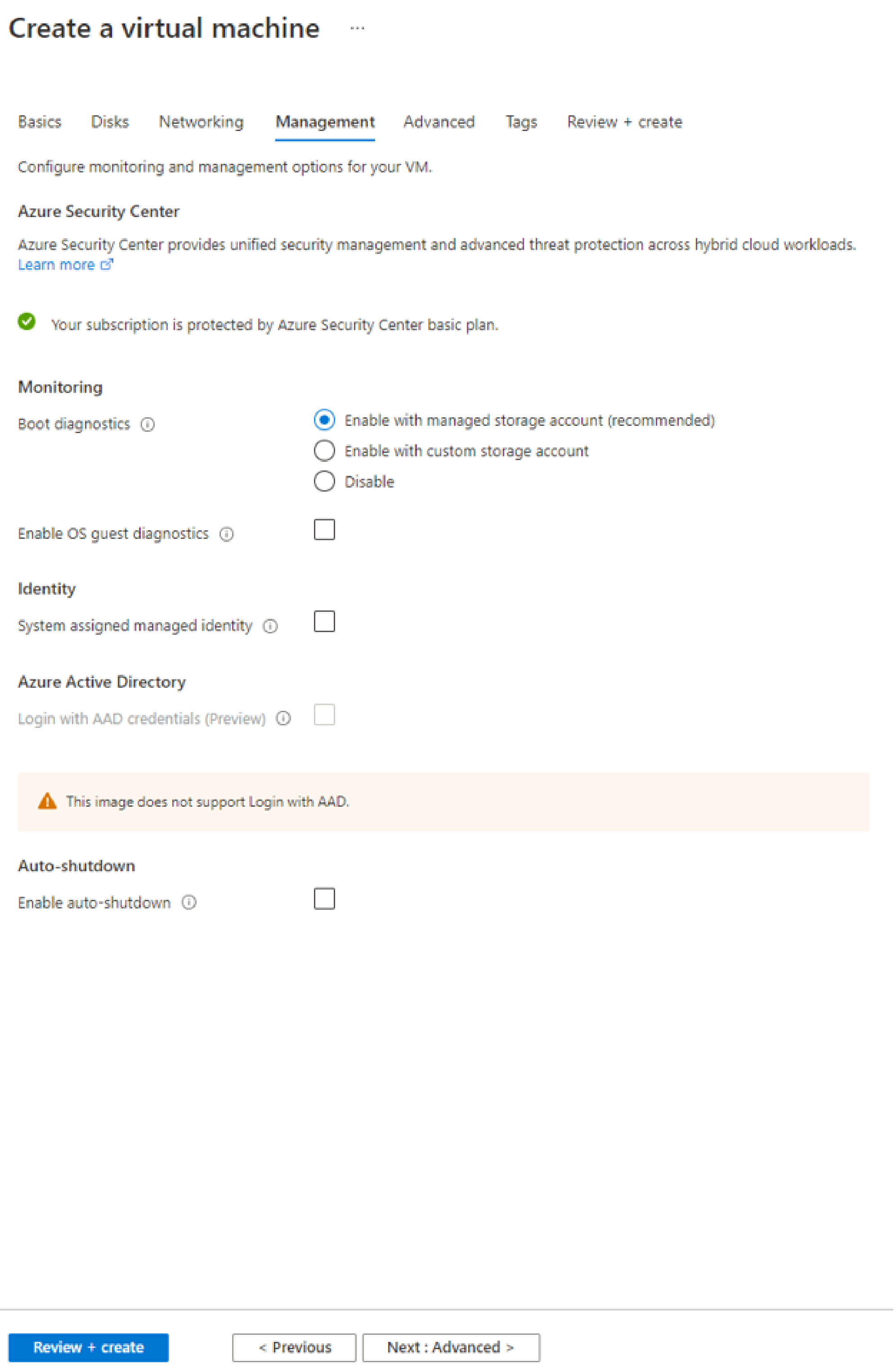
Configure network security group * : (new) Versa5-nsg

Create new

Accelerated networking □

| Field | Description |
|---|---|
| Virtual Network | Select Hub-VNet. |
| Subnet | Select the management subnet that you created in the Hub-VNet. Ensure that a new public IP address is assigned. |
| NIC Network Security Group | Select Advanced. |
| Configure Network Security Group | Create a new network security group (NSG). |

11. Click Next: Management >. The Management tab displays.



Create a virtual machine ...

Configure monitoring and management options for your VM.

Azure Security Center

Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads.
Learn more

✓ Your subscription is protected by Azure Security Center basic plan.

Monitoring

Boot diagnostics ⓘ
- ● Enable with managed storage account (recommended)
- ○ Enable with custom storage account
- ○ Disable

Enable OS guest diagnostics ⓘ □

Identity

System assigned managed identity ⓘ □

Azure Active Directory

Login with AAD credentials (Preview) ⓘ □

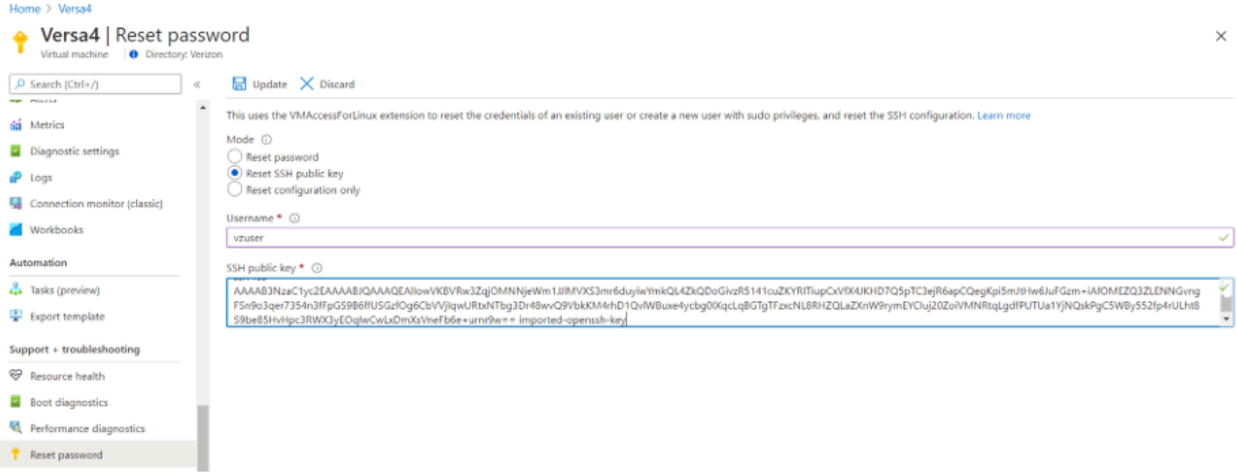
⚠ This image does not support Login with AAD.

Auto-shutdown

Enable auto-shutdown ⓘ □

12. In the Monitoring group of fields, in the Boot Diagnostics field, select Enable with Managed Storage Account.
13. Click Review + Create to create the VM.

14. If you generated the SSH key pair on your own, after the VM is created, select Reset Password in the left menu bar.



This uses the VMAccessForLinux extension to reset the credentials of an existing user or create a new user with sudo privileges, and reset the SSH configuration. Learn more

Mode

○ Reset password
● Reset SSH public key
○ Reset configuration only

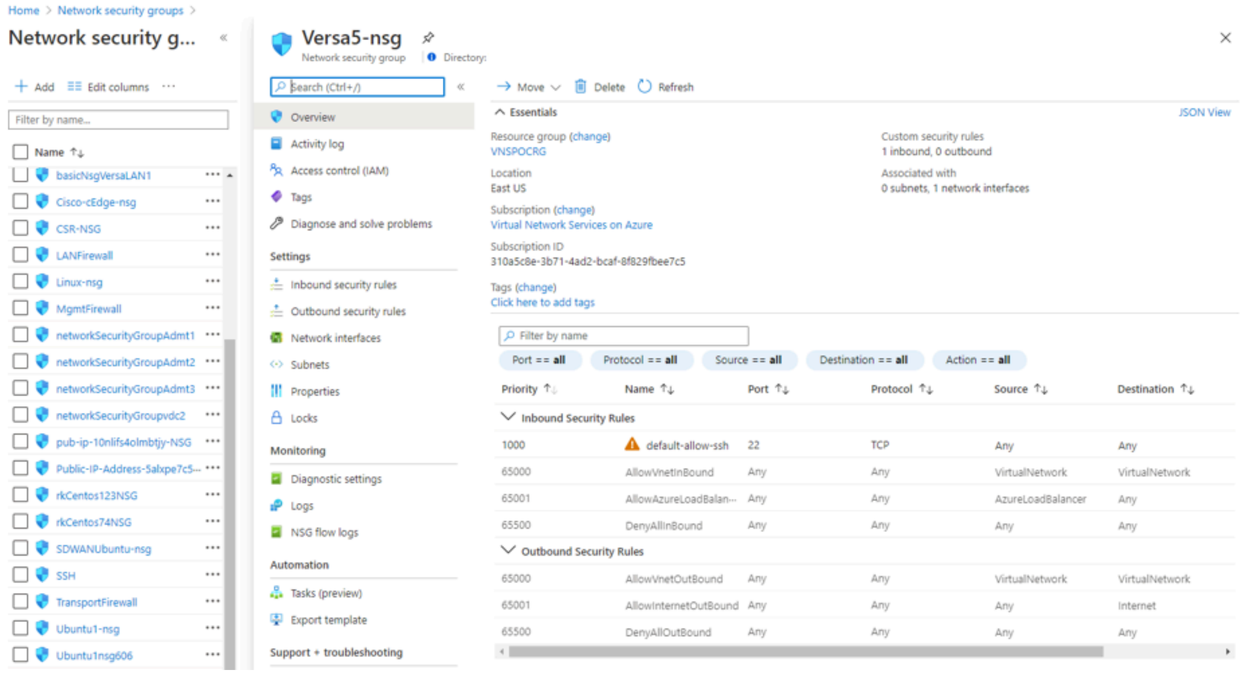
Username * vzuser

SSH public key *

```
AAAAB3NzaC1yc2EAAAABJQAAAQEAllowVKBVRw3ZqjOMNNjeWm1JJlMVXS3mr6duyiwYmkQL4ZkQDoGivzR5141cuZKYRITiupCxVfX4JKHD7Q5pTC3ejR6apCQegKpi5mJtHw6JuFGzm+iAfOMEZQ3ZLENNGvng
FSn9o3qer7354n3fFpGS9B6ffUSGzfOg6CbVVjlqwURtxNTbg3Dr48wvQ9VbkKM4rhD1QvlWBuxe4ycbg0lXqcLqBGTgTFzxcNL8RHZQLaZXnW9rymEYCluj20ZoiVMNRtqLgdfPUTUa1YjNQskPgC5WBy552fp4rULht8
S9be85HvHpc3RWX3yEOqlwCwLxDmXsVneFb6e+urnr9w== imported-openssh-key
```

15. Enter the username and public key again, and then click Update.

16. Navigate to the NSG that was created for the management interface (here, Versa5-nsg).



Resource group (change)
VNSPOCRG

Location
East US

Subscription (change)
Virtual Network Services on Azure

Subscription ID
310a5c8e-3b71-4ad2-bcaf-8f829fbee7c5

Tags (change)
Click here to add tags

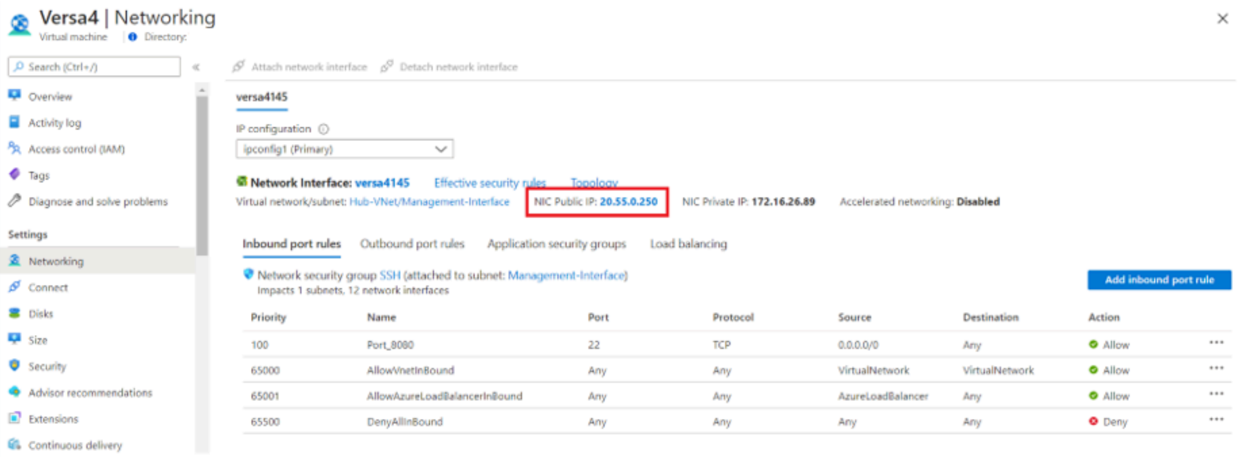
Custom security rules
1 inbound, 0 outbound

Associated with
0 subnets, 1 network interfaces

| Priority | Name | Port | Protocol | Source | Destination |
|---|---|---|---|---|---|
| Inbound Security Rules | | | | | |
| 1000 | ⚠ default-allow-ssh | 22 | TCP | Any | Any |
| 65000 | AllowVnetInBound | Any | Any | VirtualNetwork | VirtualNetwork |
| 65001 | AllowAzureLoadBalan... | Any | Any | AzureLoadBalancer | Any |
| 65500 | DenyAllInBound | Any | Any | Any | Any |
| Outbound Security Rules | | | | | |
| 65000 | AllowVnetOutBound | Any | Any | VirtualNetwork | VirtualNetwork |
| 65001 | AllowInternetOutBound | Any | Any | Any | Internet |
| 65500 | DenyAllOutBound | Any | Any | Any | Any |

17. Ensure that the source IP address range for the SSH rule allows only permitted (customer) management IP addresses.

18. Under Settings, select the Networking tab and locate the public IP address assigned to the management interface.



Versa4 | Networking

Virtual machine | Directory:

versa4145

IP configuration: ipconfig1 (Primary)

Network Interface: versa4145

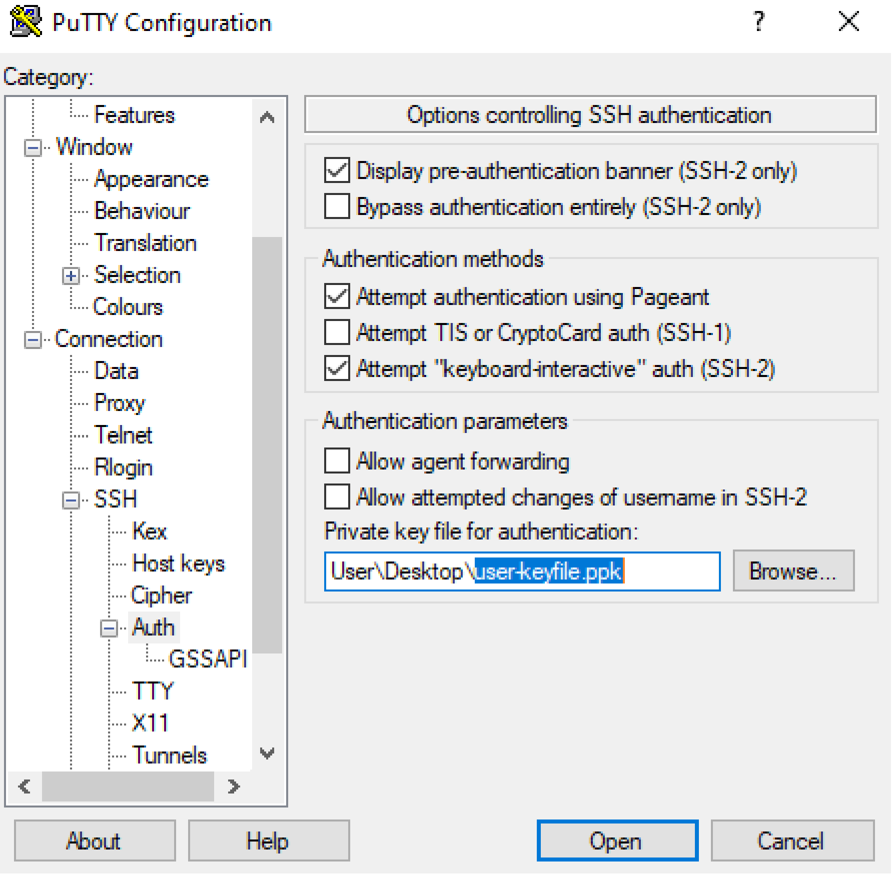
Virtual network/subnet: Hub-VNet/Management-Interface    NIC Public IP: 20.55.0.250    NIC Private IP: 172.16.26.89    Accelerated networking: Disabled

Network security group SSH (attached to subnet: Management-Interface)
Impacts 1 subnets, 12 network interfaces

| Priority | Name | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|---|
| 100 | Port_8080 | 22 | TCP | 0.0.0.0/0 | Any | Allow |
| 65000 | AllowVnetInBound | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | AllowAzureLoadBalancerInBound | Any | Any | AzureLoadBalancer | Any | Allow |
| 65500 | DenyAllInBound | Any | Any | Any | Any | Deny |

You can now ssh to the VM using the public IP address of the management interface. If you are using PuTTY from a Windows machine, you must use the SSH PPK file generated earlier for the first login. Then, you can enable password authentication in the VM's SSH file, which allows you to log in to the VM using the default username and password thereafter.

19. Log in to the VM using the PPK file username and passphrase. If you used Azure to generate the new key pair, transfer the .pem file to a Linux machine and ssh from the Linux machine instead of using PuTTY, as shown in the following sample screenshots.



Options controlling SSH authentication

☑ Display pre-authentication banner (SSH-2 only)
□ Bypass authentication entirely (SSH-2 only)

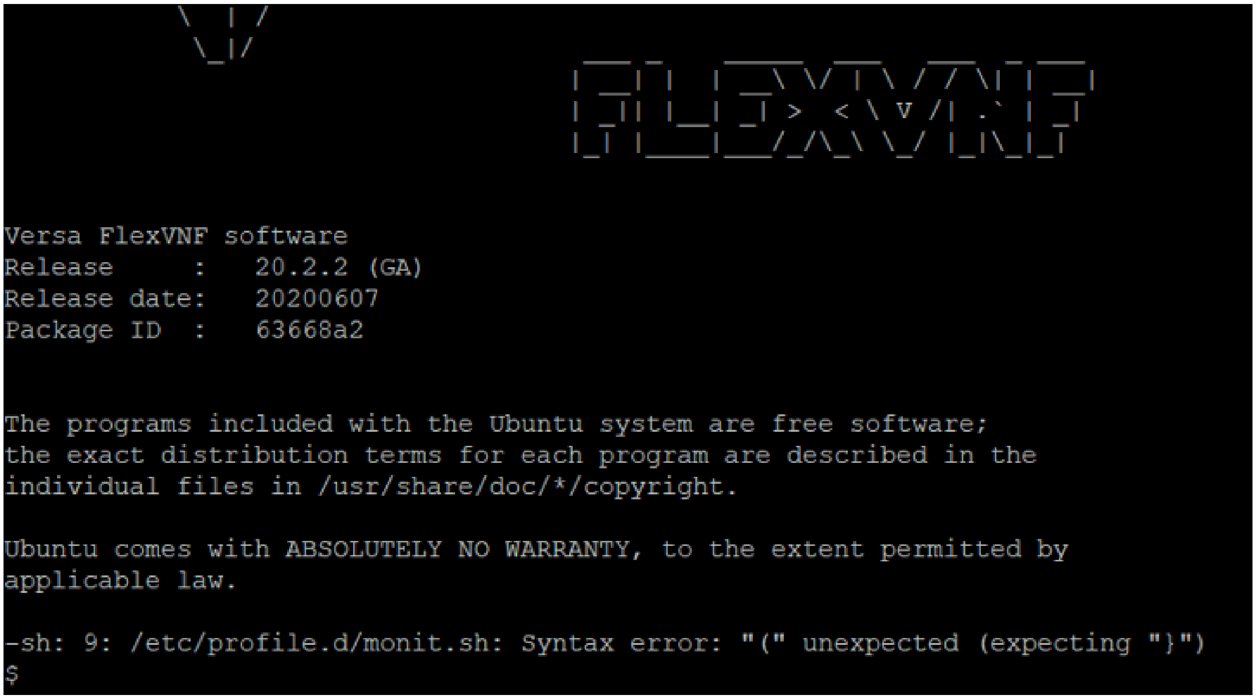
Authentication methods

☑ Attempt authentication using Pageant
□ Attempt TIS or CryptoCard auth (SSH-1)
☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

□ Allow agent forwarding
□ Allow attempted changes of username in SSH-2

Private key file for authentication: User\Desktop\user-keyfile.ppk



```
           \ | /
            \_|/
                                     _____ _     _______  ____     ___   _ _____
                                    |  ___| |   | ____\ \/ /\ \   / / \ | |  ___|
                                    | |_  | |   |  _|  \  /  \ \ / /|  \| | |_
                                    |  _| | |___| |___ /  \   \ V / | |\  |  _|
                                    |_|   |_____|_____/_/\_\   \_/  |_| \_|_|


Versa FlexVNF software
Release     :   20.2.2 (GA)
Release date:   20200607
Package ID  :   63668a2


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

-sh: 9: /etc/profile.d/monit.sh: Syntax error: "(" unexpected (expecting "}")
$
```

20. After you log in to the VM, become the administrator:

    > $ **sudo su admin**

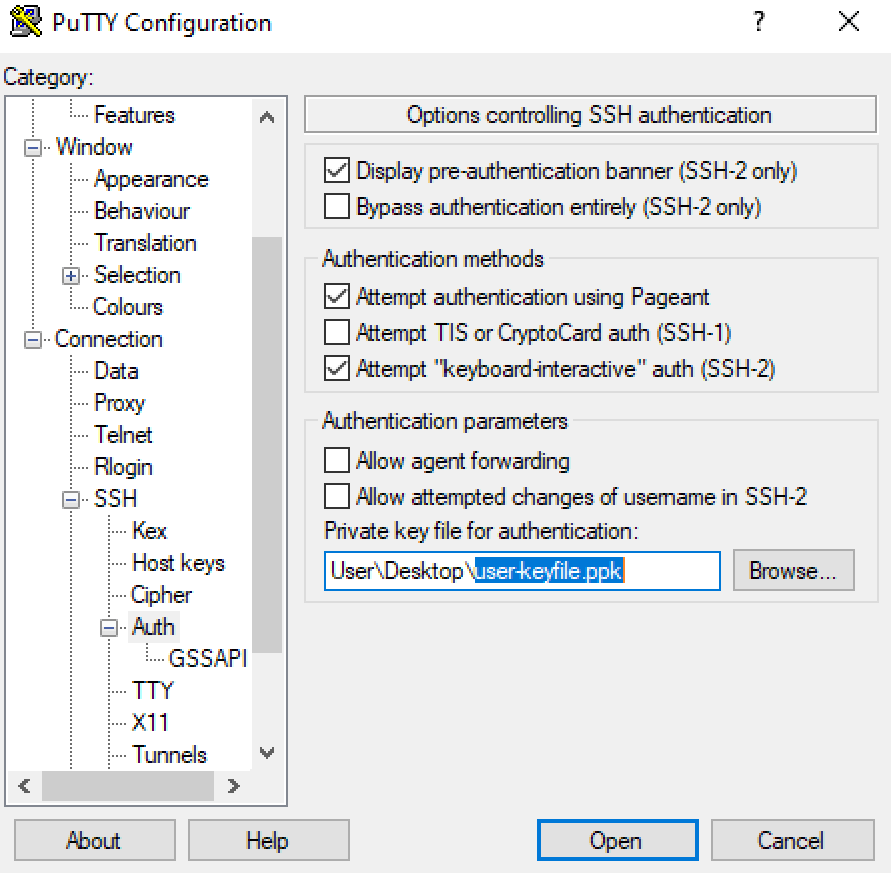
21. Edit the SSH configuration:

    > $ **sudo vi /etc/ssh/sshd_config**

22. Change password authentication from no to yes.
23. Type **quit** to exit.
24. Restart the SSH service:

    > $ **sudo service ssh restart**

25. Log out of the VM and then log back in using the traditional login username and password (admin/versa123) without using the SSH key pair.
26. Shut down the VM within Azure by clicking Overview in the left menu bar, and then clicking Stop.



☑ Display pre-authentication banner (SSH-2 only)
☐ Bypass authentication entirely (SSH-2 only)

Authentication methods

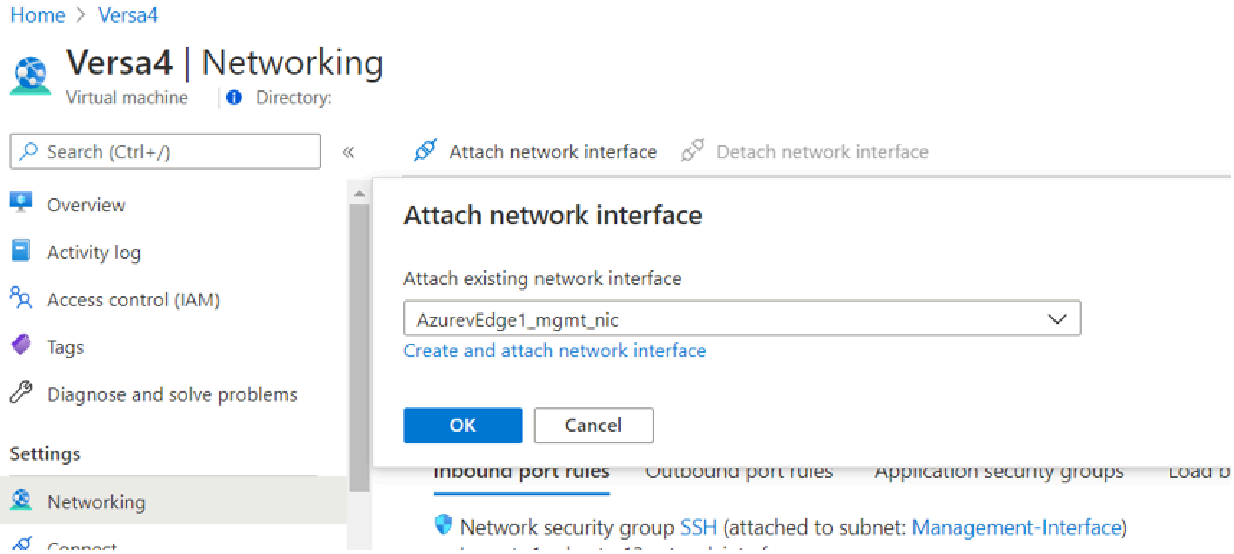
☑ Attempt authentication using Pageant
☐ Attempt TIS or CryptoCard auth (SSH-1)
☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

☐ Allow agent forwarding
☐ Allow attempted changes of username in SSH-2

Private key file for authentication: User\Desktop\user-keyfile.ppk

27. After you shut down the VM, add the remaining interfaces (WAN transport and LAN) to the Versa VNF. Note that the order to add the interfaces is important. For example, if you want internet, MPLS, and LAN, to be on VNI-0/0, 0/1, and 0/2, respectively, you must add the interfaces in the same order: internet subnet, MPLS subnet, and LAN subnet.
To attach an interface, select Networking under Settings in Azure and click Attach network interface. The Attach network interface window displays.

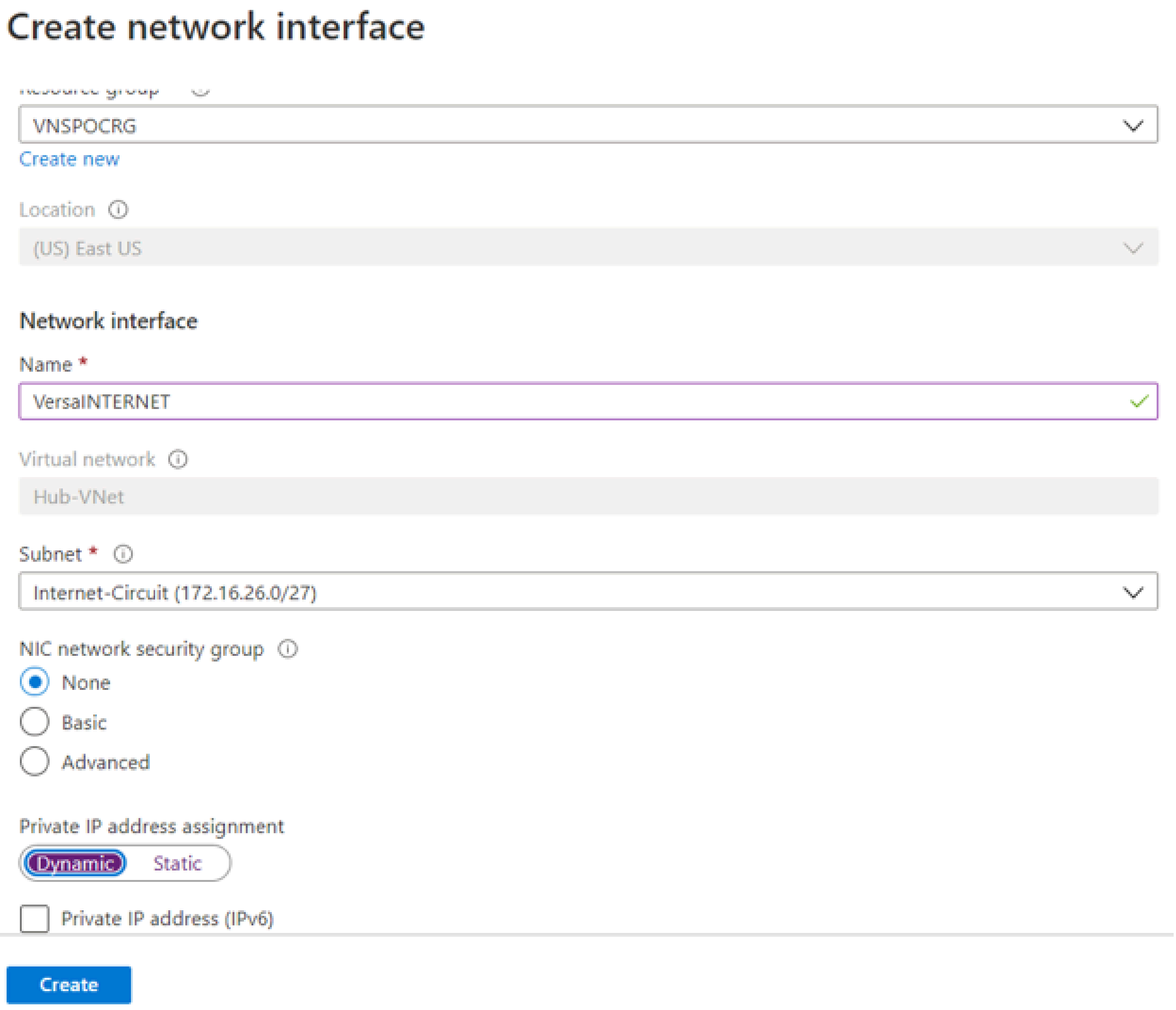


Attach network interface

Attach existing network interface: AzurevEdge1_mgmt_nic

Network security group SSH (attached to subnet: Management-Interface)

28. Click Create and attach network interface. In the Create Network Interface screen, enter information for the following fields.



Create network interface

Resource group ⓘ

VNSPOCRG

Create new

Location ⓘ

(US) East US

Network interface

Name *

VersaINTERNET

Virtual network ⓘ

Hub-VNet

Subnet * ⓘ

Internet-Circuit (172.16.26.0/27)

NIC network security group ⓘ

● None

○ Basic

○ Advanced

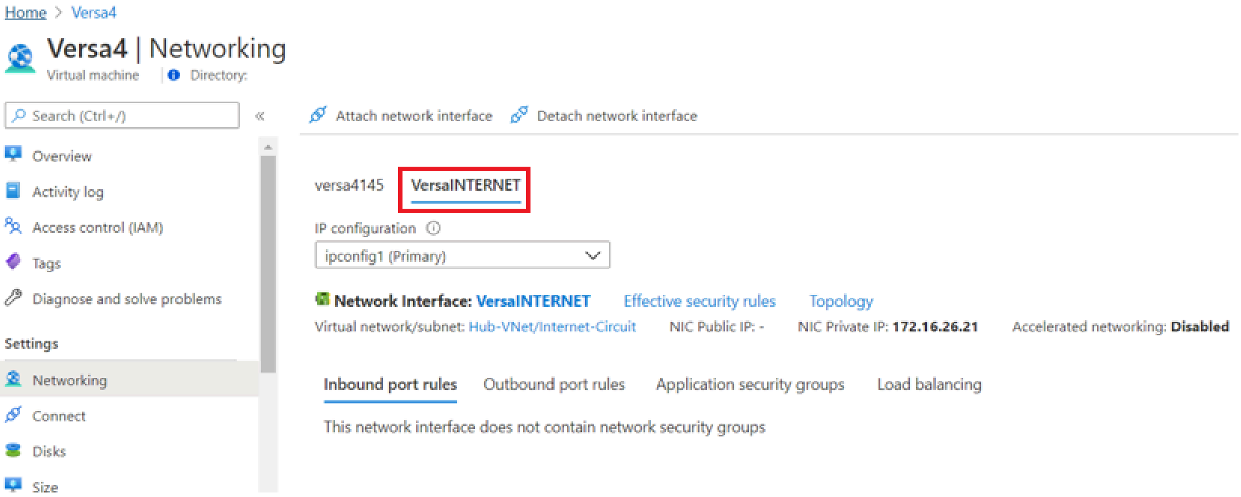
Private IP address assignment

[✓ Dynamic] Static

□ Private IP address (IPv6)

| Field | Description |
|---|---|
| Name | Enter an interface name (here, VersaINTERNET). |
| Subnet | Select the subnet from which the interface receives an IP address. |
| NIC Network Security Group | Select None. |
| Private IP Address Assignment | Select Static and assign an unused IP from the subnet as the static address |

29. Click create to add the interface to the VM.



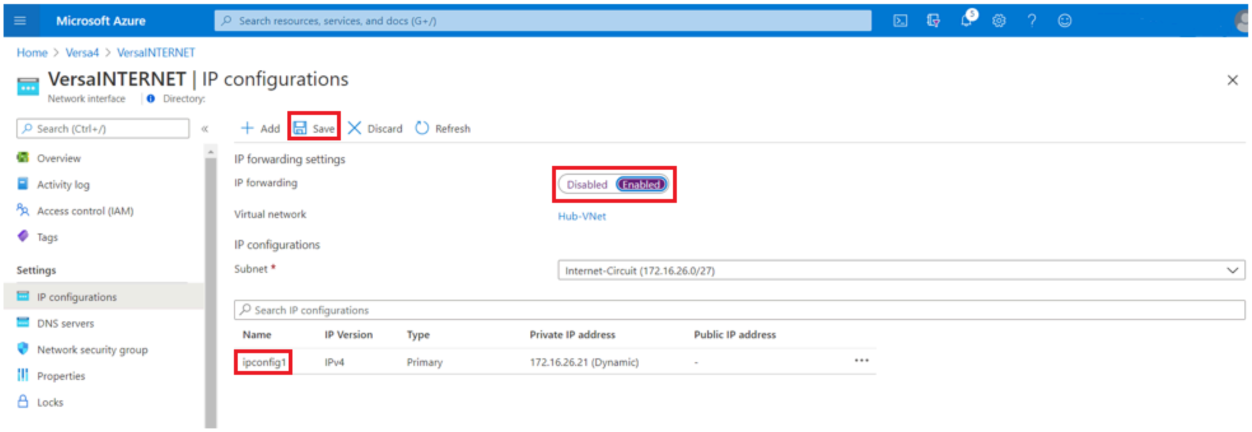
IP configuration: ipconfig1 (Primary)

Network Interface: VersaINTERNET

Virtual network/subnet: Hub-VNet/Internet-Circuit NIC Public IP: - NIC Private IP: 172.16.26.21 Accelerated networking: Disabled

This network interface does not contain network security groups

30. Click the interface name, here, VersaINTERNET.



IP forwarding settings

IP forwarding: Disabled [✓ Enabled]

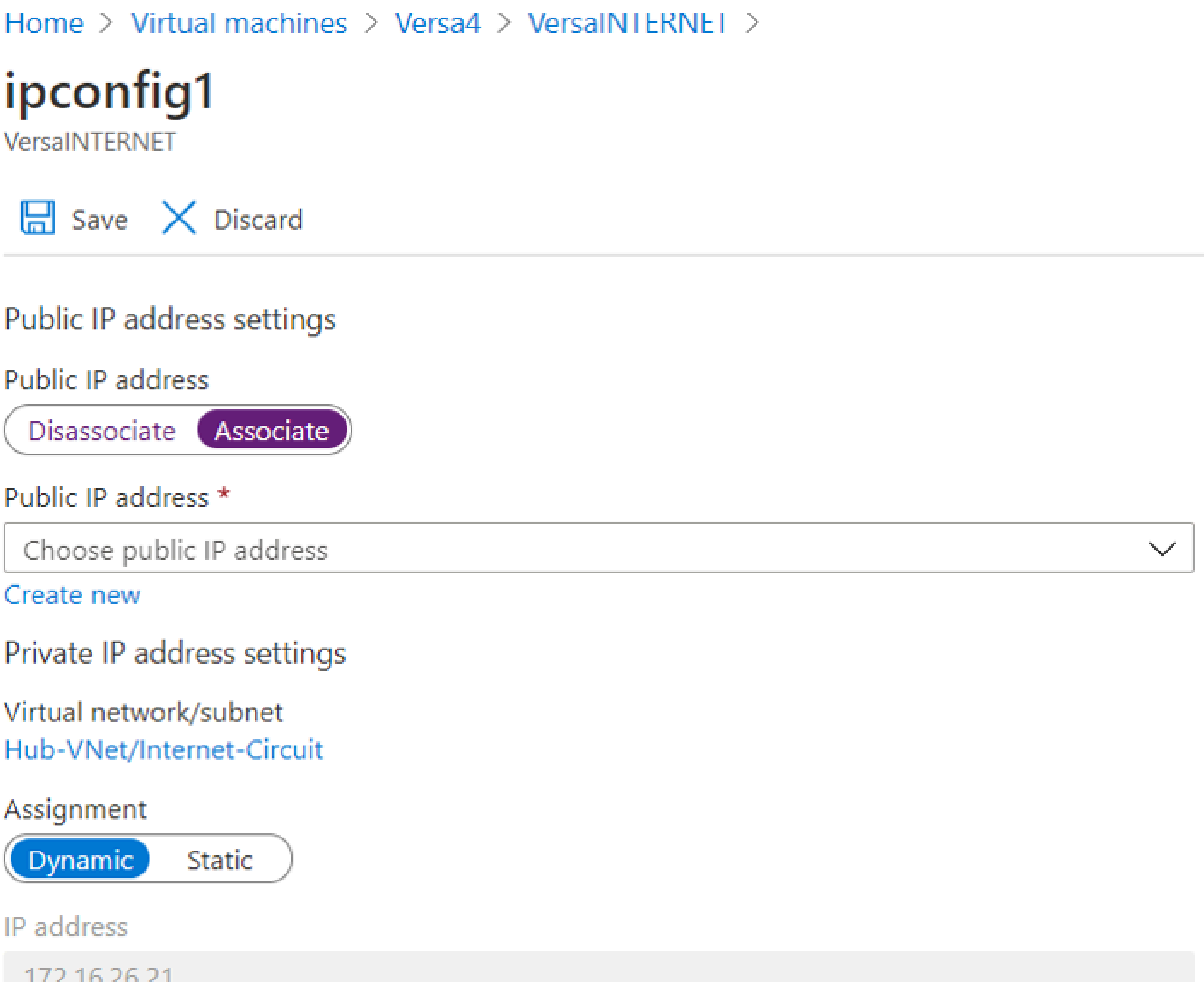
Virtual network: Hub-VNet

IP configurations

Subnet *: Internet-Circuit (172.16.26.0/27)

| Name | IP Version | Type | Private IP address | Public IP address |
|---|---|---|---|---|
| ipconfig1 | IPv4 | Primary | 172.16.26.21 (Dynamic) | - |

31. Select IP configurations in the left menu, and ensure that IP Forwarding is enabled.
32. Click save and then click ipconfig1.



ipconfig1

VersaINTERNET

Public IP address settings

Public IP address: Disassociate [✓ Associate]

Public IP address *: Choose public IP address

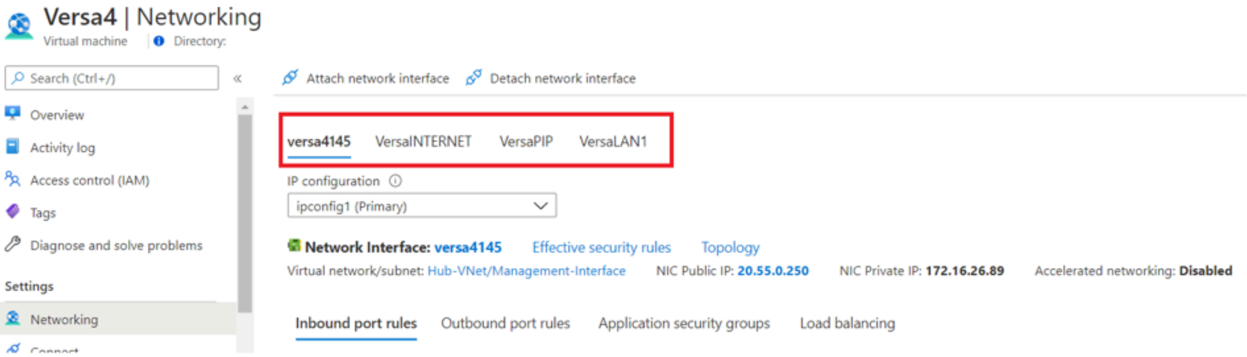
Private IP address settings

Virtual network/subnet: Hub-VNet/Internet-Circuit

Assignment: [✓ Dynamic] Static

IP address: 172.16.26.21

33. Associate a public IP address, and then choose an existing public IP address or create a new one.
34. Click save.
35. Repeat Steps 28 through 34 to add the remaining interfaces. For MPLS and LAN interfaces, you do not need to associate a public IP address, so you can skip these steps for these two interface types.

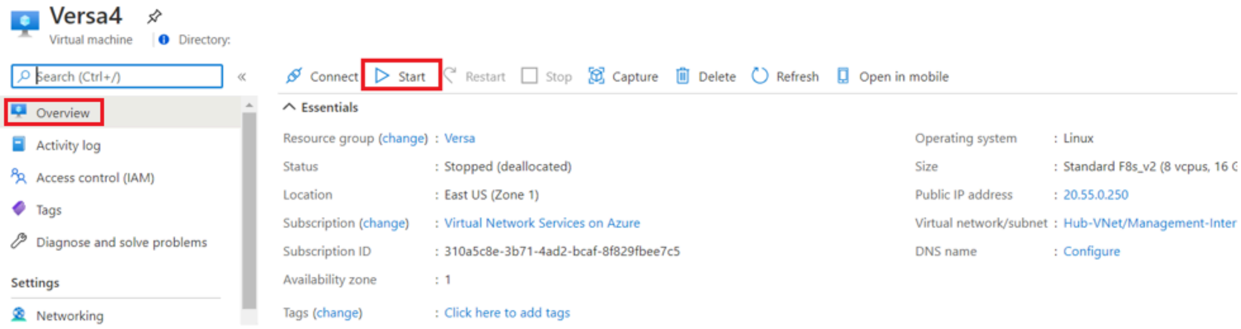


IP configuration: ipconfig1 (Primary)

Network Interface: versa4145

Virtual network/subnet: Hub-VNet/Management-Interface NIC Public IP: 20.55.0.250 NIC Private IP: 172.16.26.89 Accelerated networking: Disabled

36. Restart the VM by selecting the Overview page and clicking Start.



Resource group (change) : Versa
Status : Stopped (deallocated)
Location : East US (Zone 1)
Subscription (change) : Virtual Network Services on Azure
Subscription ID : 310a5c8e-3b71-4ad2-bcaf-8f829fbee7c5
Availability zone : 1
Tags (change) : Click here to add tags

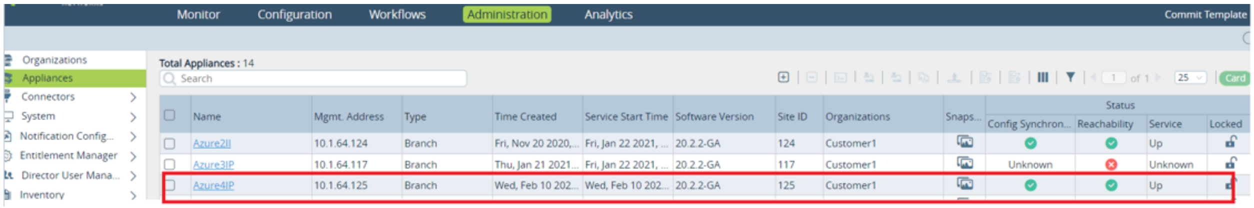
Operating system : Linux
Size : Standard F8s_v2 (8 vcpus, 16 G
Public IP address : 20.55.0.250
Virtual network/subnet : Hub-VNet/Management-Inter
DNS name : Configure

After the instance is up and running, you can ssh back into the device using the management (MGMT) interface and onboard the device to the Versa Director, similar to any CPE deployment. For more information, see Create Provider Organizations.

Note that while creating the device workflow in Versa Director, the bind data for the device must be based on the private IP address for the internet interface and not the public IP address that was associated with the interface in Step 33, above. The next hop for internet and PIP interfaces is the first usable IP address in their respective Azure subnets. For example, the default gateway for the subnet 172.16.26.0/27 is 172.16.26.1, as shown below:

```
[admin@Versa: ~] $ cd /opt/versa/scripts/
[admin@Versa: scripts] $  sudo ./staging.py -l SDWAN-Branch@customer.com -r Controller-DC1-staging@customer.com -n 411 -c ip-address -w 0 -s 172.16.26.21/27 -g 172.16.26.1
```

To view the appliance, in the Director view, go to Administration > Appliances.



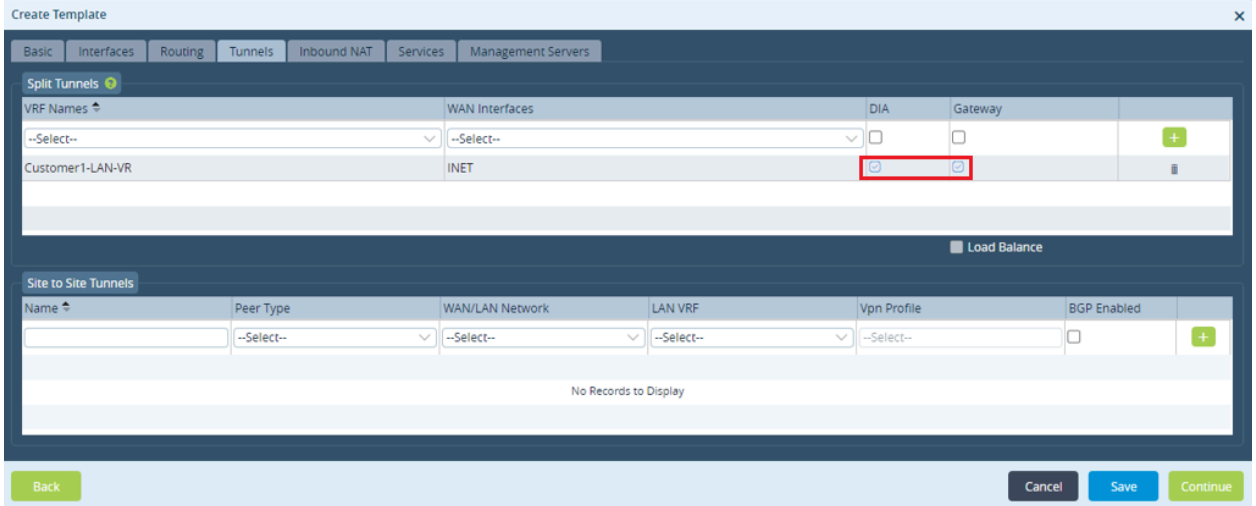
Total Appliances : 14

| □ | Name | Mgmt. Address | Type | Time Created | Service Start Time | Software Version | Site ID | Organizations | Snaps... | Status |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
|  |  |  |  |  |  |  |  |  |  | Config Synchron... | Reachability | Service | Locked |
| □ | Azure2II | 10.1.64.124 | Branch | Fri, Nov 20 2020,... | Fri, Jan 22 2021, ... | 20.2.2-GA | 124 | Customer1 |  | ✓ | ✓ | Up |  |
| □ | Azure3IP | 10.1.64.117 | Branch | Thu, Jan 21 2021... | Fri, Jan 22 2021, ... | 20.2.2-GA | 117 | Customer1 |  | Unknown | ✗ | Unknown |  |
| □ | Azure4IP | 10.1.64.125 | Branch | Wed, Feb 10 202... | Wed, Feb 10 202... | 20.2.2-GA | 125 | Customer1 |  | ✓ | ✓ | Up |  |

If you deploy a Versa VNF as an internet breakout, for the rest of the locations associated with the SD-WAN fabric, ensure that you deploy the Versa VNF using both the DIA and gateway options in the device template. Also, if you are deploying using internet breakout, you can deploy NGFW services at the same time.

To deploy a Versa VNF using DIA and gateway options, and to deploy NGFW at the same time:

1. In Director view, select the Workflows tab in the top menu bar.
2. Select Template > Templates in the left menu bar.
3. Click the ⊞ Add icon to create a new template.
4. Select the Tunnels tab.



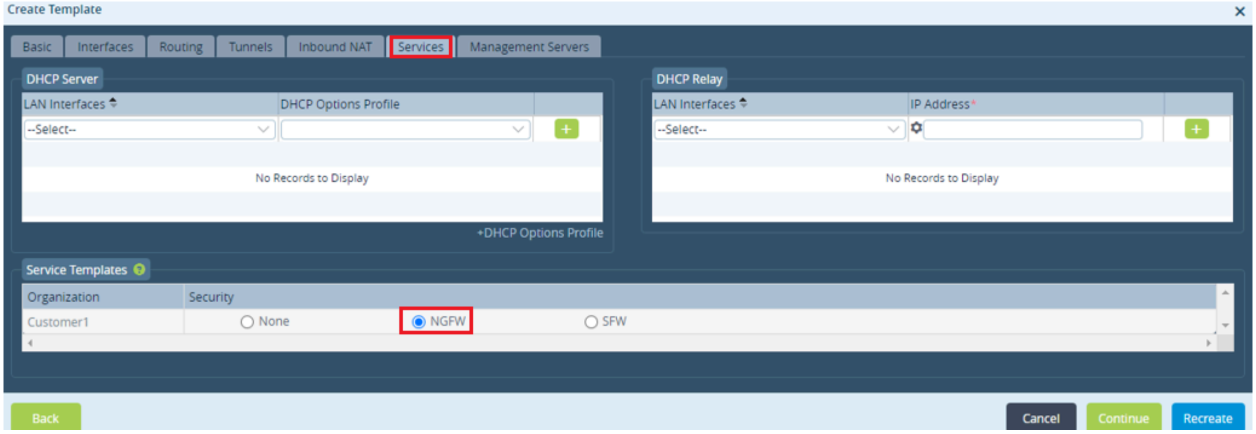
| VRF Names | WAN Interfaces | DIA | Gateway |
|---|---|---|---|
| --Select-- | --Select-- | □ | □ |
| Customer1-LAN-VR | INET | ☑ | ☑ |

□ Load Balance

| Name | Peer Type | WAN/LAN Network | LAN VRF | Vpn Profile | BGP Enabled |
|---|---|---|---|---|---|
|  | --Select-- | --Select-- | --Select-- | --Select-- | □ |

No Records to Display

5. Select DIA and Gateway for the split tunnel you select.
6. Select the Services tab, and then select NGFW under Service Templates.



| LAN Interfaces | DHCP Options Profile |
|---|---|
| --Select-- |  |

No Records to Display

| LAN Interfaces | IP Address* |
|---|---|
| --Select-- |  |

No Records to Display

| Organization | Security |  |  |
|---|---|---|---|
| Customer1 | ○ None | ● NGFW | ○ SFW |

7. For information about configuring other fields in the Create Template screen, see Create Device Templates.
8. Click Save.

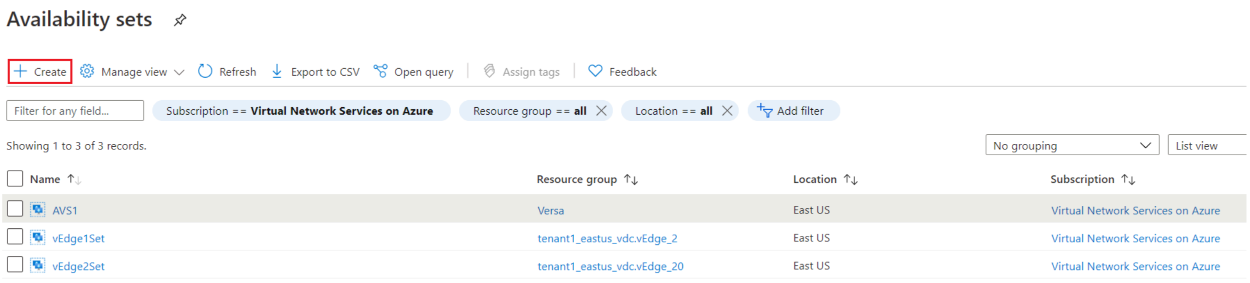
## Add Availability Sets in Azure

You can add availability sets to install VMs in different fault and update domains. Each fault domain shares a common power source and network. Using availability sets provides resiliency, or high availability (HA) within a datacenter (availability zone). Performing this step is optional.

Note that the VMs deployed in an availability set are automatically placed into different fault and update domains. Because you deploy only two Versa VNFs in the availability set, you need only two of domains of each set.

To add an availability set:

1. In Azure, click + Create in the Availability sets section. The Create Availability Set window displays.

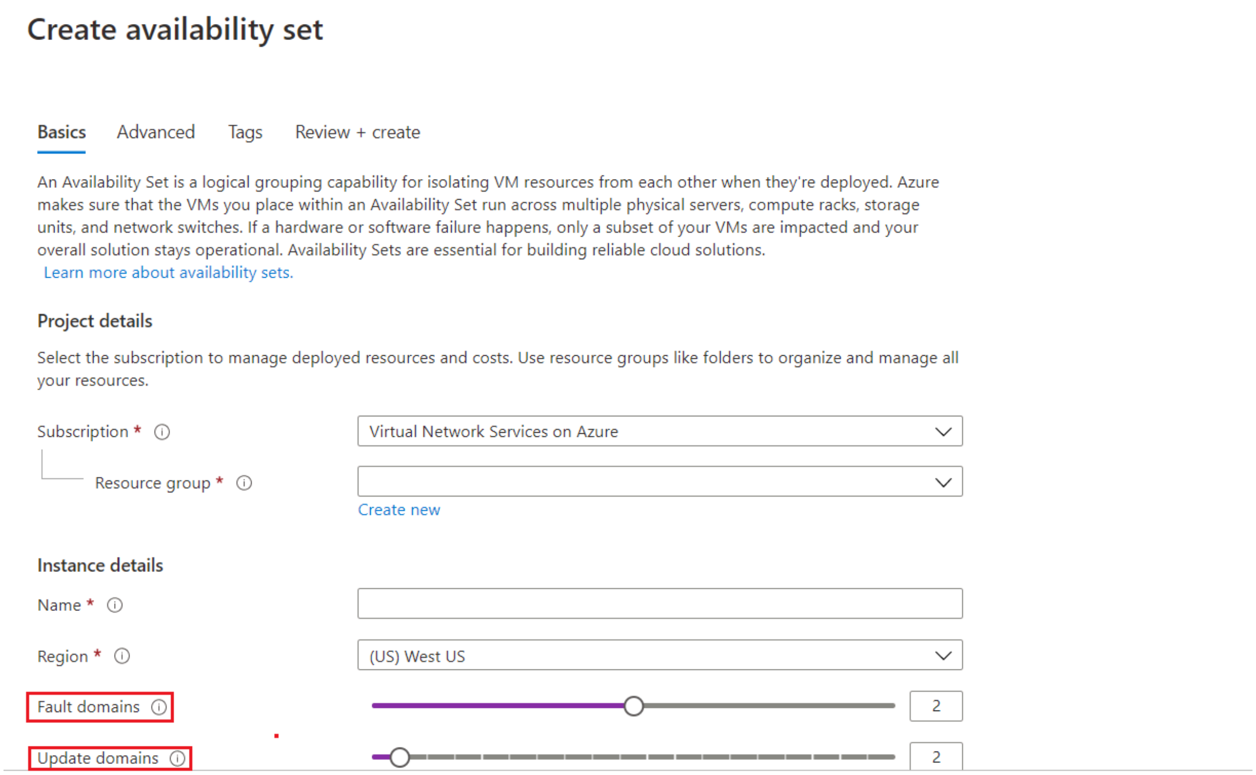


Availability sets

Showing 1 to 3 of 3 records.

| Name | Resource group | Location | Subscription |
|---|---|---|---|
| AVS1 | Versa | East US | Virtual Network Services on Azure |
| vEdge1Set | tenant1_eastus_vdc.vEdge_2 | East US | Virtual Network Services on Azure |
| vEdge2Set | tenant1_eastus_vdc.vEdge_20 | East US | Virtual Network Services on Azure |

2. In both the Fault Domains and Update Domains, enter 2 to create two of each domain in the availability set.



Create availability set

An Availability Set is a logical grouping capability for isolating VM resources from each other when they're deployed. Azure makes sure that the VMs you place within an Availability Set run across multiple physical servers, compute racks, storage units, and network switches. If a hardware or software failure happens, only a subset of your VMs are impacted and your overall solution stays operational. Availability Sets are essential for building reliable cloud solutions.
Learn more about availability sets.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Virtual Network Services on Azure

Resource group * :

Create new

Instance details

Name * :

Region * : (US) West US

Fault domains : 2

Update domains : 2

3. Enter other required information.
4. Click Review and Create.

## Peer Versa VNFs to an Azure Virtual Router BGP Endpoint

To create EBGP peering between Versa VNFs and the Azure BGP endpoint or virtual routers (VRs), you must obtain the AS number (ASN) and IP address of the virtual routers. You can do this using PowerShell, which is the same way that you created the virtual routers. For example:

> PS C:\Users\*user-name*> **Get-AzVirtualRouter -RouterName VersaVR -ResourceGroupName** *resource-group-name*

```
Name              : VersaVR
ResourceGroupName : VNSPOCRG
Location          : eastus
Id              : /subscriptions/310a5c8e-3b71-4ad2-bcaf-8f829fbee7c5/resourceGroups/VNSPOCRG/providers/
Microsoft.Net
                  work/virtualHubs/VersaVR
Etag              :
Type              : Microsoft.Network/virtualHubs
ProvisioningState : Succeeded
HostedSubnet      : /subscriptions/310a5c8e-3b71-4ad2-bcaf-8f829fbee7c5/resourceGroups/VNSPOCRG/
providers/Microsoft.Net
                  work/virtualNetworks/Hub-VNet/subnets/VR-Subnet
VirtualRouterAsn  : 65515
VirtualRouterIps  : {172.16.26.132, 172.16.26.133}
Peerings          : [
                    {
                      "PeerAsn": 65002,
                      "PeerIp": "172.16.26.109",
                      "ProvisioningState": "Succeeded",
                      "Name": "Versa2"
                    },
                    {
                      "PeerAsn": 65002,
                      "PeerIp": "172.16.26.108",
                      "ProvisioningState": "Succeeded",
                      "Name": "Versa3"
                    }
                  ]
```

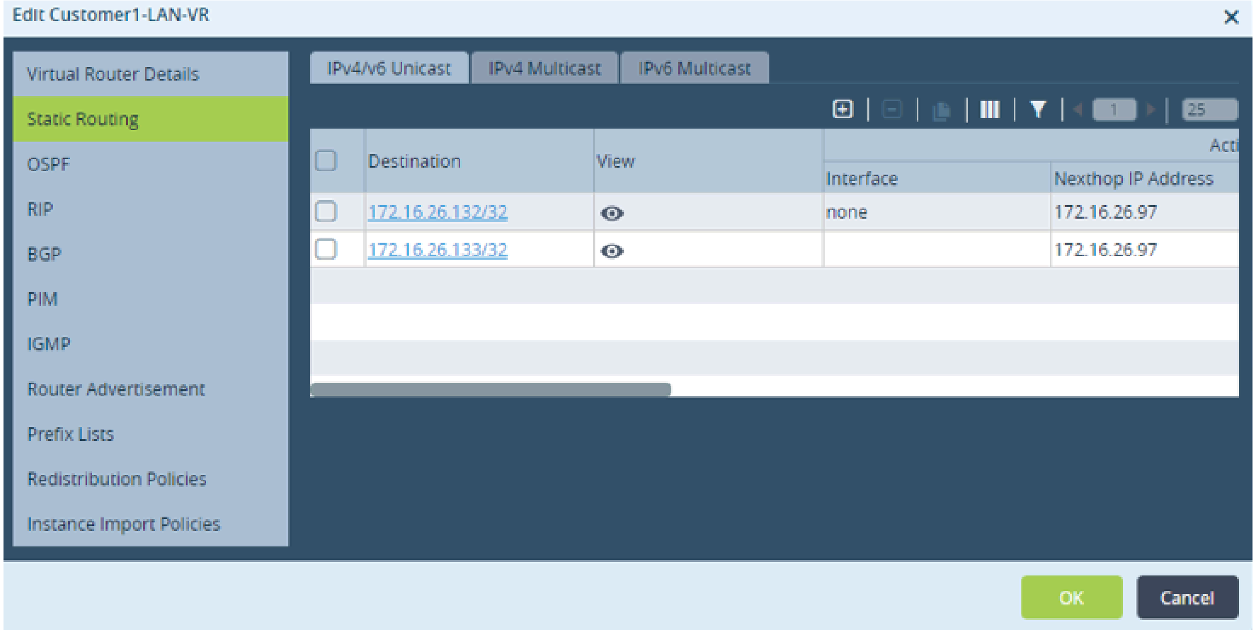
Here, the AS number is 65515 and the router has two IP addresses, one for each virtual router. The Versa VNFs peer with the Azure virtual router using the LAN interface. Because the Versa VNF LAN interface and the virtual router are on separate subnets in the Hub-V-Net (the virtual router is in its own dedicated subnet), you must configure a static route on the Versa VNF for the virtual router (here, 172.16.26.132) that points towards the Azure default gateway (route table) for the LAN subnet. This route table is the first usable IP address of the LAN subnet.

## Configure a Static Route on the Versa VNF

To configure a static route on the Versa VNF for the virtual router:

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates > Device Templates in the horizontal menu bar.
   c. Select an organization in the left menu bar.
   d. Select a post-staging template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Virtual Routers in the left menu bar.
4. Click the ⊞ Add icon. The Configure Virtual Router popup window displays.

5. Select Static Routing in the left menu bar. The following screenshot shows that 172.16.26.132 is configured with static routes. For more information, see Configure Static Routes.



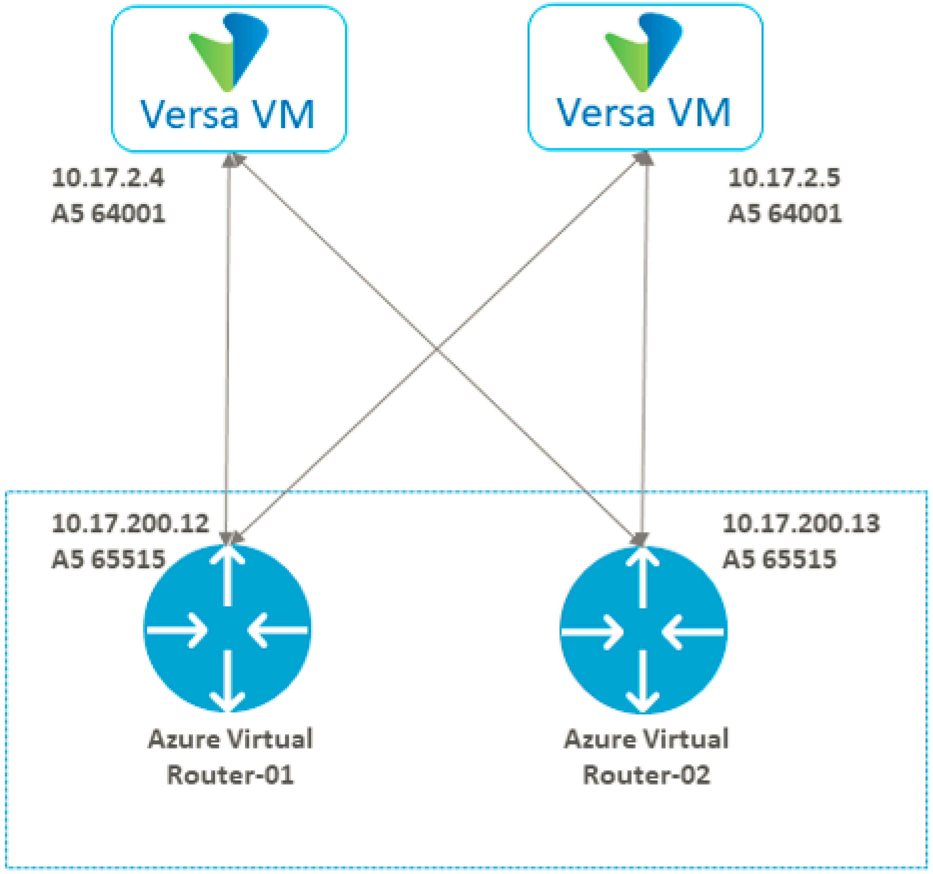
| □ | Destination | View | Acti |  |
|---|---|---|---|---|
|  |  |  | Interface | Nexthop IP Address |
| □ | 172.16.26.132/32 | 👁 | none | 172.16.26.97 |
| □ | 172.16.26.133/32 | 👁 |  | 172.16.26.97 |

After you configure a static route on the Versa VNF for the virtual router, you can ping the virtual routerss from the LAN interface on Versa VNF. For example:

```
admin@azure-cli> ping 172.16.26.132 routing-instance Customer1-LAN-VR source 172.16.26.110
PING 172.16.26.132 (172.16.26.132) from 172.16.26.110 : 56(84) bytes of data.
64 bytes from 172.16.26.132: icmp_seq=1 ttl=128 time=3.36 ms
64 bytes from 172.16.26.132: icmp_seq=2 ttl=128 time=3.31 ms
64 bytes from 172.16.26.132: icmp_seq=3 ttl=128 time=3.40 ms
64 bytes from 172.16.26.132: icmp_seq=4 ttl=128 time=7.55 ms
64 bytes from 172.16.26.132: icmp_seq=5 ttl=128 time=3.35 ms
```

## Configure EBGP Peering to Virtual Routers

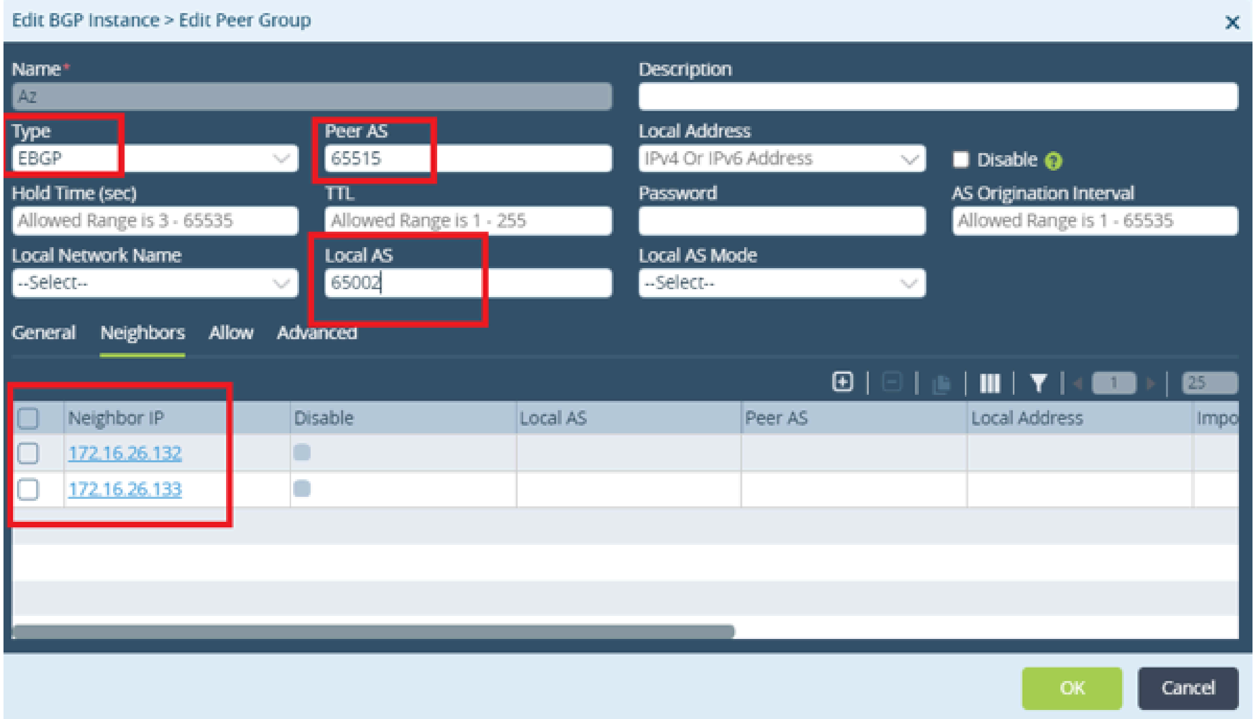
You can now configure eBGP peering to the virtual routers, starting with the Versa VNFs. The following illustration shows the peering from Versa to the virtual routers, with each Versa VNF peering to both virtual routers for redundancy.



If you deploy the Versa VNF as a internet breakout gateway, a BGP instance exists in the customer's LAN virtual router. You can use the same BGP instance and build a new peer group to the Azure virtual router IP addresses, as illustrated in the following procedure example:

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates > Device Templates in the horizontal menu bar.
   c. Select an organization in the left menu bar.
   d. Select a post-staging template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Virtual Routers in the left menu bar.
4. Select the customer LAN VR from the main tab. The Edit Configure Virtual Router popup window displays.
5. Select the BGP tab in the left menu bar. The main pane displays a list of the BGP instances that are already configured.
6. Select the BGP instance that exists in the customer's LAN VR. The Edit BGP screen displays and this BGP instance uses local AS number 64514 by default.
7. Select the BGP Peer Group tab.

8. Click the ⊞ Add icon. In the Add Peer Group popup window, enter information for the following fields. The following example uses the Edit Peer Group screen.



Edit BGP Instance > Edit Peer Group

Name* Az

Description

Type EBGP

Peer AS 65515

Local Address IPv4 Or IPv6 Address

□ Disable

Hold Time (sec) Allowed Range is 3 - 65535

TTL Allowed Range is 1 - 255

Password

AS Origination Interval Allowed Range is 1 - 65535

Local Network Name --Select--

Local AS 65002

Local AS Mode --Select--

| □ | Neighbor IP | Disable | Local AS | Peer AS | Local Address | Impo |
|---|---|---|---|---|---|---|
| □ | 172.16.26.132 | | | | | |
| □ | 172.16.26.133 | | | | | |

| Field | Description |
|---|---|
| Type | Select EBGP. |
| Peer AS | Enter 65515 as the Azure VR AS number. |
| Local AS | Enter 65002 as the local AS number. |
| Neighbors (Tab) | Select, and click the Add icon to add neighbors. Here, 172.16.26.132 and 172.16.26.132 are the neighbor IP addresses for this peer group. |

9. For information about configuring other fields, see Configure a BGP Peer Group.
10. Click OK.

If you did not deploy the Versa VNF as an internet breakout gateway, the BGP instance may not exist in the customer's LAN VR. In this case, you can add a BGP instance 3014 and the appropriate BGP and neighbor attributes, with a local AS number of 65002. Alternatively, you can configure BGP and static routing when you create the device template. For more information, see Create Device Templates.

To complete the BGP setup between the Versa VNF and Azure virtual routers, create creating the peering on the Azure virtual router in PowerShell using a Versa LAN IP address and ASN 65002. For example:

```
PS C:\Users\user-name> Add-AzVirtualRouterPeer -PeerName "Versa4" -PeerIp "172.16.26.110" -PeerAsn
"65002" -VirtualRouterName "VersaVR" -ResourceGroupName VNSPOCRG

Name              : VersaVR
ResourceGroupName : VNSPOCRG
Location          : eastus
Id                : /subscriptions/310a5c8e-3b71-4ad2-bcaf-8f829fbee7c5/resourceGroups/VNSPOCRG/providers/
Microsoft.Net
                    work/virtualHubs/VersaVR
Etag              :
Type              : Microsoft.Network/virtualHubs
ProvisioningState : Succeeded
HostedSubnet      : /subscriptions/310a5c8e-3b71-4ad2-bcaf-8f829fbee7c5/resourceGroups/VNSPOCRG/
providers/Microsoft.Net
                    work/virtualNetworks/Hub-VNet/subnets/VR-Subnet
VirtualRouterAsn  : 65515
VirtualRouterIps  : {172.16.26.132, 172.16.26.133}
Peerings          : [
                      {
                        "PeerAsn": 65002,
                        "PeerIp": "172.16.26.109",
                        "ProvisioningState": "Succeeded",
                        "Name": "Versa2"
                      },
                      {
                        "PeerAsn": 65002,
                        "PeerIp": "172.16.26.108",
                        "ProvisioningState": "Succeeded",
                        "Name": "Versa3"
                      },
                      {
                        "PeerAsn": 65002,
                        "PeerIp": "172.16.26.110",
                        "ProvisioningState": "Succeeded",
                        "Name": "Versa4"
                      }
                    ]
```

Verify the BGP peering on the Versa VNF device:

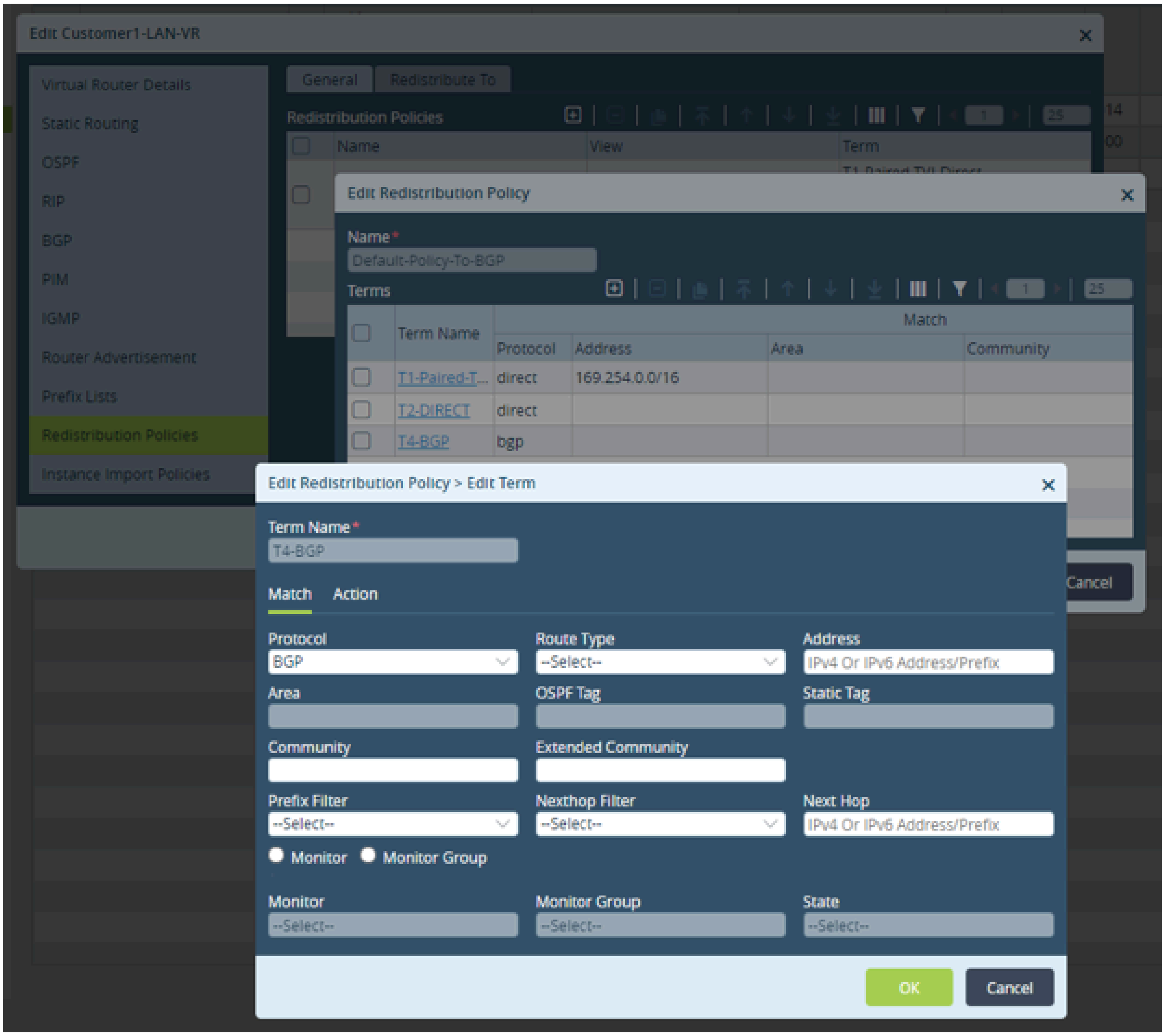
```
admin@Azure-cli> show bgp neighbor org organization-name brief
routing-instance: Customer1-Control-VR

Neighbor        Uptime      State        PfxRcd     PfxSent   local-port  remote-port
10.1.64.1       19:11:56   Established     93         12       39230        179
10.1.64.2       n/a        Connect         0          0          0          0
routing-instance: Customer1-LAN-VR

Neighbor        Uptime      State        PfxRcd     PfxSent   local-port  remote-port
172.16.26.132   00:00:34   Established      4         20       50752        179
172.16.26.133   00:00:34   Established      4         24       49936        179
```

Finally, ensure that the BGP routes learned from the Azure virtual routers are redistributed to the SD-WAN overlay IBGP control plane. To do this, ensure that BGP that part of the redistribution policy in the customer LAN virtual router has an action of Accept as shown in the following configuration example:

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates > Device Templates in the horizontal menu bar.
   c. Select an organization in the left menu bar.
   d. Select a post-staging template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Virtual Routers in the left menu bar.
4. Select the customer LAN VR from the main tab. The Edit Configure Virtual Router popup window displays.
5. Select the Redistribution Policies tab in the left menu bar.
6. In the General tab, select the BGP redistribution policy that you want to edit (here, Default-Policy-To-BGP). The Edit Redistribution Policy popup window displays.



Name* Default-Policy-To-BGP

Terms

|  | Term Name | Match |  |  |  |
|---|---|---|---|---|---|
|  |  | Protocol | Address | Area | Community |
| □ | T1-Paired-T... | direct | 169.254.0.0/16 |  |  |
| □ | T2-DIRECT | direct |  |  |  |
| □ | T4-BGP | bgp |  |  |  |

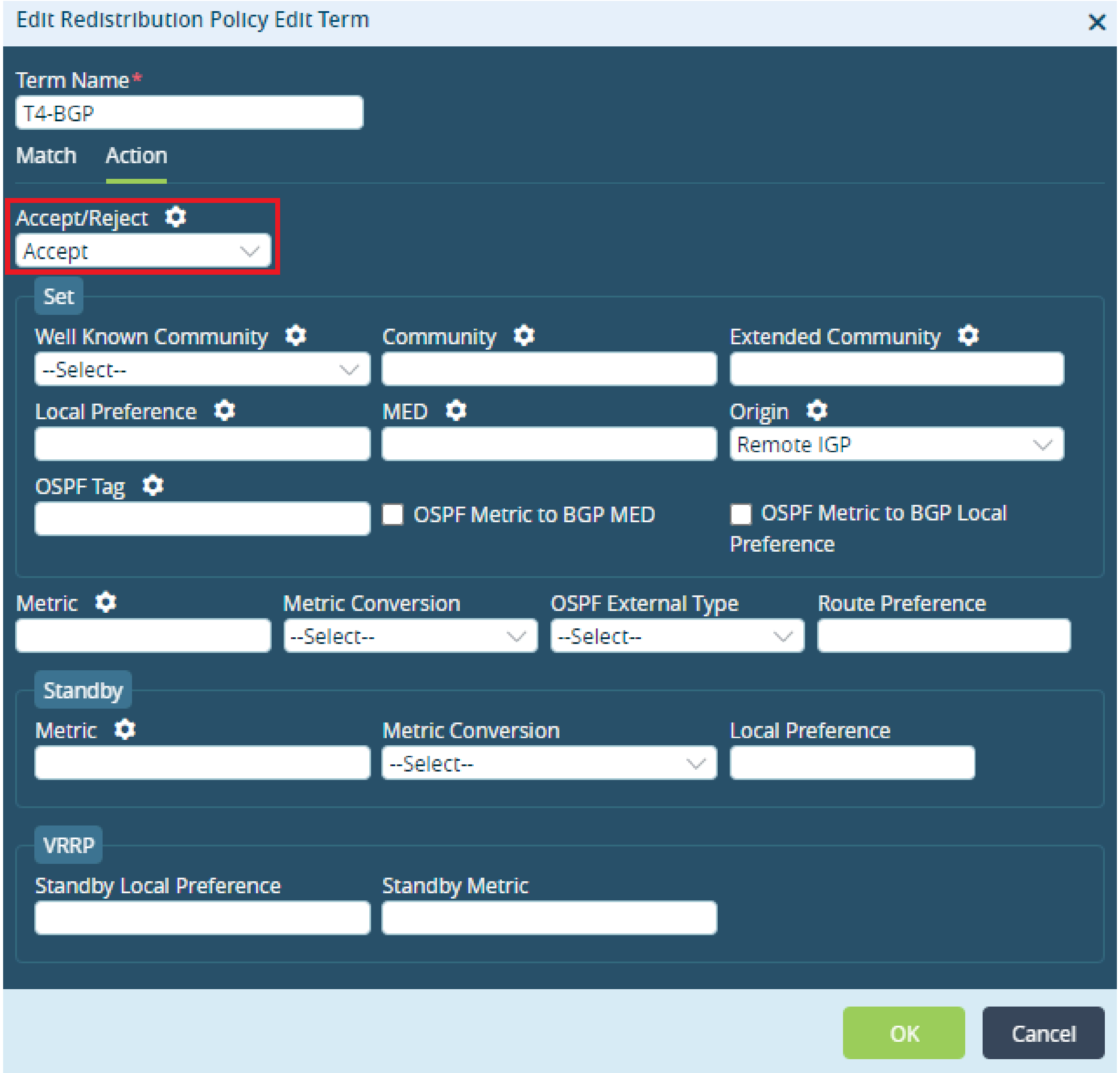
Term Name* T4-BGP

| | | |
|---|---|---|
| Protocol: BGP | Route Type: --Select-- | Address: IPv4 Or IPv6 Address/Prefix |
| Area: | OSPF Tag: | Static Tag: |
| Community: | Extended Community: | |
| Prefix Filter: --Select-- | Nexthop Filter: --Select-- | Next Hop: IPv4 Or IPv6 Address/Prefix |

○ Monitor ○ Monitor Group

| | | |
|---|---|---|
| Monitor: --Select-- | Monitor Group: --Select-- | State: --Select-- |

7. Click the BGP term (here, T4-BGP) under Terms. The Edit Redistribution Policy > Edit Term popup window displays.



Edit Redistribution Policy Edit Term

Term Name*: T4-BGP

Match | Action

Accept/Reject: Accept

Set

Well Known Community: --Select--

Community:

Extended Community:

Local Preference:

MED:

Origin: Remote IGP

OSPF Tag:

□ OSPF Metric to BGP MED

□ OSPF Metric to BGP Local Preference

Metric:

Metric Conversion: --Select--

OSPF External Type: --Select--

Route Preference:

Standby

Metric:

Metric Conversion: --Select--

Local Preference:

VRRP

Standby Local Preference:

Standby Metric:

8. Select the Action tab, and then select Accept in the Accept/Reject field, to accept all traffic for the route.
9. For more information about other fields, see Configure Redistribution Policies.
10. Click OK.

## Deploy Dual Versa VNFs in Azure

When deploying dual Versa VNFs in Azure, either in separate availability zones or in the same availability zone or availability set, you do not deploy them as a traditional VOS high availability (HA) pair. That is, you do not deploy dual Versa VNFs by selecting Redundant Pair in the Workflows template. Instead, you install them in Azure as two standalone Versa VNFs, because the dot1.q tagging that is required for the cross-connect of a traditional VOS HA pair is not supported.

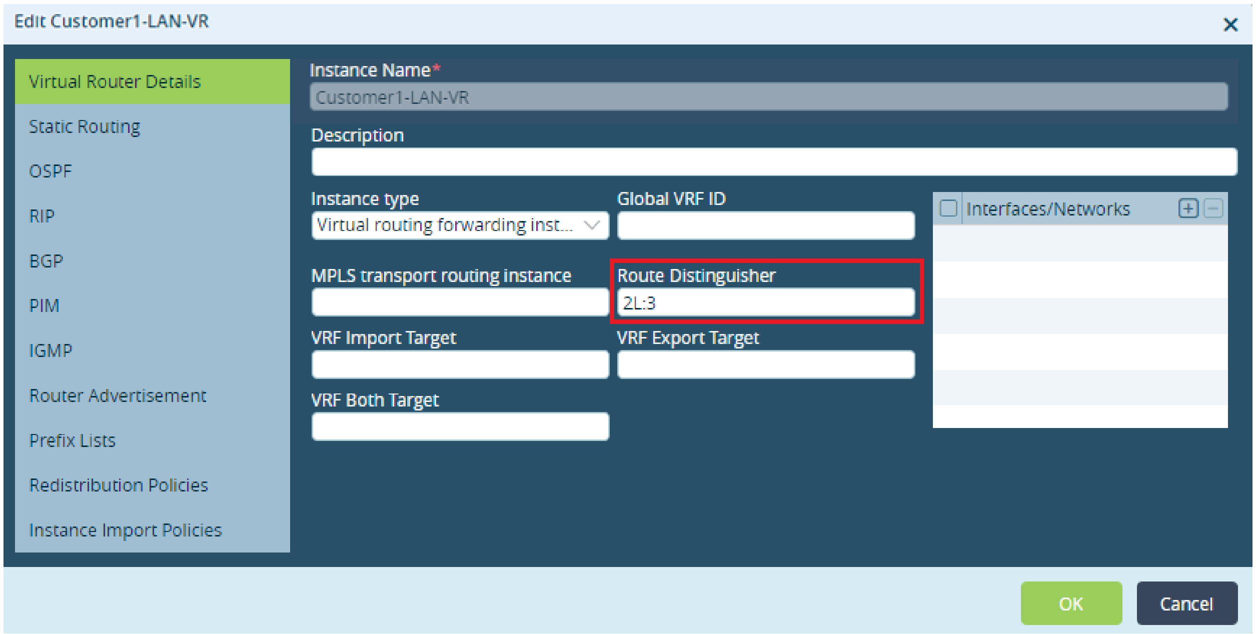
Both Versa VNFs deployed in Azure must peer with the Azure virtual router in the same way as described in Peer Versa VNFs to an Azure Virtual Router BGP Endpoint, above. Both Versa VNFs learn the spoke VNET routes and advertise them to the SD-WAN fabric. This is the same for the default route to internet if you have configured both Versa VNFs to act as internet breakout gateways for other SD-WAN sites.

Both Versa VNFs must advertise these networks with different route distinguishers to Versa Controller nodes, which allows the Controller nodes to reflect both routes to other SD-WAN locations. You change the route distinguisher only on one Versa VNF.

## Change the Route Distinguisher

To change the route distinguisher on one of the Versa VNF devices:

1. In Director view:
    a. Select the Configuration tab in the top menu bar.
    b. Select Templates > Device Templates in the horizontal menu bar.
    c. Select an organization in the left menu bar.
    d. Select a post-staging template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Virtual Routers in the left menu bar.
4. Select the customer LAN VR (here, Customer1-LAN-VR) from the main tab. The Edit Configure Virtual Router popup window displays.



Instance Name*: Customer1-LAN-VR
Description:
Instance type: Virtual routing forwarding inst...
Global VRF ID:
MPLS transport routing instance:
Route Distinguisher: 2L:3
VRF Import Target:
VRF Export Target:
VRF Both Target:

5. Change the Route Distinguisher value by one, here, from 2L:2 to 2L:3.

6. For more information about the other fields, see Set Up a Virtual Router.
7. Click OK.

Verify whether the route tables of a remote device outside of the Azure infrastructure show the routes for both Versa VNFs:

```
admin@versa-cli> show route routing-instance lan-vr-name
Routes for Routing instance : Customer1-LAN-VR  AFI: ipv4
Codes: E1 - OSPF external type 1, E2 - OSPF external type 2
IA - inter area, iA - intra area,
L1 - IS-IS level-1, L2 - IS-IS level-2
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
+ - Active Route
Prot    Type   Dest Address/Mask     Next Hop       Age      Interface Name
----    ----   -----------------     ---------      ---      --------------
BGP     N/A    +0.0.0.0/0            10.1.64.124    02:28:26  Indirect
BGP     N/A    +0.0.0.0/0            10.1.64.125    00:00:29  Indirect
BGP     N/A     172.16.26.0/24       10.1.64.124    03:14:24  Indirect
BGP     N/A    +172.16.26.0/24       10.1.64.125    00:00:29  Indirect
BGP     N/A    +172.16.26.96/27      10.1.64.124    2w6d20h   Indirect
BGP     N/A    +172.16.26.96/27      10.1.64.125    03:14:24  Indirect
BGP     N/A     172.16.27.0/24       10.1.64.124    03:14:24  Indirect
BGP     N/A    +172.16.27.0/24       10.1.64.125    00:00:29  Indirect
BGP     N/A     172.16.28.0/24       10.1.64.124    03:14:24  Indirect
BGP     N/A    +172.16.28.0/24       10.1.64.125    00:00:29  Indirect
BGP     N/A     172.16.29.0/24       10.1.64.124    03:14:24  Indirect
BGP     N/A    +172.16.29.0/24       10.1.64.125    00:00:29  Indirect
```

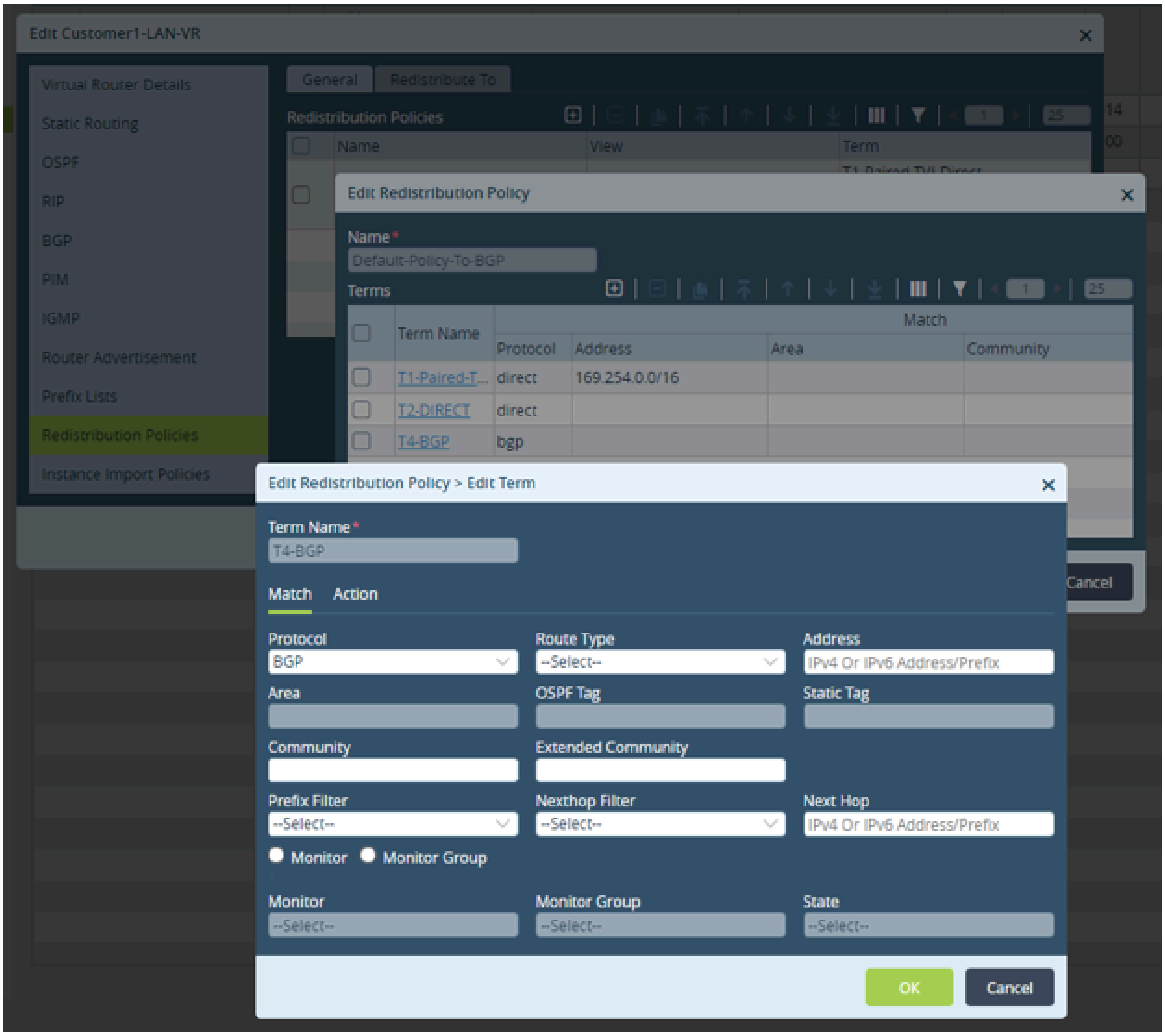
## Configure Active and Standby Versa VNF Devices

To route traffic through the Versa VNFs in a symmetrical and deterministic manner, you configure the Versa VNFs such that traffic is routed through one Versa VNF that acts as the active device and fails over to the other Versa VNF that acts as a standby device.

To do this, the standby Versa VNF device must advertise a lower local preference value than the primary Versa VNF, which forces the remote SD-WAN devices to forward traffic to the primary device. In the following example, the Versa VNF with the next hop 10.1.64.125 is configured as the secondary device by changing the local preference that it advertises to 90 for the redistributed BGP routes in the Customer-LAN-VR.

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates > Device Templates in the horizontal menu bar.
   c. Select an organization in the left menu bar.
   d. Select a post-staging template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Virtual Routers in the left menu bar.

4. Select the customer LAN VR from the main tab. The Edit Configure Virtual Router popup window displays.
5. Select the Redistribution Policies tab in the left menu bar.
6. In the General tab, select the BGP redistribution policy that you want to edit (here, Default-Policy-To-BGP). The Edit Redistribution Policy popup window displays.



Name*: Default-Policy-To-BGP

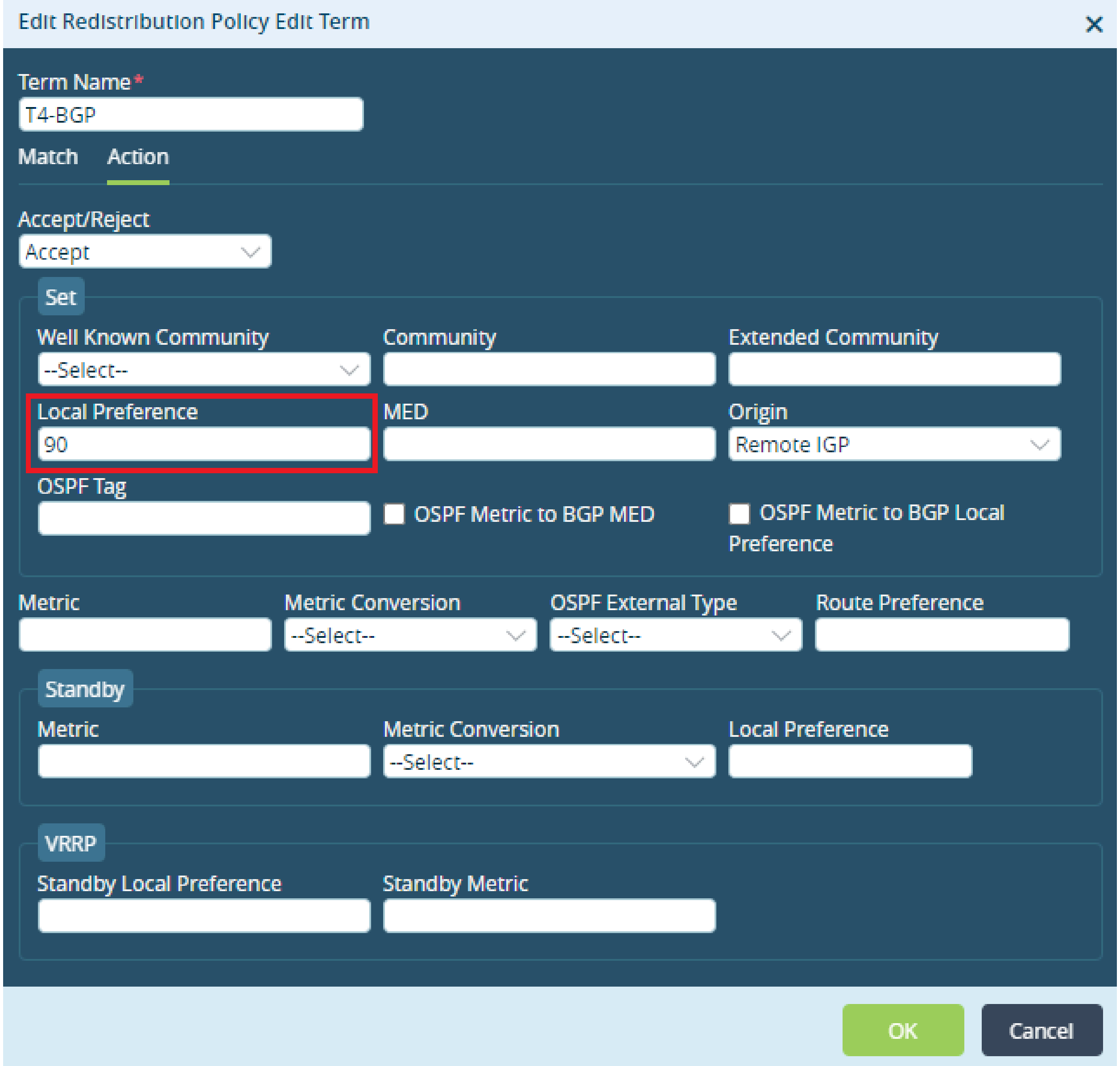
Terms

| □ | Term Name | Match | | | |
|---|---|---|---|---|---|
| | | Protocol | Address | Area | Community |
| □ | T1-Paired-T... | direct | 169.254.0.0/16 | | |
| □ | T2-DIRECT | direct | | | |
| □ | T4-BGP | bgp | | | |

Term Name*: T4-BGP

| | | |
|---|---|---|
| Protocol: BGP | Route Type: --Select-- | Address: IPv4 Or IPv6 Address/Prefix |
| Area: | OSPF Tag: | Static Tag: |
| Community: | Extended Community: | |
| Prefix Filter: --Select-- | Nexthop Filter: --Select-- | Next Hop: IPv4 Or IPv6 Address/Prefix |
| ○ Monitor ○ Monitor Group | | |
| Monitor: --Select-- | Monitor Group: --Select-- | State: --Select-- |

7. Click the BGP term (here, T4-BGP) under Terms. The Edit Redistribution Policy > Edit Term popup window displays.



Edit Redistribution Policy Edit Term

Term Name* T4-BGP

Match | Action

Accept/Reject: Accept

Set

Well Known Community: --Select--

Community:

Extended Community:

Local Preference: 90

MED:

Origin: Remote IGP

OSPF Tag:

□ OSPF Metric to BGP MED

□ OSPF Metric to BGP Local Preference

Metric:

Metric Conversion: --Select--

OSPF External Type: --Select--

Route Preference:

Standby

Metric:

Metric Conversion: --Select--

Local Preference:

VRRP

Standby Local Preference:

Standby Metric:

8. Select the Action tab, and in the Local Preference field, enter 90.
9. For information about other fields, see Configure Redistribution Policies.
10. Click OK. This forces other SD-WAN sites to forward their traffic to the primary Versa VNF, at 10.1.64.124.

To verify that traffic is being routed based on the preference values:

```
admin@versa-cli> show route routing-instance lan-vr-name
Routes for Routing instance : Customer1-LAN-VR  AFI: ipv4 SAFI: unicast
Codes: E1 - OSPF external type 1, E2 - OSPF external type 2
IA - inter area, iA - intra area,
L1 - IS-IS level-1, L2 - IS-IS level-2
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
+ - Active Route
Prot   Type   Dest Address/Mask   Next Hop       Age       Interface Name
```

```
----   ----   -----------------   --------      ---      --------------
BGP    N/A    +0.0.0.0/0          10.1.64.124   02:28:26  Indirect
BGP    N/A    +0.0.0.0/0          10.1.64.125   00:00:29  Indirect
BGP    N/A     172.16.26.0/24     10.1.64.124   03:14:24  Indirect
BGP    N/A    +172.16.26.0/24     10.1.64.125   00:00:29  Indirect
BGP    N/A    +172.16.26.96/27    10.1.64.124   2w6d20h   Indirect
BGP    N/A    +172.16.26.96/27    10.1.64.125   03:14:24  Indirect
BGP    N/A     172.16.27.0/24     10.1.64.124   03:14:24  Indirect
BGP    N/A    +172.16.27.0/24     10.1.64.125   00:00:29  Indirect
BGP    N/A     172.16.28.0/24     10.1.64.124   03:14:24  Indirect
BGP    N/A    +172.16.28.0/24     10.1.64.125   00:00:29  Indirect
BGP    N/A     172.16.29.0/24     10.1.64.124   03:14:24  Indirect
BGP    N/A    +172.16.29.0/24     10.1.64.125   00:00:29  Indirect
```

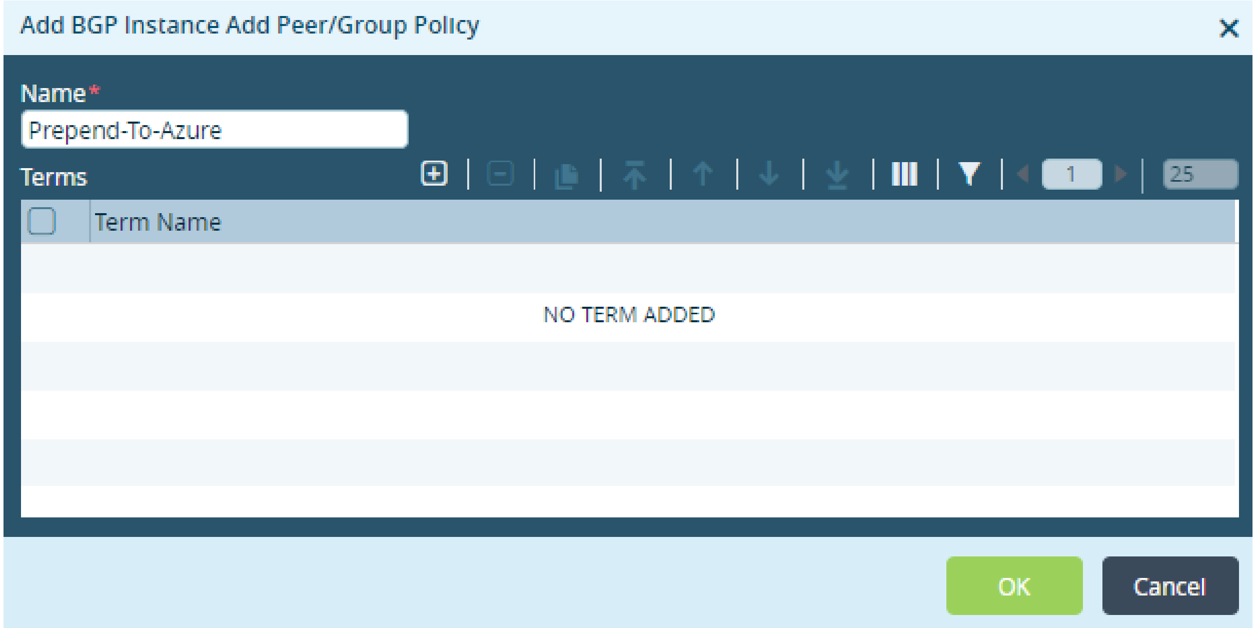
## Configure Symmetrical Traffic

You must ensure that traffic forwarded from hosts in the spoke VNETs is forwarded to the same Versa VNF, to keep traffic symmetrical. To do this, you prepend AS numbers on the standby Versa VNF when it advertises routes to the Azure BGP endpoint.

To configure the AS prepending, you create a peer and peer group policy in the BGP instance in the LAN VR, and then you prepend the local AS number twice in AS path.

To configure the peer and peer group policy:

1. In the Configure Virtual Router > BGP popup window, select the Peer/Group Policy tab. Click the ⊞ Add icon. The Add BGP Instance Peer/Group Policy popup window displays.



Add BGP Instance Add Peer/Group Policy

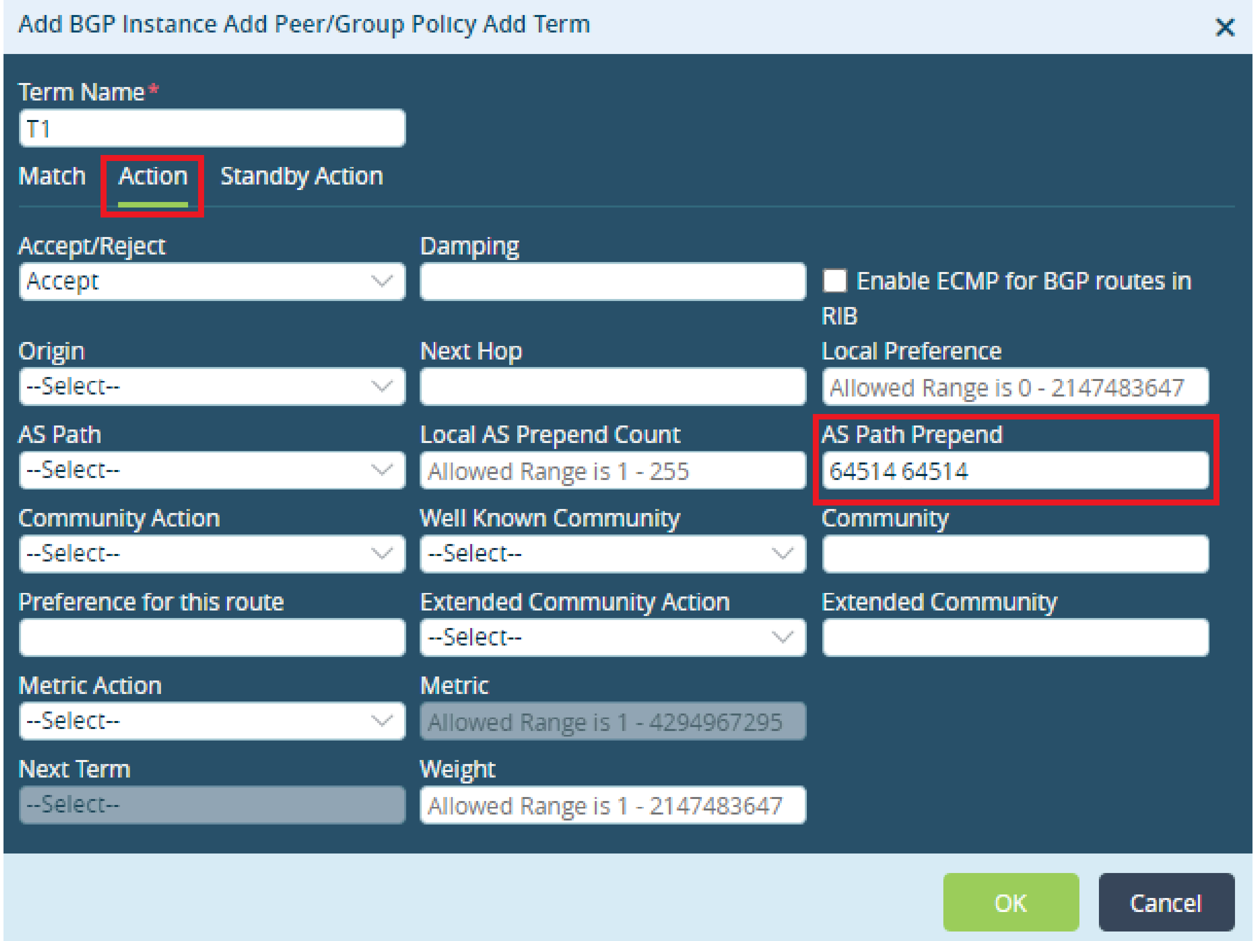
Name*
Prepend-To-Azure

Terms

| □ | Term Name |
|---|---|
| | NO TERM ADDED |

2. Enter a name for the peer group policy (here, Prepend-To-Azure).

3. Click the ⊞ Add icon to add a term. The Add BGP Instance Add Peer/Group Policy Add Term popup window displays.



Add BGP Instance Add Peer/Group Policy Add Term

Term Name* T1

Match | Action | Standby Action

Accept/Reject: Accept

Damping:

□ Enable ECMP for BGP routes in RIB

Origin: --Select--

Next Hop:

Local Preference: Allowed Range is 0 - 2147483647

AS Path: --Select--

Local AS Prepend Count: Allowed Range is 1 - 255

AS Path Prepend: 64514 64514

Community Action: --Select--

Well Known Community: --Select--

Community:

Preference for this route:

Extended Community Action: --Select--

Extended Community:

Metric Action: --Select--

Metric: Allowed Range is 1 - 4294967295

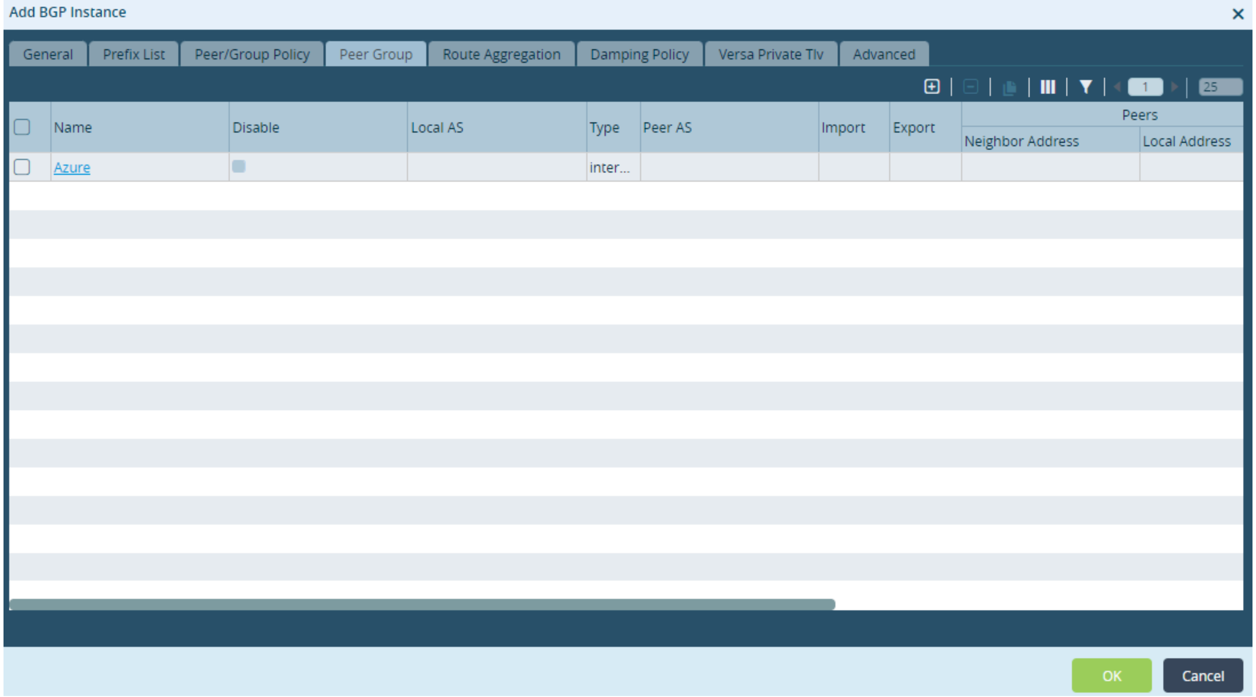
Next Term: --Select--

Weight: Allowed Range is 1 - 2147483647

4. Enter a name for the term (here, T1).
5. Select the Action tab, and in the AS Path Prepend field, enter the AS number twice (here, 64514 64514).
6. Click OK.

Then, add the peer and peer group policy to the neighbors configuration for the Azure endpoint as an export policy:

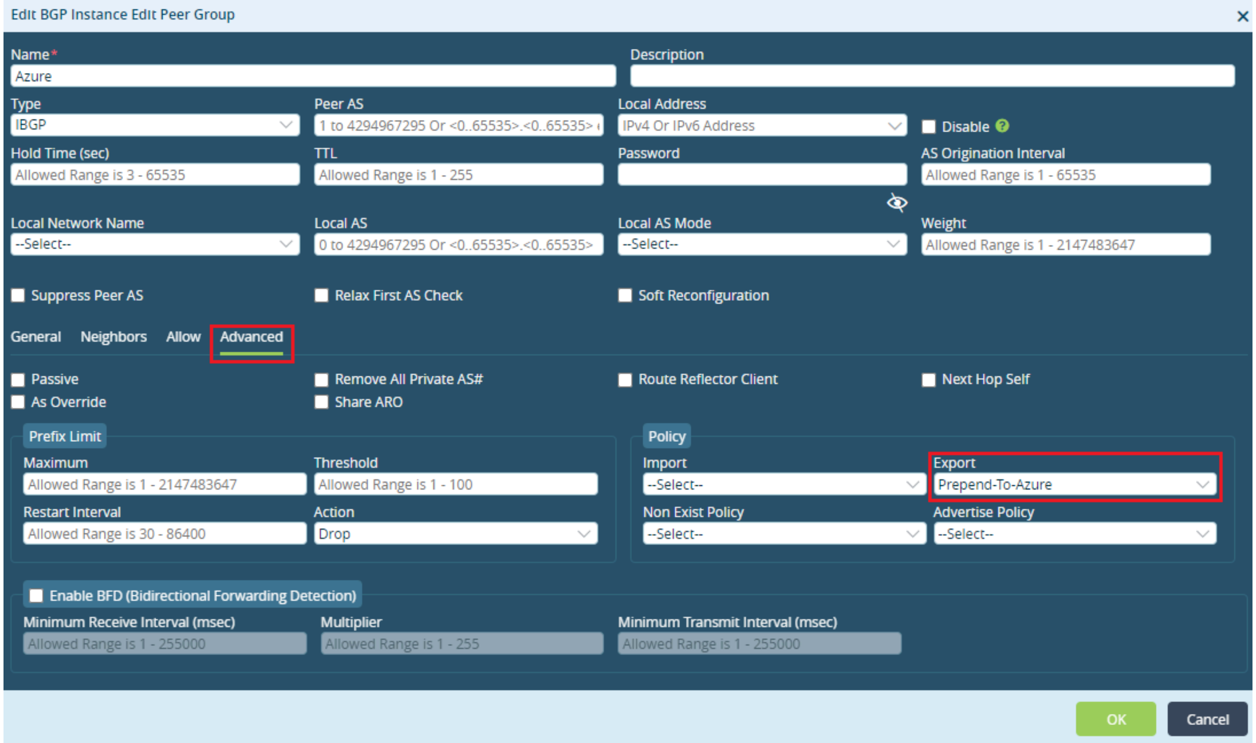
1. In the Add BGP Instance window, select the Peer Group tab.



Add BGP Instance

| ☐ | Name | Disable | Local AS | Type | Peer AS | Import | Export | Peers | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | Neighbor Address | Local Address |
| ☐ | Azure | ■ | | inter... | | | | | |

2. Select the peer group to which to add the peer and peer group policy, or click the ⊞ Add icon to add a peer group. In this example, the peer and peer group policy are added to an existing peer group, Azure. The Edit BGP Instance Edit Peer Group popup window displays.



Edit BGP Instance Edit Peer Group

- Name*: Azure
- Description:
- Type: IBGP
- Peer AS: 1 to 4294967295 Or <0..65535>.<0..65535>
- Local Address: IPv4 Or IPv6 Address
- ☐ Disable
- Hold Time (sec): Allowed Range is 3 - 65535
- TTL: Allowed Range is 1 - 255
- Password:
- AS Origination Interval: Allowed Range is 1 - 65535
- Local Network Name: --Select--
- Local AS: 0 to 4294967295 Or <0..65535>.<0..65535>
- Local AS Mode: --Select--
- Weight: Allowed Range is 1 - 2147483647
- ☐ Suppress Peer AS
- ☐ Relax First AS Check
- ☐ Soft Reconfiguration

- ☐ Passive
- ☐ As Override
- ☐ Remove All Private AS#
- ☐ Share ARO
- ☐ Route Reflector Client
- ☐ Next Hop Self

Prefix Limit

- Maximum: Allowed Range is 1 - 2147483647
- Threshold: Allowed Range is 1 - 100
- Restart Interval: Allowed Range is 30 - 86400
- Action: Drop

Policy

- Import: --Select--
- Export: Prepend-To-Azure
- Non Exist Policy: --Select--
- Advertise Policy: --Select--

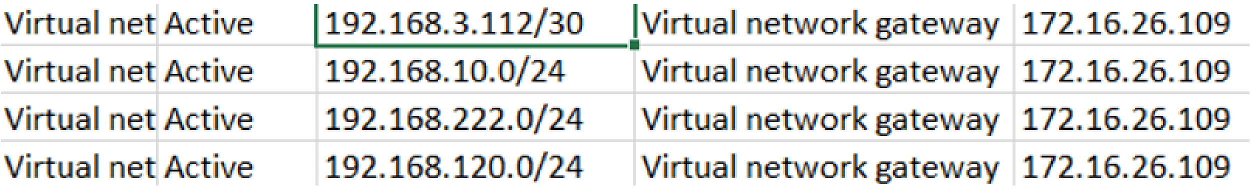
☐ Enable BFD (Bidirectional Forwarding Detection)

- Minimum Receive Interval (msec): Allowed Range is 1 - 255000
- Multiplier: Allowed Range is 1 - 255
- Minimum Transmit Interval (msec): Allowed Range is 1 - 255000

3. Select the Advanced tab.

4. In the Policy group of fields, in the Export field, select the peer and peer group policy you created above (here, Prepend-To-Azure).
5. Click OK.

This configuration forces hosts in the Azure spoke VNETs to forward traffic to the primary Versa VNF. In the following example, this behavior is displayed in the effective routes taken from a spoke VNETs VM route table (here, 172.16.26.109 is the LAN interface of the primary VNF):



| | | | | |
|---|---|---|---|---|
| Virtual net | Active | 192.168.3.112/30 | Virtual network gateway | 172.16.26.109 |
| Virtual net | Active | 192.168.10.0/24 | Virtual network gateway | 172.16.26.109 |
| Virtual net | Active | 192.168.222.0/24 | Virtual network gateway | 172.16.26.109 |
| Virtual net | Active | 192.168.120.0/24 | Virtual network gateway | 172.16.26.109 |

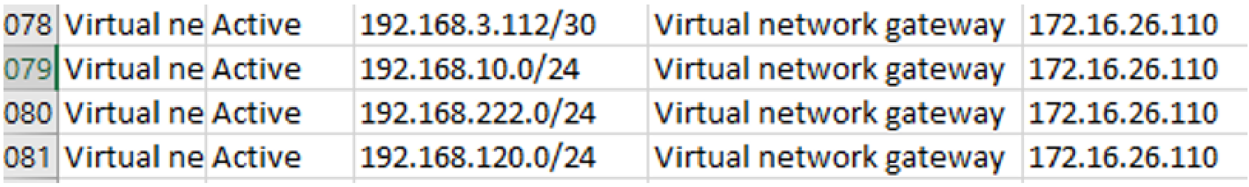
With this configuration, the spoke Versa VNFs and remote SD-WAN sites forward traffic to the primary Versa VNF in asymmetrical manner. If the primary Versa VNF goes down, the route tables switch to the secondary Versa VNF.

To verify the behavior from an SD-WAN branch:

```
admin@versa-cli> show route routing-instance lan-vr-name
Codes: El· OSPF external type 1, E2 · OSPF external type 2
IA - inter area, iA - intra area,
LI - IS-IS level-1, L2 - IS-IS level-2
NI - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
RTI - Learnt from another routing-instance
+ - Active Route

Prot   Type   Dest Address/Mask   Next hop    Age      Interface name
----   ----   -----------------   -------     ---      --------------
BGP    N/A    +0.0.0.0/0          10.1.64.125   00:08:56  Indirect
BGP    N/A    +172.16.26.0/24     10.1.64.125   00:08:52  Indirect
BGP    N/A    +172.16.26.96/27    10.1.64.125   03:35:05  Indirect
BGP    N/A    +172.16.27.0/24     10.1.64.125   00:08:52  Indirect
BGP    N/A    +172.16.28.0/24     10.1.64.125   00:08:52  Indirect
BGP    N/A    +172.16.29.0/24     10.1.64.125   00:08:52  Indirect
```

The following is an example of the Azure spoke VNET VM route table:



| | | | | | |
|---|---|---|---|---|---|
| 078 | Virtual ne | Active | 192.168.3.112/30 | Virtual network gateway | 172.16.26.110 |
| 079 | Virtual ne | Active | 192.168.10.0/24 | Virtual network gateway | 172.16.26.110 |
| 080 | Virtual ne | Active | 192.168.222.0/24 | Virtual network gateway | 172.16.26.110 |
| 081 | Virtual ne | Active | 192.168.120.0/24 | Virtual network gateway | 172.16.26.110 |

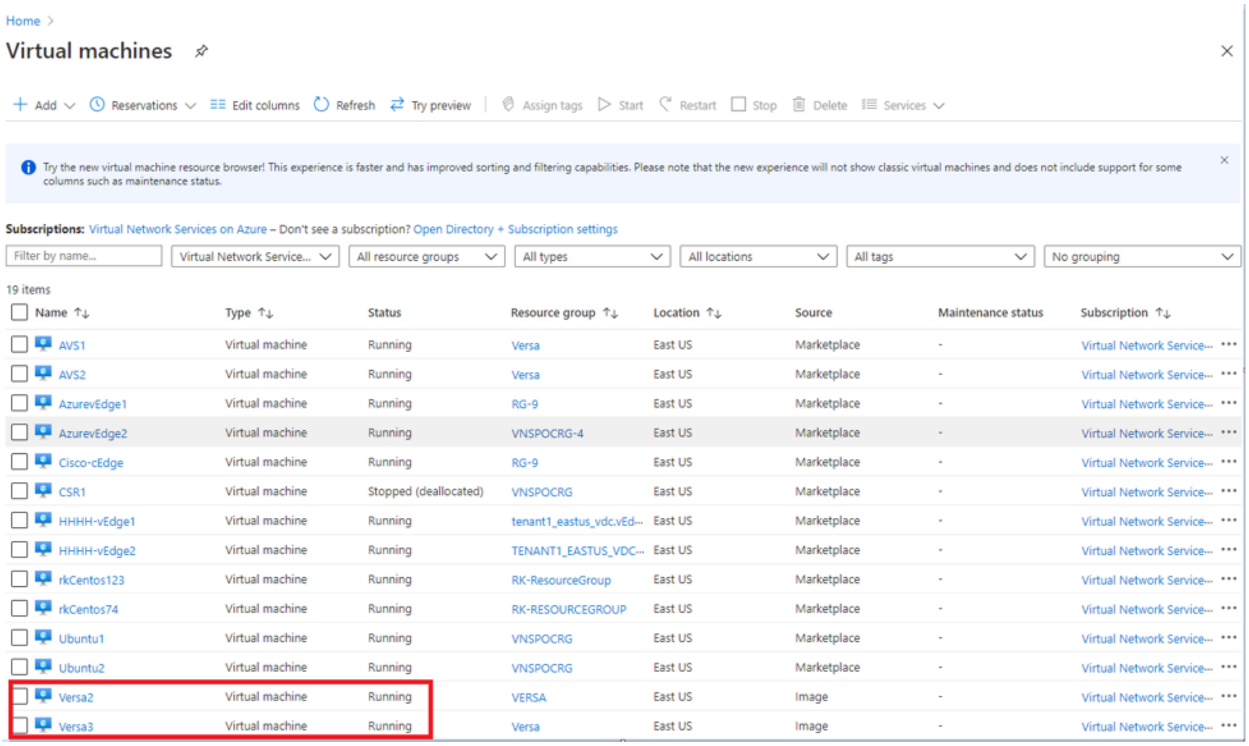
# Verify VOS Deployment on Azure

The section provides information about how to verify a VOS deployment on an Azure public cloud infrastructure.

## Verify Azure Components

You can verify the status of all Azure components from the Azure portal or using Microsoft PowerShell.

To verify the status of a Versa VNF instance from Azure, select Virtual Machines on the Home page:



Try the new virtual machine resource browser! This experience is faster and has improved sorting and filtering capabilities. Please note that the new experience will not show classic virtual machines and does not include support for some columns such as maintenance status.

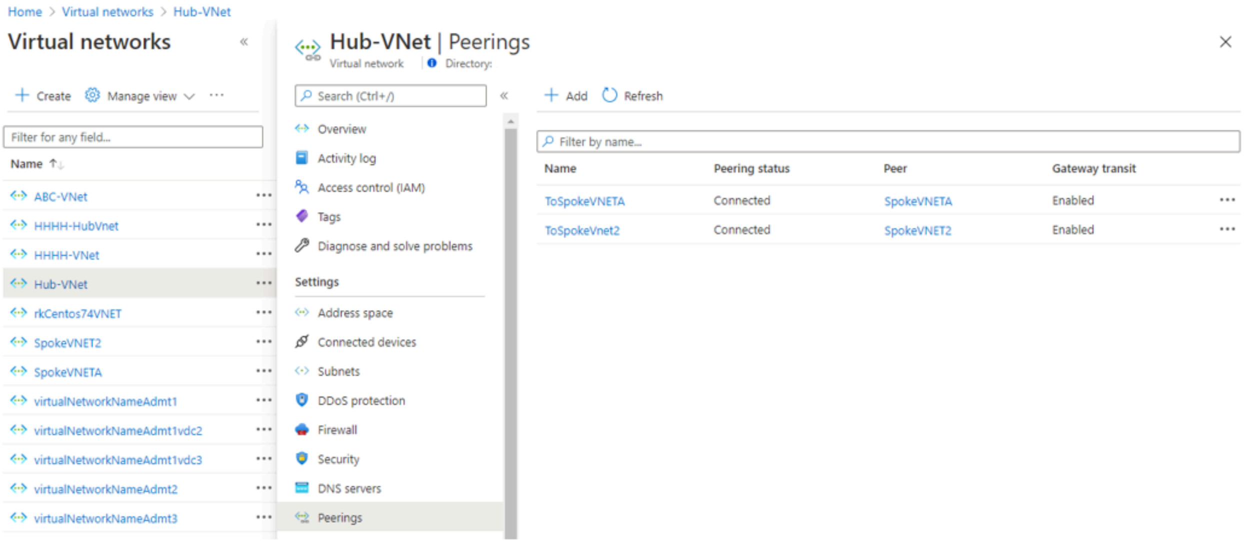
**Subscriptions:** Virtual Network Services on Azure – Don't see a subscription? Open Directory + Subscription settings

Filter by name... | Virtual Network Service... | All resource groups | All types | All locations | All tags | No grouping

19 items

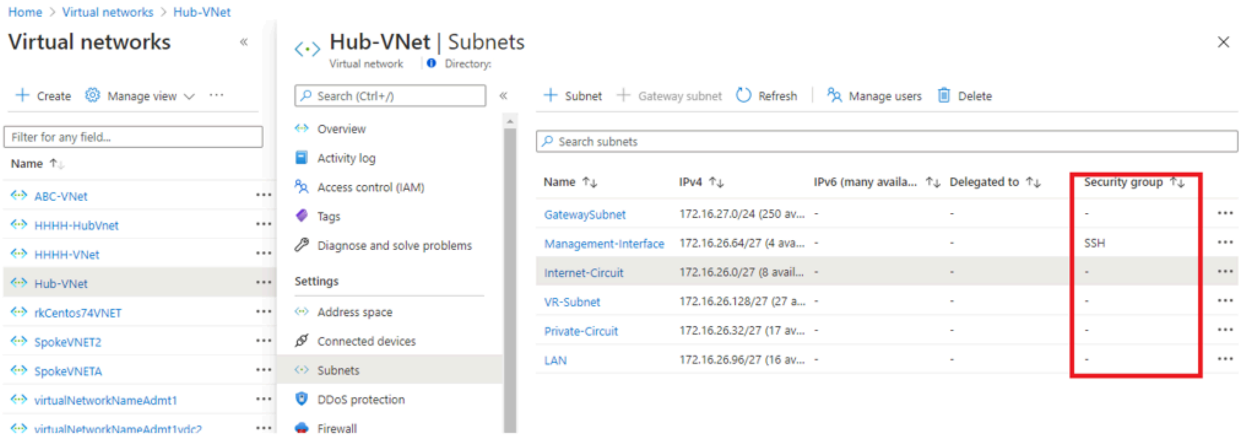
| Name | Type | Status | Resource group | Location | Source | Maintenance status | Subscription |
|---|---|---|---|---|---|---|---|
| AVS1 | Virtual machine | Running | Versa | East US | Marketplace | - | Virtual Network Service... |
| AVS2 | Virtual machine | Running | Versa | East US | Marketplace | - | Virtual Network Service... |
| AzurevEdge1 | Virtual machine | Running | RG-9 | East US | Marketplace | - | Virtual Network Service... |
| AzurevEdge2 | Virtual machine | Running | VNSPOCRG-4 | East US | Marketplace | - | Virtual Network Service... |
| Cisco-cEdge | Virtual machine | Running | RG-9 | East US | Marketplace | - | Virtual Network Service... |
| CSR1 | Virtual machine | Stopped (deallocated) | VNSPOCRG | East US | Marketplace | - | Virtual Network Service... |
| HHHH-vEdge1 | Virtual machine | Running | tenant1_eastus_vdc.vEd... | East US | Marketplace | - | Virtual Network Service... |
| HHHH-vEdge2 | Virtual machine | Running | TENANT1_EASTUS_VDC... | East US | Marketplace | - | Virtual Network Service... |
| rkCentos123 | Virtual machine | Running | RK-ResourceGroup | East US | Marketplace | - | Virtual Network Service... |
| rkCentos74 | Virtual machine | Running | RK-RESOURCEGROUP | East US | Marketplace | - | Virtual Network Service... |
| Ubuntu1 | Virtual machine | Running | VNSPOCRG | East US | Marketplace | - | Virtual Network Service... |
| Ubuntu2 | Virtual machine | Running | VNSPOCRG | East US | Marketplace | - | Virtual Network Service... |
| Versa2 | Virtual machine | Running | VERSA | East US | Image | - | Virtual Network Service... |
| Versa3 | Virtual machine | Running | Versa | East US | Image | - | Virtual Network Service... |

To confirm the status of peering between the hub VNET where the Versa VNFs exist and the spoke VNETs where the customer applications exist, navigate from the Azure Home page to the hub VNET and then check the Peerings section:



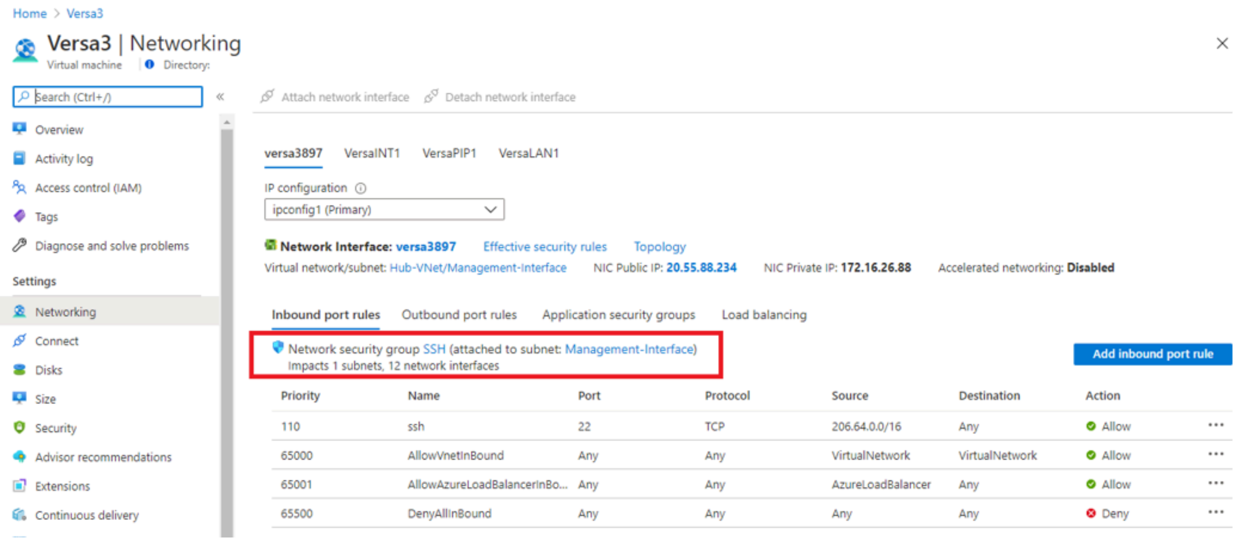
| Name | Peering status | Peer | Gateway transit |
|---|---|---|---|
| ToSpokeVNETA | Connected | SpokeVNETA | Enabled |
| ToSpokeVnet2 | Connected | SpokeVNET2 | Enabled |

An NSG may be applied to an entire subnet, to the interface of an instance, or both. To verify where an NSG is applied, check the Subnets section in the Hub VNET.



| Name | IPv4 | IPv6 (many availa... | Delegated to | Security group |
|---|---|---|---|---|
| GatewaySubnet | 172.16.27.0/24 (250 av... | - | - | - |
| Management-Interface | 172.16.26.64/27 (4 ava... | - | - | SSH |
| Internet-Circuit | 172.16.26.0/27 (8 avail... | - | - | - |
| VR-Subnet | 172.16.26.128/27 (27 a... | - | - | - |
| Private-Circuit | 172.16.26.32/27 (17 av... | - | - | - |
| LAN | 172.16.26.96/27 (16 av... | - | - | - |

You can also check the interface of VM for NSGs:



Home > Versa3

**Versa3 | Networking**

Virtual machine | Directory:

IP configuration: ipconfig1 (Primary)

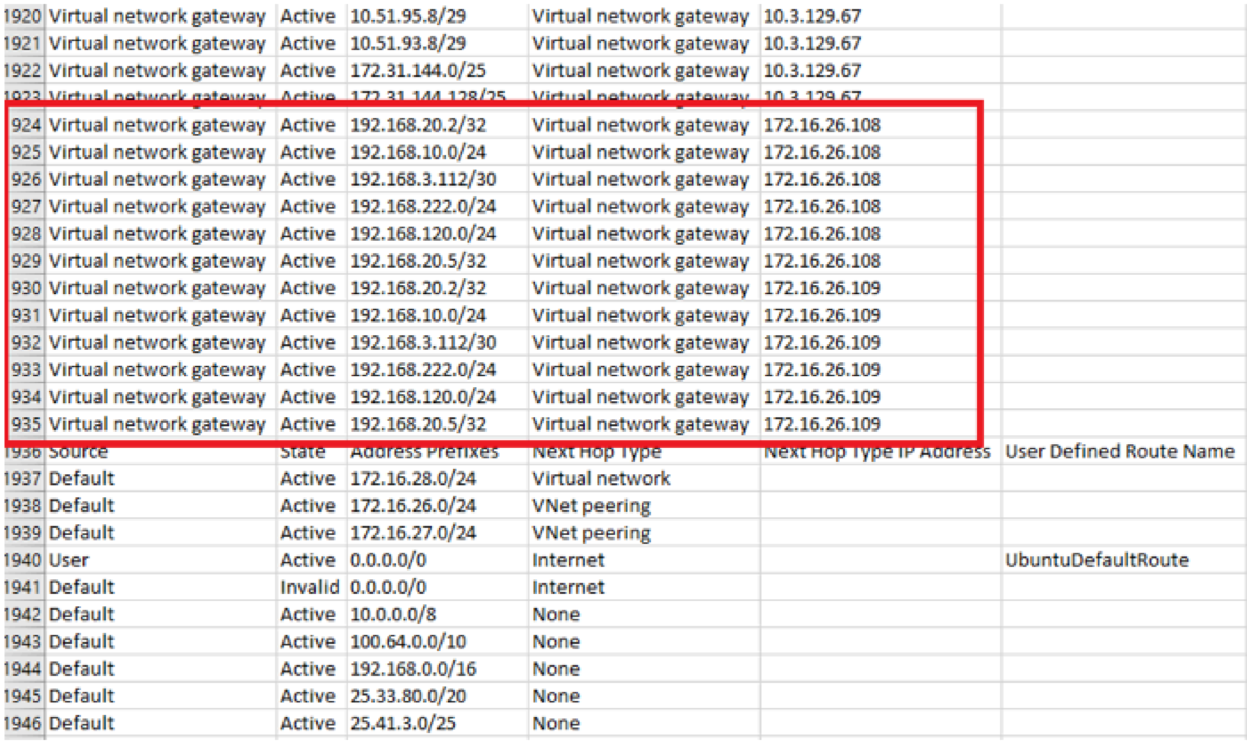
**Network Interface:** versa3897

Virtual network/subnet: Hub-VNet/Management-Interface  NIC Public IP: **20.55.88.234**  NIC Private IP: **172.16.26.88**  Accelerated networking: **Disabled**

Network security group SSH (attached to subnet: Management-Interface)
Impacts 1 subnets, 12 network interfaces

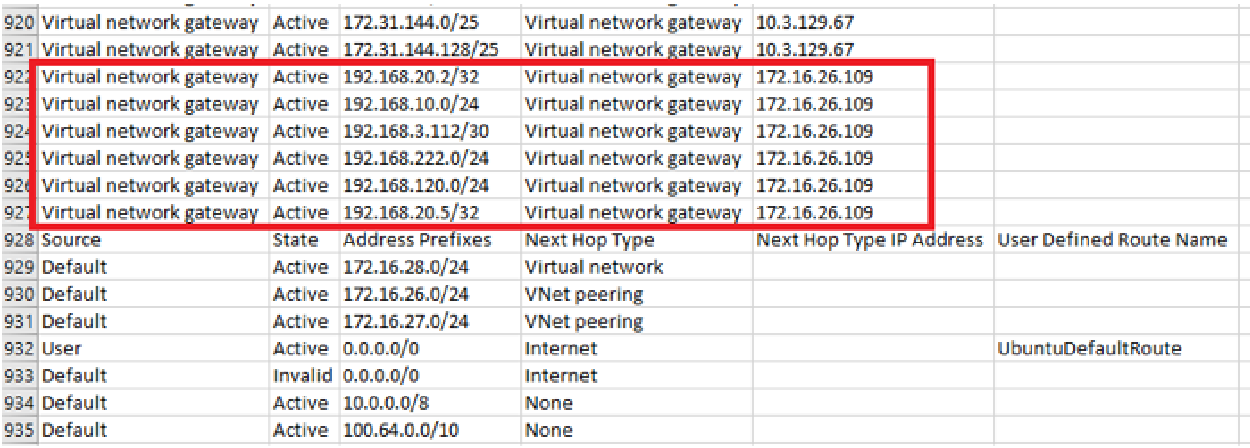
| Priority | Name | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|---|
| 110 | ssh | 22 | TCP | 206.64.0.0/16 | Any | Allow |
| 65000 | AllowVnetInBound | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | AllowAzureLoadBalancerInBo... | Any | Any | AzureLoadBalancer | Any | Allow |
| 65500 | DenyAllInBound | Any | Any | Any | Any | Deny |

In the following example, you can see a network from a remote branch attached to the SD-WAN fabric. Both Versa VNFs in Azure are advertising them to the BGP endpoint in Azure and those routes are propagating to the route tables attached to instance interfaces in the spoke VNETs. 172.16.26.109 and 172.16.26.108 are the LAN interface IP addresses for Versa VNFs:



| | | | | | | |
|---|---|---|---|---|---|---|
| 1920 | Virtual network gateway | Active | 10.51.95.8/29 | Virtual network gateway | 10.3.129.67 | |
| 1921 | Virtual network gateway | Active | 10.51.93.8/29 | Virtual network gateway | 10.3.129.67 | |
| 1922 | Virtual network gateway | Active | 172.31.144.0/25 | Virtual network gateway | 10.3.129.67 | |
| 1923 | Virtual network gateway | Active | 172.31.144.128/25 | Virtual network gateway | 10.3.129.67 | |
| 924 | Virtual network gateway | Active | 192.168.20.2/32 | Virtual network gateway | 172.16.26.108 | |
| 925 | Virtual network gateway | Active | 192.168.10.0/24 | Virtual network gateway | 172.16.26.108 | |
| 926 | Virtual network gateway | Active | 192.168.3.112/30 | Virtual network gateway | 172.16.26.108 | |
| 927 | Virtual network gateway | Active | 192.168.222.0/24 | Virtual network gateway | 172.16.26.108 | |
| 928 | Virtual network gateway | Active | 192.168.120.0/24 | Virtual network gateway | 172.16.26.108 | |
| 929 | Virtual network gateway | Active | 192.168.20.5/32 | Virtual network gateway | 172.16.26.108 | |
| 930 | Virtual network gateway | Active | 192.168.20.2/32 | Virtual network gateway | 172.16.26.109 | |
| 931 | Virtual network gateway | Active | 192.168.10.0/24 | Virtual network gateway | 172.16.26.109 | |
| 932 | Virtual network gateway | Active | 192.168.3.112/30 | Virtual network gateway | 172.16.26.109 | |
| 933 | Virtual network gateway | Active | 192.168.222.0/24 | Virtual network gateway | 172.16.26.109 | |
| 934 | Virtual network gateway | Active | 192.168.120.0/24 | Virtual network gateway | 172.16.26.109 | |
| 935 | Virtual network gateway | Active | 192.168.20.5/32 | Virtual network gateway | 172.16.26.109 | |
| 1936 | Source | State | Address Prefixes | Next Hop Type | Next Hop Type IP Address | User Defined Route Name |
| 1937 | Default | Active | 172.16.28.0/24 | Virtual network | | |
| 1938 | Default | Active | 172.16.26.0/24 | VNet peering | | |
| 1939 | Default | Active | 172.16.27.0/24 | VNet peering | | |
| 1940 | User | Active | 0.0.0.0/0 | Internet | | UbuntuDefaultRoute |
| 1941 | Default | Invalid | 0.0.0.0/0 | Internet | | |
| 1942 | Default | Active | 10.0.0.0/8 | None | | |
| 1943 | Default | Active | 100.64.0.0/10 | None | | |
| 1944 | Default | Active | 192.168.0.0/16 | None | | |
| 1945 | Default | Active | 25.33.80.0/20 | None | | |
| 1946 | Default | Active | 25.41.3.0/25 | None | | |

Routes from both Versa VNFs are displayed because AS prepending is not configured and so the route table uses both VNFs. However, when AS prepending is configured on one of the Versa VNFs, traffic from the spoke VNETs is routed to a specific Versa VNF, as shown in the following output from the effective routes:



| | | | | | | |
|---|---|---|---|---|---|---|
| 920 | Virtual network gateway | Active | 172.31.144.0/25 | Virtual network gateway | 10.3.129.67 | |
| 921 | Virtual network gateway | Active | 172.31.144.128/25 | Virtual network gateway | 10.3.129.67 | |
| 922 | Virtual network gateway | Active | 192.168.20.2/32 | Virtual network gateway | 172.16.26.109 | |
| 923 | Virtual network gateway | Active | 192.168.10.0/24 | Virtual network gateway | 172.16.26.109 | |
| 924 | Virtual network gateway | Active | 192.168.3.112/30 | Virtual network gateway | 172.16.26.109 | |
| 925 | Virtual network gateway | Active | 192.168.222.0/24 | Virtual network gateway | 172.16.26.109 | |
| 926 | Virtual network gateway | Active | 192.168.120.0/24 | Virtual network gateway | 172.16.26.109 | |
| 927 | Virtual network gateway | Active | 192.168.20.5/32 | Virtual network gateway | 172.16.26.109 | |
| 928 | Source | State | Address Prefixes | Next Hop Type | Next Hop Type IP Address | User Defined Route Name |
| 929 | Default | Active | 172.16.28.0/24 | Virtual network | | |
| 930 | Default | Active | 172.16.26.0/24 | VNet peering | | |
| 931 | Default | Active | 172.16.27.0/24 | VNet peering | | |
| 932 | User | Active | 0.0.0.0/0 | Internet | | UbuntuDefaultRoute |
| 933 | Default | Invalid | 0.0.0.0/0 | Internet | | |
| 934 | Default | Active | 10.0.0.0/8 | None | | |
| 935 | Default | Active | 100.64.0.0/10 | None | | |

You can also verify the status of the BGP endpoint and its peers by running the **Get-AzVirtualRouter –RouterName** *router-name* **–ResourceGroupName –***resource-group-name* CLI command from PowerShell. For example:

```
PS C:\Users\user-name> Get-AzVirtuaRouter VersaVR -ResourceGroupName: VNSPOCRG
Name                :VersaVR
ResourceGroupName   : VNSPOCRG
Location            : eastus
Id                  : /subscriptions/310a5c8e-3b71-4ad2-bcaf-8f829fbee7c5/resourceGroups/VNSPOCRG/providers/
Microsoft.Network/virtualHubs/VersaVR
Etag                :
Type                : Microsoft.Network/virtualHubs
ProvisioningState   : Succeeded
HostedSubnet        : /subscriptions/310a5c8e-3b71-4ad2-bcaf-8f829fbee7c5/resourceGroups/VNSPOCRG/
providers/Microsoft.Network/virtualNetworks/Hub-VNet/subnets/VR-Subnet
VirtualRouterAsn    : 65515
VirtualRouterIps    : {172.16.26.132, 172.16.26.133}
Peerings : [
           {
             "PeerAsn": 65520,
             "PeerIp": "172.16.26.109",
             "ProvisioningState": "Succeeded",
             "Name": "Versa2"
           },
           {
            "PeerAsn": 65520,
            "PeerIp": "172.16.26.108",
            "ProvisioningState": "Succeeded",
            "Name": "Versa3"
          }
          ]
```

## Verify Versa Components

To verify the BGP connection to the Azure BGP endpoint, run the **show bgp neighbor brief** CLI command. For example:

```
admin@Azure-cli> show bgp neighbor brief
routing instance: Customer-Control-VR

Neighbor       V  MsgRcvd  MsgSent   Uptime     State/PfxRcd  PfxSent    AS
l8.t.64.1      4  10304    99S4      2d23h50m   79            12         64512
l0.1.64.2      4  0        8         n/a        connect       0          64512

routing-instance: Customer1-LAN-VR

Neighbor        V  MsgRcvd  MsgSent   Uptime     State/PfxRcd  PfxSent    AS
172.16.26.132   4  454      480       03:13:52   4             12         65515
169.254.0.2     4  456      453       03:16:55   1             15         64513

routing-instance: Customer1-LAN-VR

Neighbor       V  MsgRcvd  MsgSent   Uptime     State/PfxRcd  PfxSent    AS
l69.254.0.3    4  9933     9922      03:16:50   15            1          64514
```

To view details about what is advertised to the BGP endpoint as well as the AS prepending that may be present, run the **show route table ipv4.unicast routing-instance** *routing-instance-name* **advertise-protocol bgp neighbor-address** *neighbor-ip-address*. In the example below, the local-AS is prepended twice (highlighted) to the beginning of the AS path that was added when it was advertising to the Azure BGP endpoint:

```
admin@Azure-c1i> show route table ipv4.unicast routing-instance Customer1-LAN-VR advertising-
protocol bgp neighbor-address 172.16.26.132
Routes for Routing instance : Customerl.LAN-VR AFI: ipv4 SAFI: unicast
Prefix/Mask         Next-hop          MED   Lclpref   AS path
0.0.0.0/0           172.16.26.108     0     0         65520 64514 65520 65520 64513
172.16.26.96/27     172.16.26.108     0     0         65520 64514 65520 65520
192.168.3.112/30    172.16.26.108     0     0         65520 64514 65520 65520
192.168.3.144/32    172.16.26.108     0     0         65520 64514 65520 65520
192.168.3.145/32    172.16.26.108     0     0         65520 64514 65520 65520
192.168.10.0/24     172.16.26.108     0     0         65520 64514 65520 65520
192.168.20.0/24     172.16.26.108     0     0         65520 64514 65520 65520
192.168.20.2/32     172.16.26.108     0     0         65520 64514 65520 65520
192.168.20.5/32     172.16.26.108     0     0         65520 64514 65520 65520
192.168.120.0/24    172.16.26.108     0     0         65520 64514 65520 65520
192.168.222.0/24    172.16.26.108     0     0         65520 64514 65520 65520
206.64.200.120/29   172.16.26.108     100   0         65520 64514 65520 65520 6073 701 13666
```

To view more details about what is advertised via BGP to the SD-WAN fabric, run the **show route table l3vpn.ipv4.unicast routing-instance** *routing-instance-name* **advertising-protocol bgp** CLI command. The following example shows the local preference that is advertised from the VNF for the redistributed default (for internet breakout) and spoke VNET routes:

```
admin@Azure-c1i> show route table l3vpn.ipv4.unicast routing-instance Customer1-Control-VR
advertising-protocol bgp

Routes for Routing instance : Customer1-Control-VR  AFI: ipv4  SAFI: unicast

Routing entry for   0.0.0.0/0
  Peer Address       : 10.1.64.1
  Route Distinguisher: 2L:3
  Next-hop          : 10.1.64.117
  VPN Label         : 24705
  local Preference   : 110
  AS Path           : 64513
  Origin            : Egp
  MED               : 0
  Community         : [ N/A ]
  Extended community : [ target:2L:2 ]


Routing entry for   172.16.26.0/24
  Peer Address      : 10.1.64.1
  Route Distinguisher: 2L:3
  Next-hop          : 10.1.64.117
  VPN Label         : 24705
  local Preference   : 110
  AS Path           : 65520 65515
  Origin            : Egp
  MED               : 0
  Community         : [ N/A ]
  Extended community : [ target:2L:2 ]
```

For a remote branch on the other side of the SD-WAN fabric, the route table looks as if neither Versa VNF in Azure has the BGP local preference adjusted. For example (10.1.64.117 and 10.1.64.124 are the Azure VNFs):

```
admin@Azure-c1i> show route routing-instance Customer1-LAN-VR

Routes for Routing instance : Customer1-LAN-VR AFI: ipv4 SAFI: unicast

Codes: El - OSPF external type 1, E2 - OSPF external type 2
IA - inter area, iA - intra area,
L1 - IS-IS level-1,    L2 - IS-IS level-2
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
RTI - Learnt from another routing-instance
+ - Active Route

Prot    Type    Dest Address/Mask   Next Hop       Age       Interface name
----    ----    -----------------   --------       ---       --------------
BGP     N/A    +0.0.0.0/0          10.1.64.117    05:47:22   Indirect
BGP     N/A    +0.0.0.0/0          10.1.64.124    06:01:43   Indirect
conn    N/A    +169.254.7.234/31    0.0.0.0        4w5d04h    tvi-0/2626.0
local   N/A    +169.254.7.234/32    0.0.0.0        4w5d04h    directly connected
BGP     N/A    +172.16.26.0/24      10.1.64.117    05:47:23   Indirect
BGP     N/A    +172.16.26.0/24      10.1.64.124    06:01:43   Indirect
BGP     N/A    +172.16.26.96/27     10.1.64.117    06:02:13   Indirect
BGP     N/A    +172.16.26.96/27     10.1.64.124    3d02h20m   Indirect
BGP     N/A    +172.16.27.0/24      10.1.64.117    05:47:23   Indirect
BGP     N/A    +172.16.27.0/24      10.1.64.124    06:01:43   Indirect
BGP     N/A    +172.16.28.0/24      10.1.64.117    05:47:23   Indirect
BGP     N/A    +172.16.28.0/24      10.1.64.124    06:01:43   Indirect
BGP     N/A    +172.16.29.0/24      10.1.64.117    05:47:23   Indirect
BGP     N/A    +172.16.29.0/24      10.1.64.124    06:01:43   Indirect
```

If the local preference on the VNF in Azure is configured to act as the standby router, the CLI output is similar to the following example (here, the local preference of 10.1.64.117 is lower that what 10.1.64.124 is advertising):

```
admin@Azure-c1i> show route routing-instance Customer1-LAN-VR
Routes for Routing instance : Customer1-LAN-VR    AFI: ipv4    SAFI: unicast
Codes: El - OSPF external type 1, E2 - OSPF external type 2
IA - inter area, iA - intra area,
LI - IS-IS level-1,    L2 - IS-IS level-2
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
RTI - Learnt from another routing-instance
+ - Active Route

Prot    Type    Dest Address/Mask    Next Hop        Age        Interface name
---     ----    -----------------    --------        ---        --------------
BGP     N/A    0.0.0.0/0            10.1.64.117     00:00:13   Indirect
BGP     N/A    +6.0.0.0/0           10.1.64.124     06:08:16   Indirect
conn    N/A    +169.254.7.234/31     0.0.0.0         4w5d04h    tvi-0/2626.0
local   N/A    +169.254.7.234/32     0.0.0.0         4w5d04h    directly connected
BGP     N/A    172.16.26.0/24       10.1.64.117     00:00:13   Indirect
BGP     N/A    +172.16.26.0/24      10.1.64.124     06:08:16   Indirect
BGP     N/A    +172.16.26.96/27     10.1.64.117     00:01:02   Indirect
BGP     N/A    +172.16.26.96/27     10.1.64.124     3d02h27m   Indirect
BGP     N/A    172.16.27.0/24       10.1.64.117     00:00:13   Indirect
BGP     N/A    +172.16.27.0/24      10.1.64.124     06:08:16   Indirect
BGP     N/A    172.16.28.0/24       10.1.64.117     00:00:13   Indirect
BGP     N/A    +172.16.28.0/24      10.1.64.124     06:08:16   Indirect
BGP     N/A    172.16.29.0/24       10.1.64.117     00:00:13   Indirect
BGP     N/A    +172.16.29.0/24      10.1.64.124     06:08:16   Indirect
BGP     N/A    +192.168.3.112/30     10.1.64.1       3w3d03h    Indirect
BGP     N/A    +192.168.3.144/32     10.1.64.124     3d02h27m   Indirect
BGP     N/A    +192.168.3.145/32     10.1.64.117     00:01:02   Indirect
conn    N/A    +192.168.10.0/24      0.0.0.0         4w5dOlh    vni-0/6.136
local   N/A    +192.168.10.5/32      0.0.0.0         4w5dOlh    directly connected
```

Additionally, to view the adjusted local preference in the Layer 3 VPN route table on the receiving router, run the **show route table l3vpn.ipv4.unicast routing-instance** *routing-instance-name* **receive-protocol bgp** CLI command (here, local preference is changed default to 90). For example:

```
admin@Azure-c1i> show route table l3vpn.ipv4.unicast routing-instance Customer1-Control-VR
advertising-protocol bgp

Routes for Routing instance : Customer1-Control-VR  AFI: ipv4  SAFI: unicast

Routing entry for   0.0.0.0/0
   Peer Address       : 10.1.64.1
   Route Distinguisher: 2L:9
   Next-hop           : 10.1.64.117
   VPN Label          : 24706
   local Preference   : 90
   AS Path            : 64513
   Origin             : Egp
   MED                : 0
```

```
Community          : [ 8009:8009]
Extended community : [ target:2L:2 ]
Preference         : Default
```

## Supported Software Information

Releases 20.2 and later support all content described in this article.

## Additional Information

Branch Hardware and Software Requirements
Branch Overview
Configure Basic Features
Initial Branch Software Configuration
Install Headend Components on Azure
Install on Azure
Qualified AWS and Azure Instances