Vodafone Business VMware Virtual Edge on AWS and Azure

Customer Deployment Guide R1.0

If you can re-imagine your business, you can improve it

Together we can

vodafone business

Contents

Chapter 1: Overview

VMware SD-WAN Edges, physical or virtual, are easy to monitor and manage for users working on or off site.

With the VMware SD-WAN Orchestrator, you can monitor the status of Edges and view the details of each Edge, like the WAN links, top applications used by the Edges, usage data through the network sources and traffic destinations, business priority of network traffic, system information, details of Gateways connected to the Edge, and so on.

Customers who have workloads in AWS or Azure are now able to connect these to their SD-WAN via internet. Virtual Edges can be deployed in a customer's cloud domain using a Azure Resource Manager (ARM) template in Azure or CloudFormation template in AWS. The use of default templates provides a common approach to deployment however in some cases templates may need to be altered to accommodate specific environments.

The instantiation of Virtual Edge is a joint Customer and Vodafone activity.

Using this documentation

The purpose of this document is to provide guidance on how to instantiate a Virtual Machine on Amazon Web Services (AWS) and Microsoft Azure for the purposes of activating and connecting a VMware SD-WAN Cloud Virtual Edge to the rest of your SD-WAN network.

In scope:

- Installation of VMware Cloud Virtual Edge to AWS and Azure Public Cloud.
- VeloCloud SD-WAN Virtual Edge deployed as virtual instance in AWS and Azure clouds.
- Providing all necessary information for instantiating Virtual Machine as VMware SD-WAN Cloud Virtual Edge on AWS and Azure.

Out of scope:

- Troubleshooting.
- Guidance on creating the architecture and design or building an AWS or Azure Cloud.
- Advising or recommending the Customer where to instantiate the Virtual Machine (for example: which VPC, VNet, Security Group or Resource group).
- Deployment in other cloud platforms, such as Google Cloud Platform, private cloud or hybrid.
- Non SD-WAN connectivity via Partner Gateways using IPsec for AWS/Azure.

Vodafone and Customer Responsibilities

Vodafone is responsible for completing the following actions:

- Provide the Azure Resource Manager (ARM) or AWS Cloud Formation template.
- Create the Edge in VMware SD-WAN Orchestrator.
- If required, configure the cluster between two cloud Edges.
- Configure the GRE/BGP on Edges ONLY for interconnecting with Customer configuring the Customer’s AWS Transit Gateway or Azure Virtual WAN.

> ⓘ Vodafone are providing a managed SD-WAN service but will not own, build, or deploy the customer cloud environment on which the Virtual Computing Environment (VCE) is instantiated.

The Customer is responsible for completing the following actions:

- Provide a tested Cloud environment before the SD-WAN Virtual Edge deployment can commence.
- Create the Cloud environment for the Virtual Edge. If you require support for this activity, please contact your Vodafone Sales Team for Professional Services.
- Provide internet connectivity to the Cloud infrastructure, suitable to support the SD-WAN service.
- Provide Vodafone with the configuration parameters in VMware SD-WAN Orchestrator.

Prerequisites

It is a pre-requisite for the customer to provide a tested Cloud environment before the SD-WAN Virtual Edge deployment can commence.

Also, before you attempt to instantiate a Virtual Machine on wither AWS or Azure, make sure you have received the following information from Vodafone:

- The VMware Edge Activation Key – This is a key generated when an Edge is created on VMware SD-WAN Orchestrator. It is used for authentication by the Virtual Edge to Authenticate itself.
- The VMware SD-WAN Orchestrator Domain name (FQDN) – This is the address used by Virtual Edge to identify the correct VMware SD-WAN Orchestrator.
- The Software Version of VeloCloudEdge – In the template you can select from multiple versions. If the latest version is not listed as an option in the template, select the latest from the template options and the Virtual Edge during will update itself during activation to the configured version on VMware SD-WAN Orchestrator.

Chapter 2: Deploying Virtual Edges in AWS

This section contains information about:

The Deployment Process in AWS

Deploying a Virtual Edge requires doing configurations in both VMware SD-WAN Orchestrator and in the Amazon Web Services (AWS) Portal and Console. All the VMware SD-WAN Orchestrator configurations done by Vodafone and the AWS configurations are done by the Customer.

In summary, the configurations required in order are as follows:

Step	Task	Where	Who si responsible	When
1	Configure AWS Cloud Virtual Edge profile.	VMware SD-WAN Orchestrator	Vodafone	Pre-activation
2	Configure VPCs and subnets (optional step, in case they do not exist).	AWS	Customer	Pre-activation
3	Download Cloud Formation template.	Customer Self-Service Portal	Customer	Pre-activation
4	Create Edge and send Activation Key other details.	VMware SD-WAN Orchestrator	Vodafone	Activation
5	Update Cloud Formation template and deploy Virtual Edges.	AWS	Customer	Activation
6	Create Transit Gateway and configure connectivity to VPCs. Send Transit Gateway connectivity details to Vodafone (applicable if VMware Edges and Customer applications are in Multi VPC setup).	AWS	Customer	Activation
7	Configure Transit Gateway as Non SD-WAN Destination (applicable if VMware Edges and Customer applications are in multi VPC setup).	VMware SD-WAN Orchestrator	Customer	Activation

Step	Task	Where	Who si responsible	When
8	Configure Transit Gateway tunnel connectivity from Virtual Edge LAN. (applicable if VMware Edges and Customer applications are in multi VPC setup).	VMware SD-WAN Orchestrator	Vodafone	Activation
9	Perform verifications to ensure that all the tunnels and the connectivity are functioning.	VMware SD-WAN Orchestrator and AWS	Vodafone and Customer	Activation

The following sections provide details on the steps performed by the Customer.

Step 1. Configure AWS VPCs and Subnets

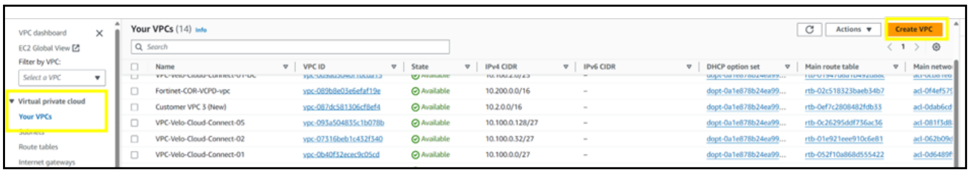
The pre-requisites to deploying a Virtual Edge in Amazon Web Services (AWS) are:

- a Connector or an AWS Transit Gateway to connect your Amazon Virtual Private Clouds (VPCs).
- at least two Subnets.

Both AWS Connect VPC and subnets contain a Route table which are important to configure properly.

The following procedure is a basic configuration guideline which can be adjusted based on your environment:

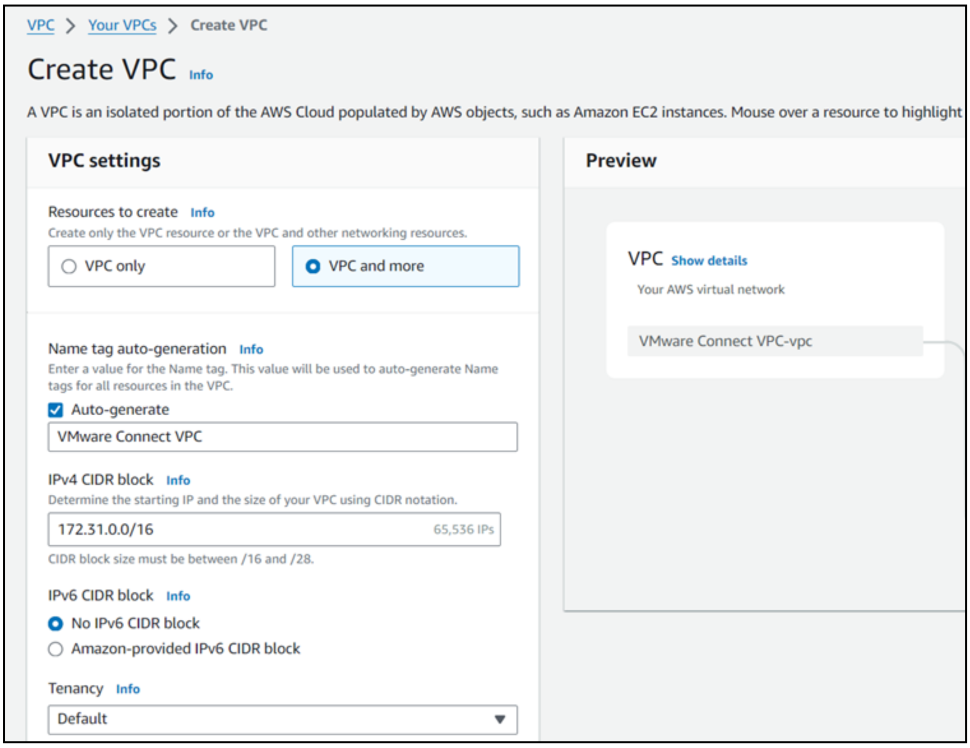
1. In your AWS Management Console, select the right **Region**, and then navigate to **AWS VPC service** > **Your VPCs** > **Create VPC**.



Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set	Main route table	Main netwo
Fortinet-COR-VCPD-vpc	vpc-089b8e03e6efaf19e	Available	10.200.0.0/16	–	dopt-0a1e878b24ea99...	rtb-02c518323baeb34b7	acl-0f4ef579
Customer VPC 3 (New)	vpc-087dc581306cf8ef4	Available	10.2.0.0/16	–	dopt-0a1e878b24ea99...	rtb-0ef7c2808482fdb33	acl-0dab6cd
VPC-Velo-Cloud-Connect-05	vpc-093a504835c1b078b	Available	10.100.0.128/27	–	dopt-0a1e878b24ea99...	rtb-0c26295ddf736ac36	acl-081f3d8
VPC-Velo-Cloud-Connect-02	vpc-07316beb1c432f340	Available	10.100.0.32/27	–	dopt-0a1e878b24ea99...	rtb-01e921eee910c6e81	acl-062b09d
VPC-Velo-Cloud-Connect-01	vpc-0b40f32ecec9c05cd	Available	10.100.0.0/27	–	dopt-0a1e878b24ea99...	rtb-052f10a868d555422	acl-0d6489f

2. Under **VPC Settings,** select **VPC and more** to create subnets and default Network connections (the Internet gateway) automatically. Click **VPC only** to perform manual configuration. Example of fields to be filled:
   - Under **Name tag auto-generation**, provide a VPC name.
   - Enter the CIDR under **IPv4 CIDR block.** No IPv6 CIDR needed.
   - Set the **Tenancy** dropdown to **Default**.
   - Under **Number of Availability Zones (AZs**), choose the number of AZ based on customer requirement. 1 AZ is selected in this example.
   - One **Public subnet** needs to be selected for each AZ. Meaning, for 2 AZ, select 2 public subnets.
   - For Internet only use cases, one **Private subnet** is required for each AZ to be used on the LAN.
   - Under **NAT Gateways ($)**, select one of the options:
     - **None** (for NAT Gateway and VPC Endpoint)
     - **In 1 AZ**
     - **1 per AZ**
   - Under **DNS Options**, select both **Enable DNS hostnames** and **Enable DNS resolution**.

The **Create VPC** window is illustrated below, in 2 images for convenience:



Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances. Mouse over a resource to highlight

VPC settings

Resources to create Info

Create only the VPC resource or the VPC and other networking resources.

○ VPC only ● VPC and more

Name tag auto-generation Info

Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

☑ Auto-generate

VMware Connect VPC

IPv4 CIDR block Info

Determine the starting IP and the size of your VPC using CIDR notation.

172.31.0.0/16 65,536 IPs

CIDR block size must be between /16 and /28.

IPv6 CIDR block Info

● No IPv6 CIDR block

○ Amazon-provided IPv6 CIDR block

Tenancy Info

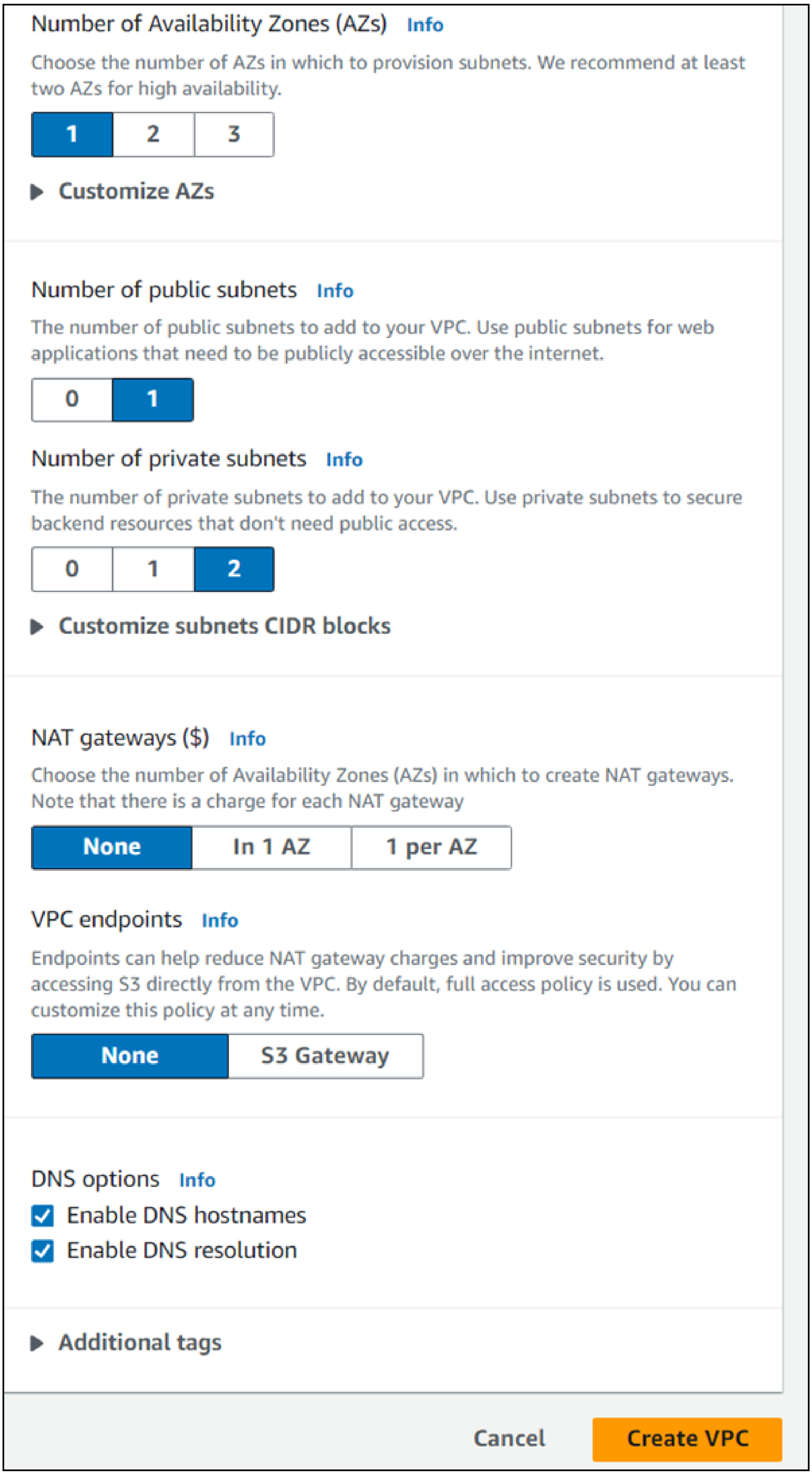
Default

Preview

VPC Show details

Your AWS virtual network

VMware Connect VPC-vpc



Number of Availability Zones (AZs) Info

Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

[✓ 1] 2 3

▶ Customize AZs

Number of public subnets Info

The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0 [✓ 1]

Number of private subnets Info

The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

0 1 [✓ 2]

▶ Customize subnets CIDR blocks

NAT gateways ($) Info

Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway

[✓ None] In 1 AZ 1 per AZ

VPC endpoints Info

Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

[✓ None] S3 Gateway

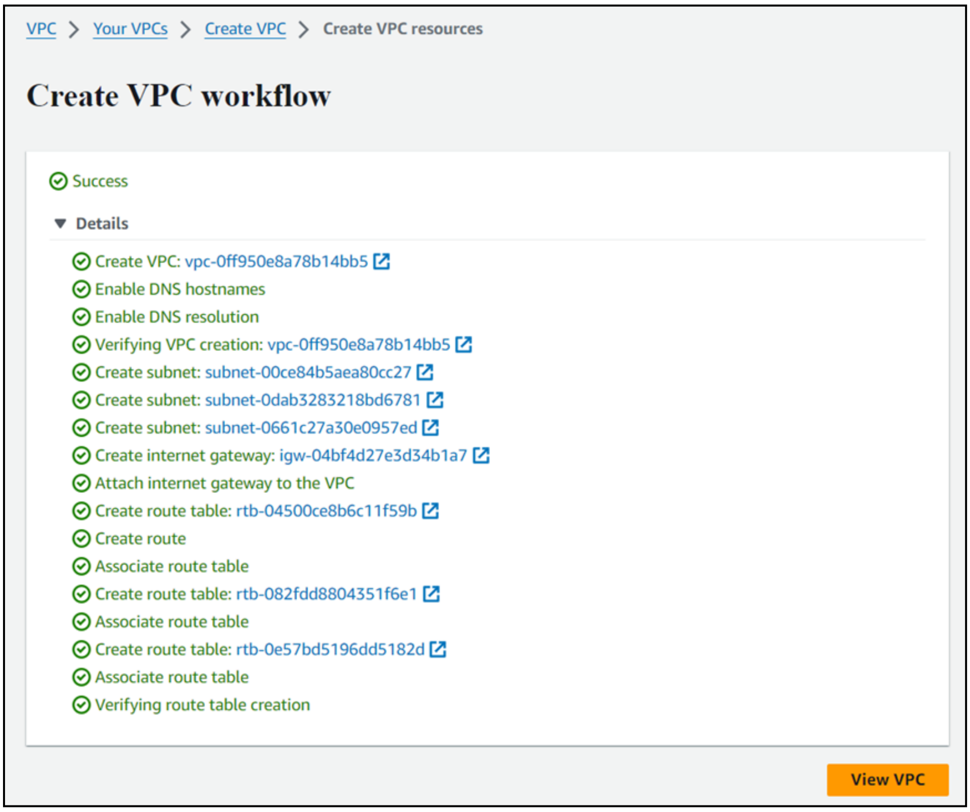
DNS options Info

☑ Enable DNS hostnames

☑ Enable DNS resolution

▶ Additional tags

3. Click **Create VPC**. Example workflow after a successful VPC creation:



VPC > Your VPCs > Create VPC > Create VPC resources

Create VPC workflow

✓ Success

▼ Details

✓ Create VPC: vpc-0ff950e8a78b14bb5

✓ Enable DNS hostnames

✓ Enable DNS resolution

✓ Verifying VPC creation: vpc-0ff950e8a78b14bb5

✓ Create subnet: subnet-00ce84b5aea80cc27

✓ Create subnet: subnet-0dab3283218bd6781

✓ Create subnet: subnet-0661c27a30e0957ed

✓ Create internet gateway: igw-04bf4d27e3d34b1a7

✓ Attach internet gateway to the VPC

✓ Create route table: rtb-04500ce8b6c11f59b

✓ Create route

✓ Associate route table

✓ Create route table: rtb-082fdd8804351f6e1

✓ Associate route table

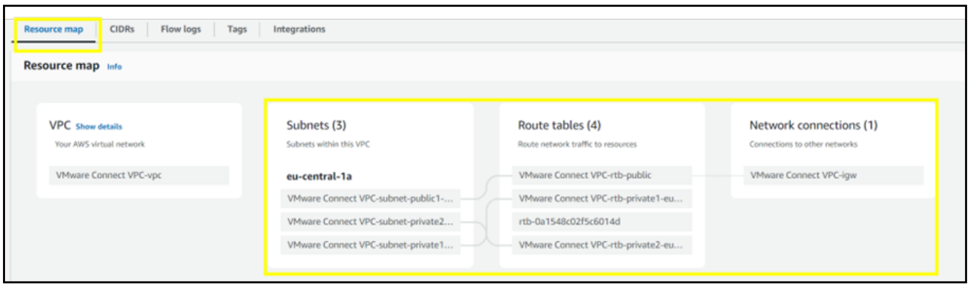
✓ Create route table: rtb-0e57bd5196dd5182d

✓ Associate route table

✓ Verifying route table creation

4. Once the VPC has been successfully created, click the **View VPC** button.

   Select the **Resource map** tab to make sure the Subnets, Route tables and Internet Gateways are created accordingly. Resource Map example:



Resource map Info

VPC Show details
Your AWS virtual network
VMware Connect VPC-vpc

Subnets (3)
Subnets within this VPC
eu-central-1a
VMware Connect VPC-subnet-public1-...
VMware Connect VPC-subnet-private2...
VMware Connect VPC-subnet-private1...

Route tables (4)
Route network traffic to resources
VMware Connect VPC-rtb-public
VMware Connect VPC-rtb-private1-eu...
rtb-0a1548c02f5c6014d
VMware Connect VPC-rtb-private2-eu...

Network connections (1)
Connections to other networks
VMware Connect VPC-igw

ⓘ Take note of the VPC name, Public and Private Subnet names as this info will be required in the next section.

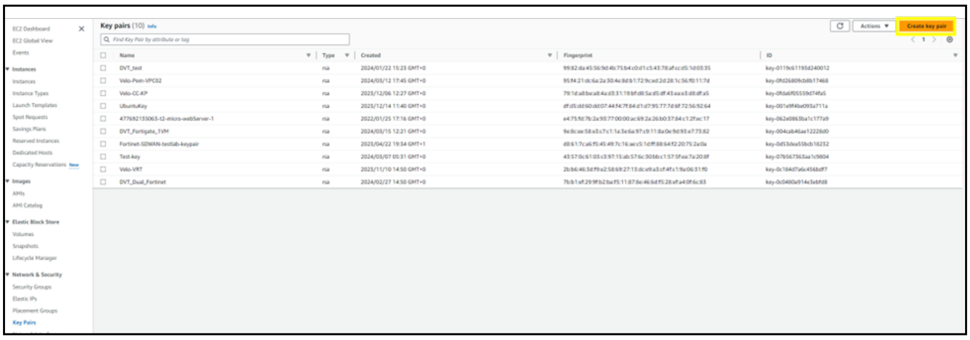
Step 2. Apply AWS Cloud Formation Template

The AWS Virtual Edge is deployed with Cloud Formation templates. There is an existing template provided by VMware for a brown field environment which means that the template will only create the Virtual Edge but not the VPCs and subnets. This template supports a single public WAN link and a LAN interface.

The Cloud Formation templates provided by Vodafone are available in Customer Self-Service Portal, under **My self care** > **Documents** section.

The following procedure is recommended for a production environment:

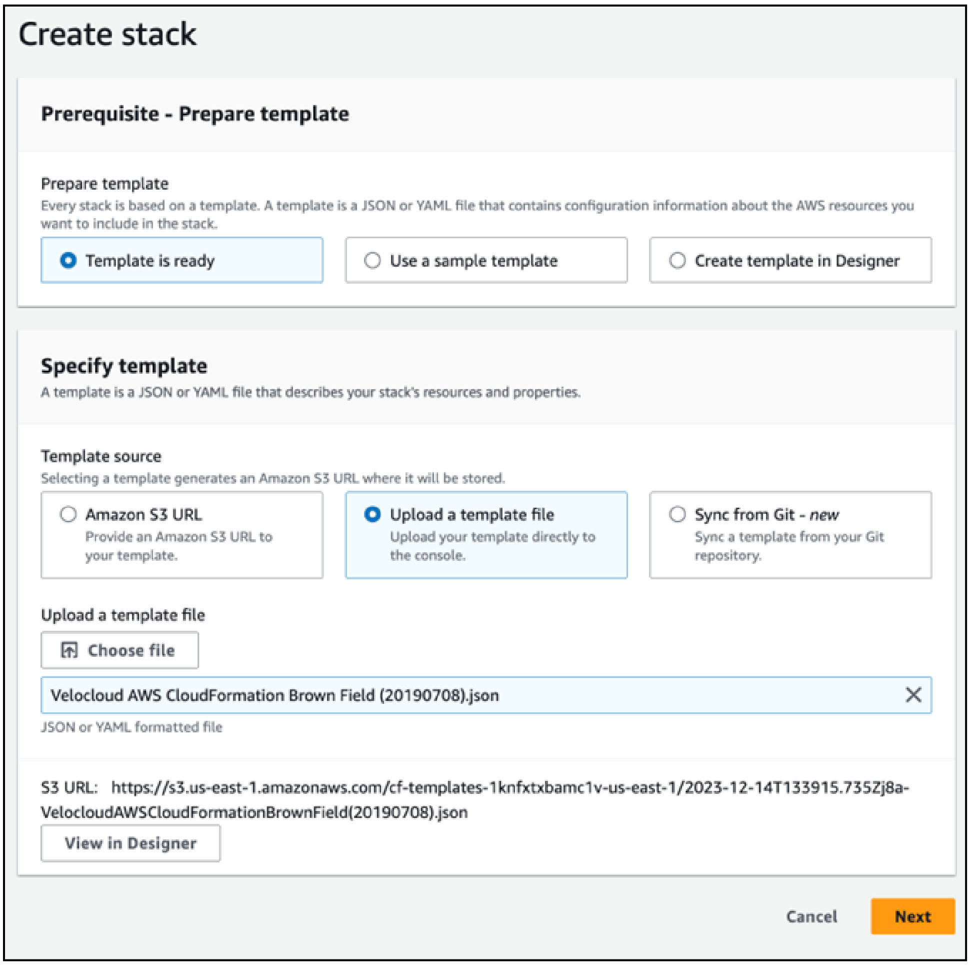
1. In your AWS Management Console, select the right **Region**, and then go to your Amazon Elastic Compute Cloud (Amazon EC2) service and under **Key pairs** click **Create Key Pair**. For example:



□	Name	Type	Created	Fingerprint	ID
□	DVT_test	rsa	2024/01/22 15:23 GMT+0	99:82:da:45:56:9d:4b:75:b4:c0:d1:c5:43:78:af:cc:d5:1d:03:35	key-0119c61193d240012
□	Velo-Pem-VPC02	rsa	2024/03/12 17:45 GMT+0	95:f4:21:dc:6a:2a:30:4e:8d:b1:72:9c:ed:2d:28:1c:56:f0:11:7d	key-0fd26809cb8b17468
□	Velo-CC-KP	rsa	2023/12/06 12:27 GMT+0	79:1d:a8:be:a8:4a:d3:31:19:bf:d8:5a:d5:df:43:ea:e3:d8:df:a5	key-0fda6f05559d74fa5
□	UbuntuKey	rsa	2023/12/14 11:40 GMT+0	df:d5:dd:60:dd:07:44:f4:7f:84:d1:d7:95:77:7d:6f:72:56:92:64	key-001e9f4ba095a711a
□	477692135063-t2-micro-webServer-1	rsa	2022/01/25 17:16 GMT+0	e4:75:fd:7b:2a:93:77:00:00:ac:69:2a:26:b0:37:84:c1:2f:ec:17	key-062e0863ba1c177a9
□	DVT_Fortigate_1VM	rsa	2024/03/15 12:21 GMT+0	9e:8c:ee:58:e3:c7:c1:1a:3e:6a:97:c9:11:8a:0e:9d:93:e7:73:82	key-004cab46ae12228d0
□	Fortinet-SDWAN-testlab-keypair	rsa	2023/04/22 19:34 GMT+1	d8:61:7c:a6:f5:45:49:7c:16:ae:c5:1d:ff:88:64:f2:20:75:2a:0a	key-0d53dea55bcb18232
□	Test-key	rsa	2024/03/07 05:31 GMT+0	43:57:0c:61:03:c3:97:15:ab:57:6c:30:bb:c1:57:5f:ea:7a:20:8f	key-07b567363aa1c9804
□	Velo-VRT	rsa	2023/11/10 14:50 GMT+0	2b:b6:46:3d:f9:e2:58:69:27:13:dc:a9:a3:cf:4f:c1:9a:06:31:f0	key-0c184d7a6c456bdf7
□	DVT_Dual_Fortinet	rsa	2024/02/27 14:50 GMT+0	7b:b1:ef:29:9f:b2:ba:f5:11:87:8e:46:6d:f5:28:ef:a4:0f:6c:83	key-0c0480a914e3ebfd8

2. Select right **Region** and then go to your AWS Cloud Formation service and click **Create Stack.**

   To create an AWS Cloud Formation Stack, the template can be uploaded on the deployment steps or provide an Amazon S3 reference if the template has been uploaded to an Amazon S3 bucket before.



Create stack

Prerequisite - Prepare template

Prepare template

Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

● Template is ready ○ Use a sample template ○ Create template in Designer

Specify template

A template is a JSON or YAML file that describes your stack's resources and properties.

Template source

Selecting a template generates an Amazon S3 URL where it will be stored.

○ Amazon S3 URL — Provide an Amazon S3 URL to your template.
● Upload a template file — Upload your template directly to the console.
○ Sync from Git - *new* — Sync a template from your Git repository.

Upload a template file

Velocloud AWS CloudFormation Brown Field (20190708).json

JSON or YAML formatted file

S3 URL: https://s3.us-east-1.amazonaws.com/cf-templates-1knfxtxbamc1v-us-east-1/2023-12-14T133915.735Zj8a-VelocloudAWSCloudFormationBrownField(20190708).json

3. Click **Next**. The main parameters being asked by the CloudFormation template under **Stack Details** are:

a. Provided by Vodafone Build Engineer during Activation:

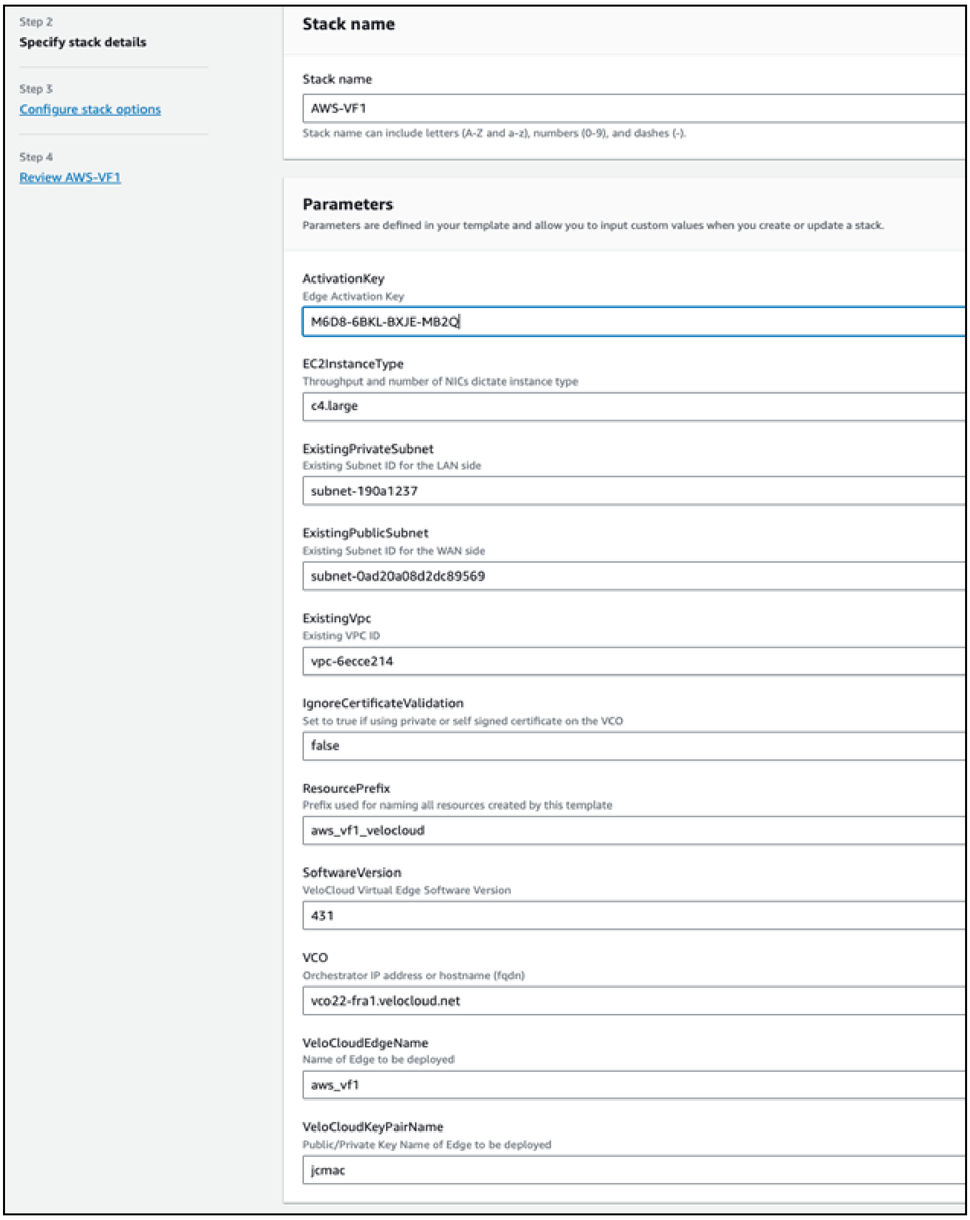
- **ActivationKey**: this is the activation key shown on VMware SD-WAN Orchestrator for the Virtual Edge.
- **SoftwareVersion**: the latest software version. Currently, 4.x.x version is the latest software version. But if on VMware SD-WAN Orchestrator the default version is 5.2.x.x, then the Virtual Edge automatically upgrades from 4.x.x to 5.2.x during provision.
- **VCO**: VMware Orchestrator domain name.

b. Provided by Customer Cloud Engineer during Activation:

- **VeloCloudKeyPairName**: the SSH key pair (created in Step 1) that allows a user to connect via SSH to the Virtual Edge.
- **EC2InstanceType**: the AWS instance type that defines the amount of memory and CPU for the Virtual Edge.
- **ExistingVPC**: the name of the Connect VPC which the Virtual Edge is deployed. Note that all subnets attached to the Virtual Edge must belong to this selected VPC.

- **ExistingPublicSubnet**: the subnet that provides Internet connectivity and allows the Virtual Edge to hold a public IP.
- **ExistingPrivateSubnet**: the subnet that provides connectivity on the LAN side.
- **VeloCloudEdgename**: Customer should choose an easily identifiable name of the Virtual Edge EC2 instance in AWS.

The **Specify Stack Details** window is illustrated below:



Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review AWS-VF1

Stack name

Stack name
AWS-VF1
Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.

ActivationKey
Edge Activation Key
M6D8-6BKL-BXJE-MB2Q

EC2InstanceType
Throughput and number of NICs dictate instance type
c4.large

ExistingPrivateSubnet
Existing Subnet ID for the LAN side
subnet-190a1237

ExistingPublicSubnet
Existing Subnet ID for the WAN side
subnet-0ad20a08d2dc89569

ExistingVpc
Existing VPC ID
vpc-6ecce214

IgnoreCertificateValidation
Set to true if using private or self signed certificate on the VCO
false

ResourcePrefix
Prefix used for naming all resources created by this template
aws_vf1_velocloud

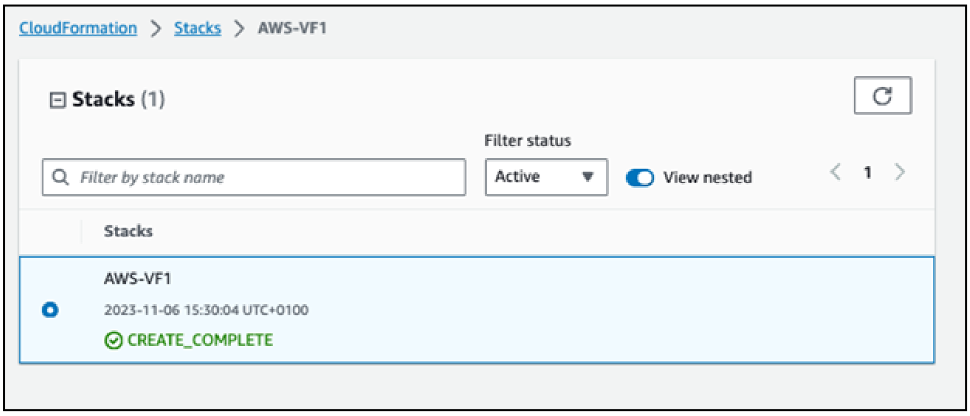
SoftwareVersion
VeloCloud Virtual Edge Software Version
431

VCO
Orchestrator IP address or hostname (fqdn)
vco22-fra1.velocloud.net

VeloCloudEdgeName
Name of Edge to be deployed
aws_vf1

VeloCloudKeyPairName
Public/Private Key Name of Edge to be deployed
jcmac

4. Click **Create stack**. Once the AWS CloudFormation Stack is deployed, the Virtual Edge is created and automatically activated:



AWS-VF1
2023-11-06 15:30:04 UTC+0100
CREATE_COMPLETE

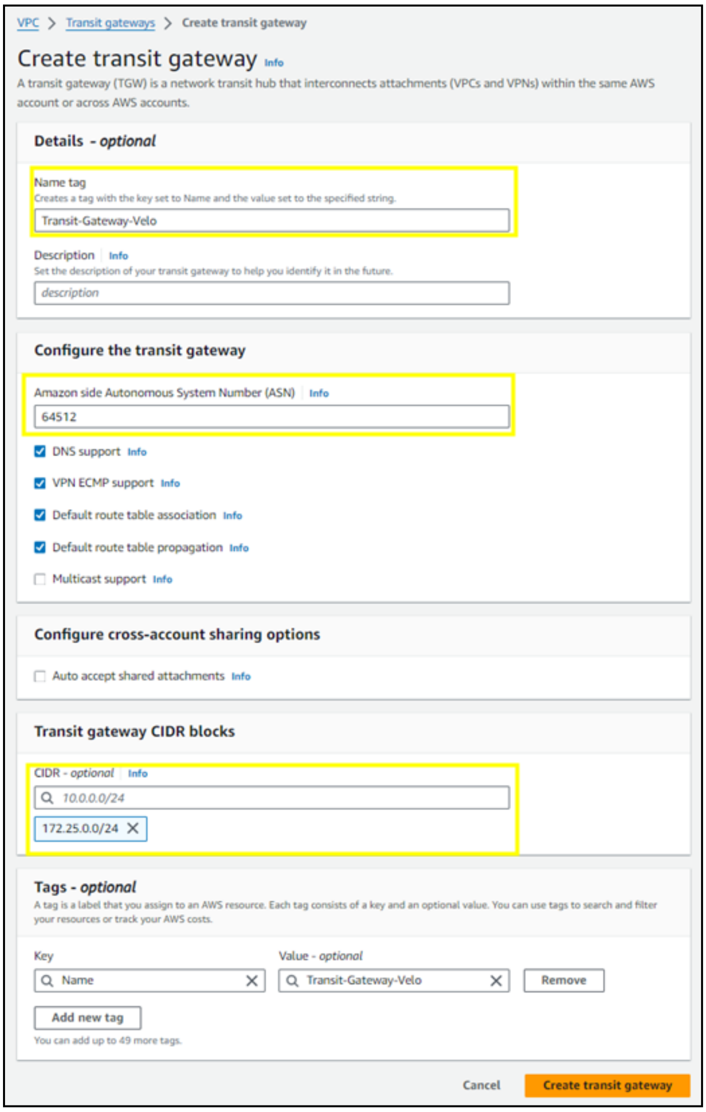
The Virtual Edge is displayed as Live in VMware SD-WAN Orchestrator.

Step 3. Configure AWS Transit Gateway

> AWS Transit Gateway is required for multiple VPC communication and for two Virtual Edges in Cluster use cases. If both the virtual Edge and Customer application are hosted in the same VPC, then a Transit Gateway is not required.

The following steps represent a basic configuration guideline which can be adjusted based on the Customer environment.

1. First, you must create the AWS Transit Gateway:
   a. In your AWS Management Console, select the right **Region** and then go to **VPC** > **Transit Gateways** and click **Create Transit Gateway**.
   b. Provide the **Name**, **CIDR block** and **ASN** which will be required later for the BGP/GRE connectivity with the Virtual Edge. For example:



VPC > Transit gateways > Create transit gateway

Create transit gateway Info

A transit gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same AWS account or across AWS accounts.

Details - *optional*

Name tag
Creates a tag with the key set to Name and the value set to the specified string.
Transit-Gateway-Velo

Description Info
Set the description of your transit gateway to help you identify it in the future.
description

Configure the transit gateway

Amazon side Autonomous System Number (ASN) Info
64512

☑ DNS support Info

☑ VPN ECMP support Info

☑ Default route table association Info

☑ Default route table propagation Info

☐ Multicast support Info

Configure cross-account sharing options

☐ Auto accept shared attachments Info

Transit gateway CIDR blocks

CIDR - *optional* Info
10.0.0.0/24
172.25.0.0/24 ✕

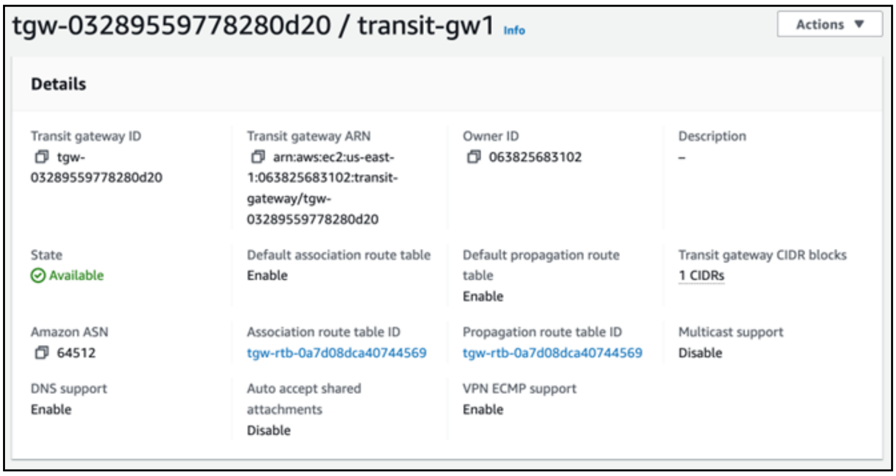
Tags - *optional*
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*	
Name ✕	Transit-Gateway-Velo ✕	Remove

Add new tag
You can add up to 49 more tags.

Cancel Create transit gateway

c. Click **Create Transit Gateway**. Transit gateway status example:



tgw-03289559778280d20 / transit-gw1 Info Actions ▼

Details

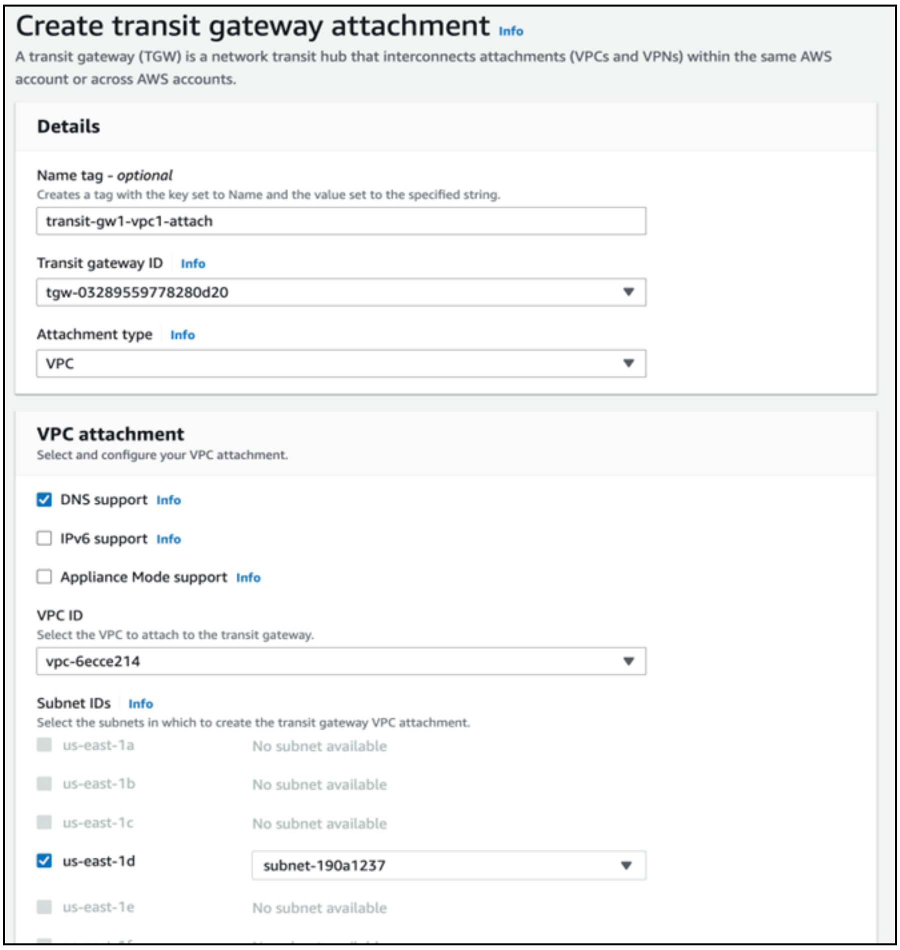
Transit gateway ID tgw-03289559778280d20	Transit gateway ARN arn:aws:ec2:us-east-1:063825683102:transit-gateway/tgw-03289559778280d20	Owner ID 063825683102	Description –
State ✓ Available	Default association route table Enable	Default propagation route table Enable	Transit gateway CIDR blocks 1 CIDRs
Amazon ASN 64512	Association route table ID tgw-rtb-0a7d08dca40744569	Propagation route table ID tgw-rtb-0a7d08dca40744569	Multicast support Disable
DNS support Enable	Auto accept shared attachments Disable	VPN ECMP support Enable	

d. Select the right **Region** and then go to **AWS Transit Gateway Attachments** and click **Create Transit Gateway Attachment**.

Transit Gateway will need to have VPC attachment to the Connect VPC where the Virtual Edges are hosted.

e. Provide a name, the allocated the Transit Gateway ID created in Step 1. Set the **Attachment type** dropdown to **VPC**. Select the **Connect VPC** in the **VPC ID** field and assign Virtual Edge LAN subnet under **Subnet IDs** field.

Transit GW VPC attachment for Connect VPC example:



Create transit gateway attachment Info

A transit gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same AWS account or across AWS accounts.

Details

Name tag - *optional*
Creates a tag with the key set to Name and the value set to the specified string.
transit-gw1-vpc1-attach

Transit gateway ID Info
tgw-03289559778280d20

Attachment type Info
VPC

VPC attachment
Select and configure your VPC attachment.

☑ DNS support Info

□ IPv6 support Info

□ Appliance Mode support Info

VPC ID
Select the VPC to attach to the transit gateway.
vpc-6ecce214

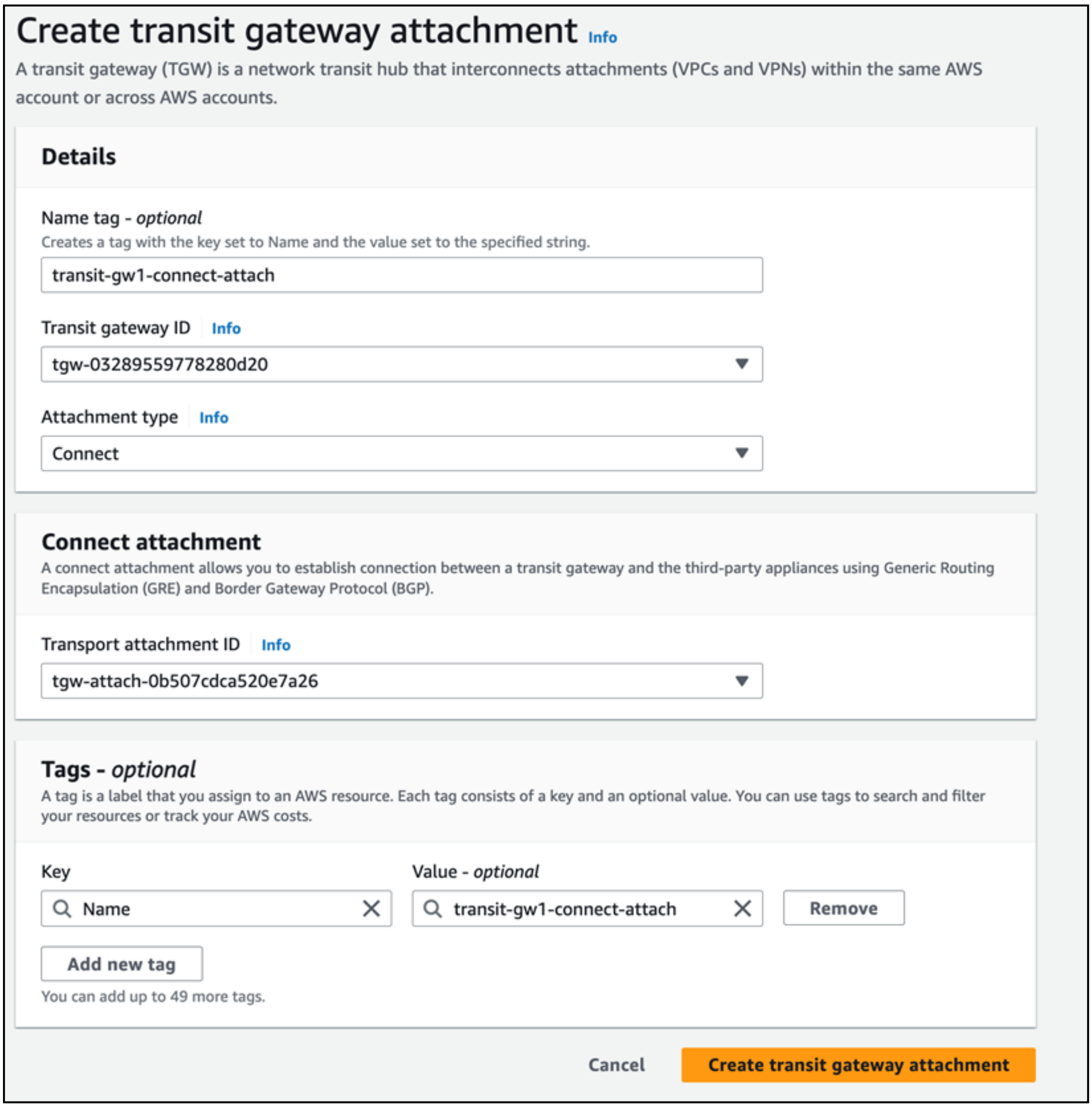
Subnet IDs Info
Select the subnets in which to create the transit gateway VPC attachment.

□ us-east-1a	No subnet available
□ us-east-1b	No subnet available
□ us-east-1c	No subnet available
☑ us-east-1d	subnet-190a1237
□ us-east-1e	No subnet available

Note that if you have several applications hosted in single or Multiple Child VPCs, each VPC that requires to be connected to the Transit Gateway needs an attachment of the **VPC** type. Repeat Steps 2 to 5 for all Child VPCs with relevant VPC ID and Subnet ID.

f. Connect/Transit VPCs hosting Virtual Edges are required to be connected to Transit Gateway using the Connect Attachment.

This is needed to configure GRE over BGP to Virtual Edges. As a transport attachment ID for the connect attachment, select the VPC attachment created in Step 2 of this procedure.



Create transit gateway attachment Info

A transit gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same AWS account or across AWS accounts.

Details

Name tag - *optional*
Creates a tag with the key set to Name and the value set to the specified string.
transit-gw1-connect-attach

Transit gateway ID Info
tgw-03289559778280d20

Attachment type Info
Connect

Connect attachment
A connect attachment allows you to establish connection between a transit gateway and the third-party appliances using Generic Routing Encapsulation (GRE) and Border Gateway Protocol (BGP).

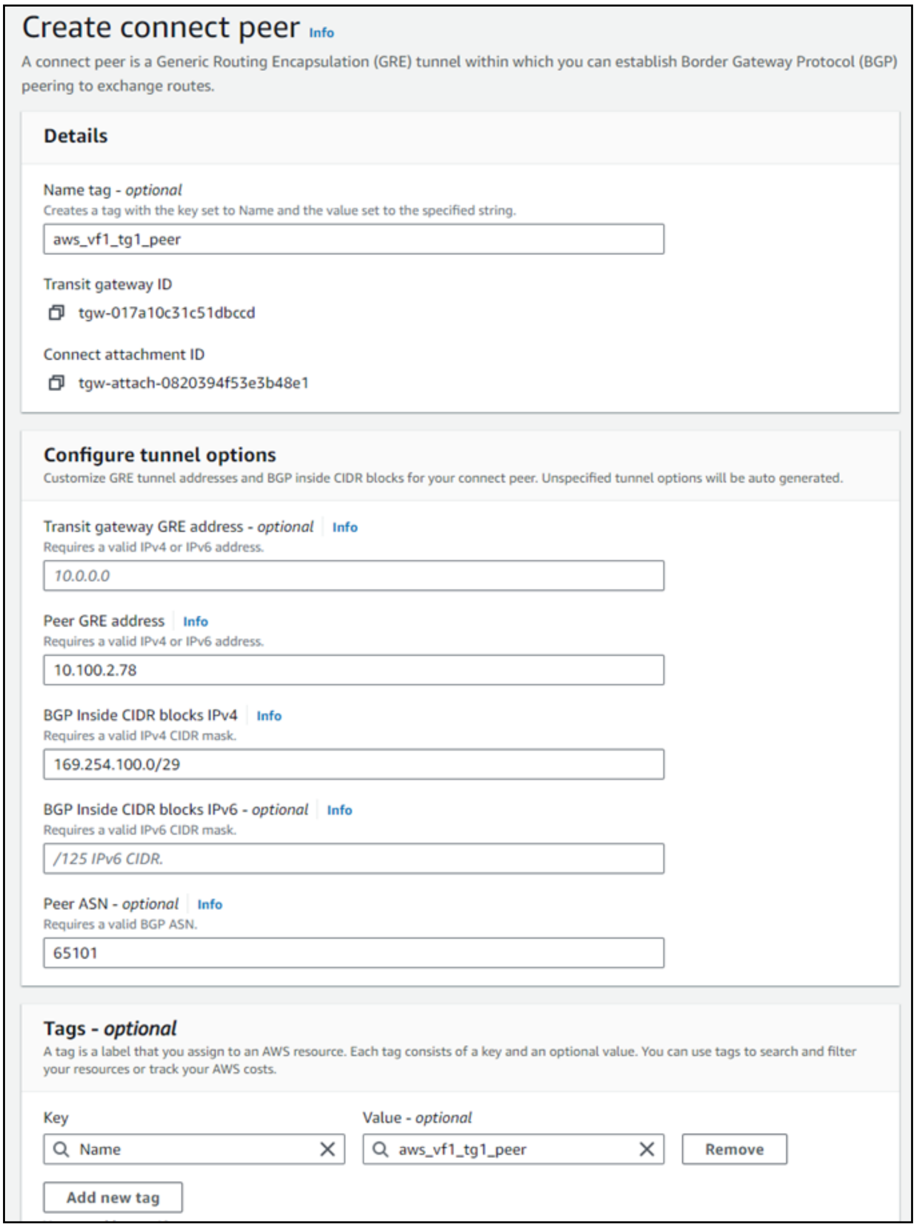
Transport attachment ID Info
tgw-attach-0b507cdca520e7a26

Tags - *optional*
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*
Name	transit-gw1-connect-attach

You can add up to 49 more tags.

2. Secondly, you must create a connect peer:
   a. Under the **Connect** attachment, click the **Connect Transit Gateway Attachments** > **Actions** > **Create Connect Peer**.



Create connect peer

A connect peer is a Generic Routing Encapsulation (GRE) tunnel within which you can establish Border Gateway Protocol (BGP) peering to exchange routes.

Details

Name tag - *optional*
Creates a tag with the key set to Name and the value set to the specified string.
aws_vf1_tg1_peer

Transit gateway ID
tgw-017a10c31c51dbccd

Connect attachment ID
tgw-attach-0820394f53e3b48e1

Configure tunnel options
Customize GRE tunnel addresses and BGP inside CIDR blocks for your connect peer. Unspecified tunnel options will be auto generated.

Transit gateway GRE address - *optional*
Requires a valid IPv4 or IPv6 address.
10.0.0.0

Peer GRE address
Requires a valid IPv4 or IPv6 address.
10.100.2.78

BGP Inside CIDR blocks IPv4
Requires a valid IPv4 CIDR mask.
169.254.100.0/29

BGP Inside CIDR blocks IPv6 - *optional*
Requires a valid IPv6 CIDR mask.
/125 IPv6 CIDR.

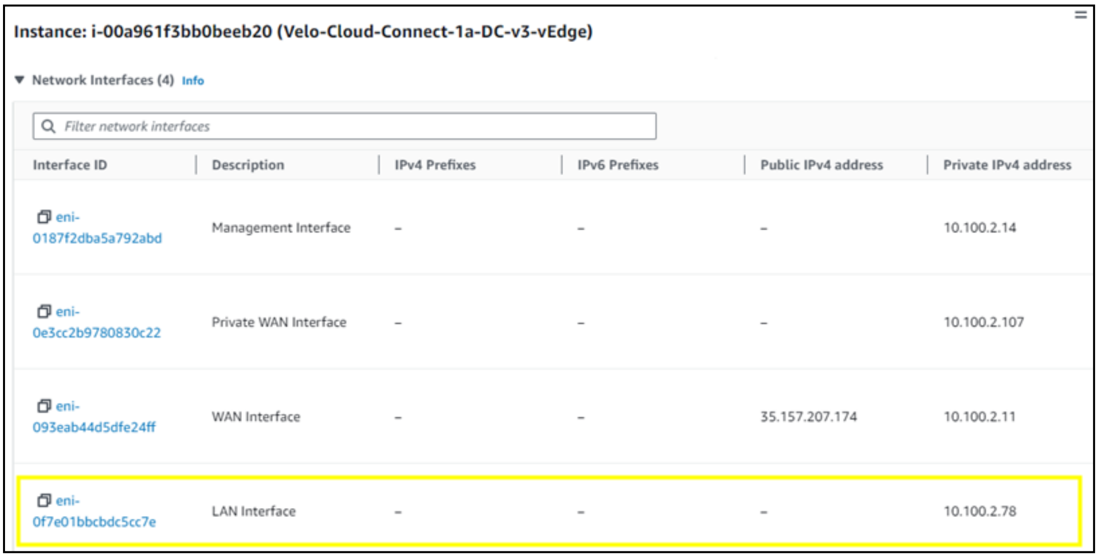
Peer ASN - *optional*
Requires a valid BGP ASN.
65101

Tags - *optional*
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*
Name	aws_vf1_tg1_peer

b. Under **Configure Tunnel Options**, the required parameters are:

- **Peer GRE address** should be Virtual Edge LAN interface IP. To get this IP, Go to EC2 instance where the Virtual Edge is configured on, then click the **Networking** tab, and scroll down to Network Interfaces to get the IP of the LAN interface.



Instance: i-00a961f3bb0beeb20 (Velo-Cloud-Connect-1a-DC-v3-vEdge)

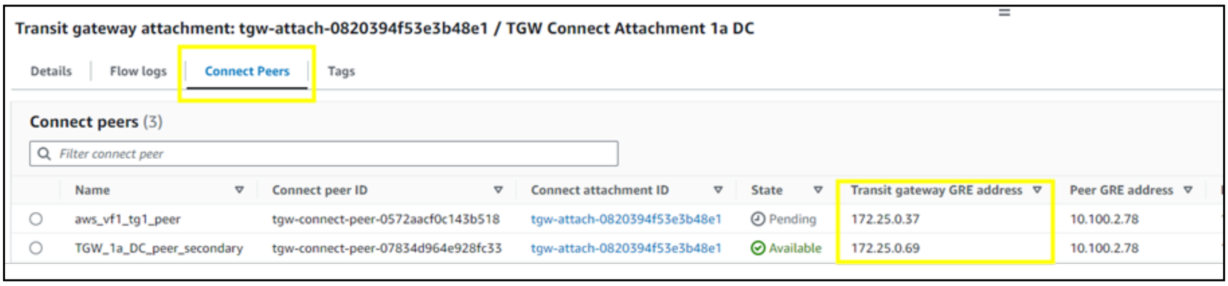
▼ Network Interfaces (4) Info

Filter network interfaces

Interface ID	Description	IPv4 Prefixes	IPv6 Prefixes	Public IPv4 address	Private IPv4 address
eni-0187f2dba5a792abd	Management Interface	–	–	–	10.100.2.14
eni-0e3cc2b9780830c22	Private WAN Interface	–	–	–	10.100.2.107
eni-093eab44d5dfe24ff	WAN Interface	–	–	35.157.207.174	10.100.2.11
eni-0f7e01bbcbdc5cc7e	LAN Interface	–	–	–	10.100.2.78

- **Peer ASN**: Virtual Edge BGP ASN (assigned by the Customer).
- **BGP Inside CIDR blocks IPv4**: An internal subnet such as 169.254.100.0/29.

c. After a Peers is created, go back to the **Connect Peer** section, it will automatically assign a GRE address for each Peer Tunnel. Take note of the Transit Gateway GRE address.



Transit gateway attachment: tgw-attach-0820394f53e3b48e1 / TGW Connect Attachment 1a DC

Connect peers (3)

Filter connect peer

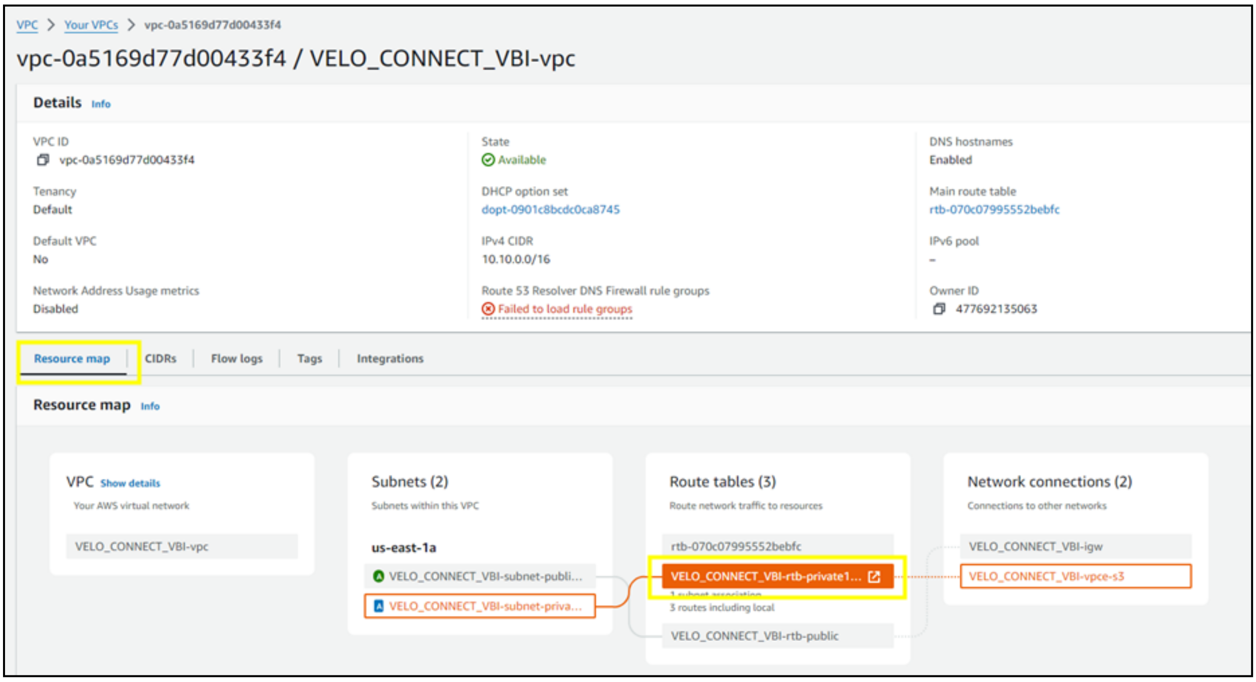
	Name	Connect peer ID	Connect attachment ID	State	Transit gateway GRE address	Peer GRE address
○	aws_vf1_tg1_peer	tgw-connect-peer-0572aacf0c143b518	tgw-attach-0820394f53e3b48e1	Pending	172.25.0.37	10.100.2.78
○	TGW_1a_DC_peer_secondary	tgw-connect-peer-07834d964e928fc33	tgw-attach-0820394f53e3b48e1	✓ Available	172.25.0.69	10.100.2.78

d. Optionally:

- You can add a Secondary Tunnel. Use a different name and BGP inside CIDR IP block. ASN and Peer GRE IP should be the same.
- If two vEdges/Cluster is required, create them with different names, ASN and BGP inside CIDR IP block, for the second Edge to Transit Gateway GRE Tunnel. Peer GRE IP should be the same.

3. Next, configure a route from Virtual Edge private LAN to Transit Gateway Subnet:

a. Go to the VPC configuration where the Virtual Edge(s) are hosted. Go to **Resource Map**, then click on the route table for the Private LAN.



VPC > Your VPCs > vpc-0a5169d77d00433f4

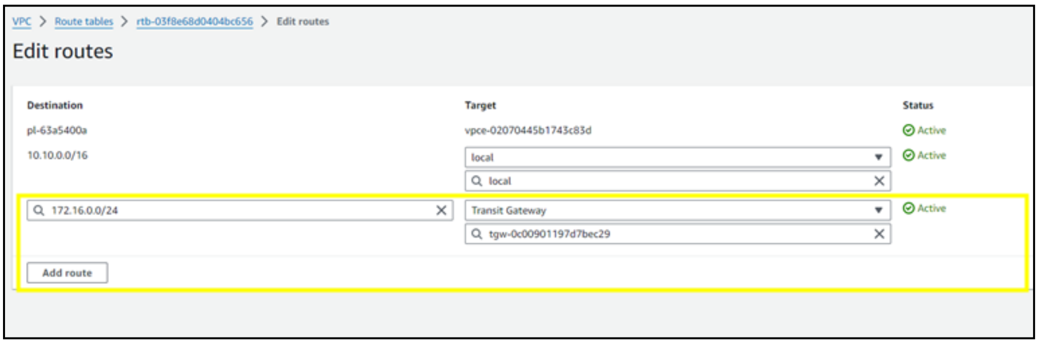
vpc-0a5169d77d00433f4 / VELO_CONNECT_VBI-vpc

Details Info

VPC ID vpc-0a5169d77d00433f4	State Available	DNS hostnames Enabled
Tenancy Default	DHCP option set dopt-0901c8bcdc0ca8745	Main route table rtb-070c07995552bebfc
Default VPC No	IPv4 CIDR 10.10.0.0/16	IPv6 pool –
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups Failed to load rule groups	Owner ID 477692135063

b. On the route table for Private LAN, click **Edit routes** > **Add route**> **As Destination**.

c. Add the Transit Gateway Subnet defined in Step 1 as Target, and add the Transit Gateway created in Step 1 ***as Destination.***



VPC > Route tables > rtb-03f8e68d0404bc656 > Edit routes

Edit routes

Destination	Target	Status
pl-63a5400a	vpce-02070445b1743c83d	Active
10.10.0.0/16	local local	Active
172.16.0.0/24	Transit Gateway tgw-0c00901197d7bec29	Active

d. Click **Save changes** to save the route.

4. Finally, provide the following details to Vodafone, so that Vodafone can configure the Transit Gateway Tunnel under the Customer Instance, in VMware SD-WAN Orchestrator:
   - BGP ASN for Virtual Edge. It will be 2 BGP ASNs for 2 vEdges in Cluster.
   - BGP ASN of Transit Gateway.
   - Transit Gateway GRE addresses.
   - Peer GRE addresses.
   - BGP inside IP block and Mask for each Transit Gateway Peer.

Once you have completed the steps, it is recommended to verify your deployment. To do so, see 'Verifying your Virtual Edges Deployment' on page 39.

Chapter 3: Deploying Virtual Edges in Azure

This section contains information about:

The Deployment Process in Azure

Deploying a Virtual Edge requires doing configurations in both VMware SD-WAN Orchestrator and in the Microsoft Azure Portal. All the VMware SD-WAN Orchestrator configurations done by Vodafone and the Azure configurations are done by the Customer.

In summary, the configurations required in order are as follows:

Step	Task	Where	Who si responsible	When
1	Configure Azure Edge profile.	VMware SD-WAN Orchestrator	Vodafone	Pre-activation
2	Create Edge and send Activation Key.	VMware SD-WAN Orchestrator	Vodafone	Activation
3	Configure VPCs and subnets (optional step, in case they do not exist).	Azure	Customer	Pre-activation
4	Download Azure Resource Manager template.	***TBD*** (maybe Customer Self-Service Portal	Customer	Pre-activation
5	Update Azure Resource Manager (ARM) template and deploy Virtual Edges.	Azure	Customer	Activation
6	Create Azure Virtual WAN and configure connectivity to VNets. Email Virtual WAN connectivity details to Vodafone (applicable if VMware Edges and Customer applications are in Multi VPC setup).	AWS	Customer	Activation

Step	Task	Where	Who si responsible	When
7	Configure Virtual WAN tunnel connectivity from Virtual Edge LAN (applicable if VMware Edges and Customer applications are in multi VPC setup).	VMware SD-WAN Orchestrator	Customer	Activation
9	Perform verifications to ensure that all the tunnels and the connectivity are functioning.	VMware SD-WAN Orchestrator and AWS	Vodafone and Customer	Activation

The following sections provide details on the steps performed by the Customer.

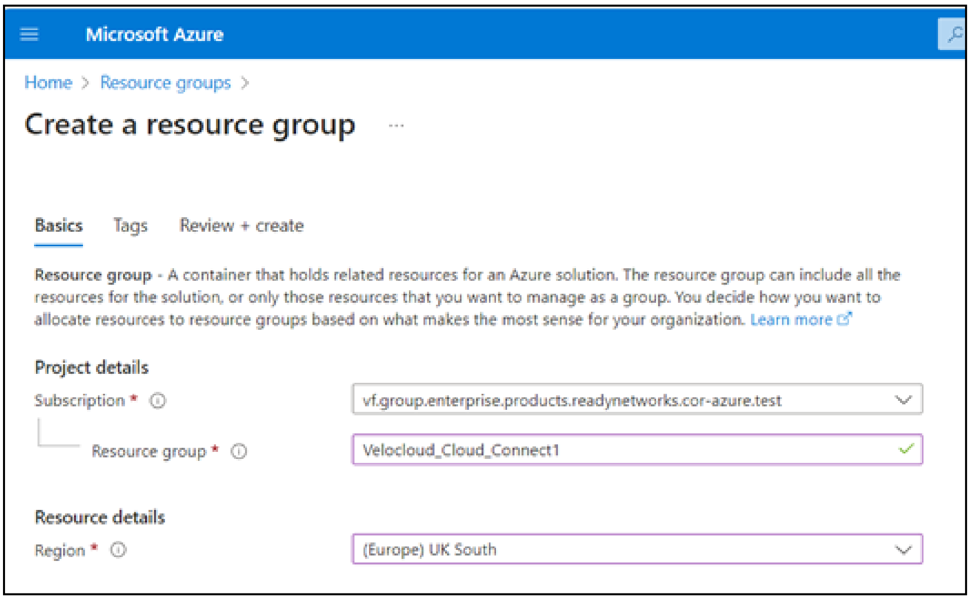
Step 1. Configure Azure VNet and Subnets

The pre-requisites to deploying a Virtual Edge in Azure are a VNet and at least two Subnets.

Both Azure VNet and Subnets contains a **Route table** and **Network Security Group**, which are important to configure properly.

The following procedure is a basic configuration guideline which can be adjusted based on your environment:

1. In your Azure Portal, click **Create a Resource group** in the desired Azure Region. For example:



Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. Learn more

Project details

Subscription * vf.group.enterprise.products.readynetworks.cor-azure.test

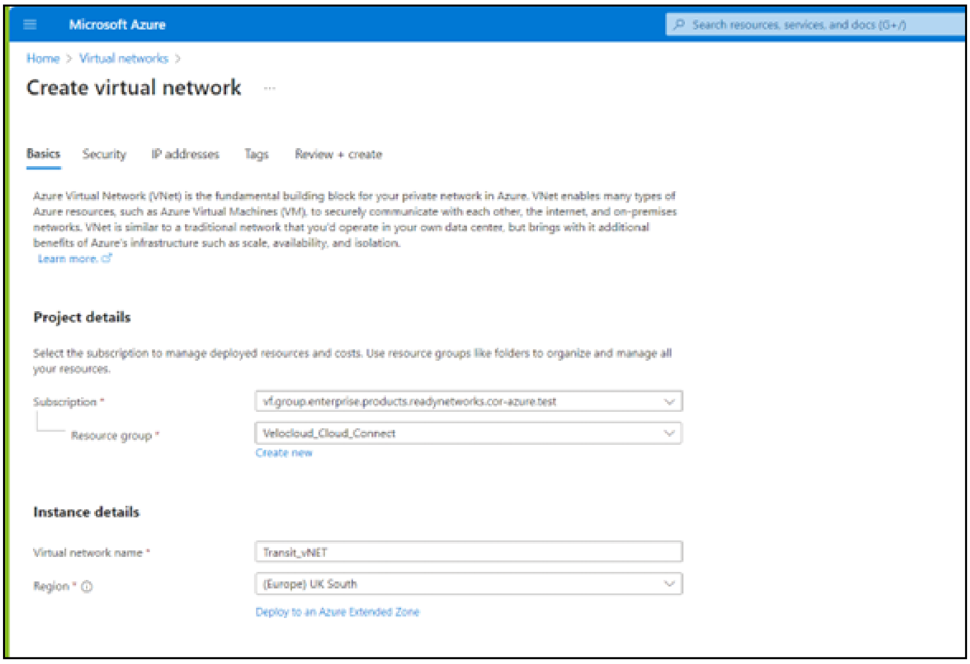
Resource group * Velocloud_Cloud_Connect1

Resource details

Region * (Europe) UK South

2. Search for Virtual Networks in Azure Portal and click **Create a Virtual Network**. Then:

   a. Under the **Basic** tab, select the Resource Group from step 1, provide a name and region.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Virtual networks >
Basics
Security
IP addresses
Tags
Review + create

Create virtual network

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation.
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 * vf.group.enterprise.products.readynetworks.cor-azure.test

Resource group * Velocloud_Cloud_Connect

Create new

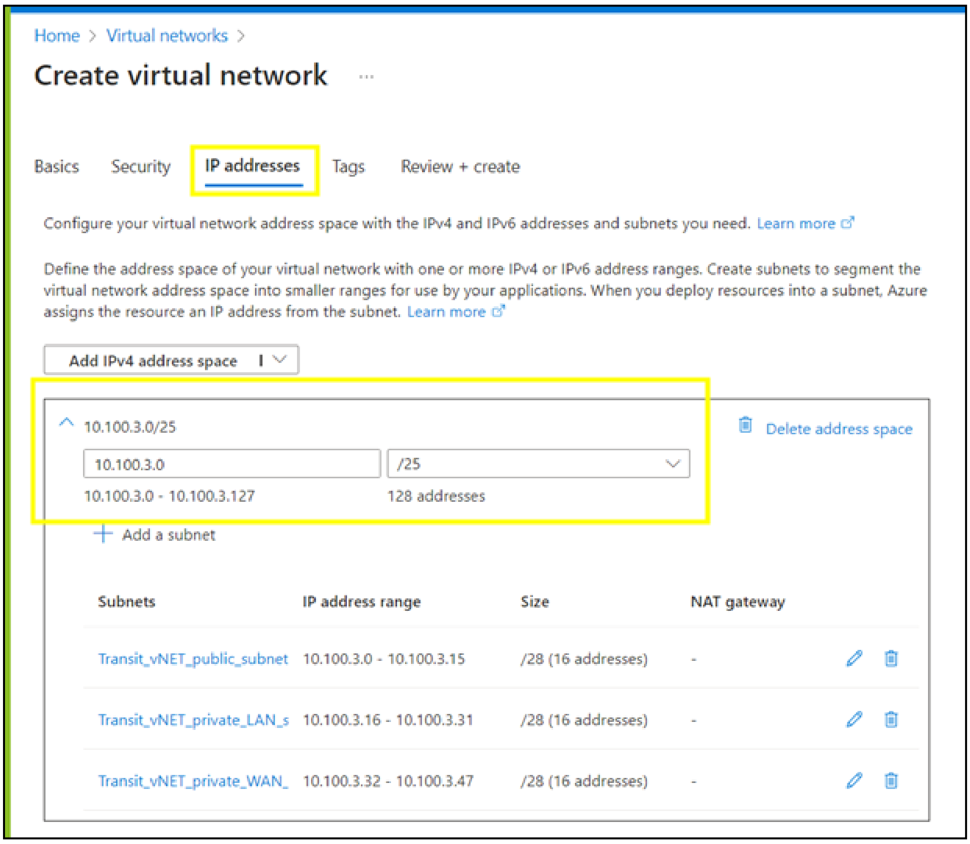
Instance details

Virtual network name * Transit_vNET

Region * (Europe) UK South

Deploy to an Azure Extended Zone

b. Under the **IP addresses** tab, define the address space and add the subnets as required. one public WAN subnet, one private LAN subnet is required for all use cases.



Create virtual network

Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. Learn more

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet. Learn more

10.100.3.0/25

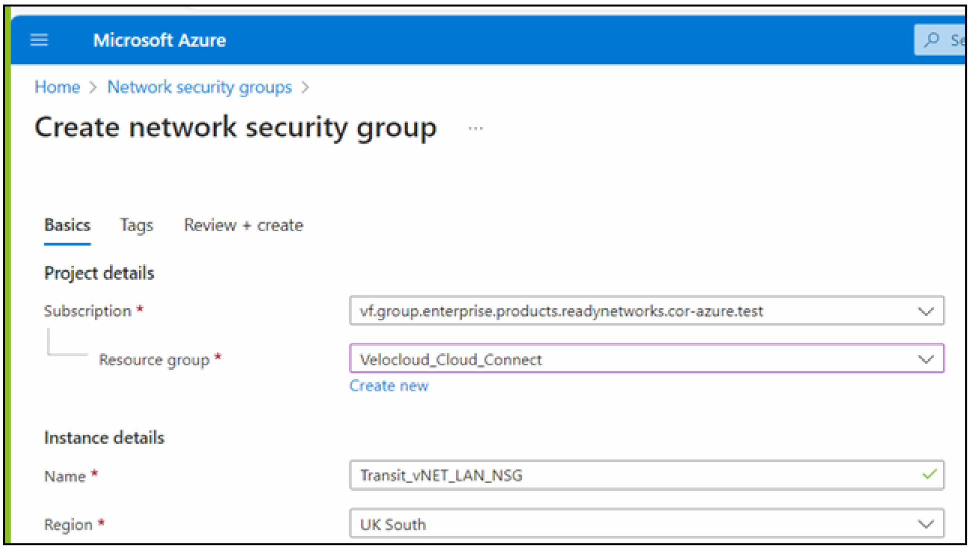
10.100.3.0 /25

10.100.3.0 - 10.100.3.127 128 addresses

Subnets	IP address range	Size	NAT gateway
Transit_vNET_public_subnet	10.100.3.0 - 10.100.3.15	/28 (16 addresses)	-
Transit_vNET_private_LAN_s	10.100.3.16 - 10.100.3.31	/28 (16 addresses)	-
Transit_vNET_private_WAN_	10.100.3.32 - 10.100.3.47	/28 (16 addresses)	-

c. When all configurations are created, go to the **Review + create** tab and click **Create**.

3. Create multiple security groups for each subnets created in Step 2 of this procedure:



Create network security group ...

Project details

Subscription * vf.group.enterprise.products.readynetworks.cor-azure.test

Resource group * Velocloud_Cloud_Connect

Instance details

Name * Transit_vNET_LAN_NSG

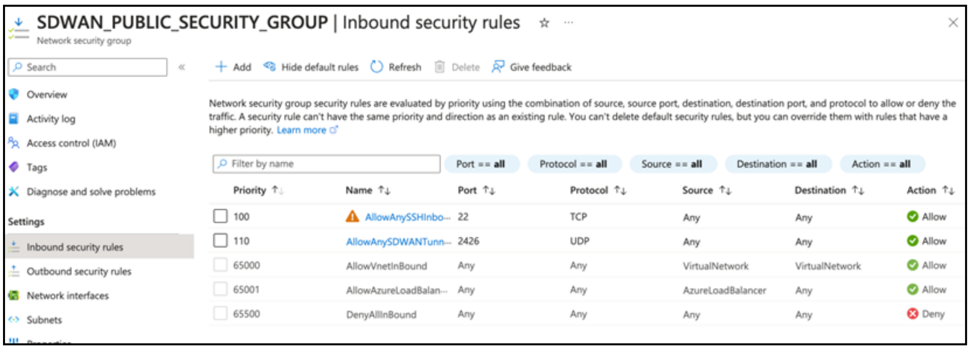
Region * UK South

4. Under **Settings**, go to **Inbound Security Rule** to assign **Security Groups** to Public Subnet to allow at least the port UDP/2426 for SDWAN tunnels to the Virtual Edge. Optionally SSH port can also be opened.

   Outbound Security Rules should be left as it is with default rules.

   To assign Security Groups to adjacent Subnets:

   a. Click **Subnets** under **Settings**.
   b. Click on **Associate**.
   c. Then select adjacent VNet and Subnets.



SDWAN_PUBLIC_SECURITY_GROUP | Inbound security rules

Network security group

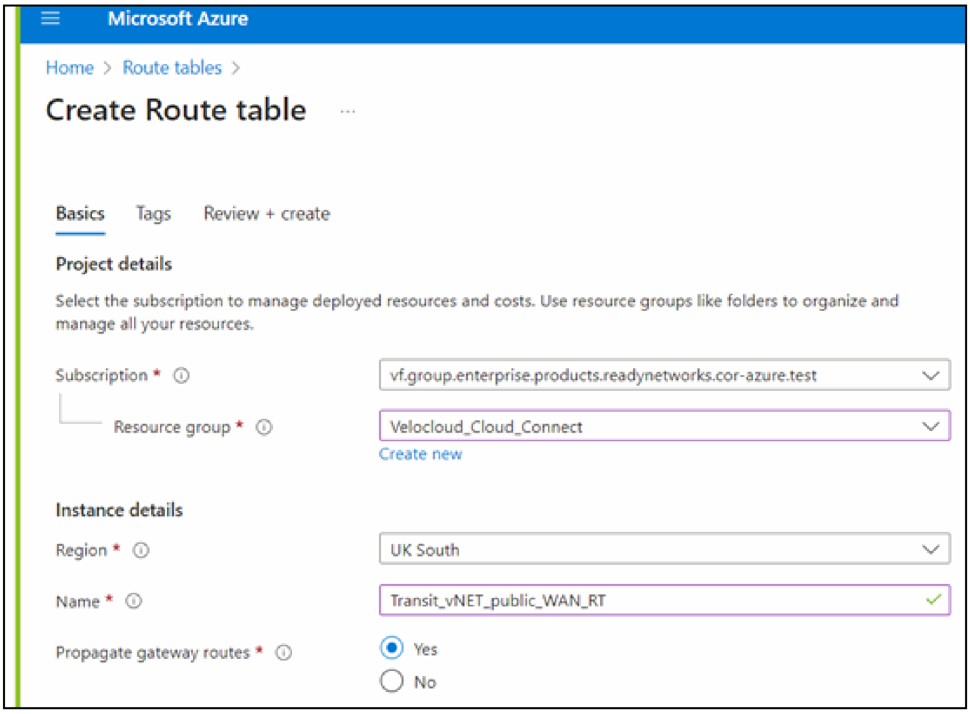
Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. Learn more

	Priority	Name	Port	Protocol	Source	Destination	Action
□	100	AllowAnySSHInbo...	22	TCP	Any	Any	Allow
□	110	AllowAnySDWANTunn...	2426	UDP	Any	Any	Allow
□	65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
□	65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	Allow
□	65500	DenyAllInBound	Any	Any	Any	Any	Deny

5. Create a Route Table and associate it with the VNet:

   For a Public WAN via Internet Route Table:

   a. Under **Settings**, click **Routes** then click **Add**. Provide a Route name, select **Destination type** to be **IP Addresses**, add **0.0.0.0/0** in **Destination IP ranges** field and select **Internet** to be **Next hop** type.



Create Route table

Project details

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

Subscription * : vf.group.enterprise.products.readynetworks.cor-azure.test

Resource group * : Velocloud_Cloud_Connect

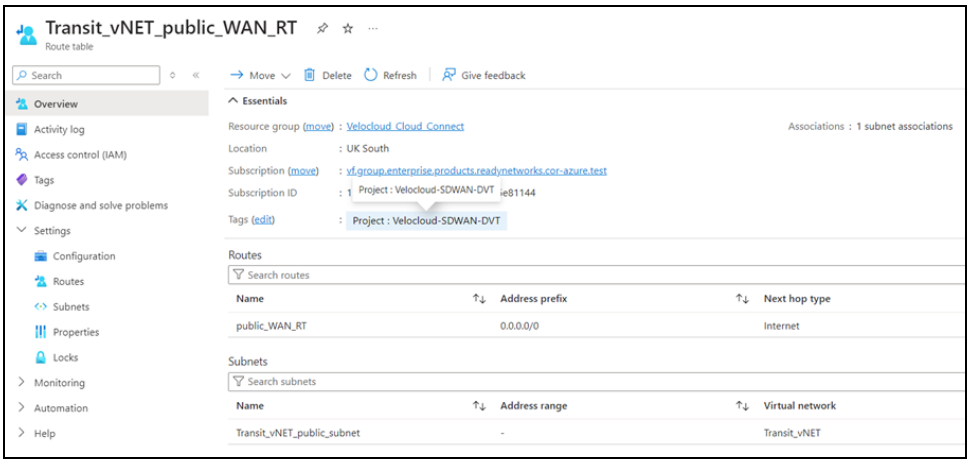
Instance details

Region * : UK South

Name * : Transit_vNET_public_WAN_RT ✓

Propagate gateway routes * : ● Yes ○ No

b. Under **Settings**, click **Subnets** then click **Associate**. Select the **VNET** created in Step 2 for **Virtual network** dropdown menu. Similarly, select the **Public WAN Subnet** created in Step 2 for **Subnet** dropdown menu.



Transit_vNET_public_WAN_RT

Route table

Resource group (move) : Velocloud Cloud Connect

Associations : 1 subnet associations

Location : UK South

Subscription (move) : vf.group.enterprise.products.readynetworks.cor-azure.test

Subscription ID : 1 Project : Velocloud-SDWAN-DVT ;e81144

Tags (edit) : Project : Velocloud-SDWAN-DVT

Routes

Name	Address prefix	Next hop type
public_WAN_RT	0.0.0.0/0	Internet

Subnets

Name	Address range	Virtual network
Transit_vNET_public_subnet	-	Transit_vNET

Route Table for Private LAN is optional based on the Customer's setup.

Step 2. Use Azure Template

The Azure Virtual Edge is deployed with an Azure template. This document assumes a brown field deployment which means the VNets, Availability Zones (AZs) and Subnets already exists with the necessary configurations.

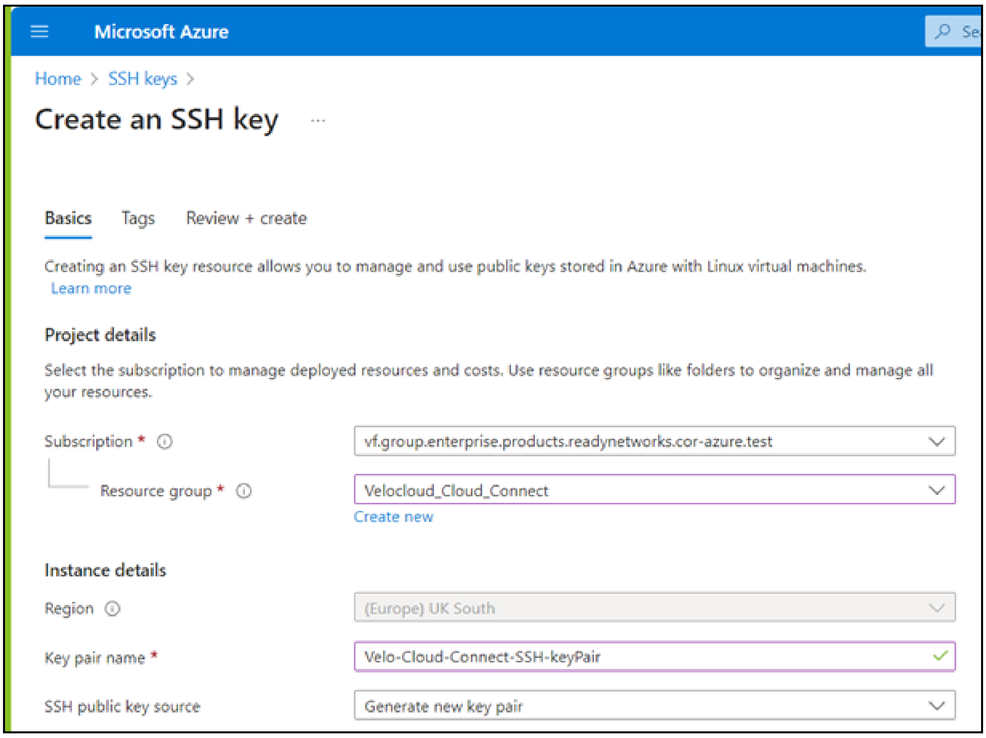
The Azure template provide by Vodafone is available in Customer Self-Service Portal, under **My self care** > **Documents** section:

image

The current Azure template supports a single public WAN link and a LAN interface. This template is appropriate for use cases with Internet Only.

The following procedure is recommended for a production environment:

1. In your Microsoft Azure Portal, search for **SSH keys** in the search bar and click **Create**.
2. In the Create an SSH Key window:
   a. Select the desired **Resource group**,
   b. Provide a **Key pair name**,
   c. Select **Generate new key pair** as **SSH Public key source** ,
   d. Click **Review + create**.



Create an SSH key

Creating an SSH key resource allows you to manage and use public keys stored in Azure with Linux virtual machines. 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 * : vf.group.enterprise.products.readynetworks.cor-azure.test

Resource group * : Velocloud_Cloud_Connect

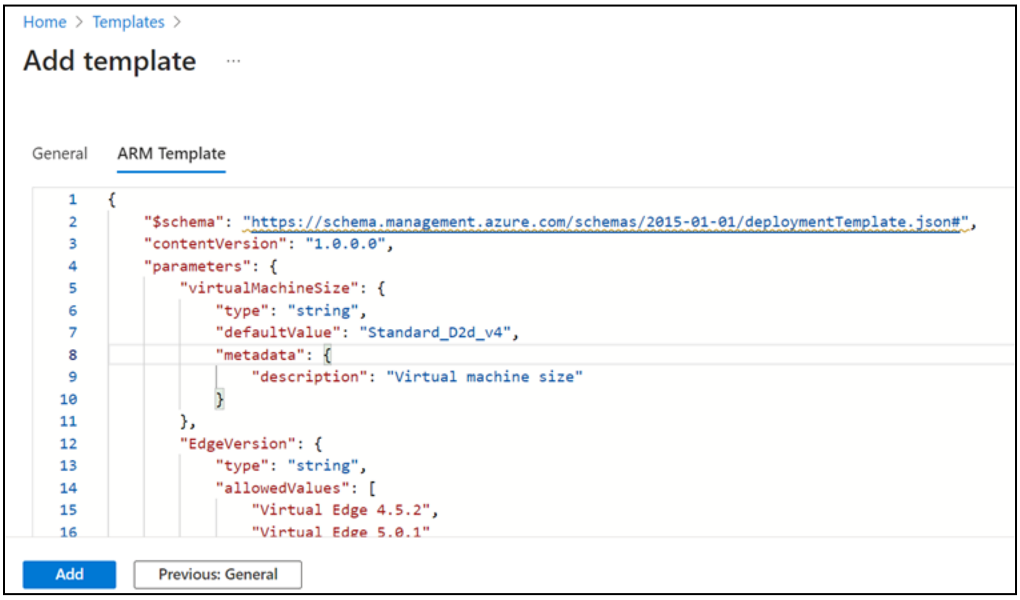
Instance details

Region : (Europe) UK South

Key pair name * : Velo-Cloud-Connect-SSH-keyPair

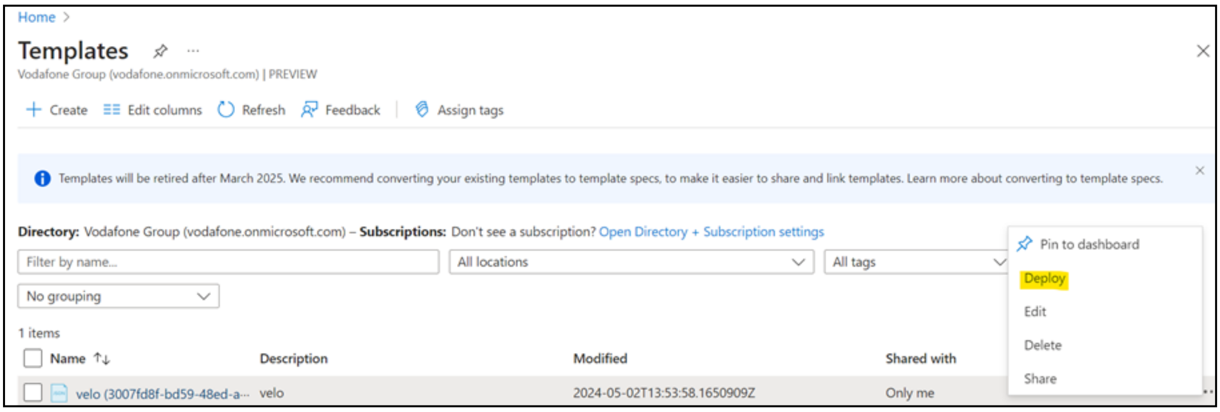
SSH public key source : Generate new key pair

3. Search for **Templates** in Azure Portal search bar and click **Create**.
4. In the Add Template window:
   a. On the **General** tab, provide a Name and Description.
   b. On the **ARM Template** tab, add the relevant ARM Template then click **Add**:



```
{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "virtualMachineSize": {
            "type": "string",
            "defaultValue": "Standard_D2d_v4",
            "metadata": {
                "description": "Virtual machine size"
            }
        },
        "EdgeVersion": {
            "type": "string",
            "allowedValues": [
                "Virtual Edge 4.5.2",
                "Virtual Edge 5.0.1"
```

c. After the ARM template is added, click the **More Actions** icon (**...**) of the newly created template and click **Deploy**:



Templates will be retired after March 2025. We recommend converting your existing templates to template specs, to make it easier to share and link templates. Learn more about converting to template specs.

Directory: Vodafone Group (vodafone.onmicrosoft.com) – **Subscriptions:** Don't see a subscription? Open Directory + Subscription settings

1 items

□ Name ↑↓	Description	Modified	Shared with
□ velo (3007fd8f-bd59-48ed-a···	velo	2024-05-02T13:53:58.1650909Z	Only me

5. In the Custom Deployment window, the following parameters which must be filled in by Customer Cloud Engineer:

a. The following parameters are provided by Vodafone Build Engineer during Activation:

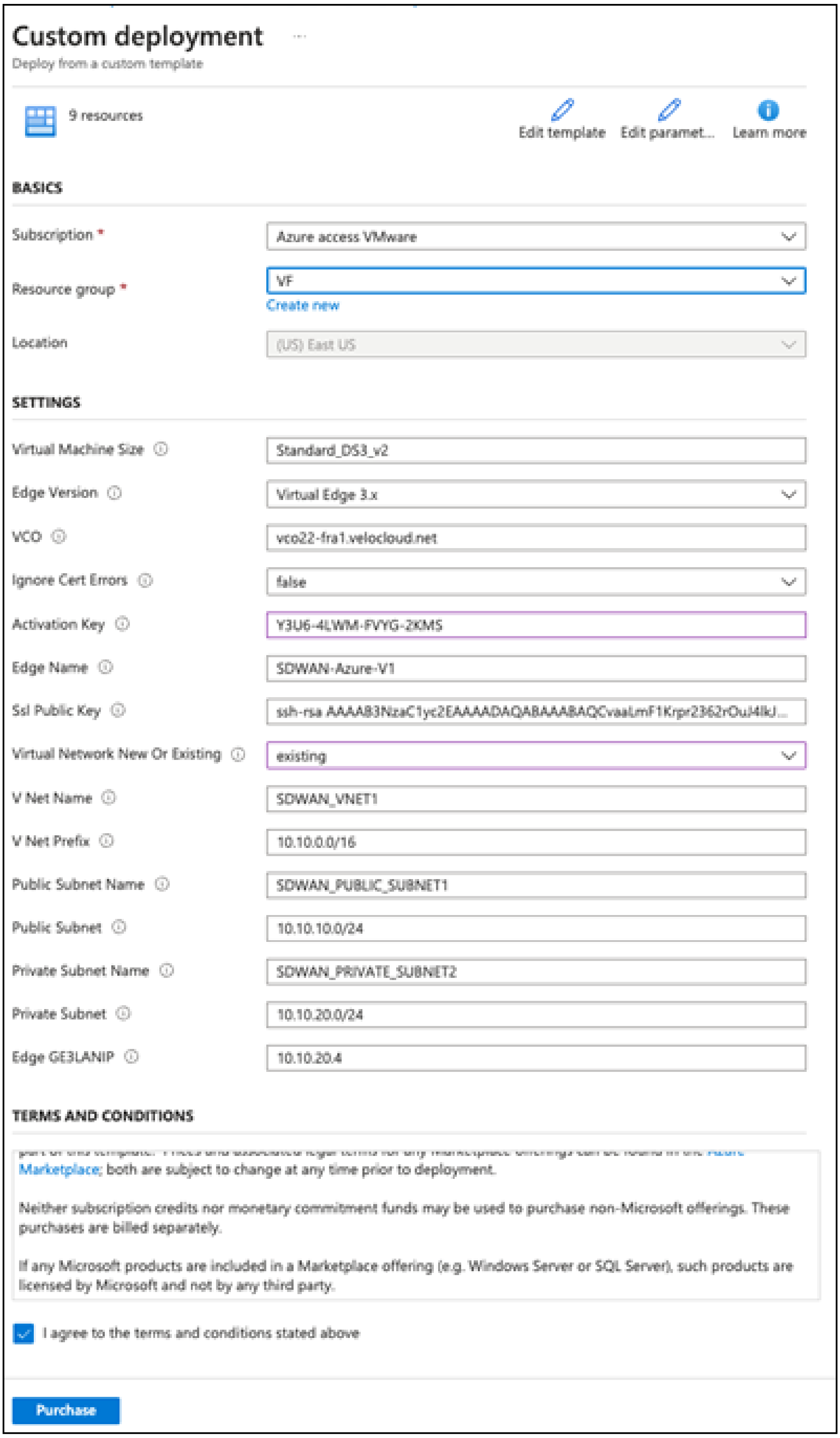
  - **VCO**: VMware Orchestrator domain name.
  - **Activation Key**: Virtual Edge Activation Key generated by Vodafone Build Engineer in VMware SD-WAN Orchestrator
  - **Edge Version**: For the template it should be 4.5.2. But If on VMware SD-WAN Orchestrator the default Edge SW is 5.2.x.x, then the Virtual Edge will upgrade from 4.5.2 to 5.2.x.x automatically during provision.

b. The following parameters are provided by the Customer Cloud Engineer during Activation:

  - **Resource Group**: Select the right resource group where all Virtual Edge services are already configured. Location should automatically be assigned.

- **Virtual Machine Siz**e: The Azure instance type that defines the amount of memory and CPU for the Virtual Edge.
- **Public Key**: the SSH key pair that allows a user to connect via SSH to the Virtual Edge.
- **VNet name & Prefix**: the name and address space of the VNet which the Virtual Edge is deployed. All Subnets attached to the Virtual Edge must belong to this selected VNet.
- **Public Subnet**: the public WAN subnet name and subnet that provides Internet connectivity and allows the Virtual Edge to hold a public IP.
- **Private Subnet**: the private subnet name and subnet range that provides connectivity on the LAN side.
- **EdgeGE3LANIP**: the IP address to assign on the LAN.

The Custom Deployment window:



Custom deployment ...

Deploy from a custom template

BASICS

Subscription *	Azure access VMware
Resource group *	VF Create new
Location	(US) East US

SETTINGS

Virtual Machine Size ⓘ	Standard_DS3_v2
Edge Version ⓘ	Virtual Edge 3.x
VCO ⓘ	vco22-fra1.velocloud.net
Ignore Cert Errors ⓘ	false
Activation Key ⓘ	Y3U6-4LWM-FVYG-2KMS
Edge Name ⓘ	SDWAN-Azure-V1
Ssl Public Key ⓘ	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCvaaLmF1Krpr2362rOuJ4lkJ...
Virtual Network New Or Existing ⓘ	existing
V Net Name ⓘ	SDWAN_VNET1
V Net Prefix ⓘ	10.10.0.0/16
Public Subnet Name ⓘ	SDWAN_PUBLIC_SUBNET1
Public Subnet ⓘ	10.10.10.0/24
Private Subnet Name ⓘ	SDWAN_PRIVATE_SUBNET2
Private Subnet ⓘ	10.10.20.0/24
Edge GE3LANIP ⓘ	10.10.20.4

TERMS AND CONDITIONS

part of this template. Prices and associated legal terms for any Marketplace offerings can be found in the Azure Marketplace; both are subject to change at any time prior to deployment.

Neither subscription credits nor monetary commitment funds may be used to purchase non-Microsoft offerings. These purchases are billed separately.

If any Microsoft products are included in a Marketplace offering (e.g. Windows Server or SQL Server), such products are licensed by Microsoft and not by any third party.

☑ I agree to the terms and conditions stated above

6. Once all the details are filled in, you must select the checkbox to agree to the Terms and Conditions.

7. Click the **Purchase** button.

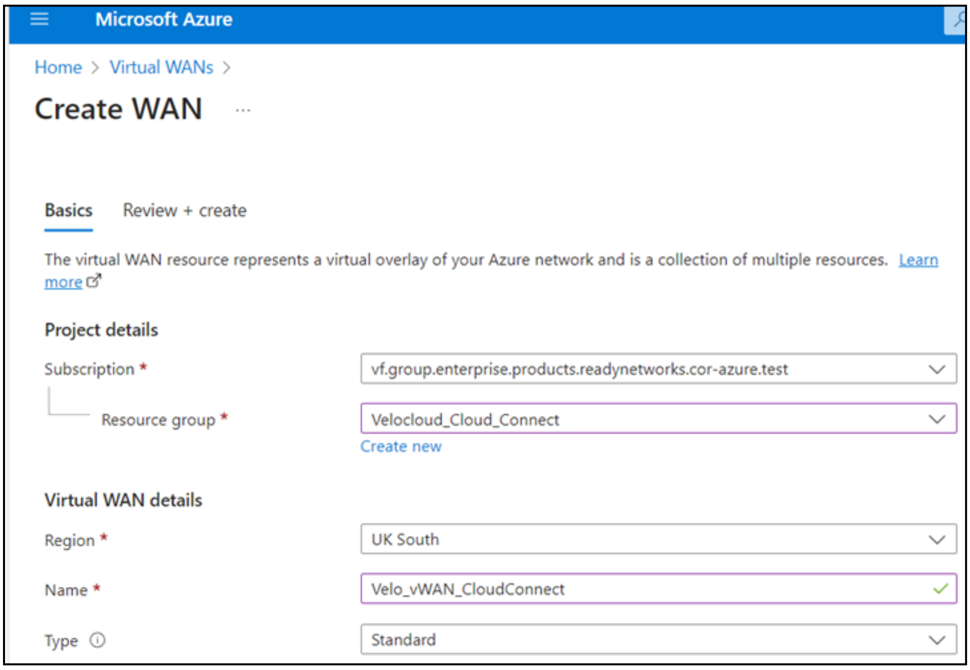
   The Azure Template activates the Virtual Edge automatically and appears as live in VMware SD-WAN Orchestrator.

Step 3. Configure Azure Virtual WAN

ⓘ Azure Virtual WAN is required for multiple VNet communication and for two Virtual Edges in Cluster Use cases. If both the virtual Edge and Customer application are hosted in same VNet, then Virtual WAN is not required.

The following procedure is a basic configuration guideline which can be adjusted based on the Customer environment:

1. Search for Virtual WAN in Azure Portal search bar and click **Create**.
   a. Select the relevant **Resource group** and **Region** from the dropdowns, provide a name and set the **Type** dropdown to **Standard**.



The virtual WAN resource represents a virtual overlay of your Azure network and is a collection of multiple resources. Learn more

Project details

Subscription * vf.group.enterprise.products.readynetworks.cor-azure.test

Resource group * Velocloud_Cloud_Connect

Create new

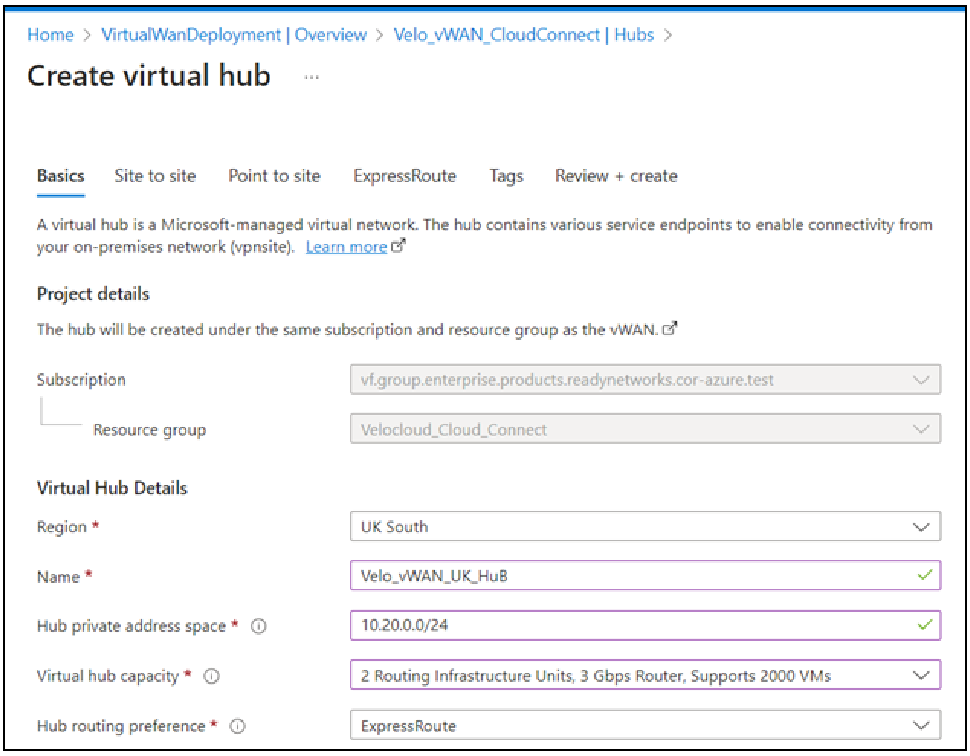
Virtual WAN details

Region * UK South

Name * Velo_vWAN_CloudConnect

Type ⓘ Standard

   b. Click **Review + Create**:
2. On the Virtual WAN page created in previous step, select **Hubs** from **Connectivity** dropdown.
   a. Click **New Hub**.
   b. On the Create Virtual Hub page, provide relevant details under **Basics** tab.



Home > VirtualWanDeployment | Overview > Velo_vWAN_CloudConnect | Hubs >
Basics
Site to site
Point to site
ExpressRoute
Tags
Review + create

Create virtual hub ...

A virtual hub is a Microsoft-managed virtual network. The hub contains various service endpoints to enable connectivity from your on-premises network (vpnsite). Learn more

Project details

The hub will be created under the same subscription and resource group as the vWAN.

Subscription: vf.group.enterprise.products.readynetworks.cor-azure.test

Resource group: Velocloud_Cloud_Connect

Virtual Hub Details

Region *: UK South

Name *: Velo_vWAN_UK_HuB

Hub private address space *: 10.20.0.0/24

Virtual hub capacity *: 2 Routing Infrastructure Units, 3 Gbps Router, Supports 2000 VMs

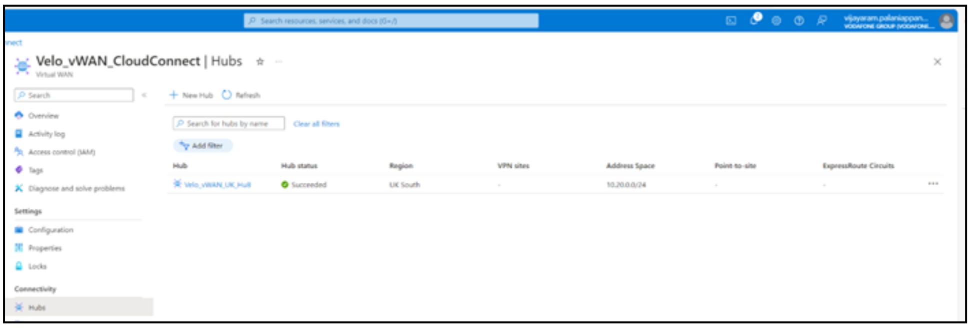
Hub routing preference *: ExpressRoute

c. Assign **Virtual hub capacity** and **Hub routing preference** based on your Azure Environment.

d. Optionally, you can add information on other tabs.

e. Click **Create** under the **Review + create** tab.

Example of Virtual WAN Hub created successfully:

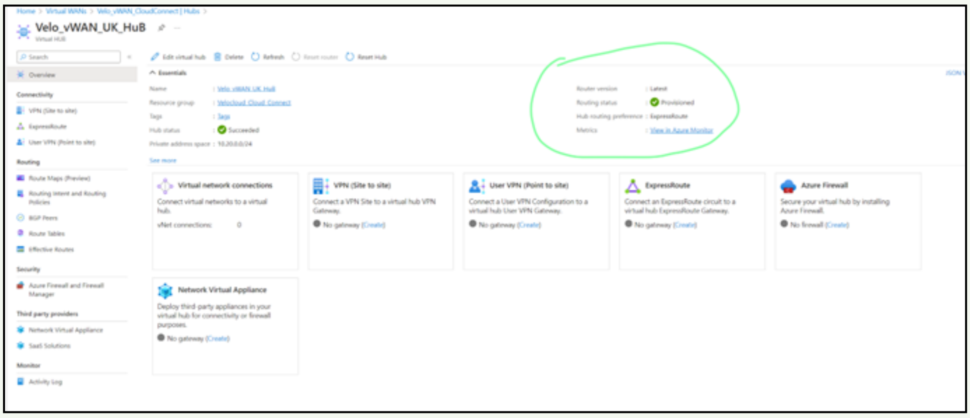


Velo_vWAN_CloudConnect | Hubs

Virtual WAN

Hub	Hub status	Region	VPN sites	Address Space	Point-to-site	ExpressRoute Circuits
Velo_vWAN_UK_HuB	Succeeded	UK South	-	10.20.0.0/24	-	-

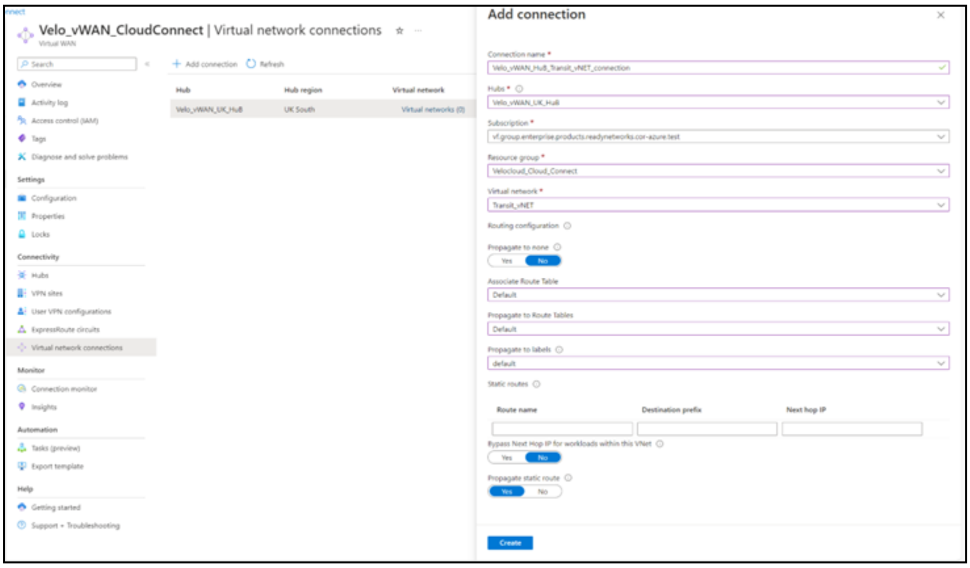
Before being able to continue with the Virtual WAN Hub configuration, the **Routing Status** of the Hub must in the **Provisioned** state. Note that it could take up to 30 minutes.



Velo_vWAN_UK_HuB

Name : Velo_vWAN_UK_HuB
Resource group : Velocloud_Cloud_Connect
Hub status : Succeeded
Private address space : 10.20.0.0/24
Router version : Latest
Routing status : Provisioned
Hub routing preference : ExpressRoute
Metrics : View in Azure Monitor

3. Next, you must create an Azure Virtual WAN Hub VNet Connection:
   a. On the Virtual WAN page, select **Virtual Network connections** from the **Connectivity** dropdown.
   b. Click **Add connection** to create Connection to the VNet that the Virtual Edge is deployed.
   c. Provide a connection name, select the relevant Hub, the resource group and the VNet for the connection.
   d. Click **Create**.



Velo_vWAN_CloudConnect | Virtual network connections

Hub	Hub region	Virtual network
Velo_vWAN_UK_HuB	UK South	Virtual networks (0)

Add connection

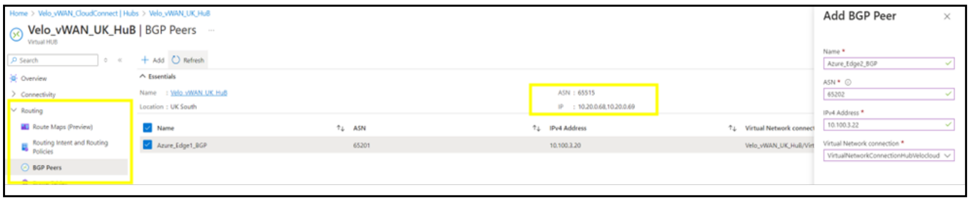
Connection name *: Velo_vWAN_HuB_Transit_vNET_connection
Hubs *: Velo_vWAN_UK_HuB
Subscription *: vf.group.enterprise.products.readynetworks.cor-azure.test
Resource group *: Velocloud_Cloud_Connect
Virtual network *: Transit_vNET
Routing configuration
Propagate to none: Yes [✓ No]
Associate Route Table: Default
Propagate to Route Tables: Default
Propagate to labels: default
Static routes

Route name	Destination prefix	Next hop IP

Bypass Next Hop IP for workloads within this VNet: Yes [✓ No]
Propagate static route: [✓ Yes] No

The VNet hosting Virtual Edge should not have any VNet GWs.

4. If you have several applications hosted in single or Multiple Child VNets, repeat Step 3 for all Child VNets with relevant details. Each VNet that requires to be connected to the Virtual WAN Hub will need have Virtual Network connections configured.
5. On the Virtual WAN Hub page created in Step 2, click **BGP Peers** from the **Routing** dropdown then click **Add**.
   a. Add a name.
   b. Allocate a Virtual Edge BGP **ASN**.
   c. Add the IP Address. This is the IP of the Virtual Edge LAN Interface (Edge GE3LANIP) which you have allocated in the provisioning template in Section 4.1.2.3.
   d. Select **Virtual Network connection** to the **Virtual Edge VNET** from the dropdown menu.
   e. Click **Add**.
6. Navigate to **Routing** > **BGP Peers** section to see the Azure BGP details which are automatically assigned. For example, in the following image, ASN 65515 and IP 10.20.0.68, 10.20.0.69 are assigned for Azure end.


Home > Velo_vWAN_CloudConnect | Hubs > Velo_vWAN_UK_HuB
Velo_vWAN_UK_HuB | BGP Peers
Virtual HUB
Search
Add
Refresh
Overview
Connectivity
Routing
Route Maps (Preview)
Routing Intent and Routing Policies
BGP Peers
Essentials
Add BGP Peer

Name : Velo_vWAN_UK_HuB
Location : UK South

ASN : 65515
IP : 10.20.0.68,10.20.0.69

Name	ASN	IPv4 Address	Virtual Network connect
Azure_Edge1_BGP	65201	10.100.3.20	Velo_vWAN_UK_HuB/Virt

Name * : Azure_Edge2_BGP
ASN * : 65202
IPv4 Address * : 10.100.3.22
Virtual Network connection * : VirtualNetworkConnectionHubVelocloud

7. Send the following BGP connectivity details to Vodafone so that Azure BGP neighbours can be configured in VMware SD-WAN Orchestrator.
   ○ Azure end ASN & IP addresses,
   ○ Virtual Edge ASN & IP address.

Once you have completed the steps, it is recommended to verify your deployment. To do so, see 'Verifying your Virtual Edges Deployment' on page 39.

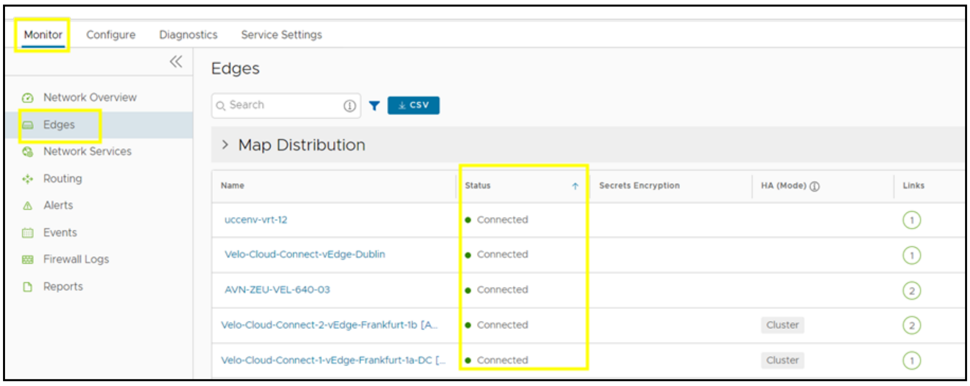
Chapter 4: Verifying your Virtual Edges Deployment

This section can be used to check if all the configurations in previous sections are valid, and the relevant services functioning as expected.

Verifications in VMware SD-WAN Orchestrator

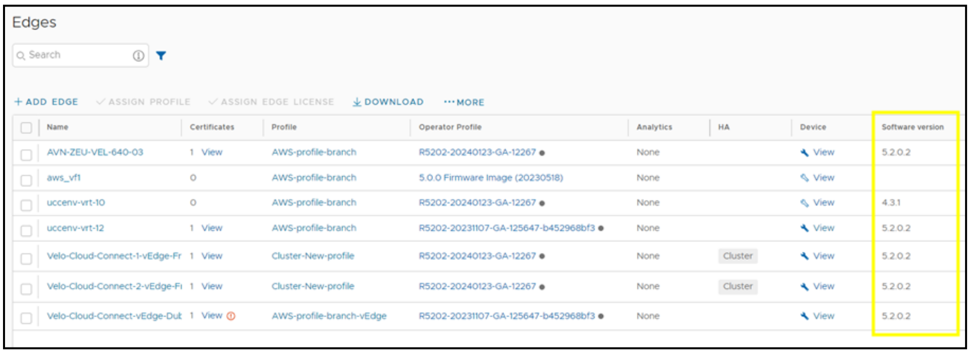
Perform these verifications in VMware SD-WAN Orchestrator for Virtual Edges deployed in AWS or Azure:

1. To check if the Virtual Edges are connected, navigate to **Monitor** > **Edges**:



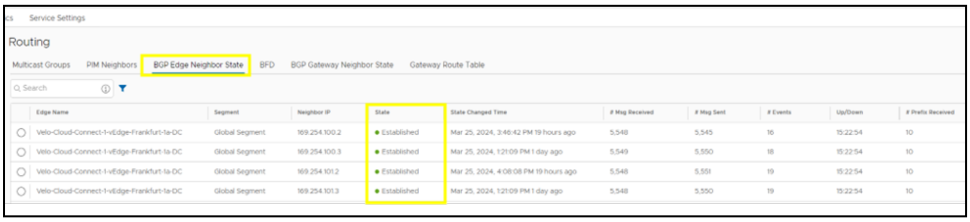
Name	Status	Secrets Encryption	HA (Mode)	Links
uccenv-vrt-12	● Connected			1
Velo-Cloud-Connect-vEdge-Dublin	● Connected			1
AVN-ZEU-VEL-640-03	● Connected			2
Velo-Cloud-Connect-2-vEdge-Frankfurt-1b [A...	● Connected		Cluster	2
Velo-Cloud-Connect-1-vEdge-Frankfurt-1a-DC [...	● Connected		Cluster	1

2. To check if the Virtual Edges' Software Version is 5.2.x.x or above, navigate to **Configure** > **Edges**. Note that GRE/BGP do not work on Edges with Software Version below 5.2.x.x.



□	Name	Certificates	Profile	Operator Profile	Analytics	HA	Device	Software version
□	AVN-ZEU-VEL-640-03	1 View	AWS-profile-branch	R5202-20240123-GA-12267 ●	None		View	5.2.0.2
□	aws_vf1	0	AWS-profile-branch	5.0.0 Firmware Image (20230518)	None		View	
□	uccenv-vrt-10	0	AWS-profile-branch	R5202-20240123-GA-12267 ●	None		View	4.3.1
□	uccenv-vrt-12	1 View	AWS-profile-branch	R5202-20231107-GA-125647-b452968bf3 ●	None		View	5.2.0.2
□	Velo-Cloud-Connect-1-vEdge-Fr	1 View	Cluster-New-profile	R5202-20240123-GA-12267 ●	None	Cluster	View	5.2.0.2
□	Velo-Cloud-Connect-2-vEdge-Fi	1 View	Cluster-New-profile	R5202-20240123-GA-12267 ●	None	Cluster	View	5.2.0.2
□	Velo-Cloud-Connect-vEdge-Dut	1 View ⓘ	AWS-profile-branch-vEdge	R5202-20231107-GA-125647-b452968bf3 ●	None		View	5.2.0.2

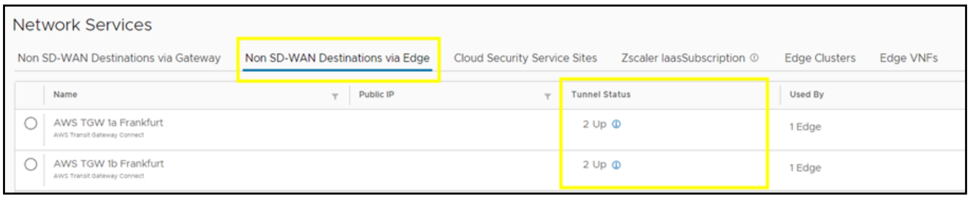
3. To check all BGP are functioning, navigate to **Monitor** > **Routing** > **BGP Edge Neighbor State**.



	Edge Name	Segment	Neighbor IP	State	State Changed Time	# Msg Received	# Msg Sent	# Events	Up/Down	# Prefix Received
○	Velo-Cloud-Connect-1-vEdge-Frankfurt-1a-DC	Global Segment	169.254.100.2	● Established	Mar 25, 2024, 3:46:42 PM 19 hours ago	5,548	5,545	16	15:22:54	10
○	Velo-Cloud-Connect-1-vEdge-Frankfurt-1a-DC	Global Segment	169.254.100.3	● Established	Mar 25, 2024, 1:21:09 PM 1 day ago	5,549	5,550	18	15:22:54	10
○	Velo-Cloud-Connect-1-vEdge-Frankfurt-1a-DC	Global Segment	169.254.101.2	● Established	Mar 25, 2024, 4:08:08 PM 19 hours ago	5,548	5,551	19	15:22:54	10
○	Velo-Cloud-Connect-1-vEdge-Frankfurt-1a-DC	Global Segment	169.254.101.3	● Established	Mar 25, 2024, 1:21:09 PM 1 day ago	5,548	5,550	19	15:22:54	10

4. To verify the tunnels' status, navigate to **Monitor** > **Network Services** > **Non SD-WAN**

Destinations via Edge:



Network Services

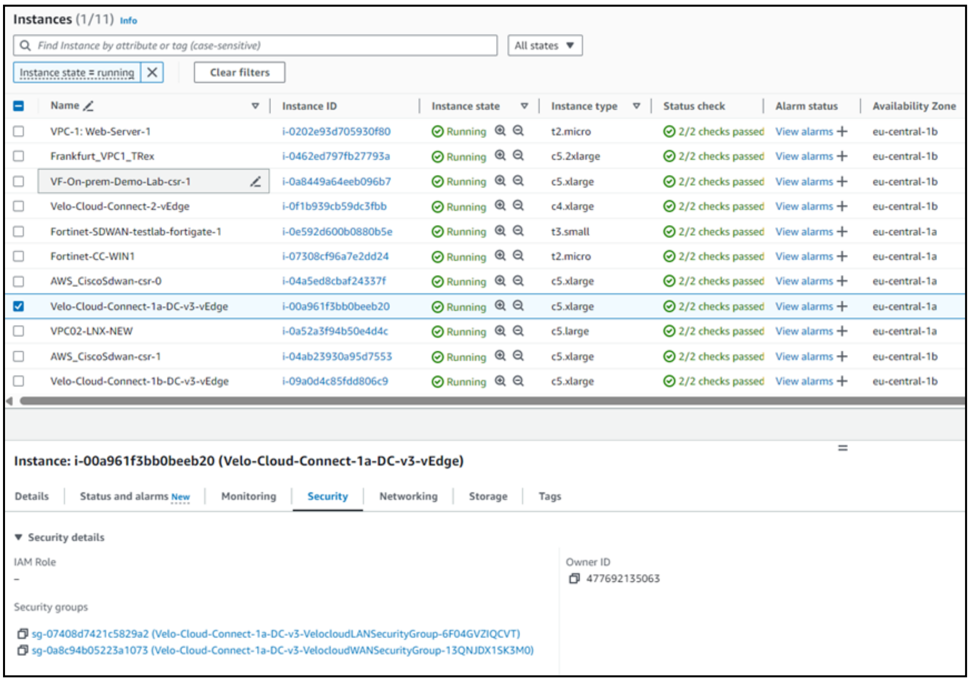
Non SD-WAN Destinations via Gateway | Non SD-WAN Destinations via Edge | Cloud Security Service Sites | Zscaler IaasSubscription | Edge Clusters | Edge VNFs

	Name	Public IP	Tunnel Status	Used By
○	AWS TGW 1a Frankfurt AWS Transit Gateway Connect		2 Up	1 Edge
○	AWS TGW 1b Frankfurt AWS Transit Gateway Connect		2 Up	1 Edge

Verifications in AWS Management Console

Perform the following verifications in your AWS Management Console for Virtual Edges deployed in Amazon Web Services (AWS).

1. To check if the Virtual Edge is running and the right configurations are applied (such as Instance Type, Security, Networking, and others), go to the Amazon EC2 service and then select the instance type that has the Virtual Edge.



Instances (1/11) Info

Find Instance by attribute or tag (case-sensitive) | All states

Instance state = running | Clear filters

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
□	VPC-1: Web-Server-1	i-0202e93d705930f80	Running	t2.micro	2/2 checks passed	View alarms	eu-central-1b
□	Frankfurt_VPC1_TRex	i-0462ed797fb27793a	Running	c5.2xlarge	2/2 checks passed	View alarms	eu-central-1b
□	VF-On-prem-Demo-Lab-csr-1	i-0a8449a64eeb096b7	Running	c5.xlarge	2/2 checks passed	View alarms	eu-central-1b
□	Velo-Cloud-Connect-2-vEdge	i-0f1b939cb59dc3fbb	Running	c4.xlarge	2/2 checks passed	View alarms	eu-central-1b
□	Fortinet-SDWAN-testlab-fortigate-1	i-0e592d600b0880b5e	Running	t3.small	2/2 checks passed	View alarms	eu-central-1a
□	Fortinet-CC-WIN1	i-07308cf96a7e2dd24	Running	t2.micro	2/2 checks passed	View alarms	eu-central-1a
□	AWS_CiscoSdwan-csr-0	i-04a5ed8cbaf24337f	Running	c5.xlarge	2/2 checks passed	View alarms	eu-central-1a
☑	Velo-Cloud-Connect-1a-DC-v3-vEdge	i-00a961f3bb0beeb20	Running	c5.xlarge	2/2 checks passed	View alarms	eu-central-1a
□	VPC02-LNX-NEW	i-0a52a3f94b50e4d4c	Running	c5.large	2/2 checks passed	View alarms	eu-central-1a
□	AWS_CiscoSdwan-csr-1	i-04ab23930a95d7553	Running	c5.xlarge	2/2 checks passed	View alarms	eu-central-1b
□	Velo-Cloud-Connect-1b-DC-v3-vEdge	i-09a0d4c85fdd806c9	Running	c5.xlarge	2/2 checks passed	View alarms	eu-central-1b

Instance: i-00a961f3bb0beeb20 (Velo-Cloud-Connect-1a-DC-v3-vEdge)

Details | Status and alarms New | Monitoring | Security | Networking | Storage | Tags

▼ Security details

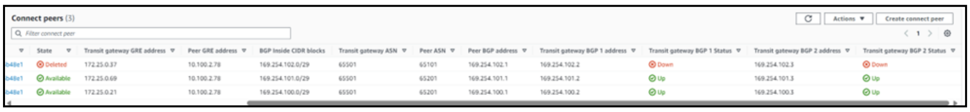
IAM Role
–

Owner ID
477692135063

Security groups

sg-07408d7421c5829a2 (Velo-Cloud-Connect-1a-DC-v3-VelocloudLANSecurityGroup-6F04GVZIQCVT)
sg-0a8c94b05223a1073 (Velo-Cloud-Connect-1a-DC-v3-VelocloudWANSecurityGroup-13QNJDX1SK3M0)

2. To check BGP status, navigate to the Transit Gateway Attachment service for the connect attachments, then click on **Connect peers** and scroll to view the columns on the right:



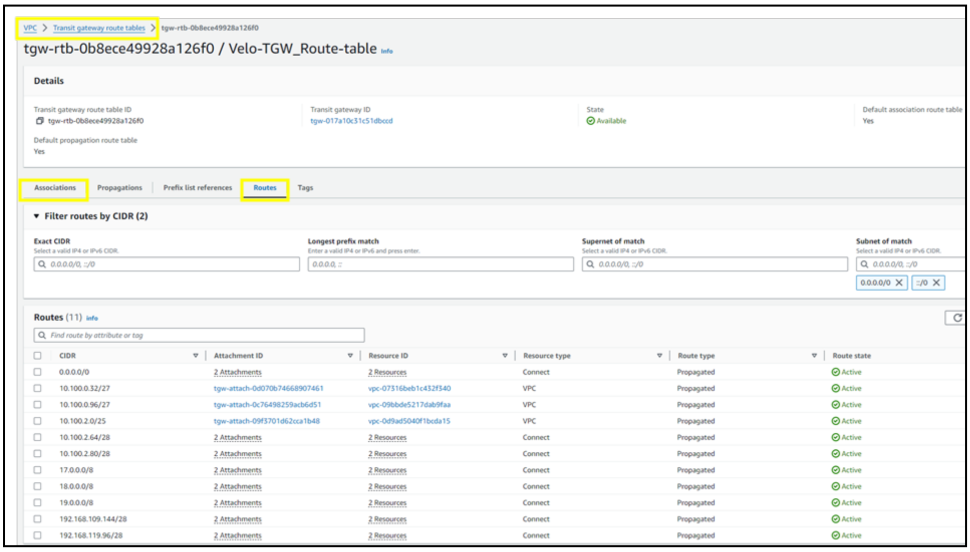
Connect peers (3)

Filter connect peer

Actions | Create connect peer

	State	Transit gateway GRE address	Peer GRE address	BGP Inside CIDR blocks	Transit gateway ASN	Peer ASN	Peer BGP address	Transit gateway BGP 1 address	Transit gateway BGP 1 Status	Transit gateway BGP 2 address	Transit gateway BGP 2 Status
b48e1	Deleted	172.25.0.37	10.100.2.78	169.254.102.0/29	65501	65101	169.254.102.1	169.254.102.2	Down	169.254.102.3	Down
b48e1	Available	172.25.0.69	10.100.2.78	169.254.101.0/29	65501	65201	169.254.101.1	169.254.101.2	Up	169.254.101.3	Up
b48e1	Available	172.25.0.21	10.100.2.78	169.254.100.0/29	65501	65201	169.254.100.1	169.254.100.2	Up	169.254.100.3	Up

3. To check if the Transit Gateway is getting all the VPC and connect attachment routes, go to **Transit Gateway** (VPC feature) then click on the **Transit Gateway ID**. In the next screen select the **Association** route table ID and then click on **Association** or click on **Routes**.



VPC > Transit gateway route tables > tgw-rtb-0b8ece49928a126f0

tgw-rtb-0b8ece49928a126f0 / Velo-TGW_Route-table Info

Details

Transit gateway route table ID: tgw-rtb-0b8ece49928a126f0

Transit gateway ID: tgw-017a10c31c51dbccd

State: Available

Default association route table: Yes

Default propagation route table: Yes

Associations
Propagations
Prefix list references
Routes
Tags

▼ Filter routes by CIDR (2)

Exact CIDR: Select a valid IP4 or IPv6 CIDR. 0.0.0.0/0, ::/0

Longest prefix match: Enter a valid IP4 or IPv6 and press enter. 0.0.0.0, ::

Supernet of match: Select a valid IP4 or IPv6 CIDR. 0.0.0.0/0, ::/0

Subnet of match: Select a valid IP4 or IPv6 CIDR. 0.0.0.0/0, ::/0 — 0.0.0.0/0 ✕ ::/0 ✕

Routes (11) info

Find route by attribute or tag

□	CIDR	Attachment ID	Resource ID	Resource type	Route type	Route state
□	0.0.0.0/0	2 Attachments	2 Resources	Connect	Propagated	✓ Active
□	10.100.0.32/27	tgw-attach-0d070b74668907461	vpc-07316beb1c432f340	VPC	Propagated	✓ Active
□	10.100.0.96/27	tgw-attach-0c76498259acb6d51	vpc-09bbde5217dab9faa	VPC	Propagated	✓ Active
□	10.100.2.0/25	tgw-attach-09f3701d62cca1b48	vpc-0d9ad5040f1bcda15	VPC	Propagated	✓ Active
□	10.100.2.64/28	2 Attachments	2 Resources	Connect	Propagated	✓ Active
□	10.100.2.80/28	2 Attachments	2 Resources	Connect	Propagated	✓ Active
□	17.0.0.0/8	2 Attachments	2 Resources	Connect	Propagated	✓ Active
□	18.0.0.0/8	2 Attachments	2 Resources	Connect	Propagated	✓ Active
□	19.0.0.0/8	2 Attachments	2 Resources	Connect	Propagated	✓ Active
□	192.168.109.144/28	2 Attachments	2 Resources	Connect	Propagated	✓ Active
□	192.168.119.96/28	2 Attachments	2 Resources	Connect	Propagated	✓ Active

Chapter 5: Glossary

A

ASN

An Autonomous System Number (ASN) is a globally unique number which enables a group of networks to be identified over the internet and exchange routing data with other networks.

AZ

Availability Zones (AZ) consist of one or more discrete data centers, each with redundant power, networking, and connectivity, and housed in separate facilities.

B

BGP

To enable access between your VMs and the outside world, you can configure an external or internal Border Gateway Protocol (BGP) connection between a gateway and a router in your physical infrastructure.

C

CIDR

Classless Inter-Domain Routing (CIDR) is a method for allocating IP addresses for IP routing.

G

GRE

Generic Routing Encapsulation (GRE) tunnels can be added to gateways to connect on-premises and cloud networks.

N

NAT

Network address translation (NAT) is a method of mapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.

S

S3

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance.

Subnet

A subnet, or subnetwork, is a network inside a network.

V

VCO

An acronym that refers to VMware SD-WAN Orchestrator.

VM

A Virtual Machine (VM) is a compute resource that uses software instead of a physical computer to run programs and deploy apps. One or more virtual “guest” machines run on a physical “host” machine.

VNet

A Virtual Network (VNet) in Azure is the primary building block for private networks within the cloud, analogous to AWS's Virtual Private Cloud (VPC)

VPC

Virtual Private Cloud (VPC) is a secure, isolated private cloud hosted within a public cloud.