VMware SD-WAN By VeloCloud

Orange Flexible Engine (FE) Virtual Edge Deployment Guide

Version beta 1.0

Overview

More customers are moving workload to Public Cloud infrastructure and expect to extend SD- WAN from remote sites to public cloud to guarantee SLA. There are multiple options offered by VeloCloud, leveraging distributed VCGs to establish IPSec towards public cloud private network or deploy virtual edge directly in Orange's Flexible Engine (FE). This document focus on how to deploy virtual edge on FE.

For small branch deployment that demand throughput less than 1G, single virtual edge can be deployed in the private network (FE VPC). For larger data center deployments that demand multi-gigabit throughput, hub clustering can be deployed.

Note: In the VeloCloud hub clustering design, we leverage a Layer 3 Instance on the LAN side to run BGP between hubs in the cluster and the Layer 3 Instance for route distribution in LAN. Since the FE VPC Router doesn't support dynamic routing protocol, a third-party virtual router is required in the FE infrastructure in case of a clustering deployment. This setup is not covered in this document, please get in touch with your dedicated VeloCloud point of contact to know more about this design option.

Table of Contents

Flexible Engine virtual VCE deployment Overview

CAUTION: Make sure to review and understand this document before deploying. This is intended as a reference and may need to be altered to accommodate specific environments.

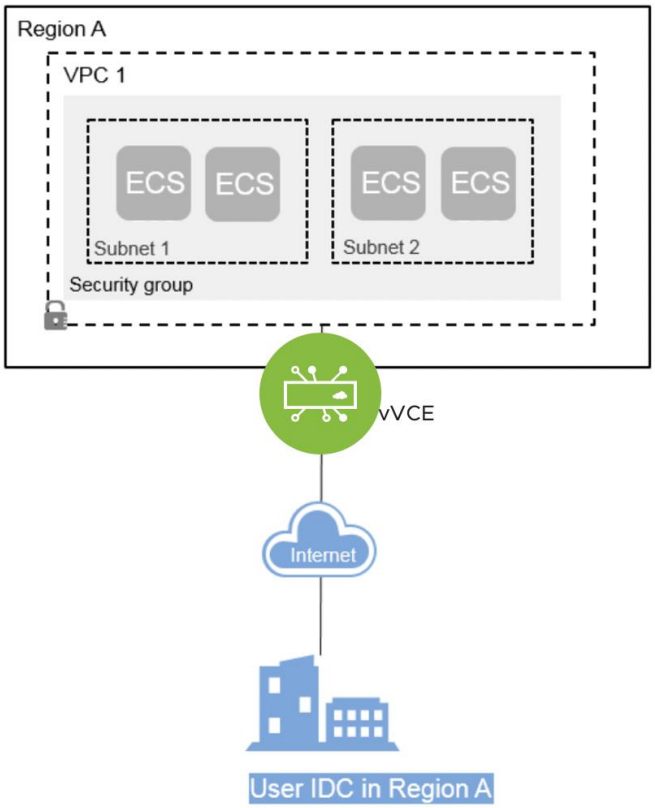
Prerequisite

The following are needed before you start:

1. FE account and login information
2. Familiarity with FE networking concepts (see: https://docs.prod-cloud-ocb.orange-business.com/en-us/vpc/index.html)
3. RSA Public Key (see: https://docs.prod-cloud-ocb.orange-business.com/en-us/ac/index.html)
4. VeloCloud Cloud-init template (given in the next section)
5. VCO target and admin account to login

Deploying Virtual Edge on FE

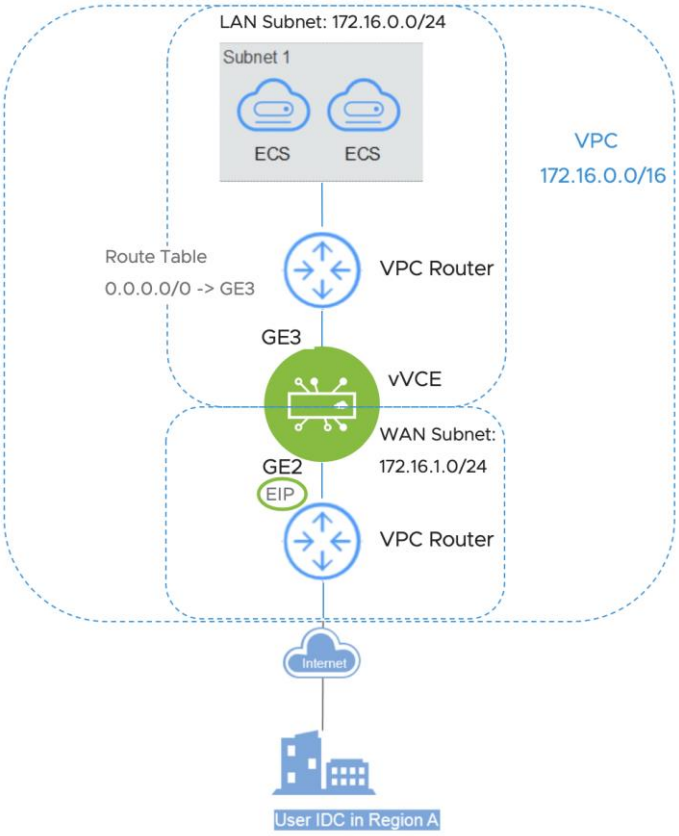
The default VeloCloud vVCE template that will be built is to achieve a common deployment within FE representative of the basic topology illustrated here:



In order to deploy a new VCE, it will be necessary to retrieve from the VCO where the site will be configured an activation key. This activation key is a One Time Password that is used to secure the onboarding of a new site. This key is retrieved driectly from the VCO and will need to be pushed to the VCE at its creation via the CLOUD- INIT process. How to create the initial vVCE template and retrieve the activation will be explained in the next section.

Basic Topology

In this example, the FE VPC (172.16.0.0/16) is divided into a Public subnet (172.16.0.x/24) and a Private subnet (172.16.1.x/24). The Virtual Edge routes between the two subnets. The VPC Router will forward all offnet traffic to the Internet Gateway. The VPC Router in the Private subnet will forward all traffic to the LAN facing interface on the Virtual Edge (GE3). In this example, a default route is used to forward "ALL" traffic from the workloads but is not necessary. RFC1918 summarization or specific branch/hub prefixes can be used to narrow what is sent to the Virtual Edge. For example, if the workloads in the Private Subnet still need to be accessible via SSH from publicly sourced IPs then the VPC Router could be configured to point the default route (0.0.0.0/0) to Internet Gateway and RFC1918 summarization to Virtual Edge.

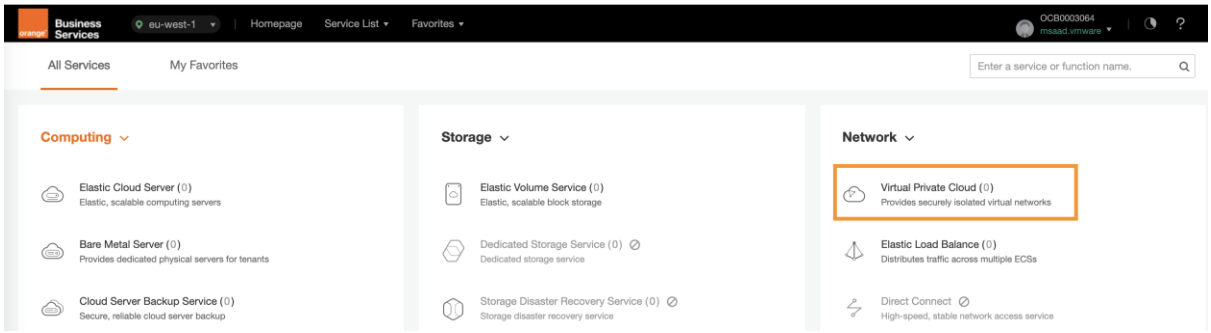


To get access to the outside world, an Elastic IP (EIP) will be tied to the WAN interface of the VCE. An EIP is a public IP address statically defined and linked to the WAN interface.

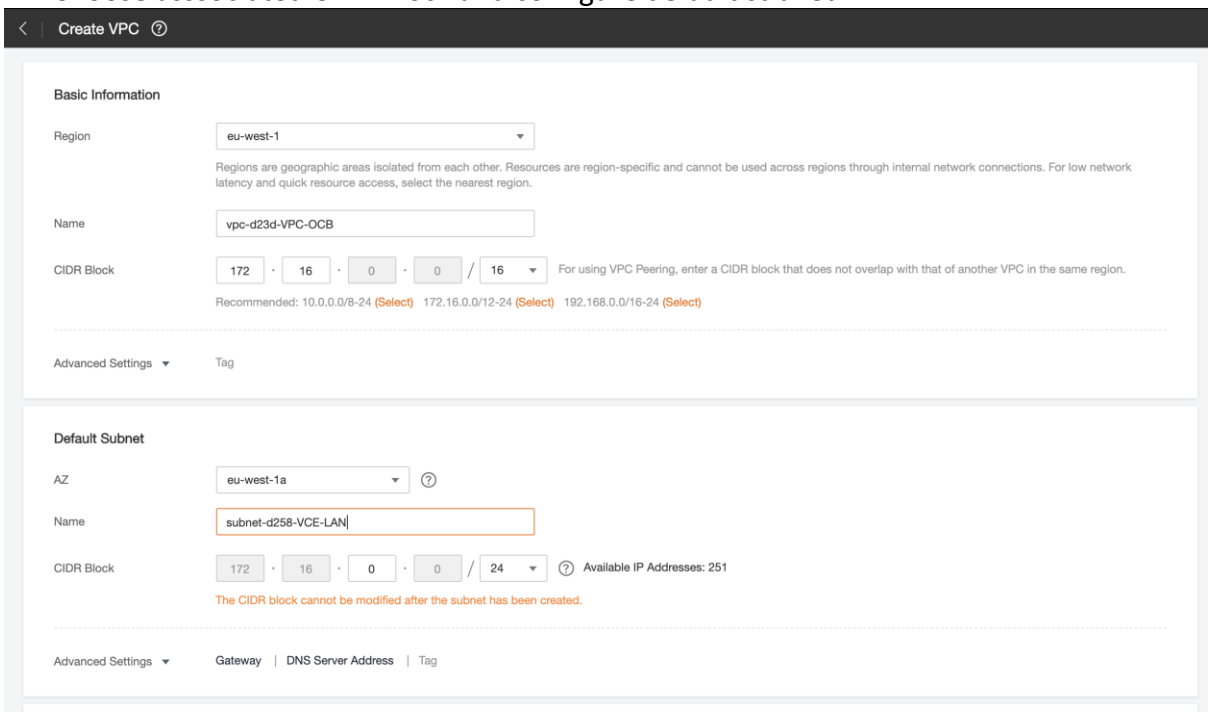
Create VPC

We assume familiarity with the VPC networking concepts of Flexible Engine. If the VPC configuration has not been done (green field), here are the steps to create the VPC and the different subnets:

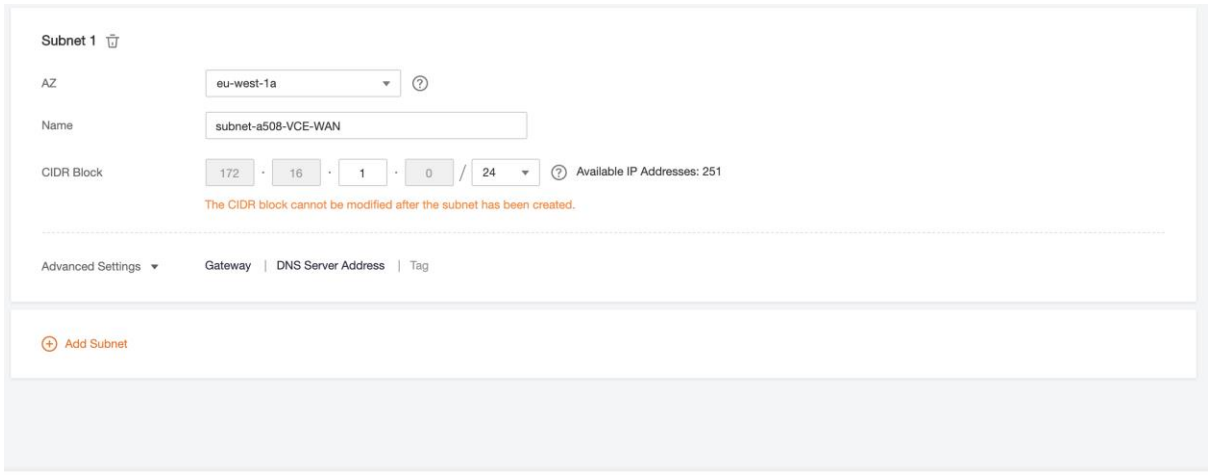
- VPC Creation:



- Choose asssociated CIDR Block and configure default subnet:



- Add another subnet:



And Create Now.

Create Security Group

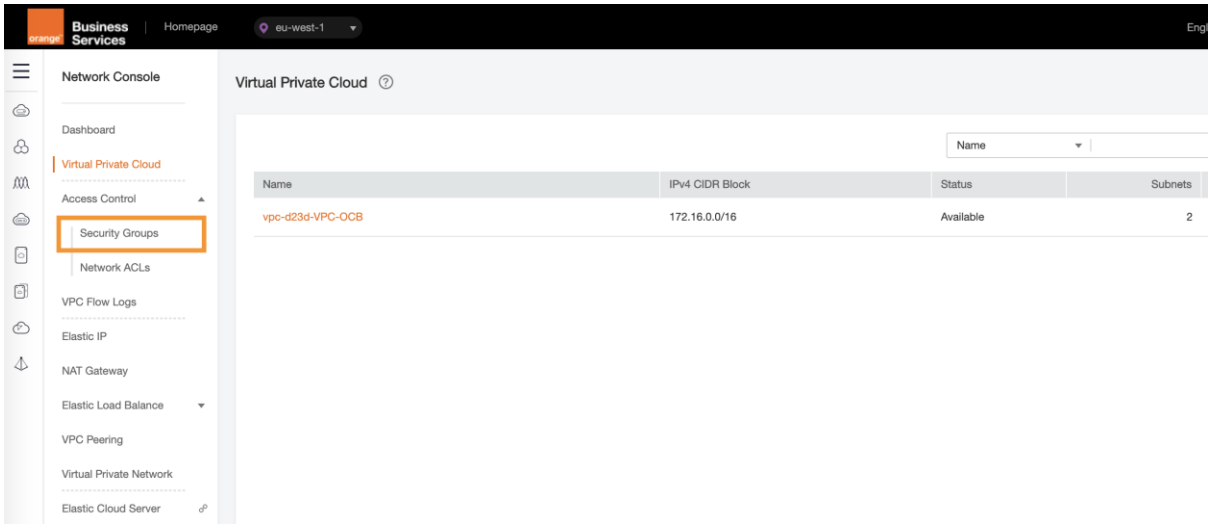
A security group will also need to be created in order to authorize communications from the outside to the VCE. We require the following ports to be allowed at a minimum on the WAN side:

- UDP/2426: for VeloCloud MultiPath Protocol (mandatory)
- TCP/22: for SSH access (optional but recommended for Support Access)
- UDP/161: for SNMP (optional but recommended)

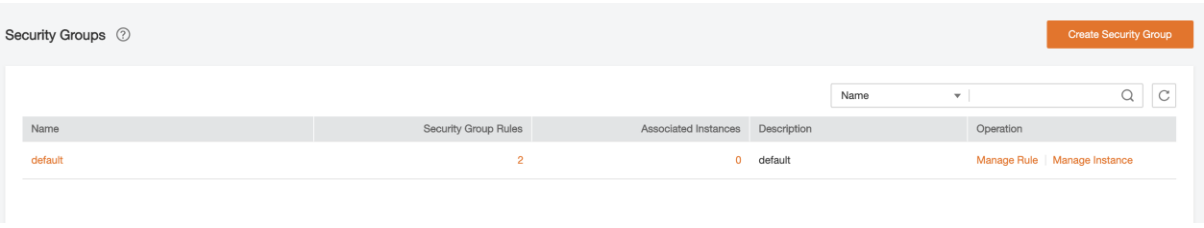
You can add additional protocols after deployment or modify the security groupe template as needed.

Here are the steps to create the security group:

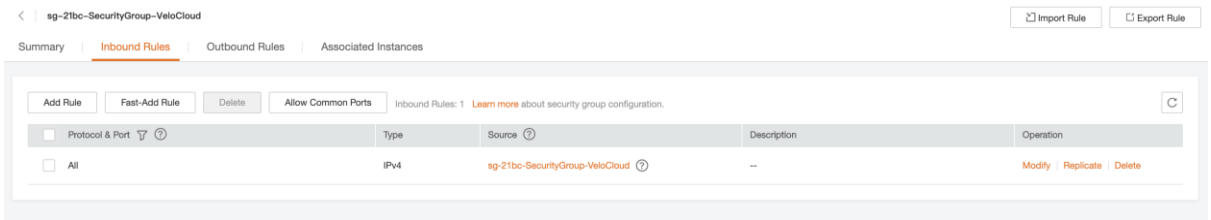
- Navitage to VPC > Access Control > Security Groups



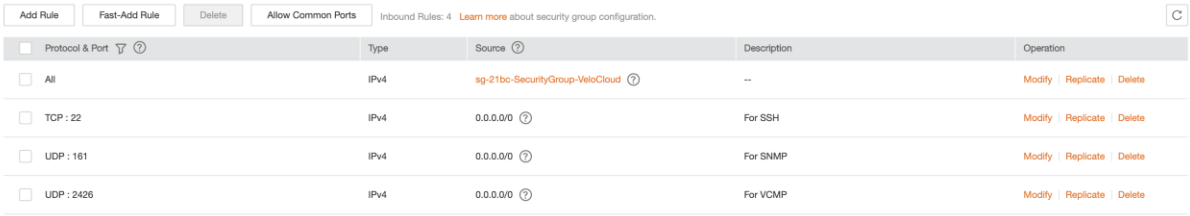
- Create Security Group



- Inbound Rules > Add:



- Input desired rules:



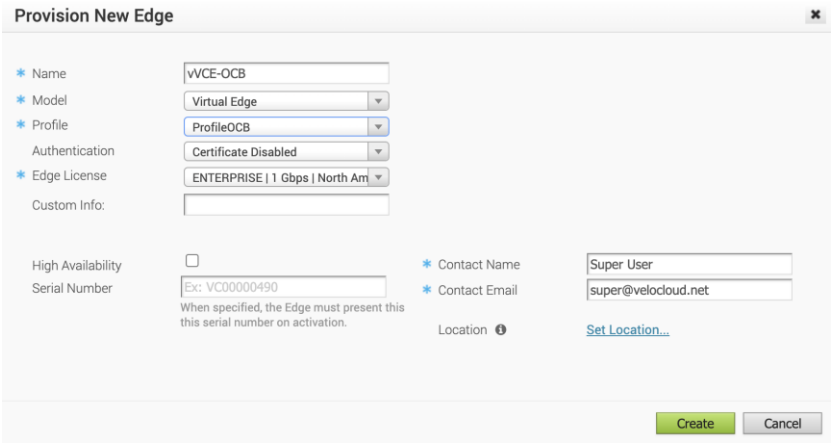
This security group will then be used later during the VCE deployment.

Add Virtual Edge to VeloCloud Orchestrator (VCO)

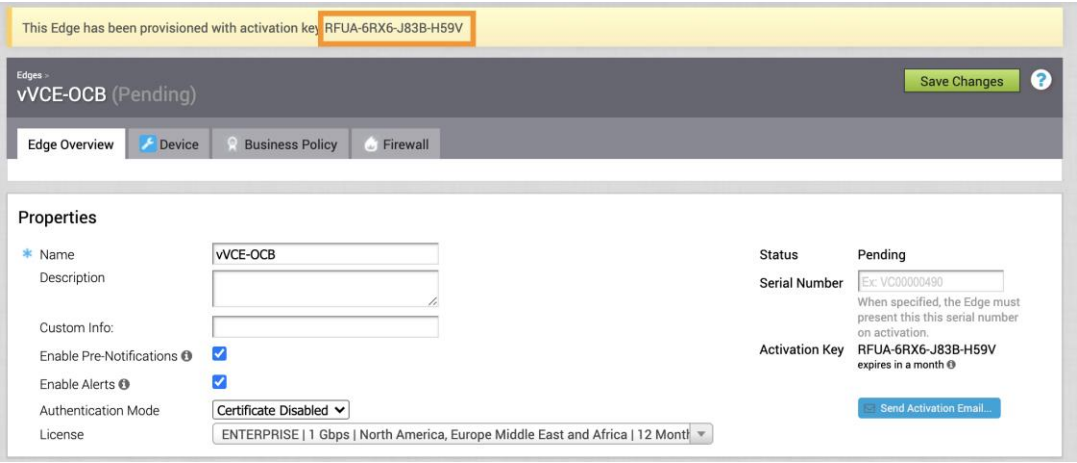
First step is to add the Virtual Edge to the Enterprise. This requires login credentials for the VCO.

Add Virtual Edge to VCO

Then input minimum information:



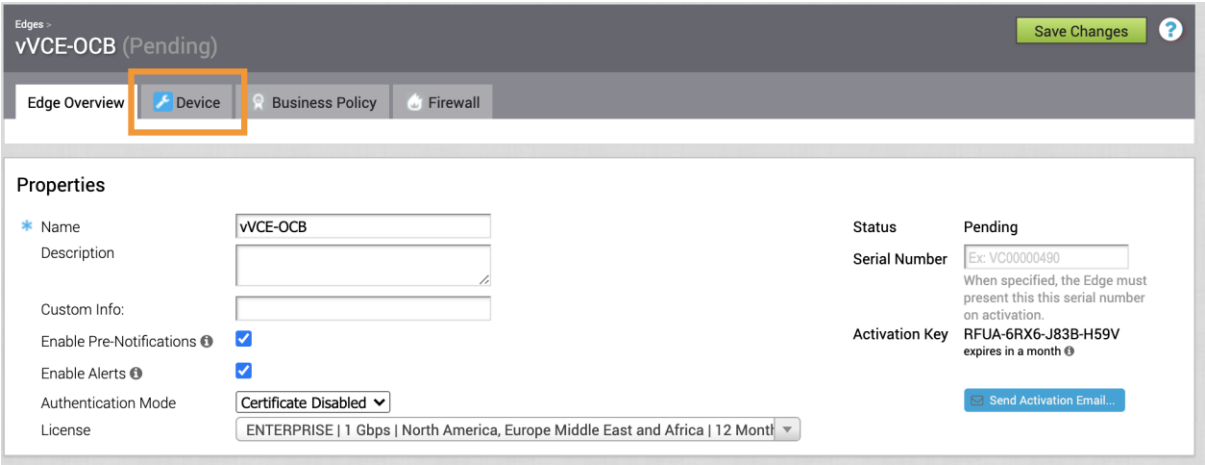
Record Activation Key



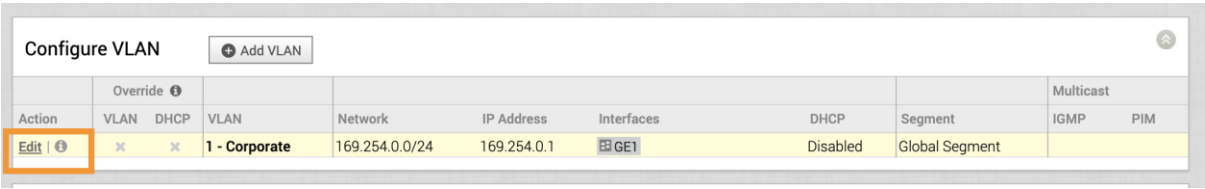
This is the key that will need to be used in the cloud-init file.

Add VLAN IP

The VLAN configuration needs to have an IP address assigned in order to save the Device Settings but will not be used. Click on Device tab:

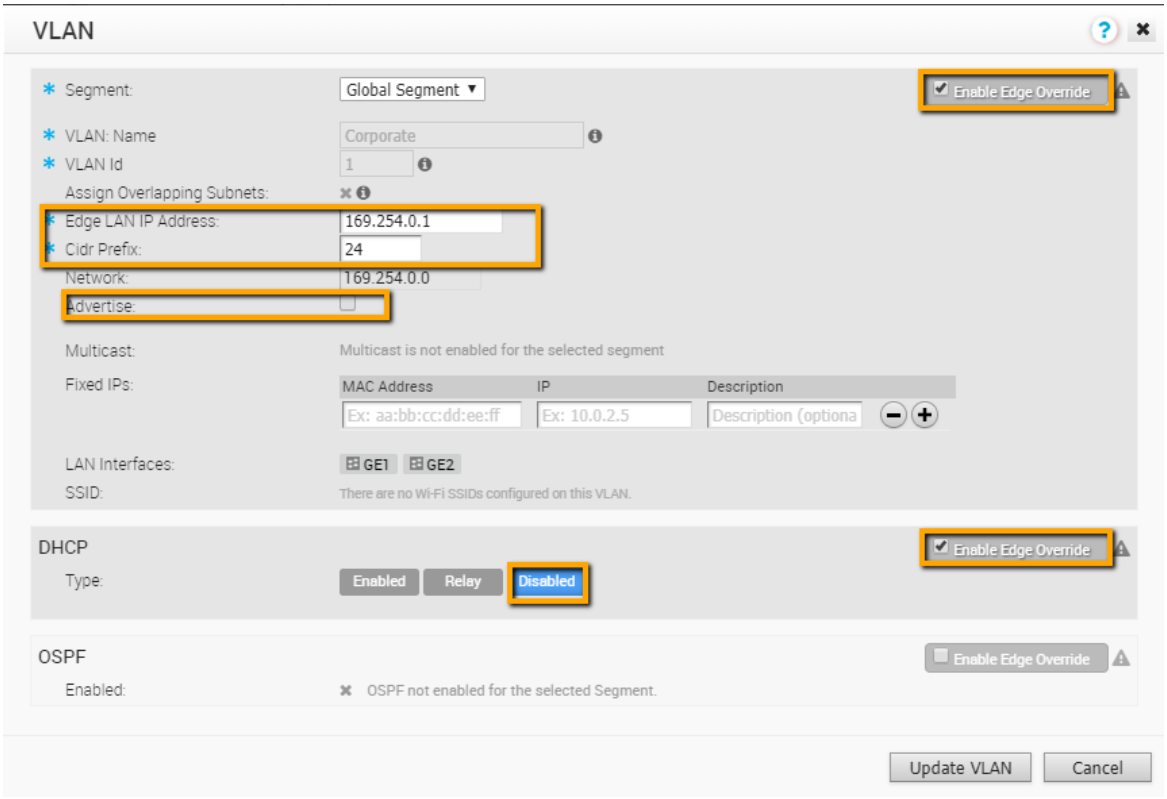


Then on Configure VLAN Section:



- Use: 169.254.0.1 /24
- Advertised: Unchecked

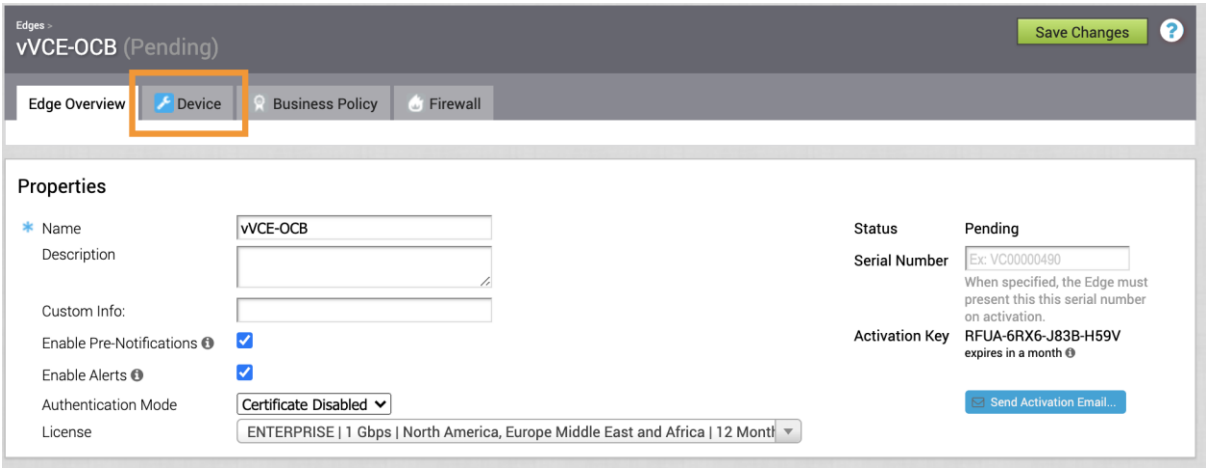
- DHCP: Disabled



Configure Virtual Edge Interfaces

CAUTION: The VCO needs the Device Settings configured first before activation. If this step is missed, the Virtual Edge activates but then goes offline a few minutes later.

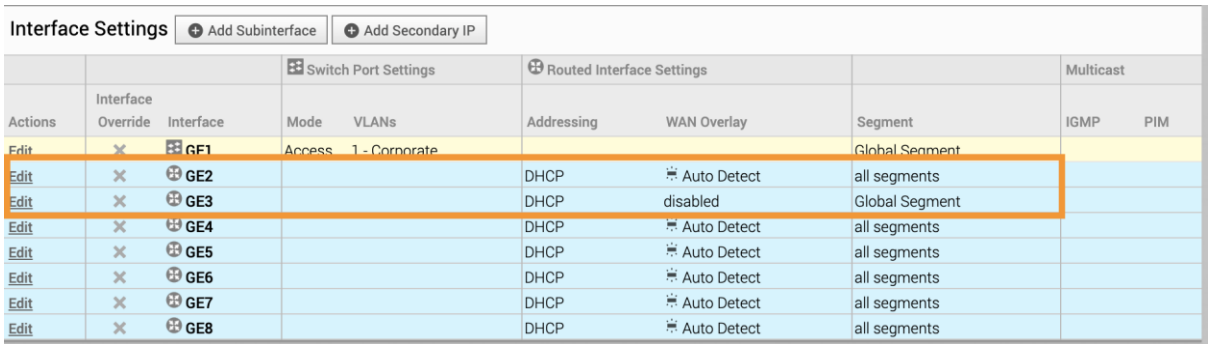
Navigate to the Virtual Edge's Device Settings:



Change the interface settings as follows:

1. Change the **GE2** interface capability from "Switched" to "Routed" and enable DHCP addressing and WAN overlay

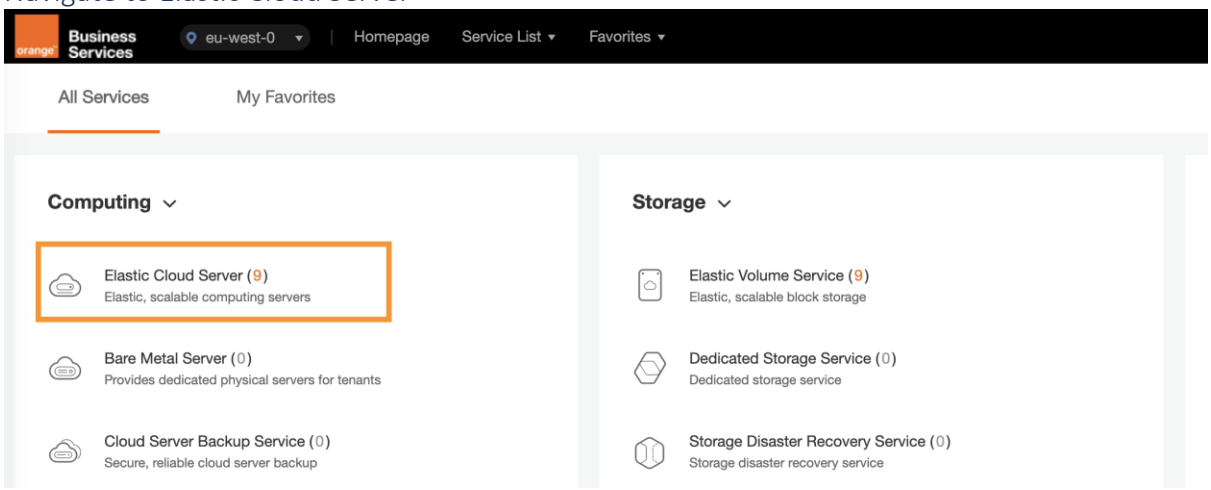
2. In the **GE3** interface, disable WAN overlay as this interface will be used for the LAN-side gateway. Also, disable NAT Direct Traffic



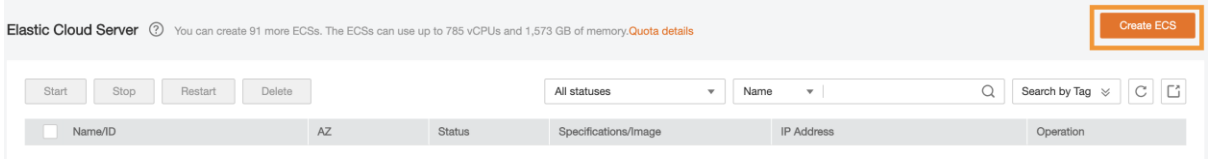
Based on architecutre or needs, you can modify interfaces parameters such as defining a static IP address, modifying interfaces selected, etc.

Deploy Virtual Edge via ECS creation

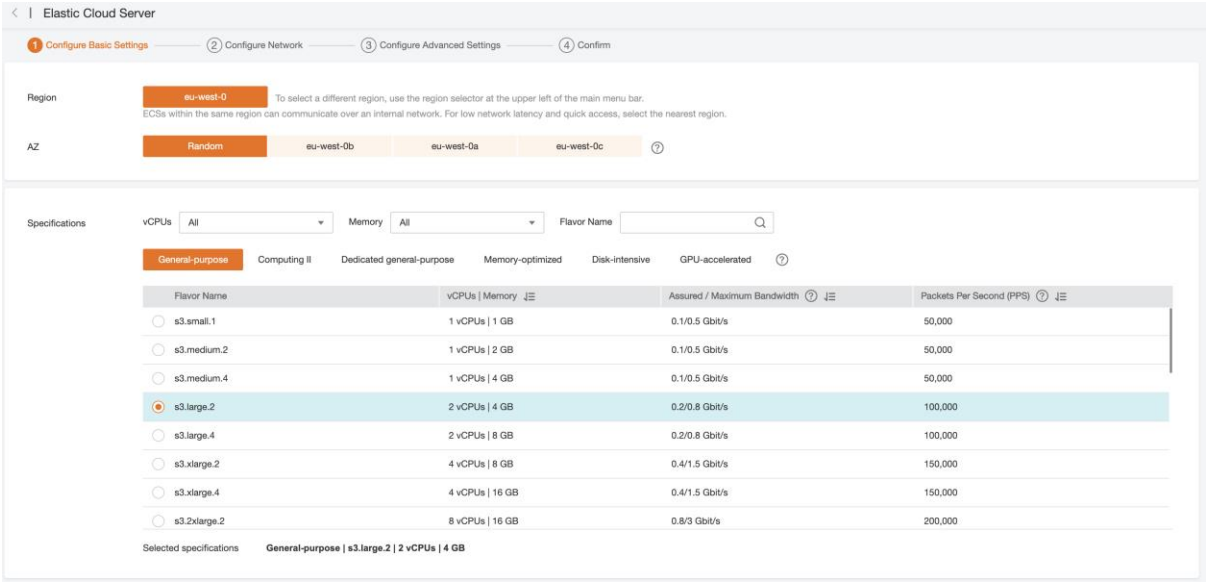
Navigate to Elastic Cloud Server



Create ECS

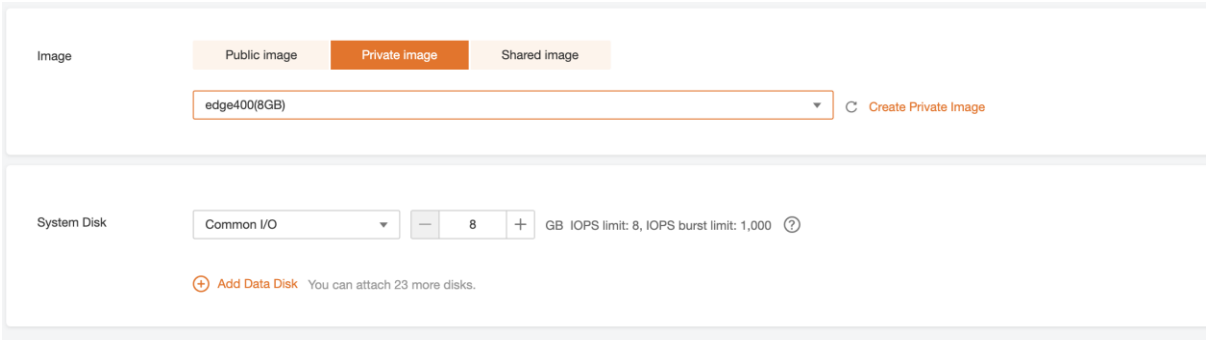


Select Virtual Machine Properties

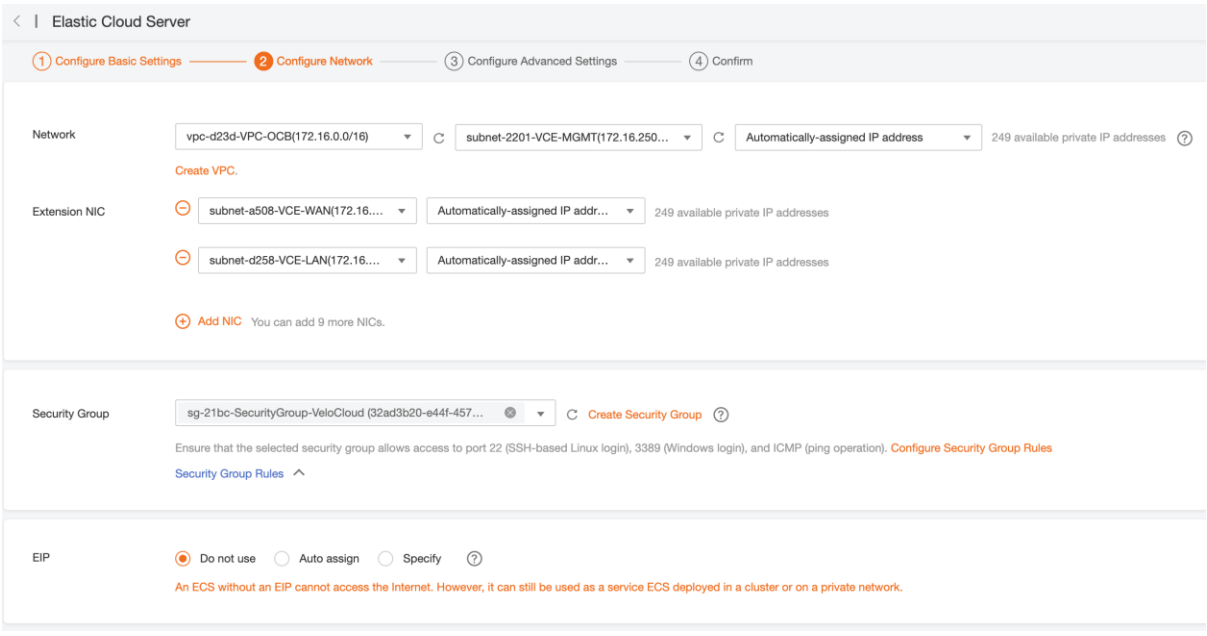


2vCPU and 4 GB of RAM are the minimum specifications supported

Select Image



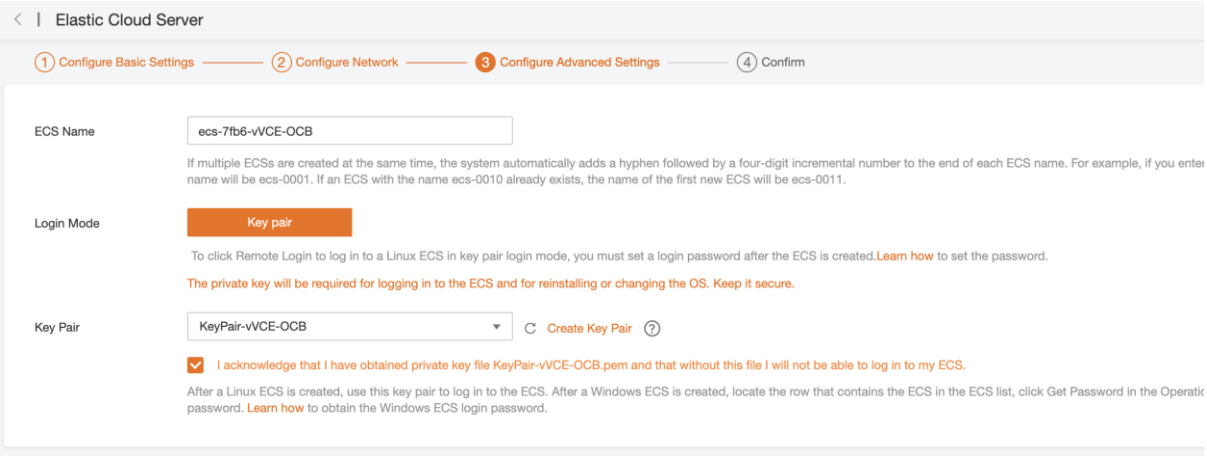
Configure Network Properties



With the following specifications:

- The first interface (eth0 or GE1) is the management interface; this interface will not be used and is tied to a dedicated MGMT subnet even if not used.
- The second interface (eth1 or GE2) is the WAN facing interface;
- The third interface (eth2 or GE3) is the LAN facing interface;
- Select the security group previously created;
- Do not assign an EIP, it will be done later.

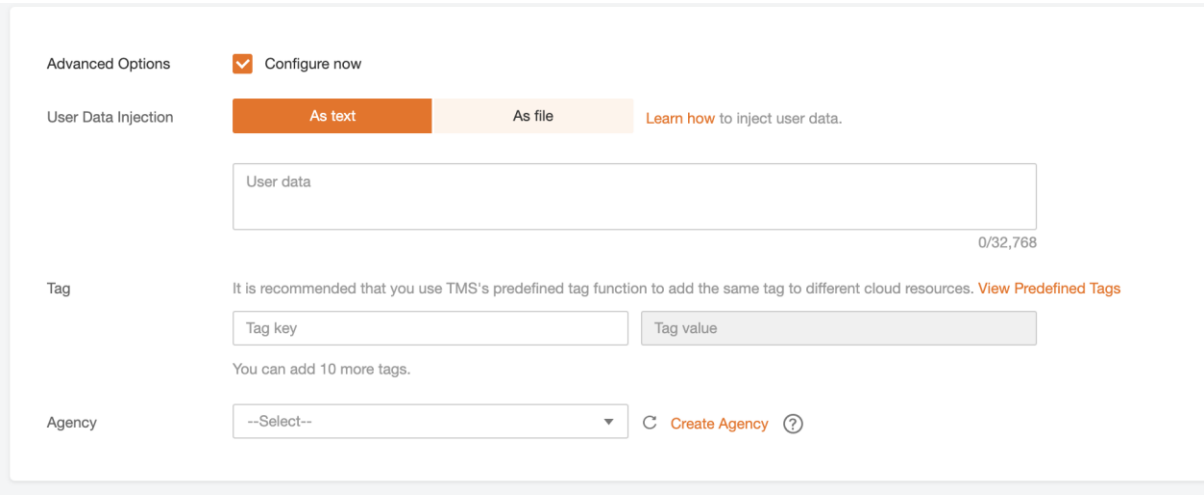
Configure Advanced Settings



If you do not have created a Key Pair previously, you can create it here at the same time.

Configure Cloud-init information

Click on the Advanced Options > Configure Now:



This is where you will input necessary information for the virtual VCE to register itself towards the VCO and take input configuration parameter you choose to include.

This configuration information must be passed following the cloud-init formatting. Cloud-init is a Linux package responsible for handling early initialization of instances. If available in the distributions, it allows for configuration of many common parameters of the instance directly after installation. This creates a fully functional instance that is configured based on a series of inputs. The cloud-init config is composed of two main configuration files, the metadata file and the user-data file. The meta-data contains the network configuration for the Edge, and the user-data contains the Edge Software configuration. The cloud-init file provides information that identifies the instance of the VMware SD-WAN Virtual Edge being installed.

Cloud-init's behavior can be configured via user-data. User-data can be given by the user at the time of launching the instance like we will do here. This file contains three main modules: SD-WAN Orchestrator, Activation Code, and Ignore Certificates Errors.

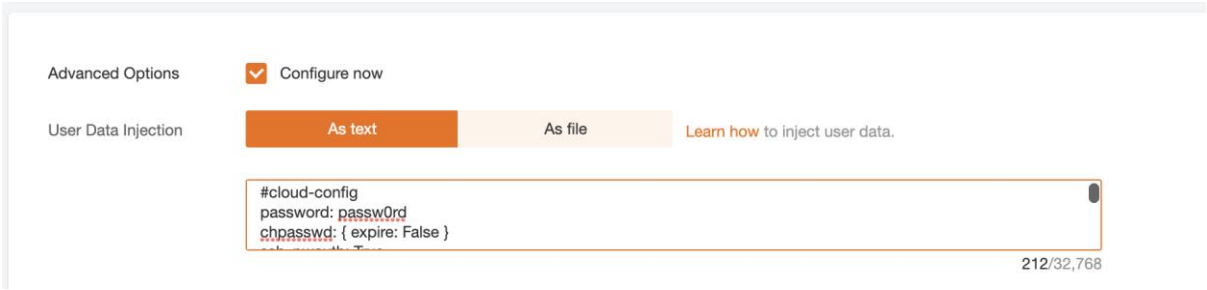
Module	Description
`vco`	IP Address/URL of the SD-WAN Orchestrator.
`activation_code`	Activation code for the Virtual Edge. The activation code is generated while creating an Edge instance on the SD-WAN Orchestrator.
`vco_ignore_cert_errors`	Option to verify or ignore any certificate validity errors.

The activation code is generated while creating an Edge instance on the SD-WAN Orchestrator (see previous steps).

Important There is no default password in SD-WAN Edge image. The password must also be provided in the user-data file.

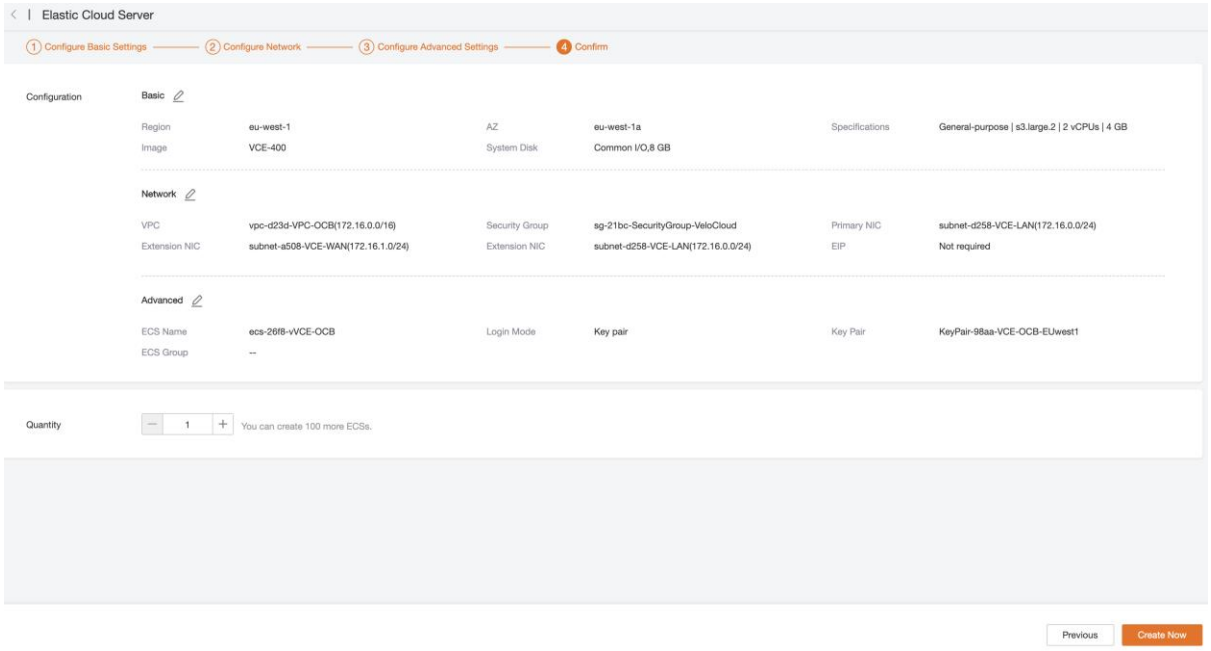
```
#cloud-config
password: passw0rd
chpasswd: { expire: False }
ssh_pwauth: True
velocloud:
  vce:
    vco: 34.208.100.185
    activation_code: RFUA-6RX6-J83B-H59V
    vco_ignore_cert_errors: true
```

You can copy/paste this template into the required field:



Using a file (option on the right) is also possible. In that case you need to put the content into a text file.

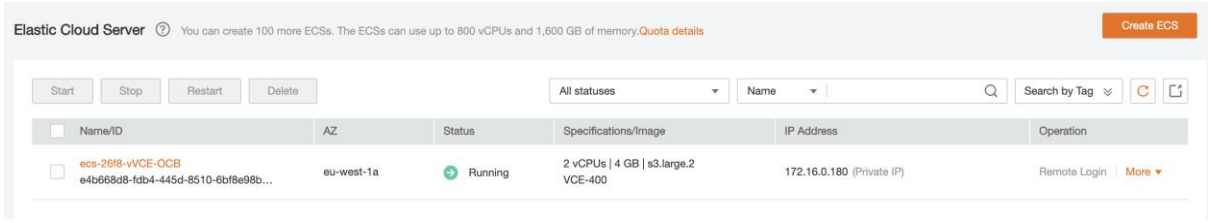
Review and Create ECS



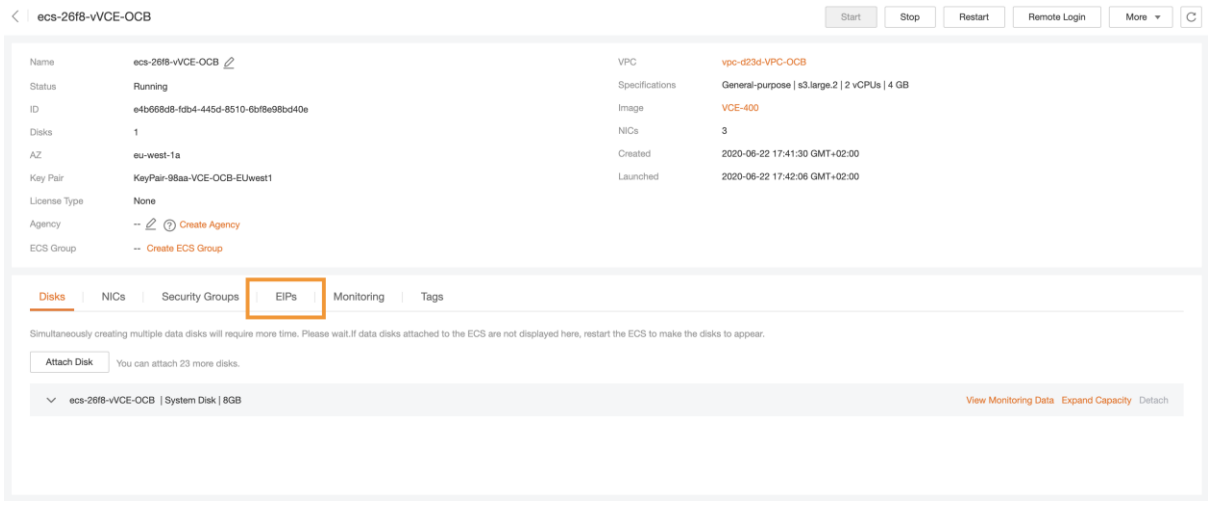
Attach Elastic IP

The next step is to attach an EIP to enable the VCE instance to communicate with the outside. This EIP will be attached to the WAN interface (on subnet 172.16.1.0/24 here).

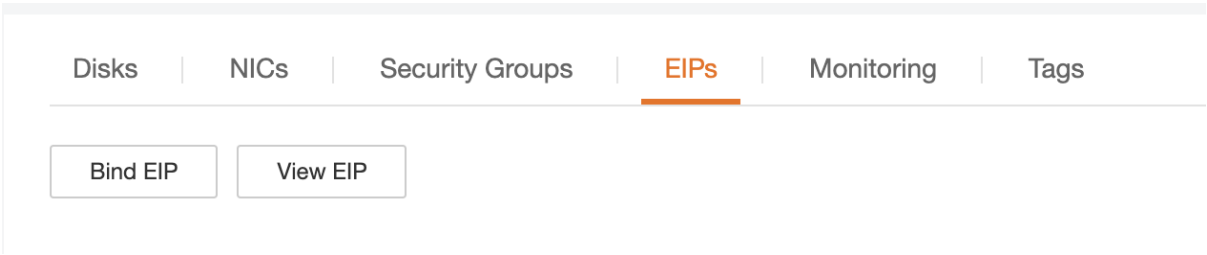
Once the ECS has been created, click on its name:



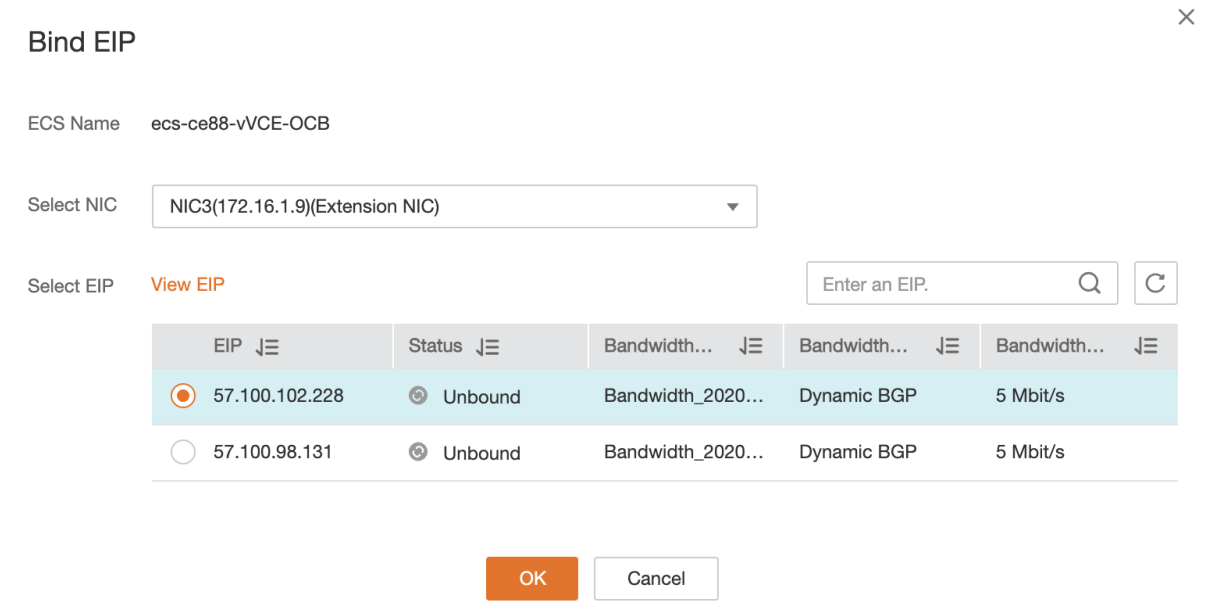
Go to the EIP Section:



Select Bind EIP:



Select an EIP and bind it to NIC2:

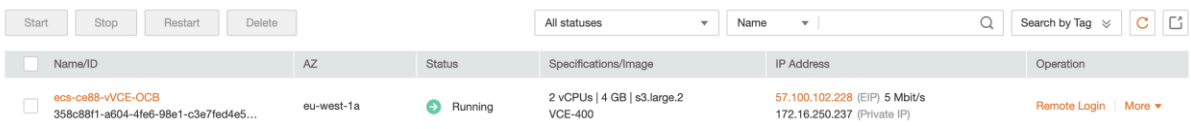


If you have not created any EIP before, you can do it at the same time.

Additional help on EIP creation is available at this location: https://docs.prod-cloud-ocb.orange-business.com/en-us/api/vpc/en-us_topic_0020090596.html

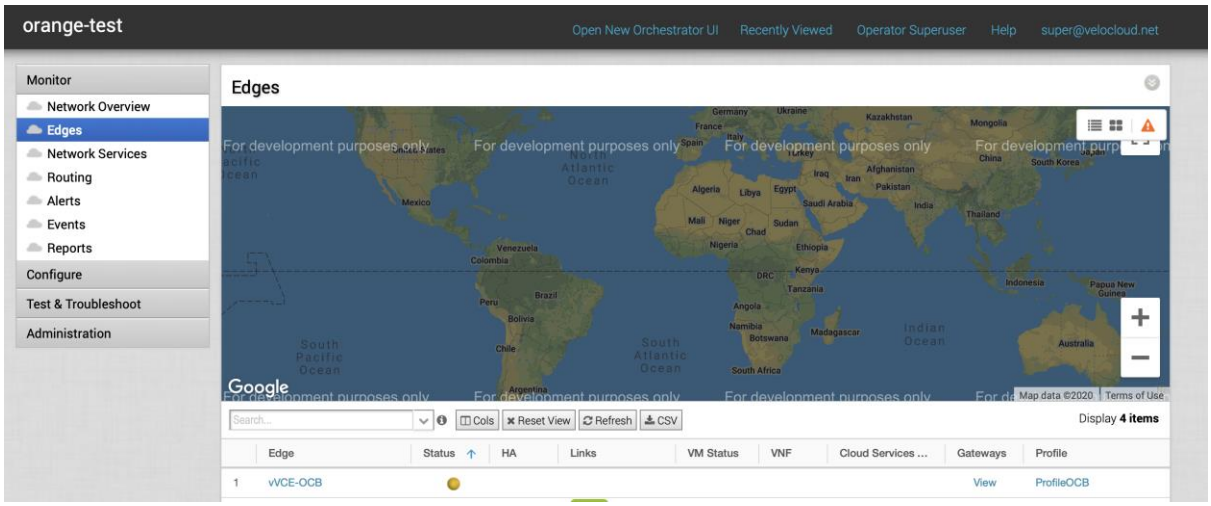
Monitor Deployment Progress

If everything has been done correctly, the instance will be created, in a running state and you can view associated EIP:

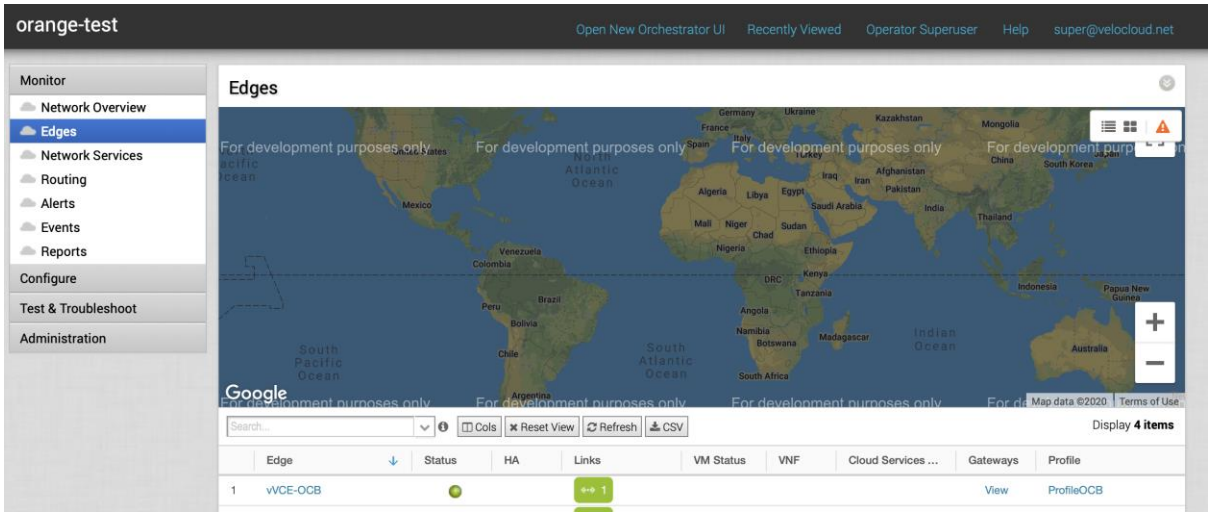


Verify Virtual Edge is Activated In VCO

Once the instance is running in FE and all information provided were correct, the virtual edge will reach out to the VCO with the activation key, activate and perform software update if needed (and reboot if upgraded). Typical deployment time is between 3 to 4 minutes.



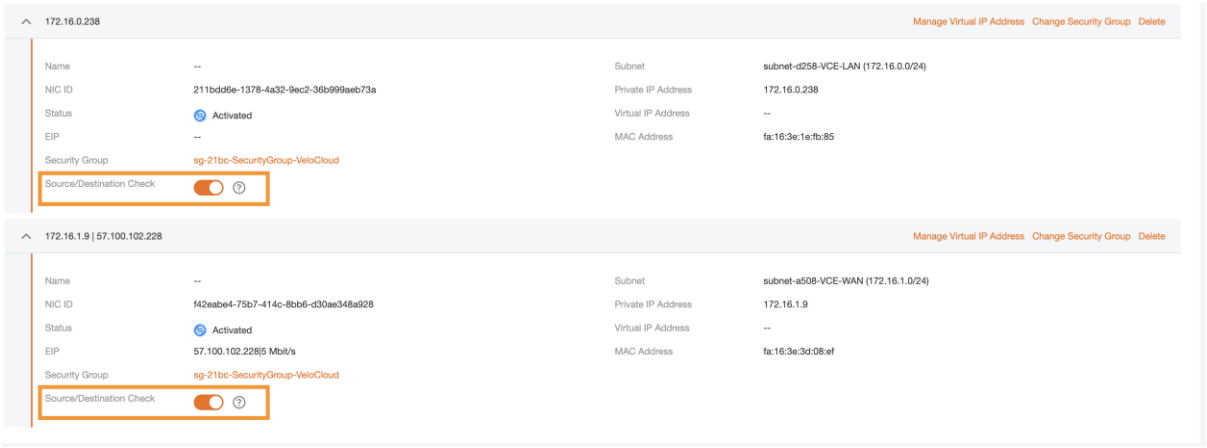
Status orange indicates the VCE has reached out to the VCO and is getting its configuration, software updates, etc. After a few minutes, the status will become green and the VCE will be ready to forward traffic:



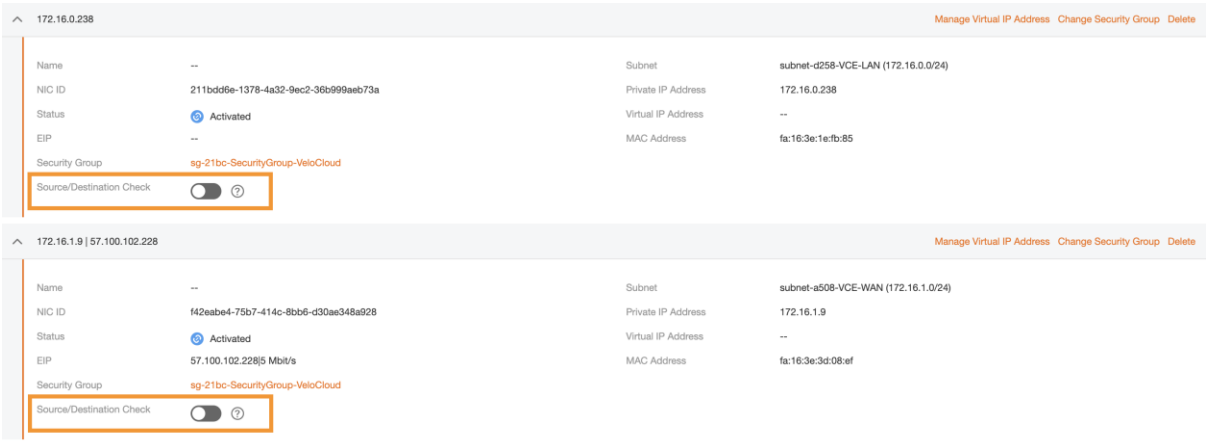
Final ECS configurations

Source/destination Checks

As with any routing ECS, you will need to make sure that source and destination checks are disabled for interfaces that will be routing traffic:

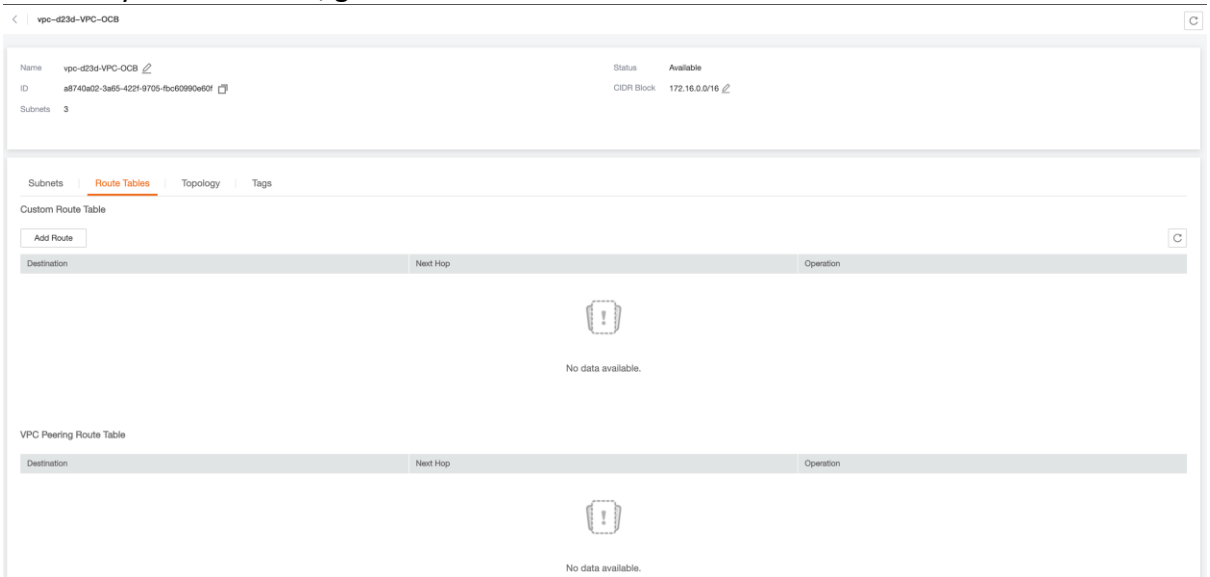


After deactivation:



Route tables

Once the VCE has been deployed, it will now need to be the default GW for all workloads hosted in the subnet carried by the VCE. Different options can be used based on architecture needs. For the sake of simplicy here, we will modify the default VPC route table to add a default route pointing towards the VCE LAN interface.
To modify a Route Table, go to VPC > Route Table:



Click on Add Route:

Specify default route and VCE Lan interface IP address for Next Hop.