Claro cloud

Enterprise Claro Cloud

User Manual

v1.1.5

Table of Contents

Version Table

No. Version	Date	Details
1.0	27/08/2021	Launch of User Manual
1.1	29/11/2021	New chapters 1. Managing Resource Limits in Resource Pool Subscriptions – Page 12 - 15 2. Distributed Firewall - Page 32 - 36 3. API Management – Page 151 - 153
1.1.2	23/12/2021	Adequacy of Open VPN Activation Process – Page 47
1.1.3	26/01/2022	Adding 2 New User Roles – Page 147 L2VPN Configuration – Page 41 – 48 Setting Up a Load Balancer – Page 60 - 64 Application Catalog Update – Page 153-154
1.1.4	29/04/2022	Added expanded K8s Tanzu Grid
1.1.5	01/09/2022	Updated sections for: - Portal with tokens via SMS - VM template creation - Kubernetes clusters - Horizontal auto-scaling

1. Introduction

This document is intended for Enterprise Claro Cloud users to configure and manage their cloud services.

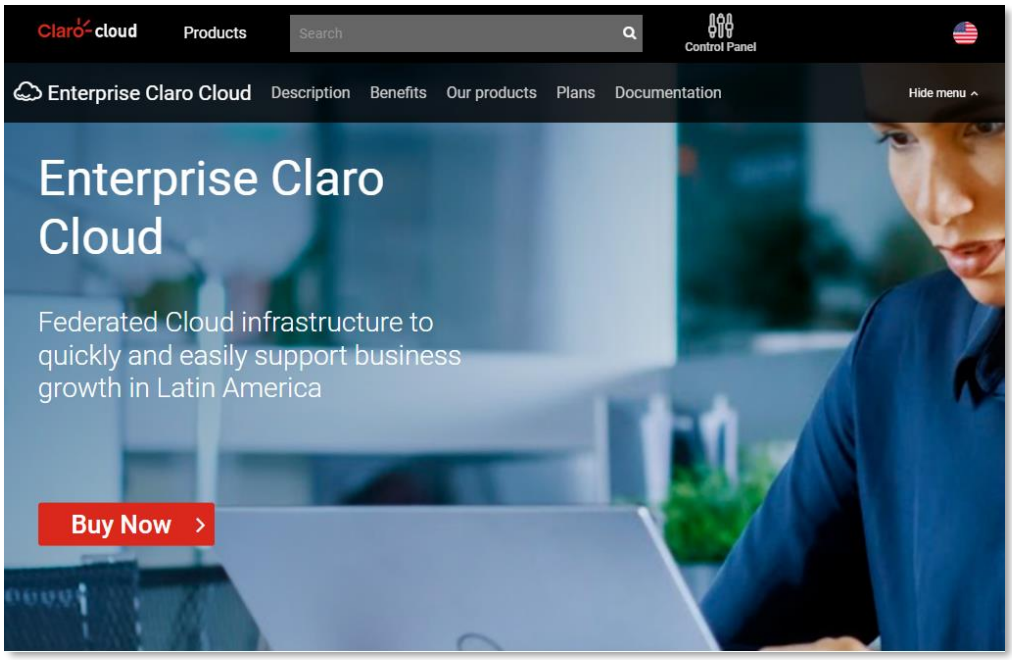
The instructions in this guide reflect the Enterprise Claro Cloud web console (HTML5-based UI) and provides you with clear and precise guidance on the processes required to manage the platform.

Enterprise Claro Cloud is a cloud platform where you can host applications and simplify the development of new applications. It integrates the cloud services needed to develop, test, deploy and manage your cloud computing resources.

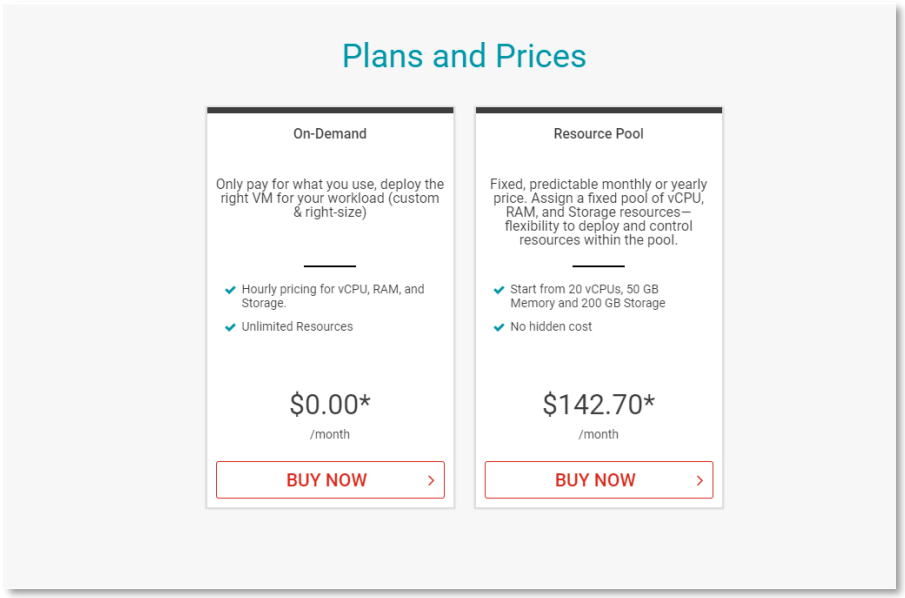
With Enterprise Claro Cloud you can easily scale your resources as your demand increases, while also offering the reliability you need to ensure high availability between different Enterprise Claro Cloud regions. The Enterprise Claro Cloud dashboard allows you to easily manage all services within Claro Cloud. In addition, you are also able to manage your cloud services using APIs.

2. How to purchase Enterprise Claro Cloud

You can purchase the Enterprise Claro Cloud service through
https://www.usclarocloud.com/portal/us/cld/products/infrastructure/enterprise-claro-cloud

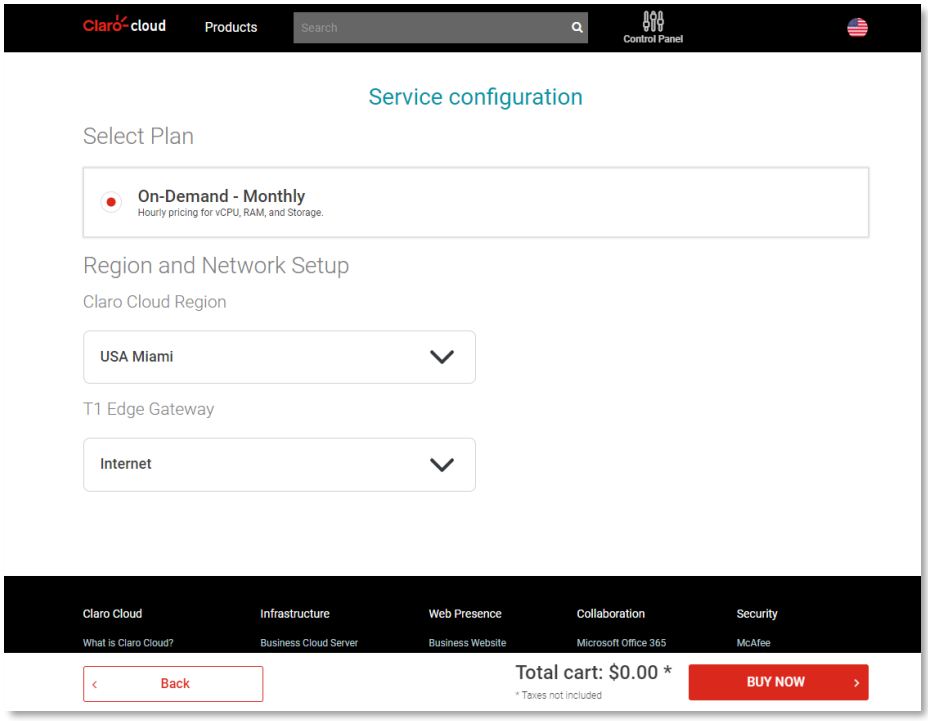


1. Go to the "plans and pricing" section where you will find the available plans of the service, by clicking on the "Buy" button of the plan that suits your needs

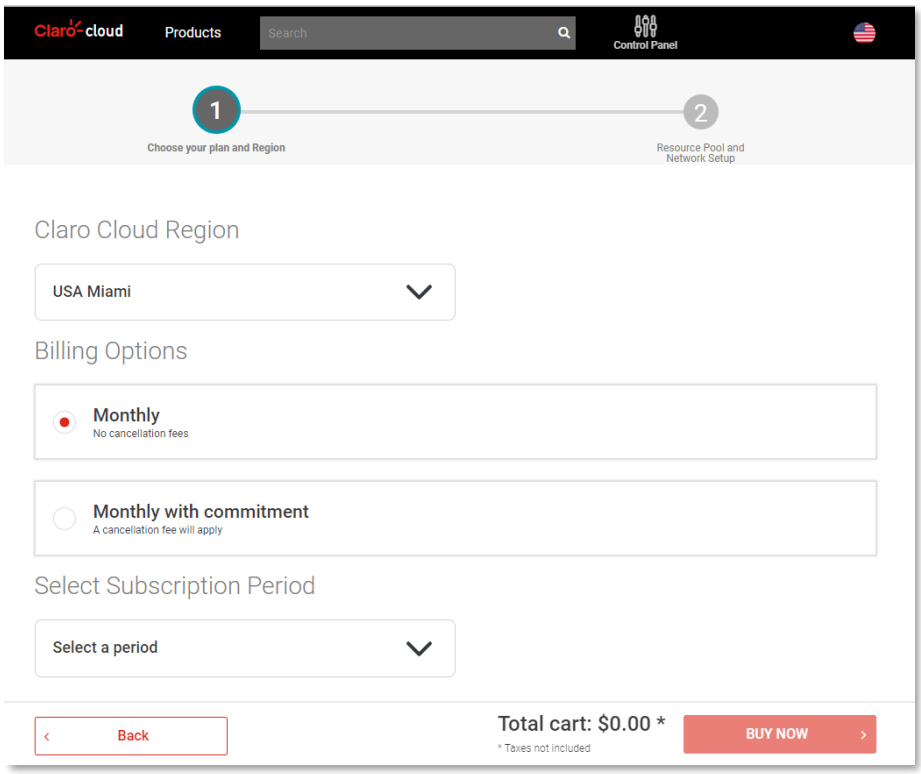


2. The following screen will be displayed, where you can select, the type of plan, contracting period, computing region and the type of connectivity you require, by clicking on "Continue"

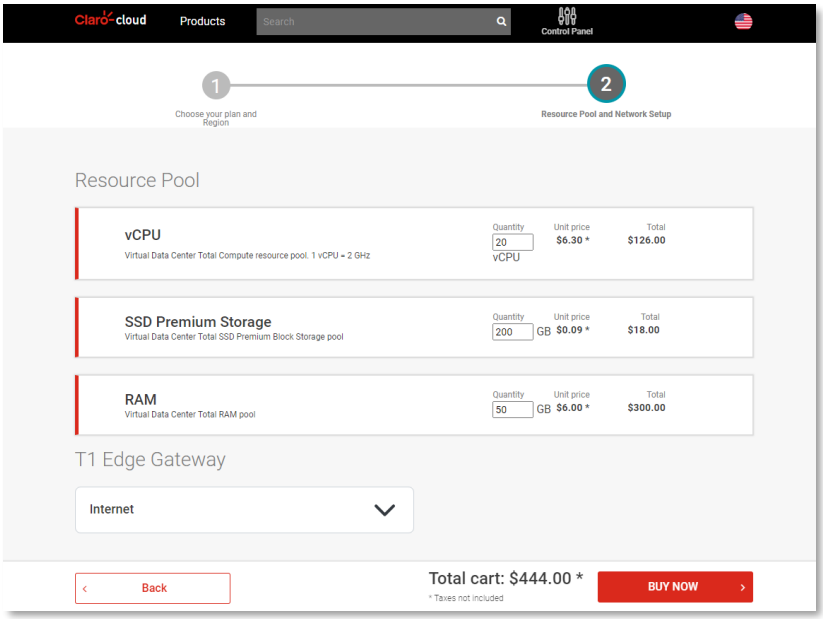
- On Demand



- Resource Pool Plan



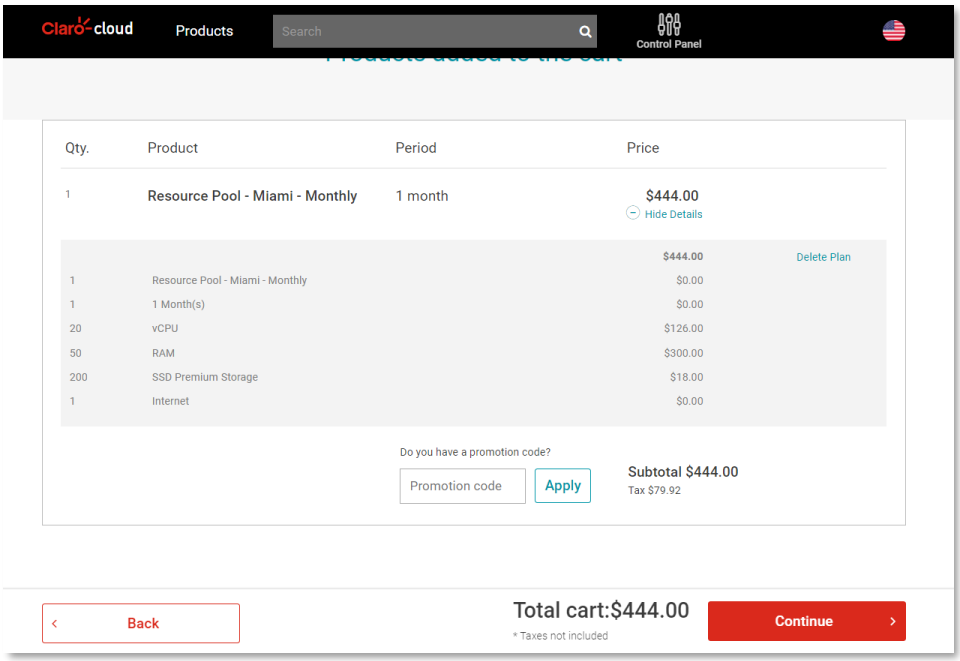
3. If you chose a Resource Pool plan, you must define the size of the Resource Pool (vCPU, RAM, and Storage), as well as the "T1 Edge Gateway" connectivity type. At the end of click "Continue"



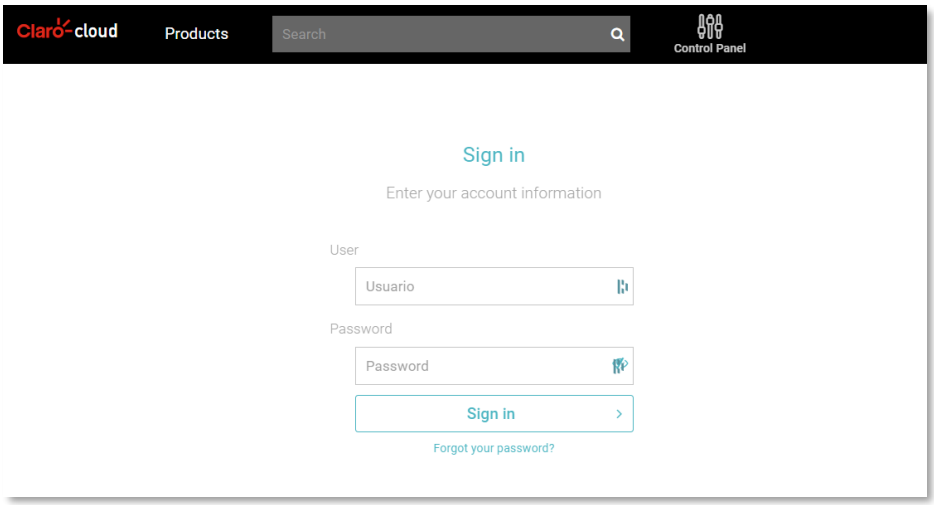
Important:

- The minimum capacity to contract is 20 vCPUs, 50 GB of RAM and 200 GB of Storage.
- The T1 Edge Gateway service in its Hybrid version, does not include the MPLS link, it can be purchased separately, through Claro.
- The contracting of the MPLS link is subject to availability and technical feasibility.
- For second purchases in the same compute region, the T1 Edge Gateway service will not be provisioned, in case a second instance is required to validate the Purchase section of an additional T1 Edge Gateway

4. The summary of the purchase will be displayed, click on "Process purchase"

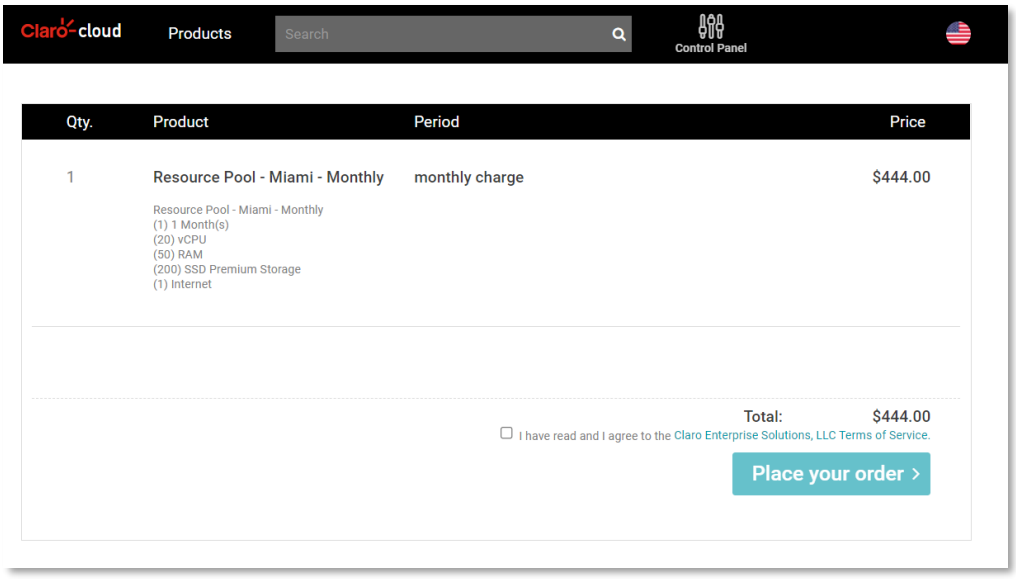


5. If you are already a Claro Cloud customer, it will be required to enter your username and password of your Cloud account, by clicking on "Login"
   If you are not a customer please call our Sales Team at +1-833-992-5276

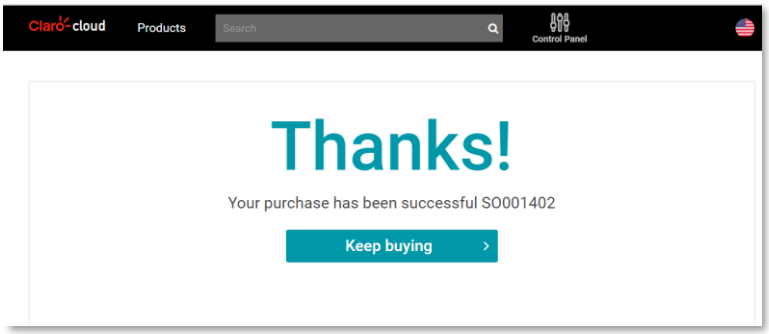


6. After login in the following screen will be displayed where you must accept the Terms and Conditions of the Enterprise Claro Cloud service, by clicking on "Place your order"

> **Important:** Payment for the service will be made through your monthly Claro invoice

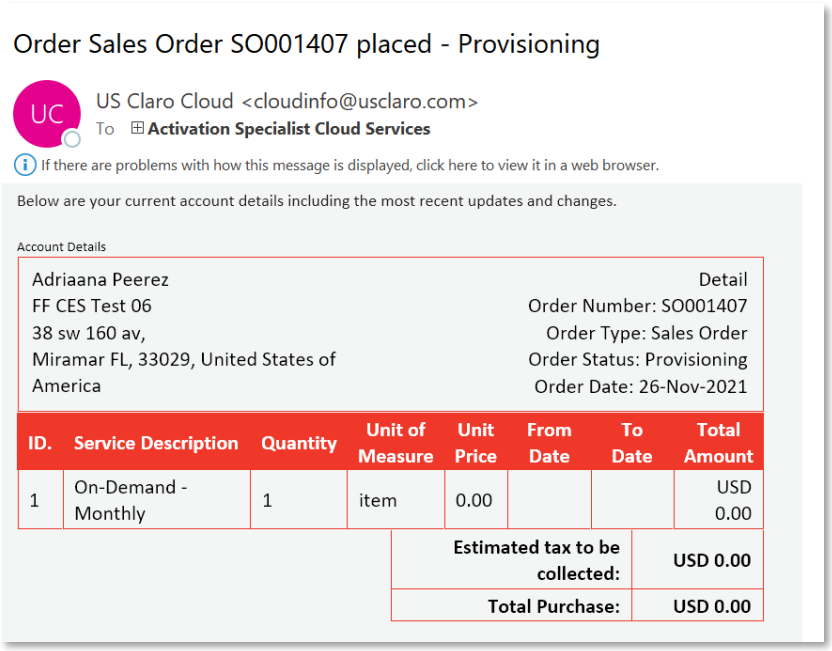


8. The following screen will be displayed confirming your order



9. You will receive two notifications to your email account:

- Purchase confirmation



Order Sales Order SO001407 placed - Provisioning

UC

US Claro Cloud <cloudinfo@usclaro.com>

To **Activation Specialist Cloud Services**

If there are problems with how this message is displayed, click here to view it in a web browser.

Below are your current account details including the most recent updates and changes.

Account Details

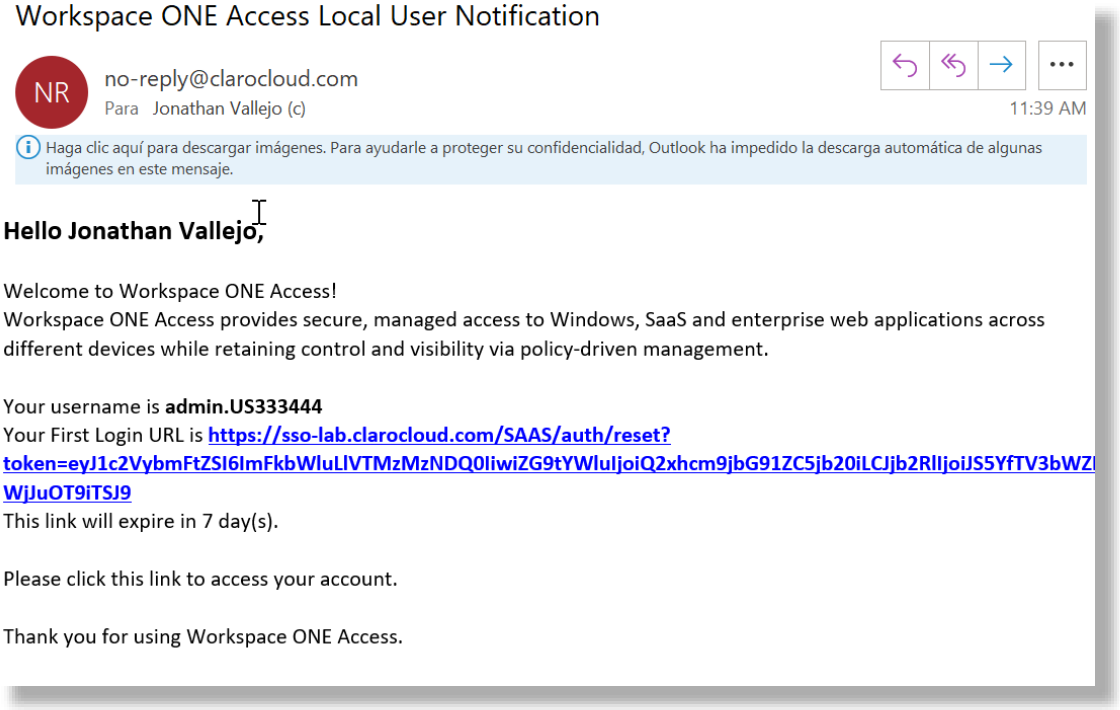
Adriaana Peerez
FF CES Test 06
38 sw 160 av,
Miramar FL, 33029, United States of America

Detail
Order Number: SO001407
Order Type: Sales Order
Order Status: Provisioning
Order Date: 26-Nov-2021

ID.	Service Description	Quantity	Unit of Measure	Unit Price	From Date	To Date	Total Amount
1	On-Demand - Monthly	1	item	0.00			USD 0.00

Estimated tax to be collected:	**USD 0.00**
Total Purchase:	**USD 0.00**

- Welcome email with your username and URL to define your password to enter the Enterprise Claro Cloud portal



Workspace ONE Access Local User Notification

NR

no-reply@clarocloud.com

Para Jonathan Vallejo (c)

11:39 AM

Haga clic aquí para descargar imágenes. Para ayudarle a proteger su confidencialidad, Outlook ha impedido la descarga automática de algunas imágenes en este mensaje.

Hello Jonathan Vallejo,

Welcome to Workspace ONE Access!
Workspace ONE Access provides secure, managed access to Windows, SaaS and enterprise web applications across different devices while retaining control and visibility via policy-driven management.

Your username is **admin.US333444**
Your First Login URL is **https://sso-lab.clarocloud.com/SAAS/auth/reset?token=eyJ1c2VybmFtZSI6ImFkbWluLlVTMzMzNDQ0IiwiZG9tYWluIjoiQ2xhcm9jbG91ZC5jb20iLCJjb2RlIjoiJS5YfTV3bWZ[illegible]WjJuOT9iTSJ9**
This link will expire in 7 day(s).

Please click this link to access your account.

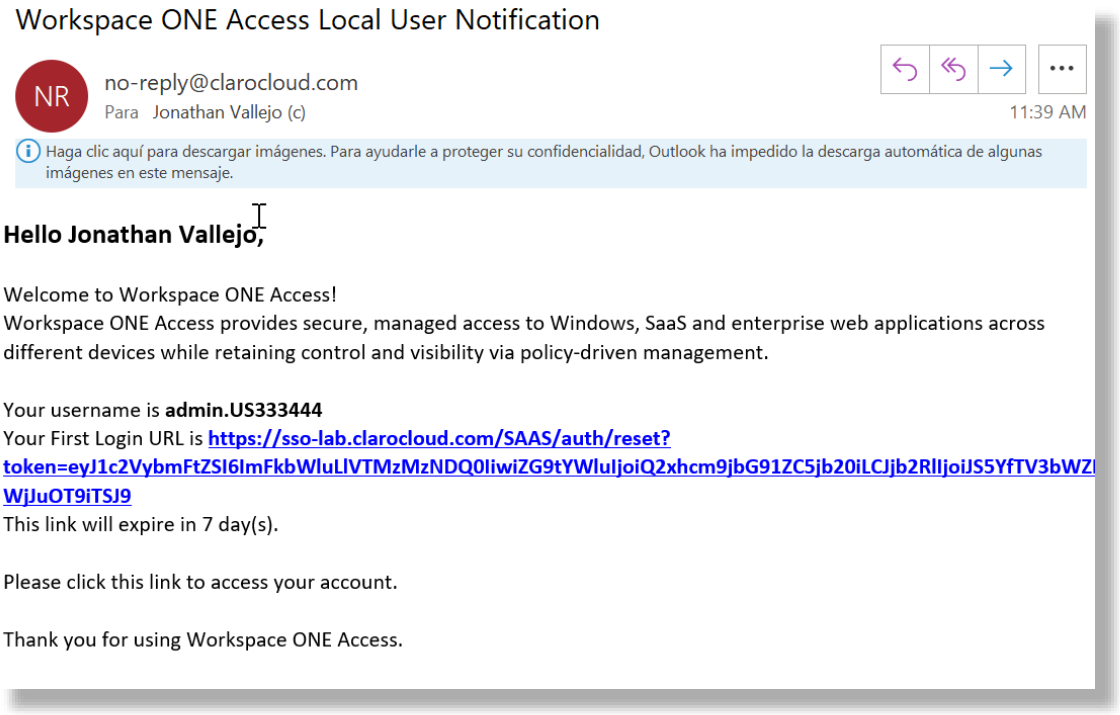
Thank you for using Workspace ONE Access.

3. How to purchase Enterprise Claro Cloud with SMS

Access to the Enterprise Claro Cloud portal with tokens via SMS

In countries such as the Dominican Republic and Puerto Rico, SMS messages may not be received for linking the Verify application, so it is necessary to run the following process to enter your service.

1. At the end of the purchase process you will receive an e-mail with the necessary access information to be able to enter your service. As shown in the following image



Workspace ONE Access Local User Notification

NR no-reply@clarocloud.com
Para Jonathan Vallejo (c) 11:39 AM

Haga clic aquí para descargar imágenes. Para ayudarle a proteger su confidencialidad, Outlook ha impedido la descarga automática de algunas imágenes en este mensaje.

Hello Jonathan Vallejo,

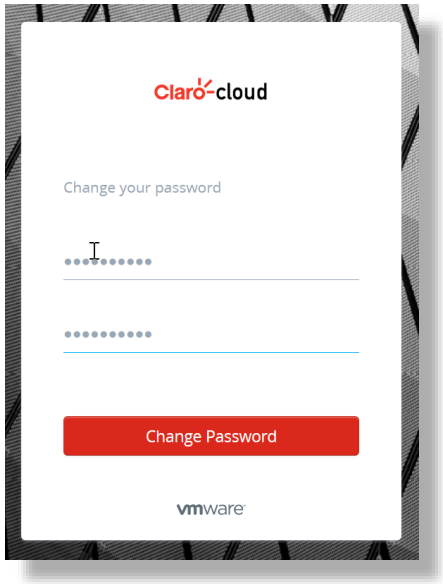
Welcome to Workspace ONE Access!
Workspace ONE Access provides secure, managed access to Windows, SaaS and enterprise web applications across different devices while retaining control and visibility via policy-driven management.

Your username is **admin.US333444**
Your First Login URL is https://sso-lab.clarocloud.com/SAAS/auth/reset?token=eyJ1c2VybmFtZSI6ImFkbWluLlVTMzMzNDQ0IiwiZG9tYWluIjoiQ2xhcm9jbG91ZC5jb20iLCJjb2RlIjoiJS5YfTV3bWZ...WjJuOT9iTSJ9
This link will expire in 7 day(s).

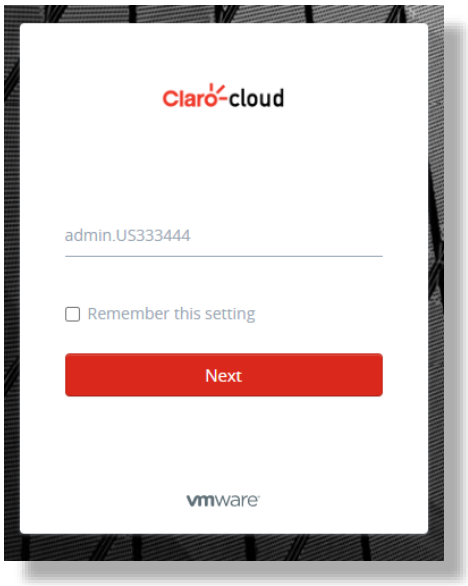
Please click this link to access your account.

Thank you for using Workspace ONE Access.

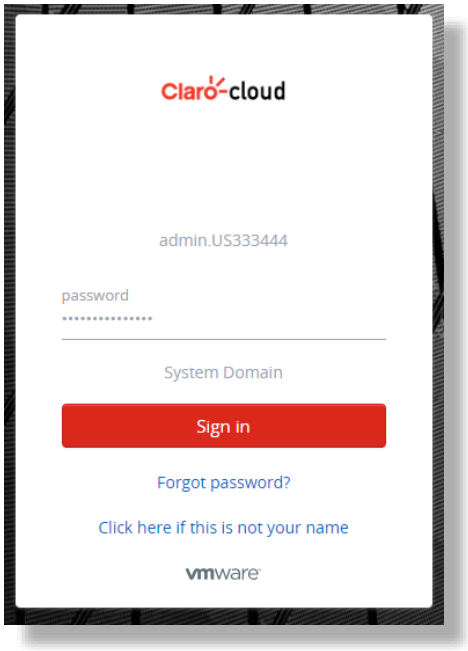
2. Enter in the web browser of your preference the URL attached to the e-mail, the following interface will be displayed where you will define your access password. At the end of clicking on the "Change Password" button



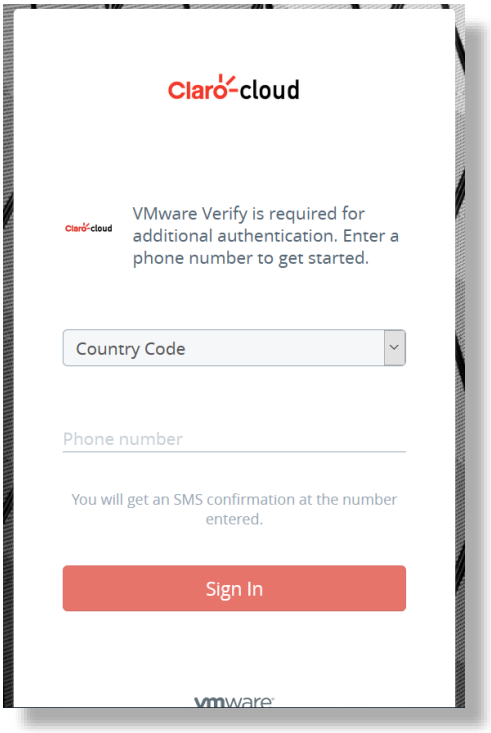
3. Enter your username, which you will find in the body of the e-mail previously received



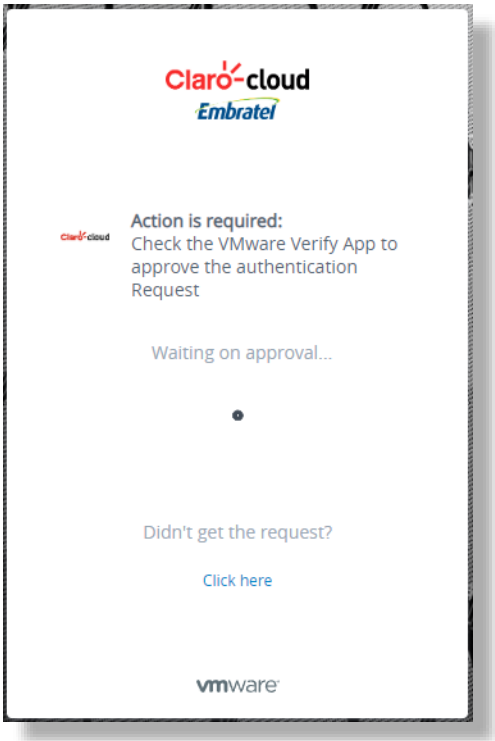
4. Enter the previously defined password



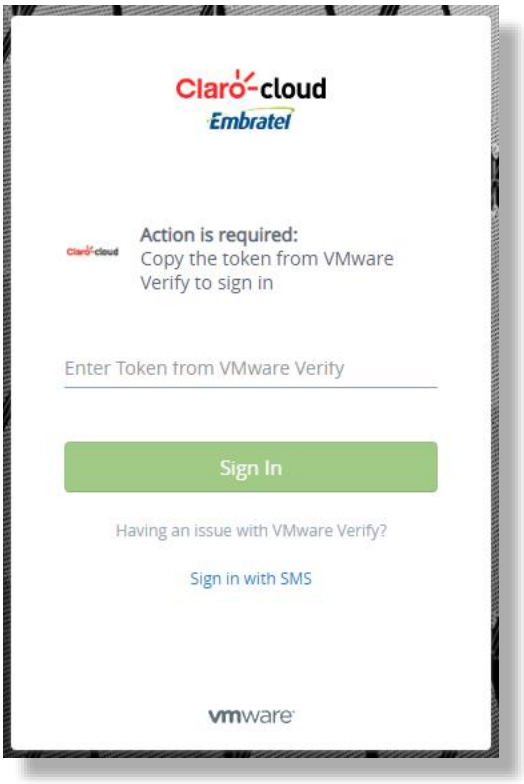
5. Enter a phone number and country code, click Sign in



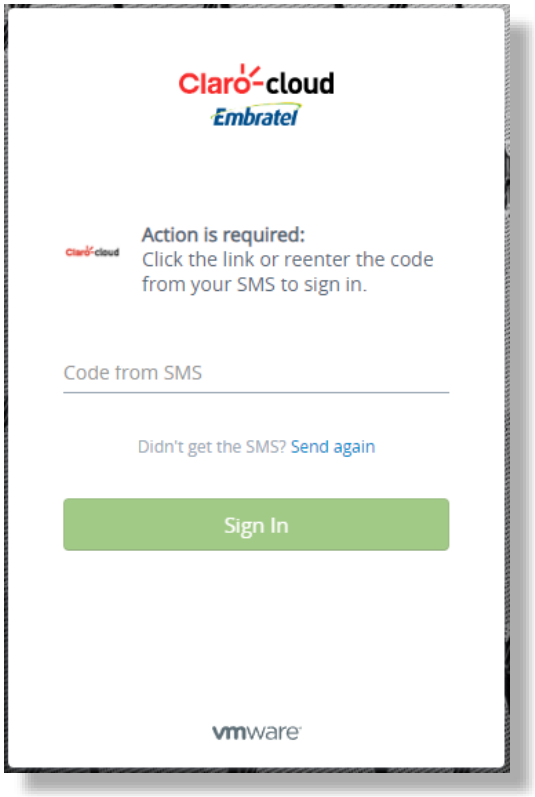
6. Enter again to https://sso.clarocloud.com/SAAS/auth/login, indicate your previously defined username and password, click on Sign In, the following screen will appear



7. By clicking on the Click here button, the following screen will appear

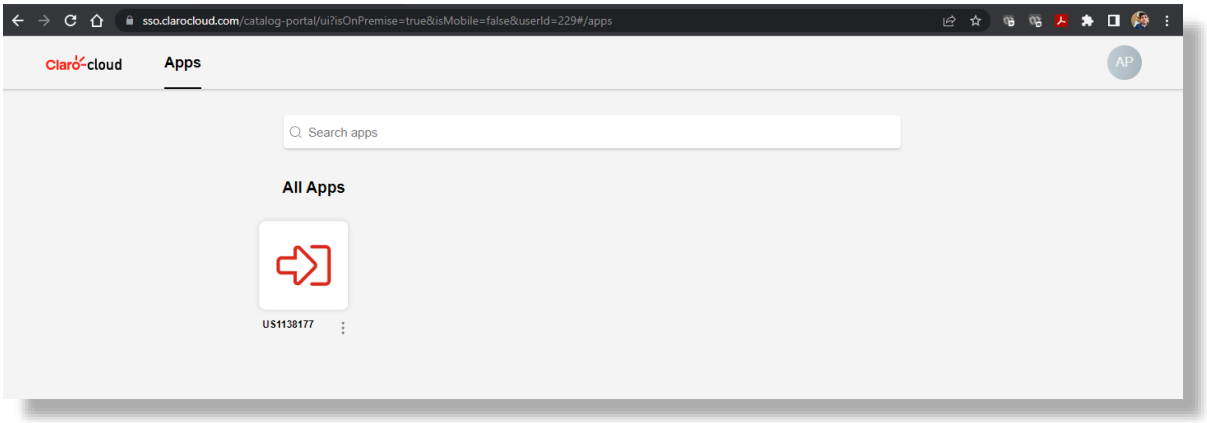


8. By clicking on the "Sign in with SMS" button, the following screen will appear.

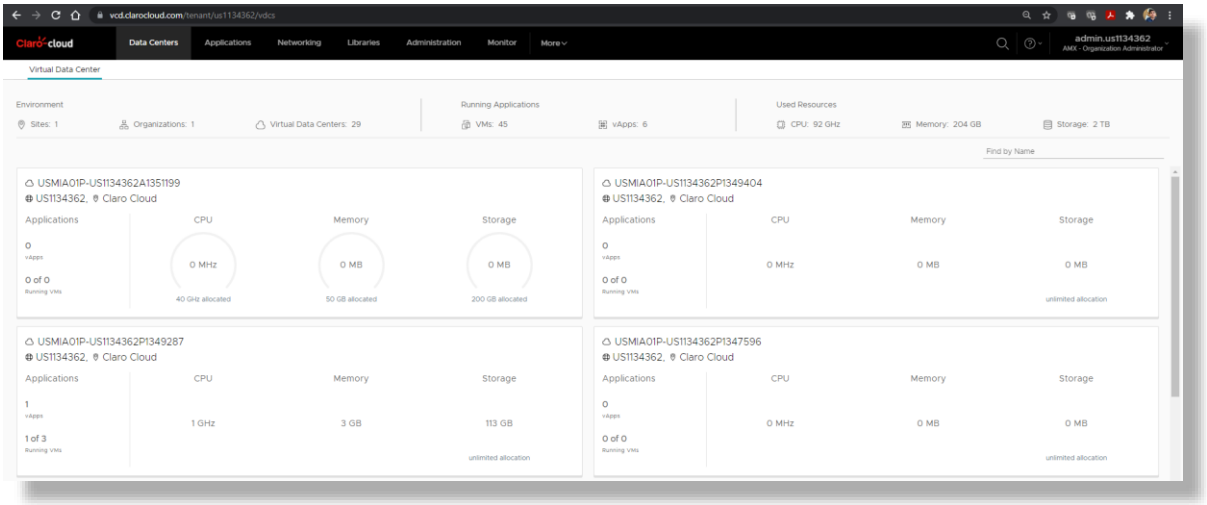


9. In parallel you will receive an SMS message to the phone registered in step 5, the SMS will contain a code which must be entered on the screen shown in the previous step, click on Sign In

10. When you enter the click code in Sign In, your web browser will open automatically the following screen



11. Click on the icon with the red arrow to enter your Claro Cloud Enterprise control panel where you can manage your cloud services. The following screen will open



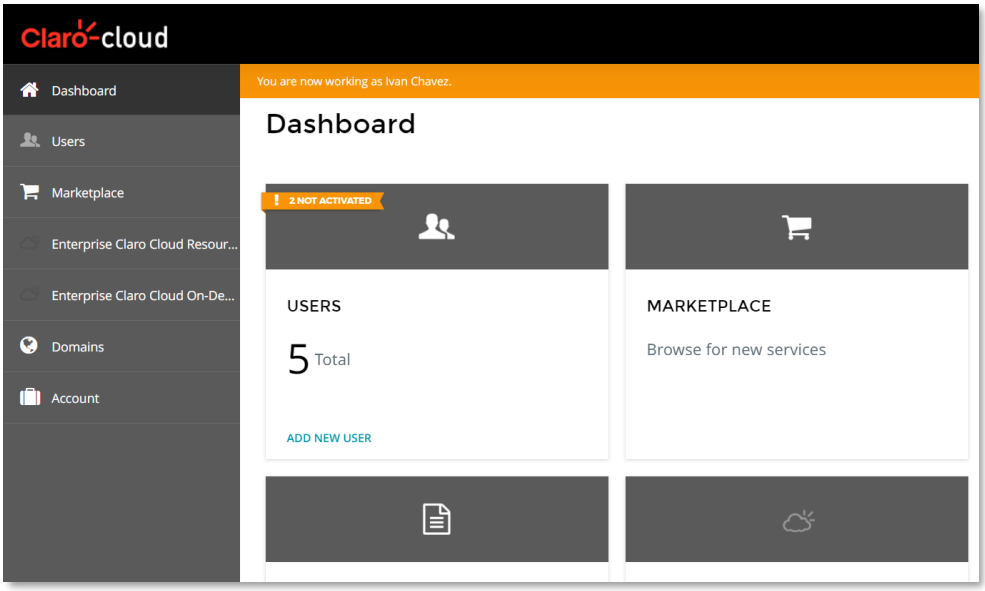
For upcoming sessions to your Claro Cloud Enterprise dashboard use the following URL: https://sso.clarocloud.com/SAAS/auth/login

Resource Limit Management in Resource Pool Subscriptions

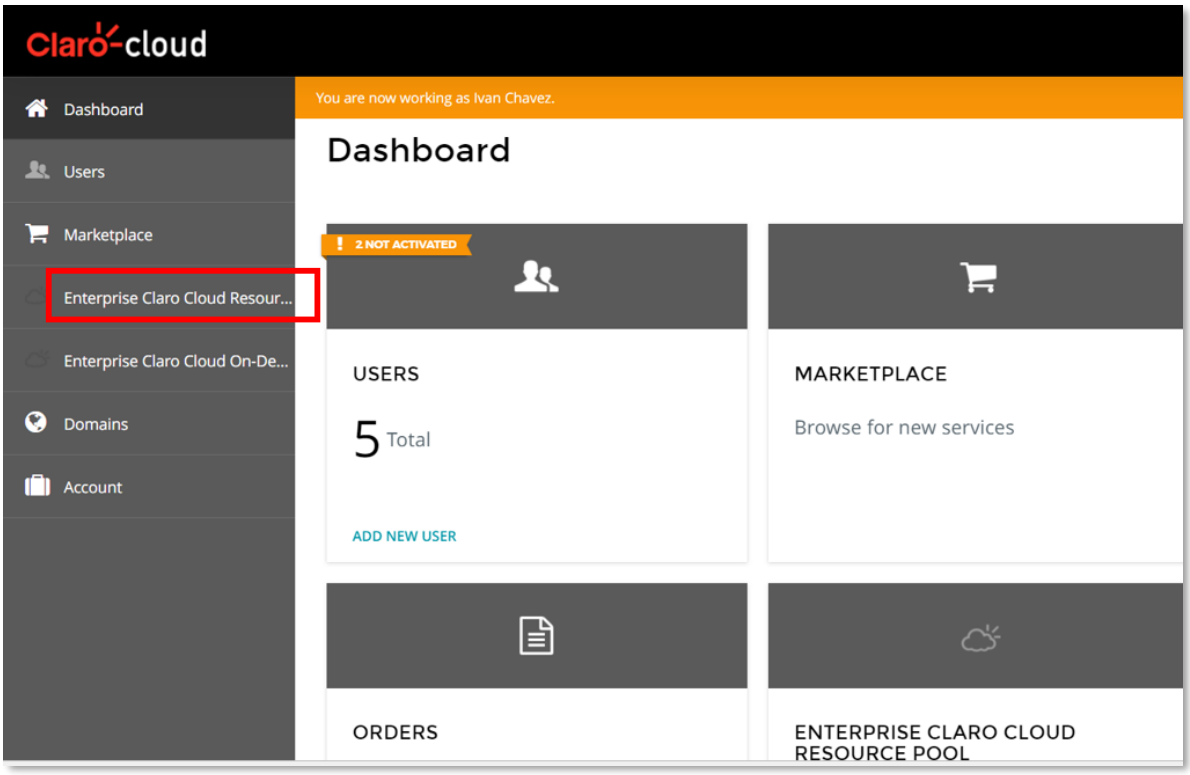
If you chose a subscription with the Resource Pool scheme you can manage the amount of vCPUs, GB of RAM and GB of storage from your portal.

> **Important:** The minimum amount of resources allowed in a data center is 20 vCPUs, 50 GB of RAM, and 200 GB of storage.

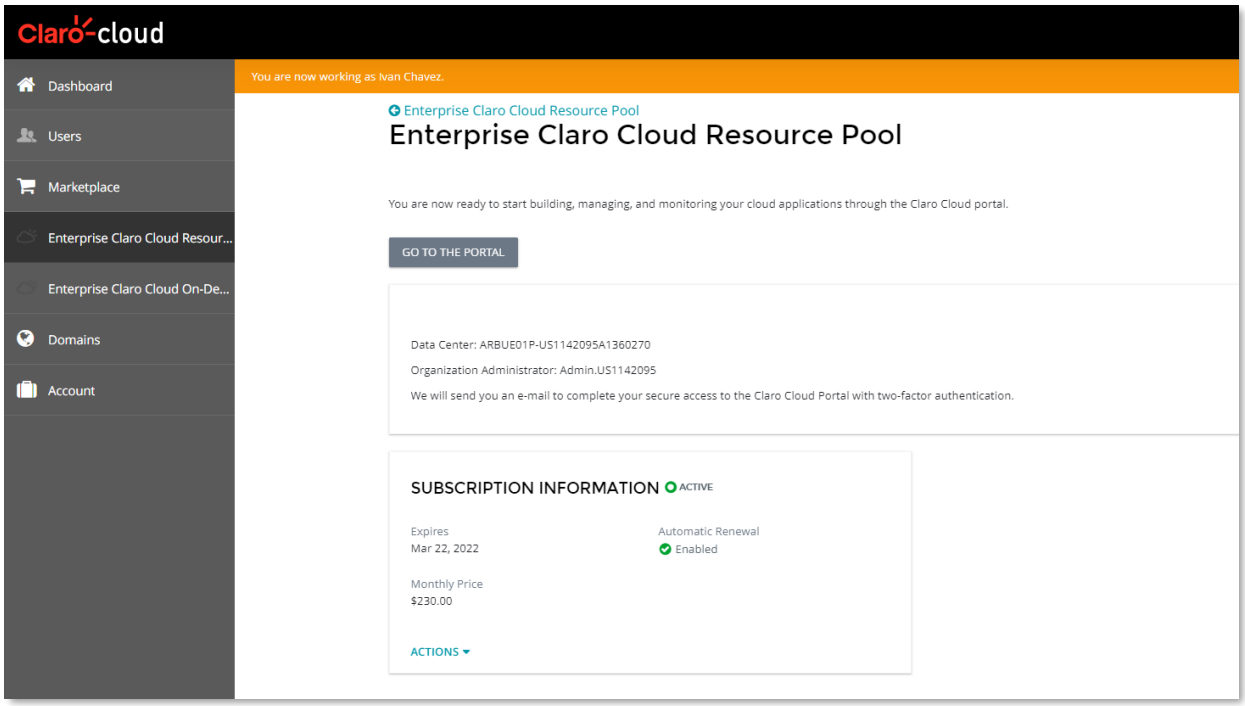
1. Log in to your admin panel https://cp.usclarocloud.com/



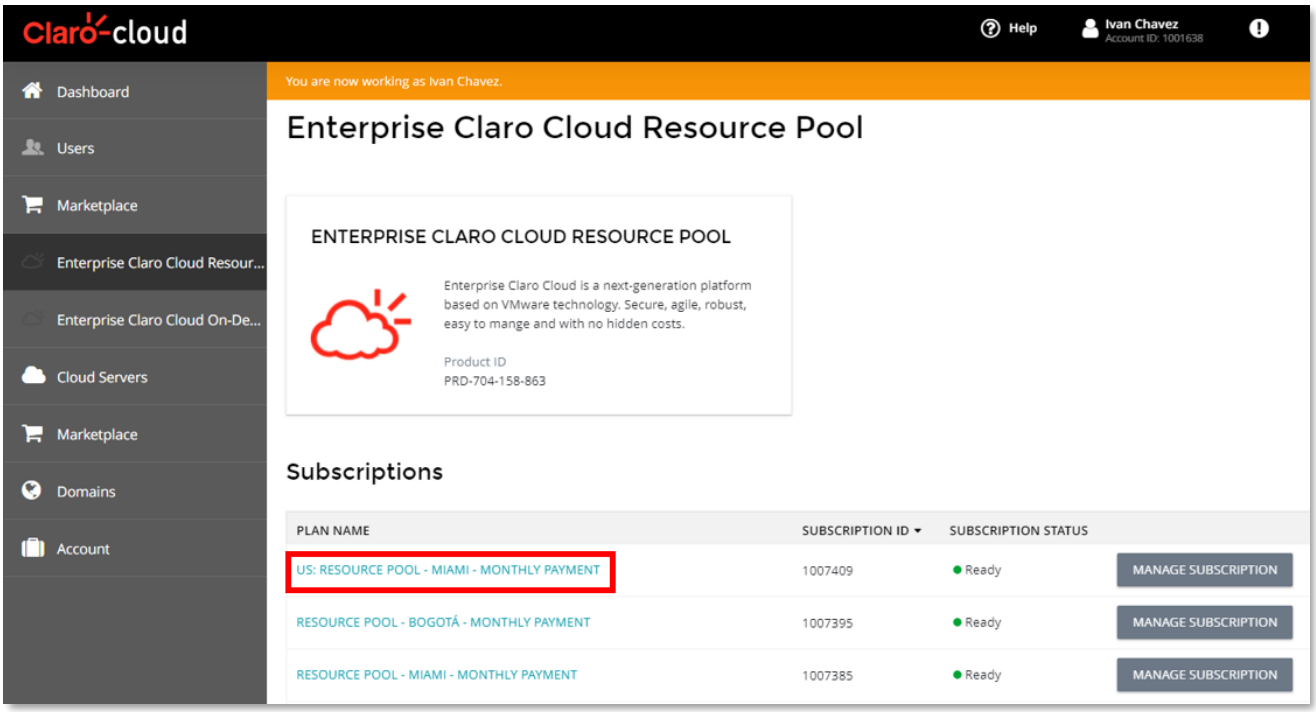
2. Click on the Enterprise Claro Cloud Resource Pool section, located on the left within the gray menu.



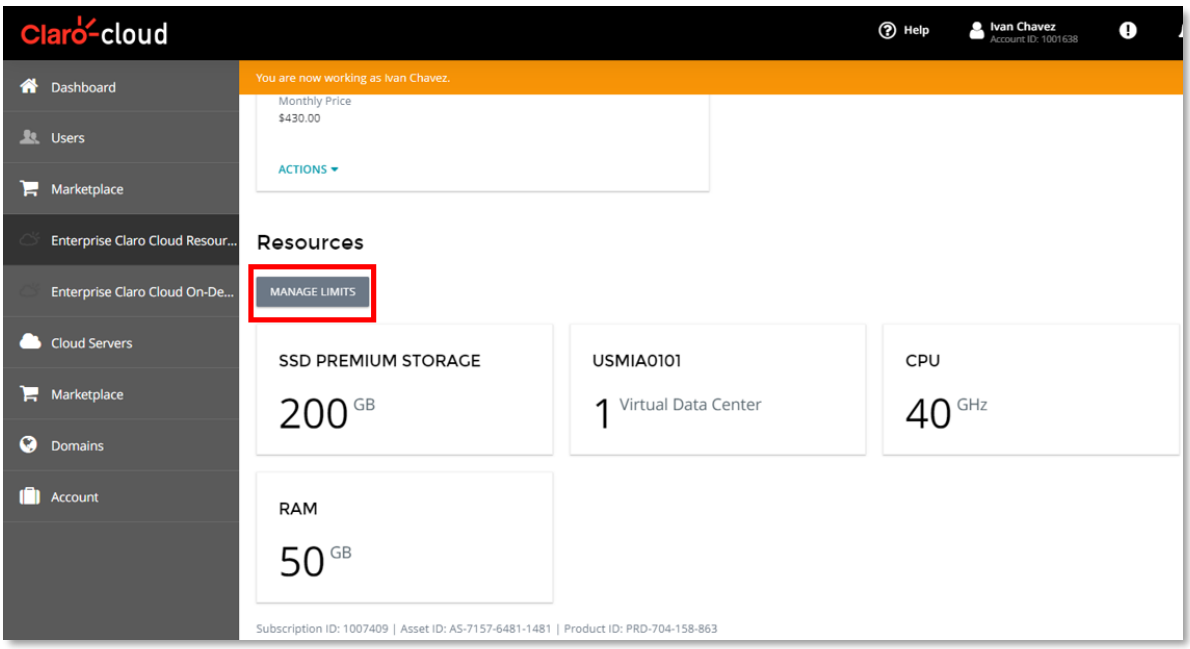
3. The following screen will open



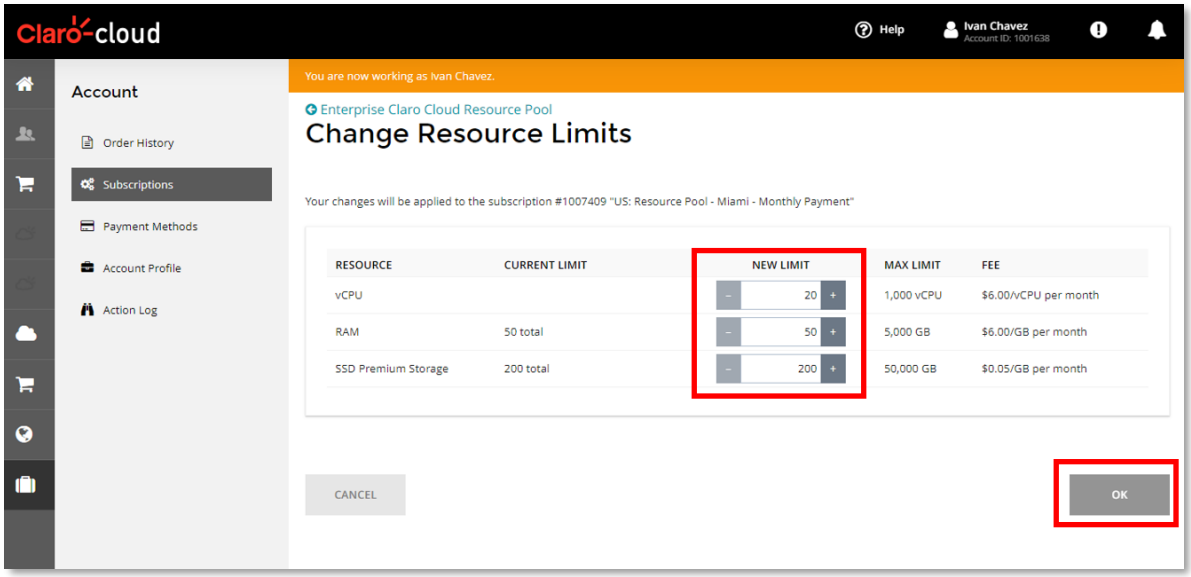
4. If you have more than one Resource Pool subscription just click on the name of the subscription you want to modify.



5. At the bottom you will find a button called "Manage Limits", click on it.



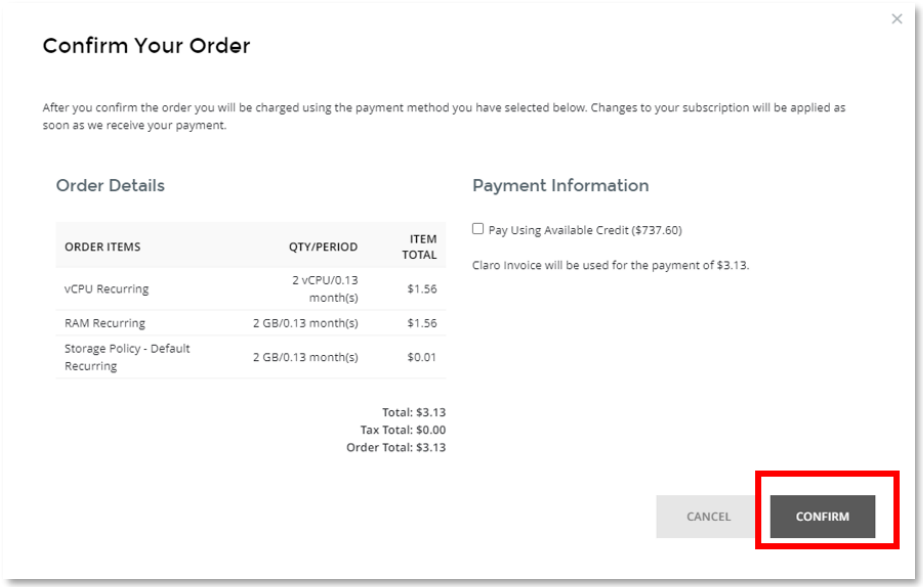
6. The following screen will open where you can select the amount of resources you want to add to your Data Center. When you finish click "OK"



Important:

- Increased compute resources are possible up to a maximum of 1,000 vCPUs, 5,000 GB of RAM, and 50 TB of storage. If you require more capacity contact your Claro support team.
- It is not possible to decrease the pool of resources to an amount lower than what was contracted. Additional resources can be decreased if they have not been used.
- 1 vCPU is equivalent to 2 GHz
- If your subscription is tied to a 12, 24, or 36 month contracting period, capacity changes are updated in the contracting period.

7. A confirmation screen with the changes and new charges resulting will be displayed, click on "Confirm" if you agree with the amounts. You will receive an email with the requested change order.



Claro Cloud USA <cloudinfo@usclaro.com>
para mí

Claro Cloud

Order Notification No. UG000076

Below are your current account details including the most recent updates and changes.

Account Details

Ivan Chavez Garcia
CES AMX
3350 SW 148th, Ave #400,
Miramar FL, 33027, United States of America

Detail
Order Number: UG000076
Order Type: Change Order
Order Status: Creating Order Details
Order Date: 26-May-2021

ID.	Service Description	Quantity	Unit of Measure	Unit Price	From Date	To Date	Total Amount
1	vCPU Recurring	20	vCPU	10.00	26-May-2021	31-May-2021	USD 33.34
2	RAM Recurring	20	GB	7.00	26-May-2021	31-May-2021	USD 23.34
3	Storage Policy - Default Recurring	200	GB	0.07	26-May-2021	31-May-2021	USD 2.33

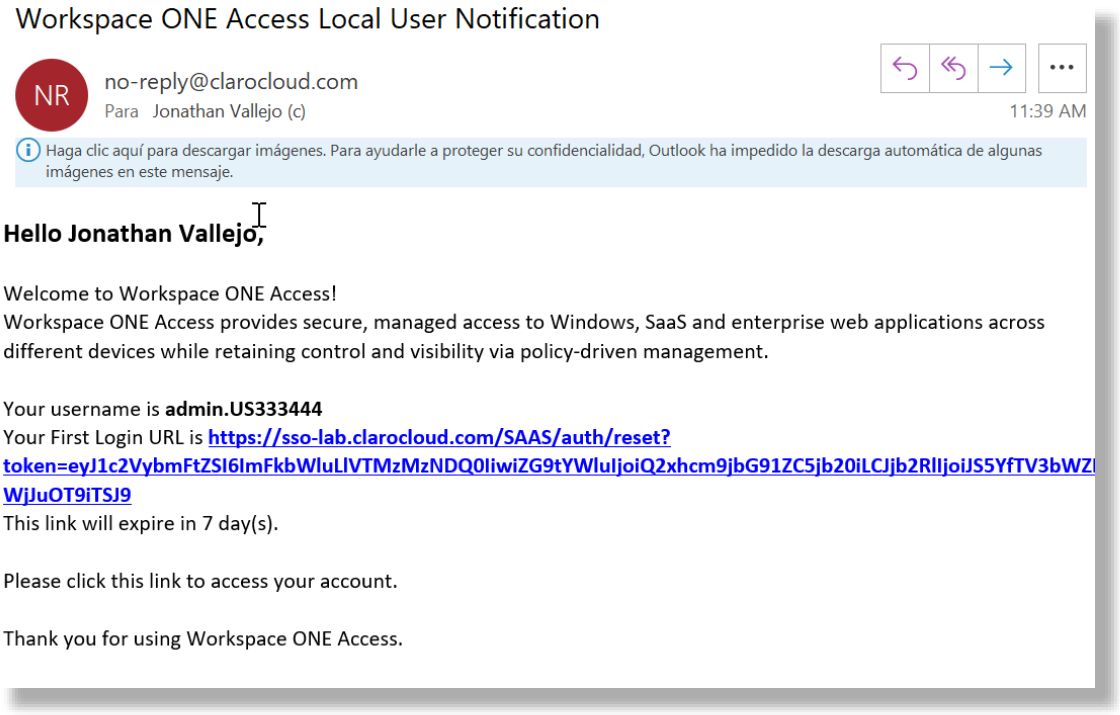
Estimated tax to be collected:	USD 0.00
	USD 59.01

8. Within two to three minutes the capacity of your data center will be updated with the requested resources.

3. How to use the Claro Cloud portal

Access to the Enterprise Claro Cloud portal

At the end of the purchase process you will receive an e-mail with the information necessary access to your service. As shown in the following image



Workspace ONE Access Local User Notification

NR no-reply@clarocloud.com
Para Jonathan Vallejo (c)
11:39 AM

Haga clic aquí para descargar imágenes. Para ayudarle a proteger su confidencialidad, Outlook ha impedido la descarga automática de algunas imágenes en este mensaje.

Hello Jonathan Vallejo,

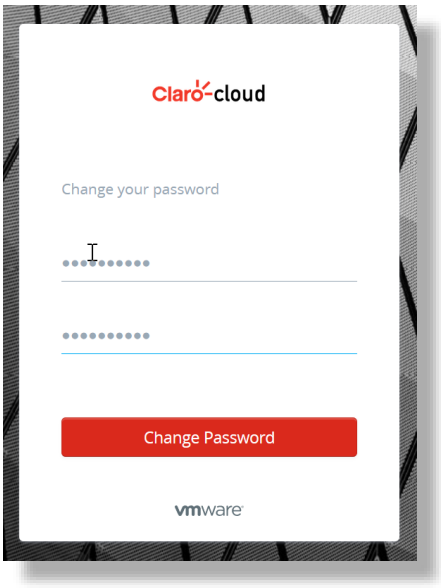
Welcome to Workspace ONE Access!
Workspace ONE Access provides secure, managed access to Windows, SaaS and enterprise web applications across different devices while retaining control and visibility via policy-driven management.

Your username is **admin.US333444**
Your First Login URL is https://sso-lab.clarocloud.com/SAAS/auth/reset?token=eyJ1c2VybmFtZSI6ImFkbWluLlVTMzMzNDQ0IiwiZG9tYWluIjoiQ2xhcm9jbG91ZC5jb20iLCJjb2RlIjoiS5YfTV3bWZ...WjJuOT9iTSJ9
This link will expire in 7 day(s).

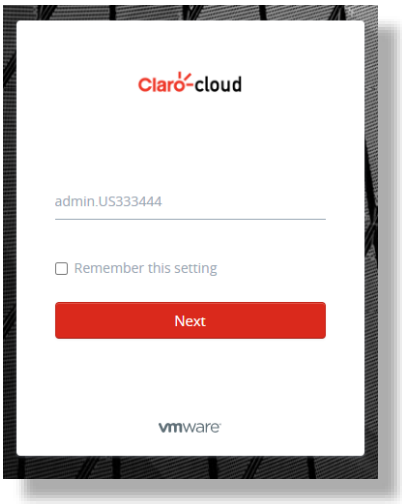
Please click this link to access your account.

Thank you for using Workspace ONE Access.

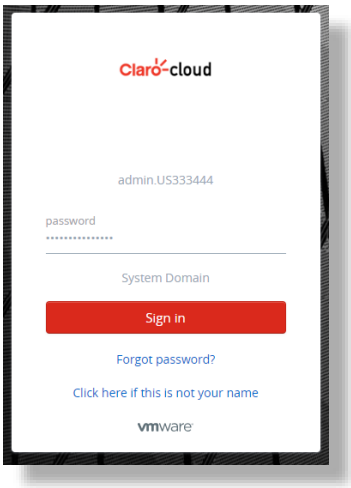
1. Utilizing the web browser of your preference, enter the URL provided in the e-mail. The following interface will be displayed where you will set your password. When finished, click on the "Change Password" button



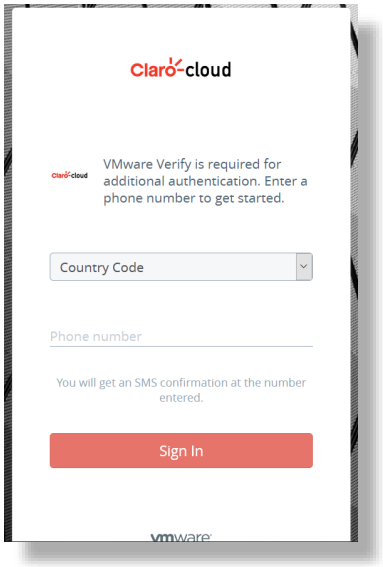
2. Enter your username, which you will find in the body of the e-mail previously received



3. Enter the previously defined password



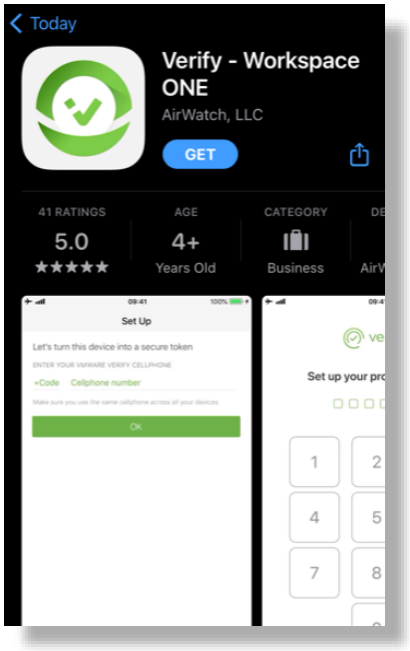
4. Enter a phone number and country code, This is required to be able to send download information in order to activate the two-factor authentication



5. Via text message you will receive a link to download the mobile application that is utilized to generate an access validation token for your account.

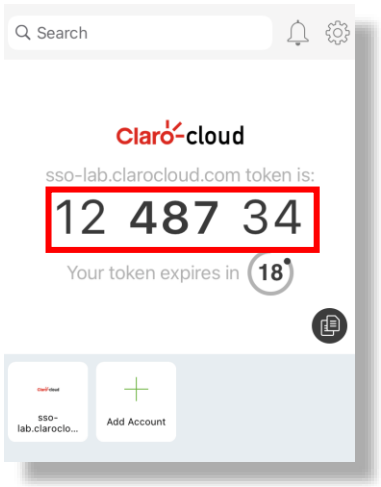
6. Click on the download URL indicated in the text message which will redirect you to your mobile application store (Google Play / Apple App Store)

7. Click to download "Verify – Workspace ONE"

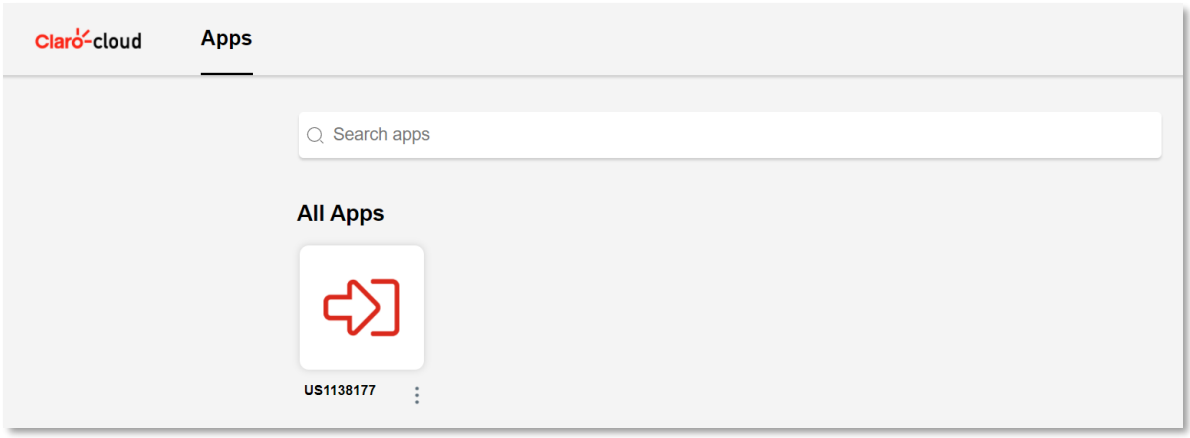


8. After downloading, click open, enter the PIN provided in the second text message.

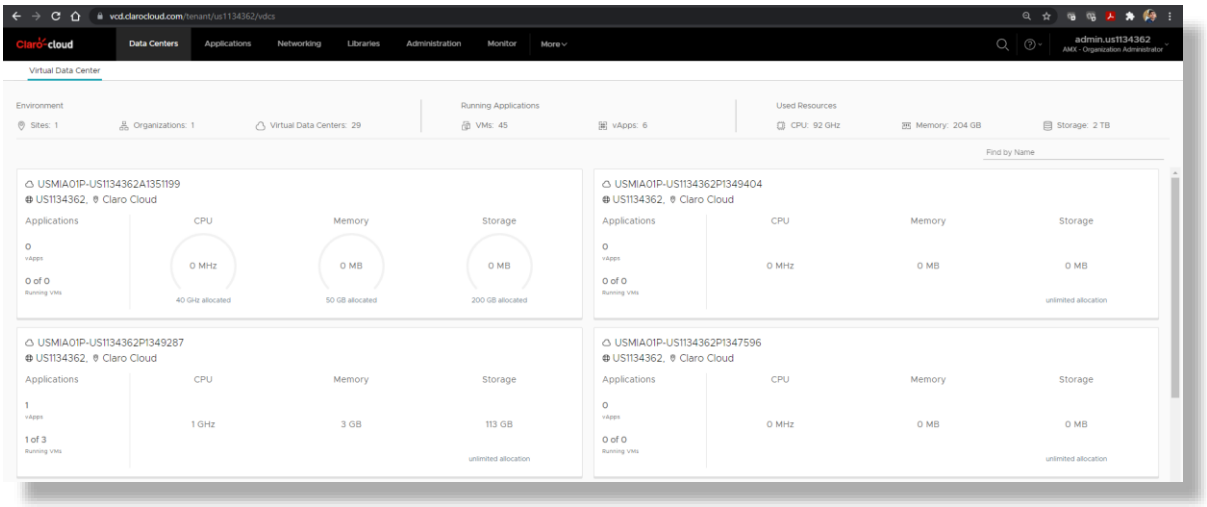
9. Your mobile token will automatically be linked with the information in your Enterprise Claro Cloud account.



10. In your web browser the following screen will open automatically



11. Click on the icon to enter your Enterprise Claro Cloud dashboard where you can manage your cloud services. The following screen will open



12. After this initial setup you will access your Enterprise Claro Cloud dashboard via the following URL: https://sso.clarocloud.com/SAAS/auth/login

4. Introducing Enterprise Claro Cloud

Enterprise Claro Cloud is an efficient and flexible public cloud technology based on VMware services with components such as vCloud Director, NSX, AVI, CSE among others. In the following chapters you will find the necessary processes for the management of the different services.

In the Enterprise Claro Cloud control panel you can find multiple menus that will help you with the creation, administration, monitoring, and management of your services.

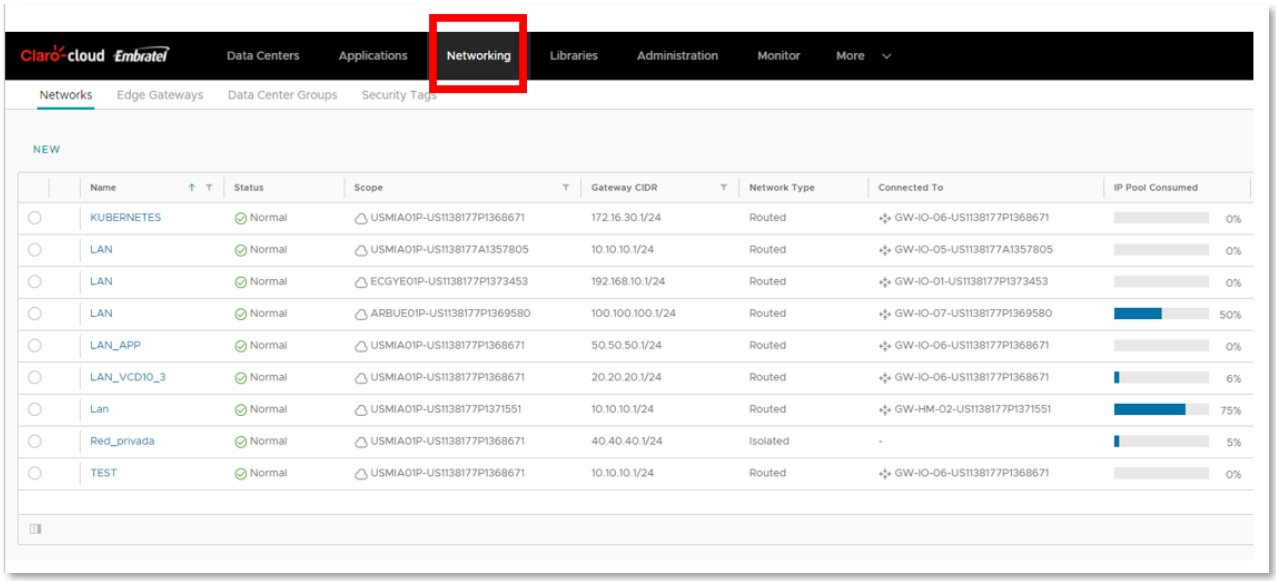
Listed below are the different sections that you will have in your admin panel:

Main menu options	Description
Data Center	Distribution of data centers deployed in the different regions of Claro Cloud
Applications	Visualization and management of virtual applications, Virtual Machines and Scale Groups
Networks	Management of T1 Edge Gateway instances, virtual networks, VPN connections, NAT, DHCP, LB, etc.
Library	Viewing and managing public and private catalogs, installation media (.ISO images) and deployment of point workloads
Administration	Managing users, roles, groups, and certificates
Supervise	Visualization of logs related to events and tasks performed on the platform
App Launchpad	Application Catalog for creating virtual machines in your Virtual Data Center
Kubernetes Container Cluster	Managing and creating Kubernetes clusters based on virtual machines
Autoscale	In this section you will find the management of the scale-up rules for your applications and virtual machines
Operations Manager	Visualization of health dashboards and monthly consumption reports in your data centers
Availability	Manage and execute workload migrations to different compute regions available in Claro Cloud through the vCloud Availability solution
Guided Tours	Short capsules of most frequent and common operations on the Enterprise Claro Cloud dashboard

5. Network Configuration in Enterprise Claro Cloud

This section will show the steps necessary to be able to configure all the network services available in Enterprise Claro Cloud, taking into account the T1 Edge Gateway service as the main element.

To be able to access the general network administration panel click on the top menu to the "Networks" option.

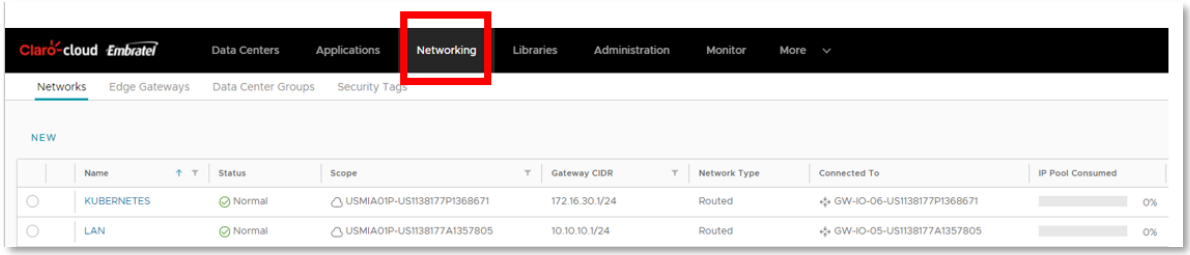


> **Note:** We recommend that you configure at least one routed network before creating Kubernetes virtual machines or clusters. For Edge instances that are generated during the default purchase process, they have the first routed network configured.

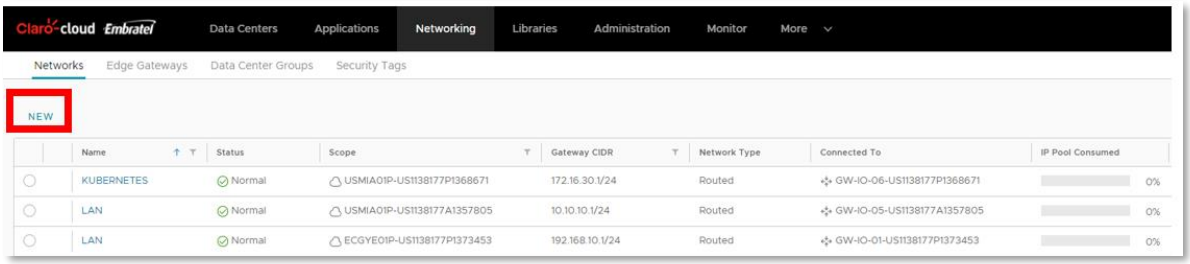
Creating a network in Enterprise Claro Cloud

Process for creating a new network in your Virtual Data Center

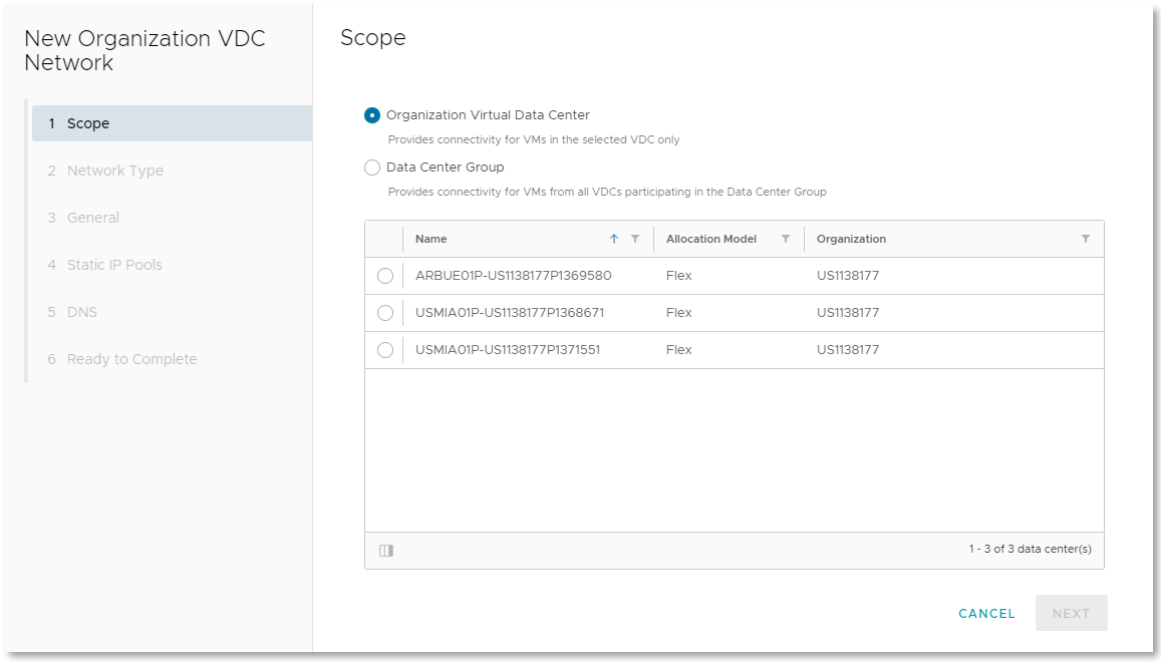
1. Enter in the top menu to the Networks section, select in the submenu the Networks section



2. Click "New"

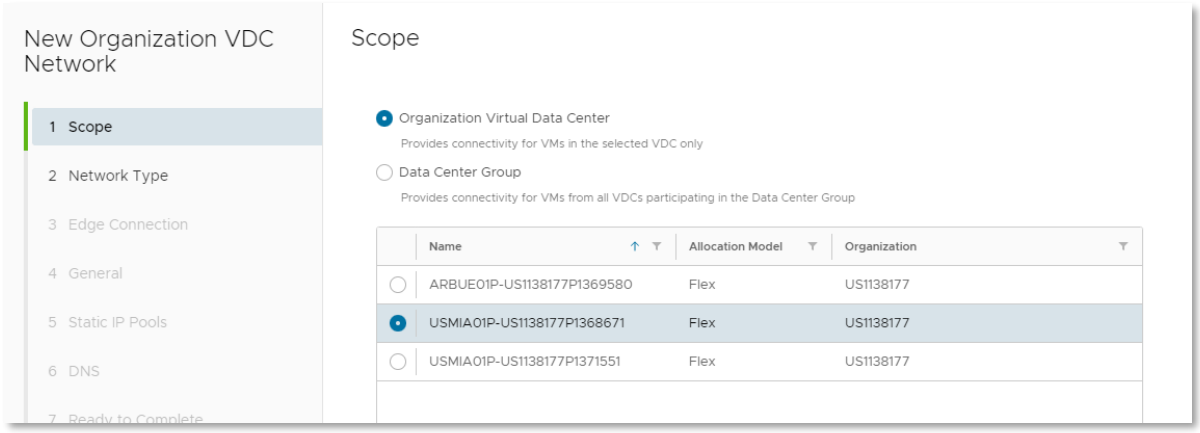


3. The following screen will be displayed

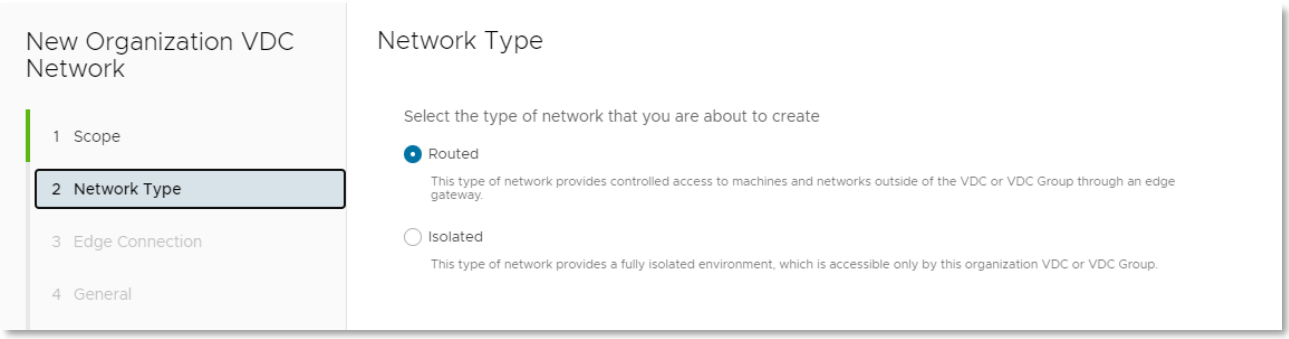


4. Choose the network range type and select the Virtual Data Center to which the network will be linked, then click Next.

Scope Type	Description
Organization Virtual Data Center	Provides connectivity only for virtual machines in a single Virtual Data Center
Data Center Group	Provides connectivity to virtual machines that are part of a Virtual Data Center group



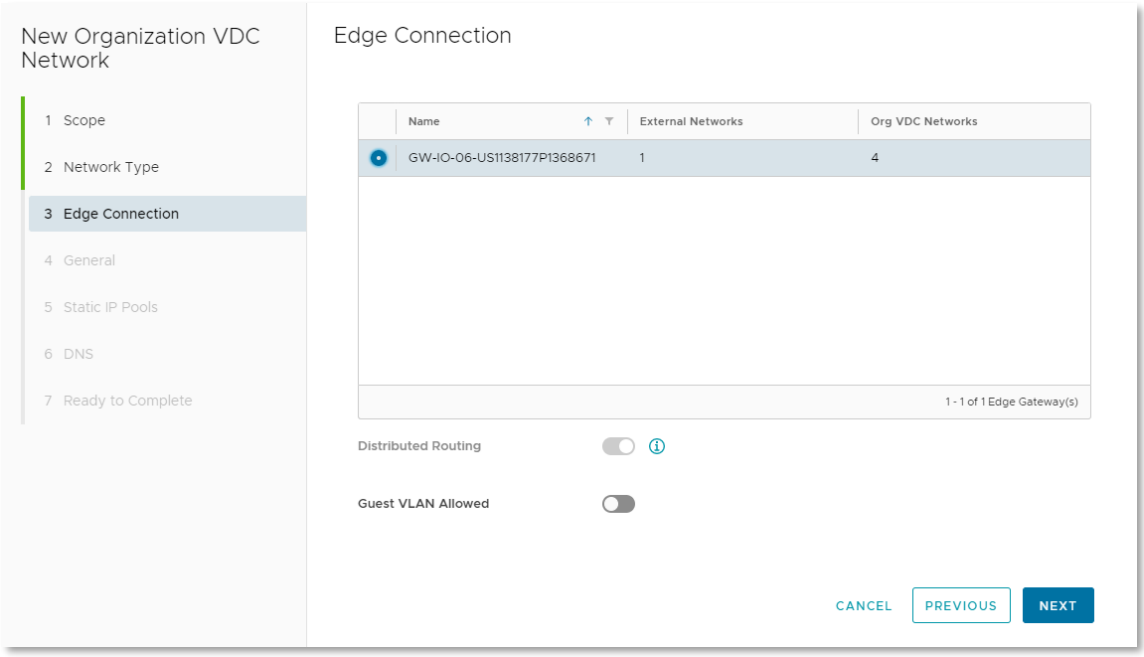
5. Choose the type of network you want to create



Network Type	Description
Isolated	Provides a fully isolated environment, to which only virtual machines can communicate within a Virtual Data Center or Virtual Data Center Group
Routed	Provides controlled virtual machine access to networks outside the Virtual Data Center or Virtual Data Center Group

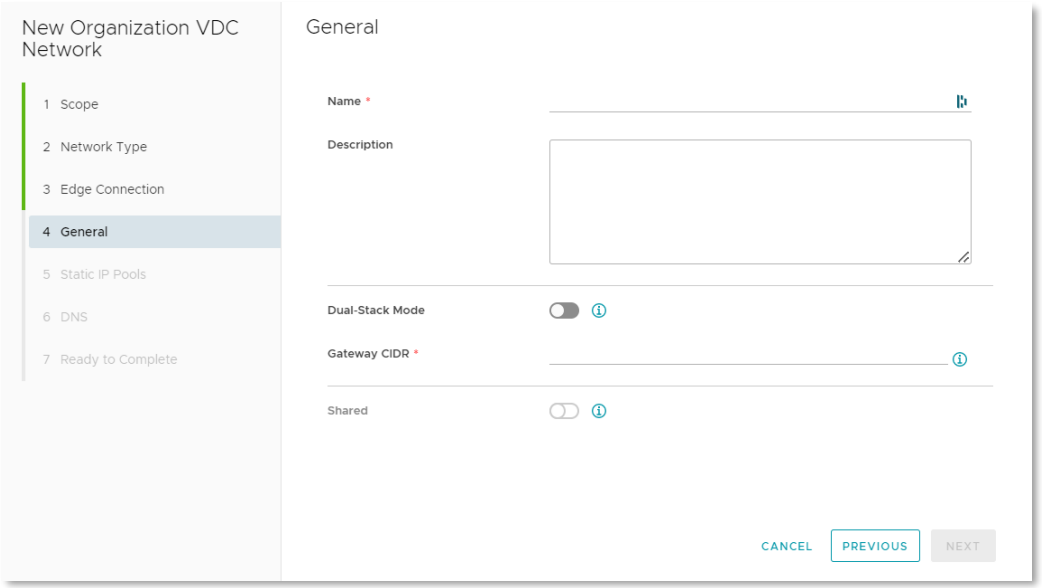
Note: If the Routed option is selected, an additional step will be displayed regarding the Edge connection

6. (For routed networks only), select the Edge Gateway where you want to host the network, click next



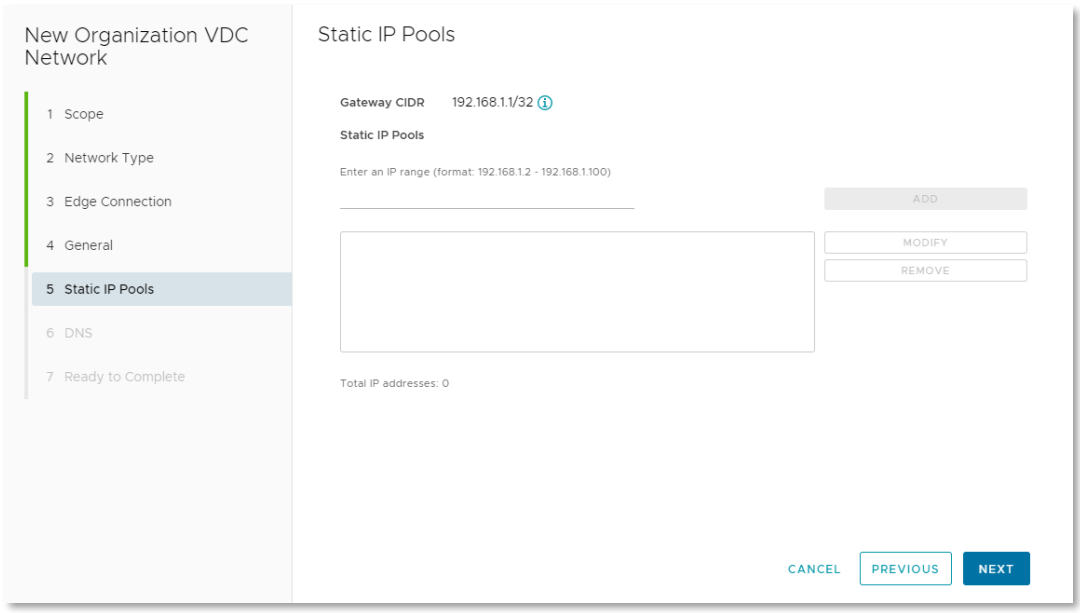
7. Set the following parameters then click next

Item	Description
Name	Name of the network to be assigned, field without character restriction
Gateway CIDR	Private IP address to be assigned as network gateway
Description (optional)	It is recommended to fill in this field for documentation and network administration purposes



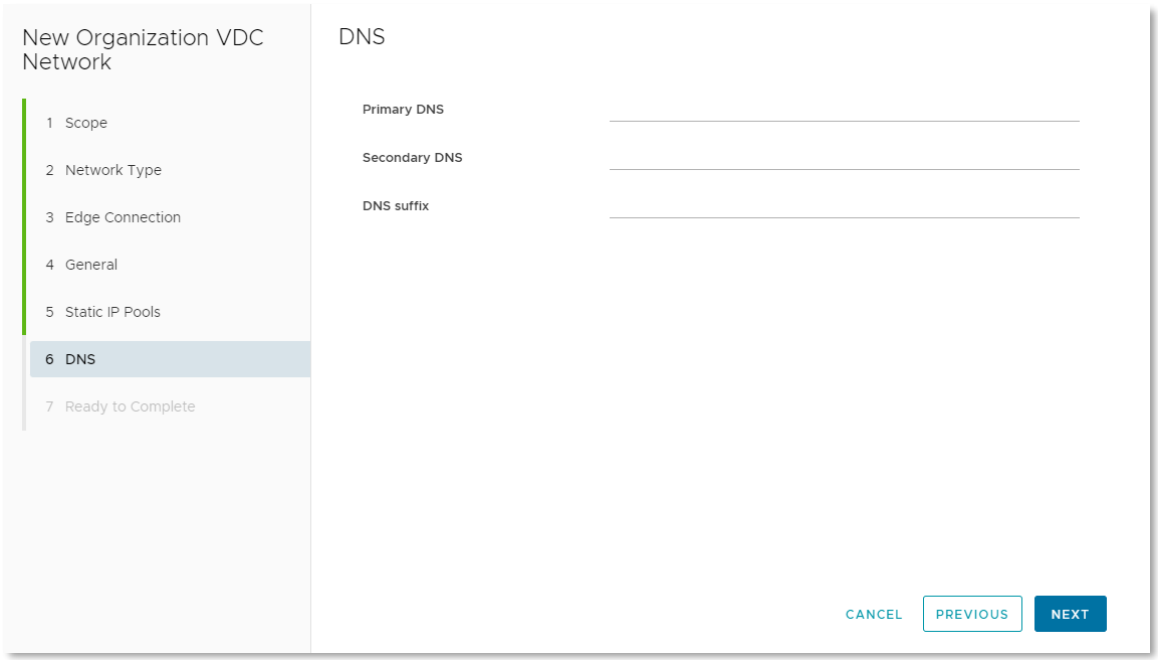
8. Add the private IP segment that you want to enable on the network, this segment needs to be compatible with the Gateway defined in the previous step. When finished click next

Important: The gateway CIDR field is set by default with the information from the previous step.

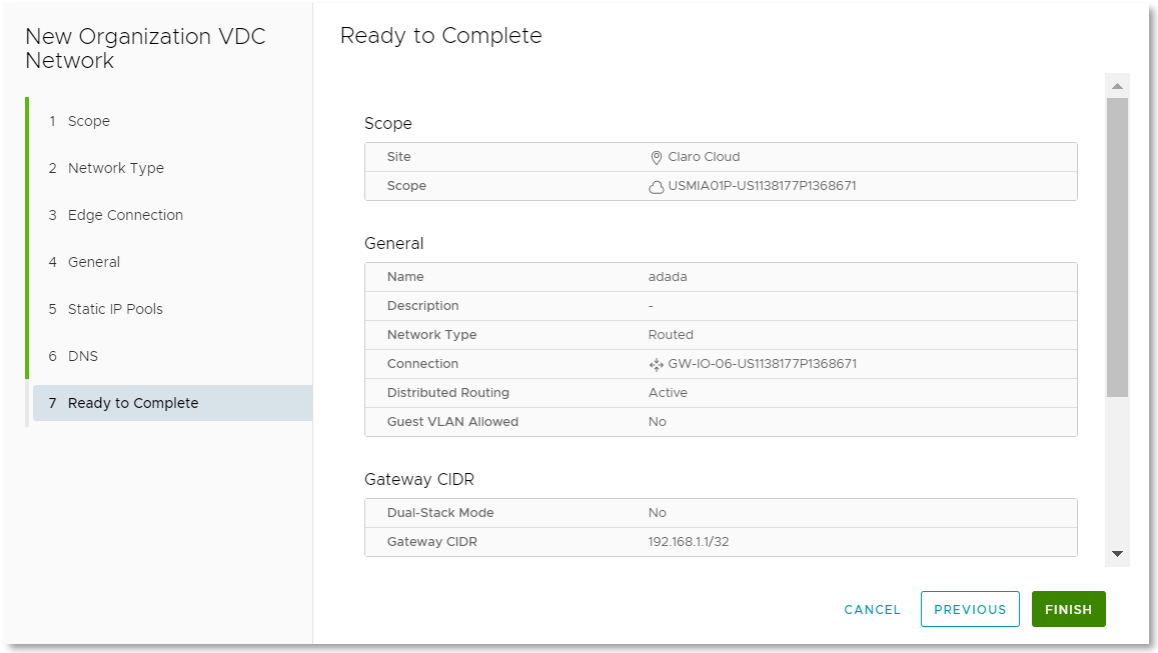


9. Enter the information regarding your DNS. If you do not have one you can use 8.8.8.8 / 8.8.4.4.

Important: If your network is intended for private access, you must use private DNS instead of public DNS



10. The summary of the network configuration will be displayed, click on finish



Configuring an Edge Gateway

During the purchase process of your first Data Center in Enterprise Claro Cloud, an Edge Gateway is added by default and at no cost

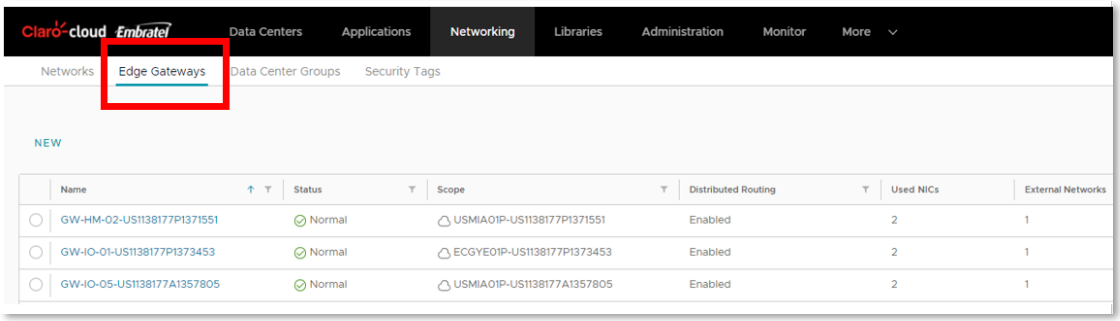
> **Note:** If you require an additional T1 Edge Gateway, you can purchase it for an additional fee. If you have Virtual Data Center in different Enterprise Claro Cloud regions, you will need to have at least one T1 Edge Gateway per region

The processes will be able to configure each available network services listed below:

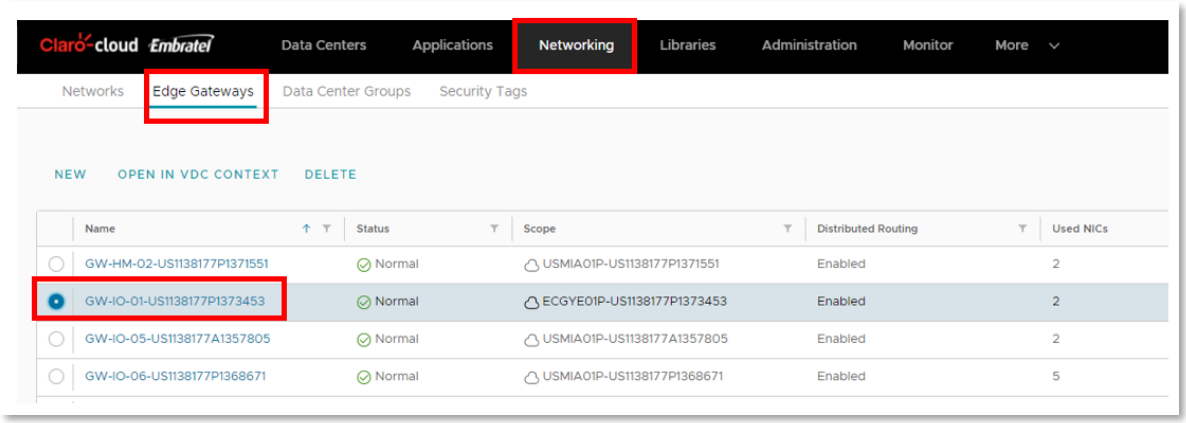
- Firewall
- NAT
- VPN IPSec
- Load Balancer
- Safety
- IP Address Management
- Routing

To access the network services management panel, follow these steps:

1. Enter in the top menu to the Networks section, then in the submenu select Edge Gateways

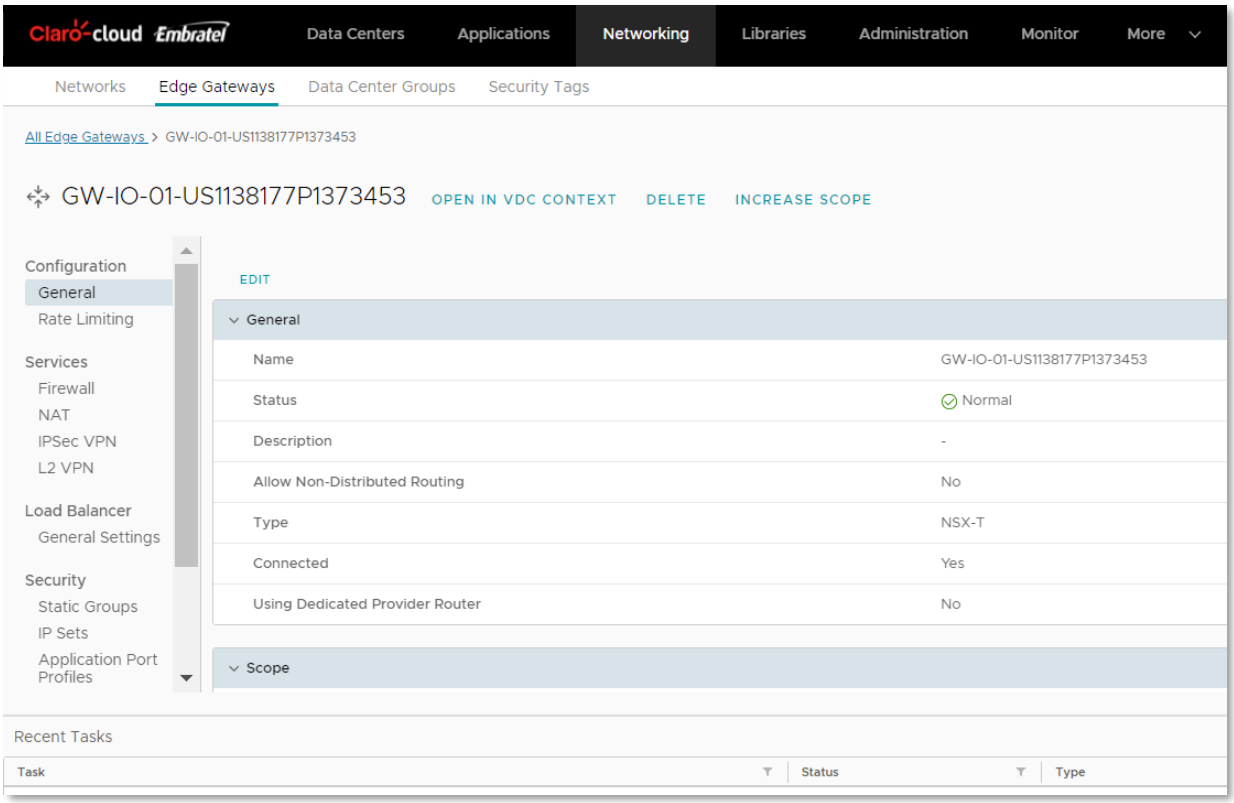


2. Select the Edge Gateway to configure



> **Important:** In the Scope column, you can see which Virtual Data Center or Group each Edge Gateway is linked to

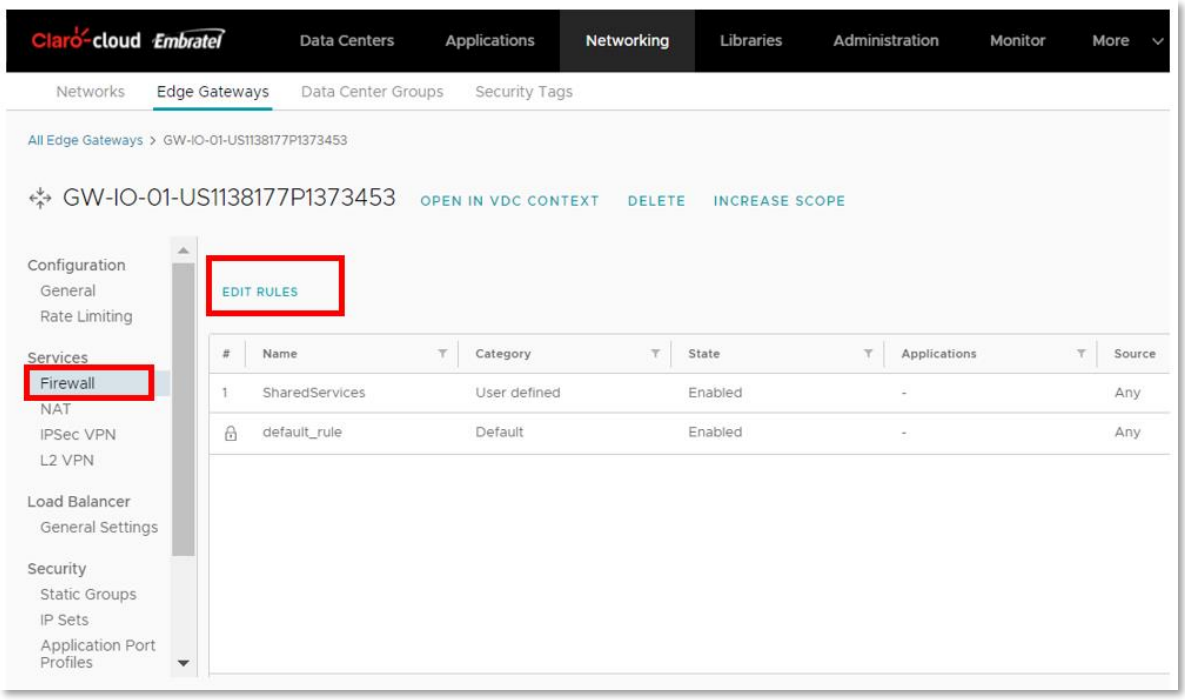
3. The following screen will be displayed which is the interface where you can configure your network services



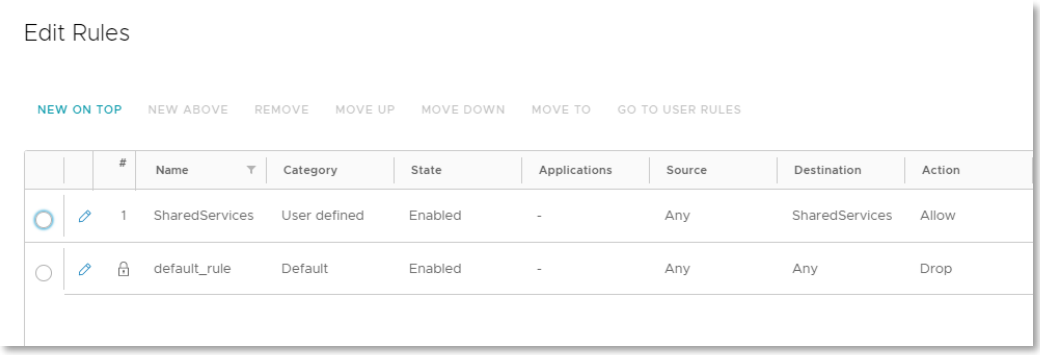
Configuring Firewall Rules

Firewall rules settings are available in this section. It is possible to create, edit and delete rules according to the needs of your organization,

1. Select the Firewall option and click the "Edit Rules" button



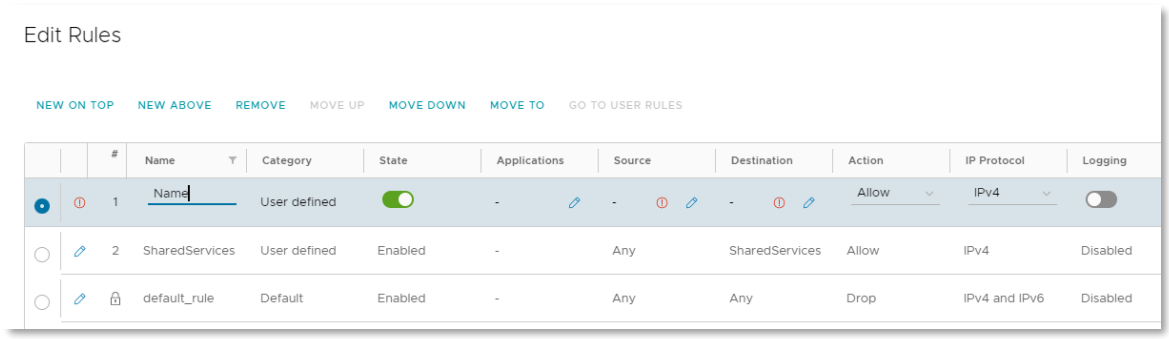
2. The following screen will be displayed, where you must click on the "New On Top" button



3. A line will be added in the table, where you will need to enter the following information. When finished, click the save button

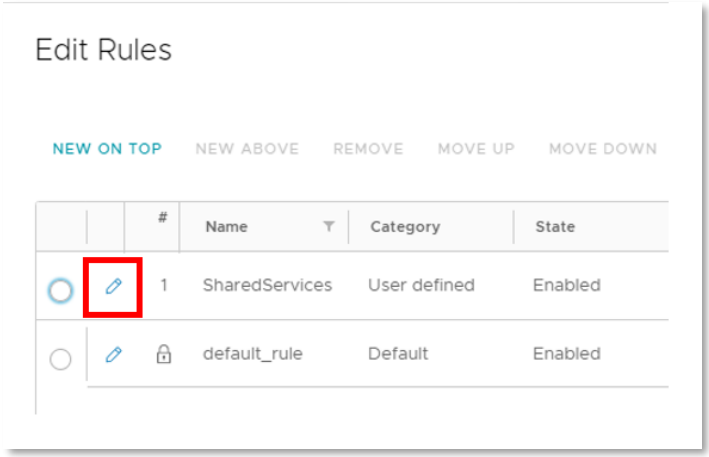
Item	Description
Number	Firewall rule name
State	Enabled | Disabled
Applications	TCP/UDP access ports
Origin	Source IP segment
Destiny	Source IP segment
Action	Allow / Block / Deny
Protocol	Protocol used for IPv4 / IPv6 communication

Registration	Enable/Disable Event Logging over the Firewall

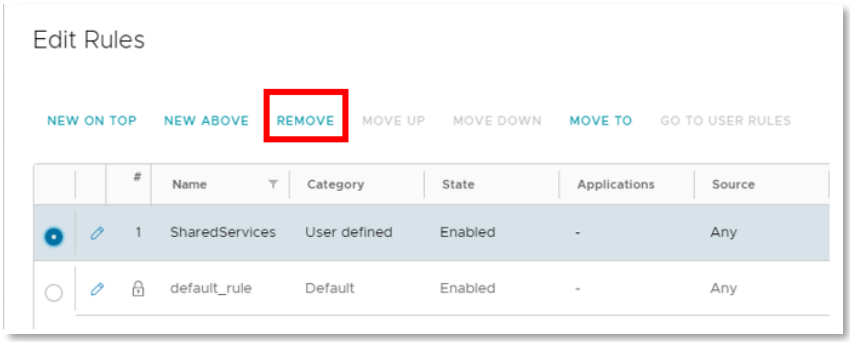


Process for Editing or Deleting Firewall Rules

4. To edit a rule click the pencil button, then click save button when finished



5. To delete a firewall rule, select the rule and click Remove, then click on save button.



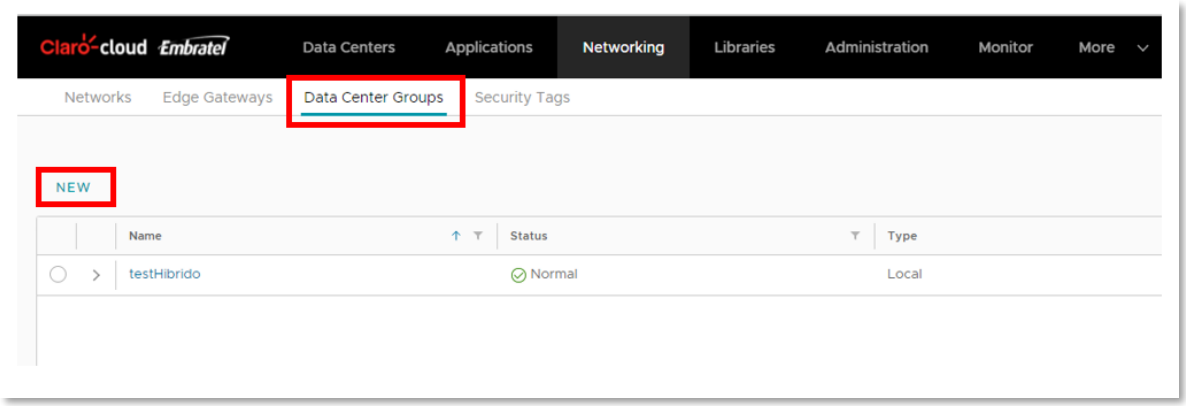
Enabling and Configuring Distributed Firewall

In this section you can activate and configure your Distributed Firewall.

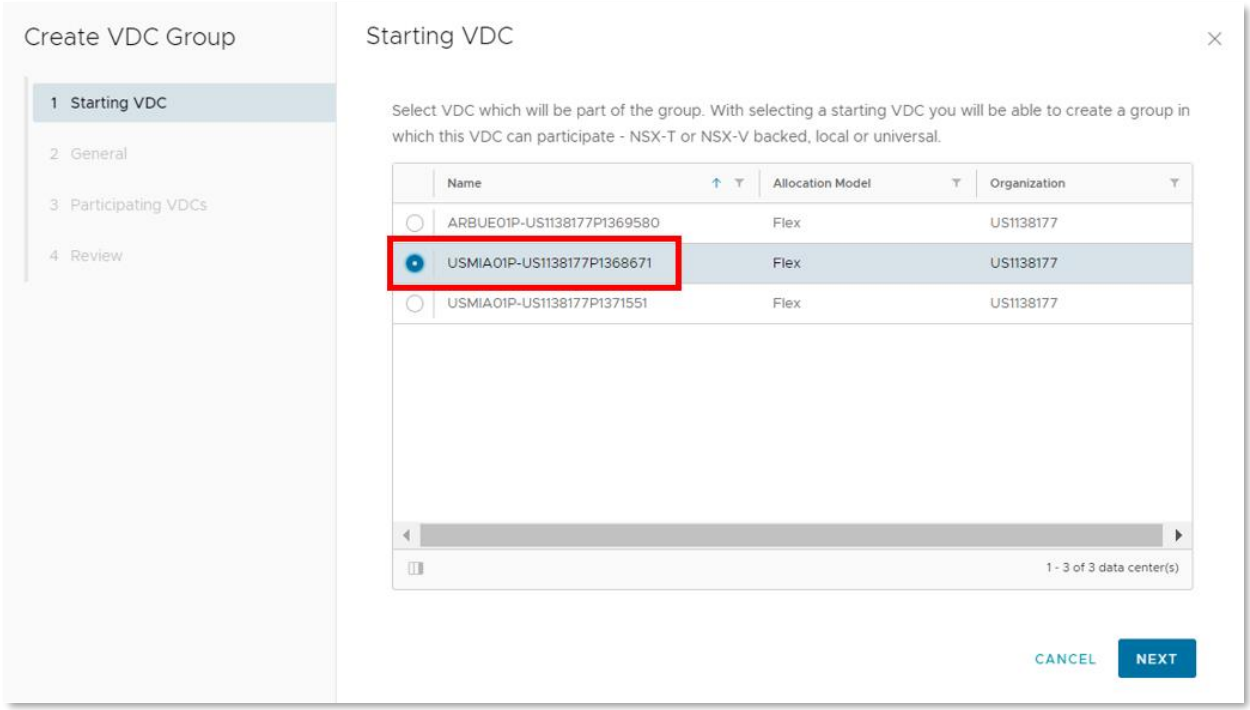
Within the available functionalities of Enterprise Claro Cloud, you will be able to communicate through extended networks with multiple data centers in the same region, these communications can be managed and segmented through a Distributed Firewall.

Before you can activate the Distributed Firewall service, you must create a Data Center group with the following process.

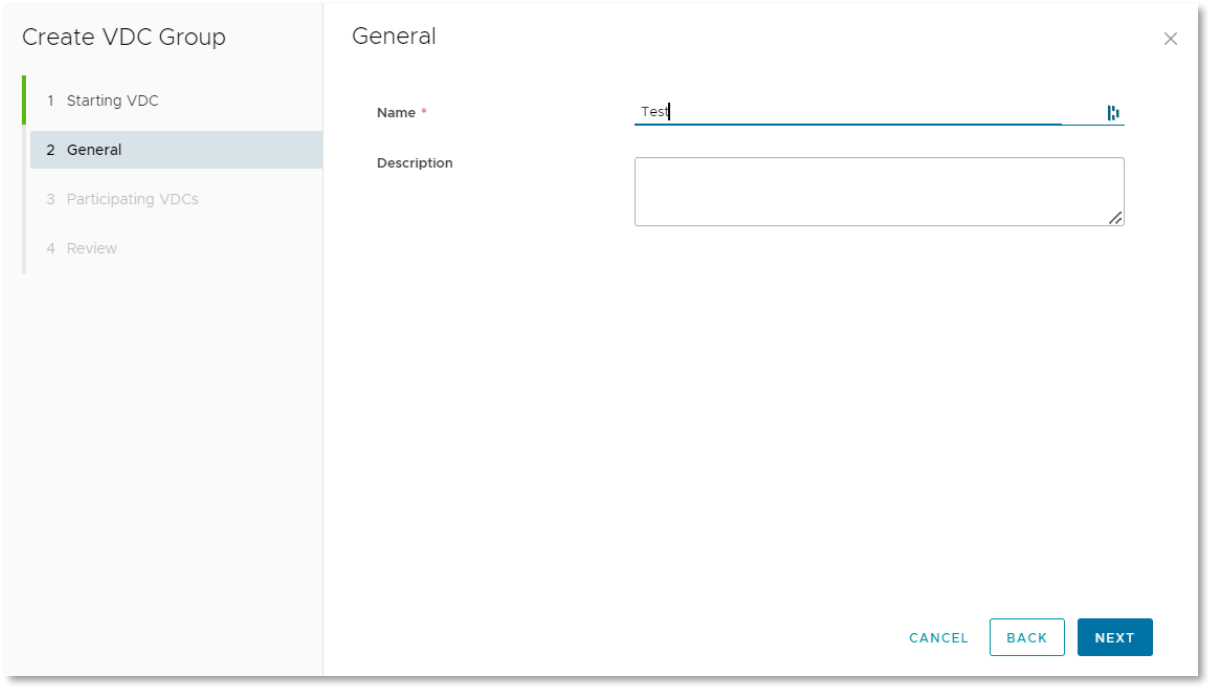
1. Enter in the top menu to the Networks section, in the submenu select Data Center Groups, click on "New"



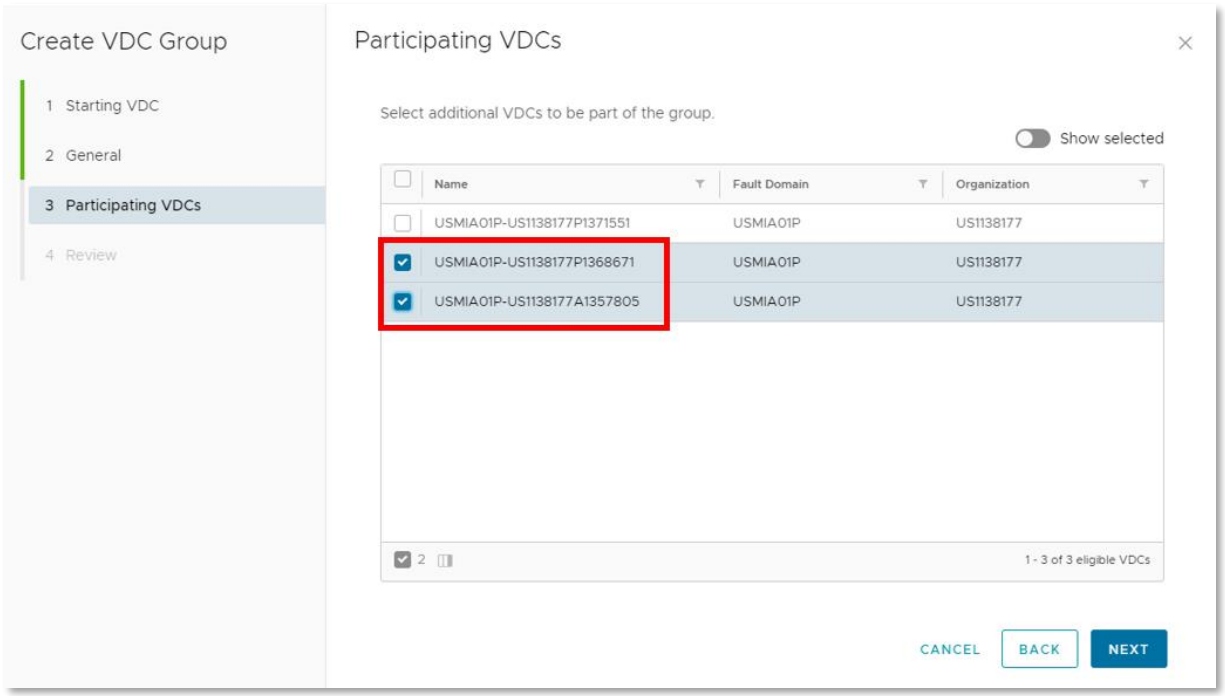
2. The following screen will be displayed where you must select the initial Data Center, it is advisable to select a Data Center that has an Edge instance assigned to allow connections to the outside (Internet or MPLS), if required. Click "Next"



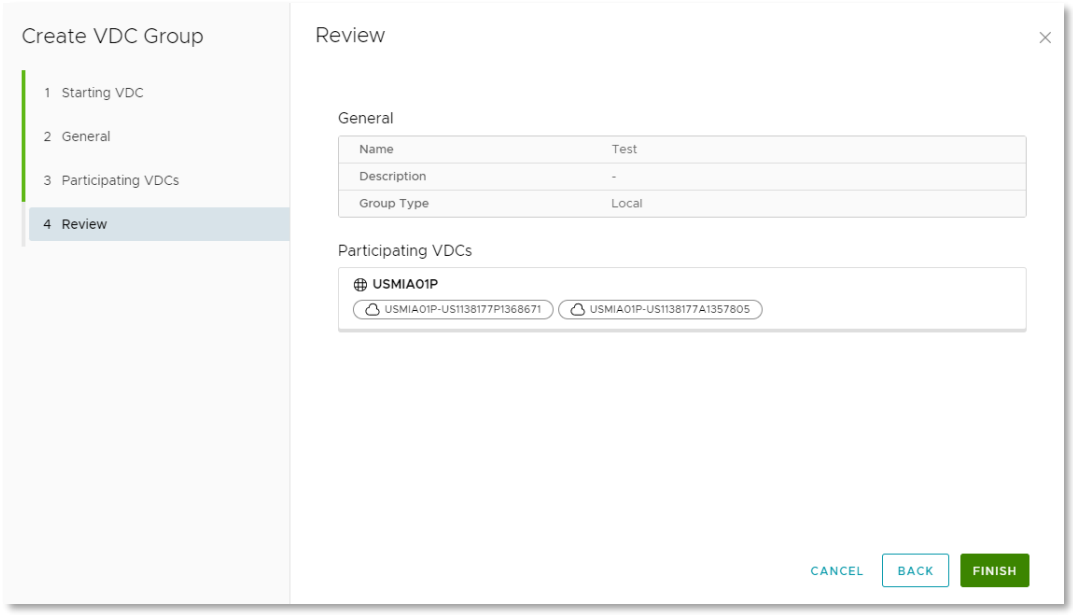
3. Enter the name and optionally a description, when finished click on "Next"



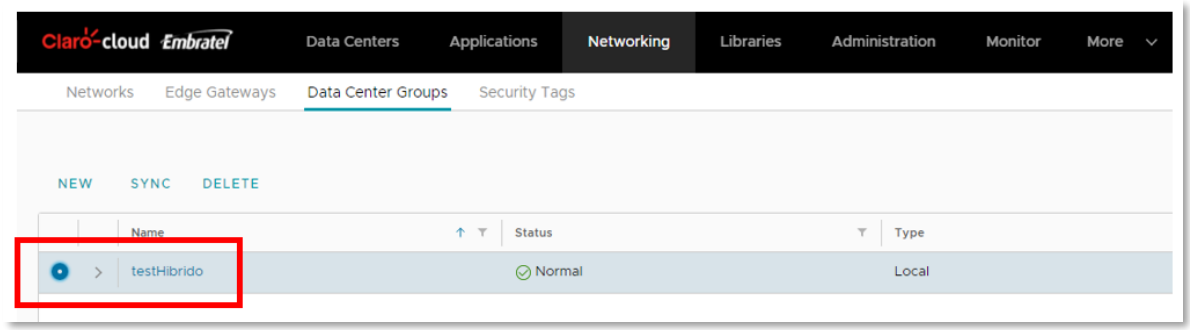
4. Select the Data Centers that will be added to the group, by default the Data Center indicated in step 2 will be preselected, when finished click on "Next"



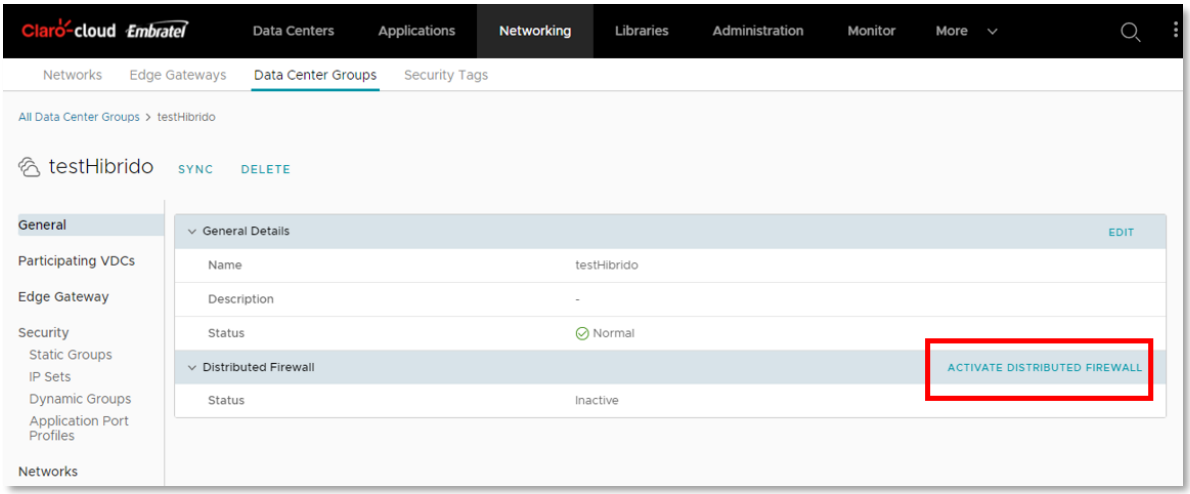
5. A summary with the defined group configuration will be displayed, click "Finish" to start the creation of the Group. Upon end of group creation, you will be able to view your group in the Data Center Groups section.



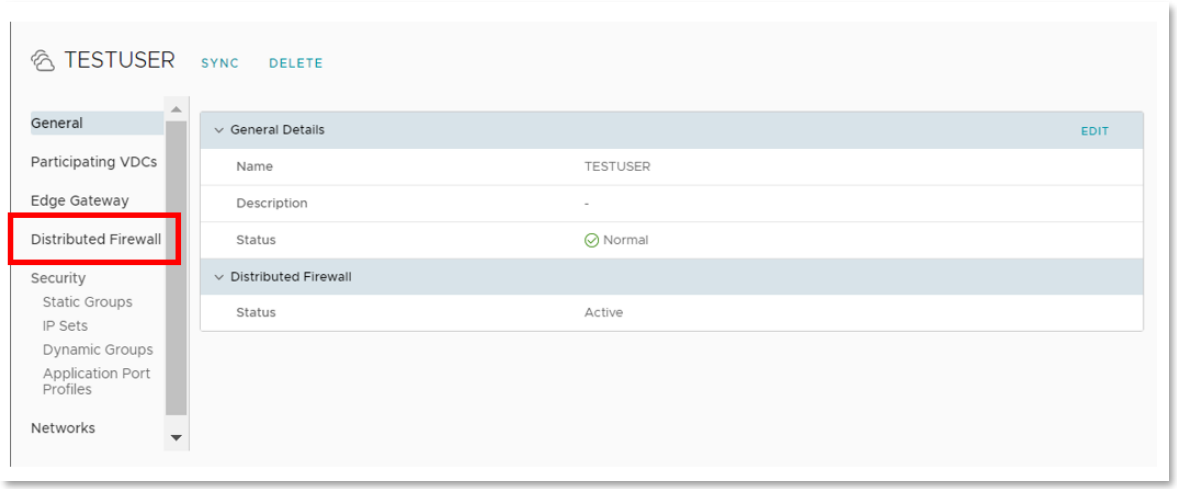
6. To enable distributed firewall, click the name of the group created.



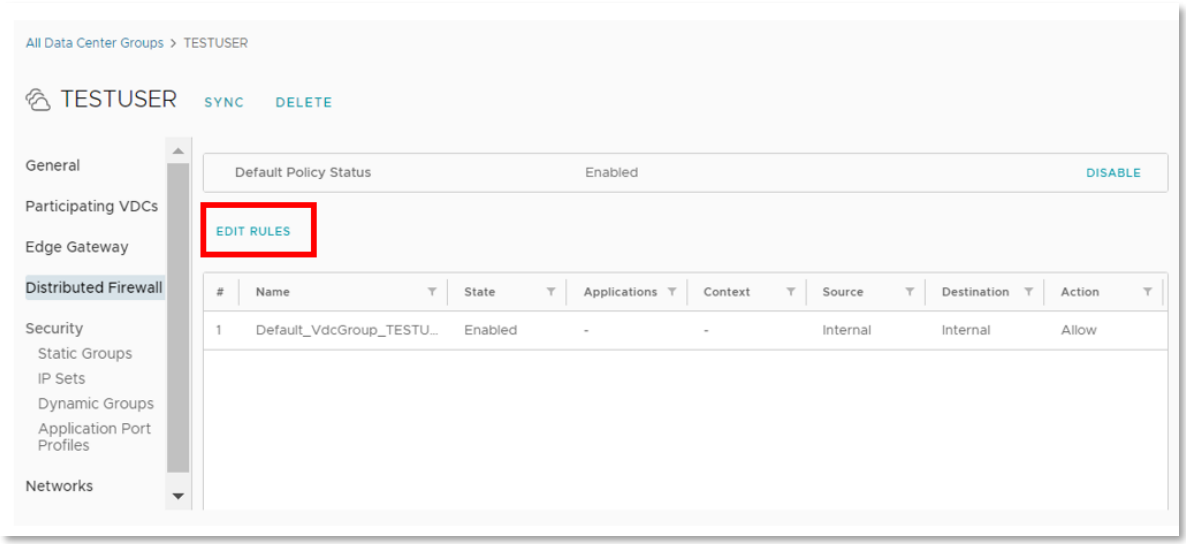
7. The following screen will be displayed, in General within the line Distributed firewall, click on "Activate"



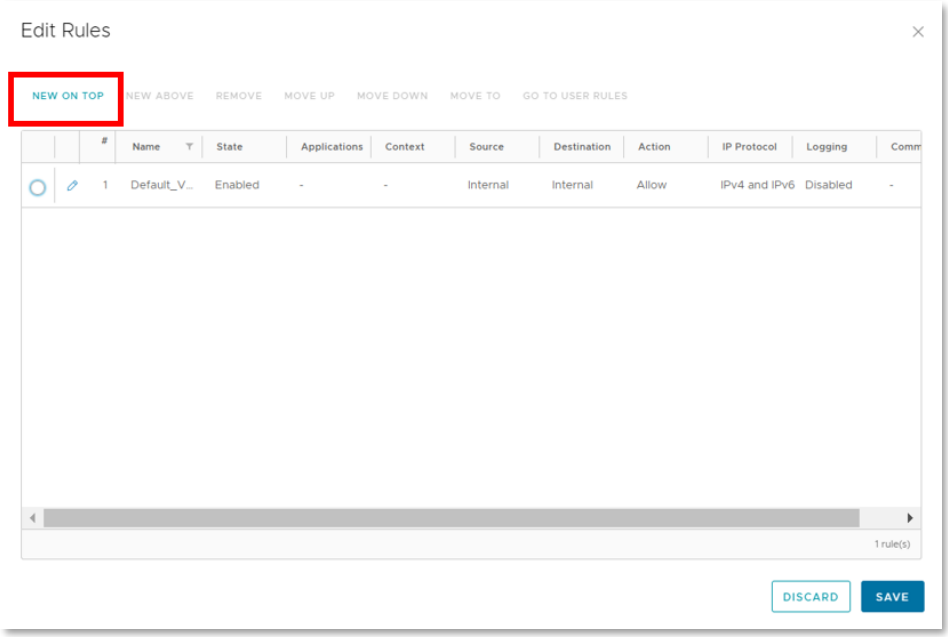
8. A new option will be enabled within the left menu "Distributed Firewall", click on the new option



9. The dashboard for configuring firewall policies is displayed. To create a firewall rule click "Edit Rules"



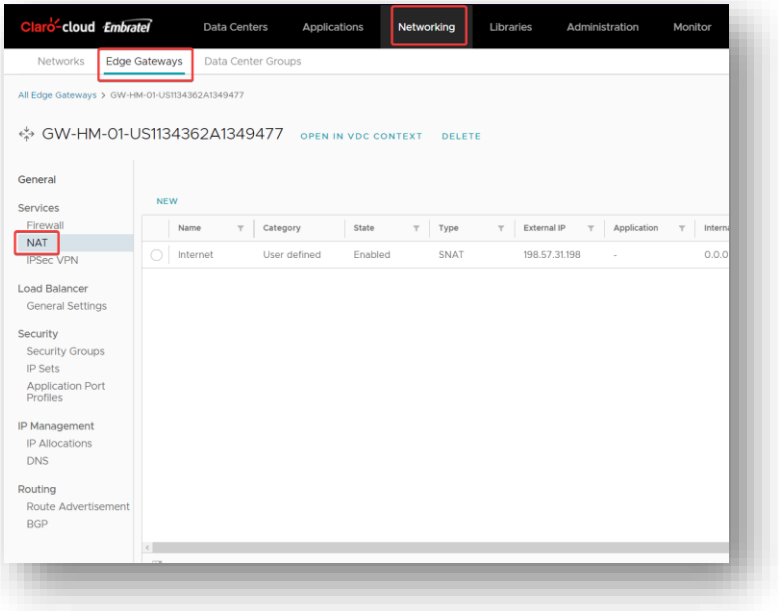
10. The following screen will open, click "New at the top", follow the process described in the chapter "Configuring Firewall Rules"



11. At the end click on "Save"

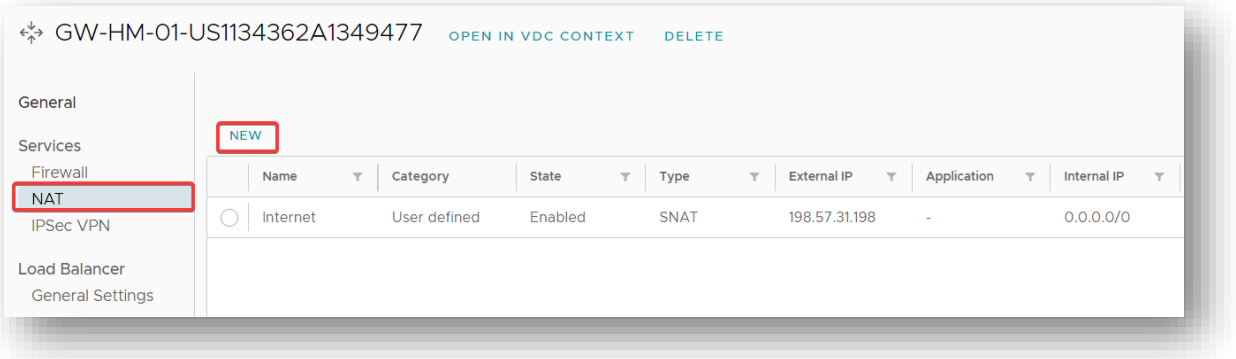
Configuring NAT Rules

In this section, you can configure, edit, and delete NAT rules according to your organization's needs.



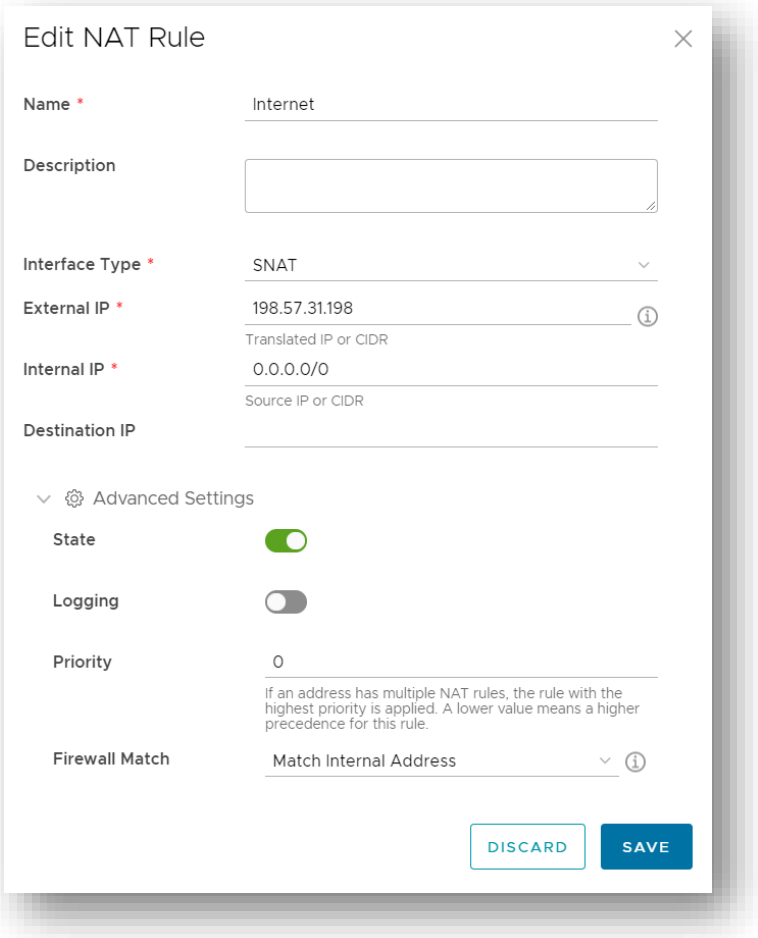
To configure a NAT rule, follow the following process

1. Select the NAT option and click the "New" button

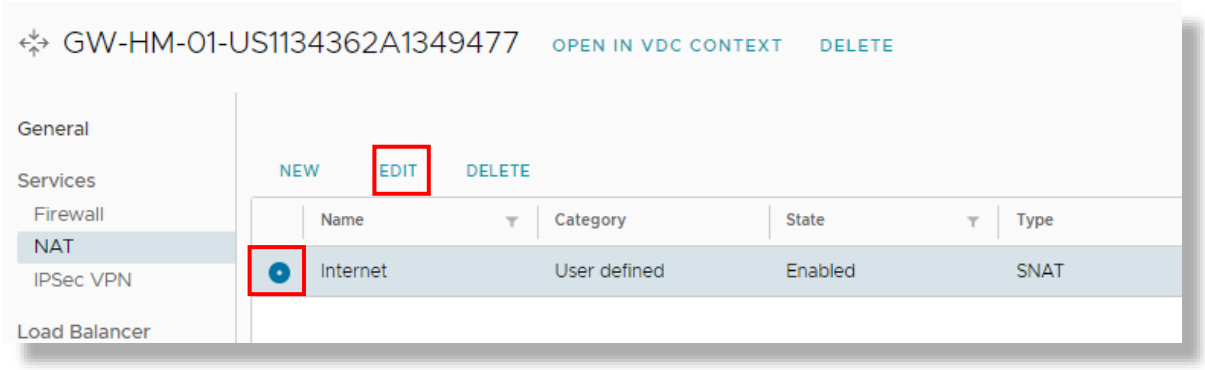


2. The following screen will be displayed where you will have to enter the following information. At the end of clicking the save button

Item	Description
Name	NAT rule name
Description (Optional)	Description of the NAT rule
Interface Type	Select NAT Type DNAT / SNAT / NO DNAT / NO SNAT
External IP	External IP where NAT will be applied
External port	External source port
Internal IP	IP to where the redirect is made
Application	Port where the service is exposed
Status (Advanced Settings)	Service enabled/disabled
Registration (Advanced Settings)	Events
Priority	NAT rule priority (Lower value higher priority)
Firewall Match	Match Internal Address / Match External Address / Bypass

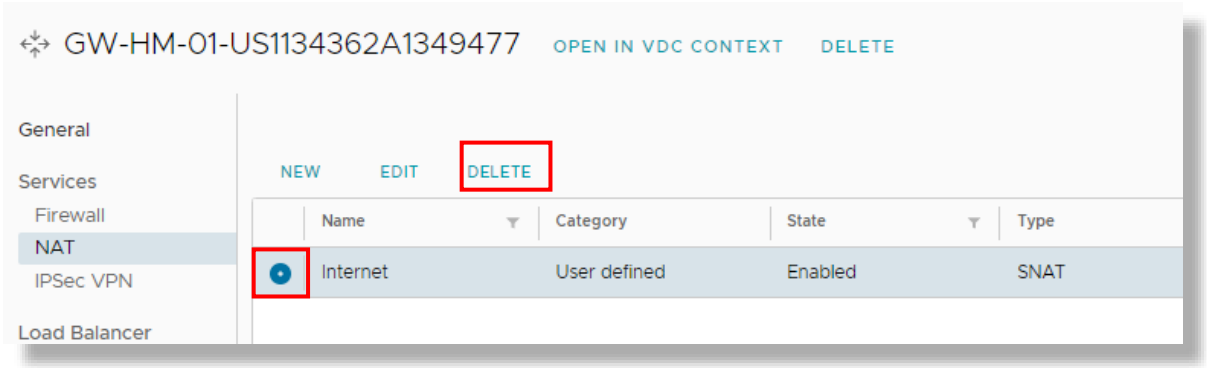


3. To Edit a rule, select the rule to edit and click the Edit button



4. The screen shown in step 4 will open to edit all previously configured parameters. When finished click save

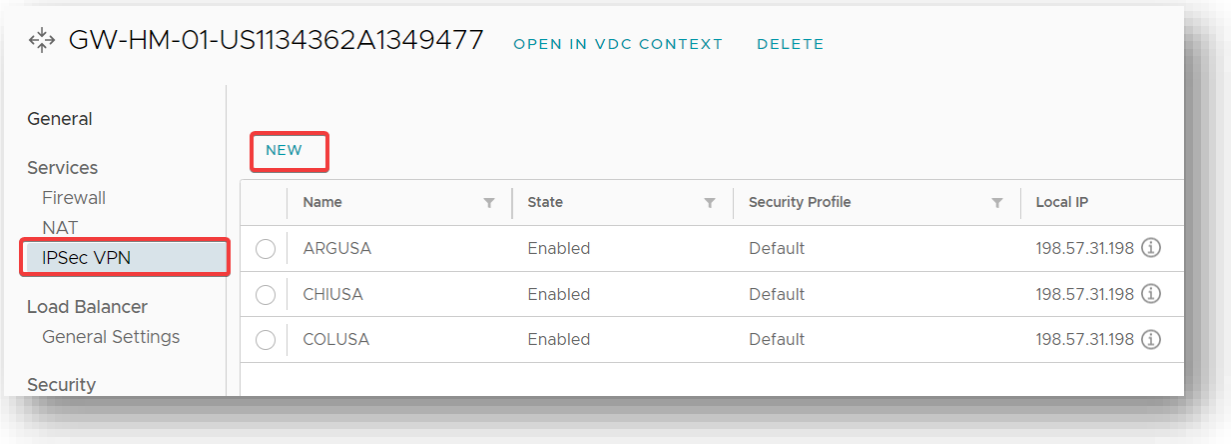
5. To Delete a rule, select the rule and click the Delete button



Configuring IPsec VPN

in this section you will find the procedure to configure an IPsec VPN

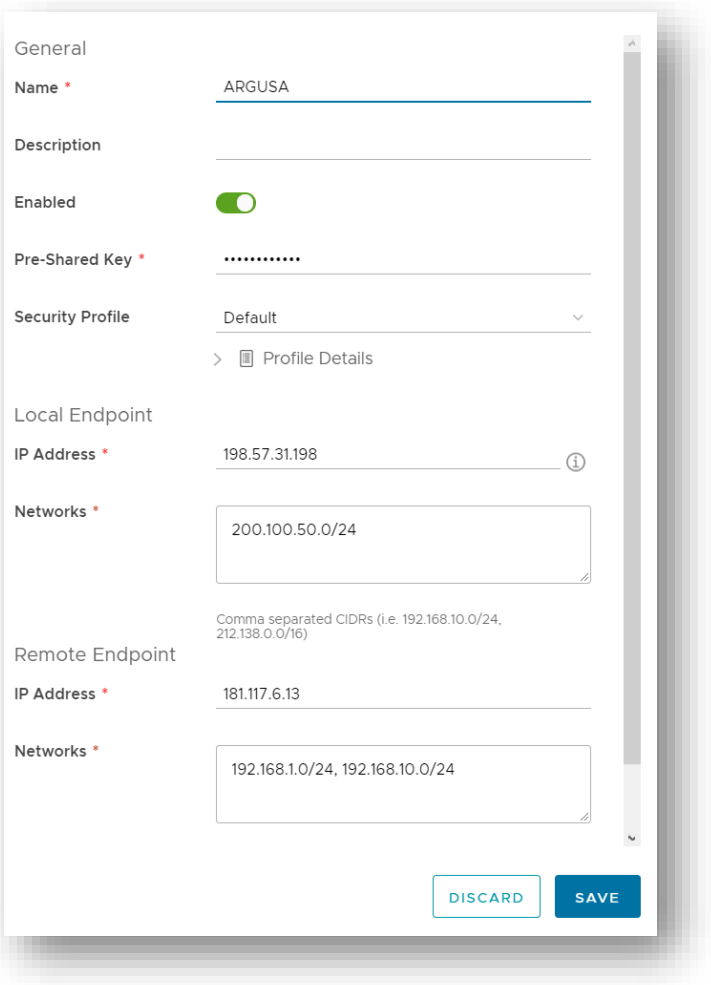
1. Within the T1 Edge Gateway panel, select the "IPsec VPN" option and click the "New" button



2. The following screen will be displayed where you will have to enter the following information. When finished click save

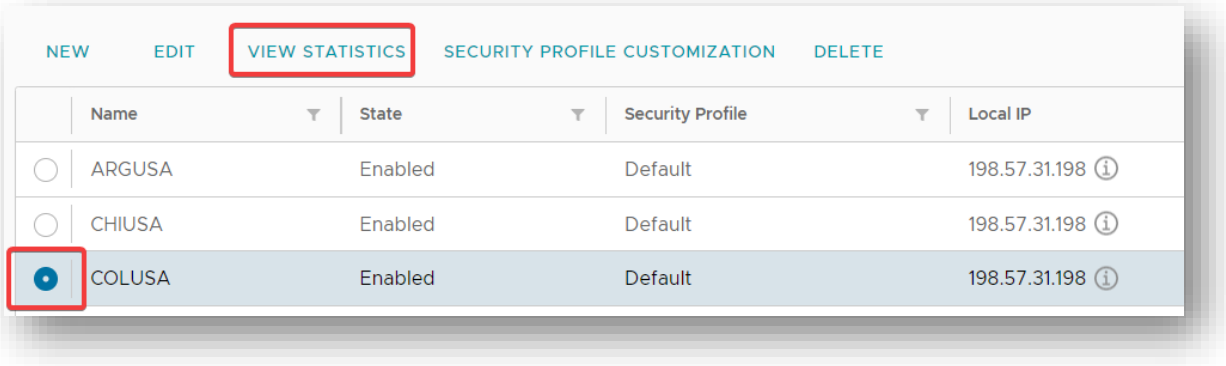
Item	Description
Enabled	Slider button to enable/disable connection
Pre-shared key	Security key, must be shared with the other party to ensure connection settings
Safety Profile	Keep in the standard option
IP Address (Local Endpoint)	Edge Gateway public address
Redes (Endpoint Local)	Local networks which will have access from the VPN connection
IP Address (Remote Endpoint)	Remote Gateway Public Address

Networking (Remote Endpoint)	Remote networks which will have access from the VPN connection

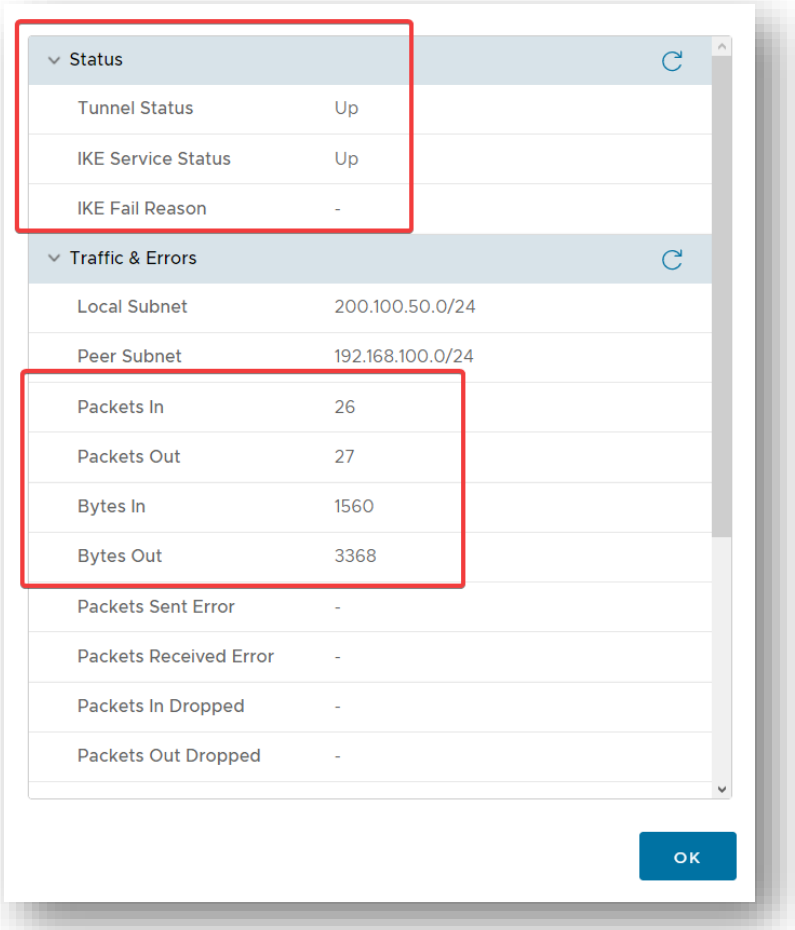


Important: You need to replicate step 1 and 2 to the other end of the VPN connection. Whereas this extreme is now considered the destination

3. To validate the correct VPN configuration select "View statistics"



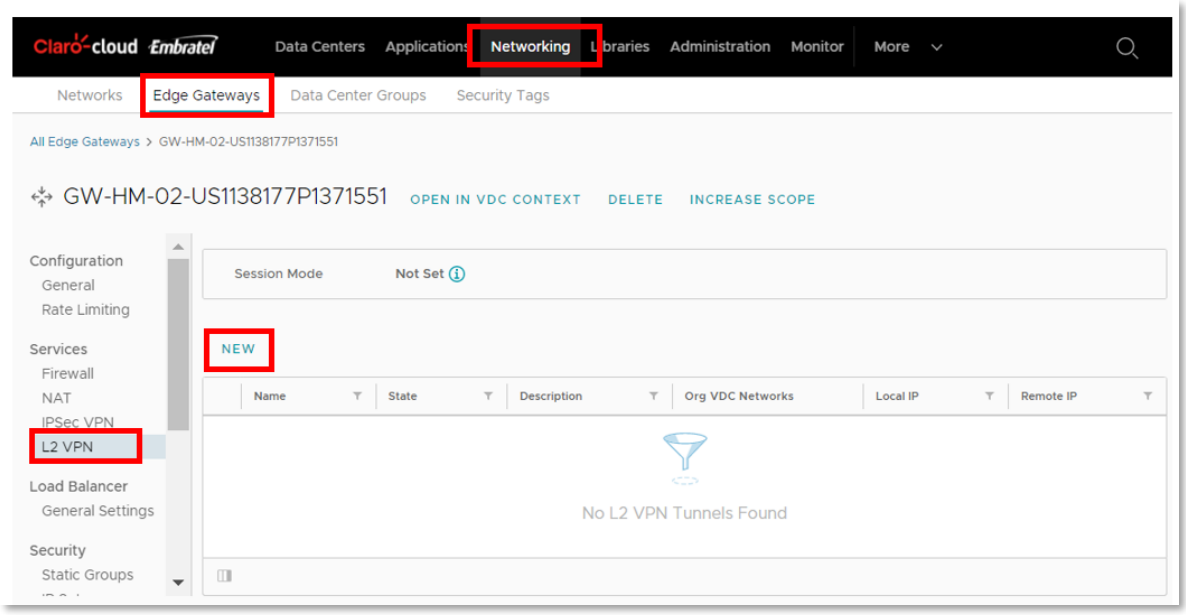
4. The following screen will open where you can view the status of the tunnel as well as the incoming and outgoing byte packets



L2 VPN Configuration

In this section you will find the procedure to set up an L2 VPN from your control panel.

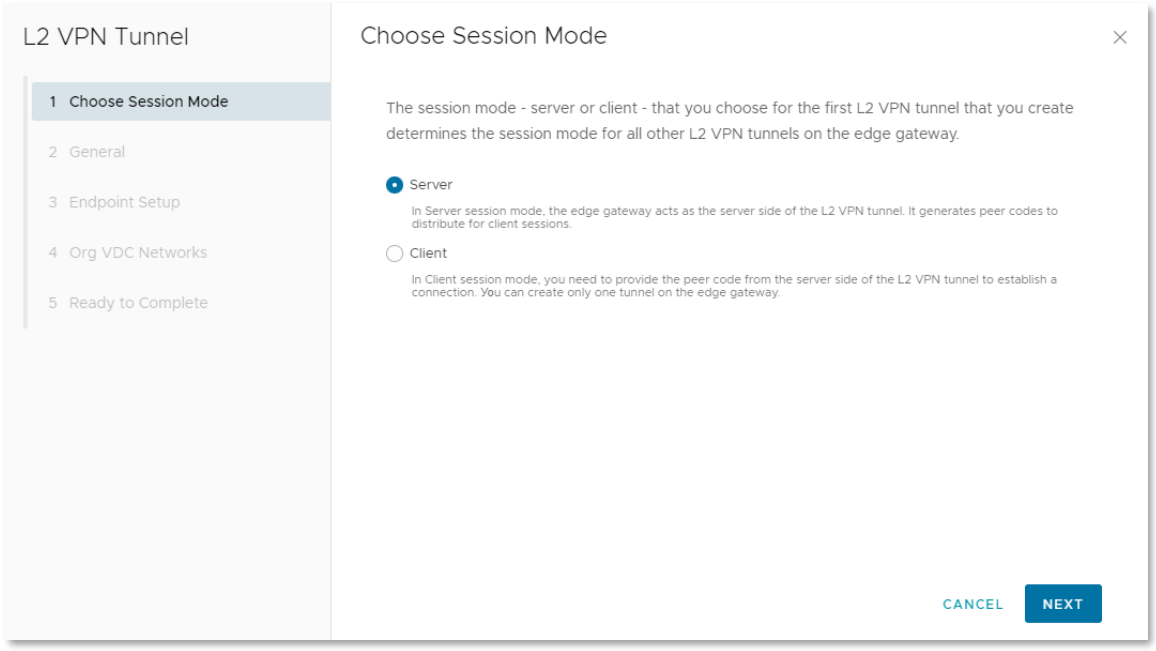
1. Within the T1 Edge Gateway dashboard, select the "L2 VPN" option and click the "New" button



2. The following screen will be displayed, where you must specify the type of session with which you want to configure the T1 Edge Gateway instance, click next.

Session type	Description
Server	In "Server" session mode, the T1 Edge Gateway acts as the server side of the L2 VPN tunnel. Generates peer codes to distribute for client sessions.
Customer	In the "Client" session mode, you must provide the pair code generated from the server side of the L2 VPN tunnel to establish a connection. Only one tunnel can be created on the T1 Edge Gateway.

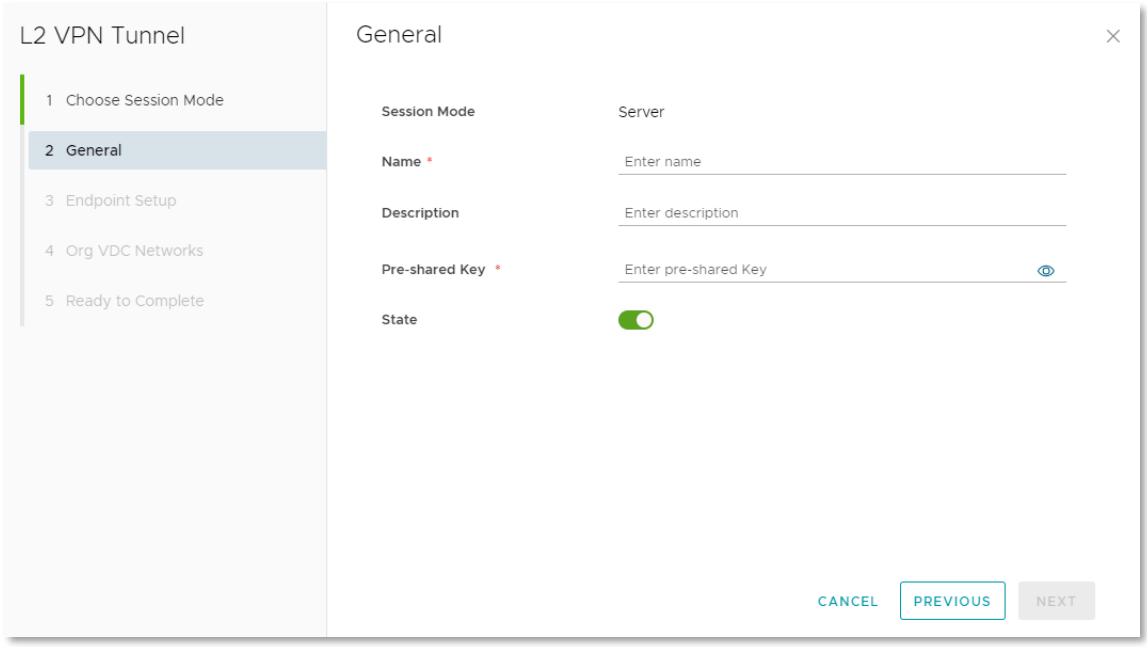
Important: You will be unable to change the session type of the T1 Edge Gateway after the first VPN tunnel is established



Server Mode

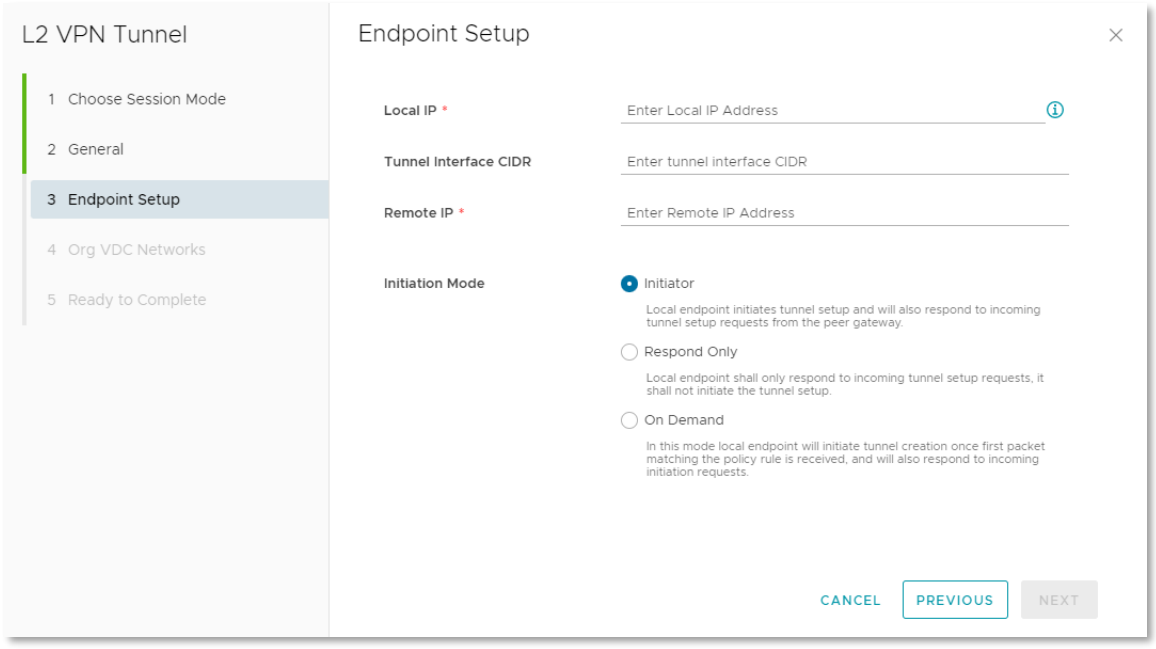
3.1.1. The following information must be entered in the General section, at the end click next

Item	Description
Name	Name by which the VPN tunnel will be identified
Description	Optional field, for a brief description
Pre-Shared Key	Secure key with which clients can link to the tunnel
State	Enabled or Disabled

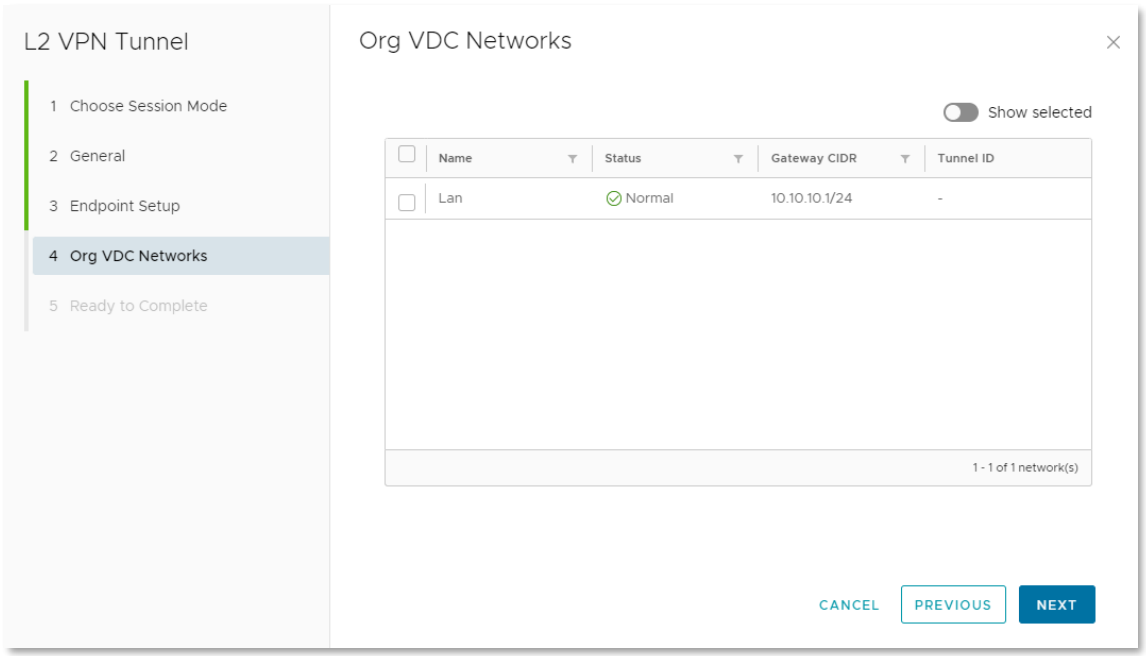


3.1.2. The Endpoint Setup section will be displayed, where the following information must be entered, when finished click on Next

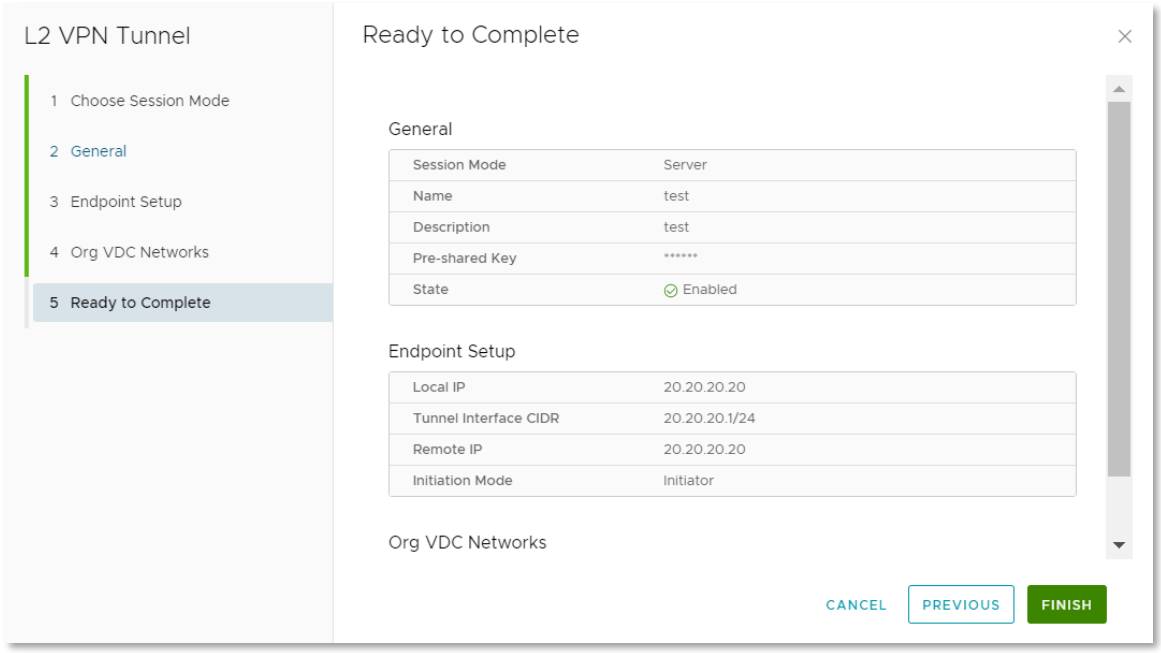
Item	Description
Local IP	Enter the public IP of the T1 Edge Gateway
Tunnel Interface CIDR	Enter the segment to be published inside the VPN tunnel
Remote IP	Enter the public IP of the remote node to connect "Client"
Initiation mode	Select the communication initiation mode from the server to the client, there are 3 options: 1. Initiator - The Endpoint initiates tunnel configuration and will also respond to incoming requests from the Edge Gateway. 2. Respond Only - will only respond to incoming tunnel configuration requests, it will not start tunnel configuration. 3. On Demand - will initiate tunnel creation once the first packet matching the policy rule is received and will also respond to incoming startup requests.



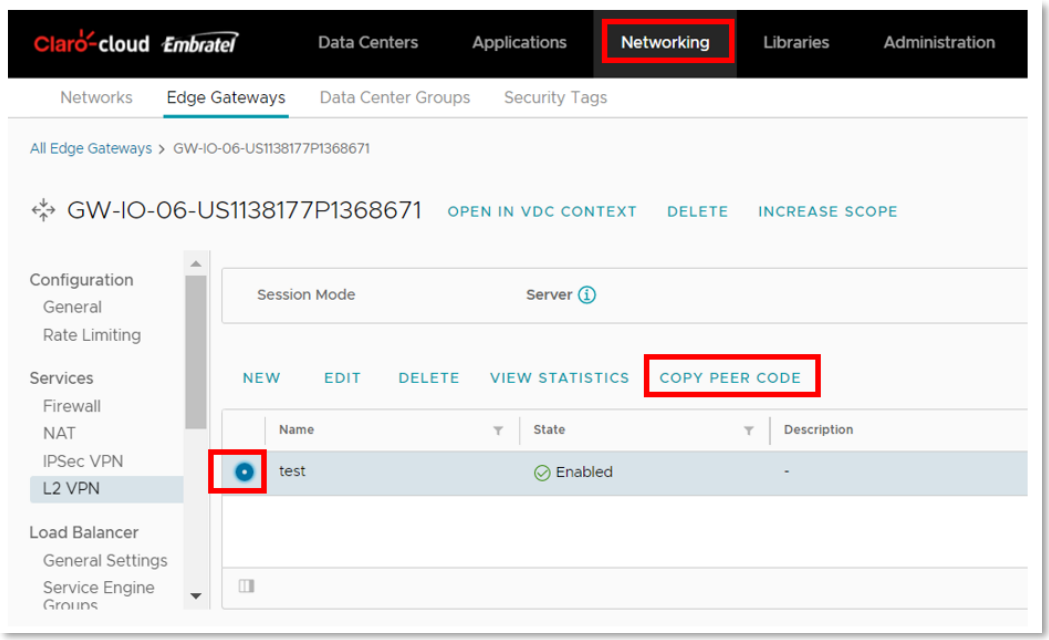
3.1.3. The Org VDC Networks section will be displayed, where the internal networks of the DCV that will allow the client to be published through the VPN tunnel must be selected, at the end click Next.



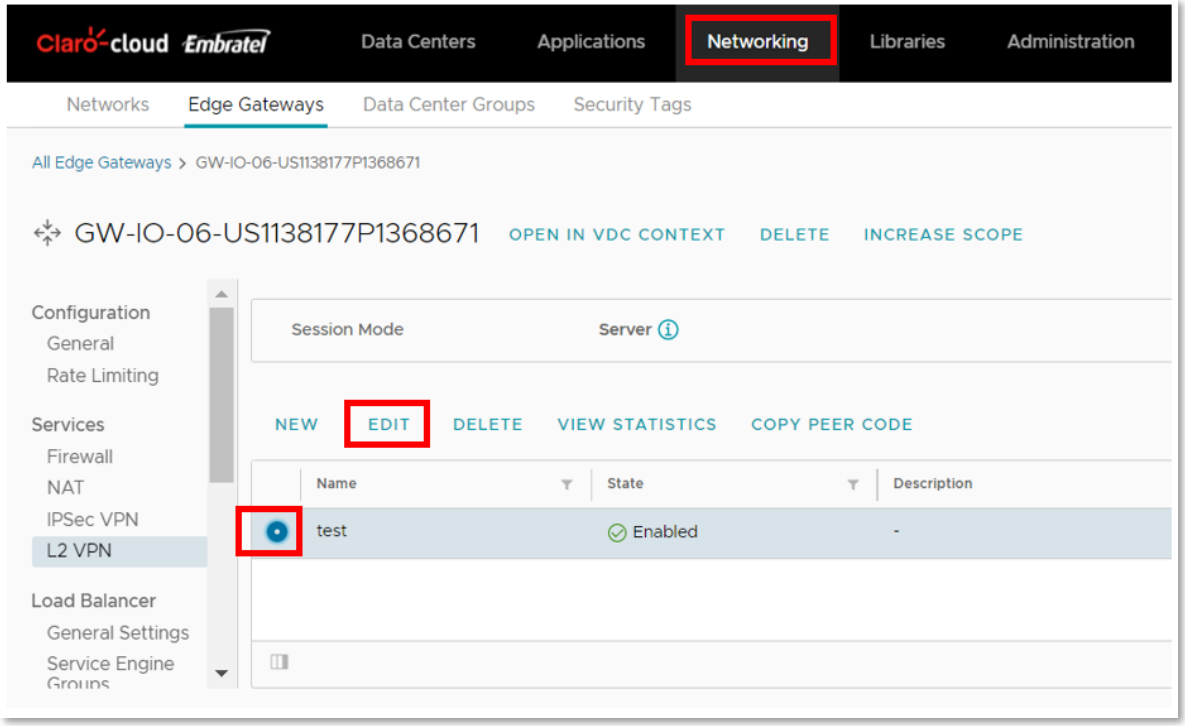
3.1.4. A summary with the configuration made will be displayed, click Finish



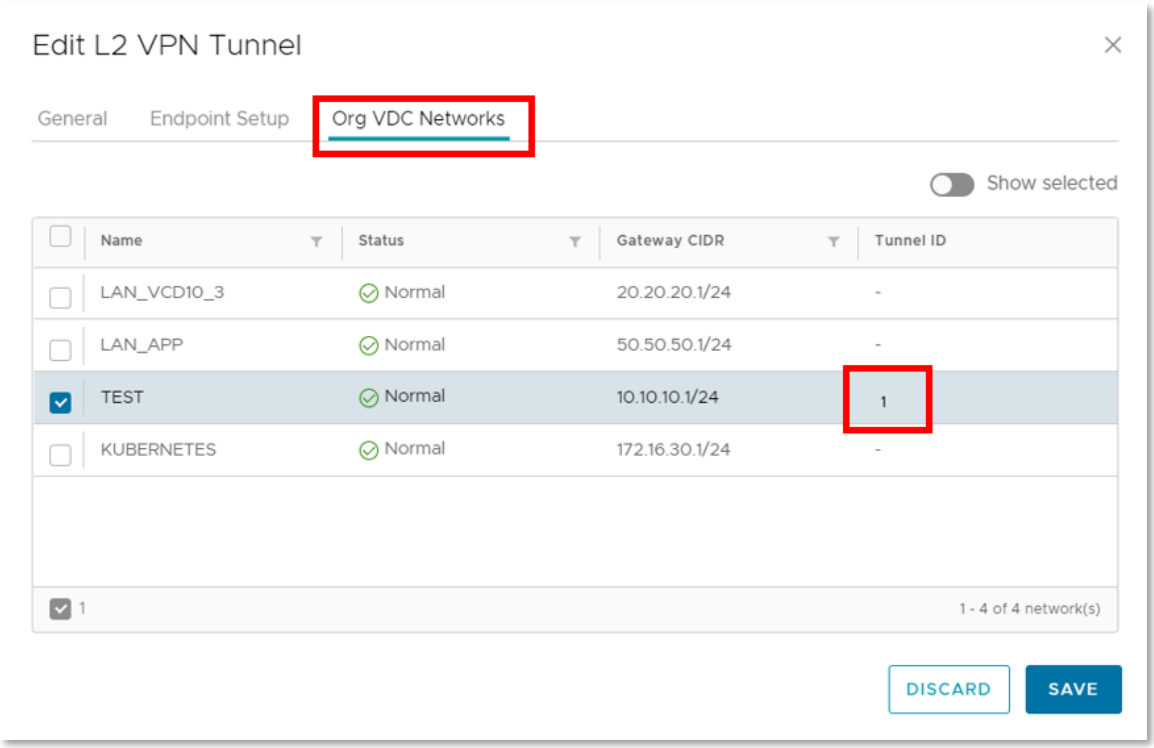
3.1.5. Once the provisioning of the link is finished, the peer code can be generated, which the client requires to establish communication, select the link and click on the "Copy Peer Code" button



3.1.6. To display the Tunnel ID parameter simply click on "Edit"



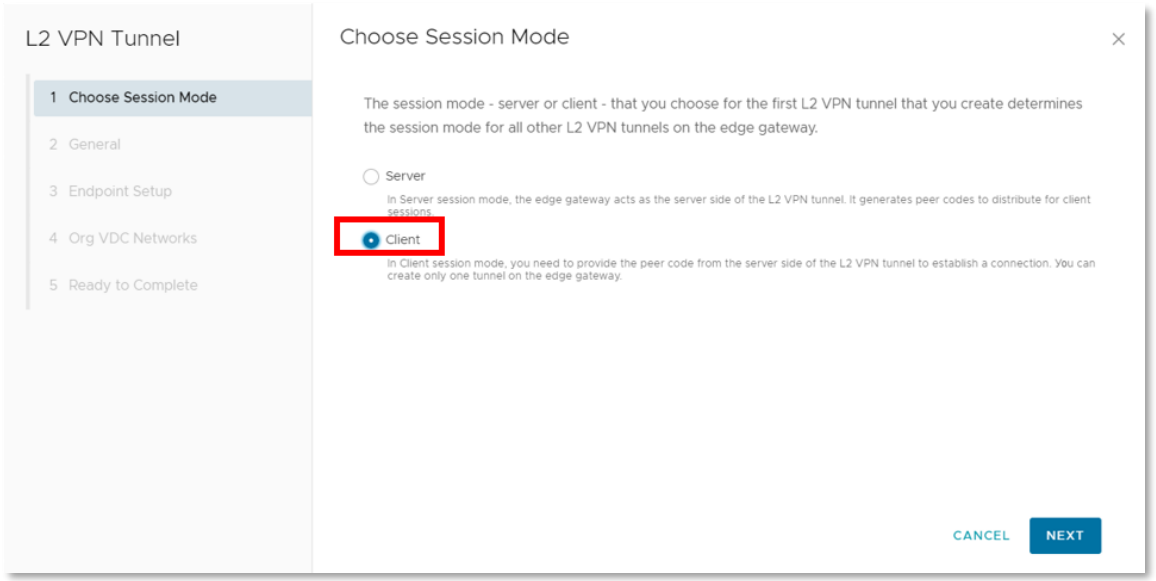
The following screen will open, select the Org VDC Networks option and copy the Tunnel ID parameter

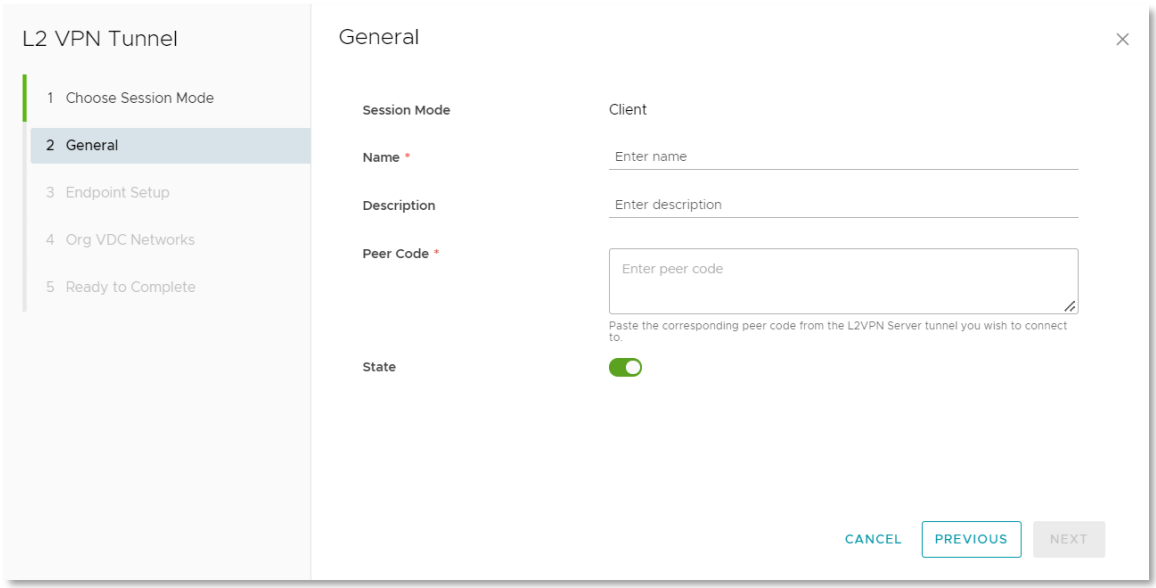


Client Mode

3.2.1. The following information must be entered in the General section, at the end click on next

Item	Description
Name	Name by which the VPN tunnel will be identified
Description	Optional field, for a brief description
Peer Code	This parameter must be shared by the server (see step 3.1.5 of a server mode configuration)
State	Enabled or Disabled

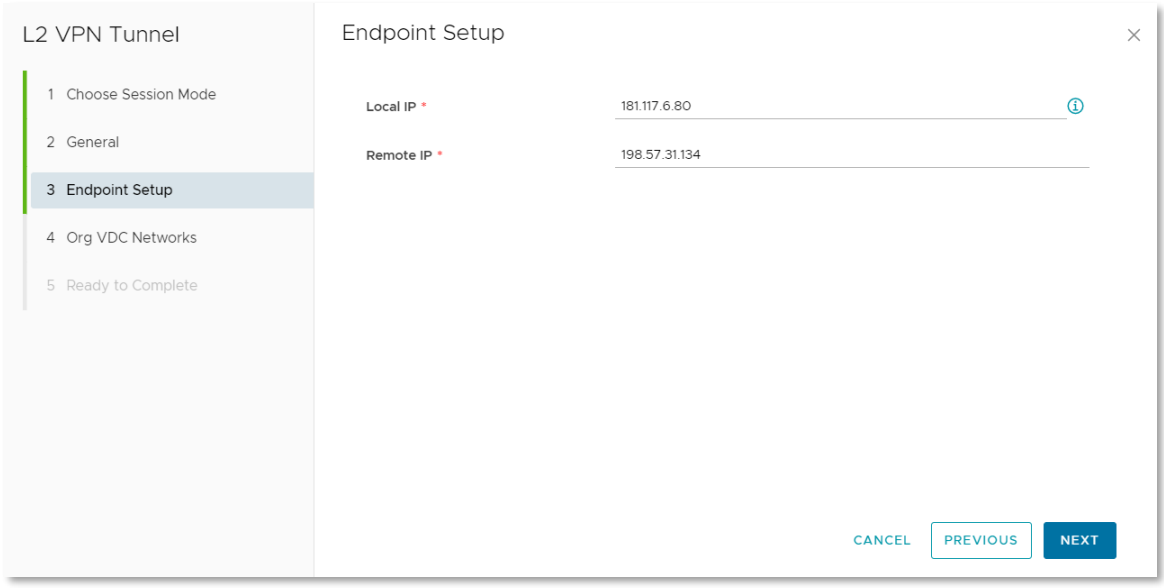




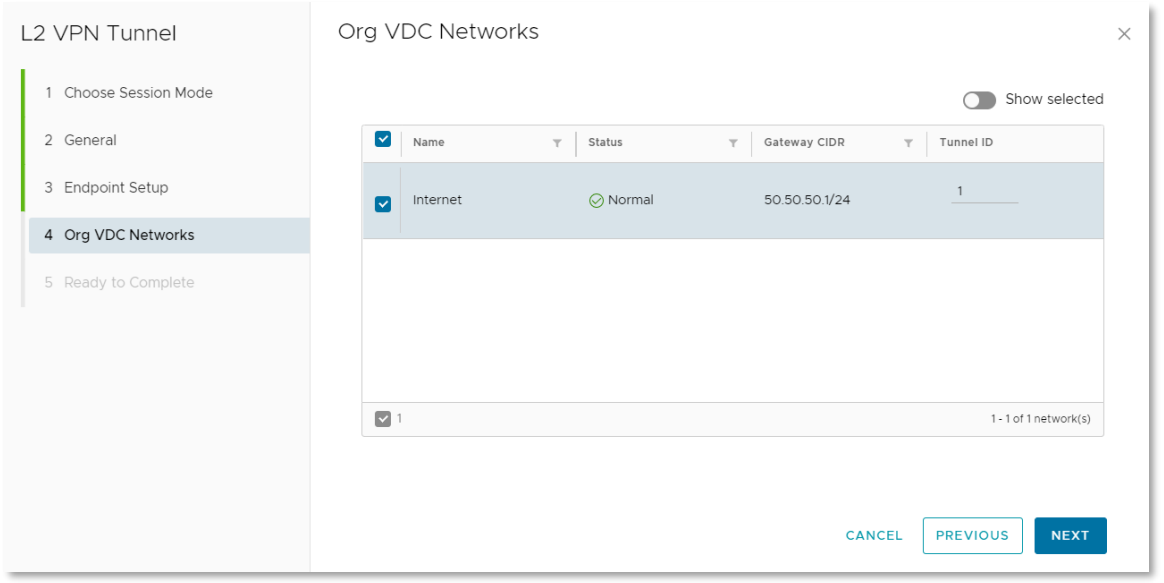
3.2.2. The Endpoint Setup section will be displayed, where the following information must be entered, at the end click Next

Item	Description

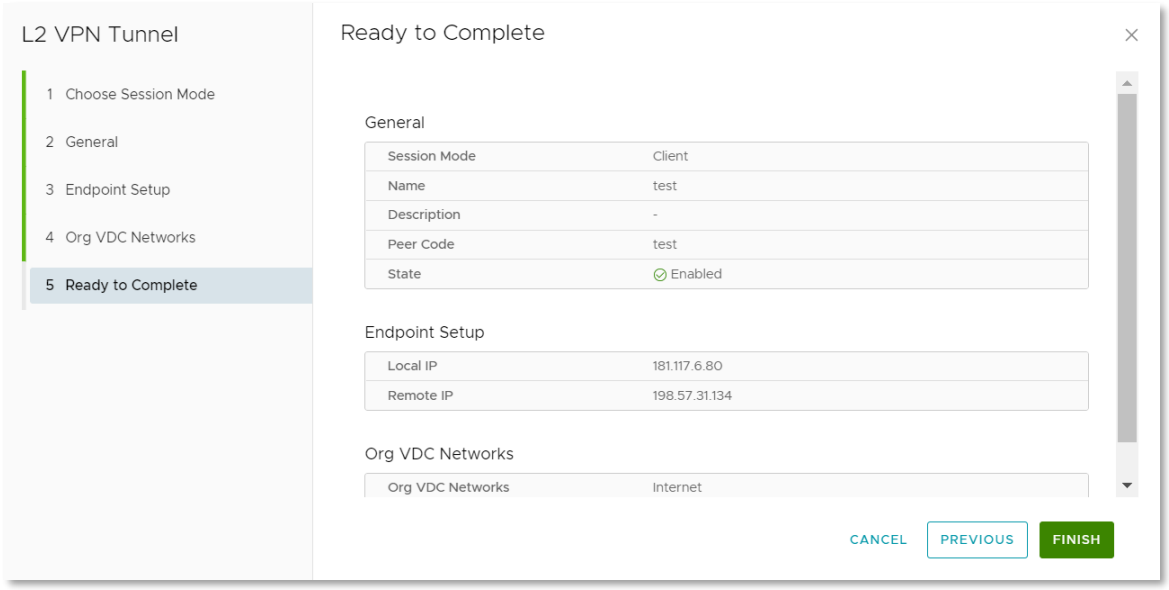
Local IP	Enter the public IP of the T1 Edge Gateway
Remote IP	Enter the public IP of the remote node to connect "Server"



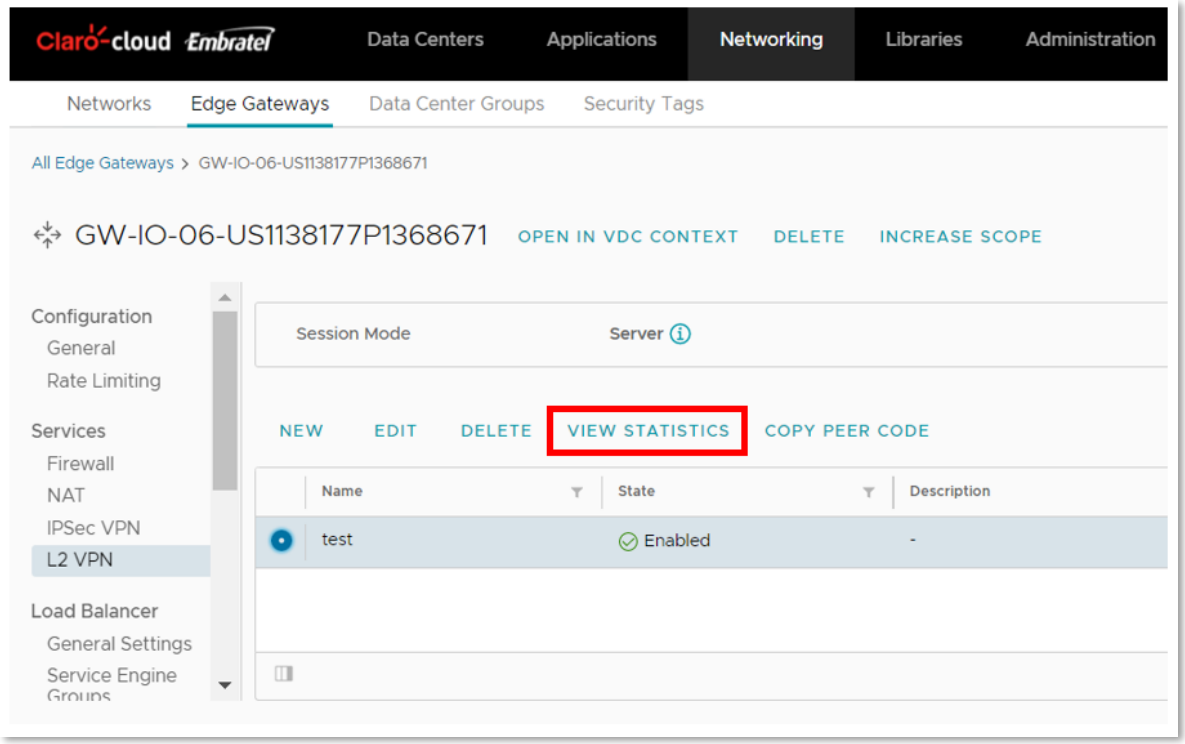
3.2.3. The Org VDC Networks section will be displayed, where the internal networks of the DCV that will allow the client to be published through the VPN tunnel must be selected, it is required to indicate the Tunnel ID, this parameter must be specified by the Server (see step 3.1.6), at the end click Next

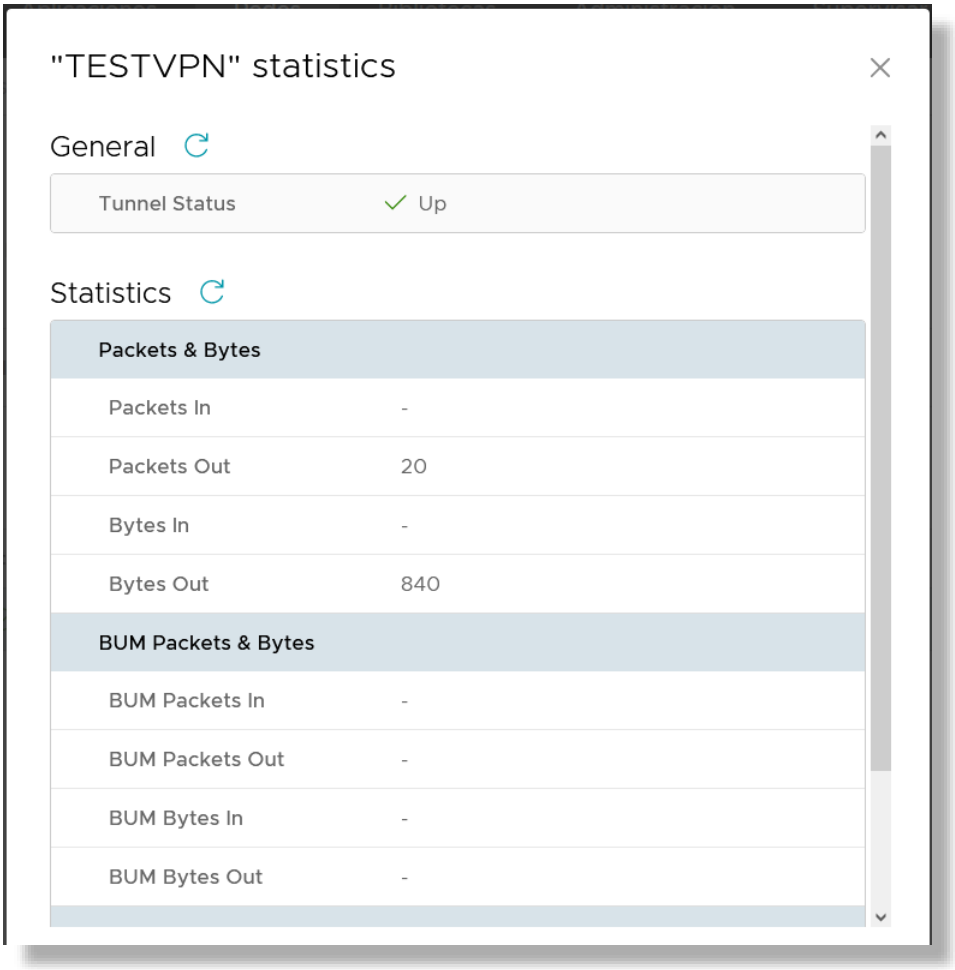


3.2.4. A summary with the configuration made will be displayed, click Finish



4. Once the Edge Gateway has been configured in "Server" and "Client" mode, you can validate the status of the link by clicking on the View Statistics button





Client-Server VPN Configuration (OpenVPN)
In this section you will find the procedure to configure a Client-Server VPN, by means of an OpenVPN template

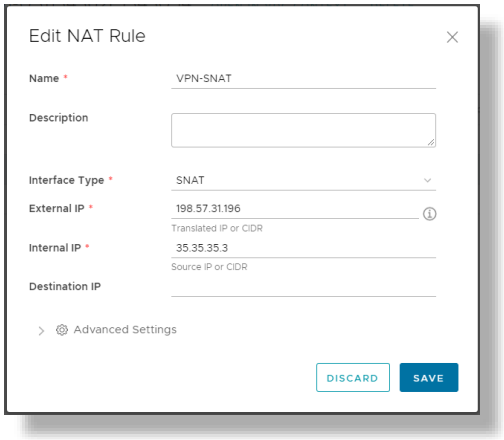
> **Important:** Each virtual Appliance allows 2 concurrent sessions. If more sessions are required, you will need to purchase a separate license with OpenVPN

It is necessary before provisioning the virtual machine with the VPN software, to configure the network environment within your T1 Edge Gateway with which the Appliance will communicate in order to extend connections.

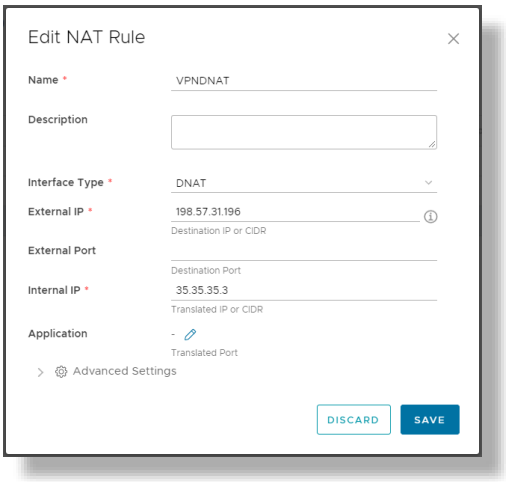
1. Create a routed network with Internet access, please refer to how to configure a network in Enterprise Claro Cloud

2. Within the T1 Edge Gateway control panel, select the "NAT" section and create the following rules

    - SNAT – Allow the output of the IP or segment configured in step 1 through the Public IP of the T1 Edge Gateway

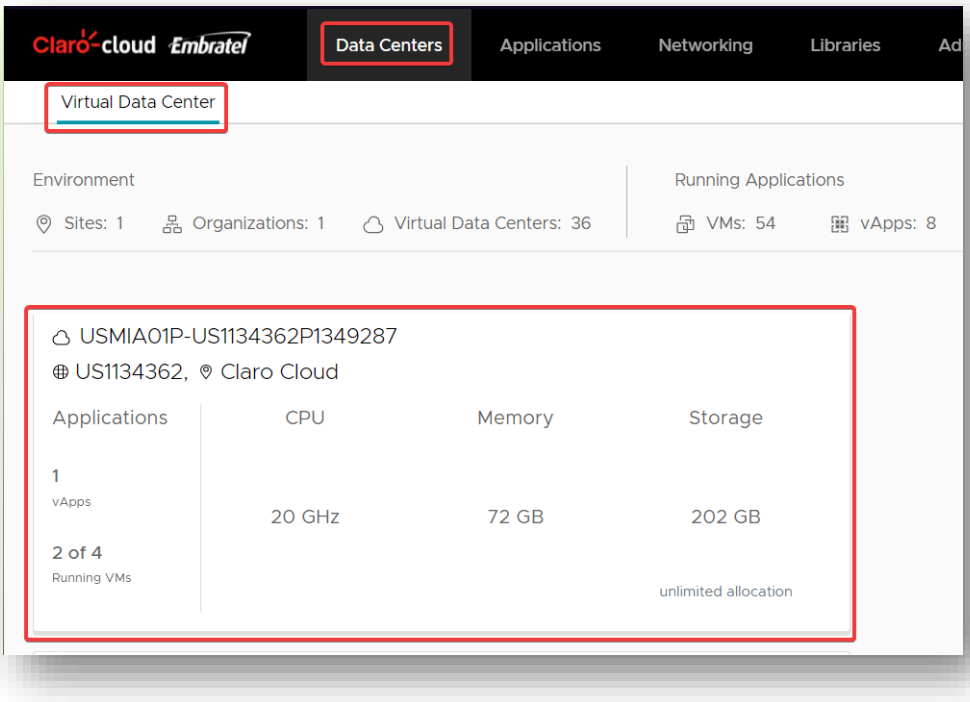


- DNAT - Allow output of the IP or segment configured in step 1 through the Public IP of the T1 Edge Gateway

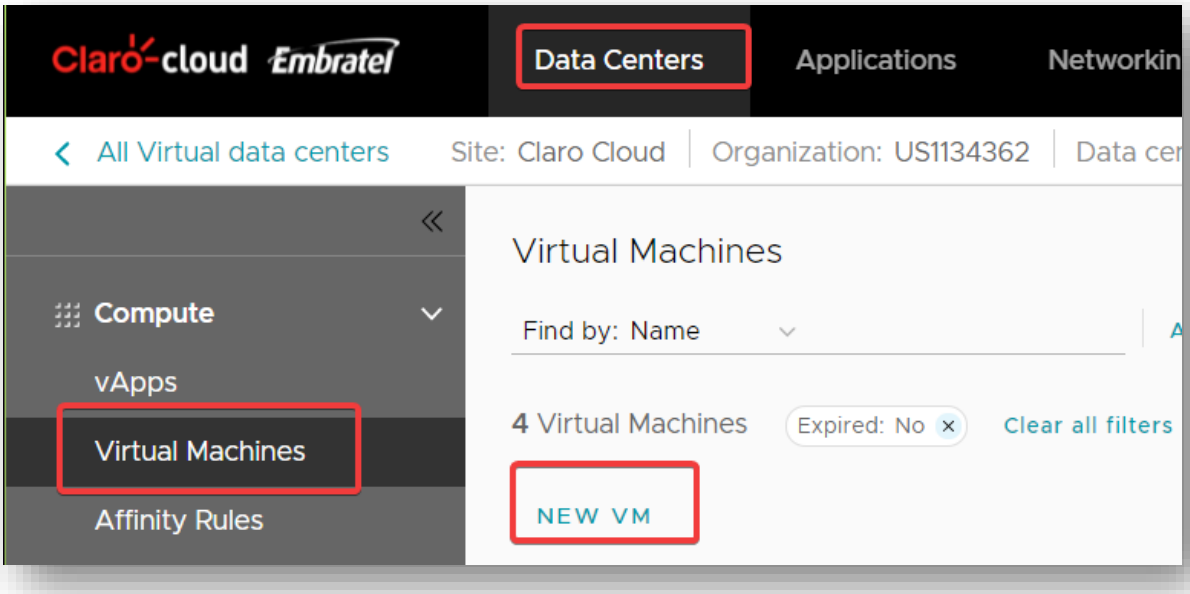


Important: Validate that in the firewall of your T1 Edge Gateway, there is no rule that can block outbound internet traffic from the private segment created in step 1

3. Within the main menu select the "Data Center" option and click on the Virtual Data Center box where the VPN service will be deployed. It must be the same Data Center to which the T1 Edge Gateway configured in steps 1 and 2 is associated



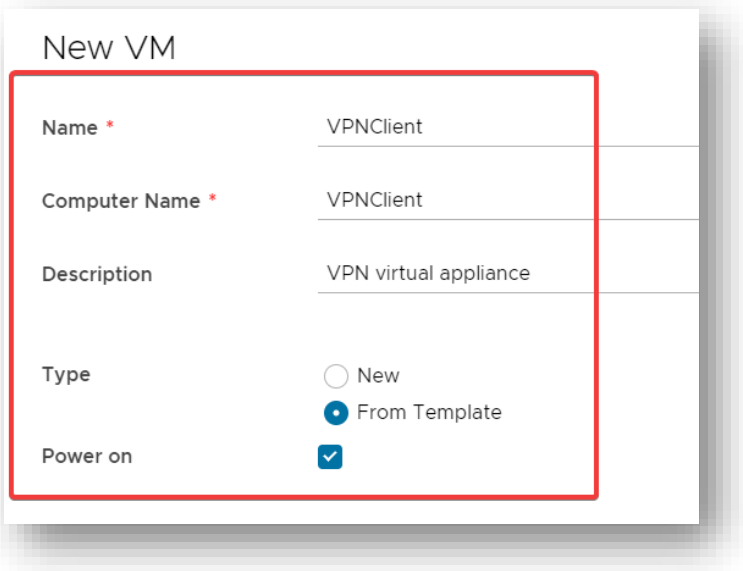
4. Within the Data Center select the option "Virtual Machines" and click on "New VM"



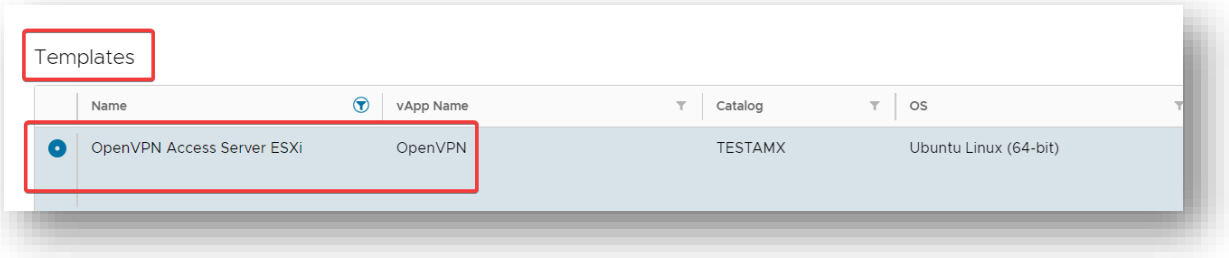
5. The following screen will be displayed where you will have to enter the following information. At the end of clicking on "OK" button

Item	Description
Name	Appliance Name

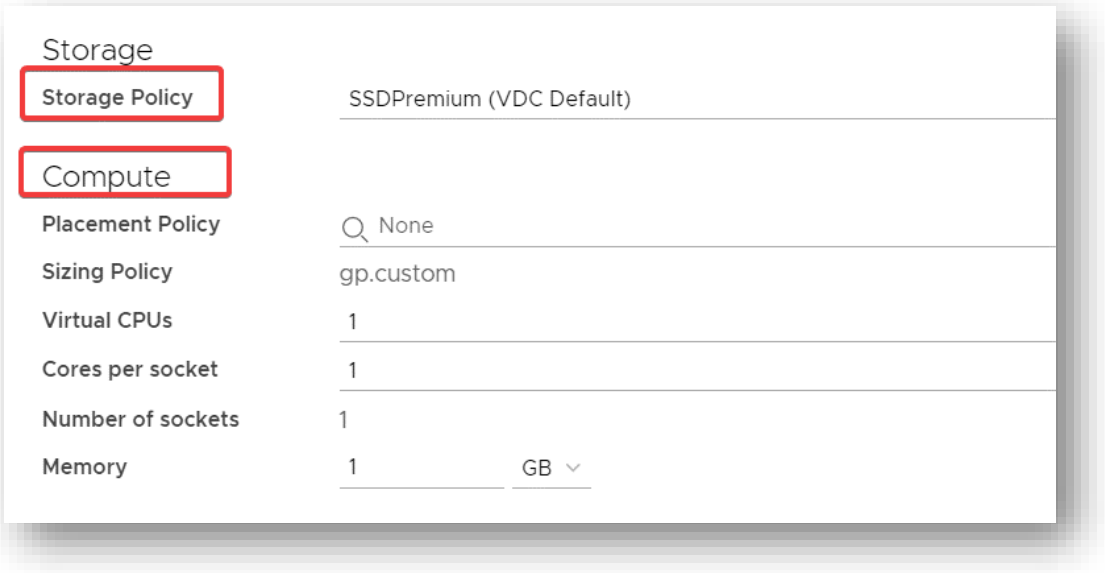
Computer Name	Name that will appear within operating system
Description (Optional)	It is recommended to enter "VPN virtual appliance".
Type	Select From Template
Power on	Keep the check selected



6. In the "Templates" section select the "OpenVPN Access Server" option

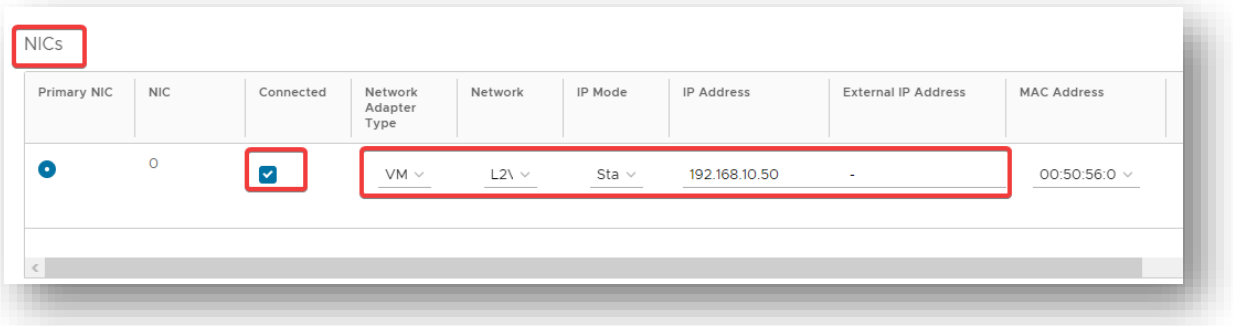


7. In the storage and compute sections keep the standard configuration parameters

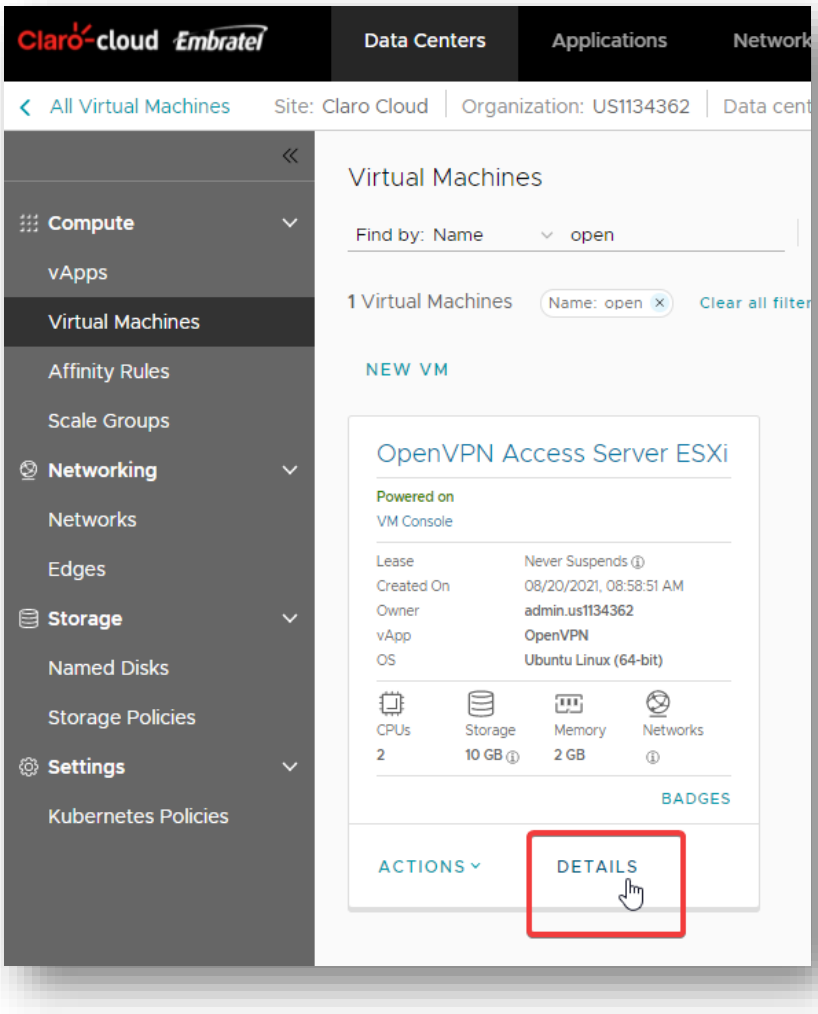


8. In the "NIC" section enter the following information. When you finish clicking "OK", you will start provisioning the virtual machine

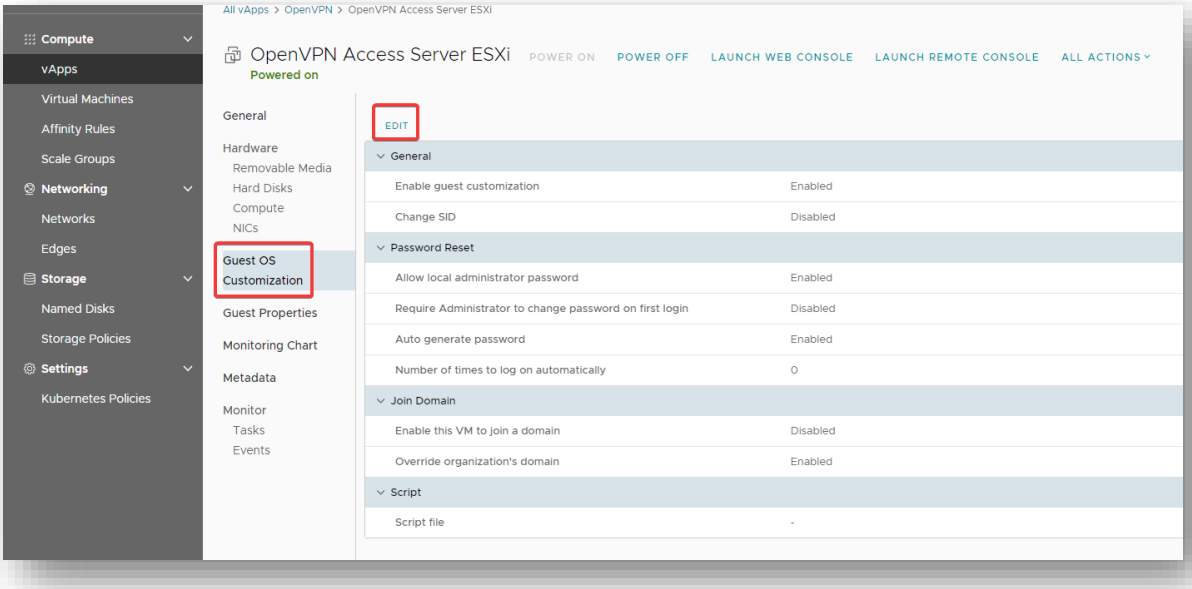
Item	Description
Connected	Enable check
Network adapter type	Select VMXNET
Network	Select the network created in step 1
IP Mode	Select Static - Manual
IP address	Enter a valid IP of the selected network



9. At the end of provisioning you will be able to view the virtual machine within your data center, by clicking on details.

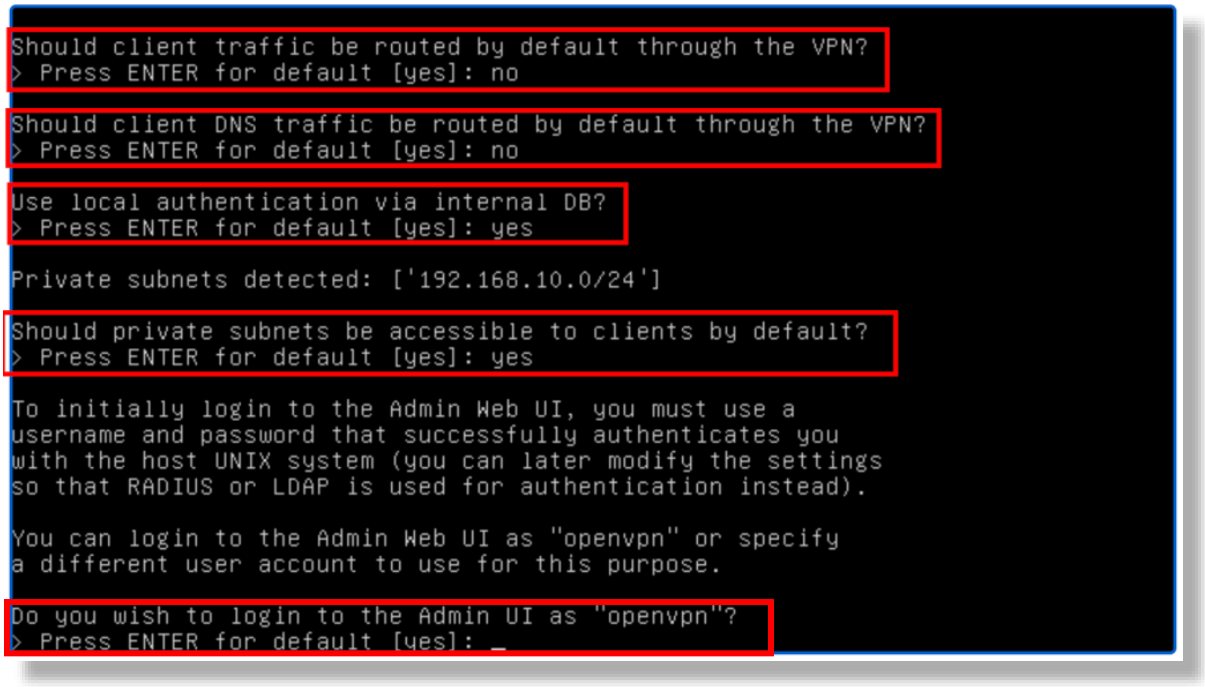


10. Within the virtual machine panel select "Guest OS Customization" and click "Edit". A screen will open where you can view the default assigned startup password.



11. Open the console of your preference to be able to enter the virtual machine, enter as “root” user and with the password obtained in the previous step. Once logged in you will be prompted to answer the following questions

Question	Answer
Please enter ‘yes’ to indicate your agreement	Yes
Will this be the primary Access Server node?	Yes
Please specify the network interface and IP Address to be used by the Admin Web UI	Enter the number where the card is indicated with the IP address with which I configured the NIC in step 8
Please specify the port number for the admin Web UI.	943
Please specify the TCP port number for the OpenVPN Daemon	443
Should client traffic be routed by default through the VPN?	No
Should client DNS traffic be routed by default through the VPN?	No
Use local authentication via internal DB?	Yes
Should private subnets be accessible to clients by default?	Yes
Do you wish to login to the admin as “openvpn”	Yes



12. You will be prompted to enter an activation key, leave blank and click "Enter"

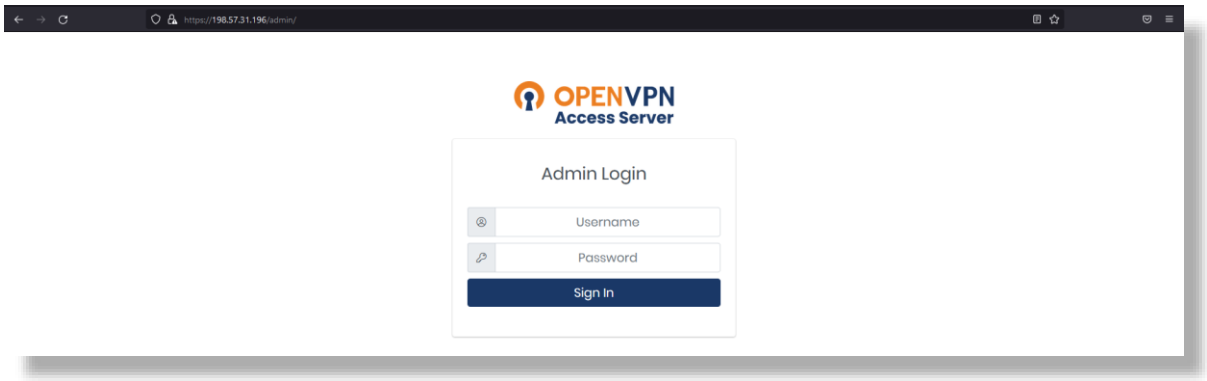
> **Important:** If you require a license, it must be purchased directly with OpenVPN

13. Finally, it will be required to specify a password which will be used to enter your administration console, click "Enter", and wait for the installation of the service to finish

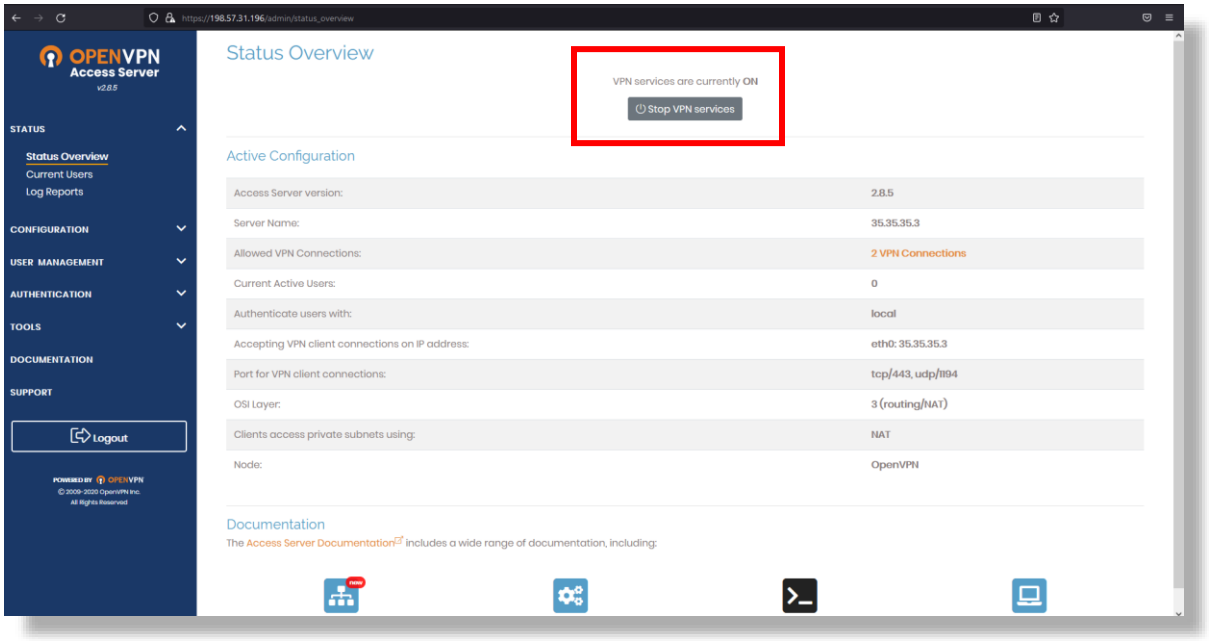
> **Important:** If the option to set the password does not appear, enter the following command
> >passwd OpenVPN

14. After the installation is complete, accessing a web browser will require the public IP of your T1 Edge Gateway which was used to configure NAT policies in step 2

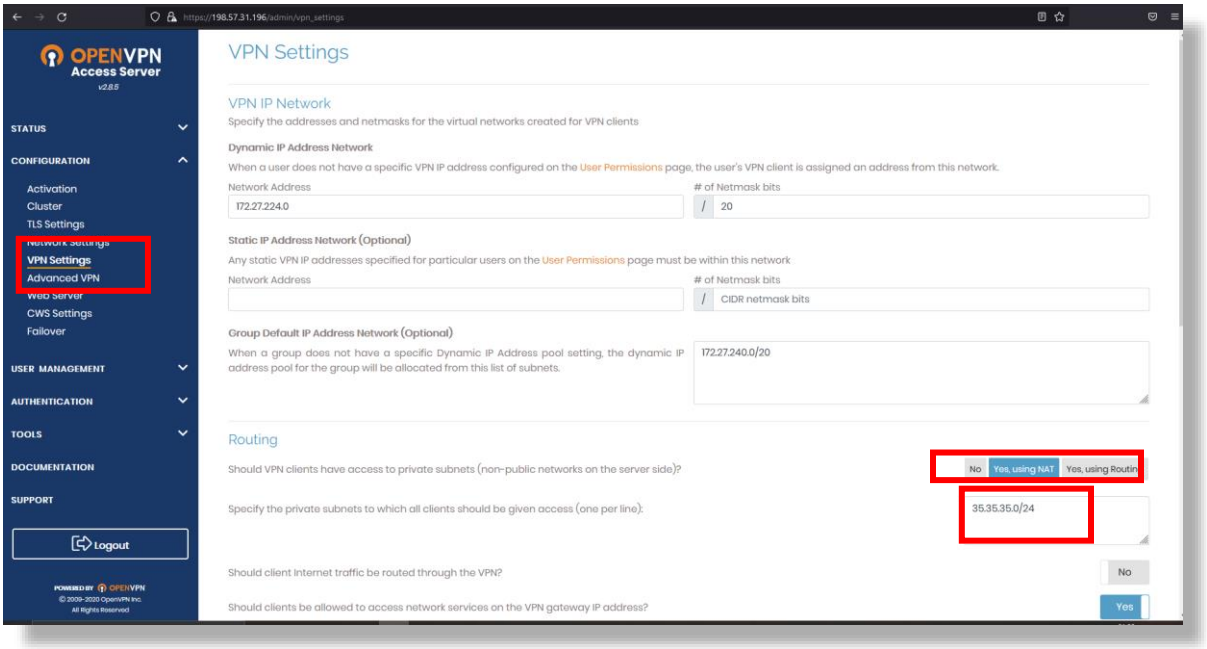
    Enter https://<ip_publica_edge>:943/admin/, the next screen will open



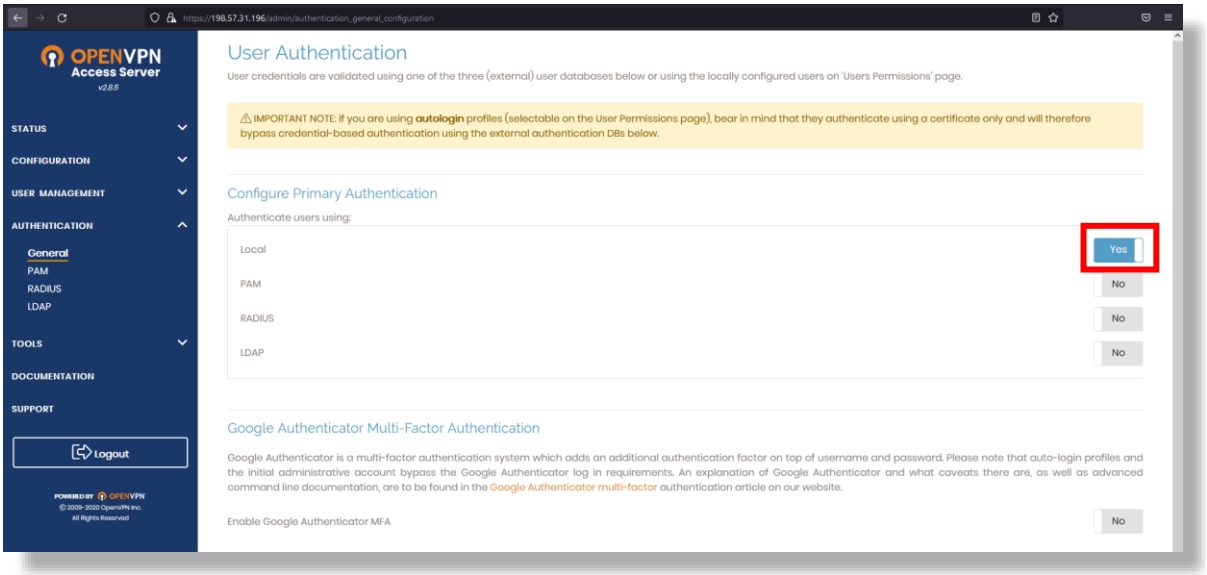
15. Enter in Username: openvpn and Password the password defined in step 13 then you can access your administration console. Validate that the service is Powered on



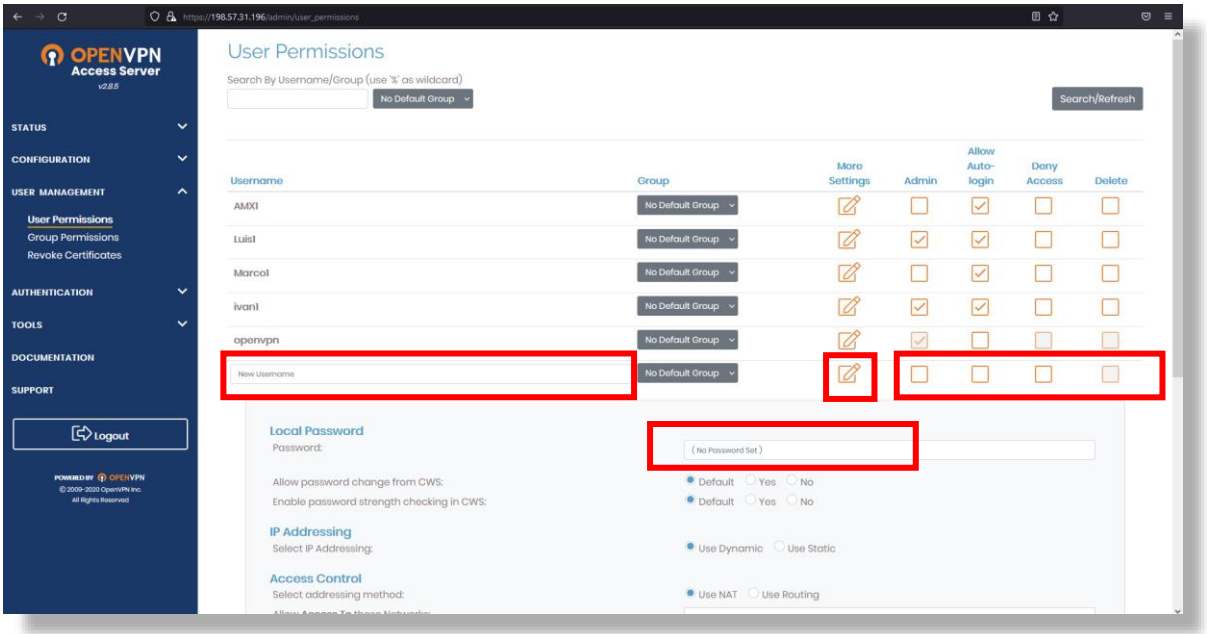
16. In the menu within the "configuration" section click on the "VPN Settings" option. Locate the Routing section and select the "Yes, using NAT" button and within the text box enter the private segments to which you will allow access via VPN



17. Before creating your users go to the "Authentication" section in the generate option, validate that the authentication settings are Local, if not, just slide the button to activate the option

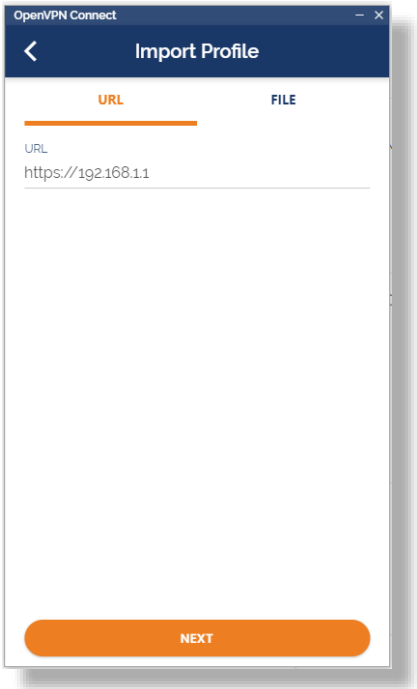


18. To create your users, within the menu enter the "User Management" section and click on the "User Permissions" option. Enter the username and select the permissions you want to assign to the users. Finally, click on the "more settings" button and define the access password

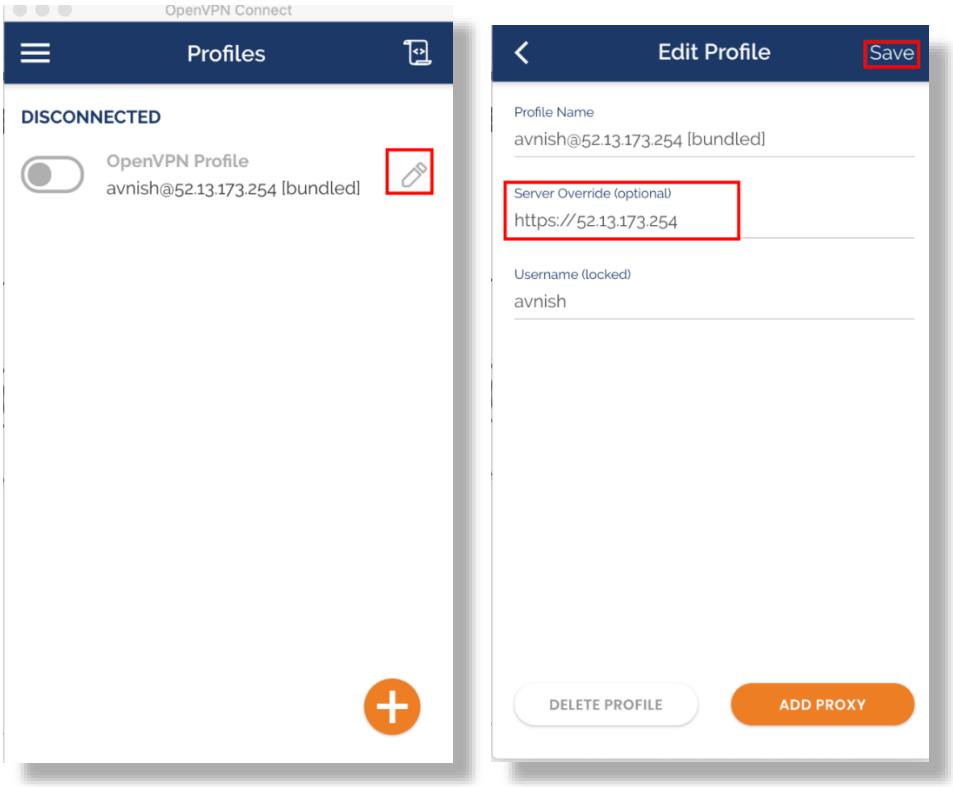


19. New users will be able to enter through the URL https://<ip publica edge>/, with the username and password with which was registered. At the time of accessing the next page will open, where you can download the client to connect to your VPN

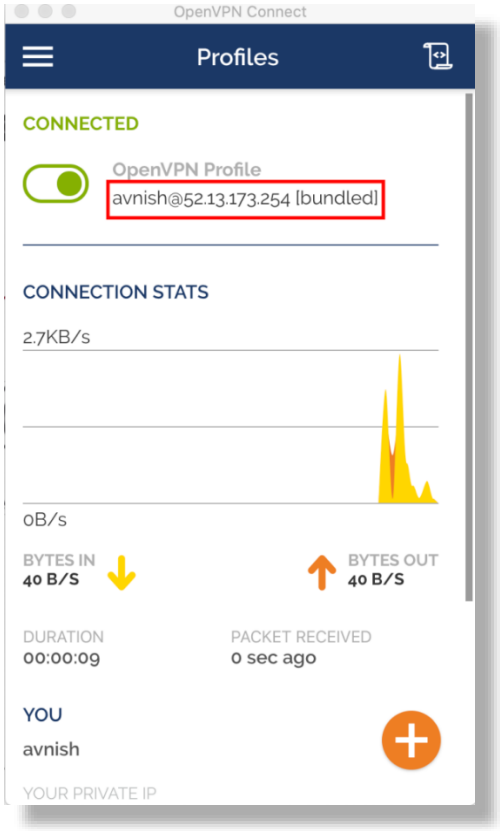
20. Once the application is downloaded and installed the user must enter the public IP of their service from step 19, and their username and password



21. In your Profile you must ensure that in the Server Override option your public IP from the previous step is shown. If this is not the case, enter it and click on "Save"



22. Finally, just swipe the button on your profile, wait a few seconds, and you can connect to your VPN link


OpenVPN Connect
Profiles
CONNECTED
OpenVPN Profile
avnish@52.13.173.254 [bundled]
CONNECTION STATS
2.7KB/s
0B/s
BYTES IN
40 B/S
BYTES OUT
40 B/S
DURATION
00:00:09
PACKET RECEIVED
0 sec ago
YOU
avnish
YOUR PRIVATE IP

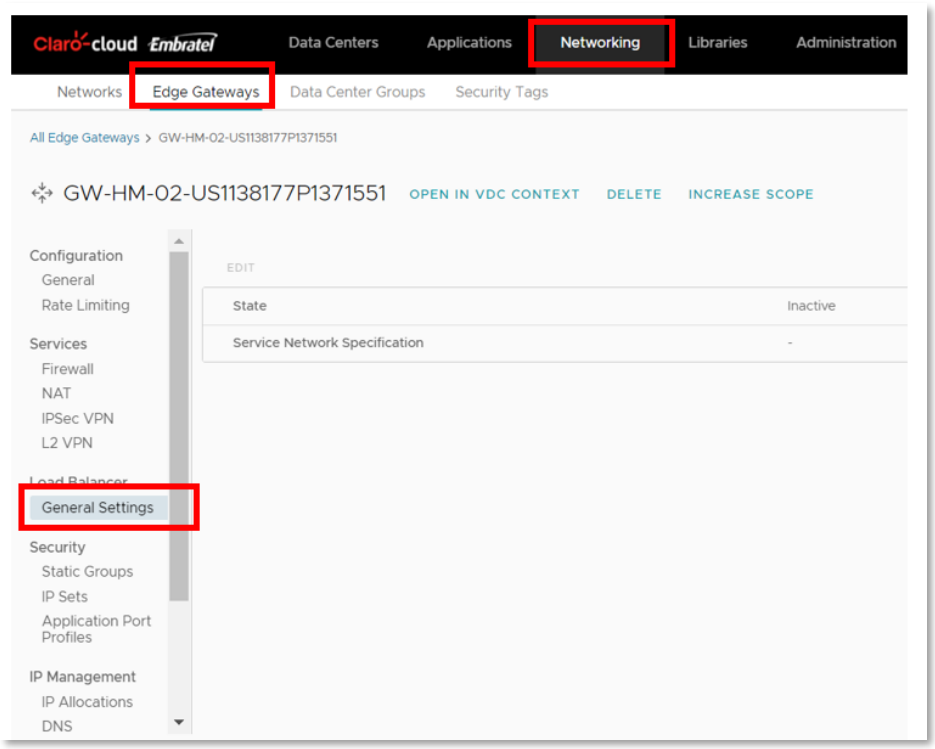
Load Balancer Configuration

This section describes how to configure a load balancer

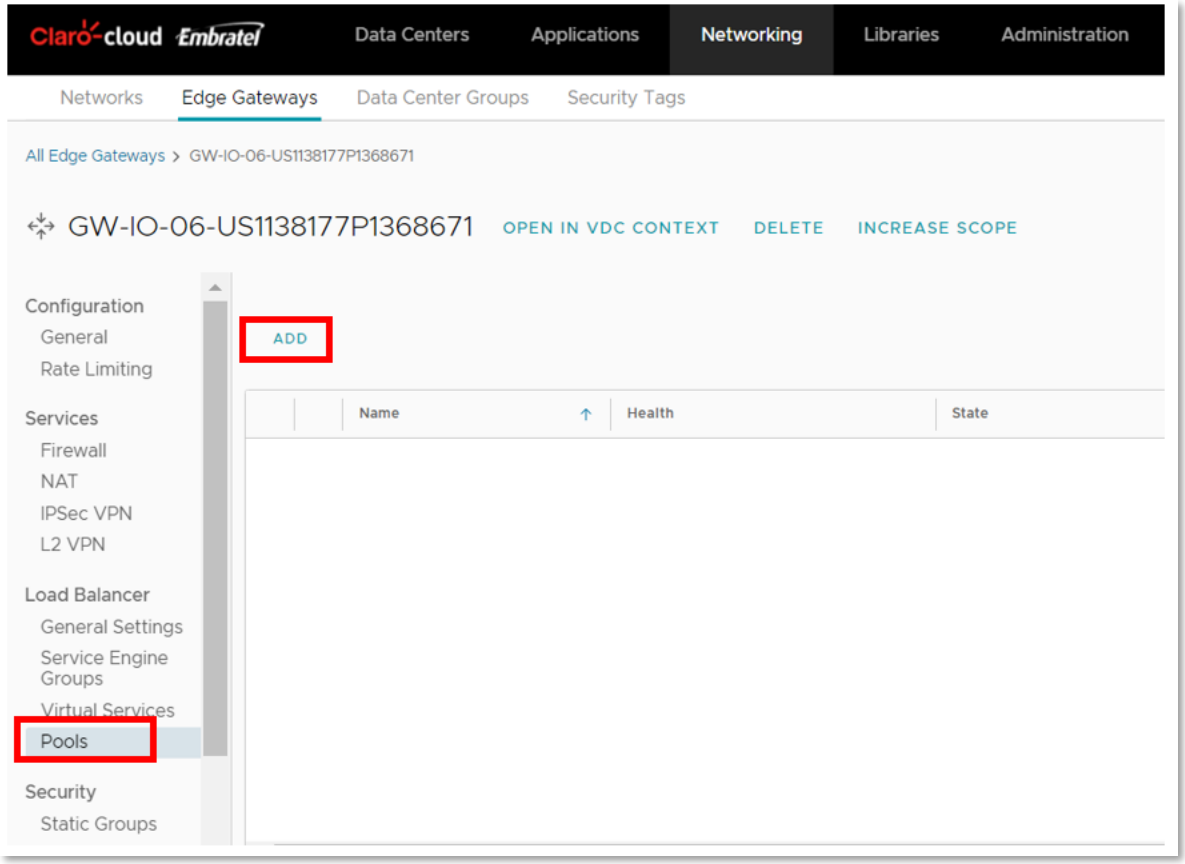
> **Important:** It is necessary to request the activation of the service through Claro technical support

1. Within the panel of the T1 Edge Gateway, in the Load Balancer section select the "General Settings" option, the following screen will be displayed that will contain

Item	Description
State	Indicate whether the service is active or inactive
Service Network Specification	Indicates the address assigned to the balancing instance



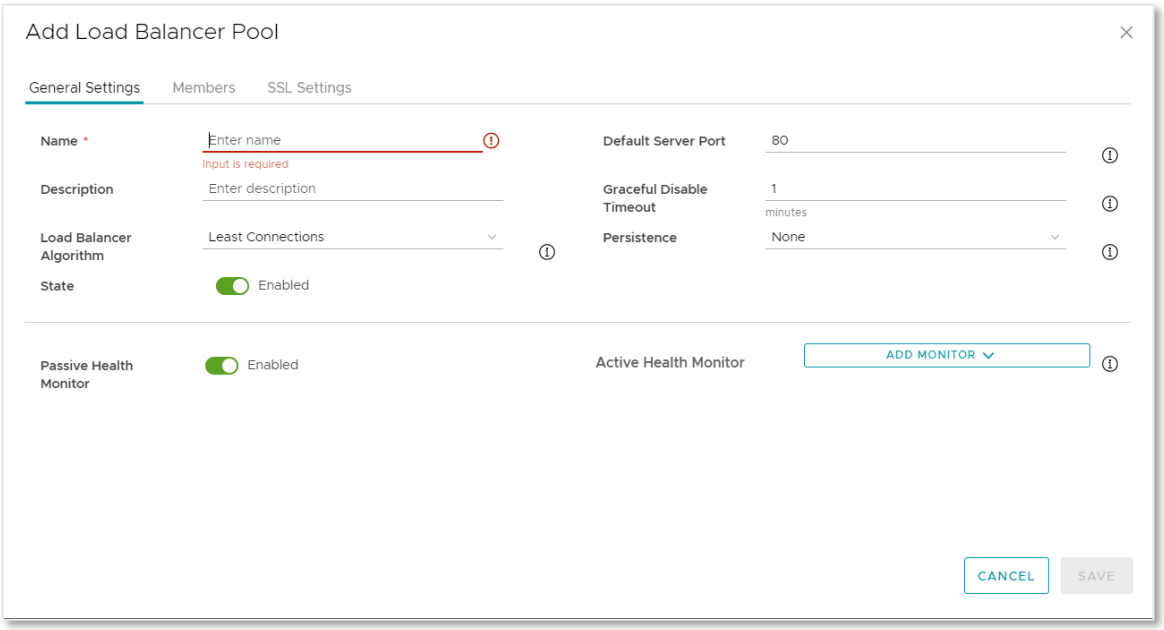
2. It is necessary to first configure a group, click within the panel of the T1 Edge Gateway, in the Load Balancer section select the option "Pools"



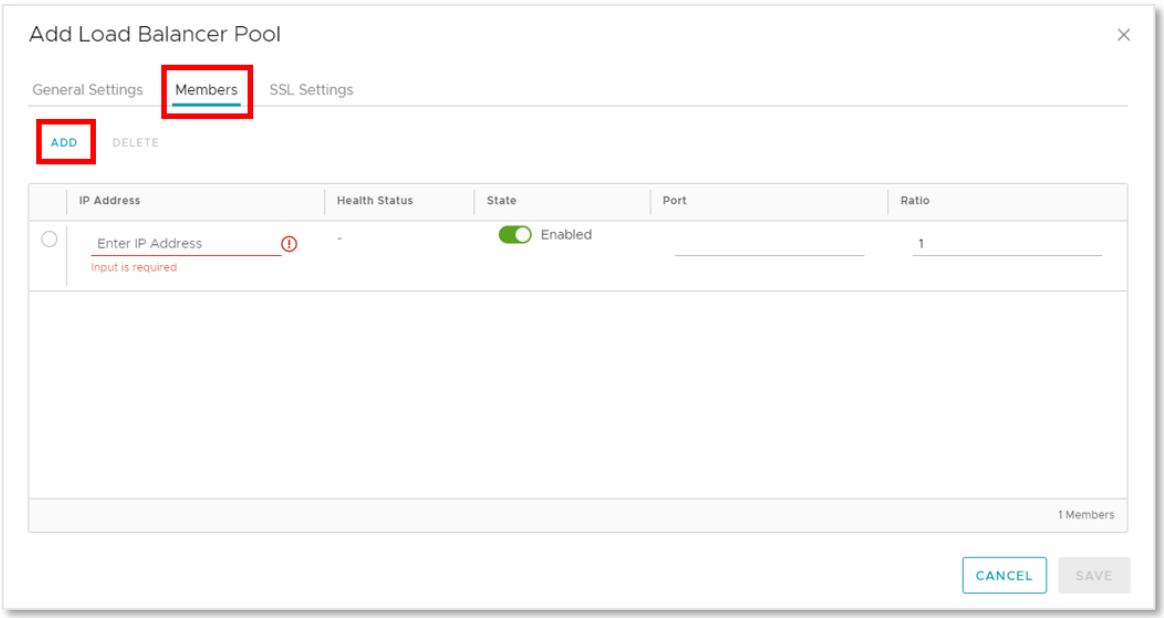
3. Clicking on Add will open the following screen where you will need to enter the following information in the General Settings section:

Item	Description
Name	Enter the name of the group to be configured
Description	Enter a brief description
Load balancer algorithm	Specifies the algorithm by which traffic will be distributed
State	Enable or disable group status
Default server port	The port of the destination server that the traffic that is sent to the member
Successful de-enablement timeout	Maximum time (in minutes) to successfully disable a member. The virtual service waits for the specified time before terminating existing connections to members that are disabled. Special values: • 0 represents "immediate" • -1 represents "infinity"
Persistence	Specifies the persistence profile of a load balancer group. The persistence profile will ensure that the same user adheres to the same server for a desired period of time

Passive state monitoring	Enables or disables passive state
Active health monitoring	Select the protocol with which the status is checked

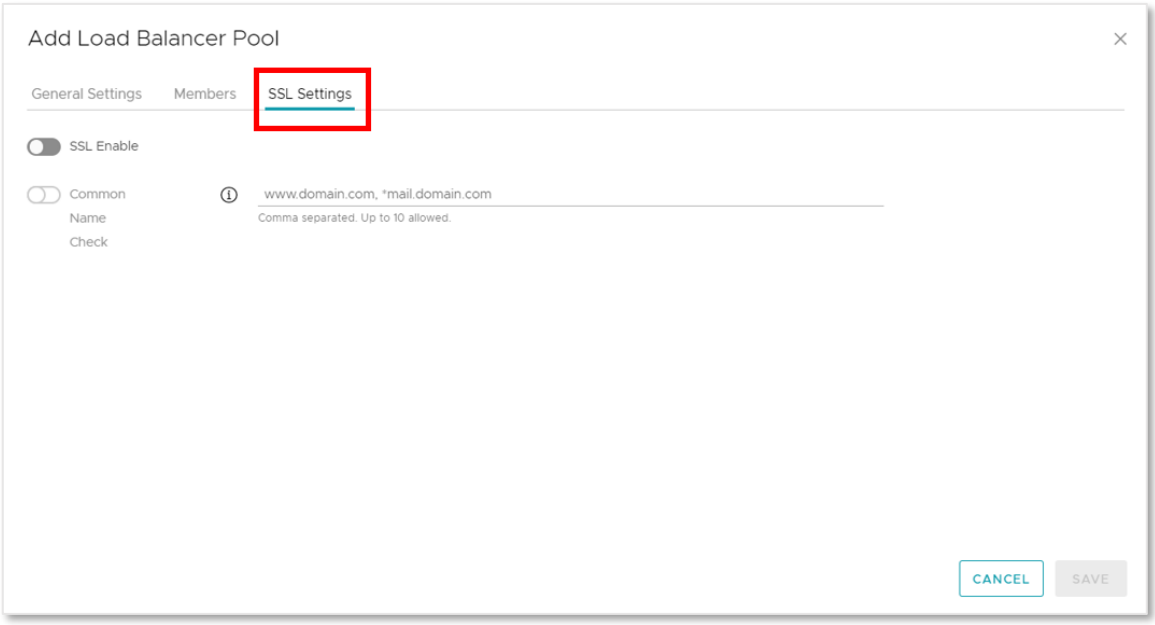


4. In the Members section, click on Add, a line will be displayed where you can define the members of the group, entering their IP address and port



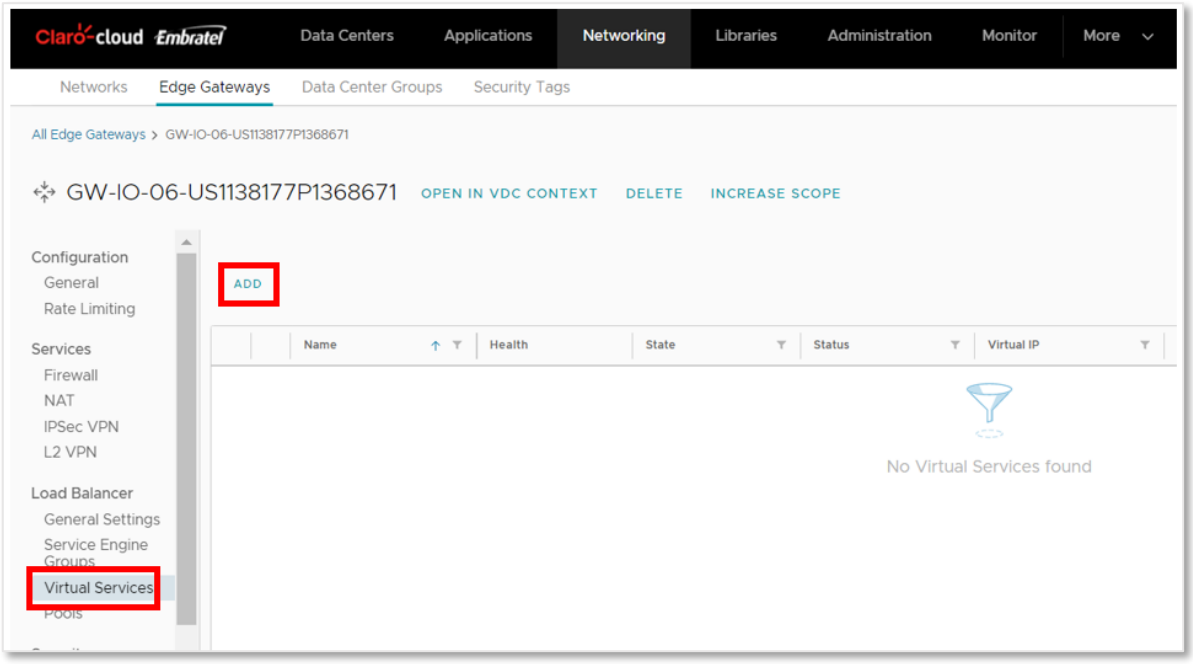
5. In the SSL section, you can enable SSL and verification by a domain

Note: Enable common name checking for the server certificate. if it is enabled and no explicit domain name is specified the incoming host header is used to perform the match check



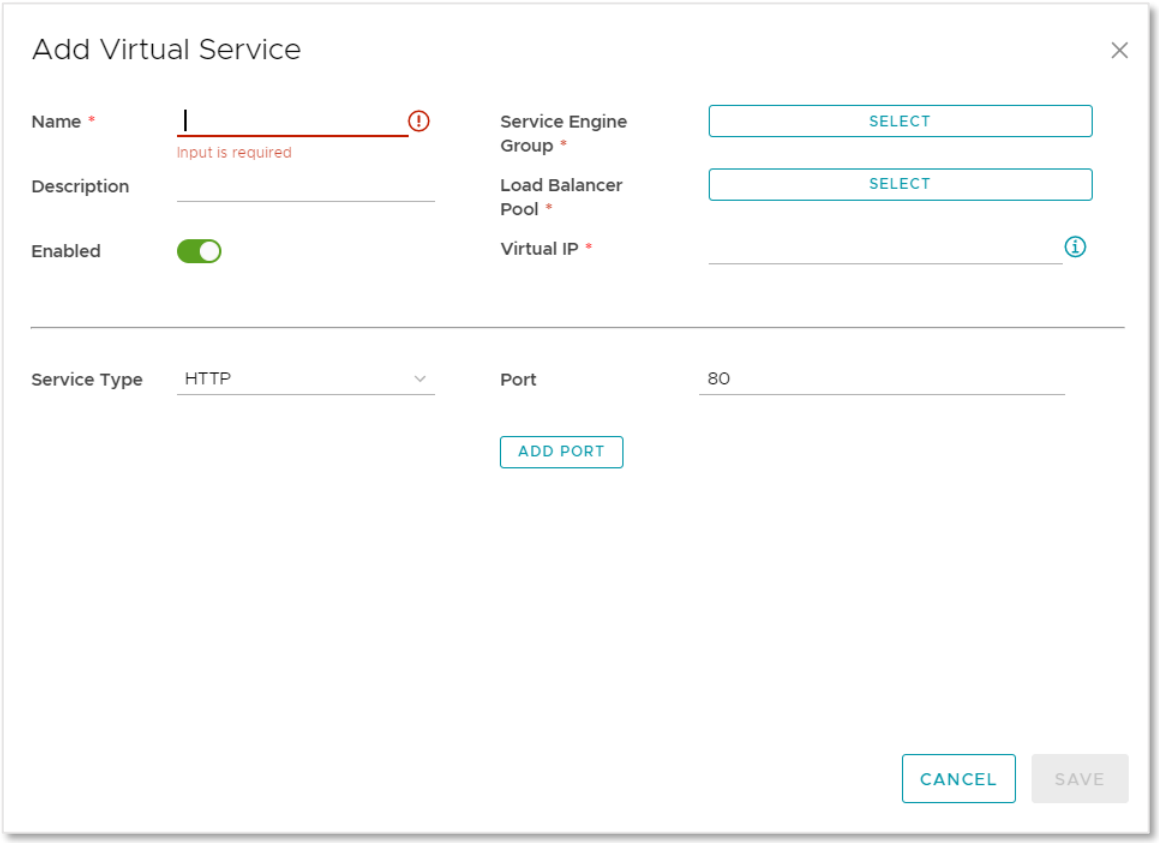
6. When finished, click on Save and the group will be created

7. Now the Virtual Services must be created. Click inside the panel of the T1 Edge Gateway, in the Load Balancer section, and select the option "Virtual Services"



8. Click on Add, the next screen will open, where you will have to enter the following information, click save when finished

Item	Description
Name	Enter the name of the Service
Description	Enter a brief description
Enabled	Specifies the status of the service
Service Engine Group	Select the service engine, at the time of activating the service a default engine is added
Load balancer group	Select the group that you want to link to the service
Virtual IP	Virtual IPs can be internal or external. External virtual IPs must belong to the IP pool assigned to the virtual service owner's Edge gateway **Important**: If it is required to utilize a public IP, it is not possible to reuse an IP in use, it is necessary to acquire a new one.
Type of service	Select the service you want to configure. **Note:** In cases requiring a reverse HTTP and HTTPS
Port	Enter the port for load balancing

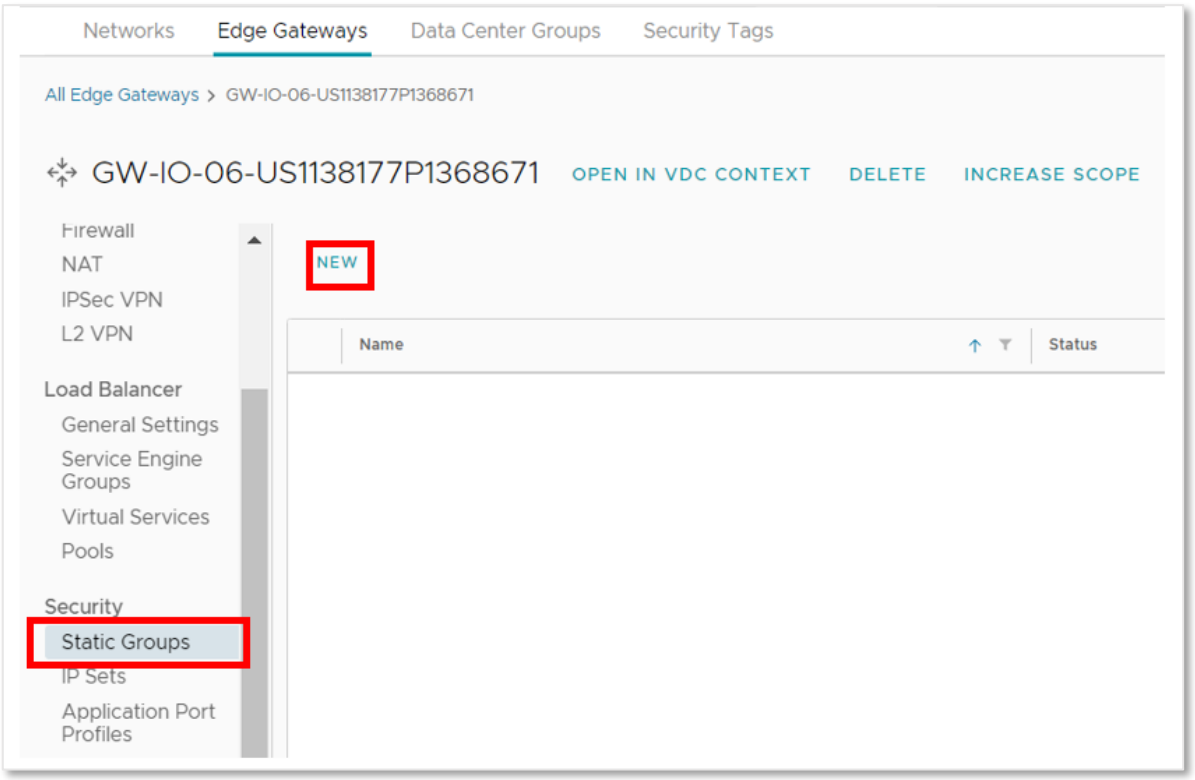


Configuring Security Groups

This section describes how to configure static security groups to more efficiently establish permissions and access to internal and external networks in a data center

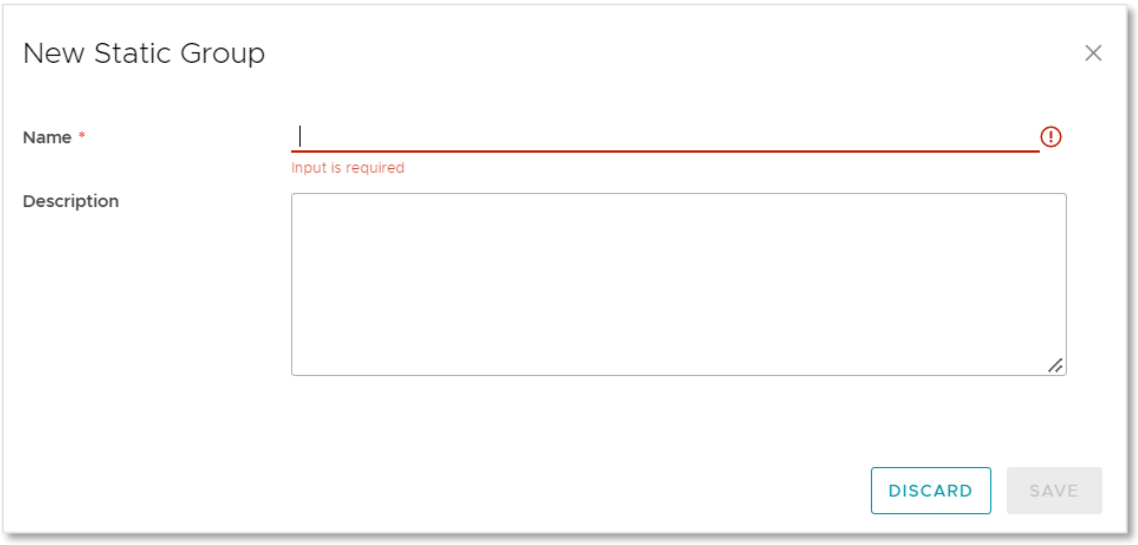
Before you can create the static security group, perform the following process.

1. Within the T1 Edge Gateway dashboard, select the "Static Groups" option and click the "New" button



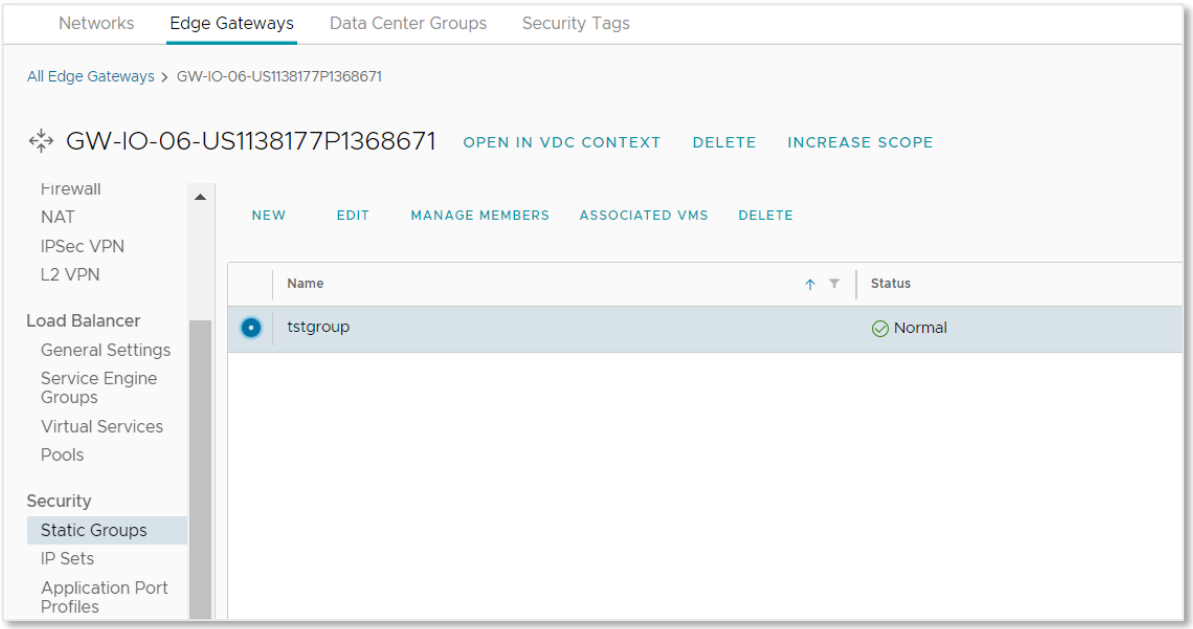
2. The following screen will be displayed where you will have to enter the following information. When finished, click the save button

Item	Description
Name	Security group name
Description	Description of the Static Group



3. The created static security group will be listed and the following options will be enabled

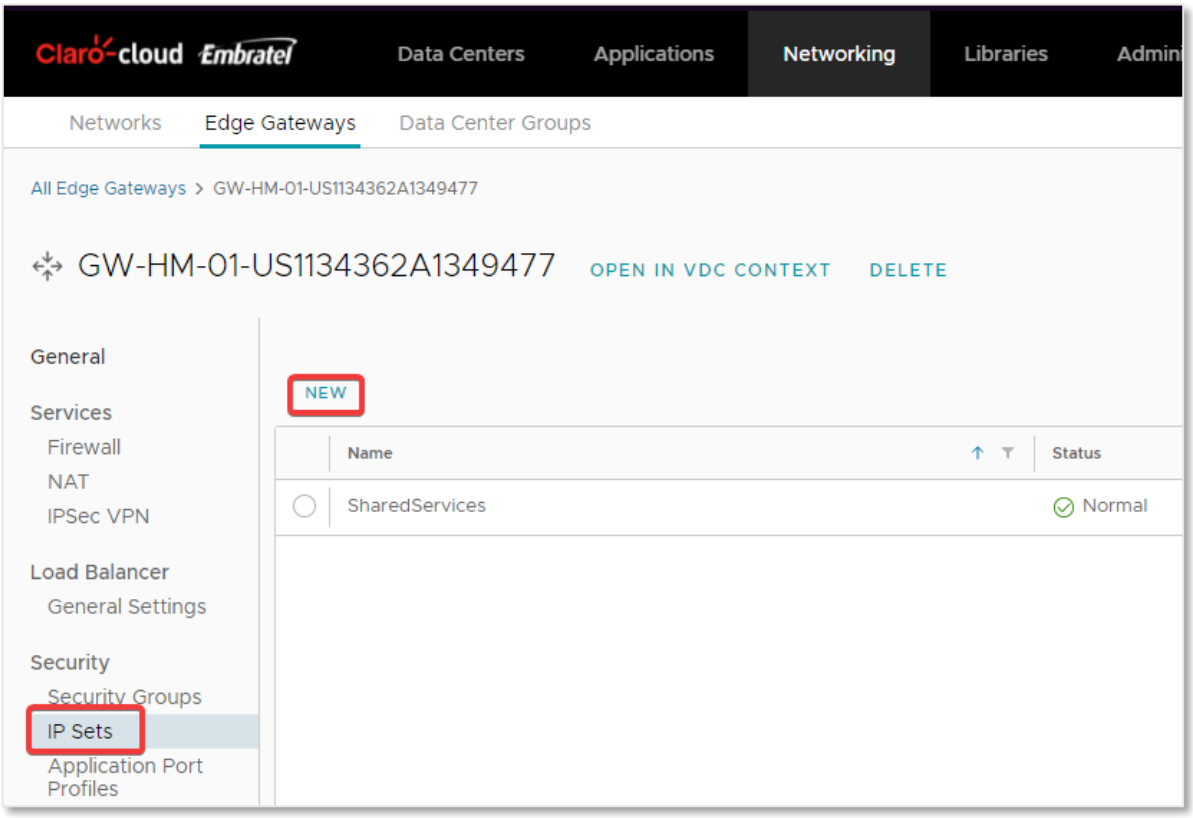
Item	Description
Edit	Edit the name and description of the created group
Manage members	Link the local networks of the Virtual Data Center to the security group
Associated VMS	Lists virtual machines associated with networks linked to the security group
Delete	Deletes the security group



IP Address Set Configuration

This section creates the IP address sets that will help you efficiently define firewall rules

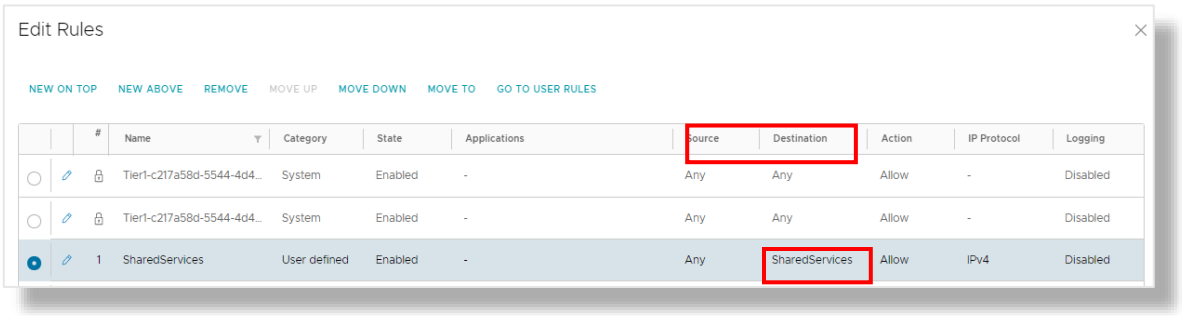
1. Within the T1 Edge Gateway dashboard, select the "IP Sets" option and click the "New" button



2. The following screen will be displayed where you will have to enter the following information. At the end of clicking the save button

Item	Description
Name	IP address set name
Description (optional)	Optional description of the IP address set
IP addresses	Define pool of IP addresses or IP address.

3. The set of defined IP addresses will be listed and can be used later in the configuration of firewall rules in the source and destination fields



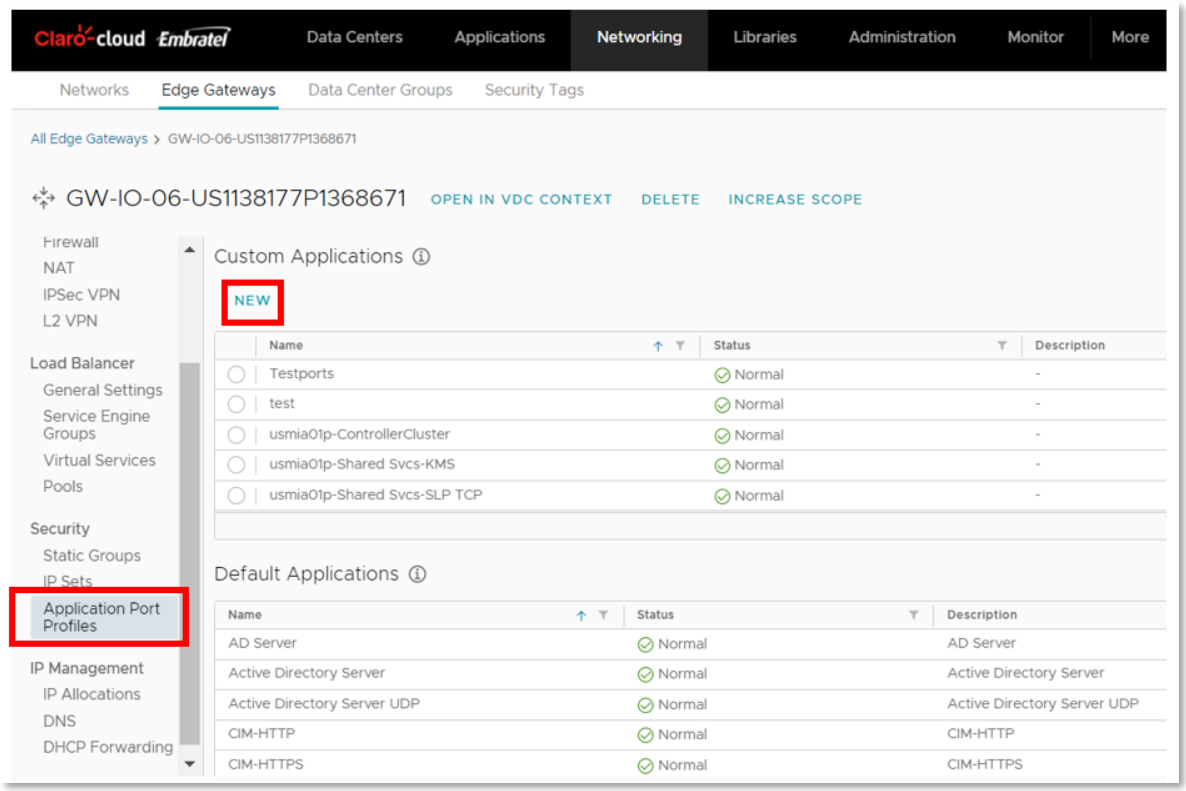
Configuring Application Port Profiles

In this section you can view the profiles with the most common network ports and you can configure unusual port(s) profiles for later use in firewall rules

> **Important:** The following unusual ports are blocked for security.
>
> - TCP/UDP 27000-27050, TCP/UDP 5790-5850, UDP 2300-2400, TCP/UDP 3475-3480, TCP/445, UDP/161/ SNMP, TCP/UDP 135-139
>
> In cases requiring these ports being open, it must be requested through Claro Cloud support, to evaluate the feasibility and its opening

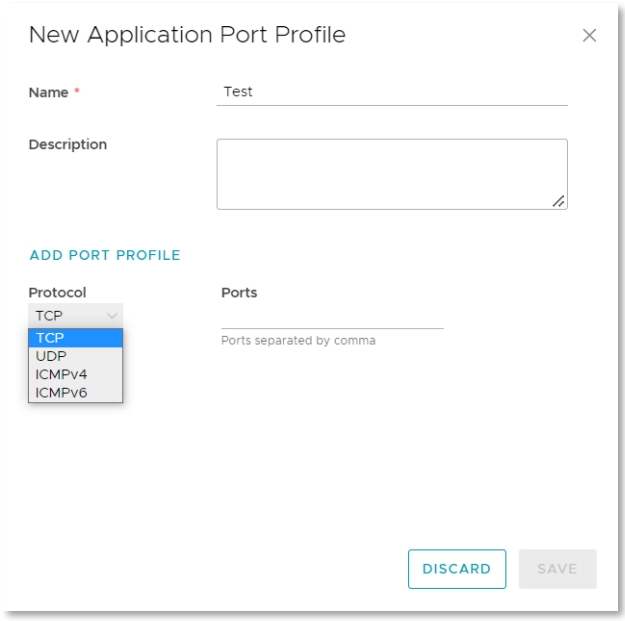
Process for creating an application port profile

1. Within the T1 Edge Gateway dashboard, select the "Application Port Profiles" option and click the "New" button



2. The following screen will be displayed where you will have to enter the following information. At the end of clicking the save button

Item	Description
Name	Port profile name
Description (optional)	Optional port profile description
Protocol	Define the TCP port protocol | UDP | ICMP
Ports	Enter the port(s) to be included in the profile separated by commas

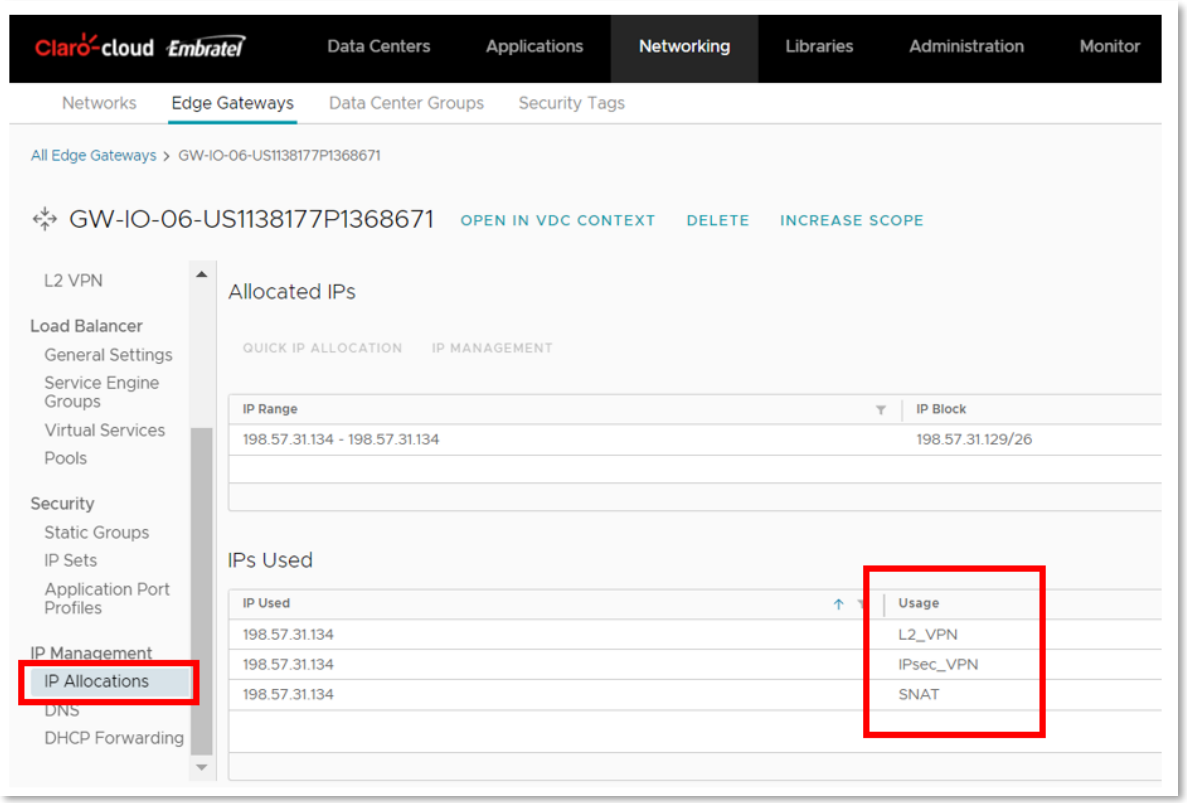


Note: The protocol field may not show the selected option, but the selected option will be considered.

IP Address Management

In this section you can view the public address assigned to your T1 Edge Gateway service, as well as the DNS configuration

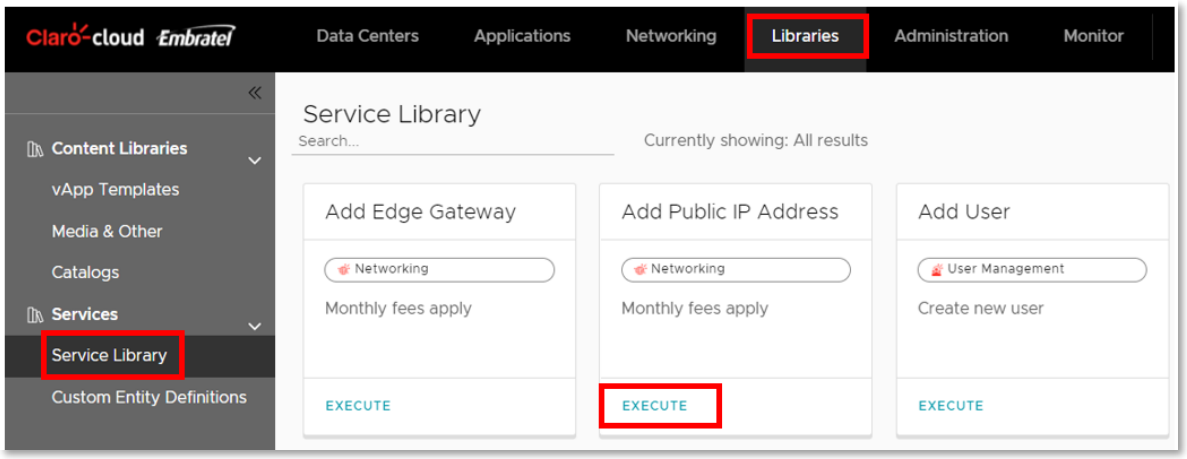
1. Within the dashboard of the T1 Edge Gateway, select the option "IP Assignments", inside you can view the range or public IP addresses assigned to your T1 Edge Gateway, and the services to which the address is linked



2. If you require additional public IP addresses, click on the top menu in the "Libraries" section and select the "Service Libraries" option from the submenu

> **Important:** Each T1 Edge Gateway includes a public IP address. Additional public addresses have an additional cost

3. In the "Add Public IP Address" box click the "Execute" button



4. The following screen will be displayed where you will have to enter the following information. When finished click the "Run" button

Item	Description
Edge GW	Identify the T1 Edge Gateway service to which you want to assign public IP addressing
Quantity	Enter the number of public IP addresses to be purchased

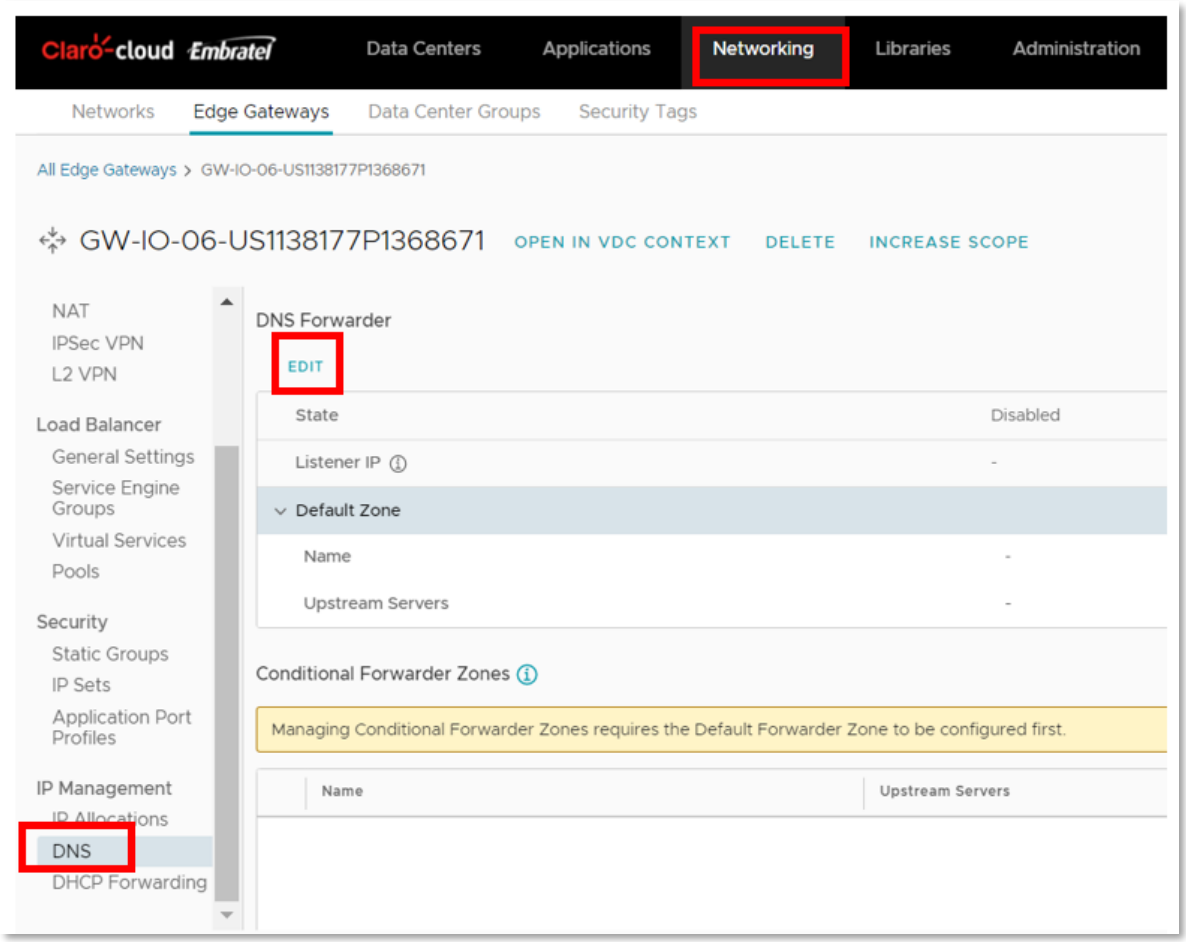
DNS Configuration

In this section, you can configure the DNS settings that the Edge will use for name resolution.

> **Important:** The Domain service is not included in the T1 Edge Gateway service. If you do not have a specific DNS, keep the configuration defined by default

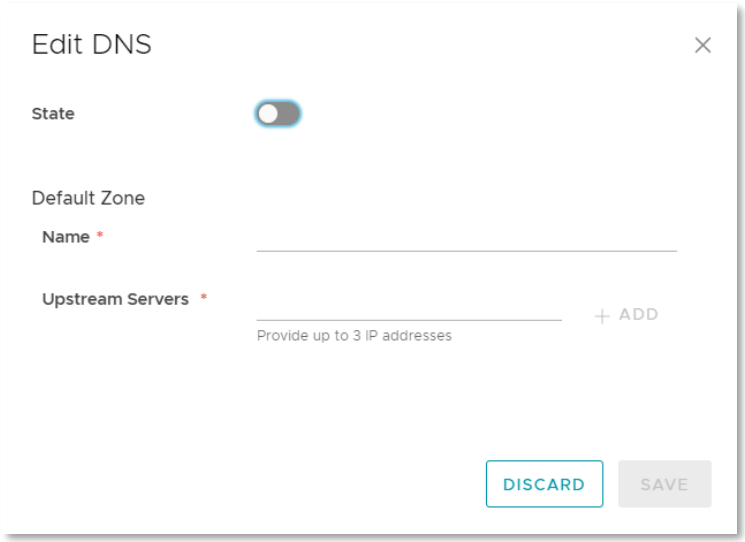
To configure the DNS, follow the following process

1. Within the T1 Edge Gateway panel, select the "DNS" option, click the "Edit" button



2. The following screen will be displayed where you will have to enter the following information. When finished, click the save button

Item	Description
State	Enable/Disable service
Use default value	Enable/Disable Default IP
IP address	DNS listener IP address
Upstream servers	DNS rule name



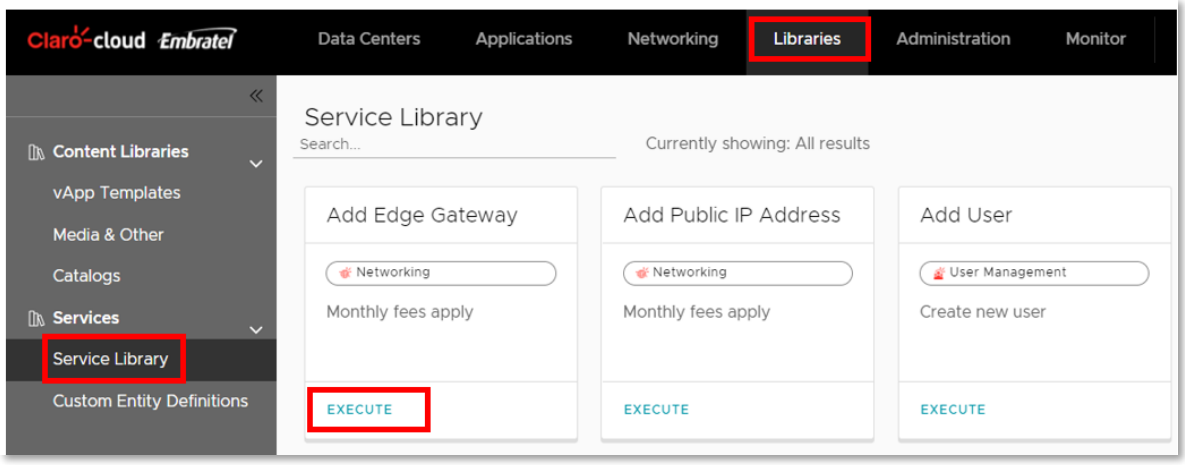
Purchase of an additional T1 Edge Gateway

> **Important:** The T1 Edge Gateway service can manage the networks of more than one Virtual Data Center in the same compute region.

1. If you require a T1 Edge Gateway, click on the top menu in the "Libraries" section and select the "Service Libraries" option in the submenu

> **Important:** Each T1 Edge Gateway includes a public IP address. Additional public addressing has an additional cost

2. In the "Add Edge Gateway" box click the "Execute" button



3. The following screen will be displayed where you will have to enter the following information. When finished, click the "Finish" button

Item	Description

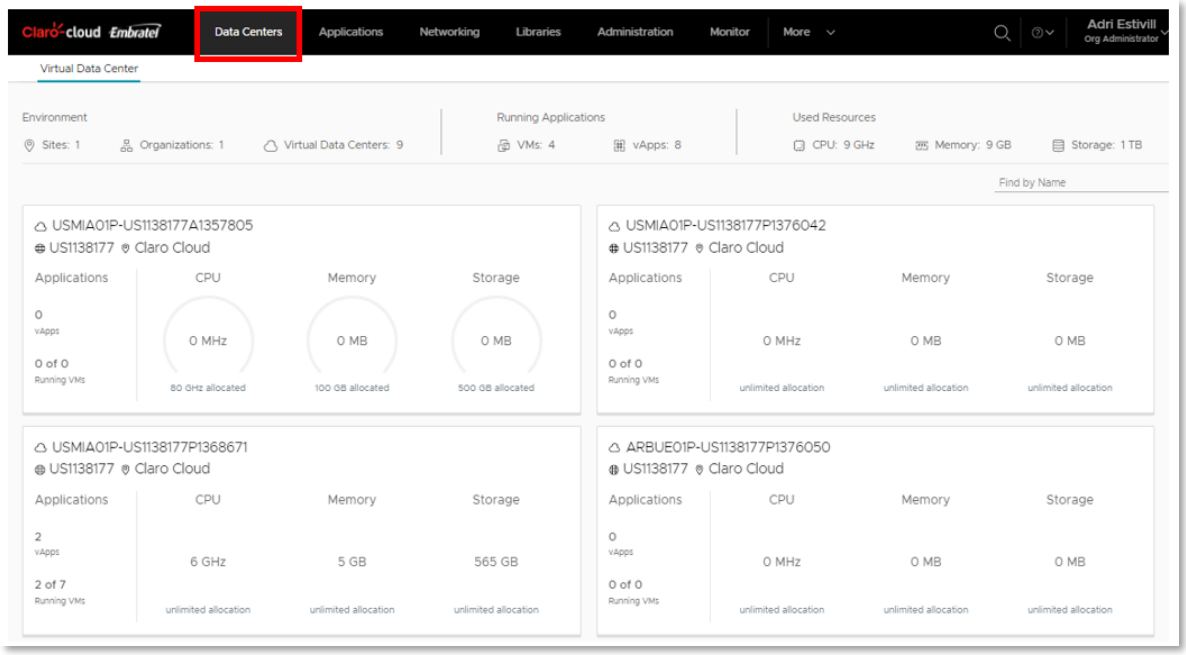
DataCenter	Data center where the new Edge Gateway will be deployed
WAN Access	Connectivity type, you can select Internet or an MPLS hybrid connection
CIDR	Private network segment
LAN Name	Name to be assigned to this network

6. Virtual Machines

In Enterprise Claro Cloud you will find two different methods for deploying virtual machines, provisioning through our Public Catalog or from a custom image (Private Catalog)

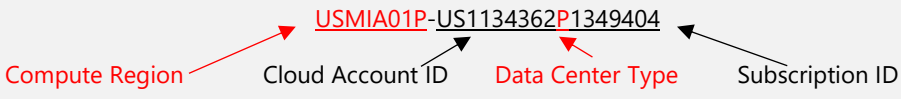
To access the virtual infrastructure management panel follow the following process

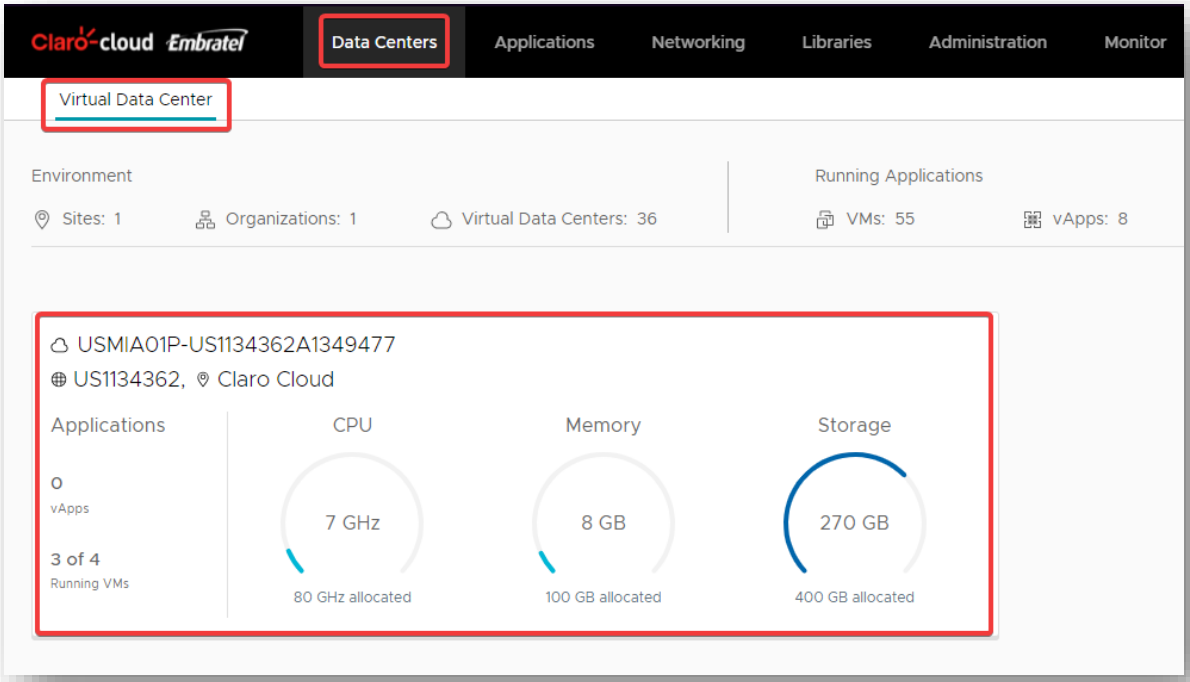
1. Click on the top menu to the "Data Center" option.



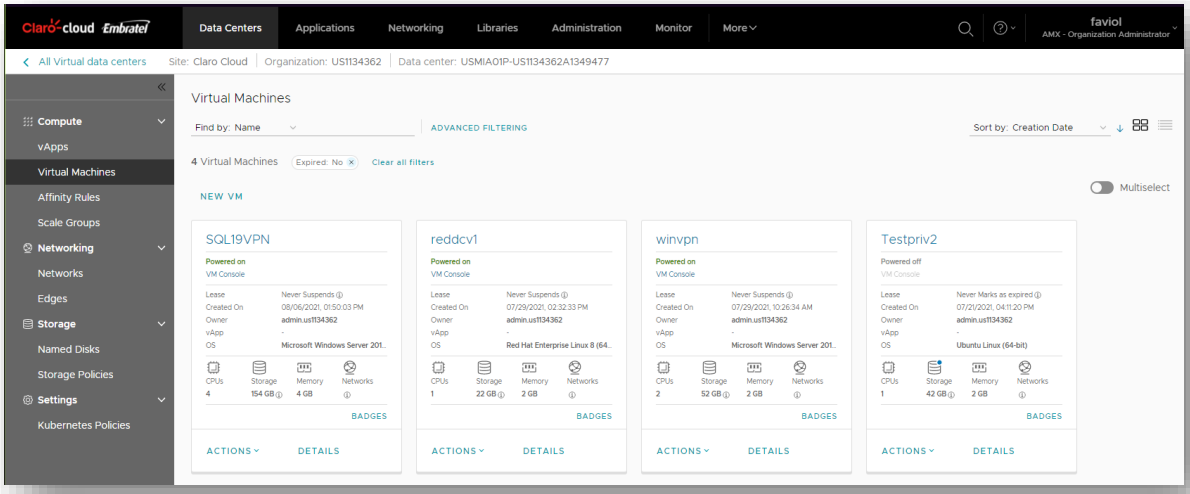
2. Select the Data Center where you need to create virtual machines, click the box.

Note: To identify the purchased data center, consider the following nomenclature





3. The following screen will be displayed, where you can deploy your virtual machines



Create a Virtual Machine from the Public Catalog

In this section you will see the process to be able to deploy a virtual machine from the Enterprise Claro Cloud public catalog

It is important to know that you will be able to find the following catalogs by default

Item	Description
VM-Catalog	Includes available operating systems.

App-Cat	Includes templates for deploying apps through App LaunchPad.
K8s-Catalog	Includes Kubernetes cluster deployment templates.

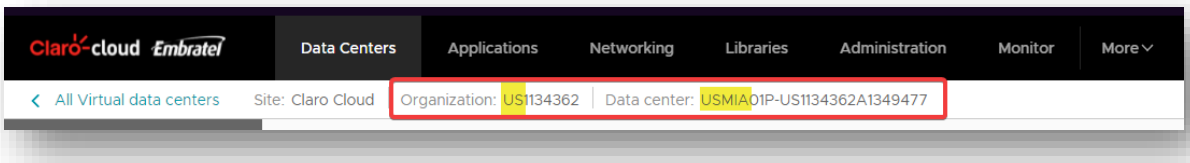
Important: All catalogs have a country-defined nomenclature. For example, United States: **USMIA01P**

Operating systems available in the VM-Catalog:

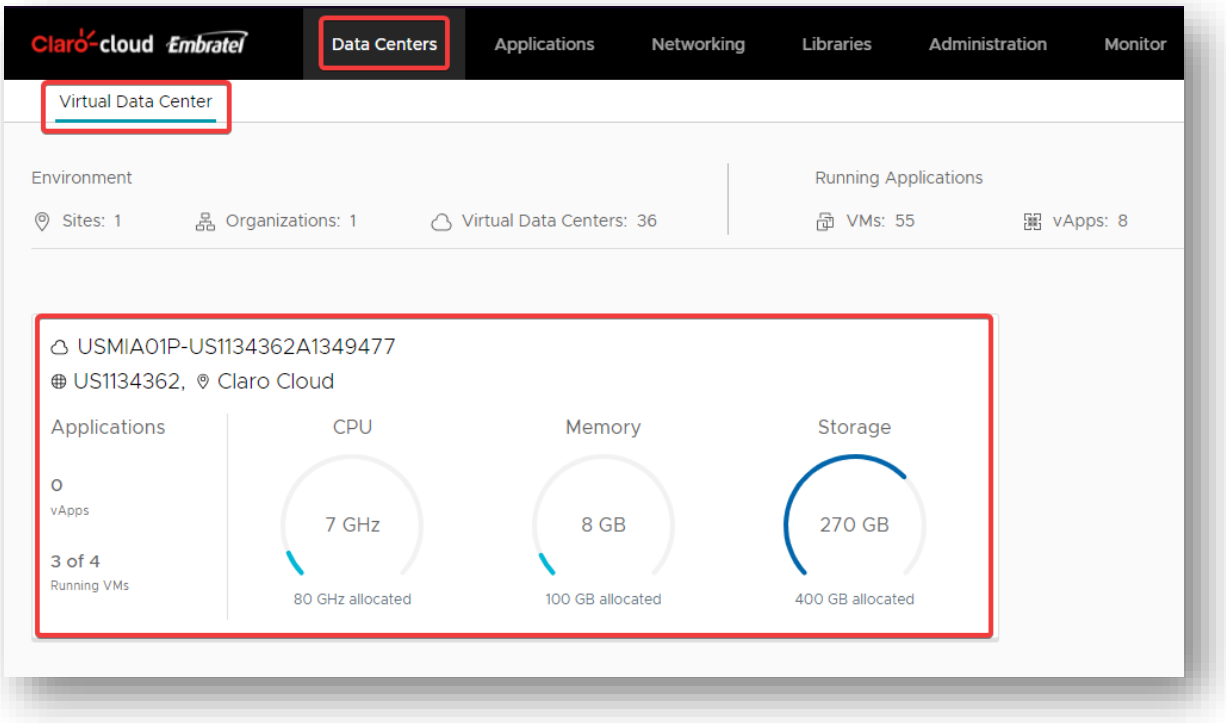
- Windows Server 2012 Standard R2
- Windows Server 2016 Standard R2
- Windows Server 2019
- Windows Server 2012 Standard R2 + SQL ST 2012
- Windows Server 2016 Standard R2 + SQL ST 2017
- Windows Server 2019 + SQL ST 2019
- RedHat 7
- RedHat 8
- RedHat Load Balancer
- RedHat for SAP HANA
- SUSE Enterprise Server 15
- SUSE Enterprise Server 12 for SAP HANA
- Debian Standard 10
- CentOS 7
- CentOS 8
- Ubuntu Server 16.04 LTS
- Ubuntu Server 18.04 LTS
- Ubuntu Server 20.04 LTS
- VeloCloud

Note: It is important to validate the Claro Cloud region where the data center is located in order to deploy the catalog templates corresponding to that same region.

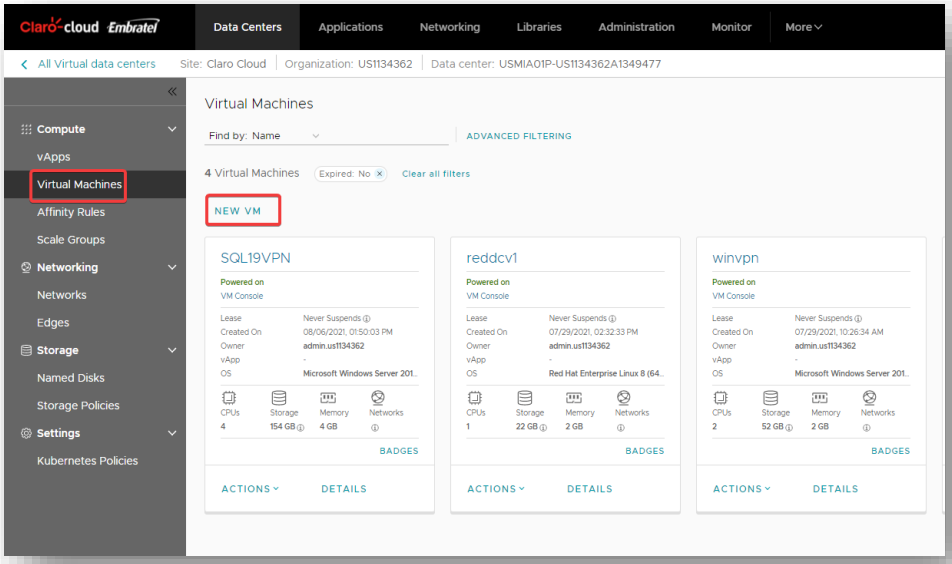
This definition can be found in the data center nomenclature and templates as shown in the example below



1. In the Datacenter menu, select Virtual Data Center, click the check box

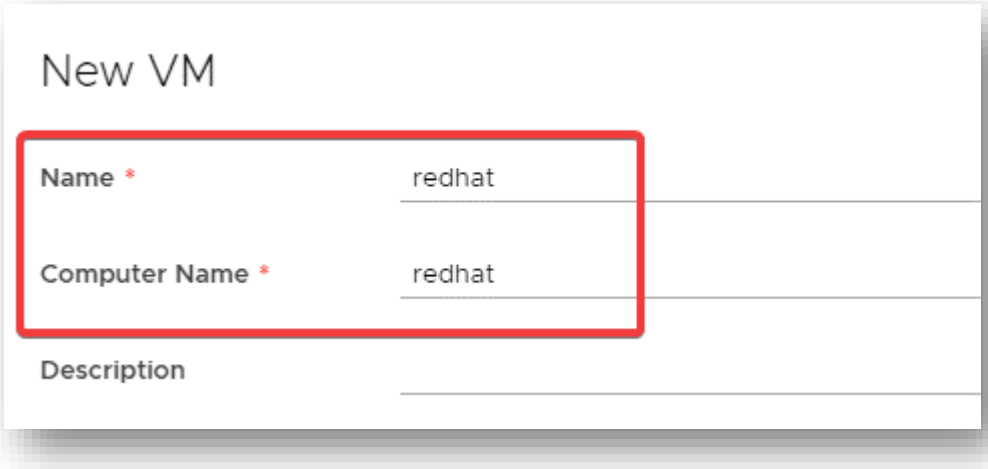


2. Within the Data Center panel, select the "Virtual Machines" option in the left panel and then click on "New Virtual Machine".

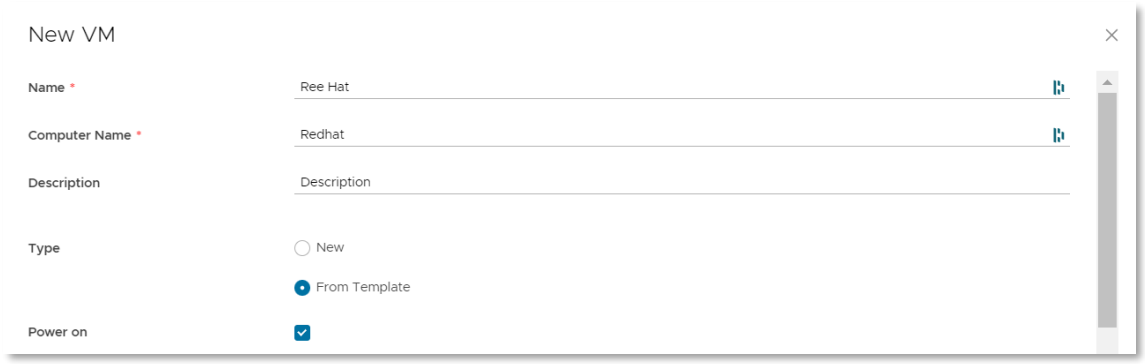


3. The following screen will be displayed where you will have to enter the following information. At the end of clicking on "OK" button

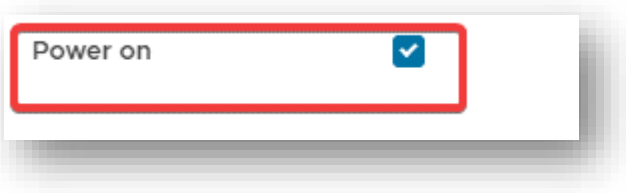
Item	Description
Name	Virtual machine name
Computer Name	Name that will appear within operating system
Description (Optional)	Description of the virtual machine. It is recommended to fill this field with something descriptive for documentation purposes.



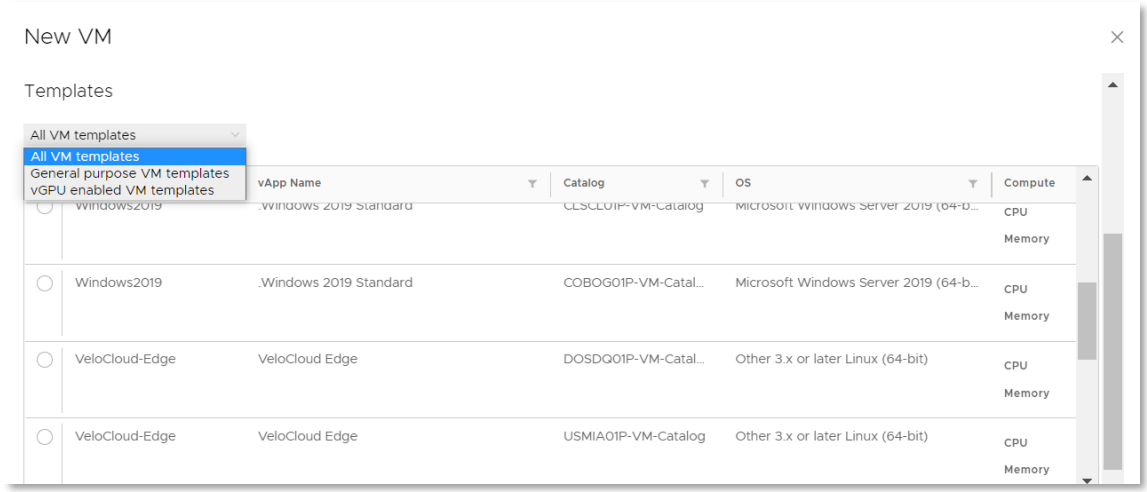
4. Select the "From Template" option to upload the catalog of available virtual machines.



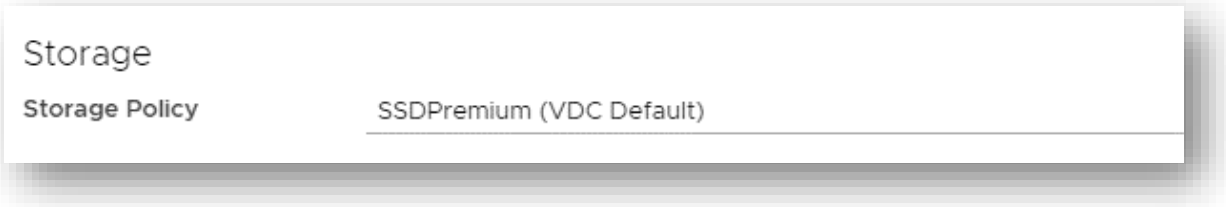
5. Select the Power on option if you require the virtual machine to power on automatically after creation.



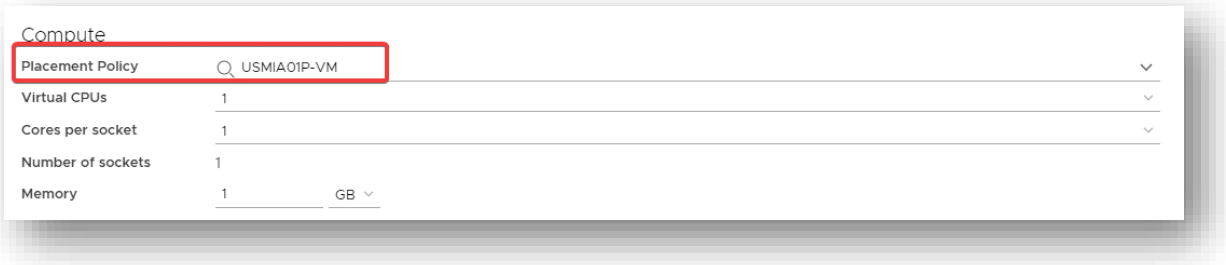
6. In the Templates section you can find the different operating system images available in the Enterprise Claro Cloud catalog for all regions where you have hosted data centers.



7. In the Storage section, SSDPremium will load by default.



8. By default, the placement policy will be preloaded, in the computing region where the virtual machine will be provisioned and indicated



Important: If you select a template from a region other than the datacenter, the following alert will appear: *The selected virtual machine template is labeled with the "DOSDQ01P-VM" policy, which is not valid for this VDC. Select another template.*

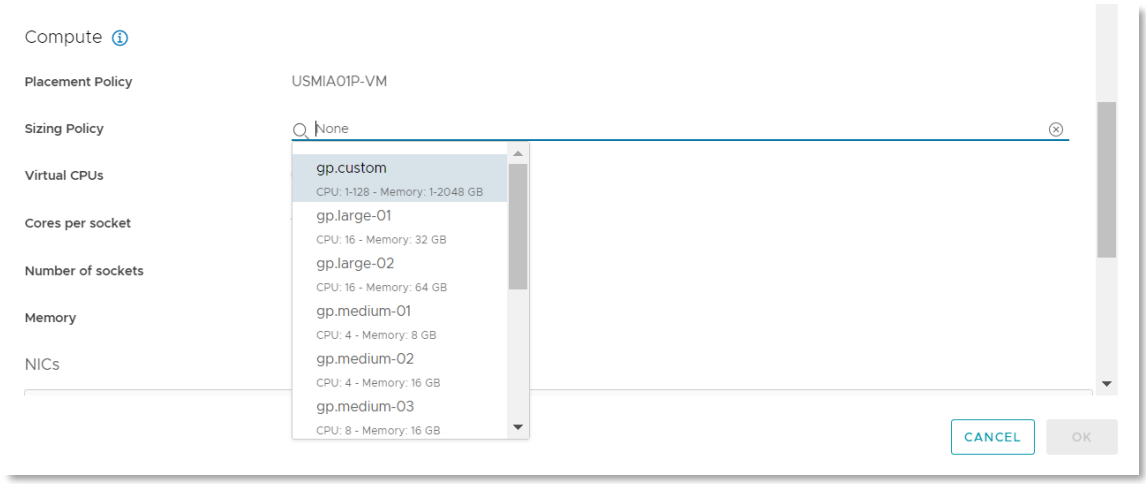
10. Set the size policy, where you can choose from the following options:

- Preconfigured templates:

Templates	vCPU	RAM (GB)
gp.xsmall-01	1	1
gp.small-01	2	4
gp.small-02	2	8
gp.medium-01	4	8
gp.medium-02	4	16
gp.medium-03	8	16
gp.medium-04	8	32
gp.large-01	16	32
gp.large-02	16	64
gp.xlarge-01	32	96
gp.xlarge-02	32	128

- Custom template – You will be able to define the size in a custom way

Resource	Limit
vCPU	1 - 128
RAM (GB)	1 - 2048

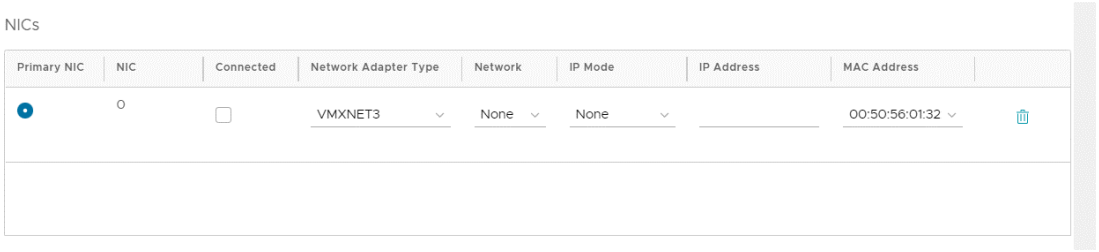


Important: By default, a base disk is added to each virtual machine, which will be used to install the Operating System

20 GB for Linux Operating Systems and 50 GB for Windows Operating Systems

11. In the NICs section, you will be able to enter the settings for the virtual machine's network card(s).

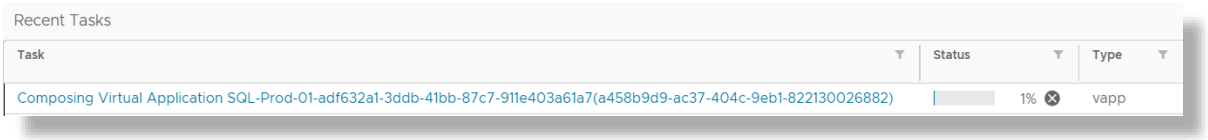
Item	Description
Primary NIC	Select the primary NIC of the virtual machine.
NIC	Order of the NIC on the virtual machine.
Connected	NIC status (Connected/Disconnected).
Network adapter type	Adapter type in the virtual machine E100E / SRIOVETHERNETCARD / VMXNET3 (Recommended)
Net	The network to which the NIC will connect. For the generation of a new network, see the section How to configure networks in Claro Cloud
IP Mode	Mechanism for IP assignment None / DHCP / Static – IP Address Pool (Recommended) / Manual Static
IP address	IP address of the network adapter
MAC Address	The physical address of the network adapter. Loads automatically



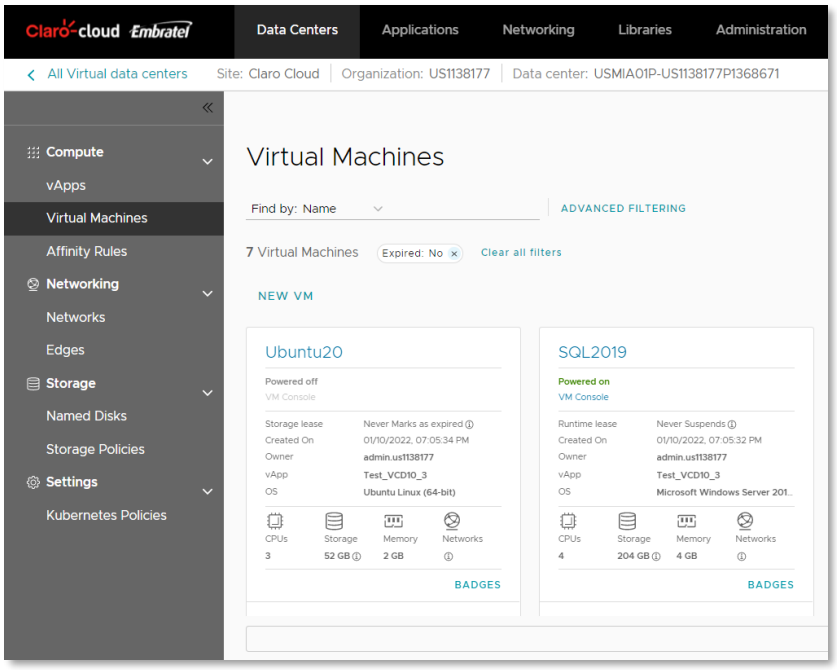
Important: We recommend that you configure at least one NIC in the virtual machine provisioning process.

Otherwise, the configuration can be done, but it is necessary to finish it at the operating system level manually

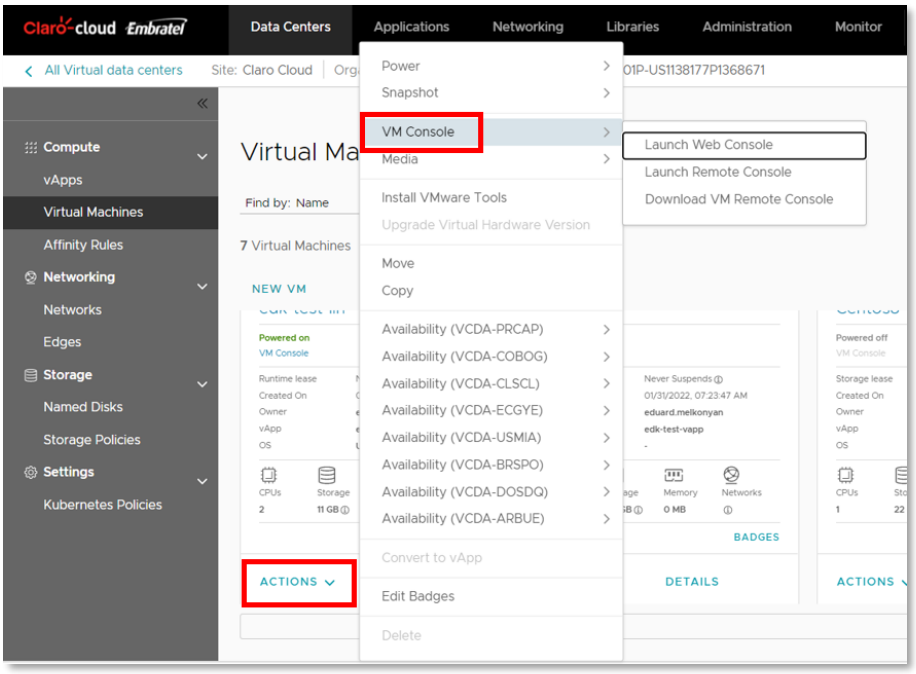
12. Click "OK" to finish deploying the virtual machine. This may take a few minutes; you will be able to see the progress on the taskbar.



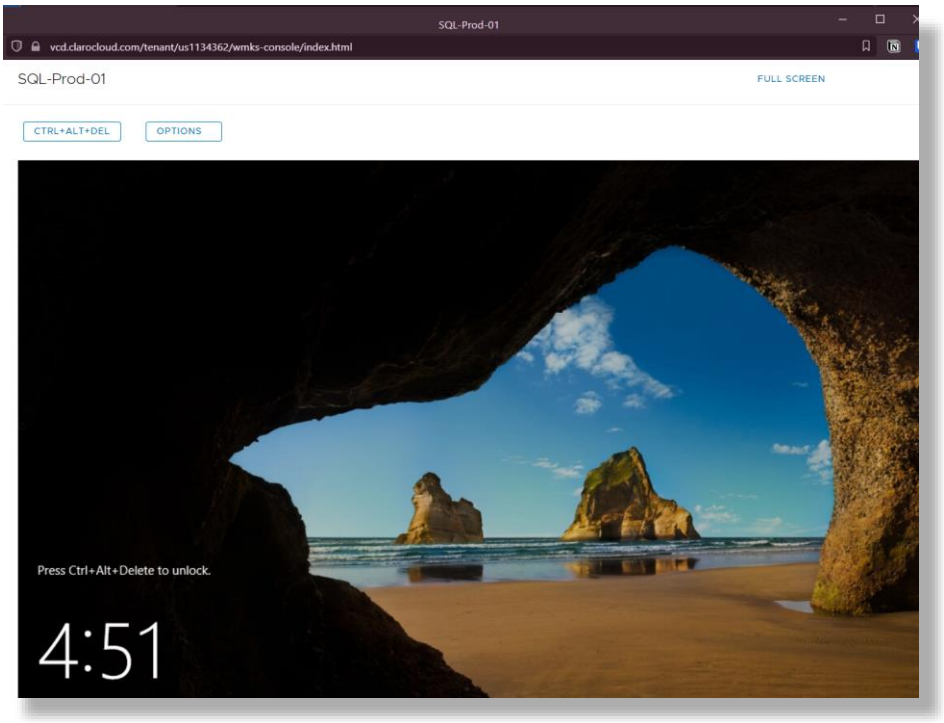
13. When the process is finished, you will find the virtual machine available on the "Virtual Machines" menu



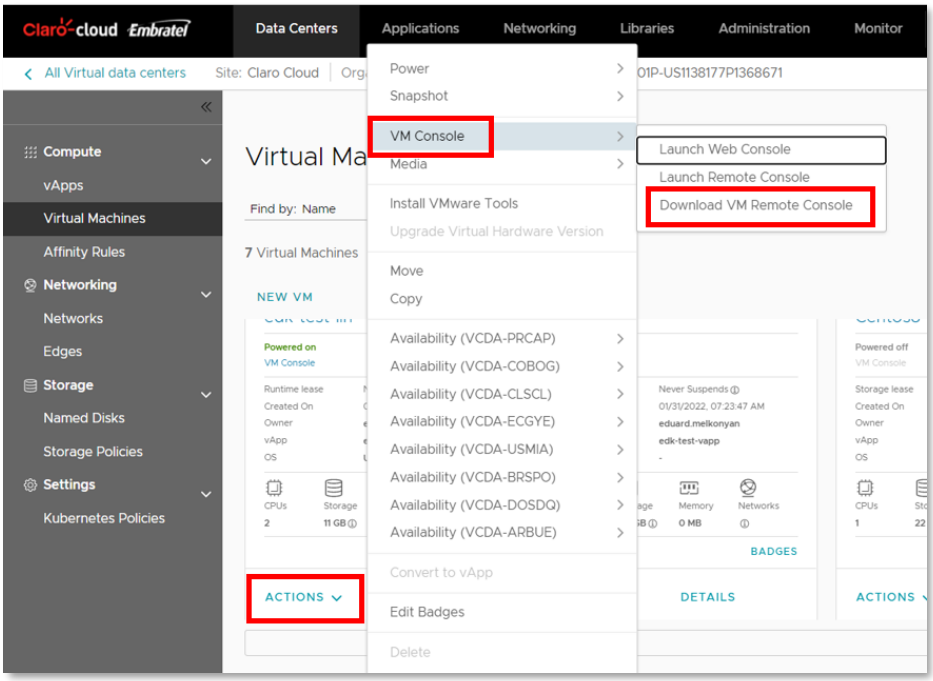
14. To enter the virtual machine, click on "Actions" within the virtual machine box, select "Virtual Machine Console" and then "Launch Web Console".



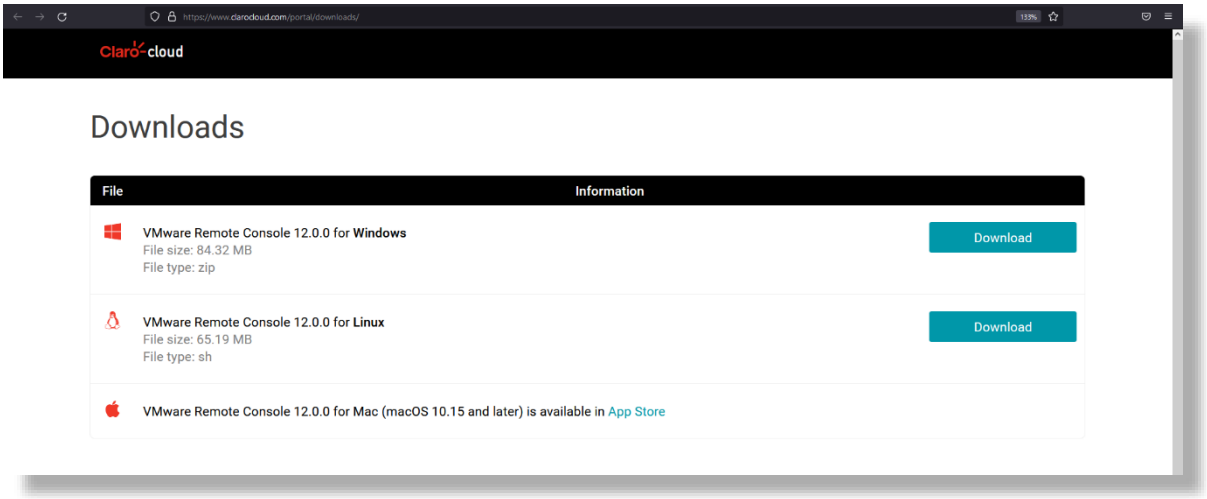
15. The following console will be deployed through which it is possible to access the virtual machine:



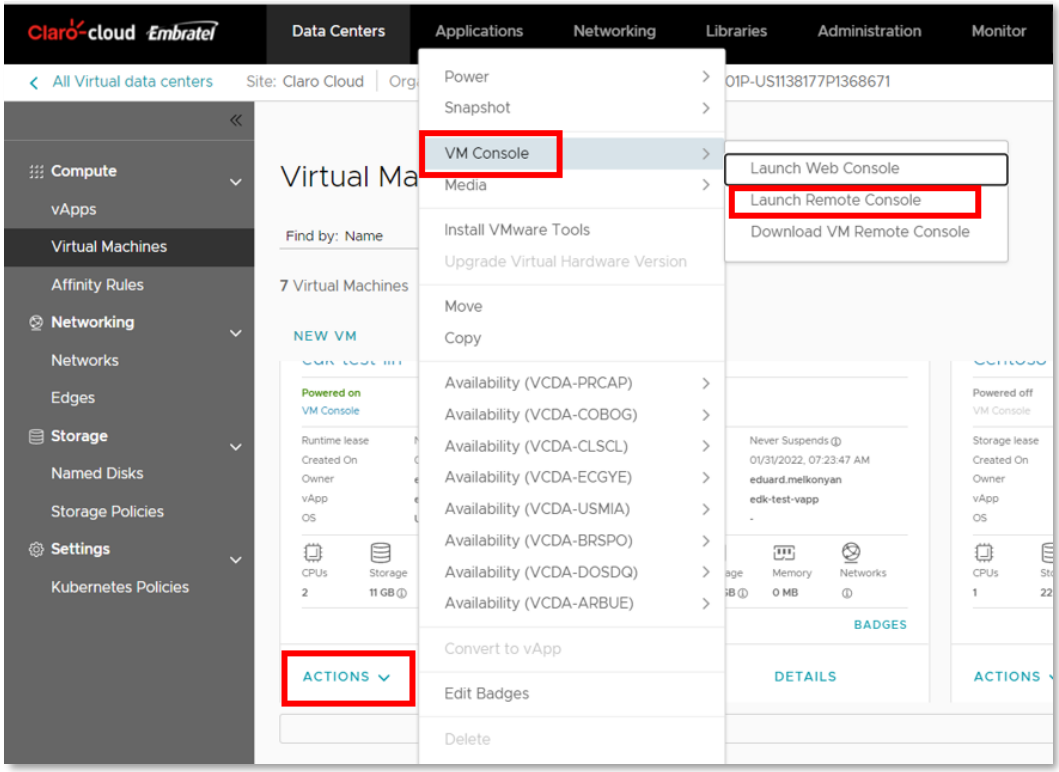
16. You can also enter your virtual machine through a remote console, which will require you to install an application, which you can download in the "Virtual machine console" option and then in "Download VM Remote Console"



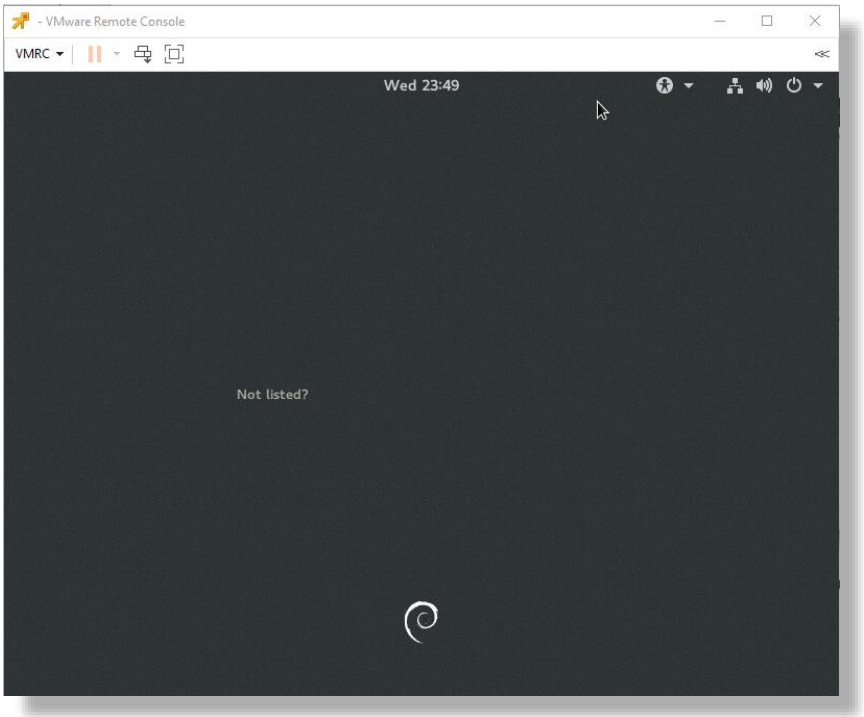
Clicking will open an alternate web page where you can download the application suitable to your computer's operating system



17. At the completion of the download, return to the Enterprise Claro Cloud control panel, click "Actions" within the virtual machine box, select "Virtual Machine Console" and then "Launch Remote Console".

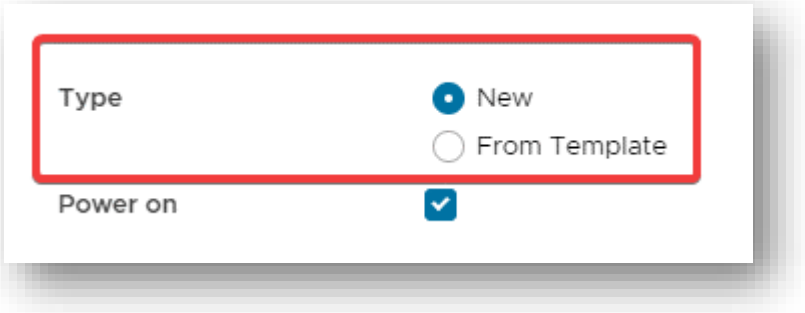


18. The VMware Remote Console application will open, where you can enter your virtual machine



Create a Virtual Machine from a custom image
To be able to create a virtual machine with this option you must create the private catalog beforehand, see the Section Creating Private Catalog

1. Perform the first 5 steps just like in the Virtual Machine Creation process from the Public Catalog.
2. Select in the "Type" field the "New" option



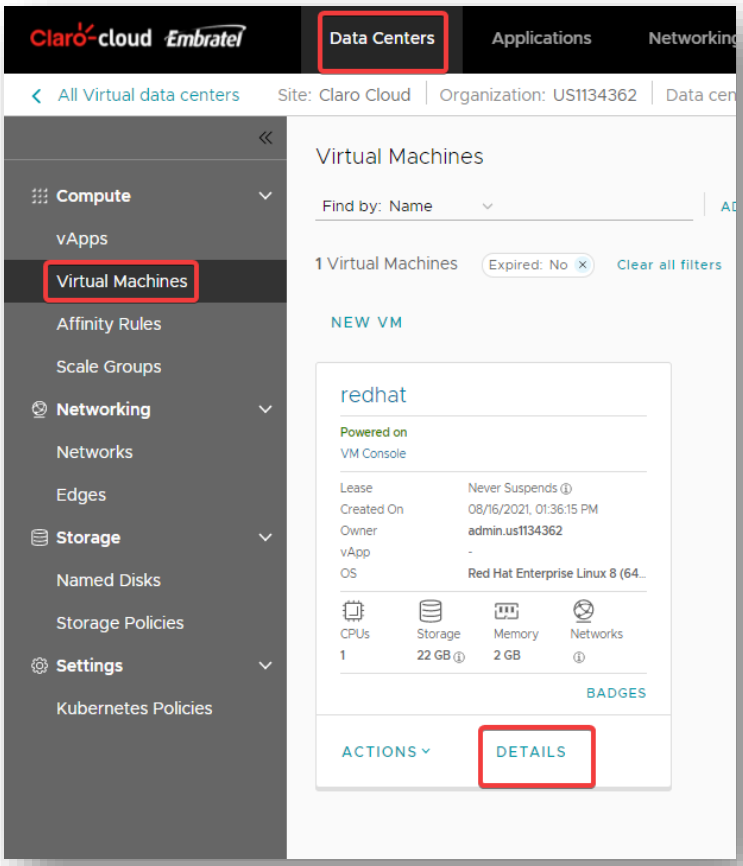
3. The following options will be displayed:

Item	Description
OS Family	Choose the operating system family to which the image to be deployed belongs
Operating system	Specify the operating system version to deploy. For Linux, if the desired option does not exist, select Other Linux
Boot image	Select the ISO image that has previously been uploaded to the catalog

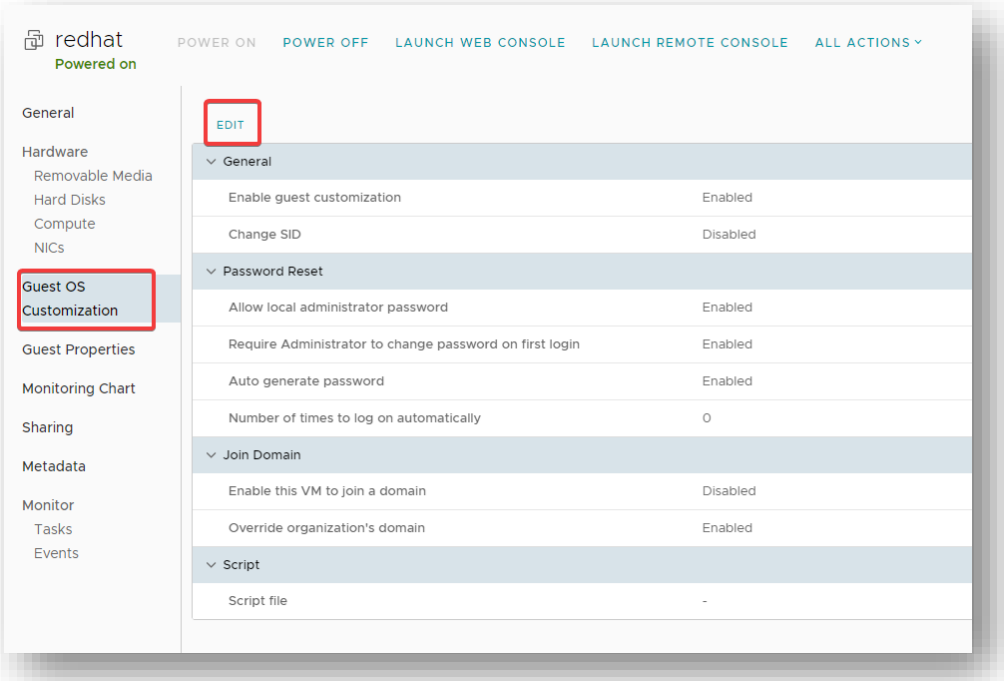
4. Continue from step 9 of the virtual machine creation process from the public catalog

First access to a virtual machine
To access for the first time, a default password is generated, which you can find through the following steps:

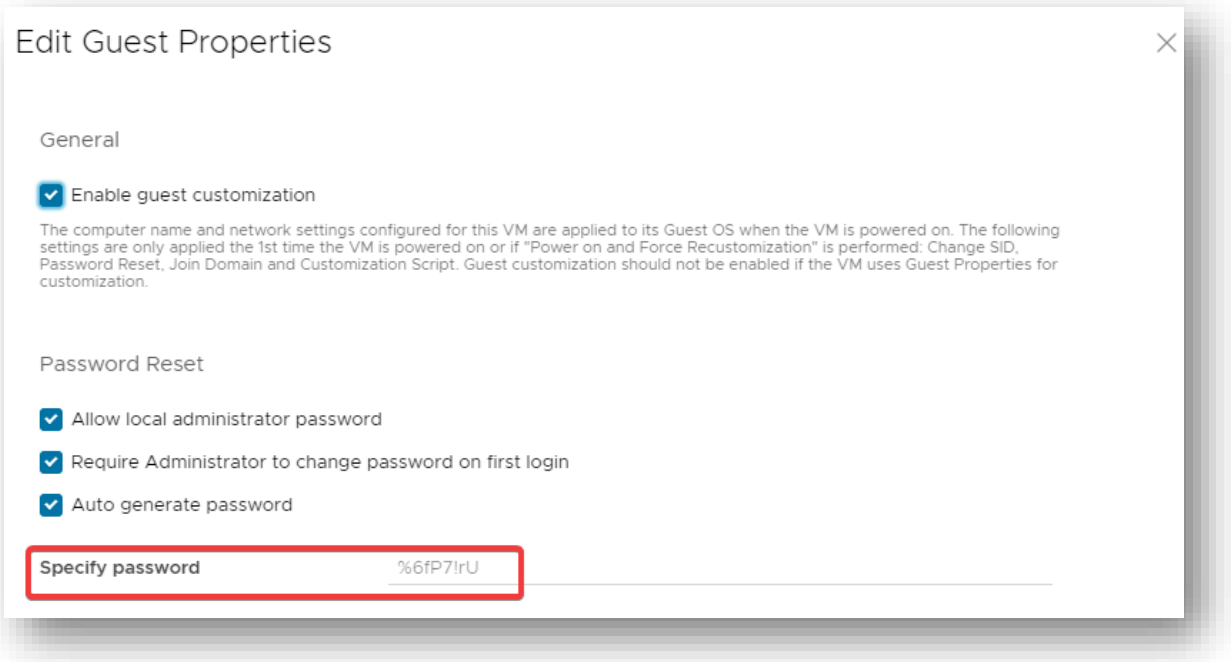
1. Select the virtual machine and click Details.



2. Go to Guest OS Customization and click Edit



3. The default password is located in the Specify Password field



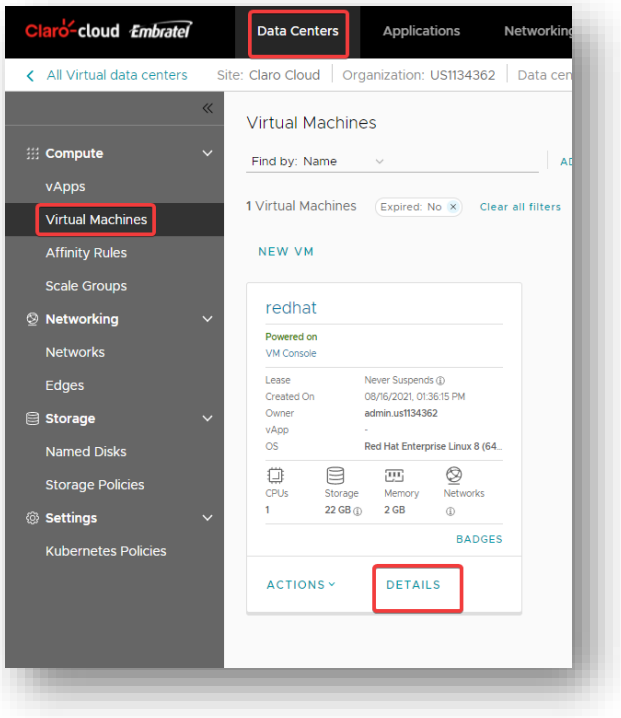
Important: It is advisable not to clear this password manually. At the time of first entering the virtual machine, the operating system will request the password change.

Edit properties of a virtual machine

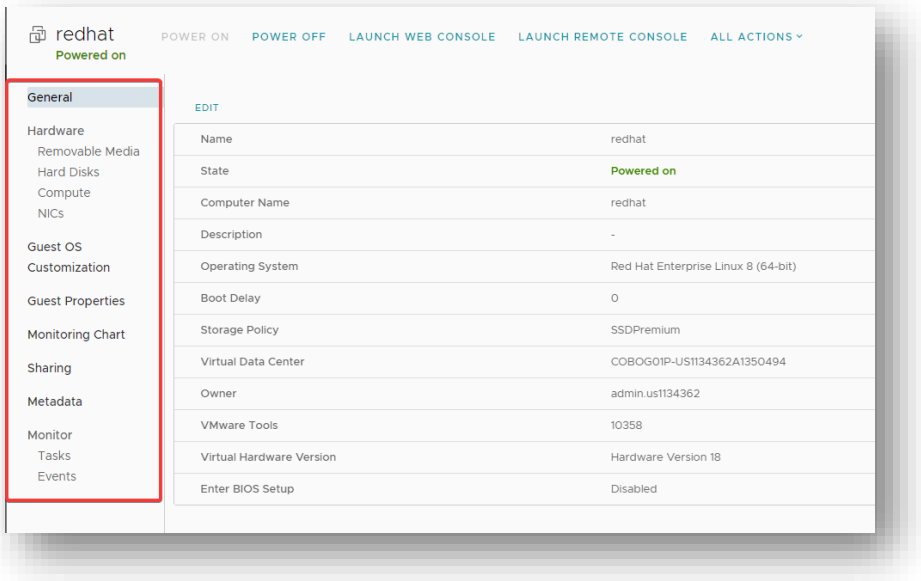
In this section you can view the main features of your virtual machines such as hostname, description, and other properties of a virtual machine.

To change certain properties as an operating system, the virtual machine will be required to be powered off.

1. In the Datacenter pane, click Virtual Datacenter, and from the menu on the left select Virtual Machines
2. Select the virtual machine to edit and then Details



3. The following options described below will appear:



Item	Description
General	Properties such as virtual machine name and operating system family
Hardware	Properties of compute, storage, and network resources

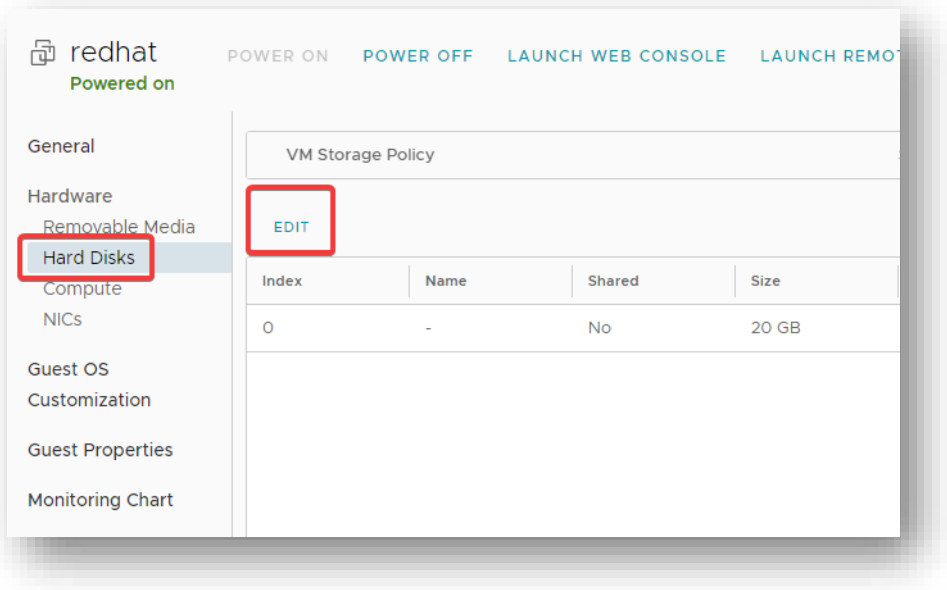
Guest OS Customization	Configurations about the operating system such as SID, passwords, domains, use of boot scripts
Monitoring chart	Disk, CPU, and memory usage metrics
Metadata	Additional tag-based information about the virtual machine
Tasks	Tasks performed on the platform, states, initiator, start and end time, among others
Events	Important events about the platform

Configuring Hard Drives

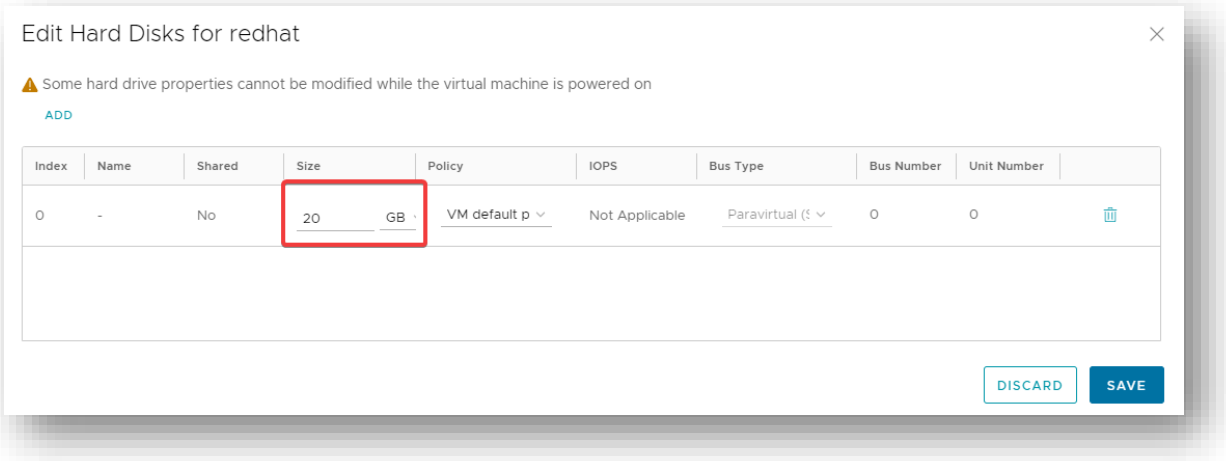
In this section, you can access disk configuration, expand disks, and add new disks to the virtual machine.

Increasing the capacity of a hard disk

1. Within the panel of a virtual machine, select in the submenu the option "Hard Disks" and click on "Edit"



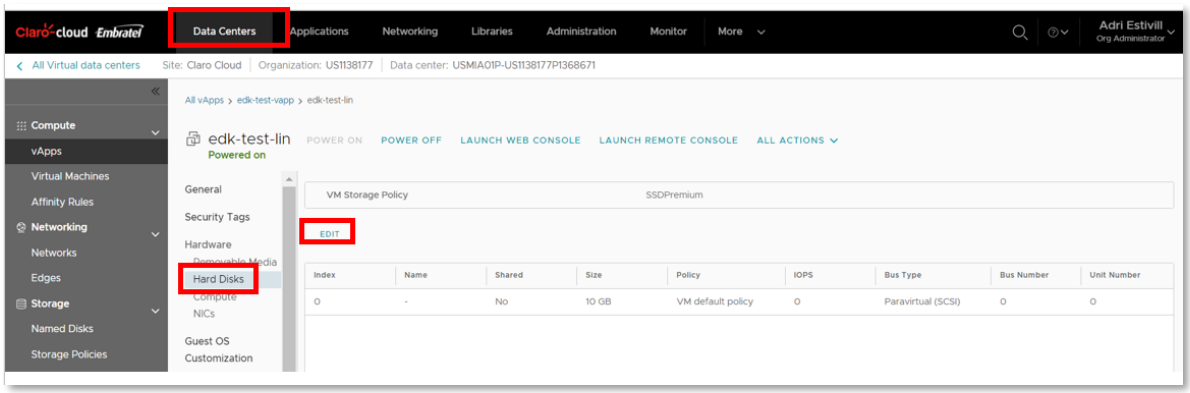
2. The following screen will be displayed where you can increase the capacity of your hard drives



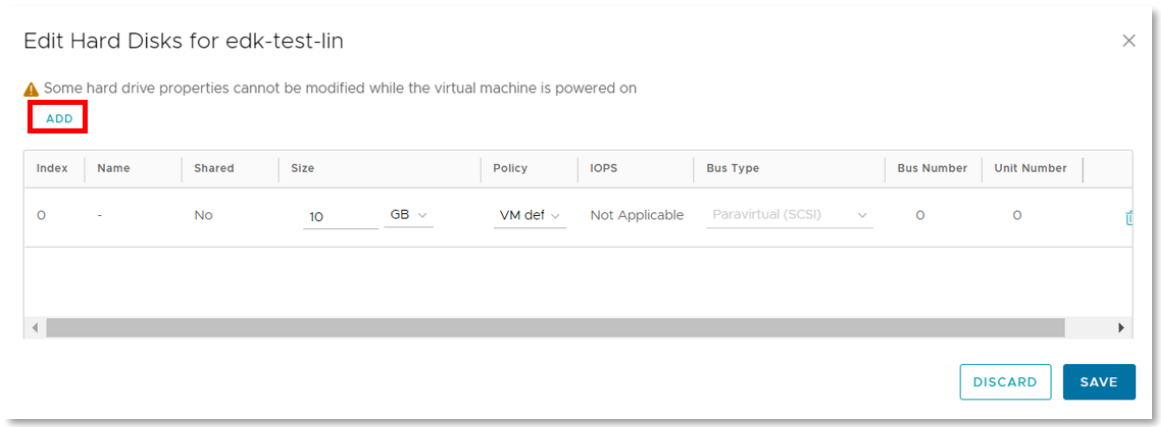
Important: It is not possible to decrease the capacity of a hard disk.

Create a new Hard Drive

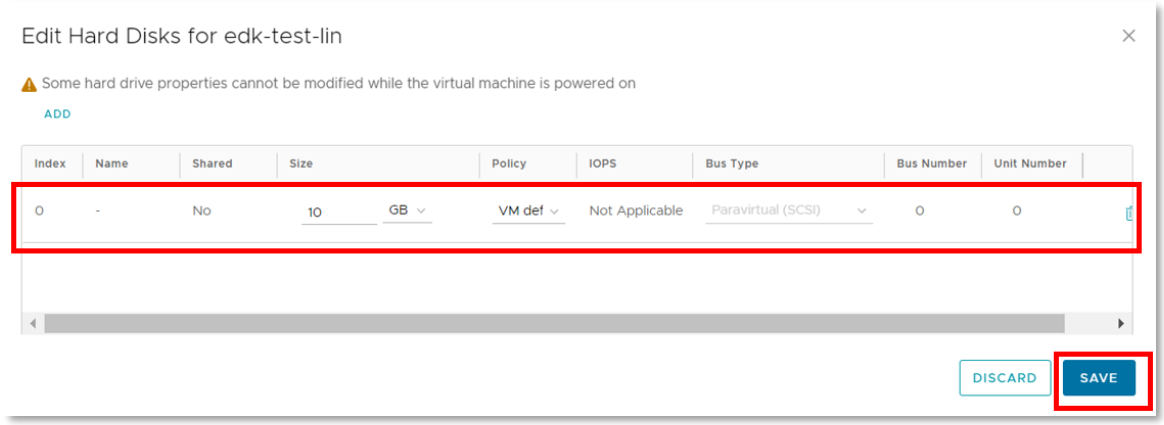
1. Within the panel of a virtual machine, select in the submenu the option "Hard Disks" and click on "Edit"



2. The following screen will be displayed, click on "Add"



3. Enter the information for the new hard drive. When finished, click "Save"



> **Important:** For Windows Operating Systems it is necessary to choose in the Bus Type the option "Paravirtual".
>
> All hard disks at the time of attachment to the virtual machine are added unformatted so it is the customer's responsibility to format them and mount them to the appropriate partition

Configuring Separate Hard Drives

Enterprise Claro Cloud allows you to create virtual disks independent of virtual machines, which can be used to increase the capacity of one or multiple virtual machines. The activation of this functionality can be requested through Claro Technical Support.

> **Note:** Like hard disks associated with virtual machines, independent drives are created unformatted, so it is the customer's responsibility to give them the required format and mount them to the partition of their preference to be used in virtual machines

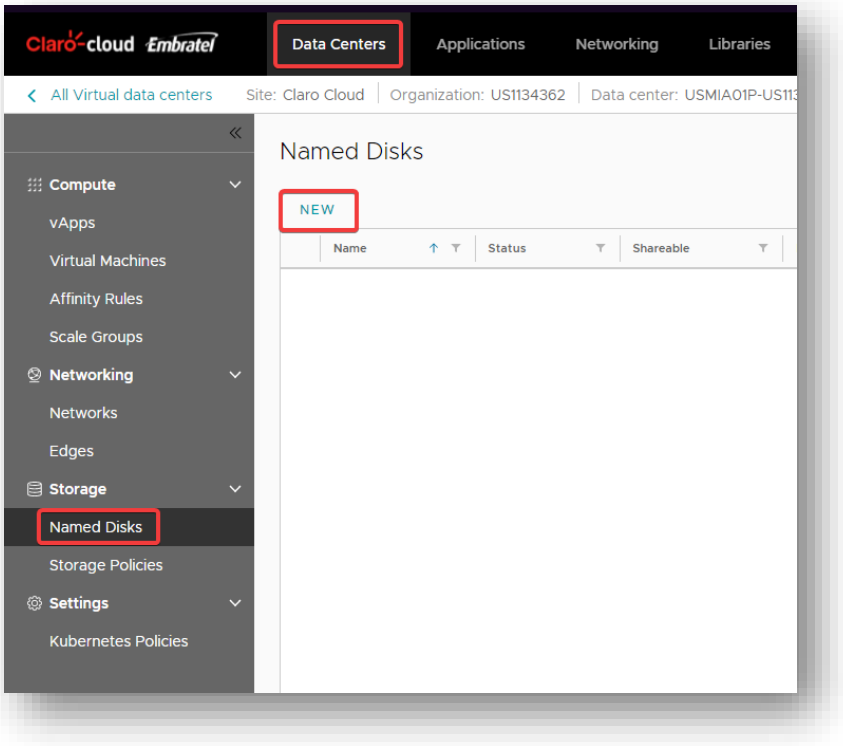
If you attach a named disk, you cannot take VM snapshots. If a shared disk is connected to a virtual machine, you cannot edit its hard disk settings from the virtual machine's details view.

If your organization's VDC has a storage policy with virtual machine encryption enabled, you can encrypt virtual machines and disks by associating them with storage policies that have virtual machine encryption capability.

Creating a separate disk

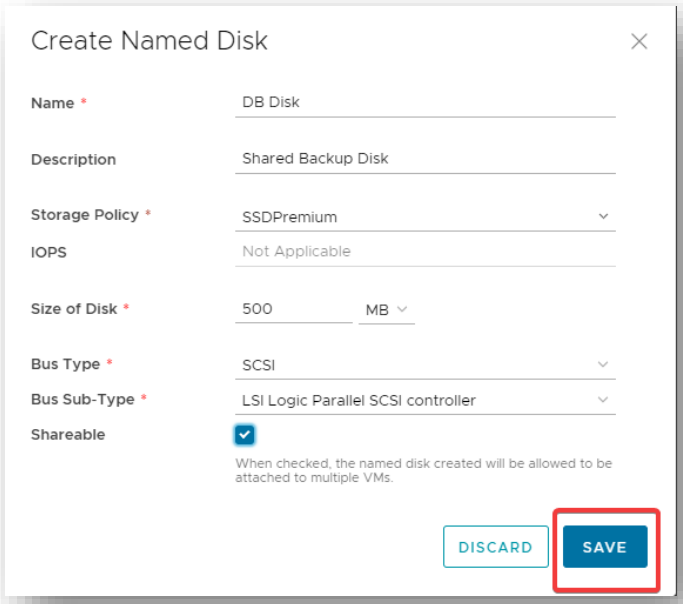
1. Verify that you have the appropriate administrator permissions to perform these tasks. Otherwise, they can be requested from Claro Technical Support through your Administrator.

2. In the main menu select "Data Center", then in the menu on the left, select "Named Disks", click "New"

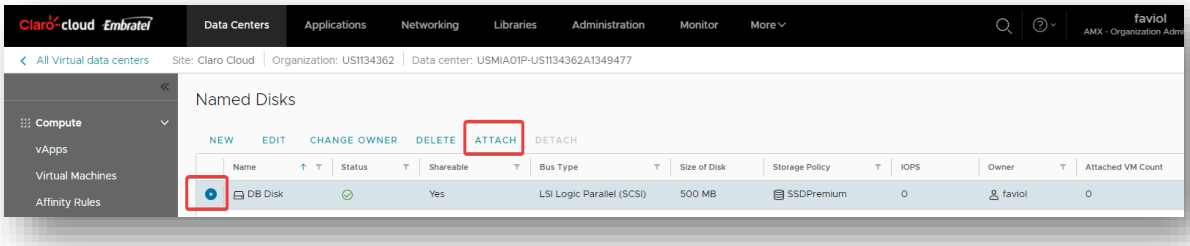


3. The following screen will be displayed where you will have to enter the following information. When finished click the "Save" button

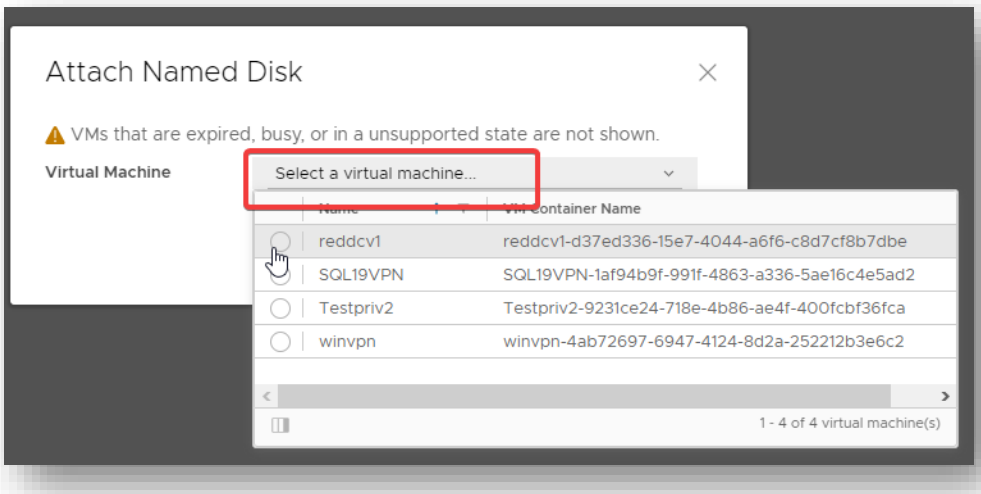
Item	Description
Name	Disk name
Description	Disc description
Storage Policy	Disk storage policy
Disk size	Disk capacity, can be specified in MB/GB
Bus type	Selecting bus to use SCSI (Recommended) / IDE / SATA / NVME
Bus subtype	Bus Subtype Parallel Buslogic SCSI Controller / Parallel LSI Logic SCSI Controller (Recommended) / LSI Logic SAS SCSI Controller / Paravirtual SCSI Controller (Recommended for Windows)
Shareable	When this option is selected the disk is allowed to be associated with more than one virtual machine



4. At the end of the creation process, select the created disk and click on the "Connect" button

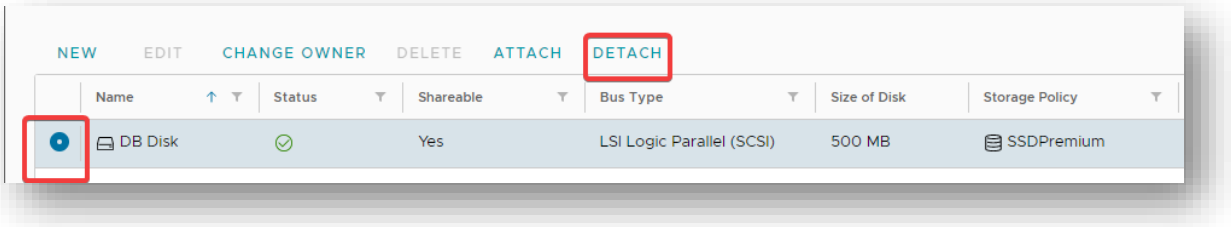


5. The following screen will open where you can select the virtual machine to which you will be presented with the hard disk

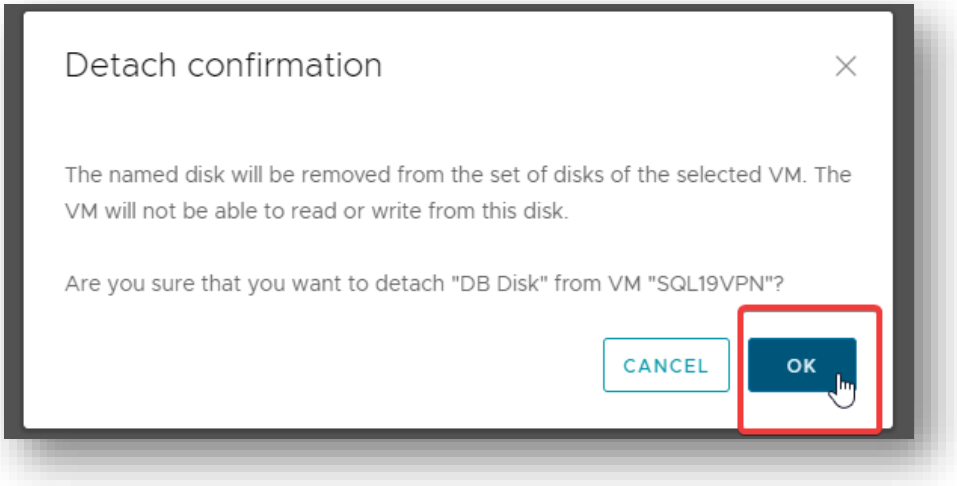


Note: If you enable "shareable" check in step 3, you can connect more machines to the disk, repeating step 4 and 5.

6. If you need to disconnect a separate disk from a virtual machine, select the disk and click "Detach"



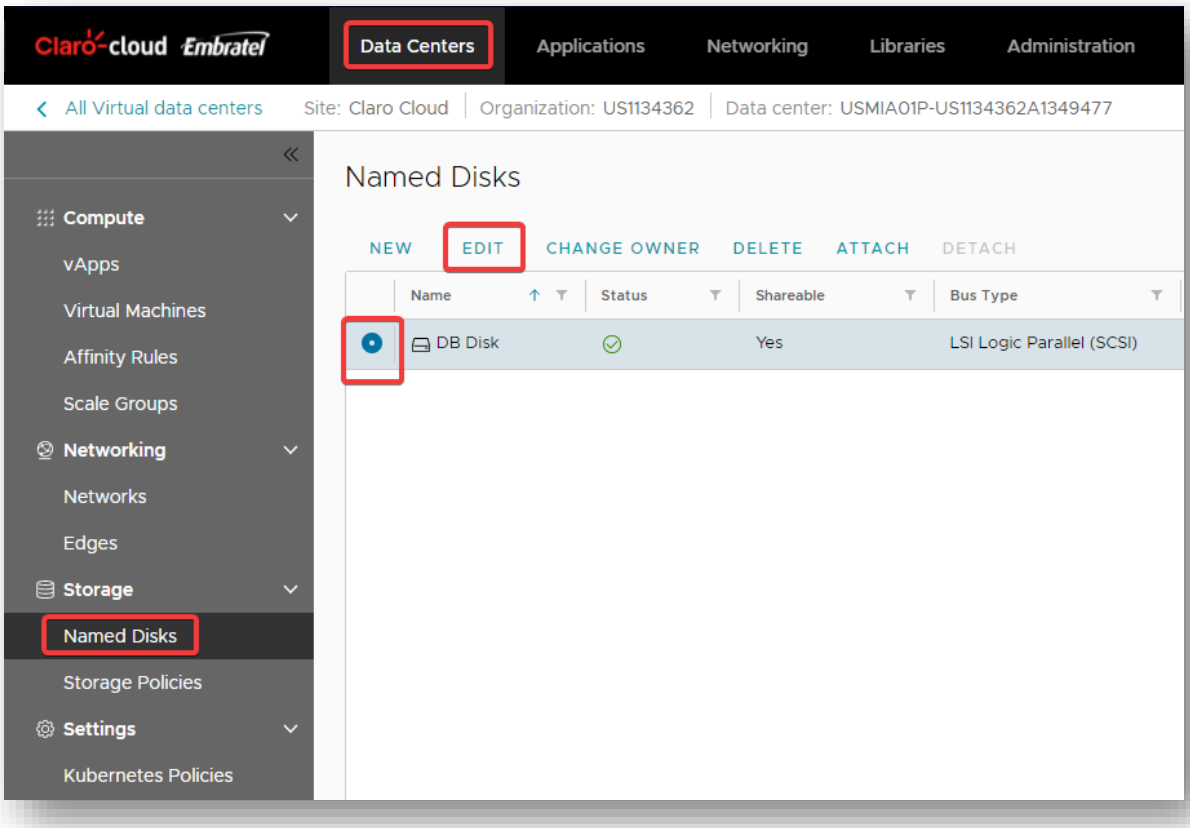
7. The following screen will open where you can select the virtual machine to which the hard disk will be disconnected, click on "OK" to finish the process



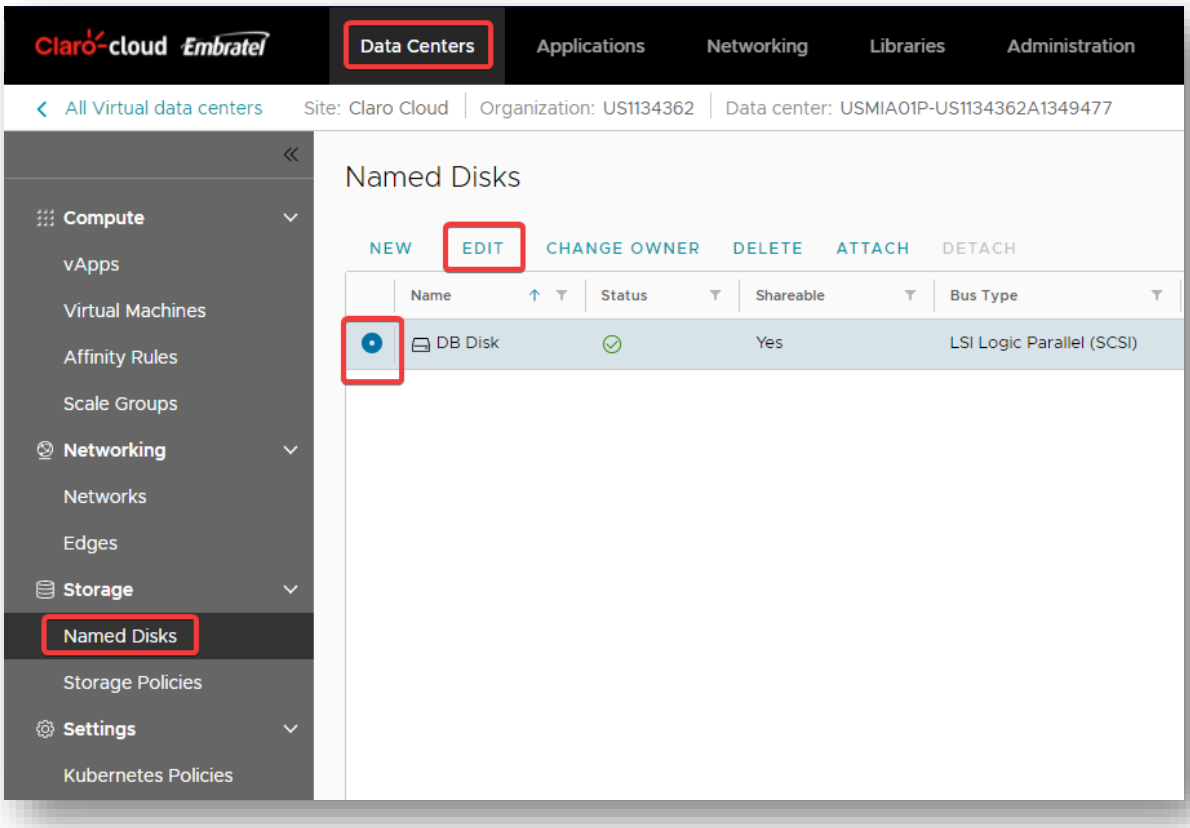
Resize an independent disk

Once the disk is created, you can modify its name, description, storage policy, and size. Consider that making any changes to the disk requires that it not be associated with any virtual machine.

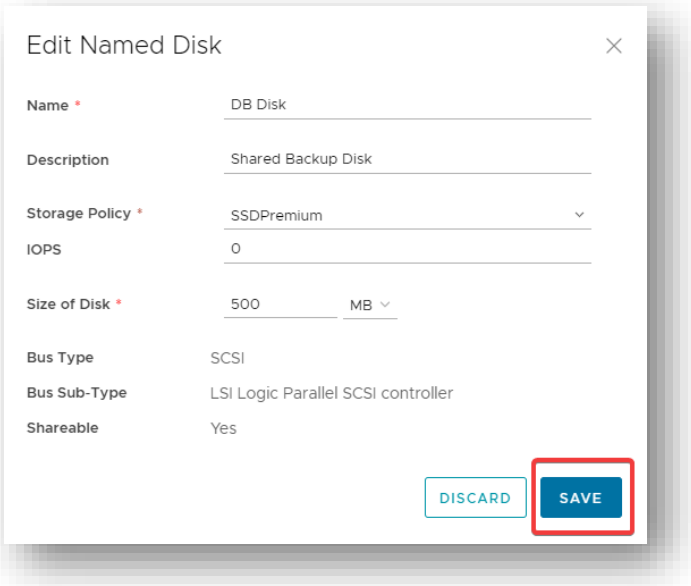
1. In the main menu click on "Data Center", in the left menu select "Named Disks"



2. Select the disk and click Edit

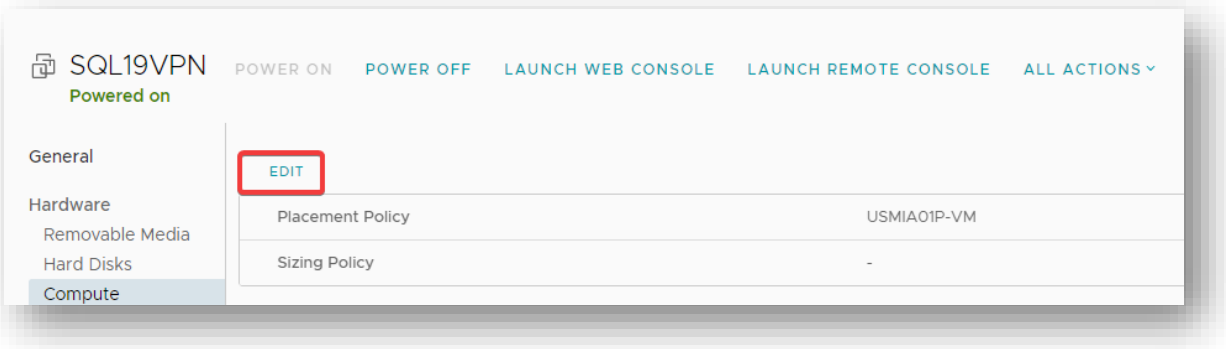


3. The next screen will open where you can modify the disk parameters. At the end of clicking on "Save"

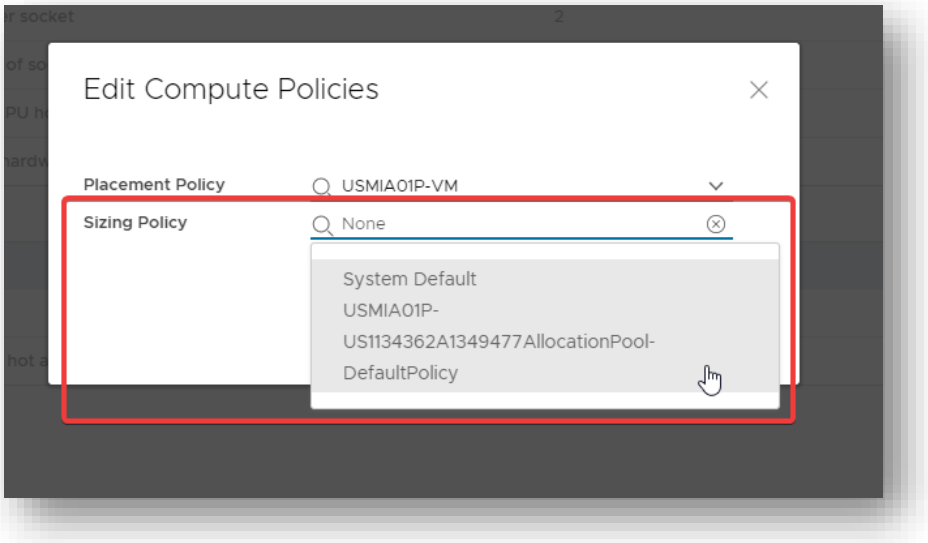


Changing the capacity of a virtual machine

1. Within the panel of a virtual machine, select the "Compute" option in the submenu and click "Edit" in the first table.



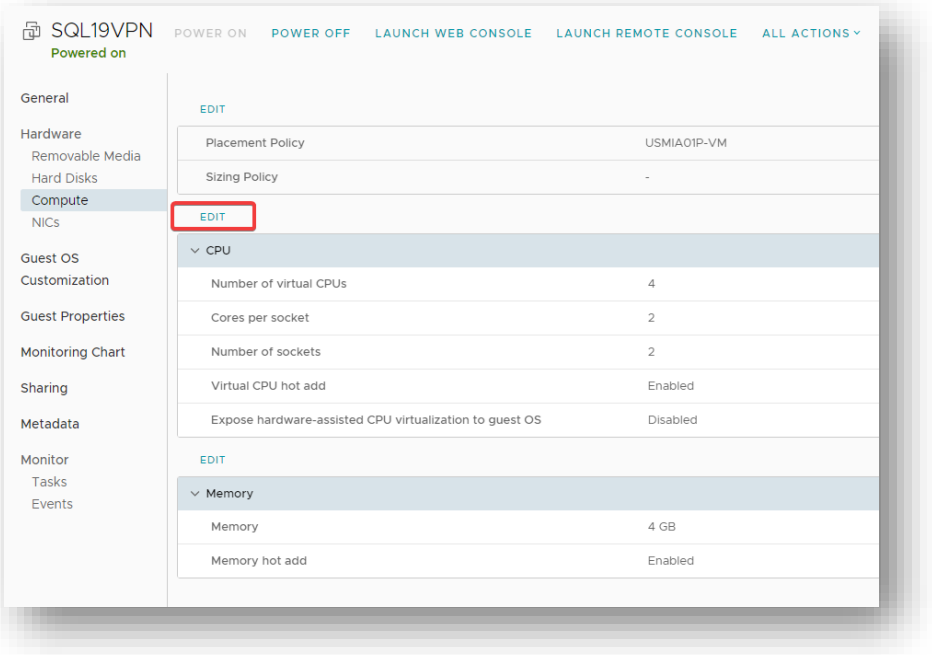
2. The following screen will be displayed, where you can choose the new size of your virtual machine



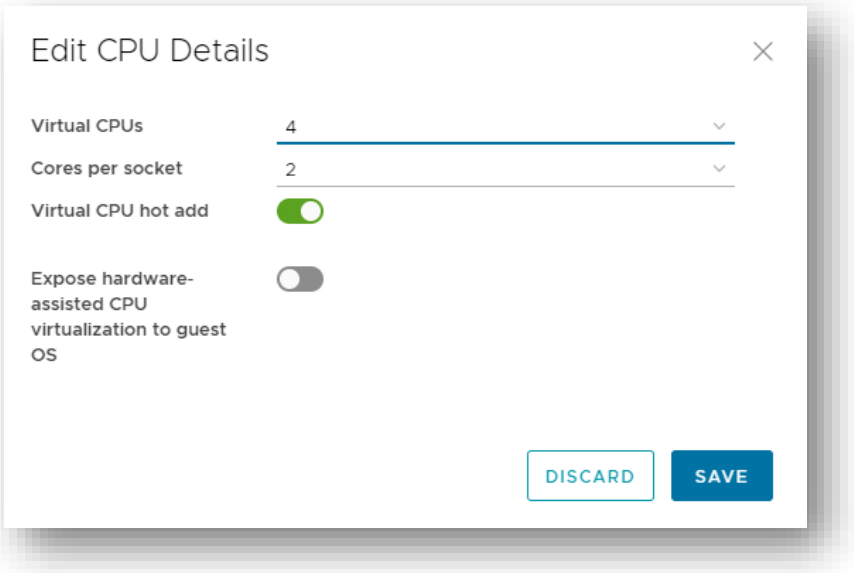
In case of choosing the "gp.custom" option, you can configure the size of your vCPU and RAM in a personalized way. Follow these steps

CPU configuration of a virtual machine:

1. Within the Compute section, select Edit in the CPU section.

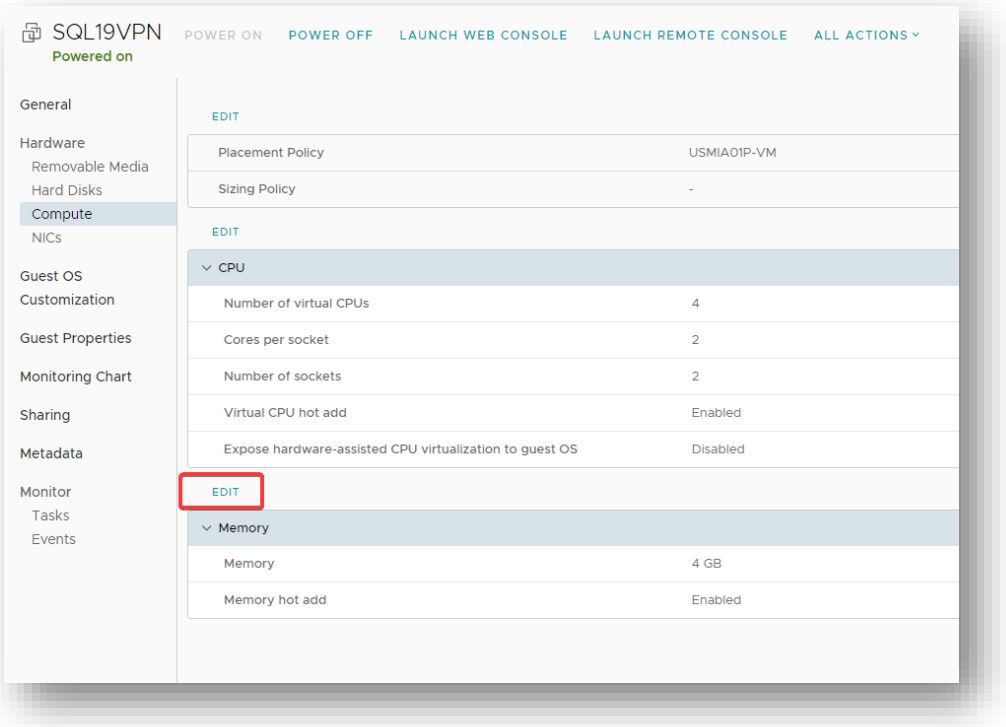


2. Modify the required parameters and CPU distribution by sockets. At the end, click on "Save" to finish the configuration.

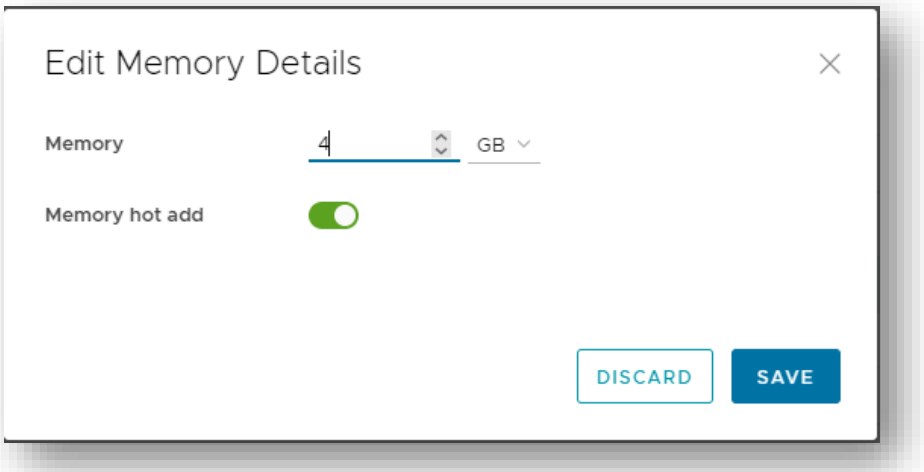


To modify the memory settings of a virtual machine:

1. Within the Compute section, select Edit in the Memory section.



2. Allocate the required memory for the virtual machine. At the end, click on "Save" to finish the configuration.

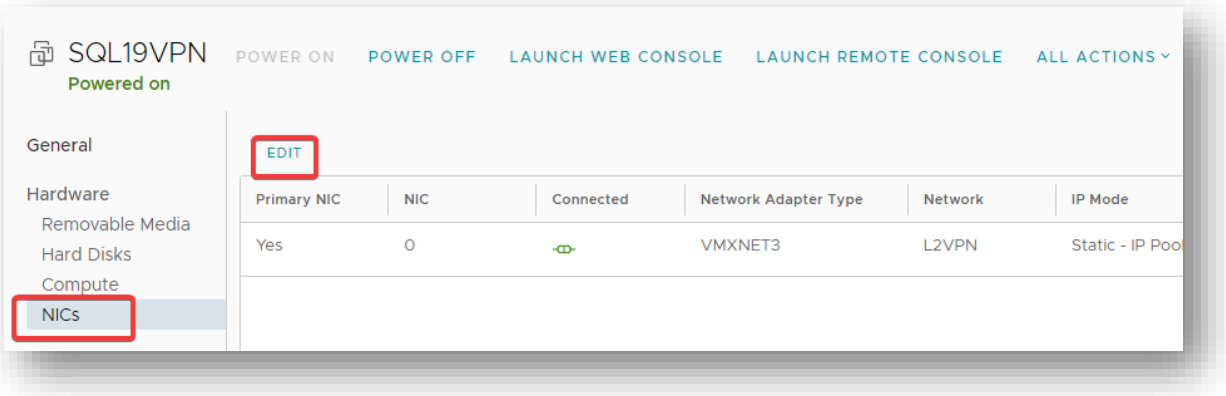


Important:

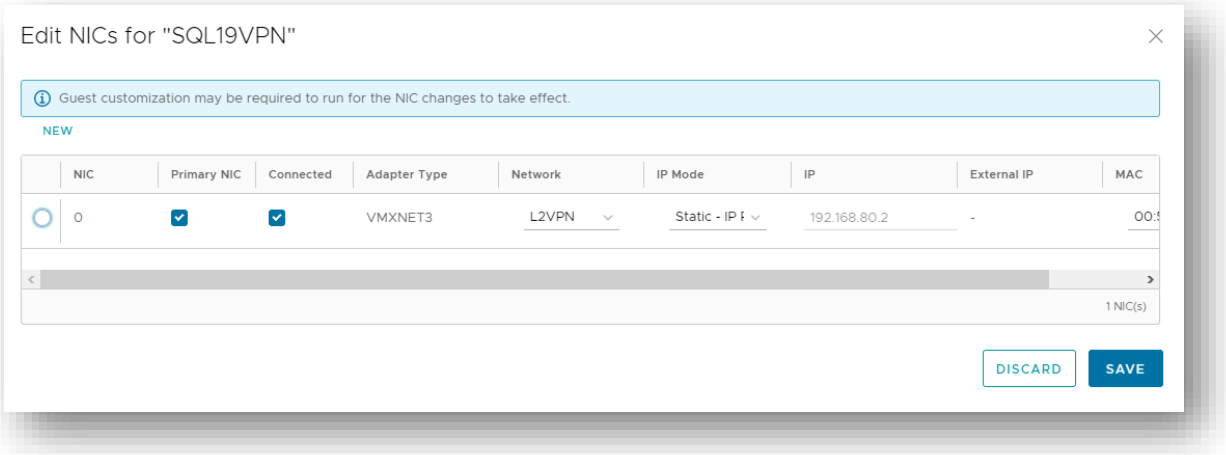
- By default, virtual machines have the Hot Add parameter active, which allows for hot adding of CPU and hot Memory resources from 4 vCPUs.
- For virtual machines smaller than 4 vCPUs or 4 GB of memory, you must shut down the virtual machine if you need to increment/decrease resources.
- For data centers with on-demand schemes, you can increase/decrease virtual machine capacity through predefined capacity templates or through custom sizes.
- For data centers with Resource Pool schemes, it is possible to increase/decrease the capacity of virtual machines only through custom sizes.

Configuring NICs
In this section you can modify the settings of the network cards assigned to the virtual machine.

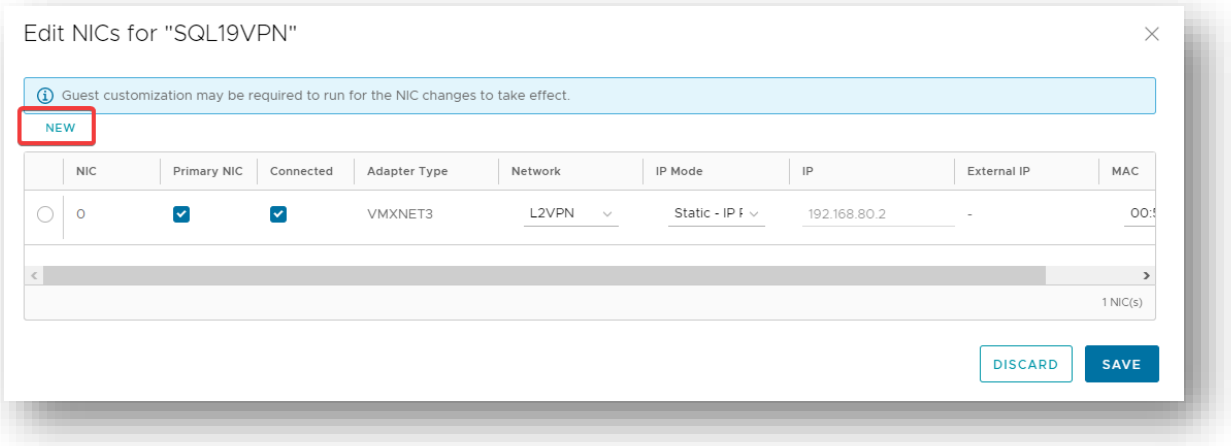
1. Within the panel of a virtual machine, select the "NIC" option in the submenu and click "Edit" in the first table.



2. The following screen will appear where you can add a new NIC or modify an existing one:

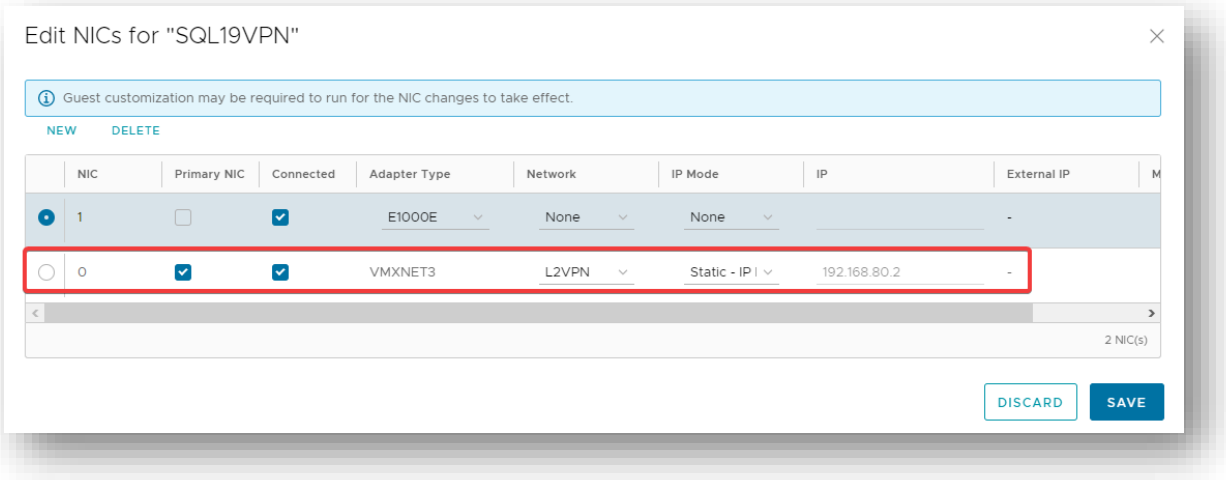


3. Select the NIC to configure or click "New" to add a new NIC.



4. Enter the following data to perform the NIC configuration. At the end, click "Save"

Item	Description
Primary NIC	Select the primary NIC of the virtual machine.
Connected	NIC status (Connected/Disconnected).
Network adapter type	Adapter type in the virtual machine E100E / SRIOVETHERNETCARD / VMXNET3 (Recommended)
Network	The network to which the NIC will connect. For the generation of a new network, see the section How to configure networks in Claro Cloud
IP Mode	Mechanism for IP assignment None / DHCP / Static – IP Address Pool (Recommended) / Manual Static
IP address	IP address of the network adapter
MAC Address	Physical address of the network adapter



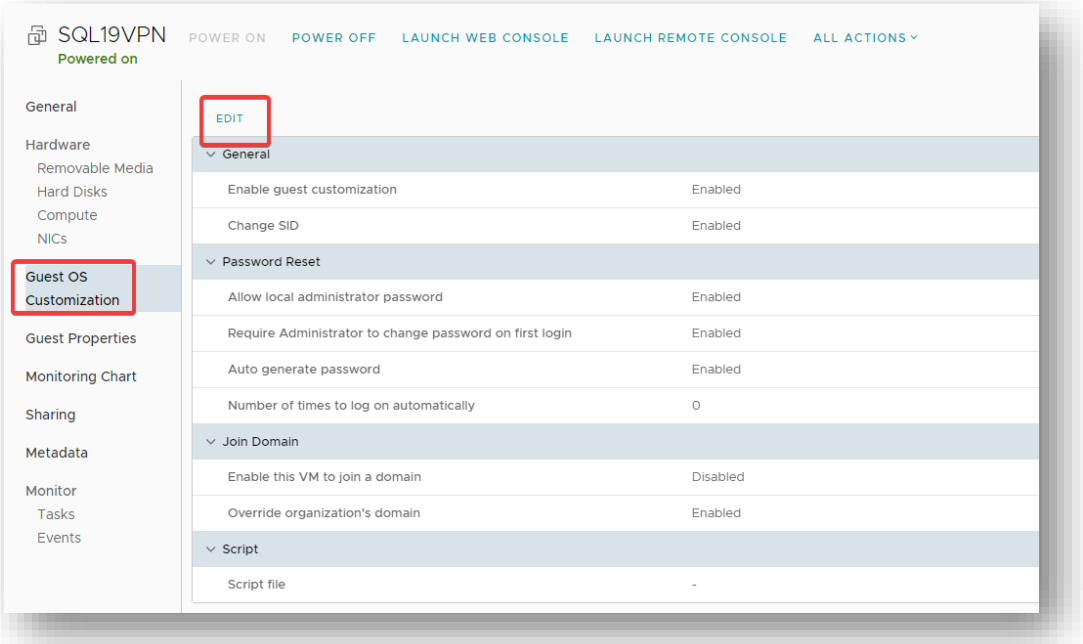
Note: In the event that the NIC at the Operating System level is not active, repeat step 1 and 2 by deselecting the "Connected" check and clicking "Save". Repeat step 1 and 2 but now enable the "Connected" check and click "Save"

Guest OS Customization

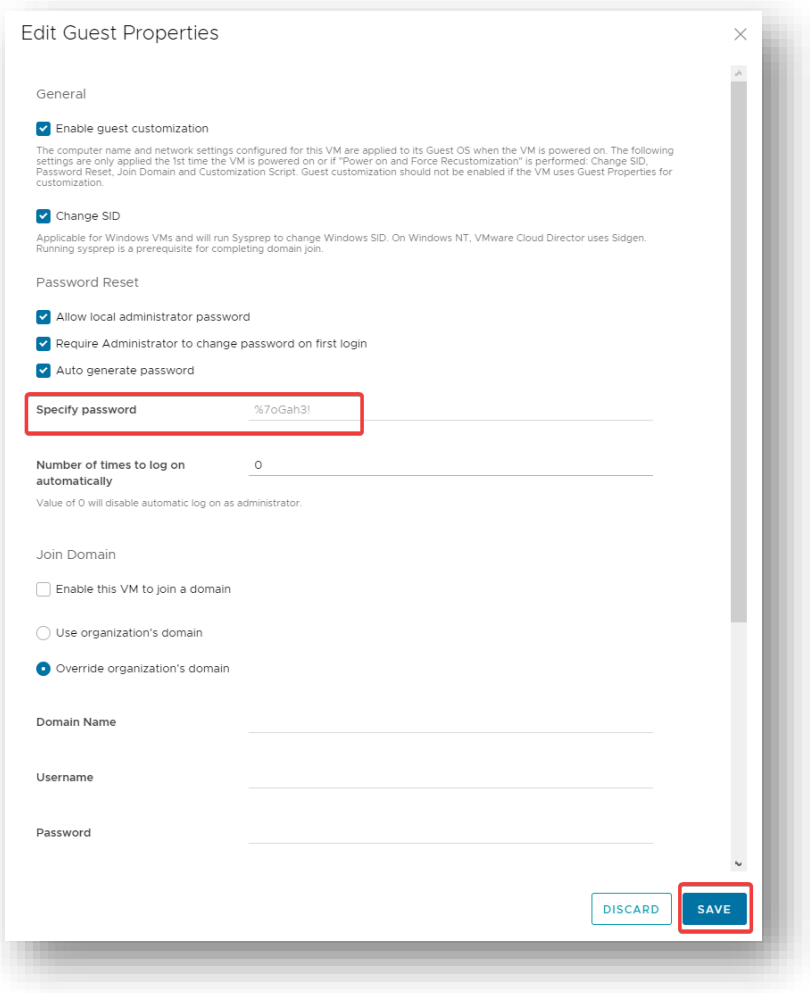
In this section you can configure basic operating system options, such as default generation of a password or forced assignment of a new password.

Reset the default password:

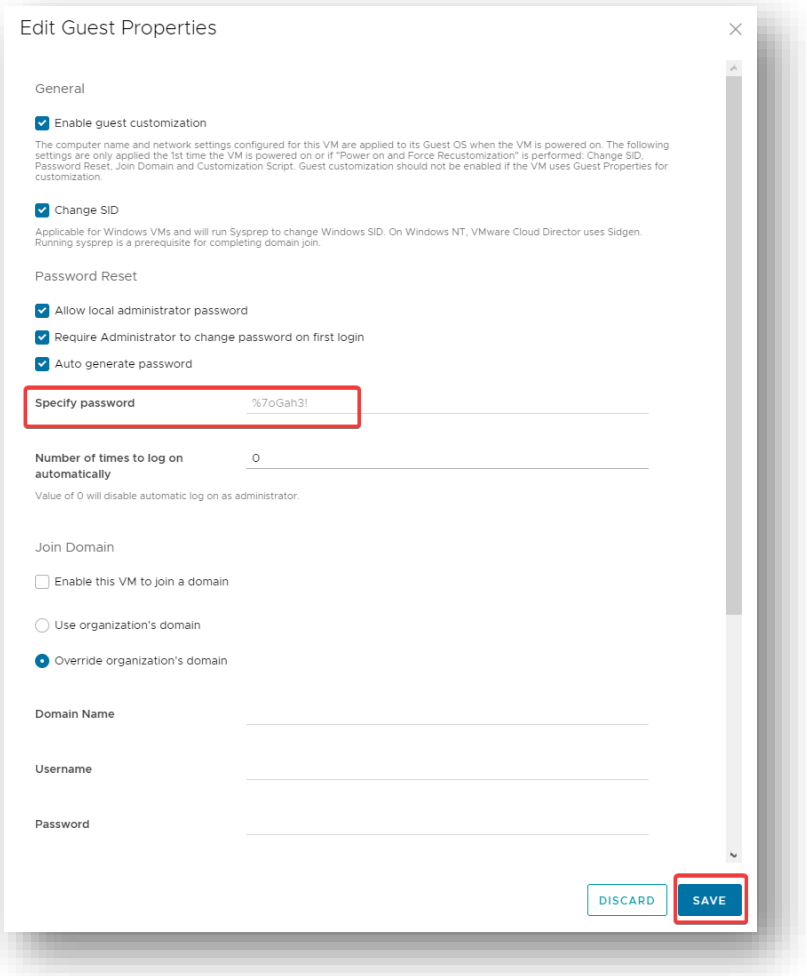
1. Within the control panel of a virtual machine, select the "Guest OS customization" option, click "Edit".



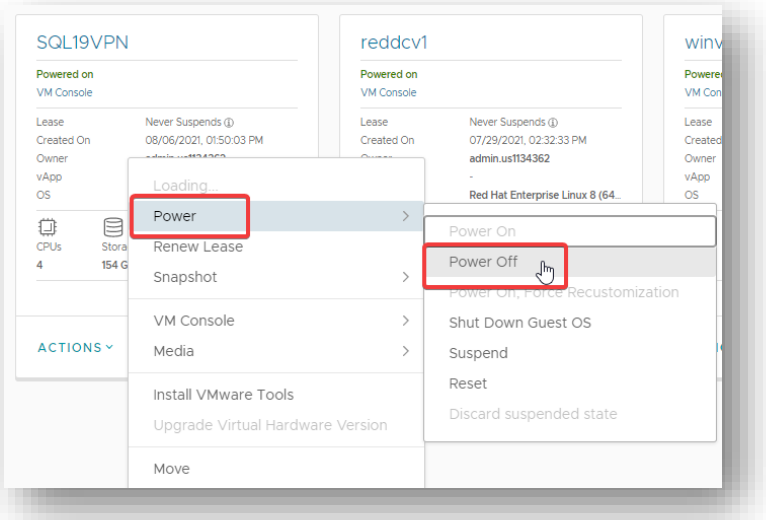
2. The next screen will open, disable the check "Generate password automatically" and click "Save"



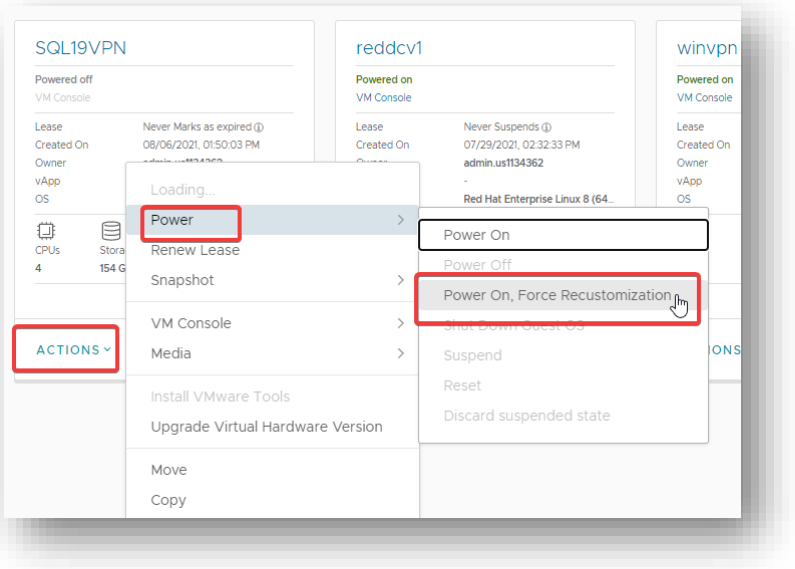
3. Edit the Guest OS Customization again, and enable the "Generate password automatically" check, click "Save".



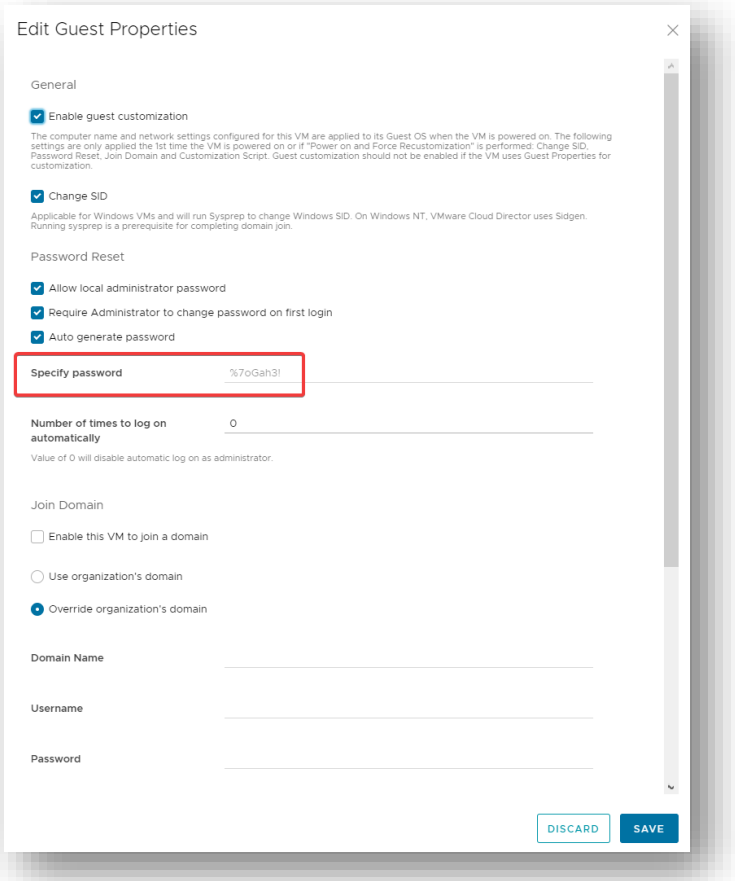
4. Shut down the virtual machine from the Power, Power Off option.



5. Power on the virtual machine with the Power on, Force Recustomization option.

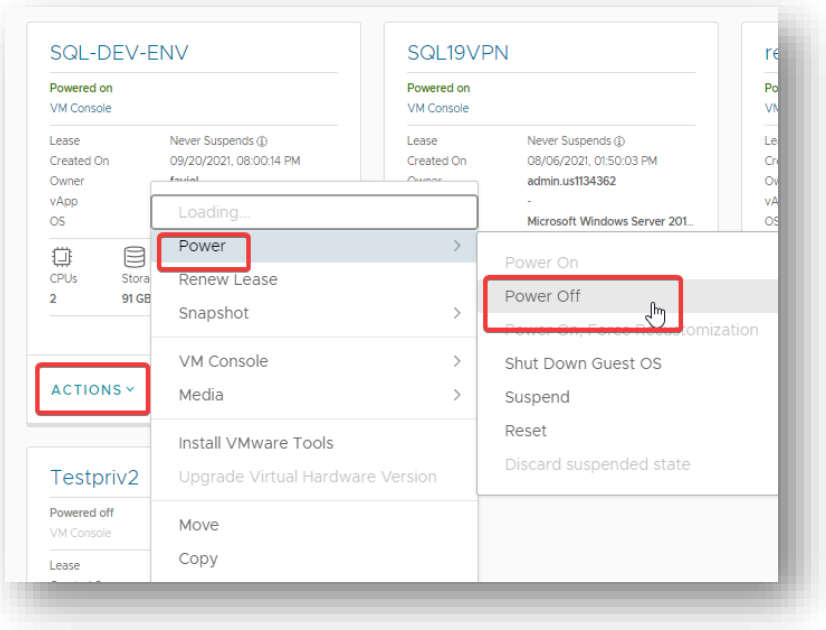


6. Within the control panel of a virtual machine, select again the option of "guest OS customization", click on "Edit", you will be able to display the new password of your virtual machine

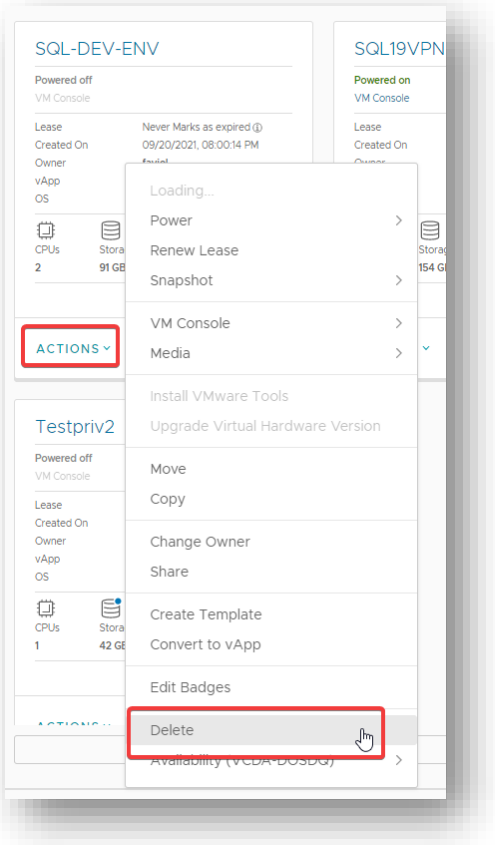


Delete a virtual machine

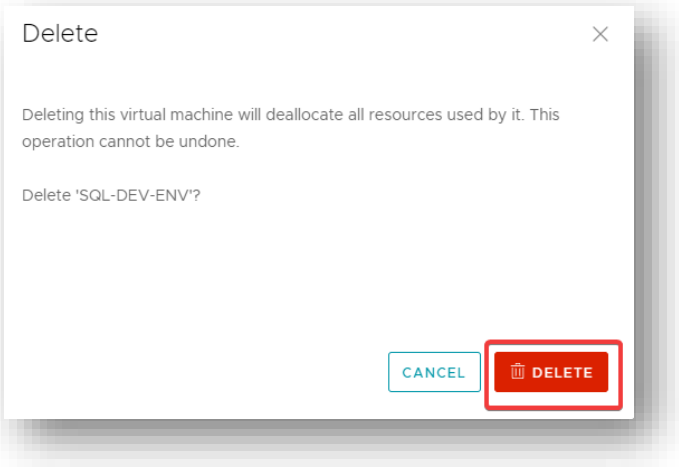
1. Shut down the virtual machine by clicking "Actions" / "Power" / "Power Off"



2. Once turned off, click "Actions" and then "Delete".



3. Confirm the action by clicking Delete to finish the process.

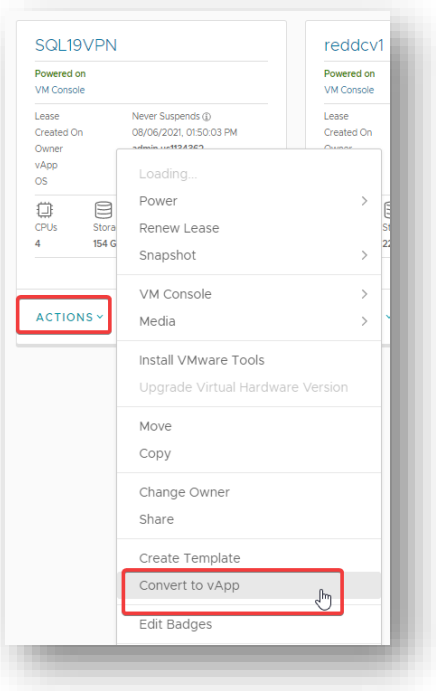


Important: If you try to delete a virtual machine that was connected to the network and has not been explicitly associated with a vApp, you may receive the following error message:

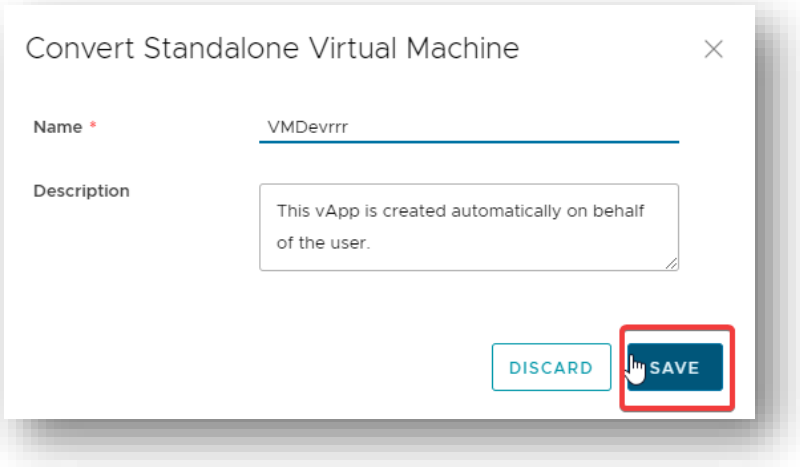
The requested operation could not be executed on vApp <VM Name>. Stop the vApp and try again.

Perform steps 4 through 9

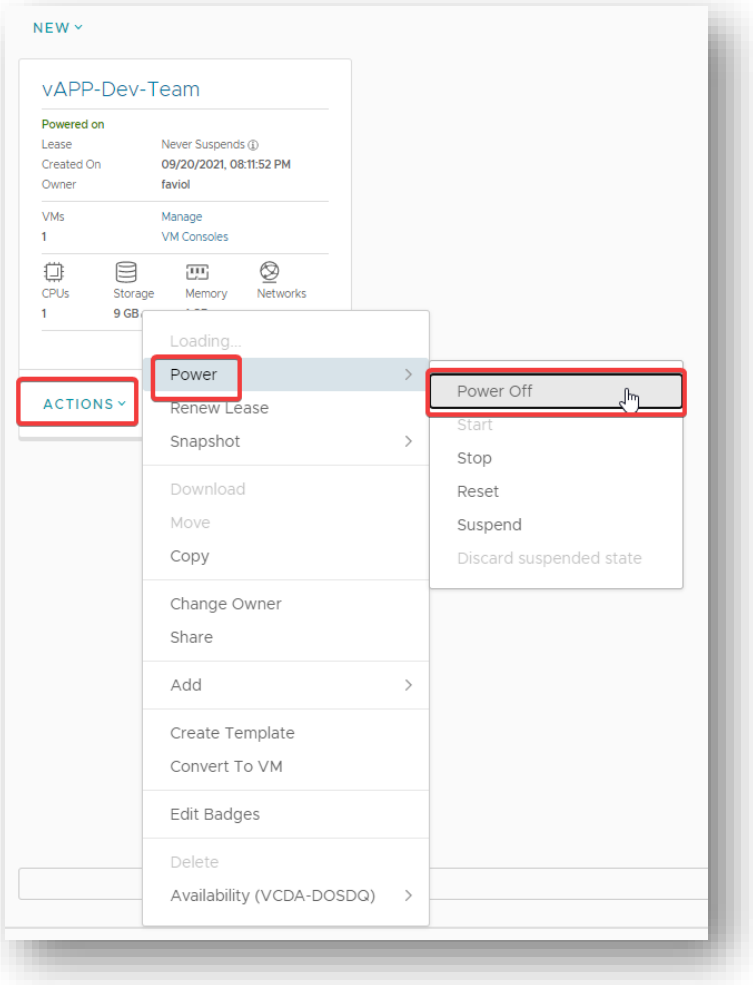
4. Select Actions on the virtual machine to delete and then the Convert to vApp option



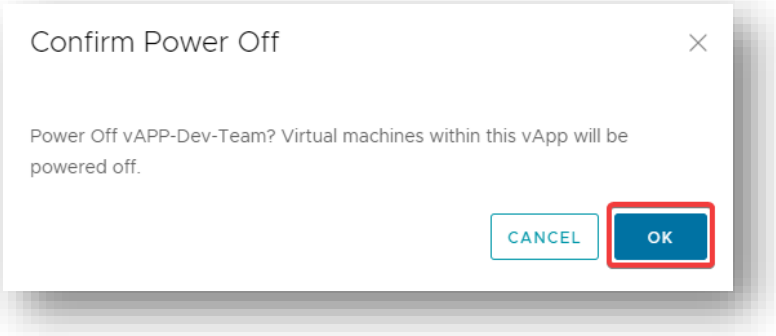
5. Assign a name to identify the vApp and press Save.



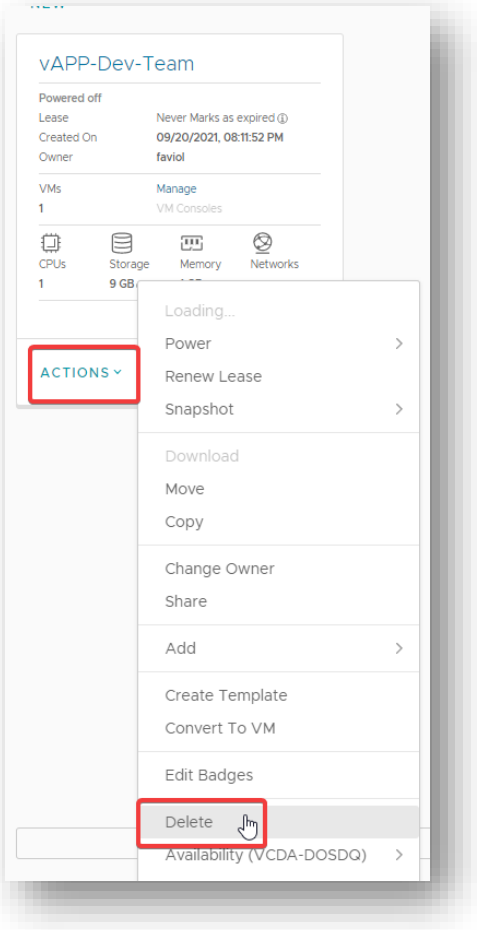
6. In the vApps section of your Data Center, you will find the newly created vApp. Select Actions for that vApp and then Power and Power Off.



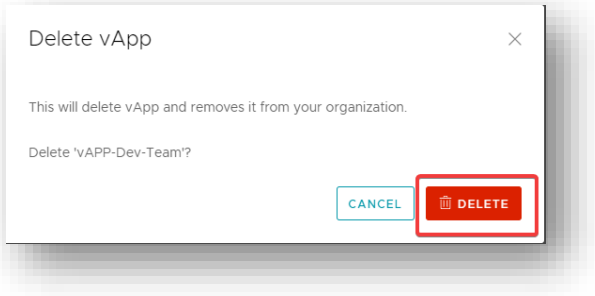
7. Press the OK button in the dialog box to confirm the action.



8. Select Actions again and then Delete.



9. Press Delete again in the dialog box to confirm the action and permanently remove the vApp and its associated virtual machine from your organization.



Copy a virtual machine to a different vApp

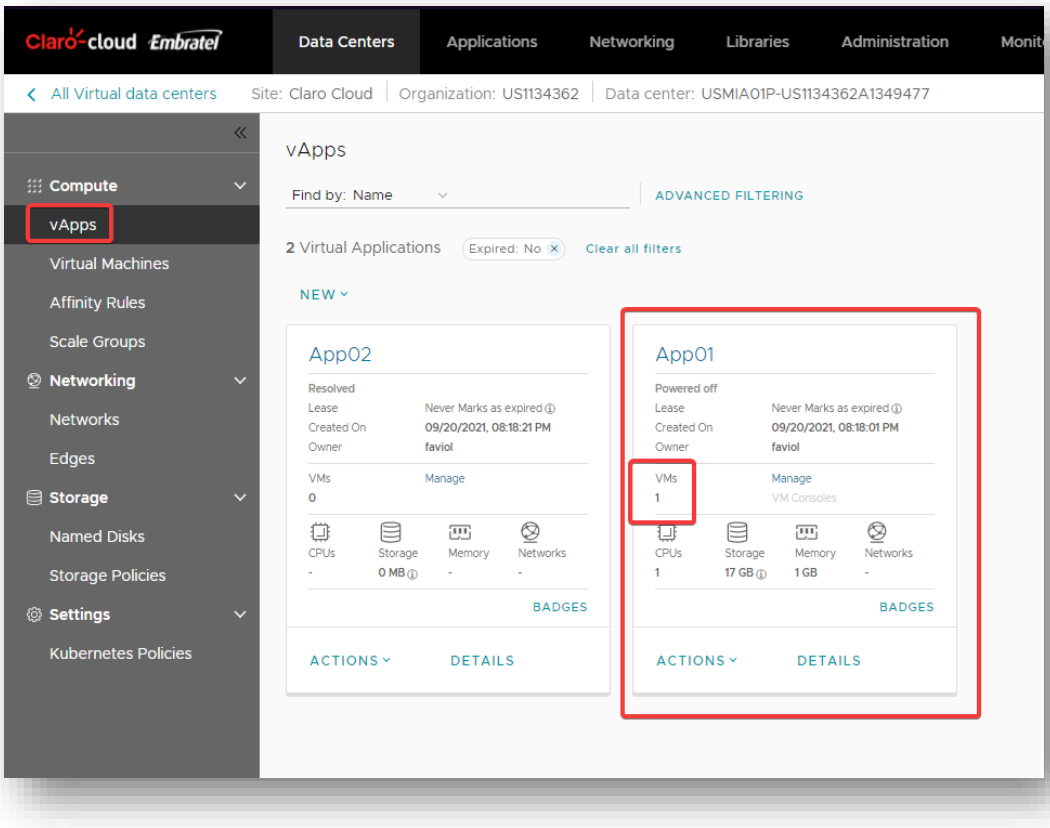
You can copy one virtual machine to another vApp.

When a virtual machine is copied:

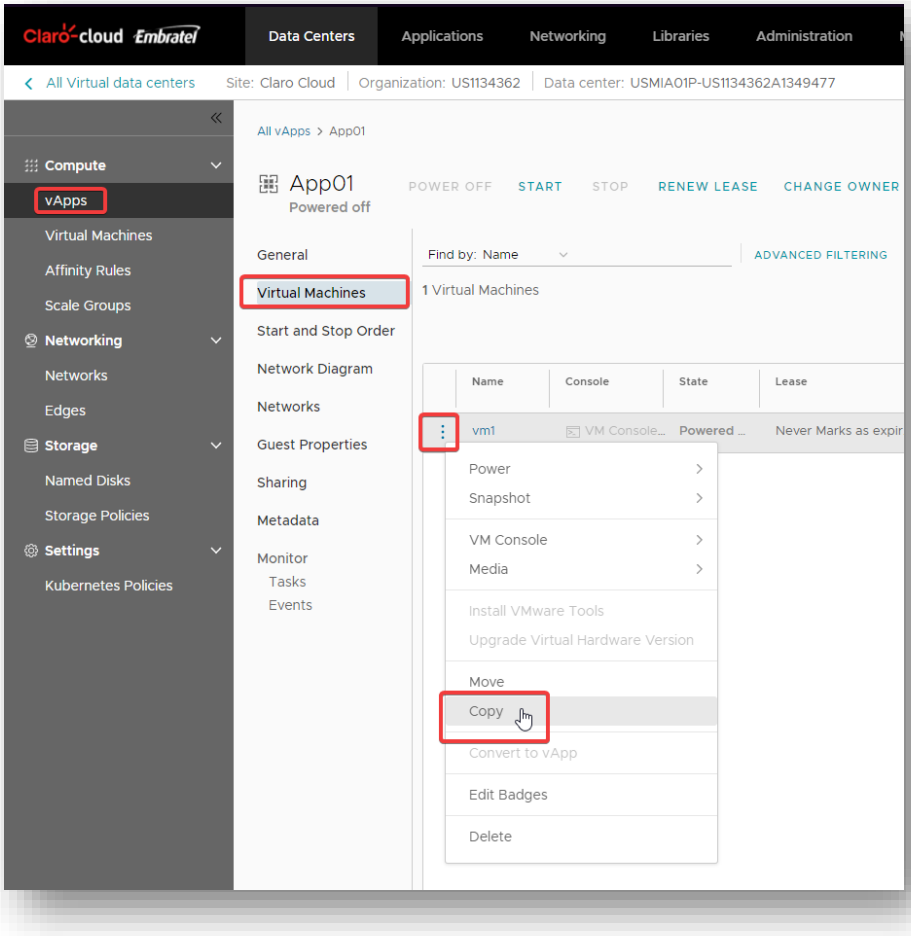
- The original virtual machine remains in the source vApp.
- Snapshots are not included.

Important: This operation can only be executed by the owner of the virtual machine or users with an "Organization Administrator" profile

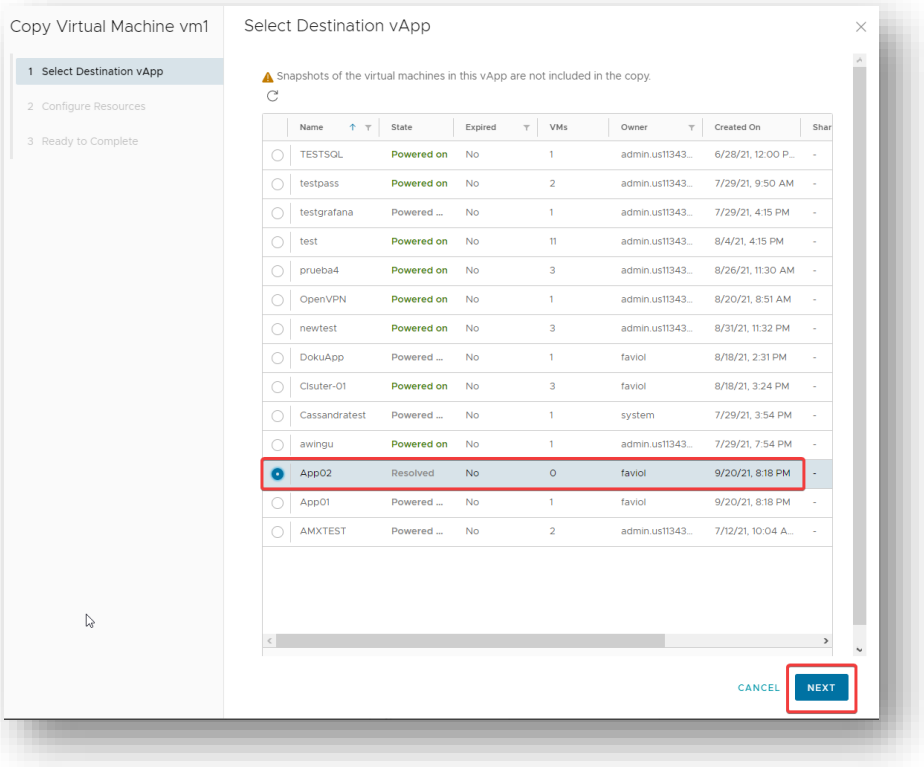
1. From the Datacenter menu, vApps, select the vApp where the virtual machine you want to copy is located.



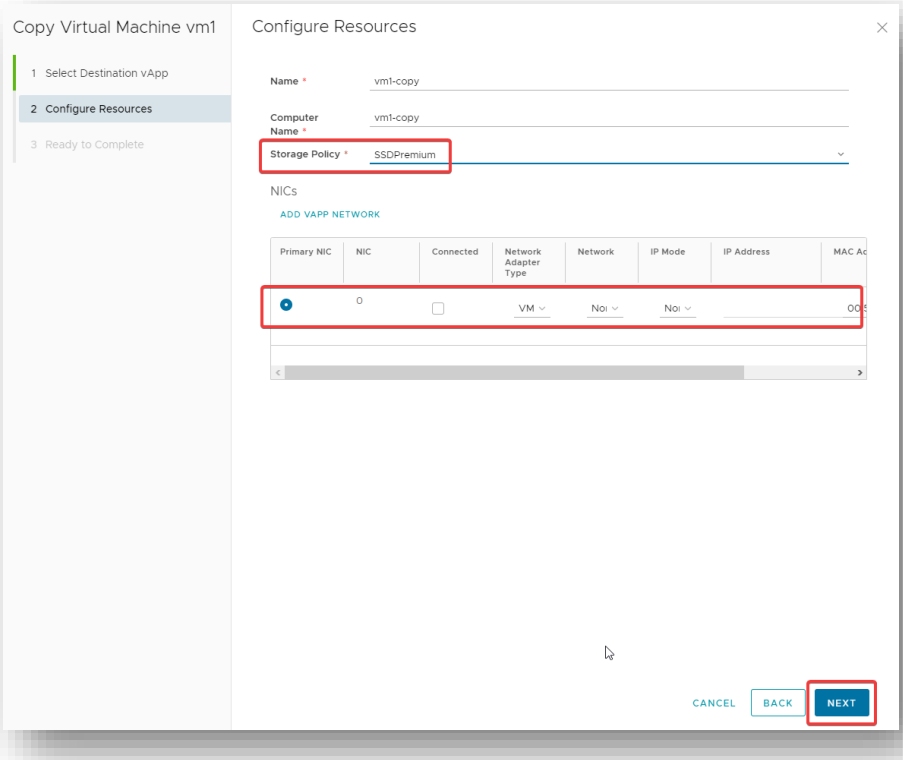
2. Click on the "Details" button and select the "Virtual Machines" option in the submenu. Click on the three-dot button of the machine you want to copy and click "copy".



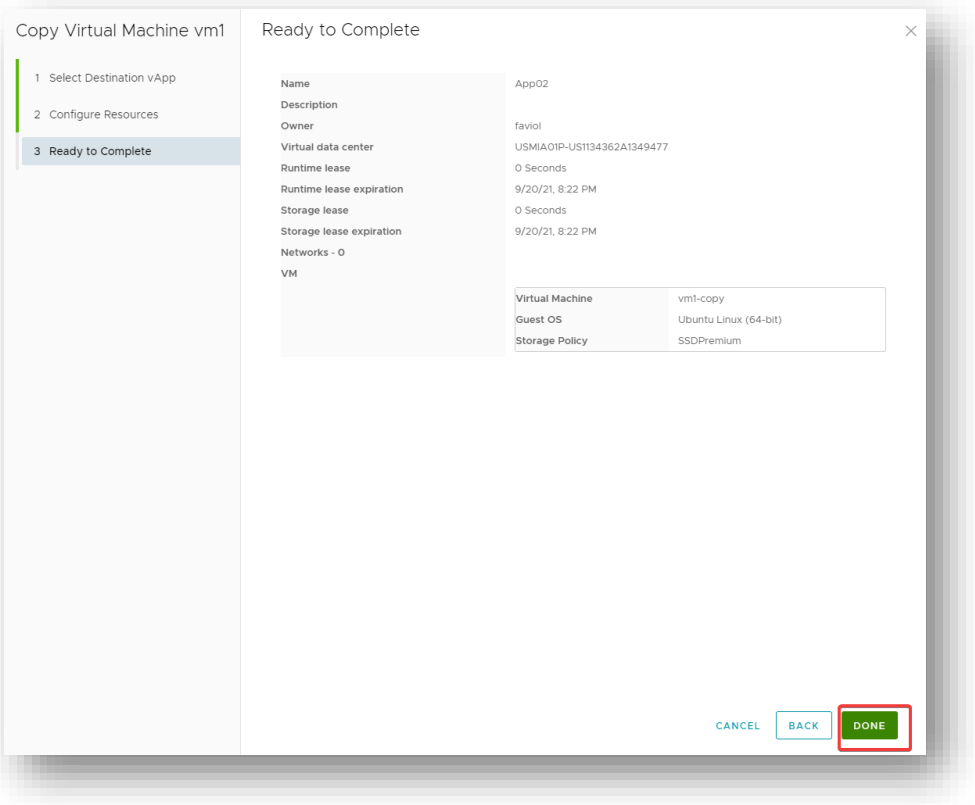
3. The next screen will open where you can select the target vApp, by clicking "Next"



4. Validate the preloaded parameters "Configure Resources" page, and if necessary adjust the parameters. Click "Next"



5. Check the summary of the operation, and press "Done" to finish the process.

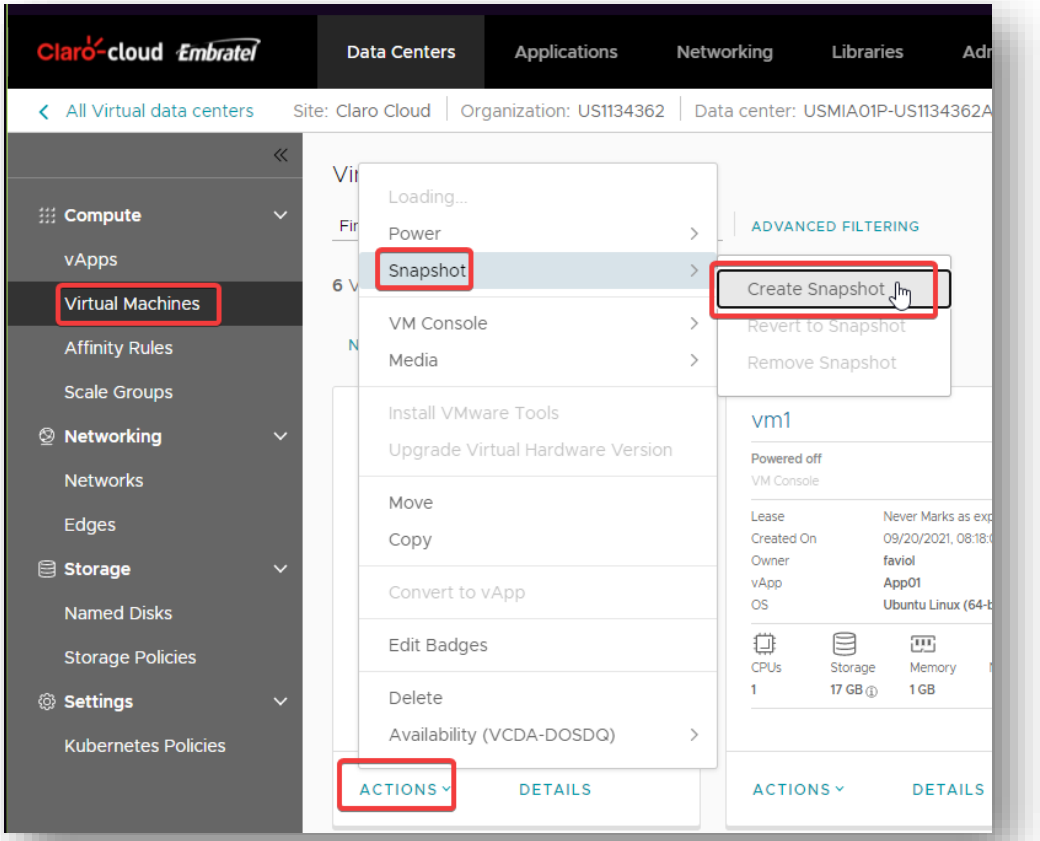


Configure Snapshots

It is possible to take a snapshot of a virtual machine to future return the virtual machine to a previous state. It is not a substitute for a backup.

> **Important:** Snapshots do not save NIC settings.

1. From the Datacenters menu, Virtual Machines, select the virtual machine from which you want to take a snapshot. Click on "Actions" / "Snapshot" / "Create Snapshot"

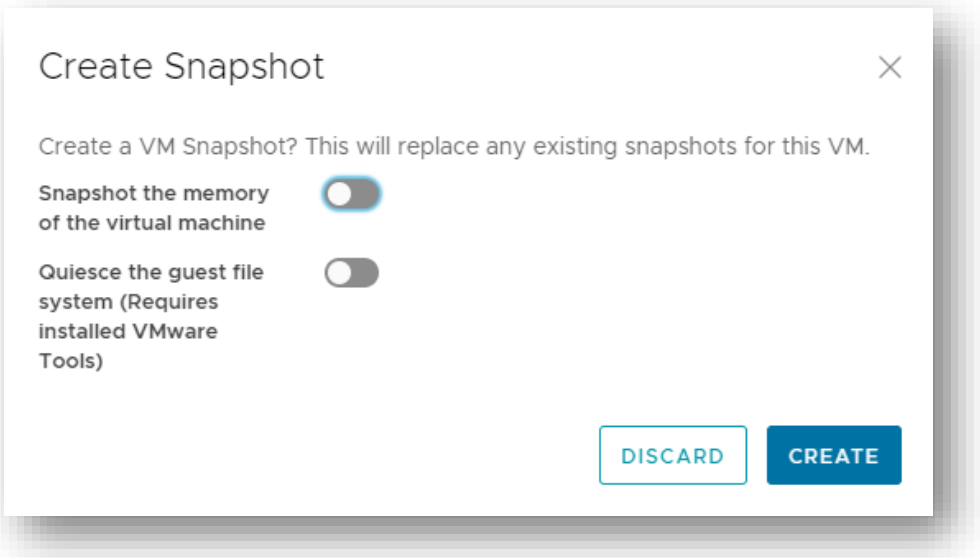


2. The following optional screen opens, with the following options

Item	Description
Take snapshot of virtual machine memory	When the virtual machine memory state is captured, the snapshot retains the active state of the virtual machine. Snapshots created with memory take a snapshot at a precise time, for example, to update software that is still in operation. If you create a snapshot of memory and the update does not finish as expected, or if the software does not meet your expectations, you can revert to the previous state of the virtual machine. When memory state is captured, you do not need to idle the virtual machine files. If the memory state is not captured, the snapshot does not save the active state of the virtual machine, and the disks are fault-consistent unless they are put into idle mode.
Put the guest file system into idle mode (requires VMware Tools be installed)	For this operation, VMware Tools must be installed on the virtual machine. When you put a virtual machine into idle mode, VMware Tools puts the virtual machine's file system into idle

	mode. An inactive mode operation ensures that the snapshot disk represents a consistent state of the guest file systems. Snapshots in idle mode are suitable for automated or periodic backups. For example, if the activity of the virtual machine is unknown, but you want to have several recent backups for rollbacking, you can put the files into idle mode. Virtual machines that have large capacity disks cannot be put into idle mode.

3. Click "Create" to finish.

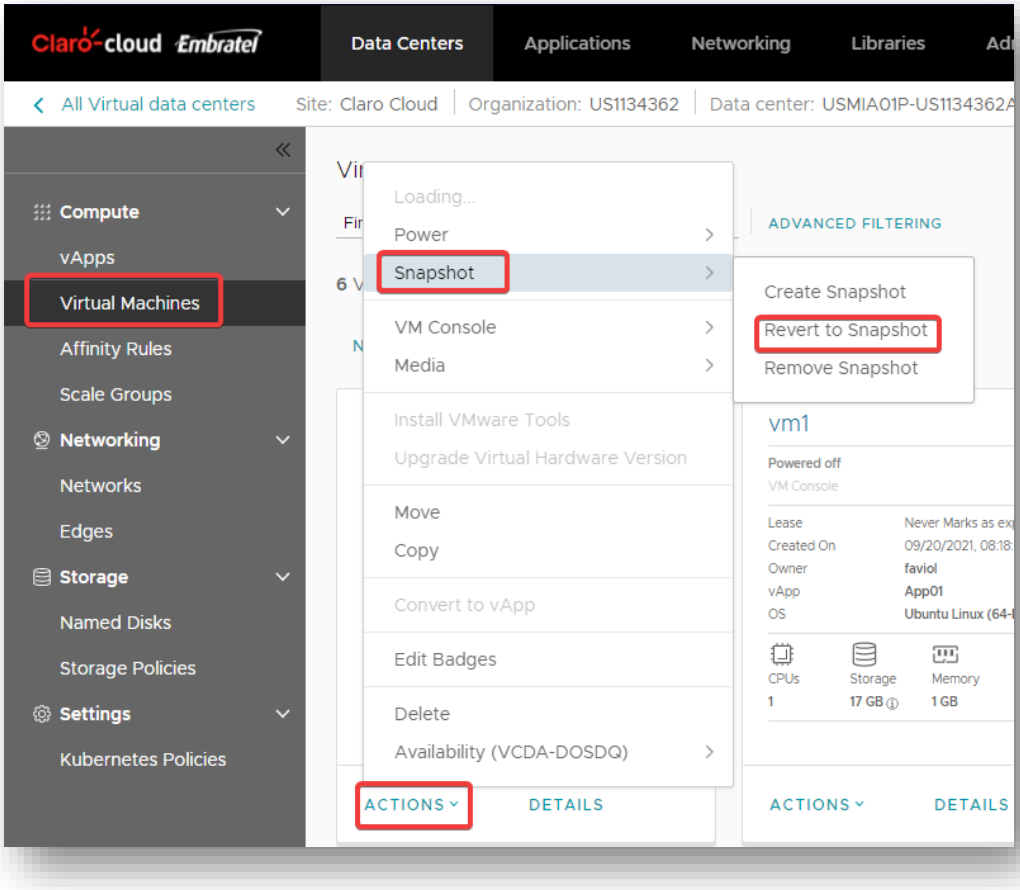


Important: Snapshots are not a Backup mechanism, therefore, it is not recommended to have Snapshots for more than 5 days on the platform, since this causes a growth in the delta disk and can overwhelm the capacity of the contracted storage.

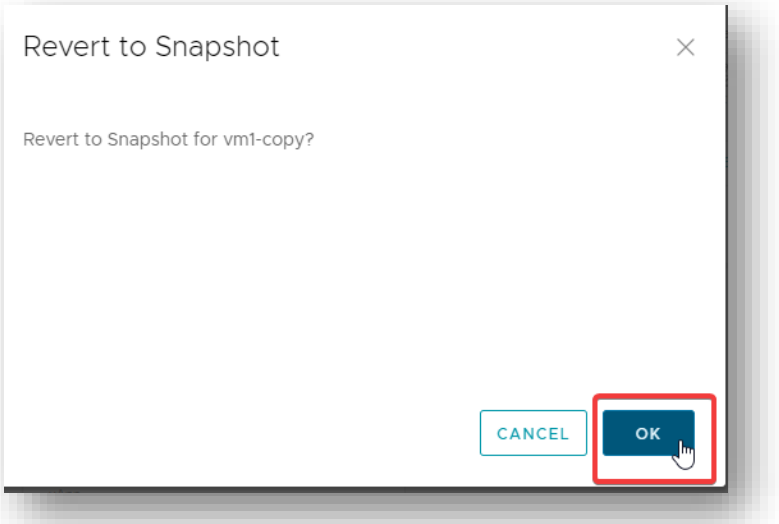
Additionally, the larger the snapshot size, the more the performance of the virtual machine will be negatively affected. Therefore, it is recommended that the snapshot be deleted once the activity for which it was taken has been performed.

Revert a virtual machine to a snapshot
You can restore a virtual machine to the state it was in when the snapshot was created.

1. In the main panel select Data Centers, Virtual Machines click on "Actions" / "Snapshot" / "Revert to Snapshot"



2. The following pop-up window will be displayed, click "OK".



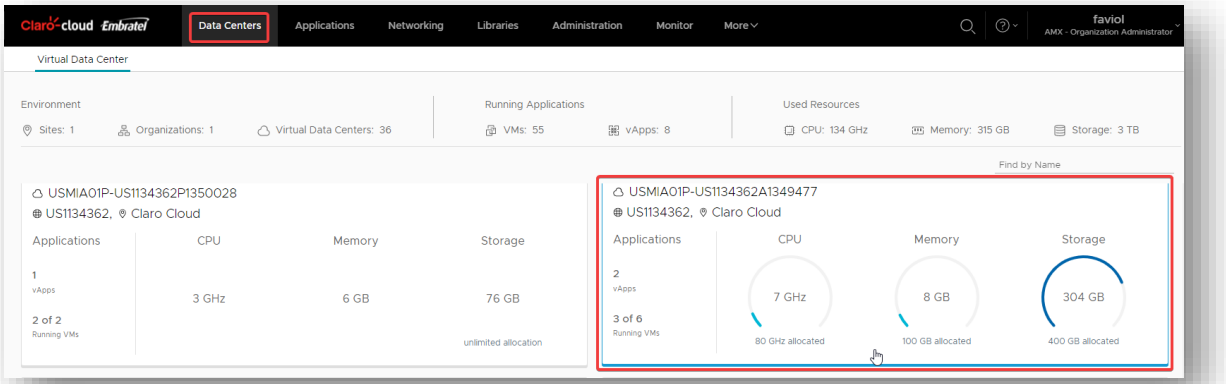
7. Working with vApps

Creating a vApp

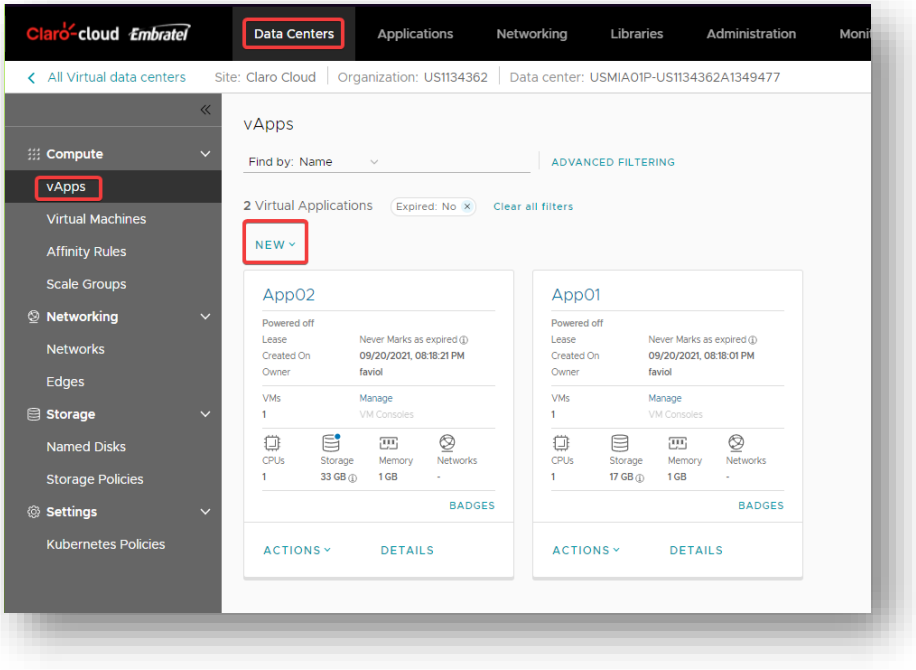
Enterprise Claro Cloud allows you to create a logical entity consisting of one or more virtual machines, which use the OVF/OVA format to specify and encapsulate all the components of a multilevel application, as well as the policies and service levels associated with it.

To create a vApp, follow these steps:

1. Select in the datacenter in which the VApp will be deployed.



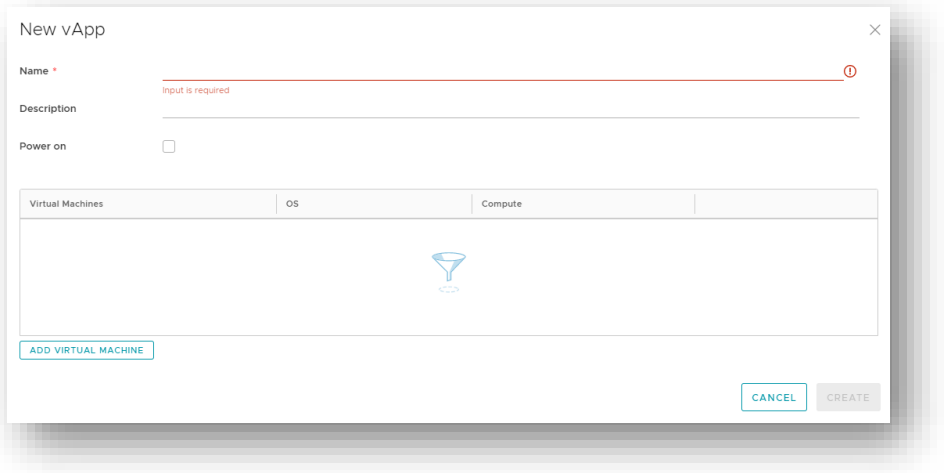
2. Select vApp from the left menu, then New.



3. You will be asked to enter the following data:

Item	Description

Name	The name by which the vApp will be identified in the VDC. (Required field).
Description	Field to assign a label which describes the vApp (Optional).
Power on	Button to select whether the VMs to be associated in the vApp are deployed powered on or not.
Add Virtual Machine	Button to start assigning VMs to the vApp.



4. Clicking on the "Add Virtual Machine" button will prompt you to enter the characteristics of the VMs that will be associated with the vApp. To do this follow the steps in the section Create a virtual machine from the public catalog

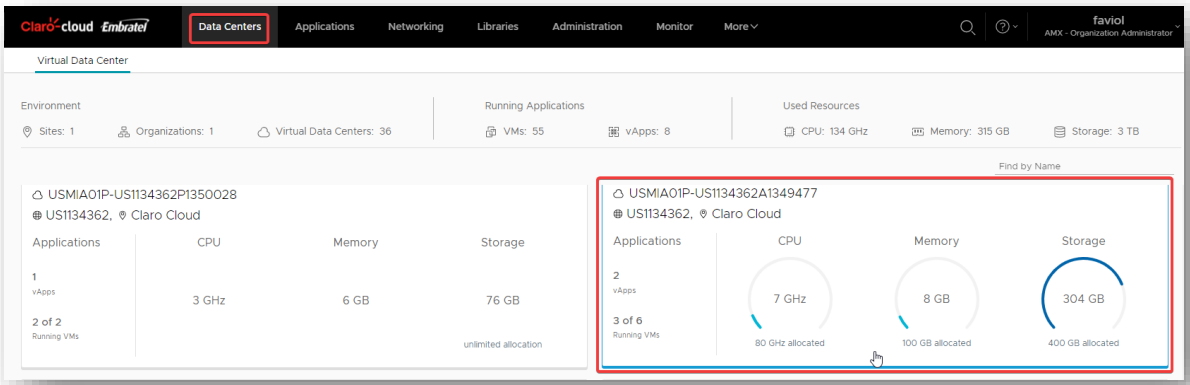
5. Once all the VMs to be deployed in the vApp are associated, the create button is enabled.

Create a vApp from an OVF/OVA package.

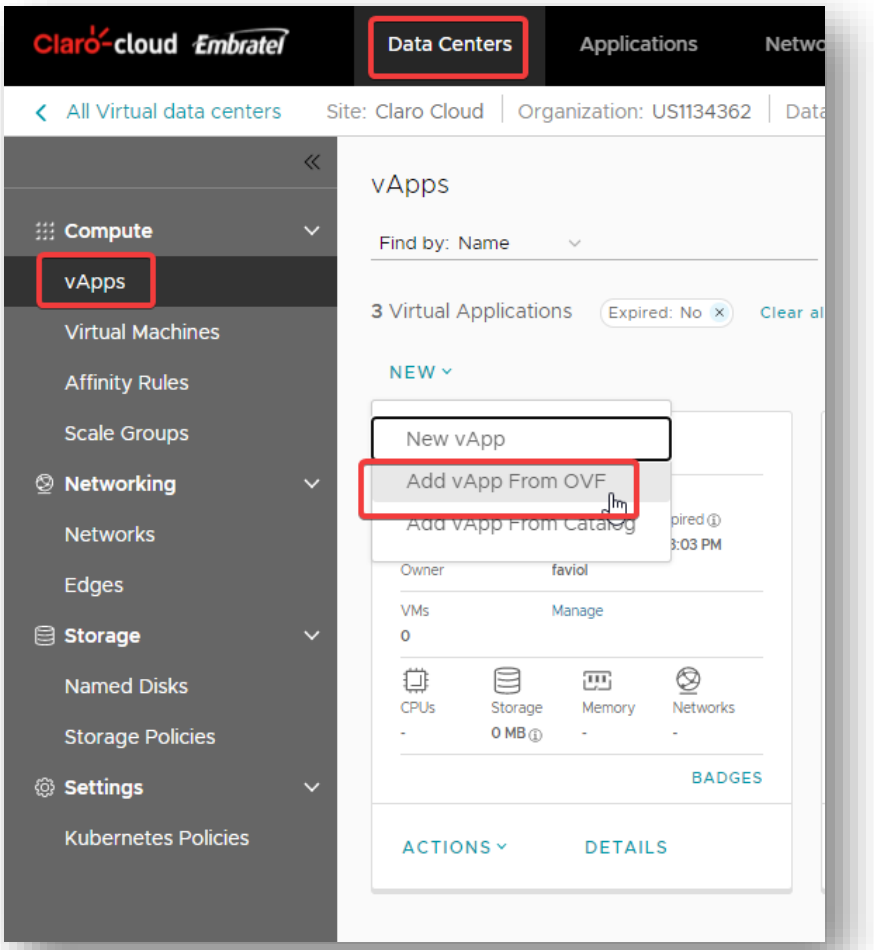
Enterprise Claro Cloud supports the Open Virtualization Format (OVF) and Open Virtualization Appliance (OVA) specifications. They can be uploaded to create vApp templates through a private catalog. If the uploaded OVF file includes OVF properties, those properties are preserved in the vApp template.

> **Note:** This operation can be executed by users under the role organization administrator

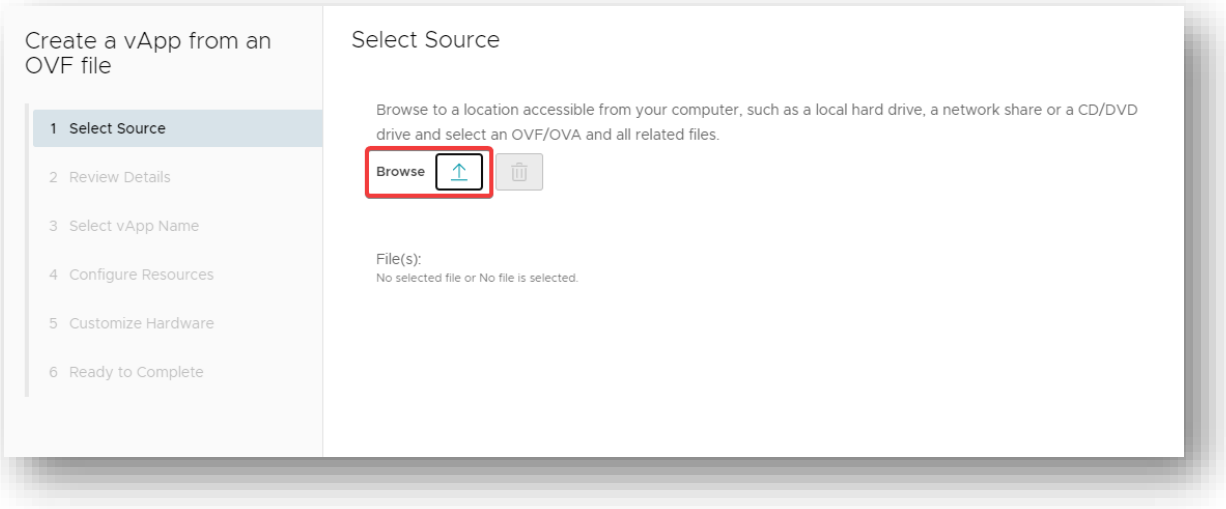
1. Select in the datacenter in which the VApp will be deployed.



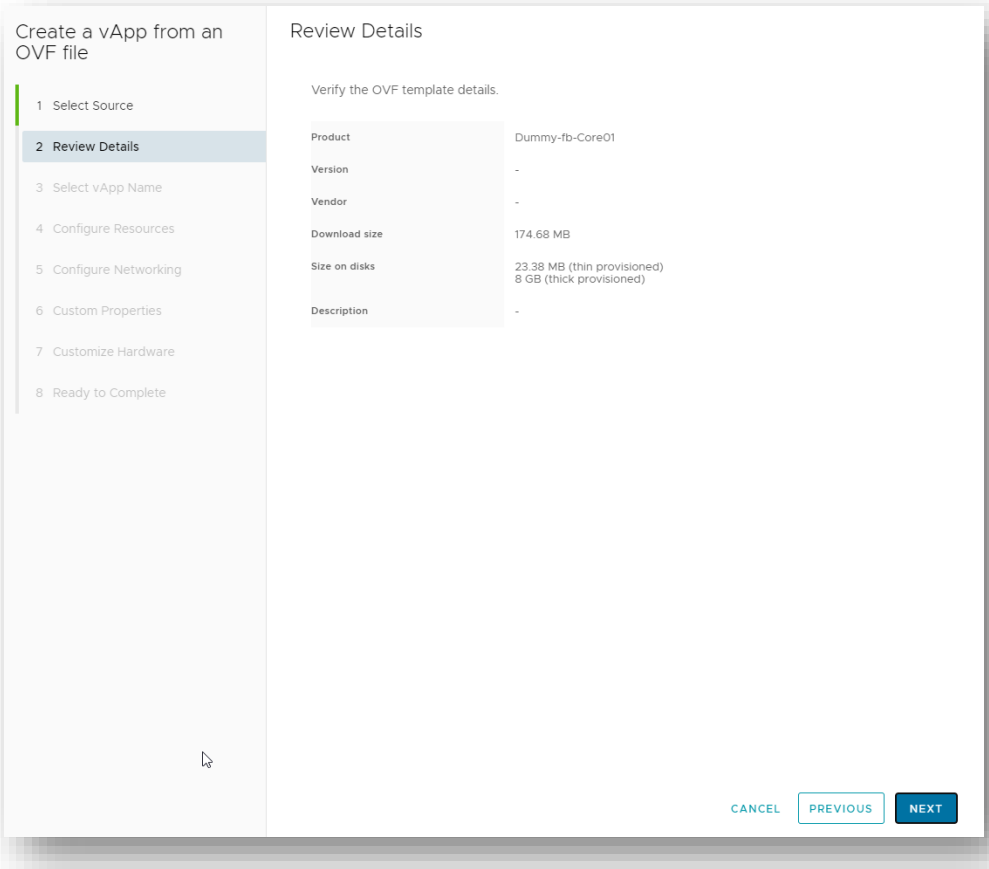
2. Select in the left menu vApp, then Add vApp.



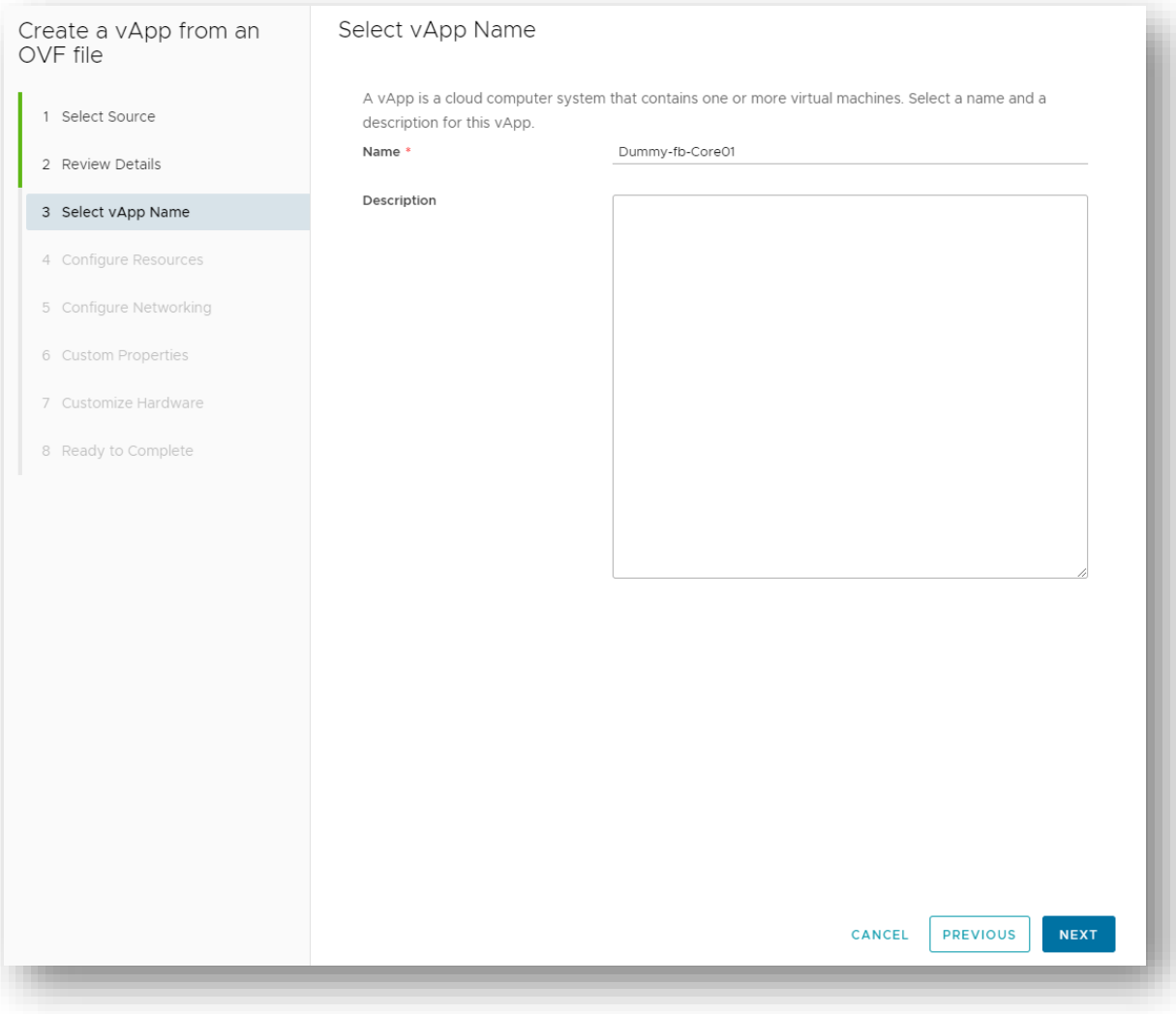
3. The following screen will open, click "Browse" to search for the file on your computer, click "Next".



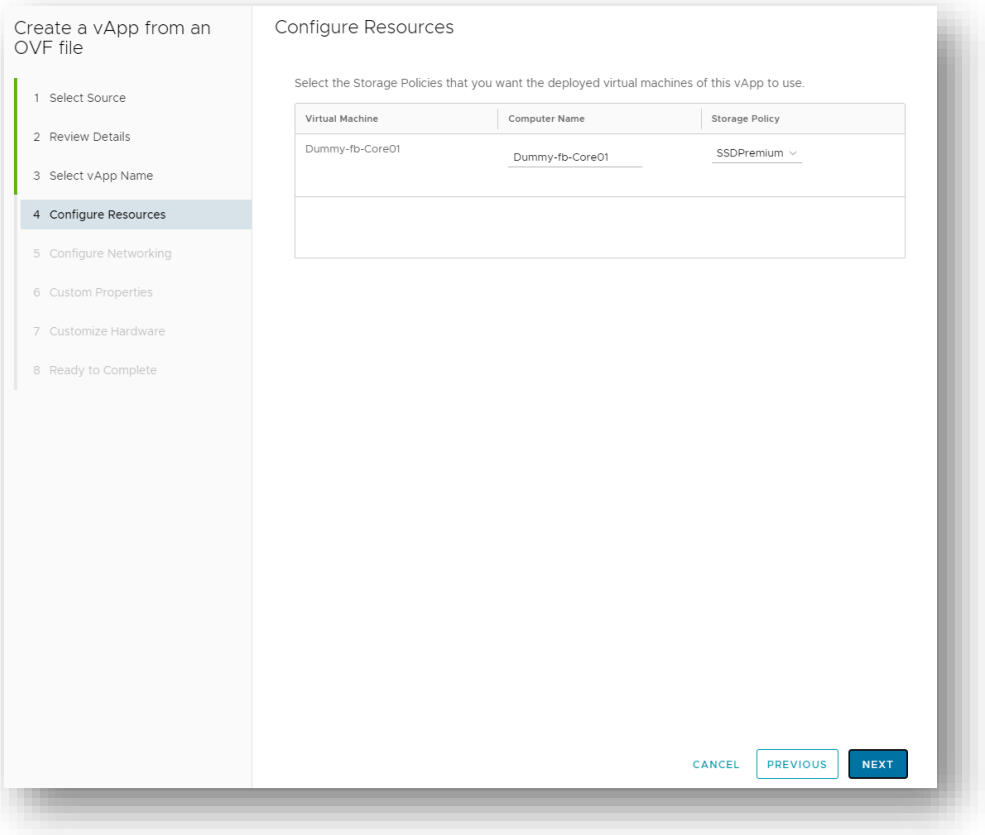
4. The step of reviewing details is enabled, in this option it indicates the size of the OVF / OVA that will be used to deploy the VM, as well as the size of the disks, click on "Next".



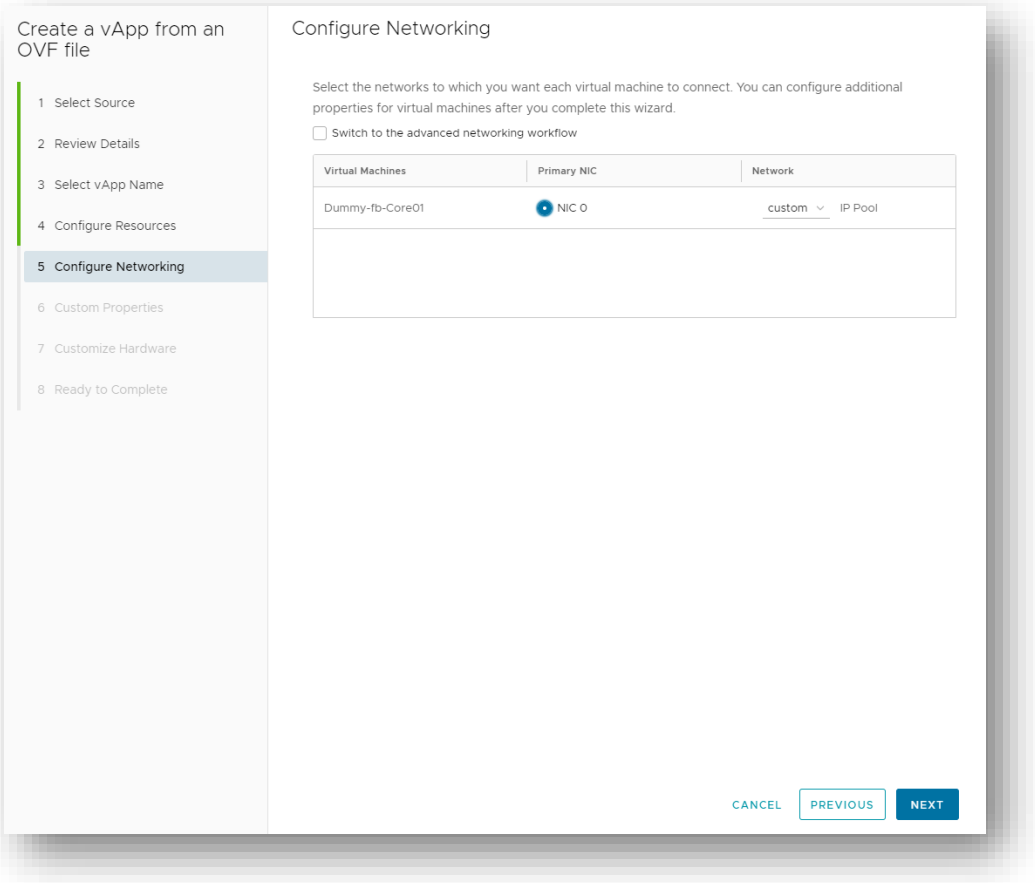
5. Select the name of the vApp and its description, click "Next".



6. Configure the resources, in this step the assignment of the storage policy to be used by the VM is made, click on "Next".



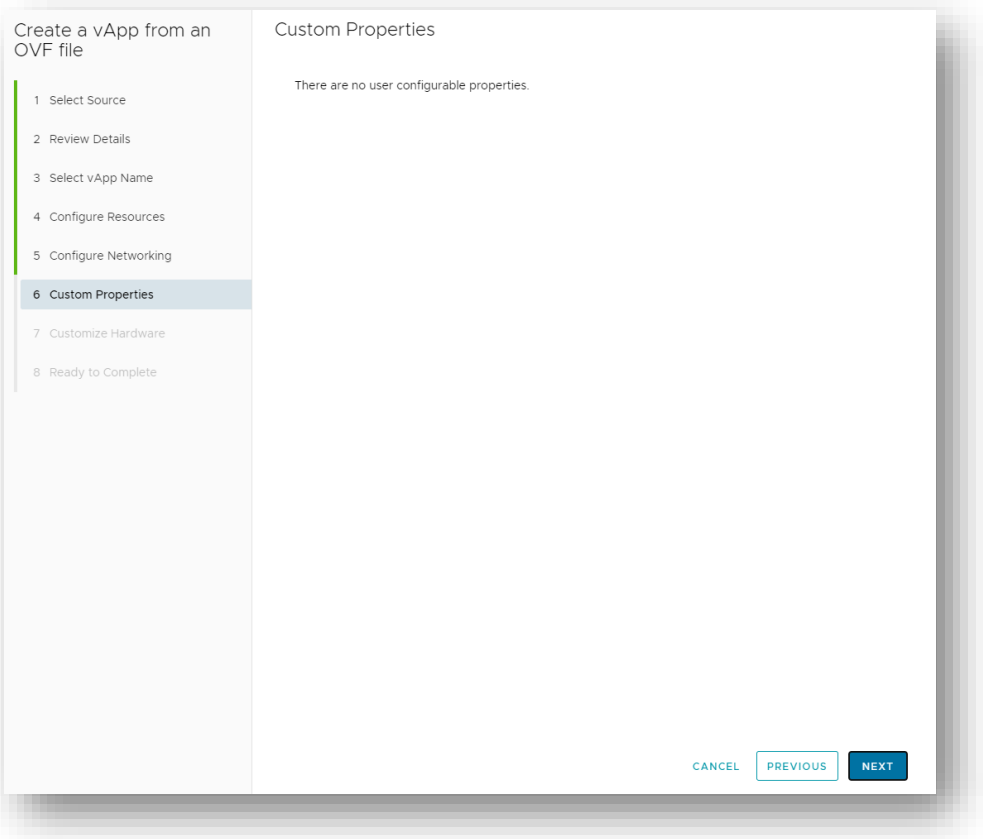
7. Configure the networks to be used in the vApp, click next.



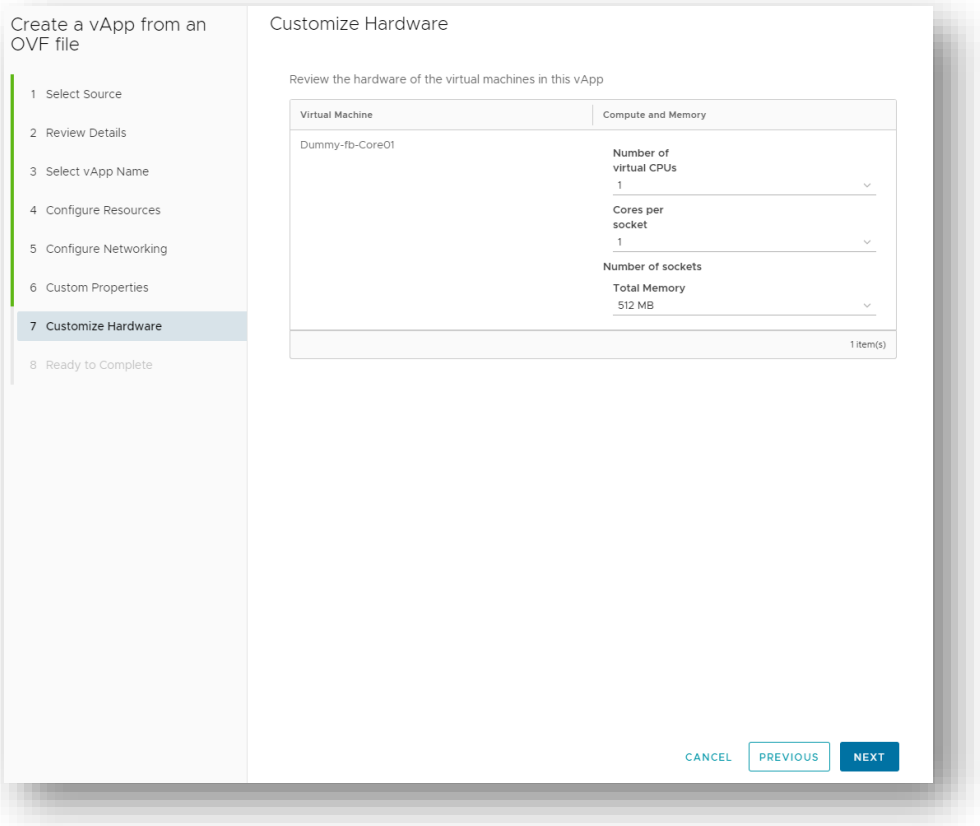
Note: On this screen you can enable the option "Switch to Advanced Networking Workflow" which allows you to select the type of network adapter, network, IP mapping.

If your application requires downloading packages from external repositories, make sure that the network to be mapped in the NIC is of type Routed with Internet access, validate the chapter [Configuring a network in Enterprise Claro Cloud]

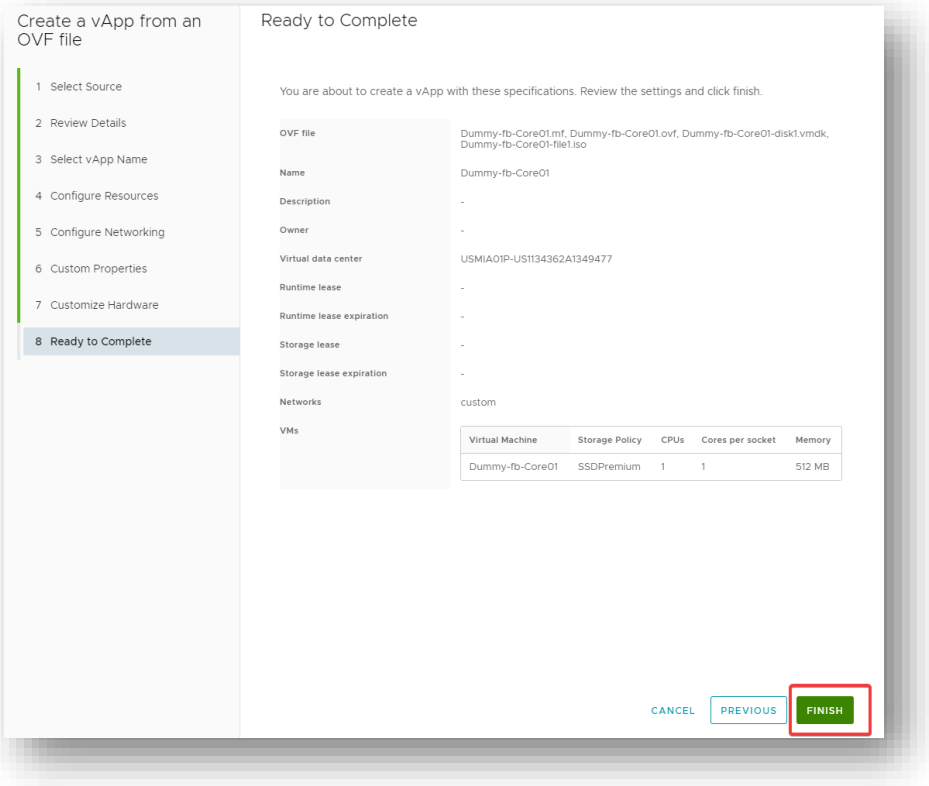
8. Custom property settings, apply if your .OVA /.OVF file requires additional configurations. If not required, click next.



9. Customize hardware, select the compute characteristics for the VM, at the level of vCPU, number of sockets, RAM, click "Next".

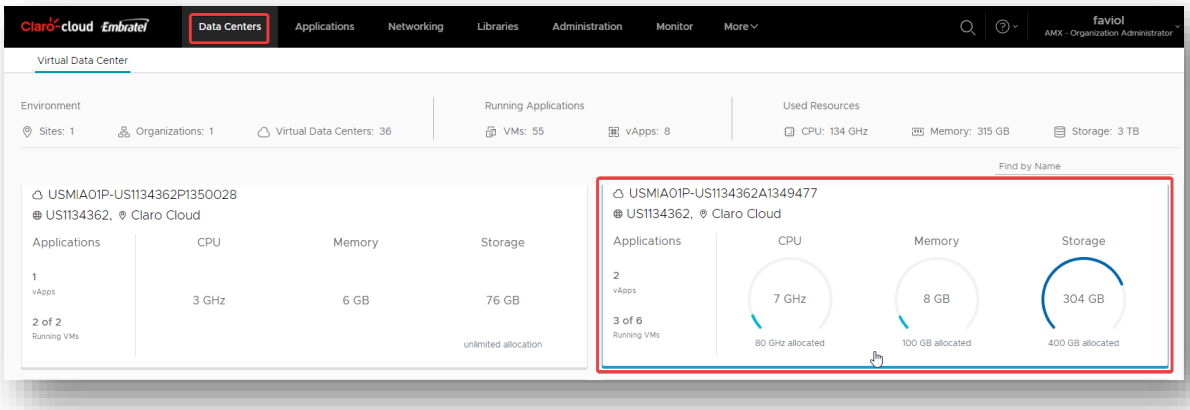


10. Summary of your configuration will be displayed, click "Finish".

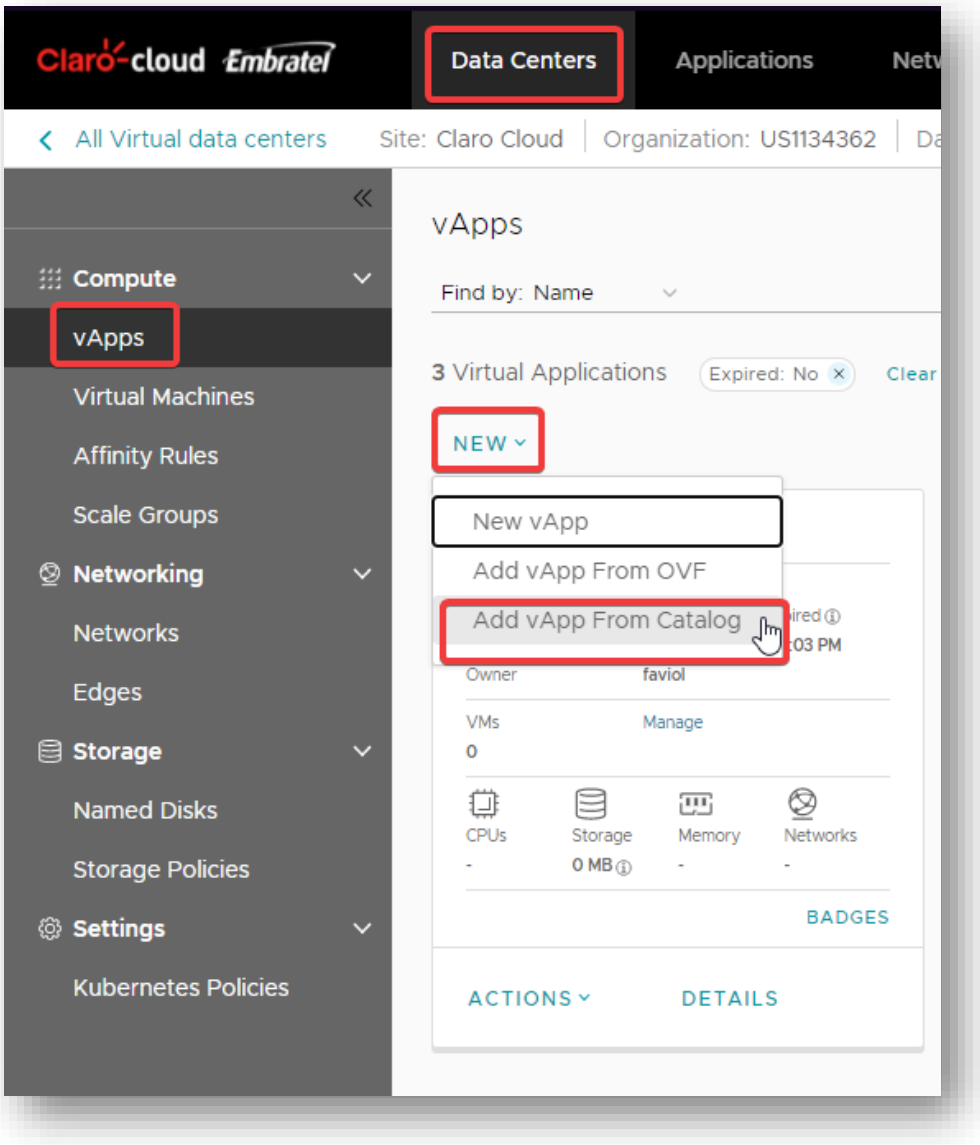


Create a vApp from Catalog

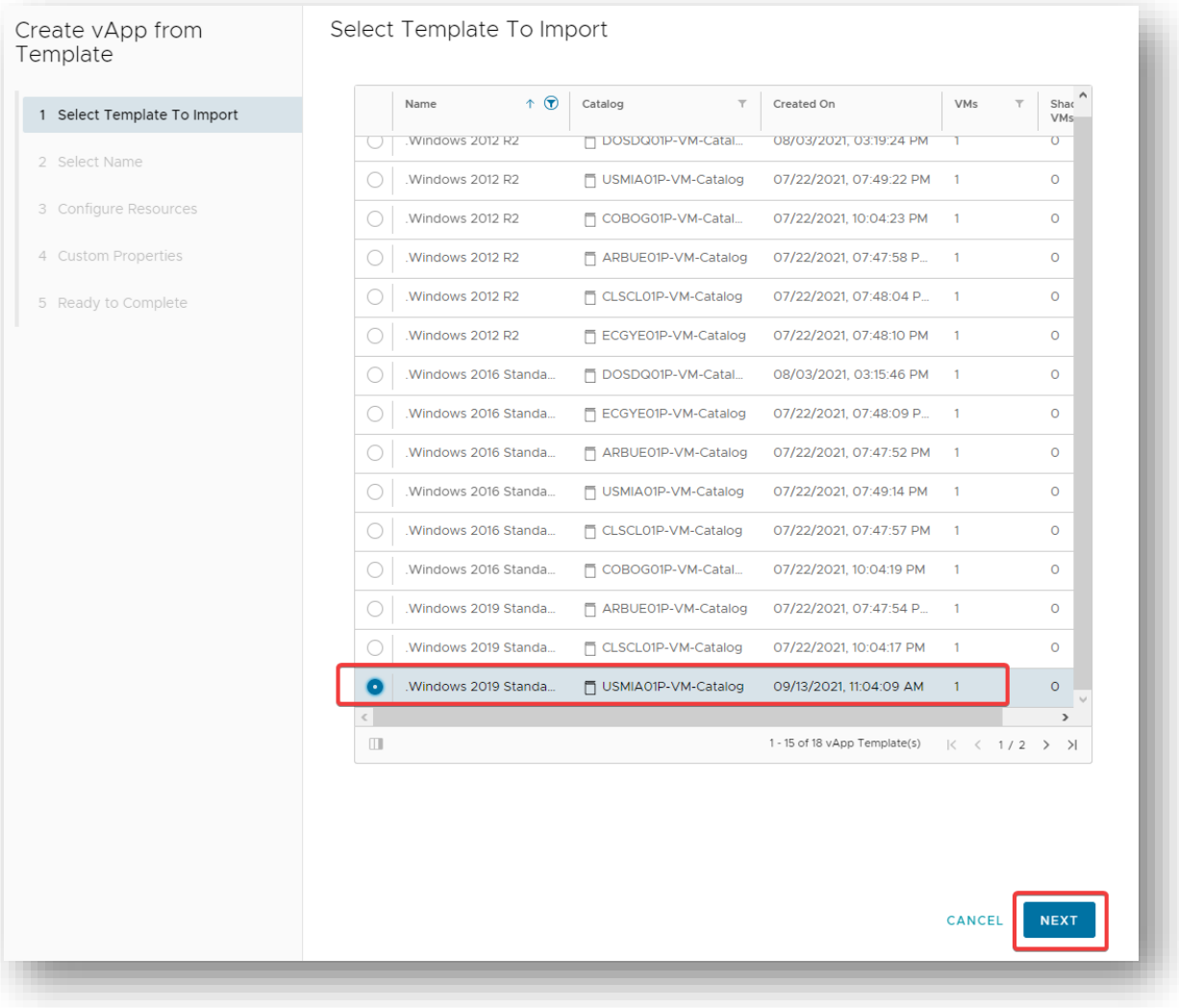
1. Select in the datacenter in which the VApp will be deployed.



2. Select vApp from the left menu, then new vApp.

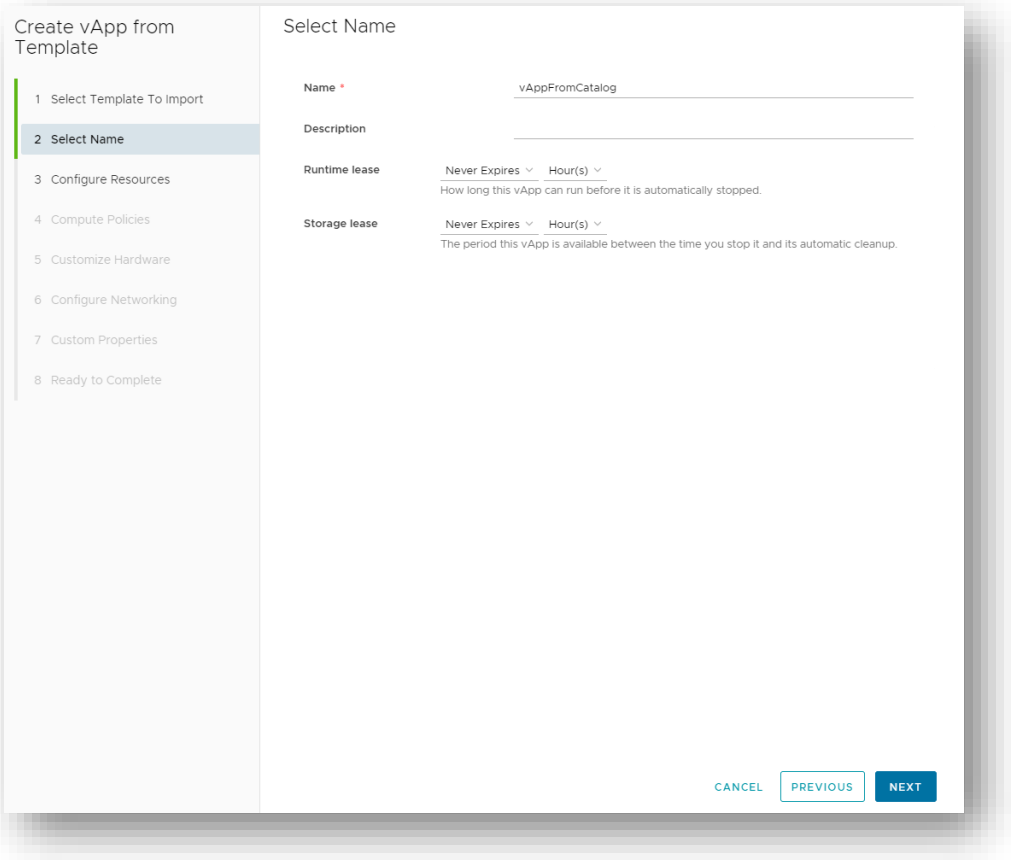


3. The next screen will open, select the template with which the virtual machines will be created within the vAPP, click on "Next".

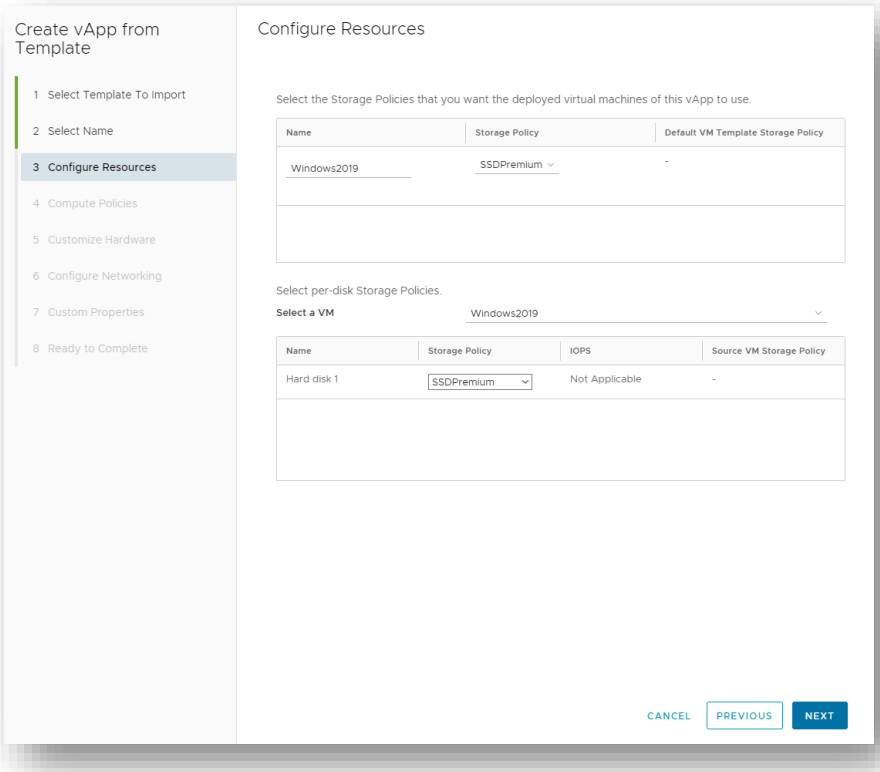


4. Enter the requested parameters, click next.

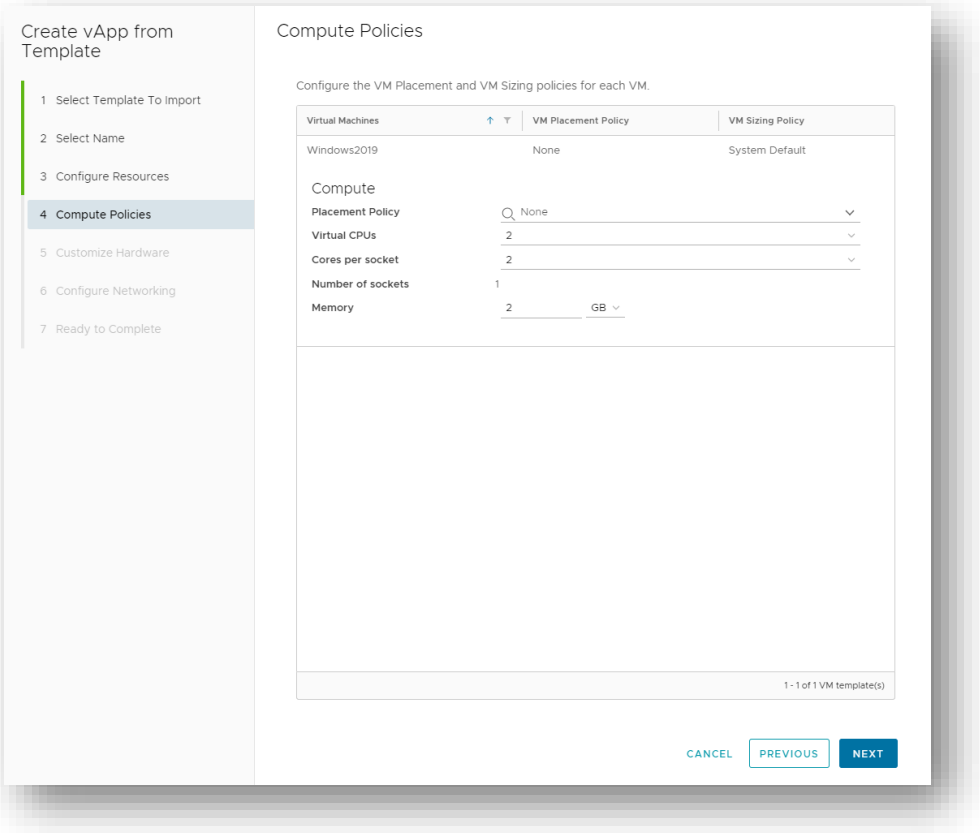
Item	Description
Name	The name by which the vApp will be identified in the VDC. (Required field).
Description	Field to assign a label which describes the vApp (Optional).
Runtime lease	How long the vApp can run before it stops automatically.
Storage lease	The period in which this vApp is available between the time it stops and the time when the automatic cleanup occurs.



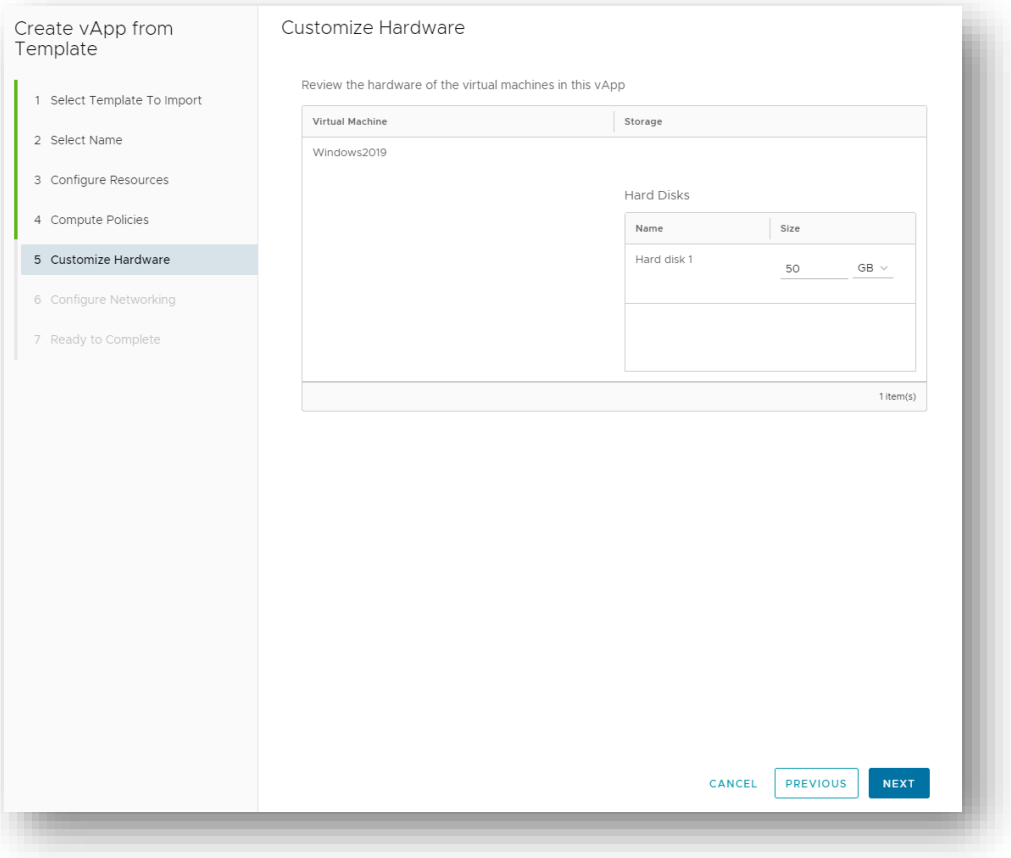
5. In storage policies select "Premium SSD" which will be used by the virtual machine, then click "Next".



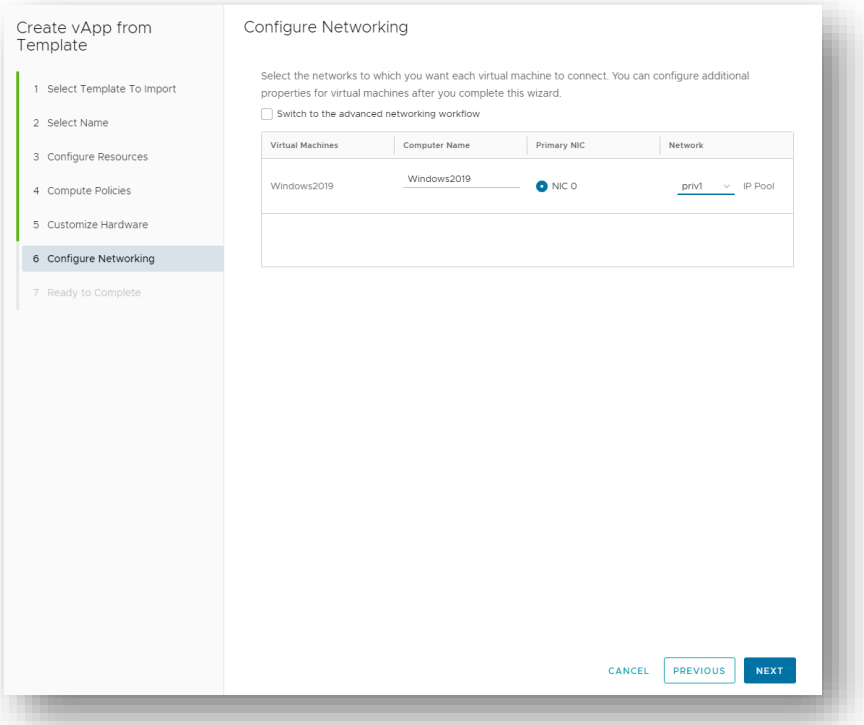
6. Then select the vCPU capacity and RAM with which the virtual machines will be created within the vApp. When finished, click "Next".



7. Select the storage capacity with which the virtual machines will be created within the vApp, then click "Next".

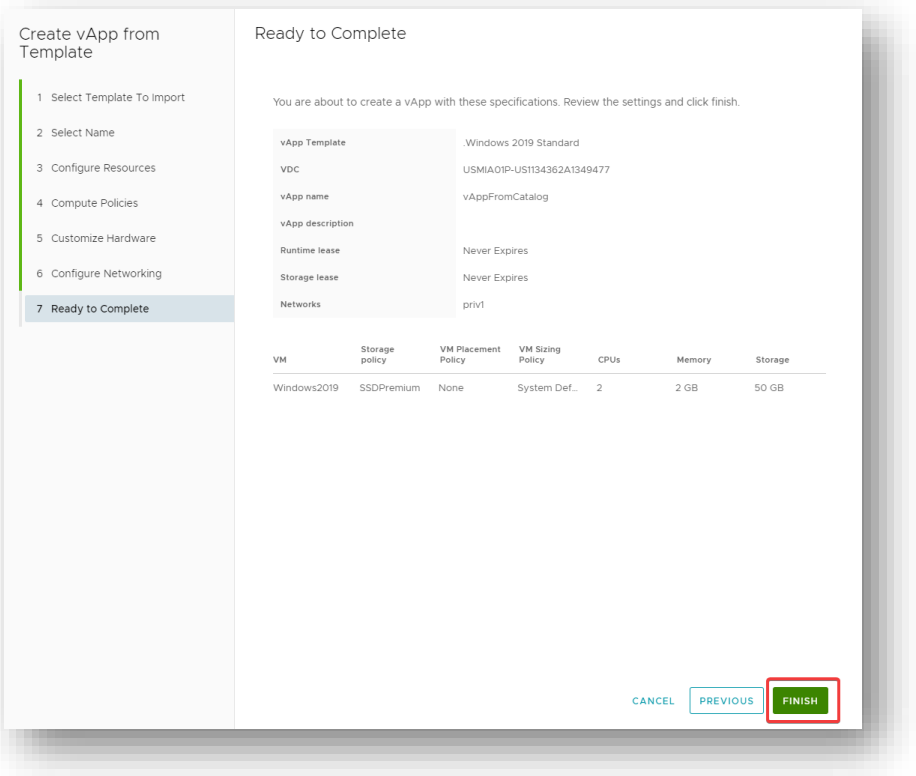


8. Configure the networks to be used in the vApp, click on "Next".



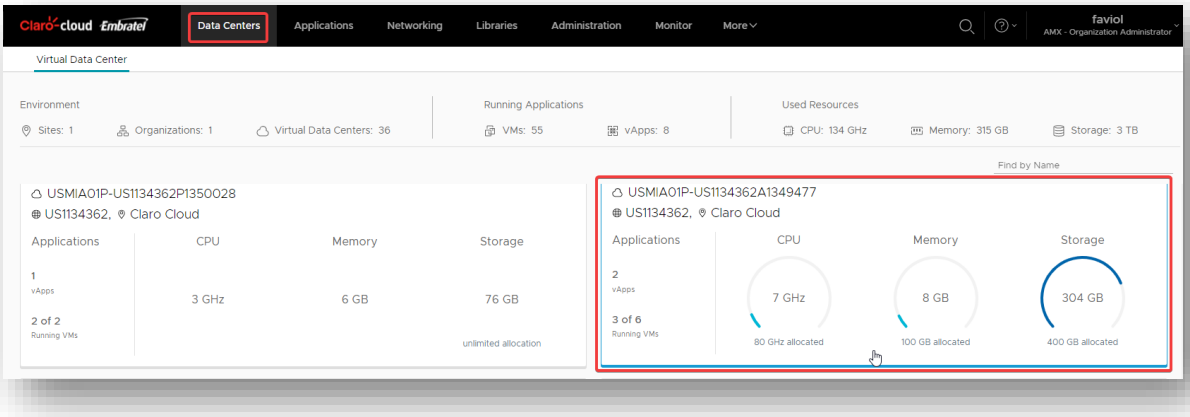
Note: On this screen you can enable the option "Switch to Advanced Networking Workflow" allows you to select the type of network adapter, network, IP mapping

9. Once all the steps are configured, a summary of your configuration will be displayed, by clicking on "Finish".

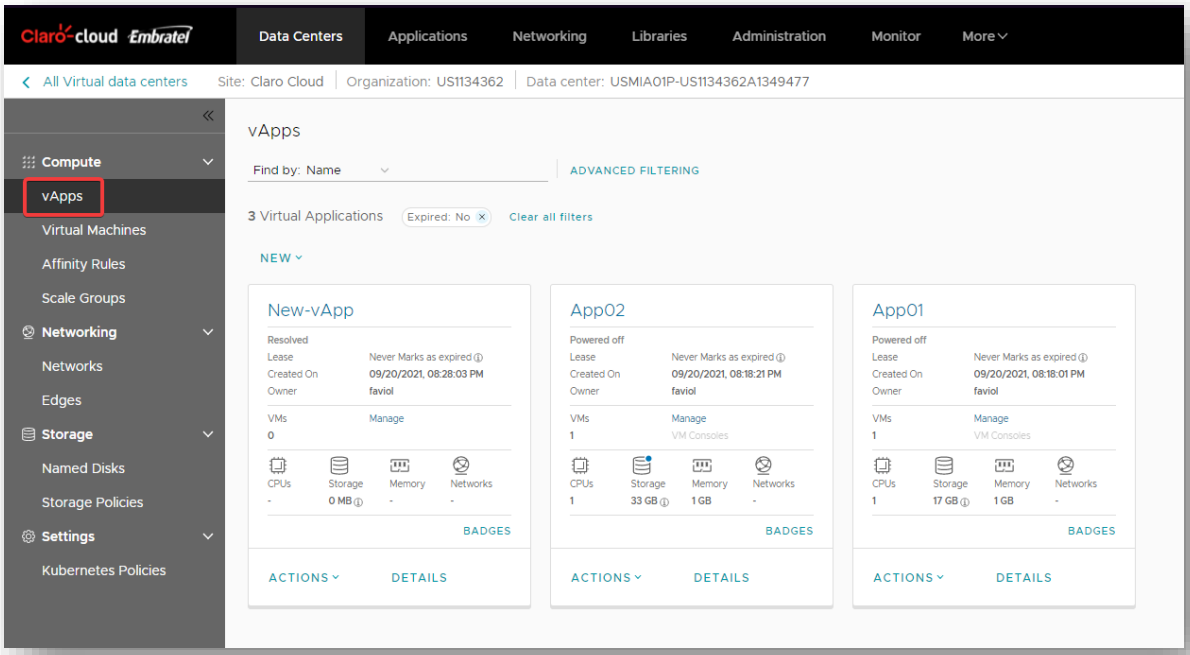


Delete a vApp

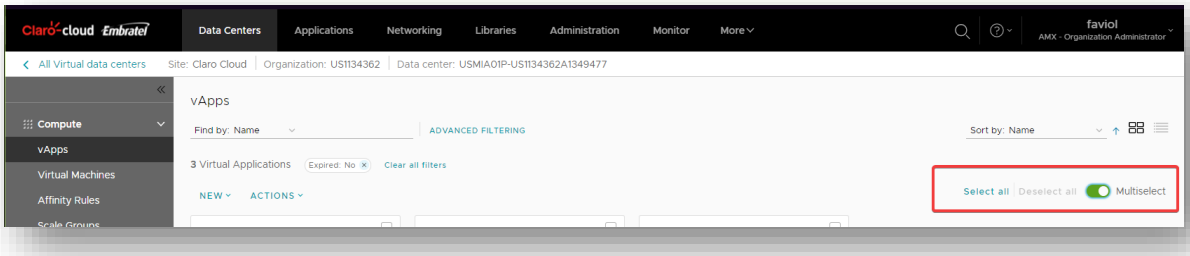
1. Select in the datacenter where the VApp to be removed is located.



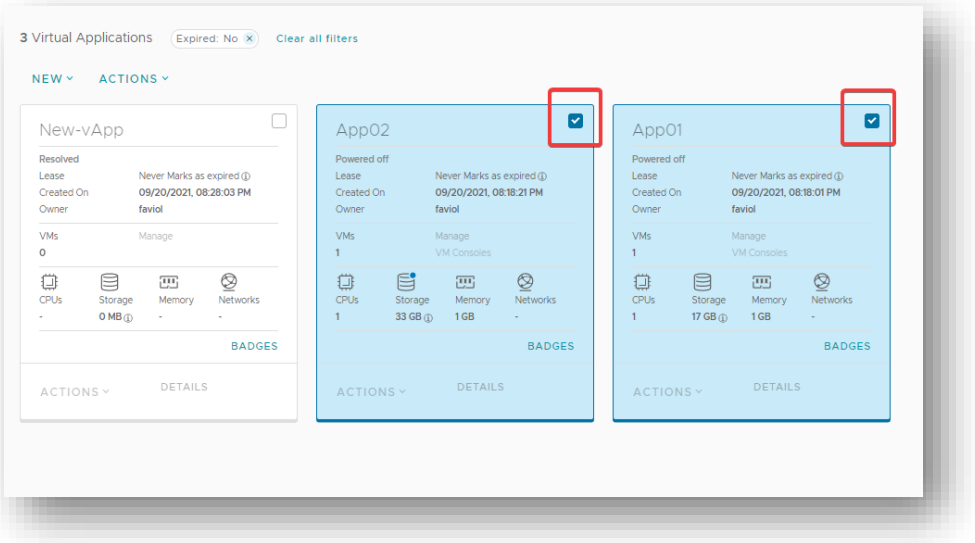
2. Enter the "vApps" section and select the vApp to be deleted



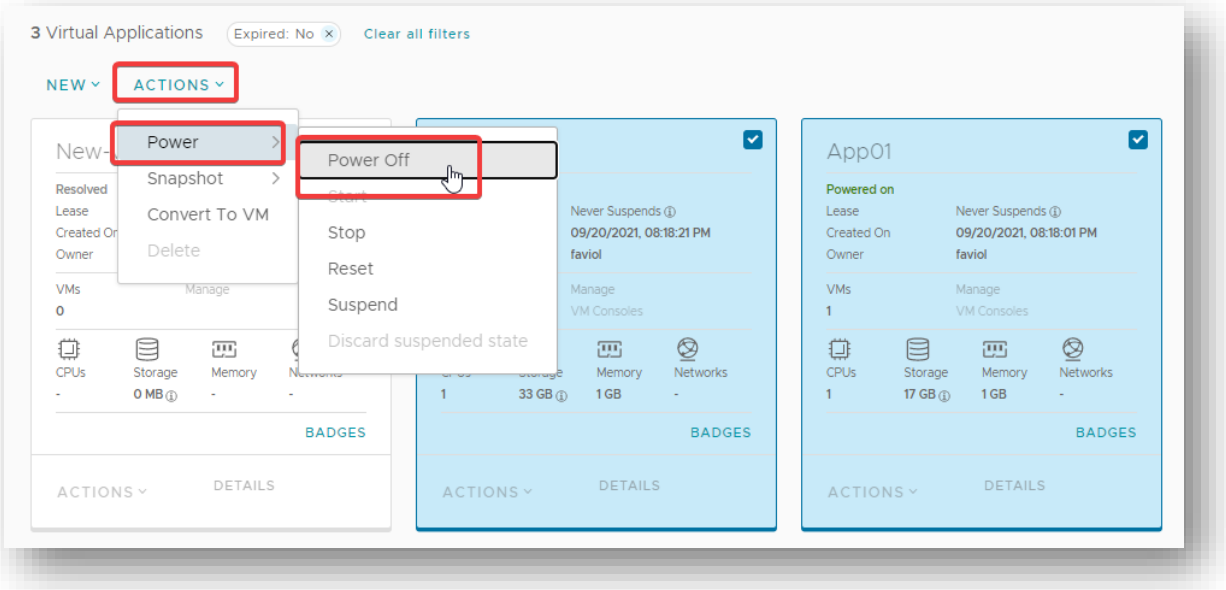
3. If you need to run this action on multiple instances, enable the "multiple-select" button located at the top of the vApps panel



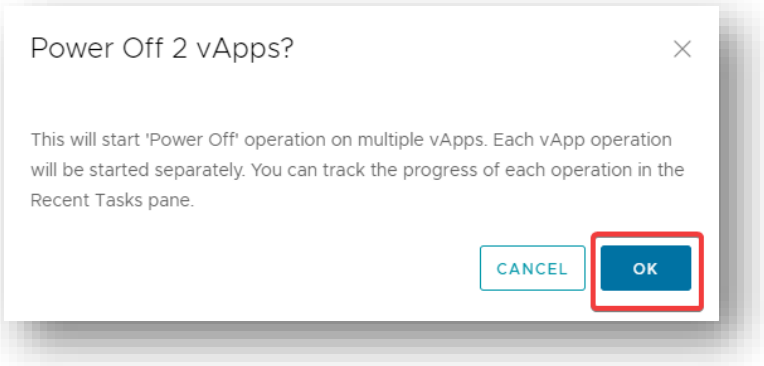
4. Select the vApps you want to change

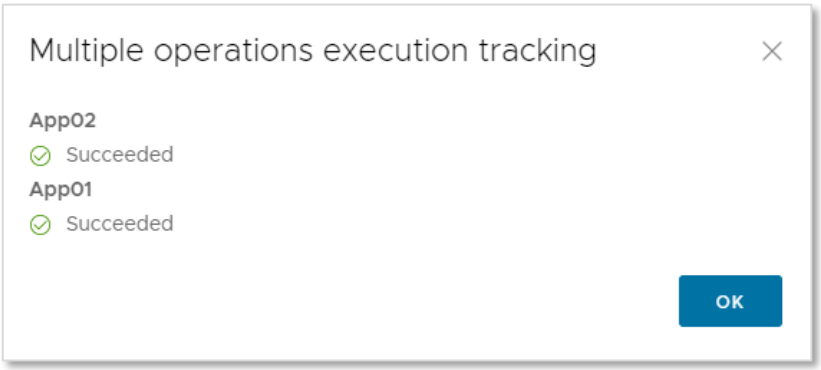


5. Turn off the vApp(s) you want to delete, by clicking "Actions" / "Power" / "Power Off"

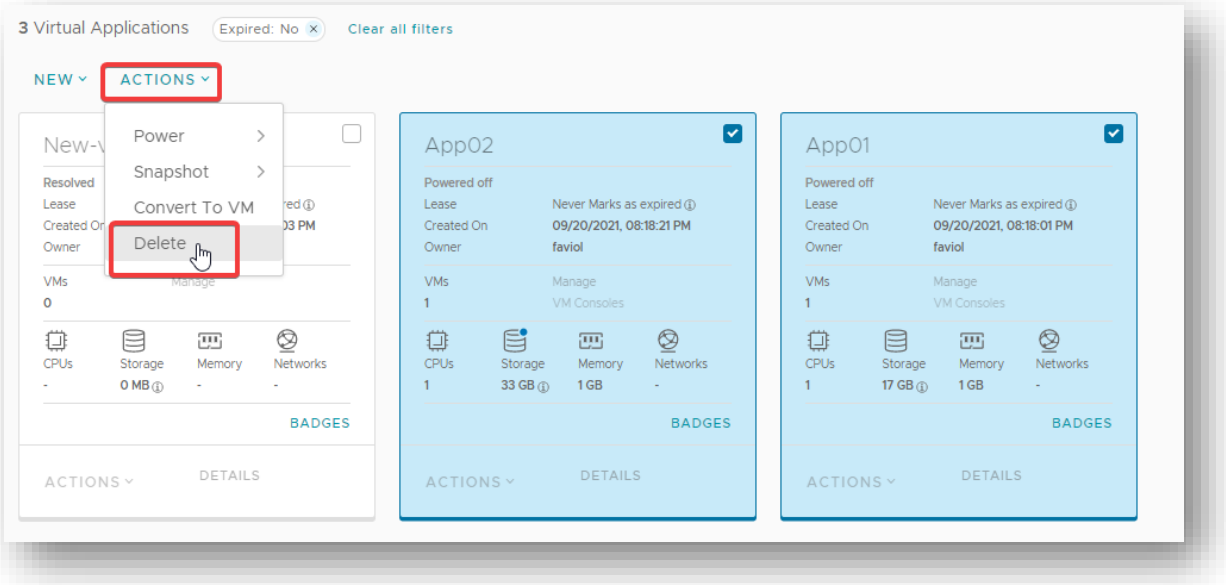


6. Confirm shutdown

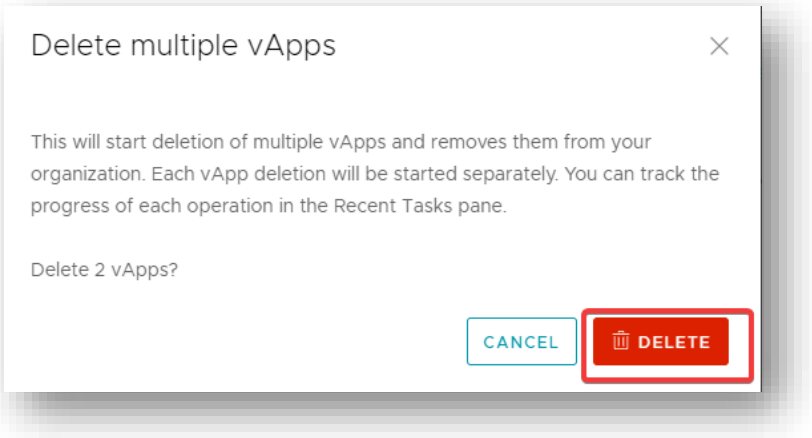




7. Once powered off, click on "Actions" and select "Delete"



8. Confirm Delete to finish the process



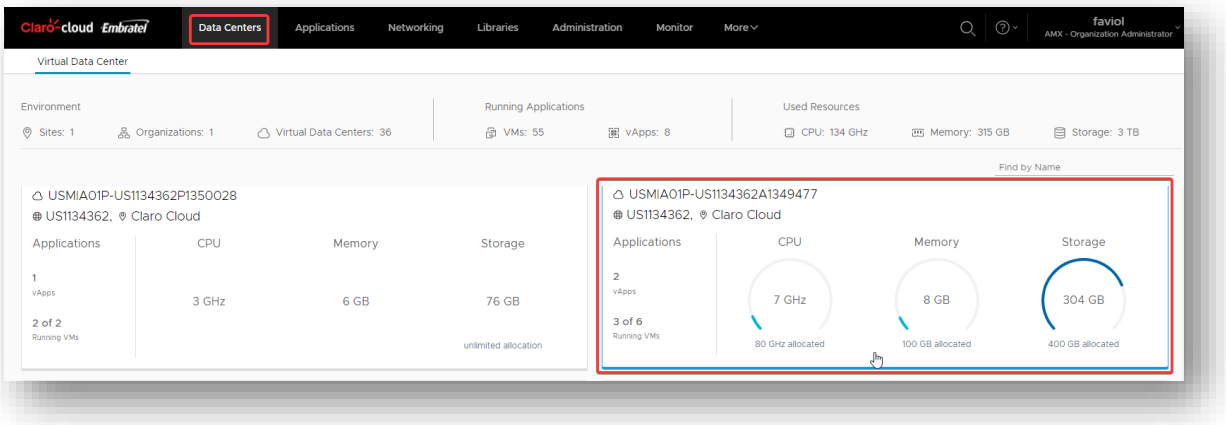
Creating Snapshot in vApps

Taking a snapshot of a vApp takes a snapshot of all virtual machines in the vApp. After you take the snapshot, you revert all virtual machines in the vApp to the snapshot or delete it if you don't need it.

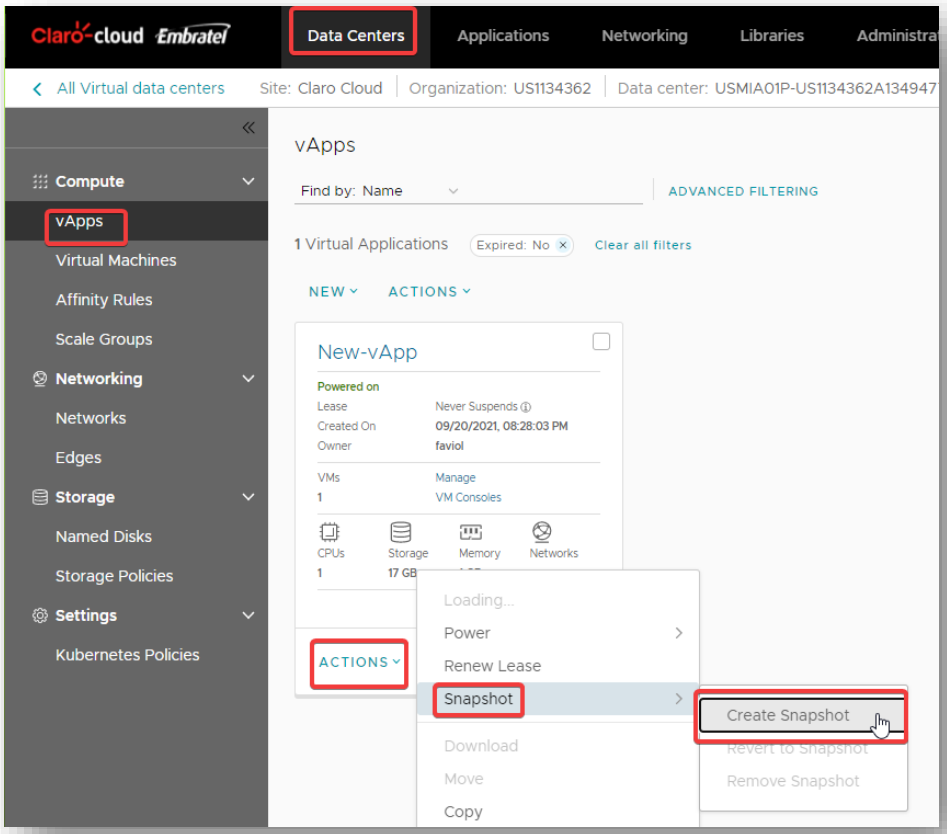
vApp snapshots have some limitations.

- vApp snapshots do not capture NIC configurations.
- If any vApp virtual machine is connected to a named disk, it cannot take a snapshot of the vApp.

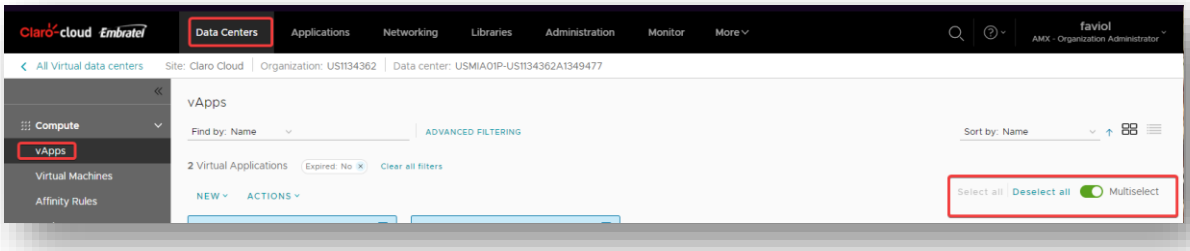
1. To take the snapshot select "Data Center" from the top menu, identify and click on the Data Center box that contains the vApp



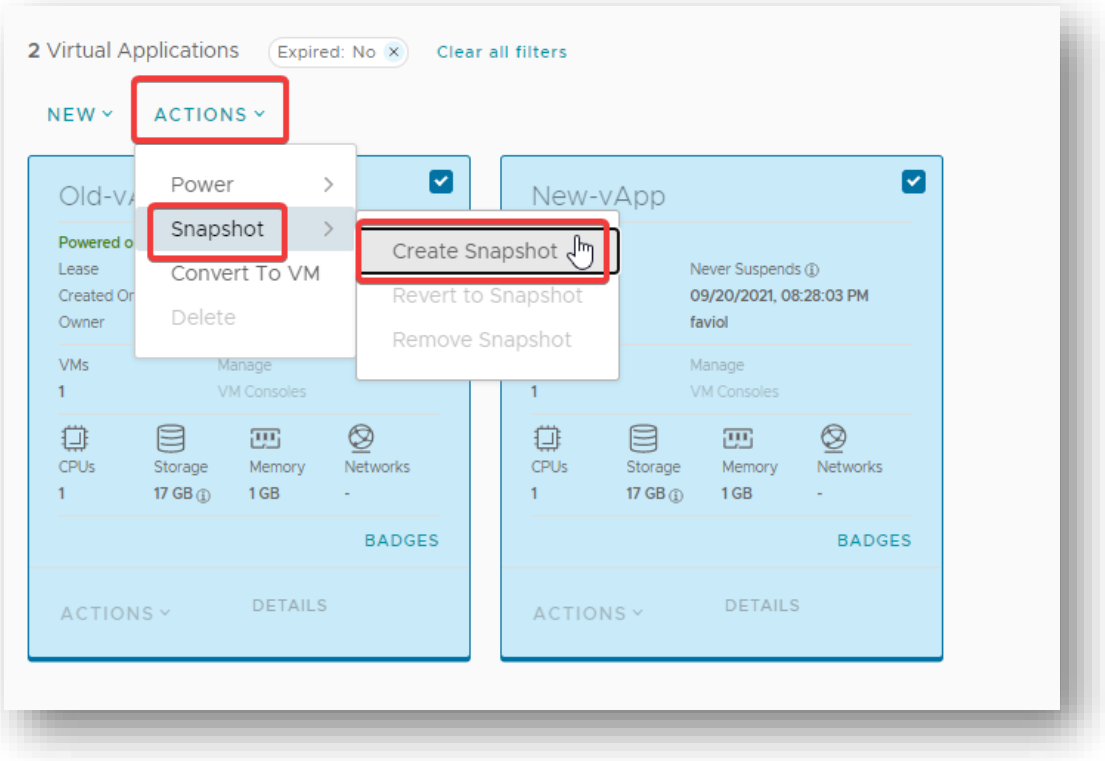
2. Within the data center, select "vApps". Identify the vApp from which the snapshot will be taken, by clicking on the "Actions" / Snapshot " / "Create snapshot"



3. If you need to run this action on multiple instances, enable the "Multiselect" button located at the top of the vApps panel



4. Select the vApps you want to change and click on "Actions" / "Snapshot" / "Create Snapshot"

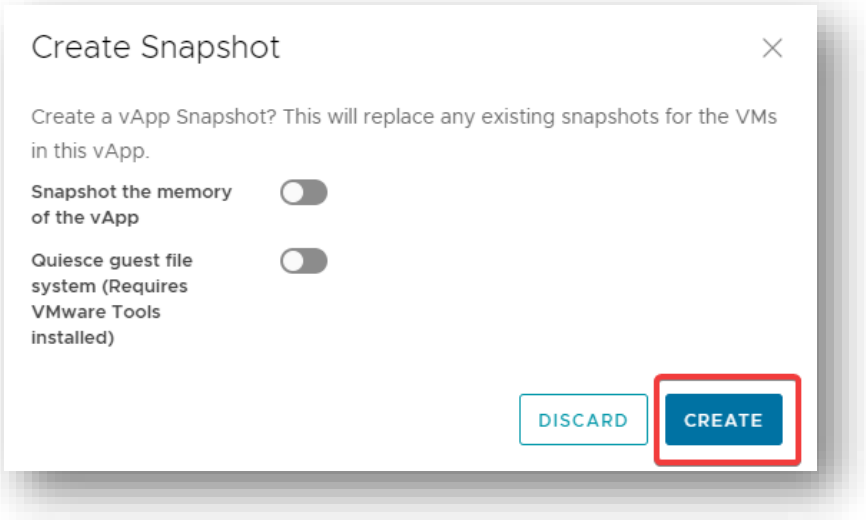


5. The following optional screen will open, with the following options

Item	Description
Take snapshot of virtual machine memory	When the virtual machine memory state is captured, the snapshot retains the active state of the virtual machine. Snapshots created with memory take a snapshot at a precise time, for example, to update software that is still in operation. If you create a snapshot of memory and the update does not finish as expected, or if the software does not meet your expectations, you can revert to the previous state of the virtual machine. When memory state is captured, you do not need to idle the virtual machine files. If the memory state is not captured, the snapshot does not save the active state of the virtual machine, and the disks are fault-consistent unless they are put into idle mode.
Put the guest file system into idle mode (requires VMware Tools be installed)	For this operation, VMware Tools must be installed on the virtual machine. When you put a virtual machine into idle mode, VMware Tools puts the virtual machine's file system into idle mode. An inactive mode operation ensures that the snapshot disk represents a consistent state of the guest file systems. Snapshots in idle

	mode are suitable for automated or periodic backups. For example, if the activity of the virtual machine is unknown, but you want to have several recent backups for rollbacking, you can put the files into idle mode. Virtual machines that have large capacity disks cannot be put into idle mode.

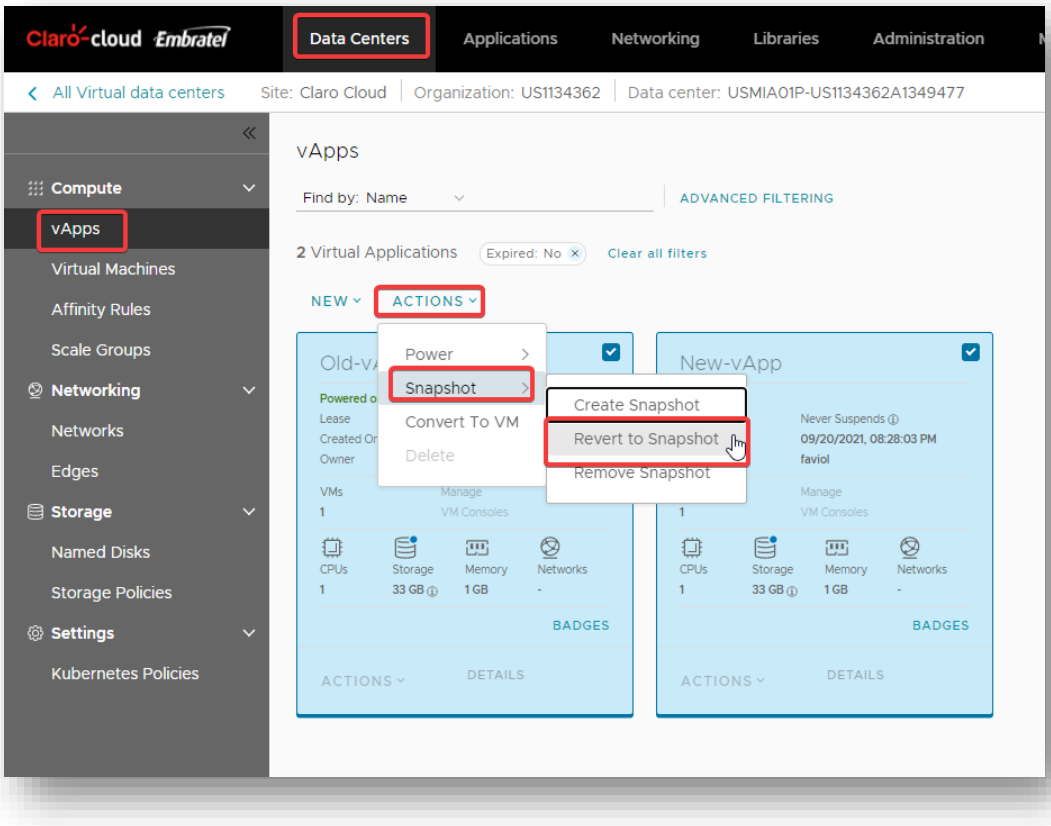
6. Click "Create"



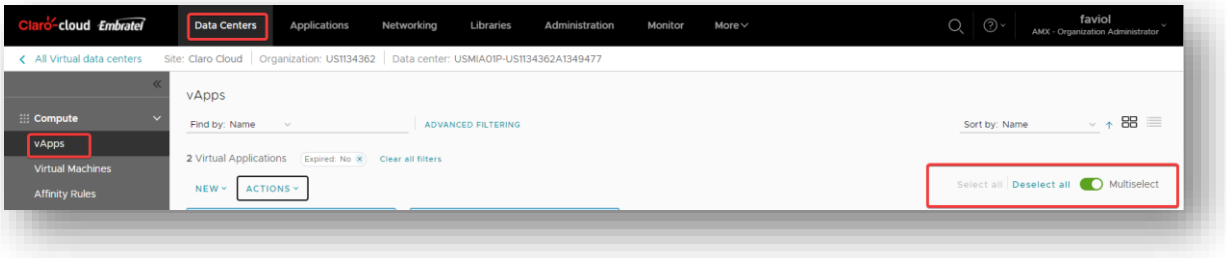
Revert a Snapshot of a vApp

Snapshots can be rolled back for all virtual machines in a vApp to the state they were in when you created the vApp snapshot. To perform this process follow these steps:

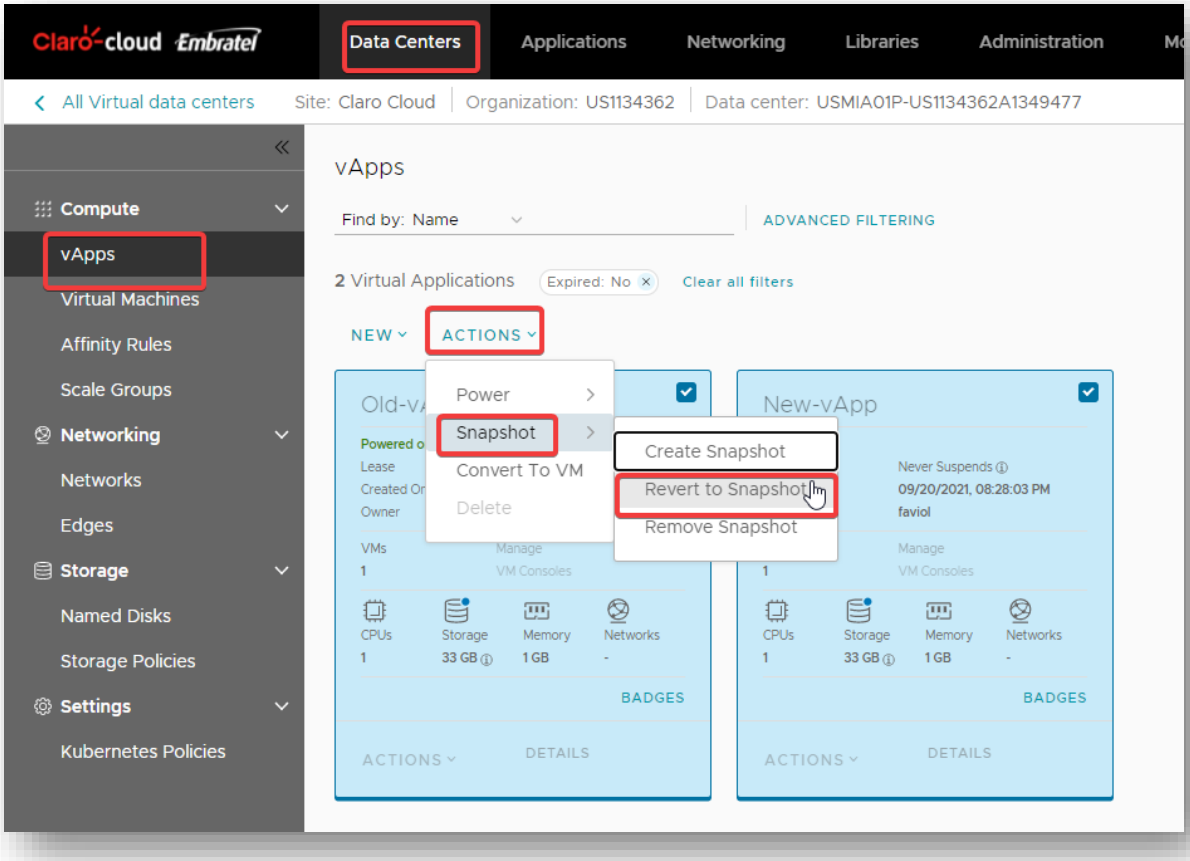
1. In the Data Center menu, select vApps, then choose the vApp to which you want to revert the snapshot, later in the Actions menu select Snapshot and then “Revert to Snapshot”



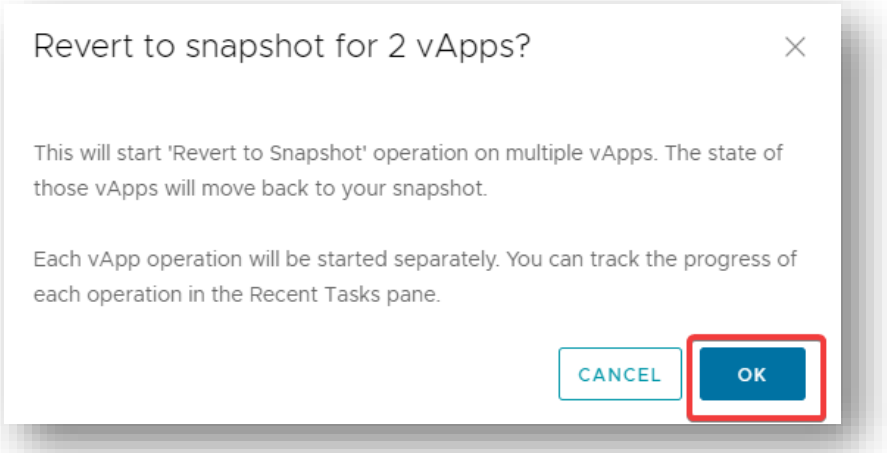
2. If you need to run this action on multiple instances, enable the "Multiselect" button located at the top of the vApps panel



3. Select the vApps you want to occupy and click on "Actions" / "Snapshot" / "Revert to Snapshot"



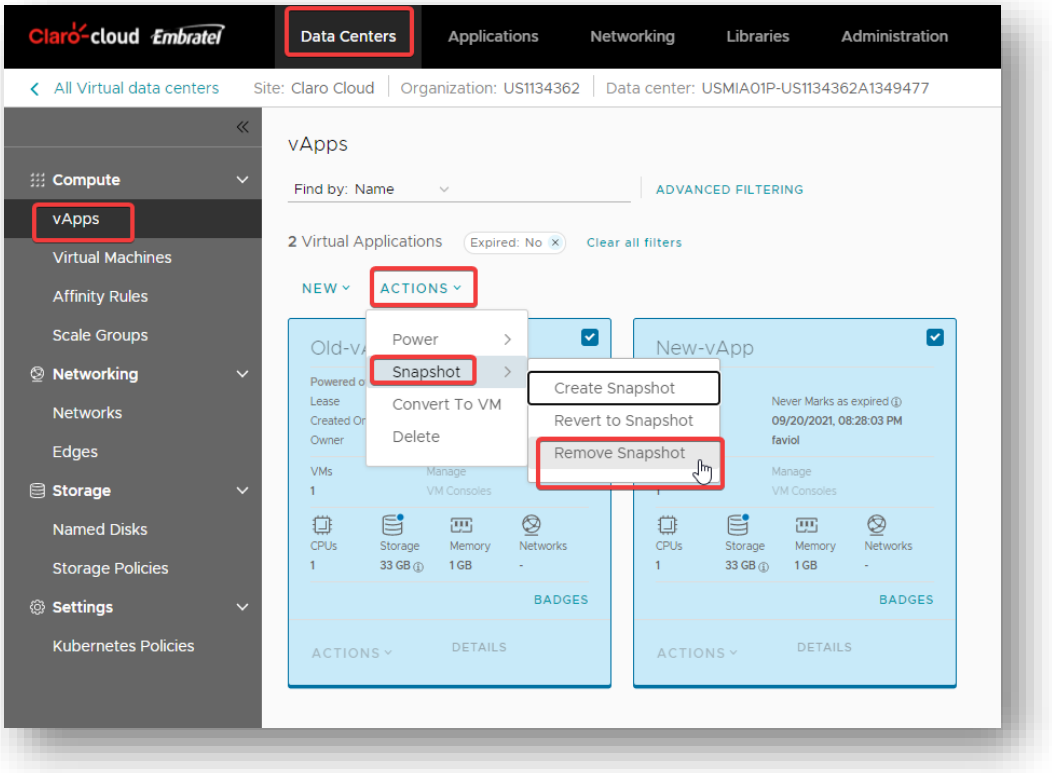
4. Then click "OK" to finish the process



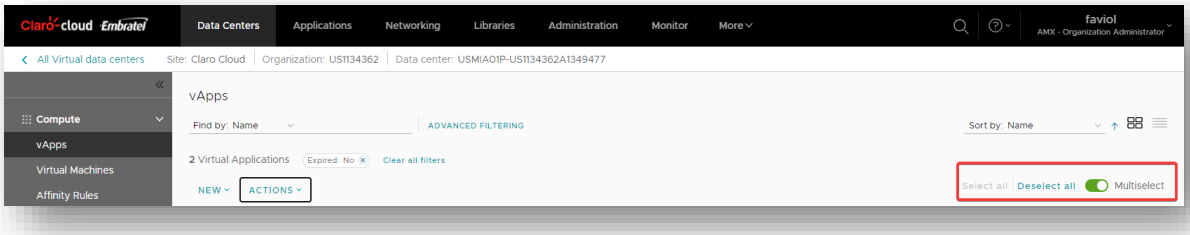
Remove a snapshot from a vApp

You can delete a snapshot from a vApp. When you delete a vApp snapshot, you delete the state of the virtual machines in the snapshot and cannot revert to that state again. Deleting a snapshot does not affect the current state. You may remove a vApp snapshot by the following process:

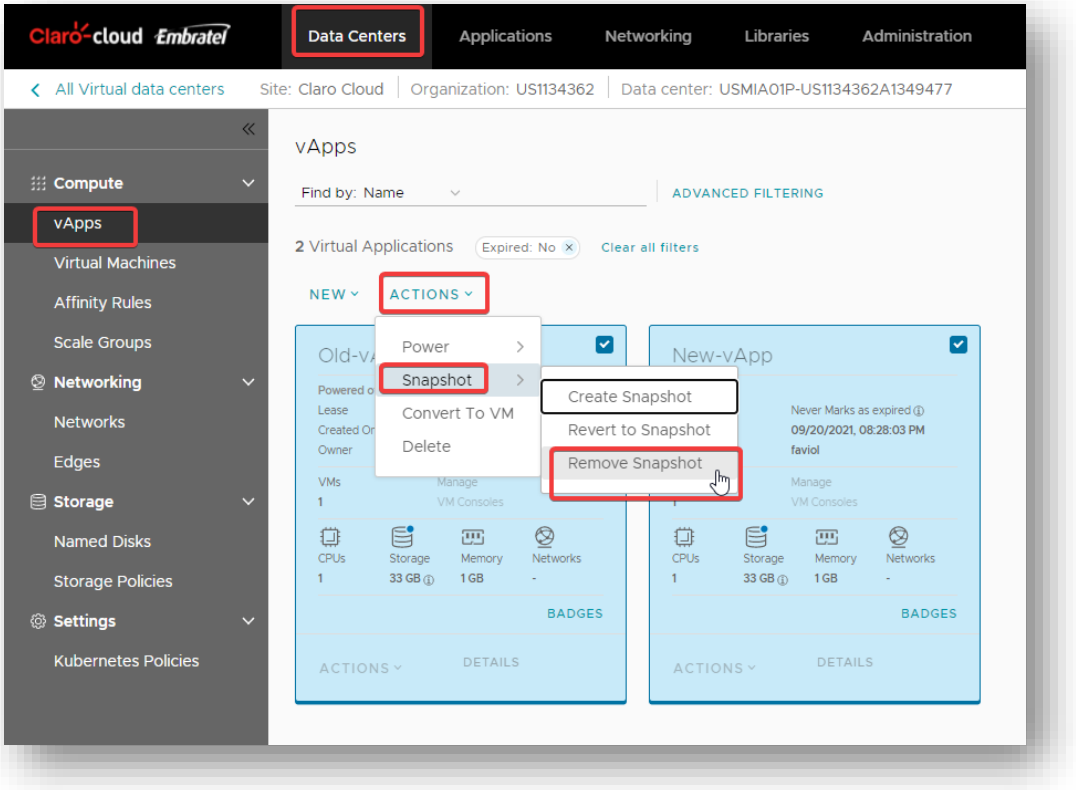
1. On the Data Centers menu, select vApps, then click Actions, then click Snapshot, then click Remove Snapshot



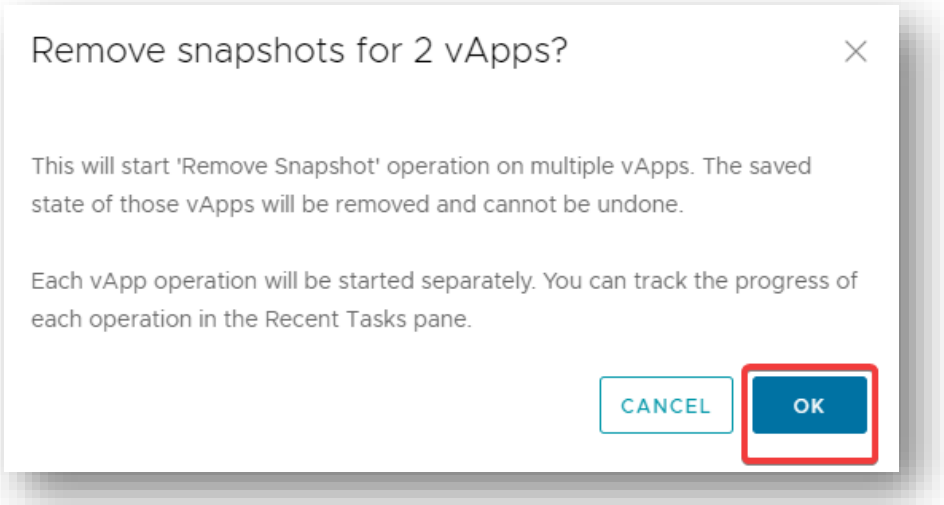
2. If you need to run this action on multiple instances, enable the "Multiselect" button located at the top of the vApps panel



3. Select the vApps you want to change and click on "Actions" / "Snapshot" / "Remove Snapshot"



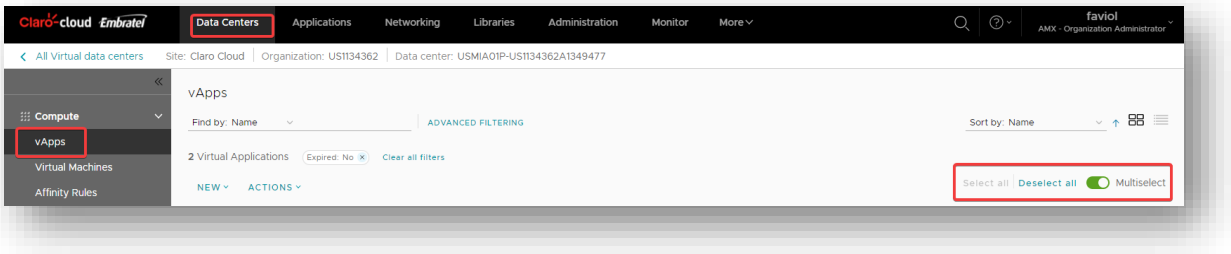
4. Click "OK" to finish the process



Common actions applied to multiple vApps

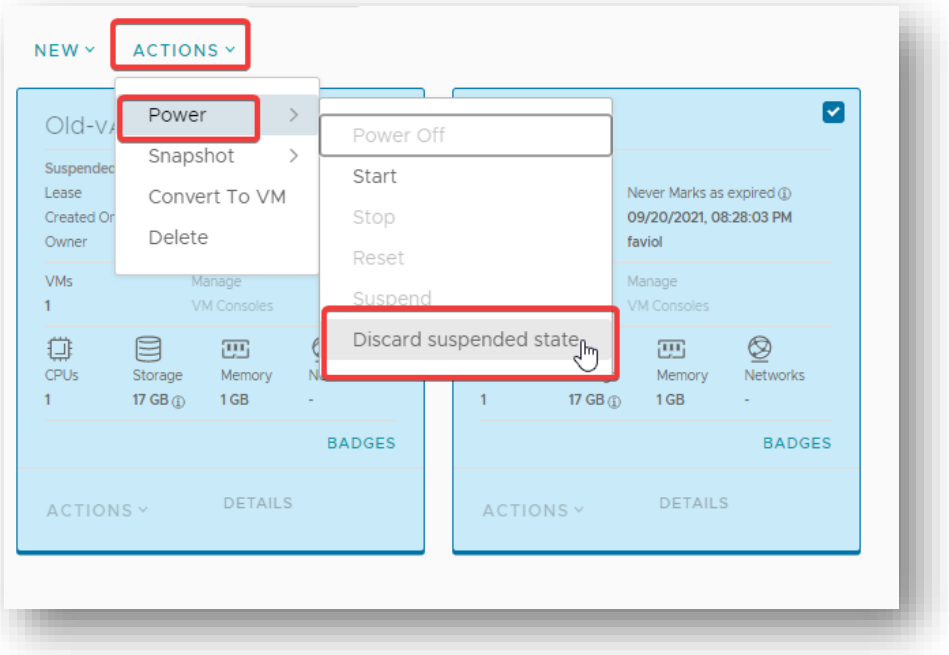
You can perform the Shutdown, Power, Restart or Sleep on multiple vApps through the Enterprise Claro Cloud panel

1. Above the Data Center menu, slide the "Multiselect" button to the right

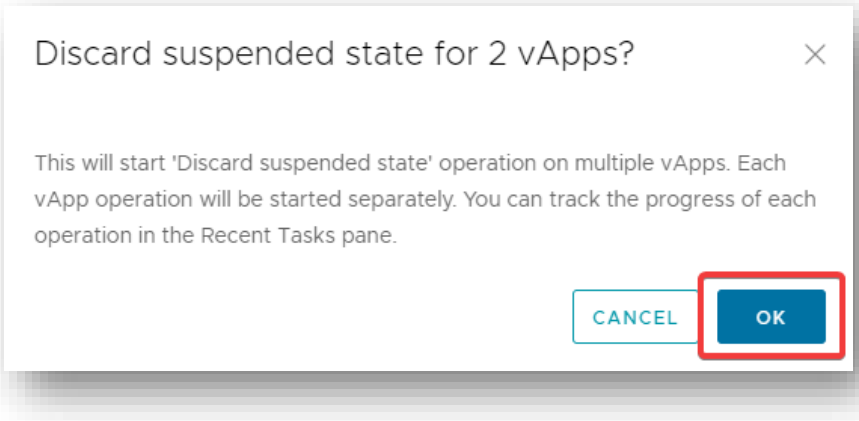


2. Select the vApps that you want to apply an action to them

3. Click on the "Actions" button, then click on "Power" and you can click on the option that you need to apply

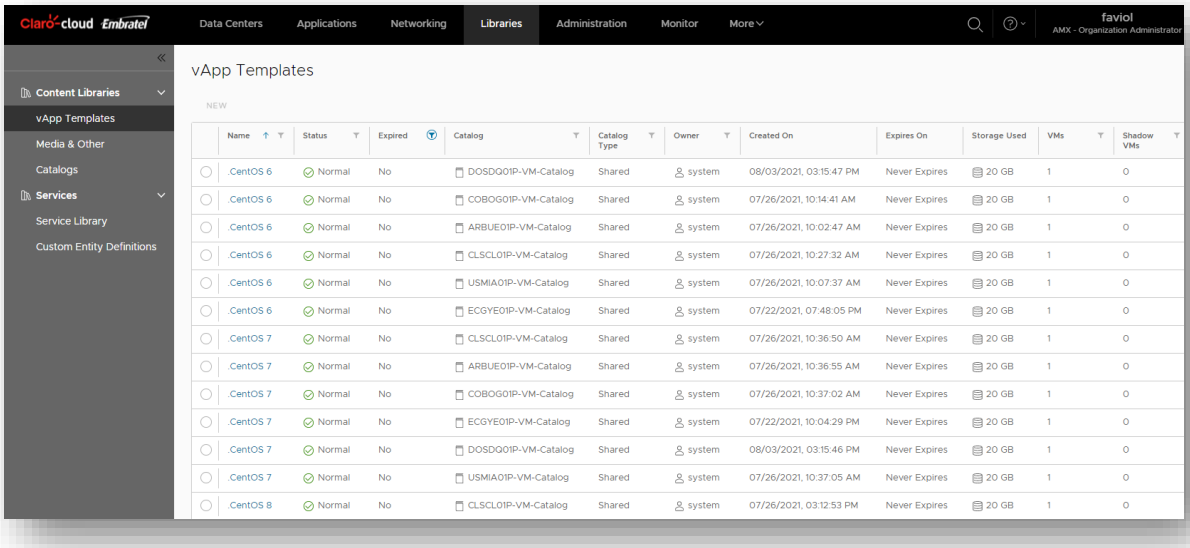


4. Confirm the action by clicking OK


Discard suspended state for 2 vApps?
This will start 'Discard suspended state' operation on multiple vApps. Each vApp operation will be started separately. You can track the progress of each operation in the Recent Tasks pane.
CANCEL
OK

8. Public and Private Catalogs

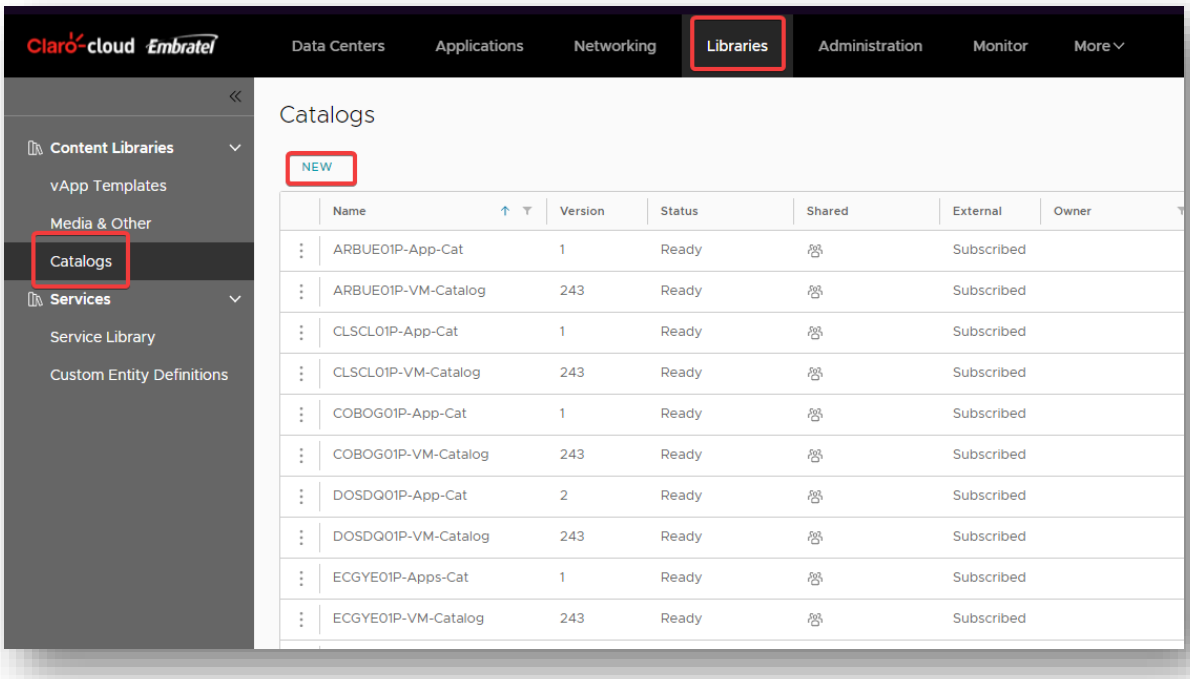
In this section you will find the different available catalogs and images, library of services for workflows such as adding a Gateway, a new public IP, user management, among others.



Create a Catalog

To create new catalogs and associate them with a storage policy, follow these steps

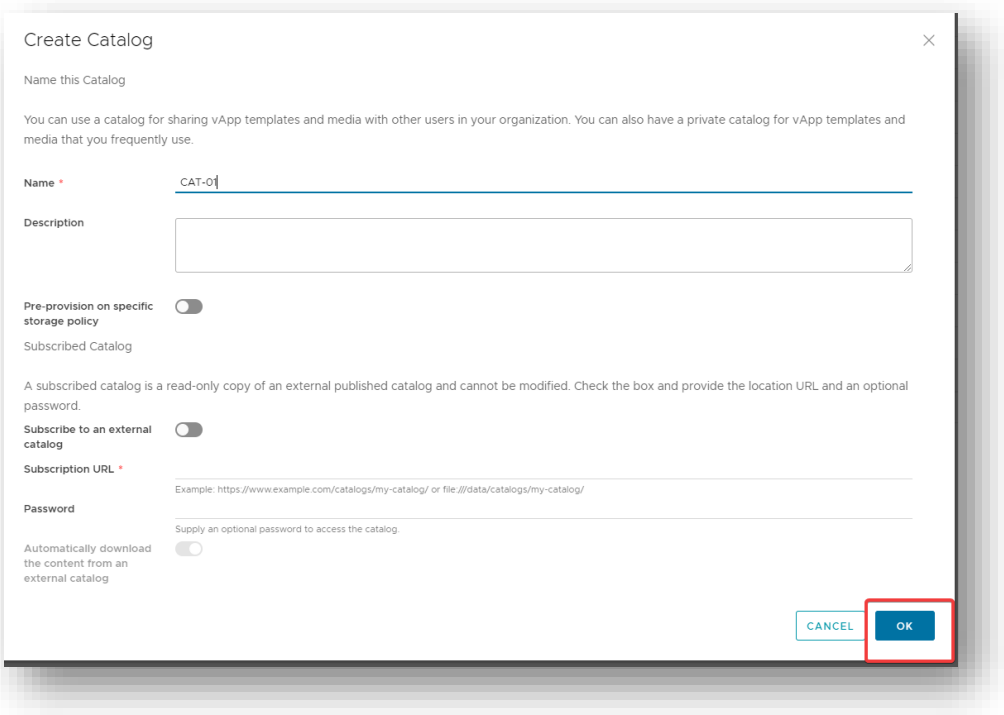
1. On the main menu, point to Libraries, in the left pane, click Catalog, and then click New



2. Fill in the information requested in the form

Item	Description

Name	Catalog name
Description	Catalog description
Pre-provisioning on specific storage policy	Define what type of storage policy the catalog is deployed to
Subscribe to an external catalog	Enable/Disable External Catalog Subscription
Subscription URL	External catalog address
Password	External catalog password



Add templates to a private catalog

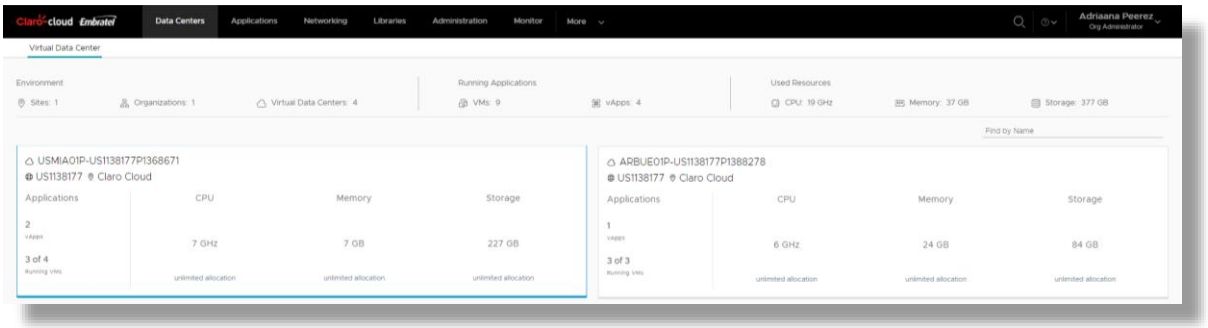
You will be able to upload .ISO images of Operating Systems and customized applications automatically. These templates can only be viewed by the catalog owner and users within your organization who share access to them

Create a template from an existing virtual machine

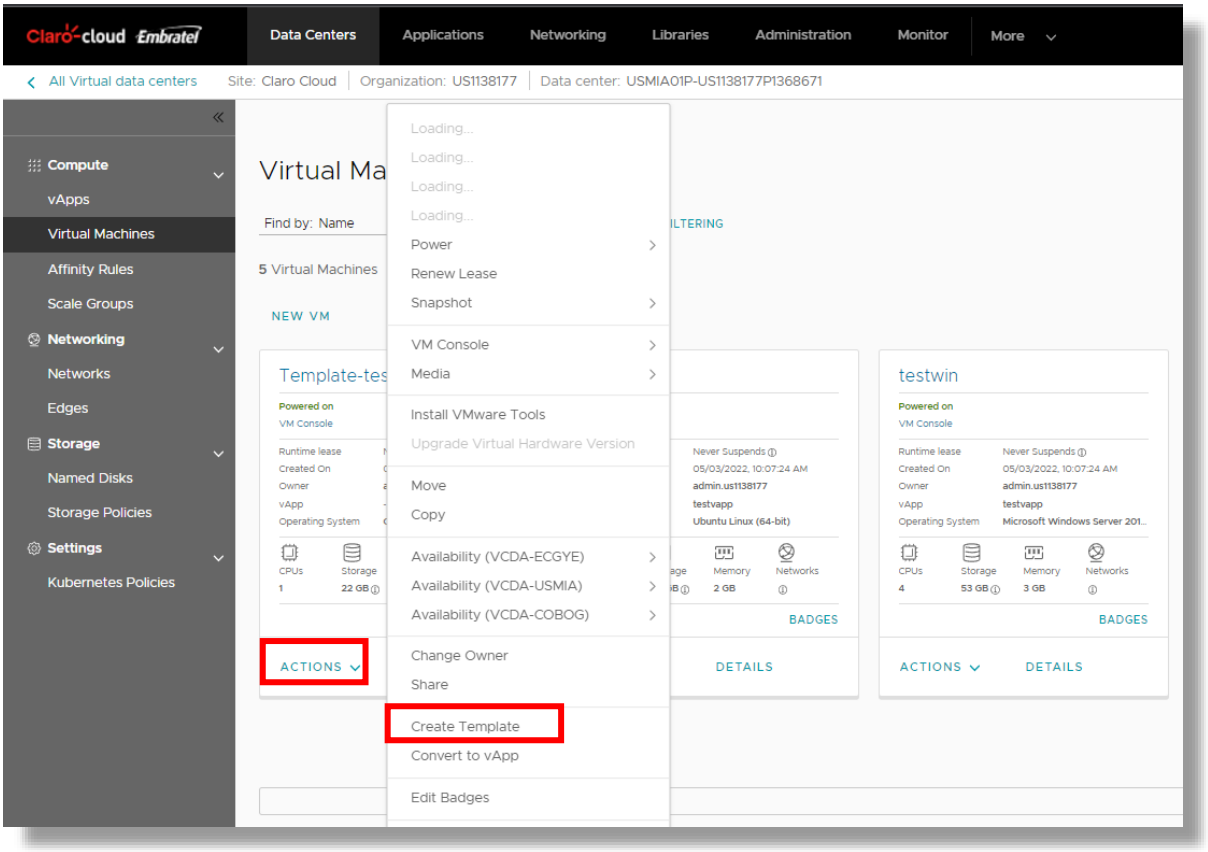
You can create templates from an existing virtual machine, with the goal of being able to create new virtual instances with the same configuration.

1. On the main menu, click Data Center, select the DCV where the virtual machine with which you need to create the template is hosted.

> **Important:** A template does not replace a backup, the template only maintains the base configuration of the source virtual machine, but does not store the data on disk.



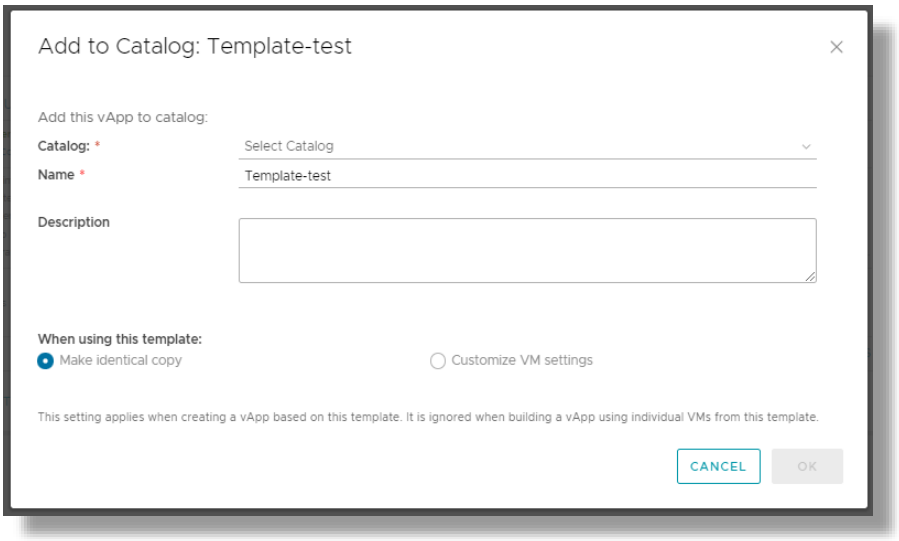
2. Select the Virtual Machines option and identify the Virtual Machine with which you need to create the template, by clicking on the action button within the virtual machine box, a menu will be displayed, click on create template.



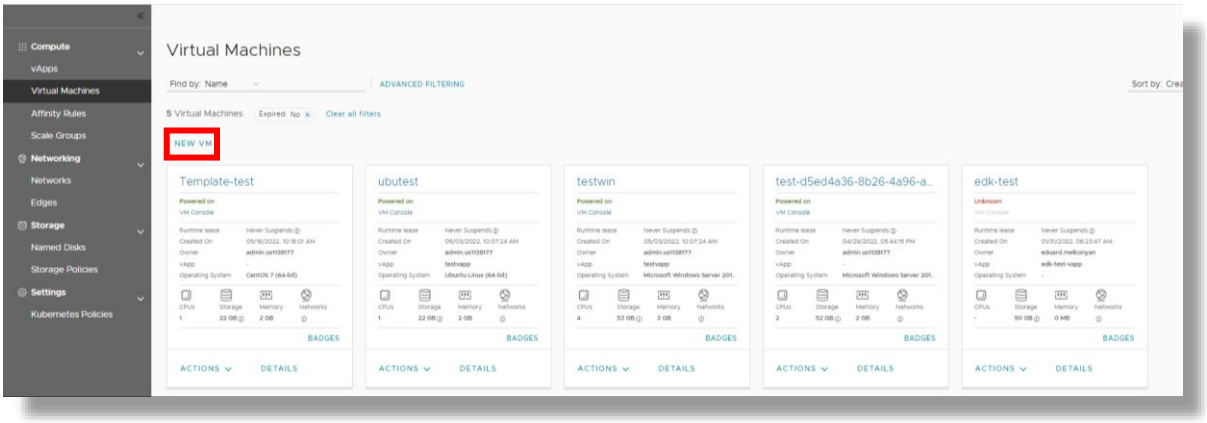
3. The next screen will open, where you must enter the following information, at the end of clicking on the Ok button

Item	Description
Catalogue	Select the catalog where you want to host the template. **Important**: Only private catalogs can be modified.

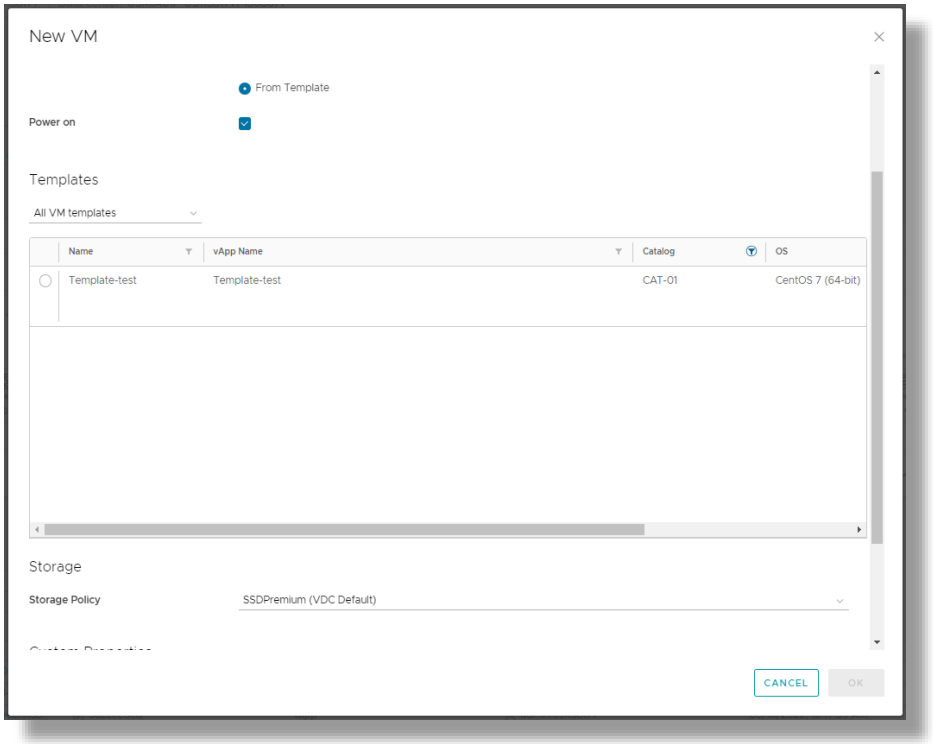
Name	Enter the name you want to give the template within the catalog.
Description	Optional enter a short description, it is recommended to indicate the features of the template
When using this template:	If your VM is not associated with a default vApp, the "Make an identical copy" option will be preselected



4. To create a virtual machine from the new template, enter the panel of your DCV and click on New Virtual Machine.



5. In the Templates section filter by the name of the created catalog, the new template(s) will be deployed, follow the standard process for creating Virtual Machines.

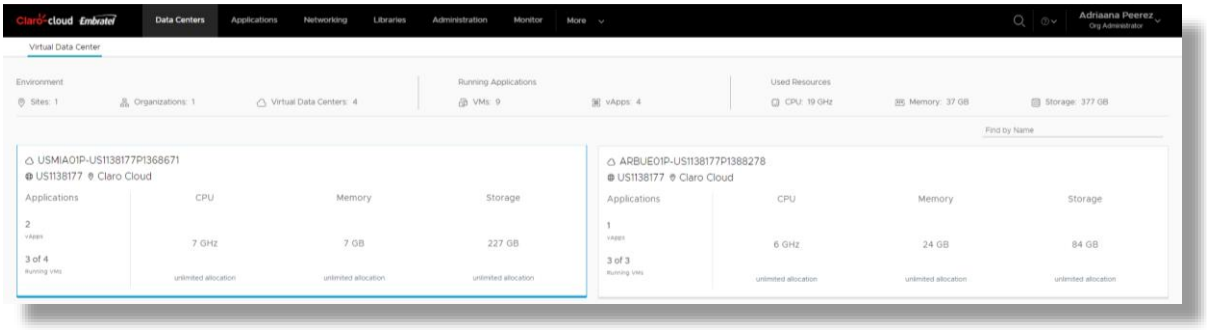


Create a template from an existing vApp

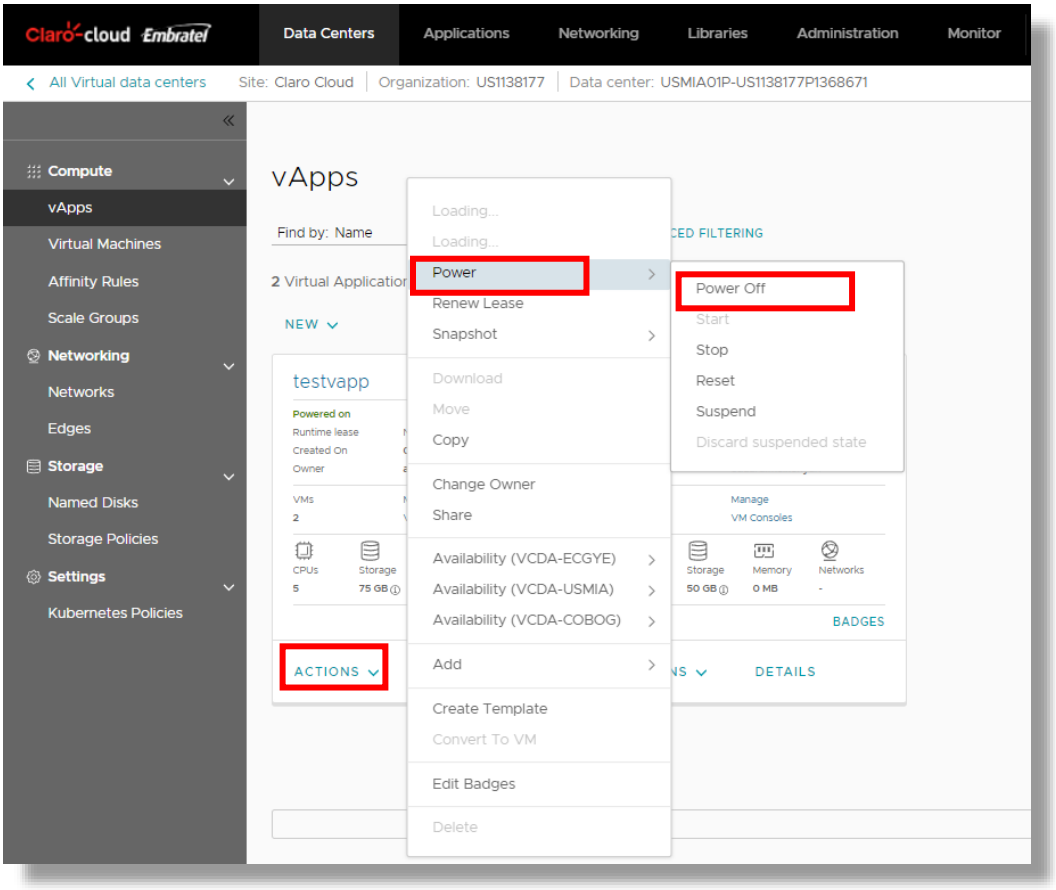
You can create templates from an existing vApp, the template will include the features of all the Virtual Machines associated with the vApp.

1. On the main menu, click Data Center, select the DCV where the vApp with which you need to create the template is hosted.

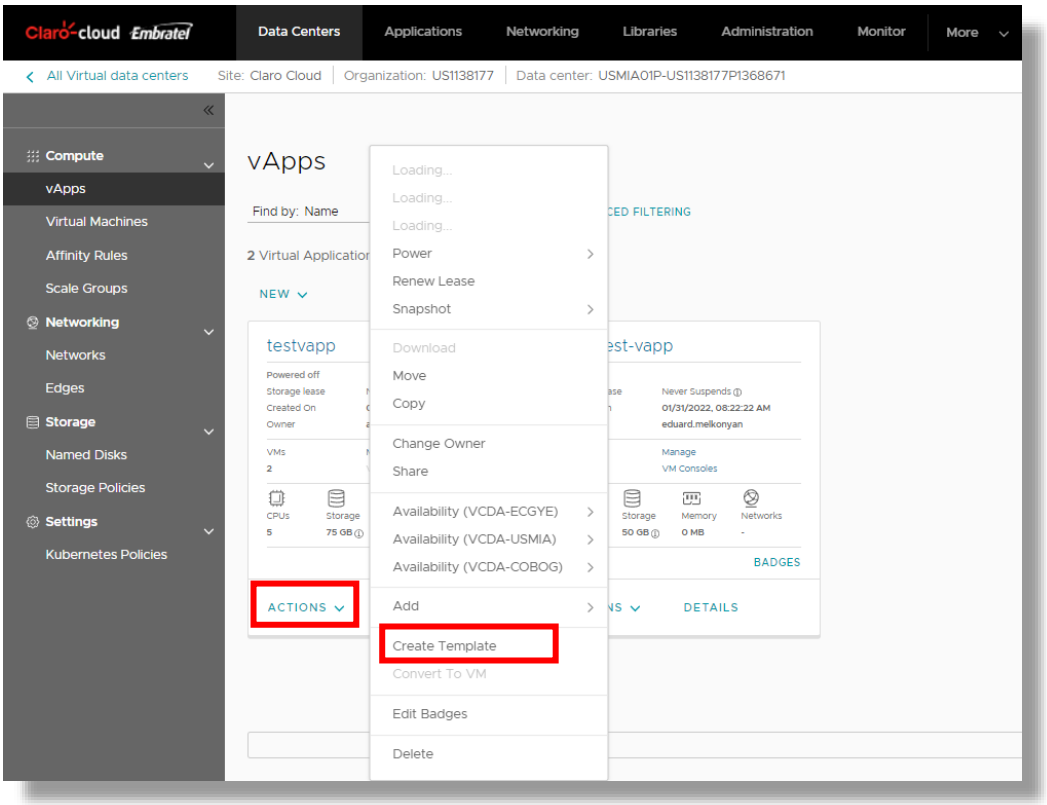
> **Important:** A template does not replace a backup, the template only maintains the base configuration of the source virtual machine, but does not store the data on disk.



6. Select the vApp option and identify the vApp with which you need to create the template, it will be required to turn off the vApp, click on Actions, a click menu on Power / Power Off will be displayed.



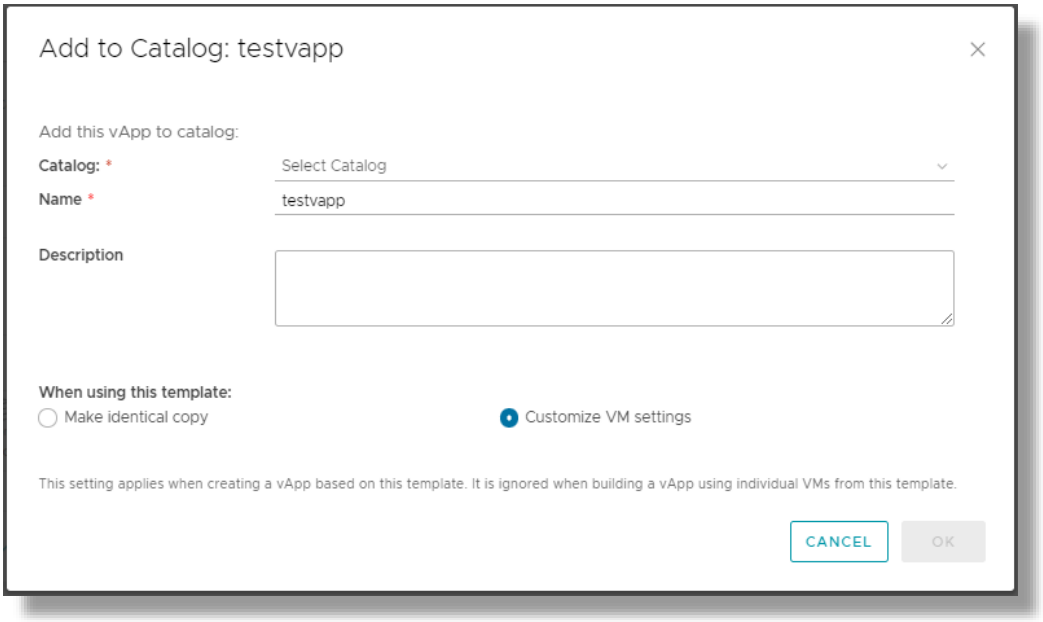
2. Once the vApp is turned off, click the Actions button again, click the Create Template option



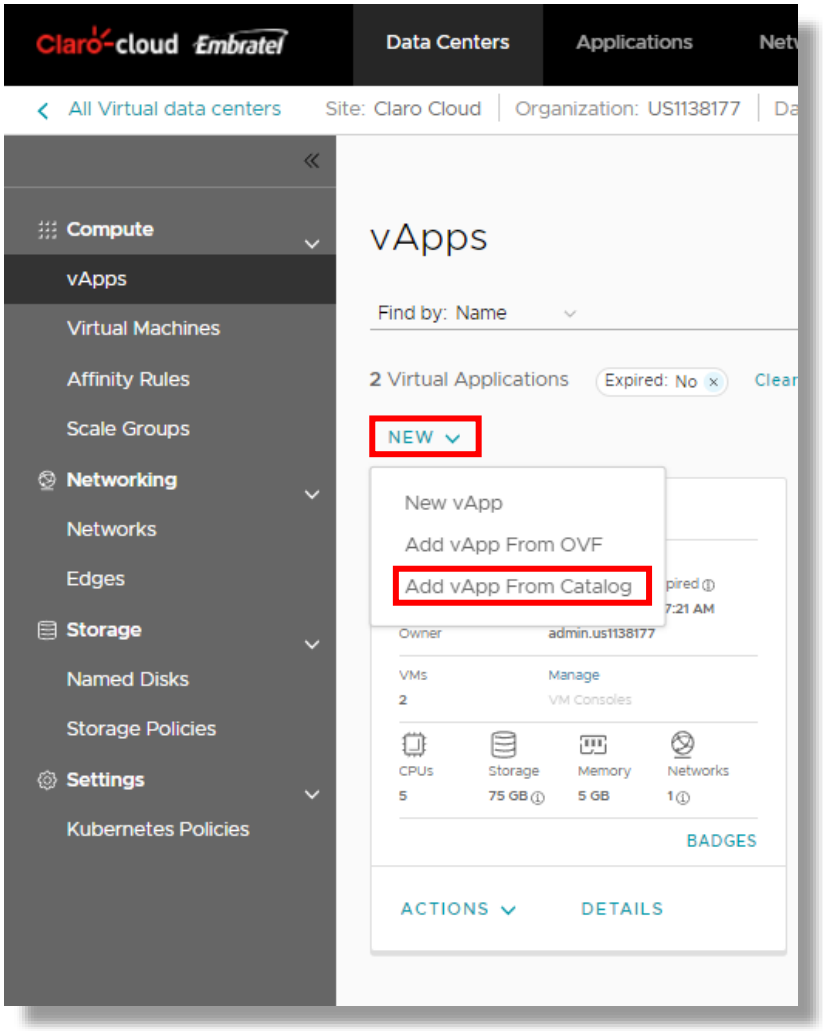
3. The next screen will open, where you will need to enter the following information, at the end of clicking on the Ok button

Item	Description
Catalogue	Select the catalog where you want to host the template. **Important**: Only private catalogs can be modified.
Name	Enter the name you want to give the template within the catalog.
Description	Optional enter a short description, it is recommended to indicate the features of the template
When using this template:	Keep the default option "Customize virtual machine settings"

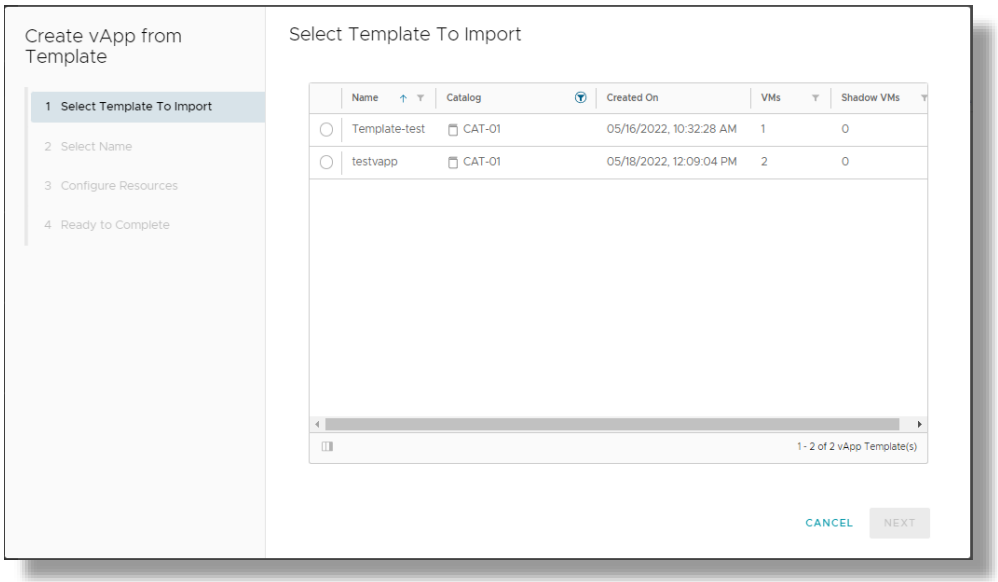
Important: If any VM within the vApp has separate disks associated with it, it is necessary to unlink them. Otherwise the creation of the template will fail



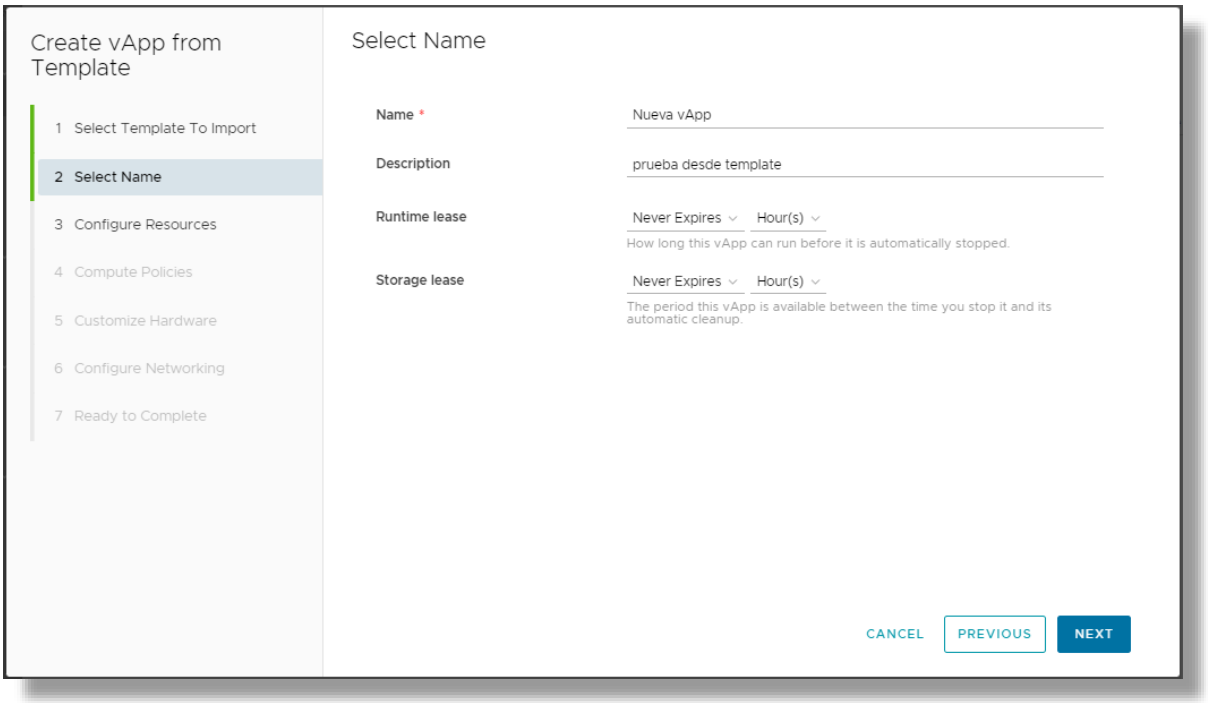
4. To create a vApp from the new template, enter the panel of your DCV and enter the vApps section, click on New / Create vApp from catalog



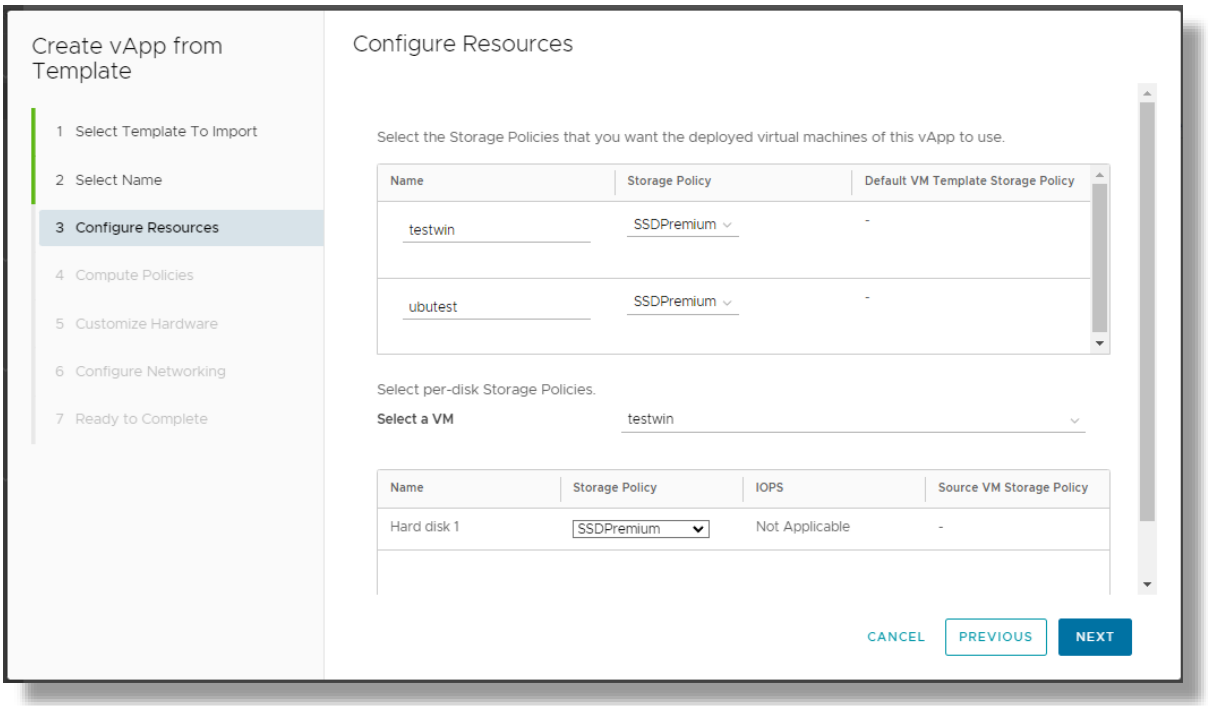
5. The next screen will open, in the template section I filtered by the name of the Catalog, and selected the template you want to occupy, click next.



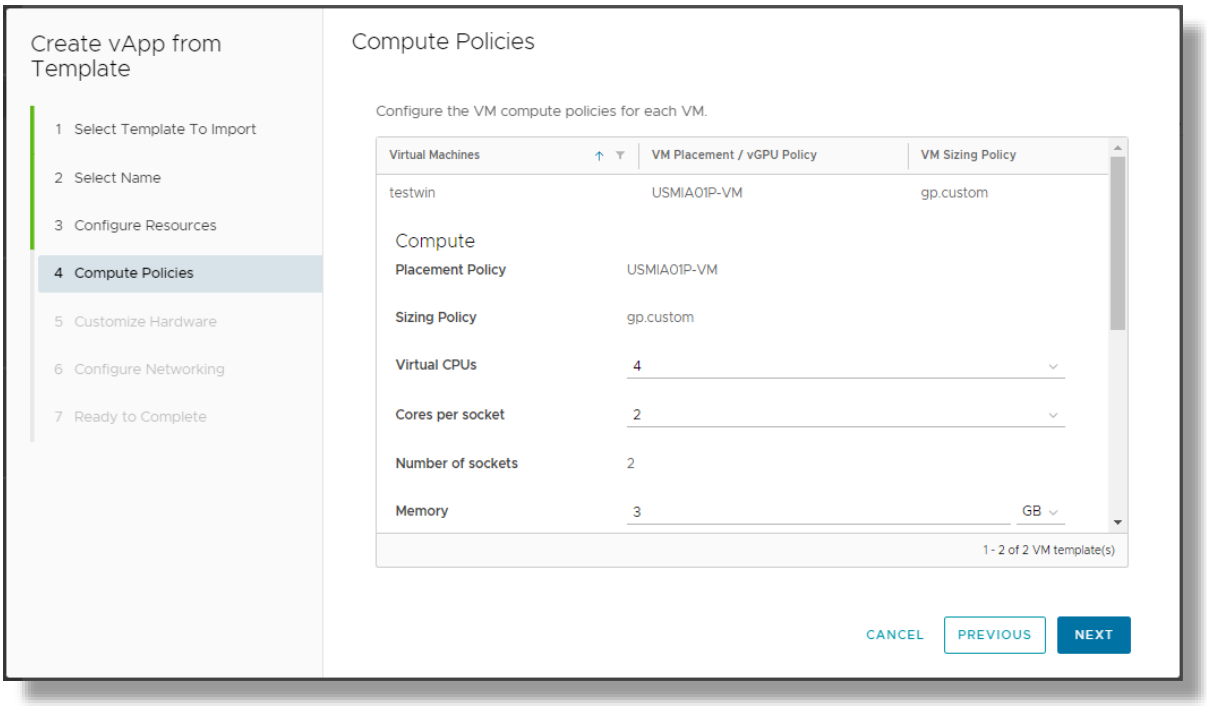
6. In the Name section, enter the name and description of the new vApp, keep the default values of Runtime lease and Storage lease, click next.



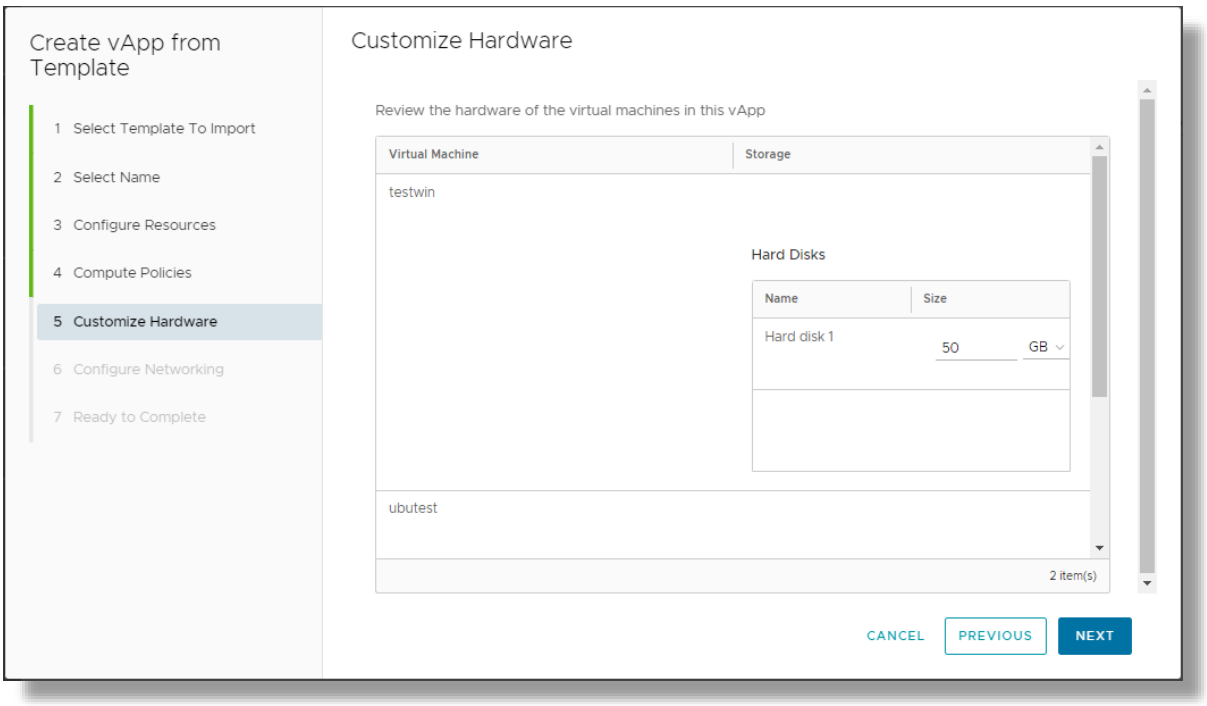
7. In the "Configure Resources" section, the name and storage policies of the new VMs to be created will be displayed, the names of the VMs can be changed, keep the rest of the parameters with the default values, click on next



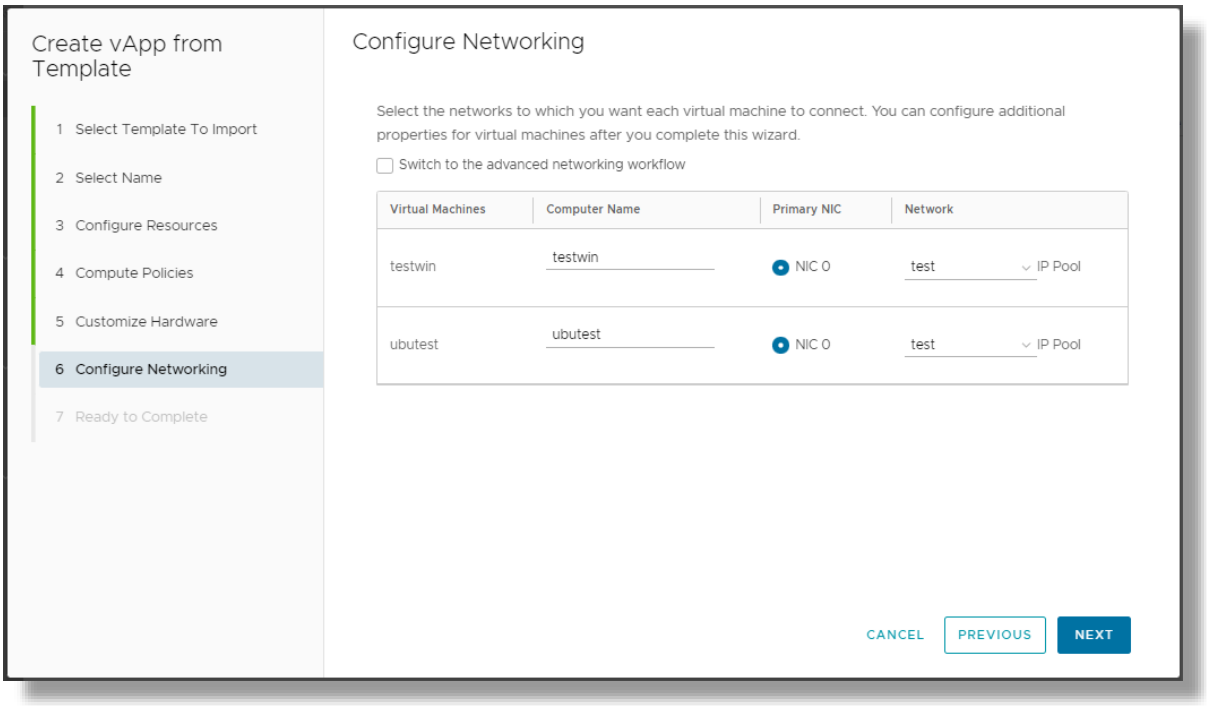
8. In the "Compute Policies" section, the distribution of compute resources by Virtual Machine will be displayed.



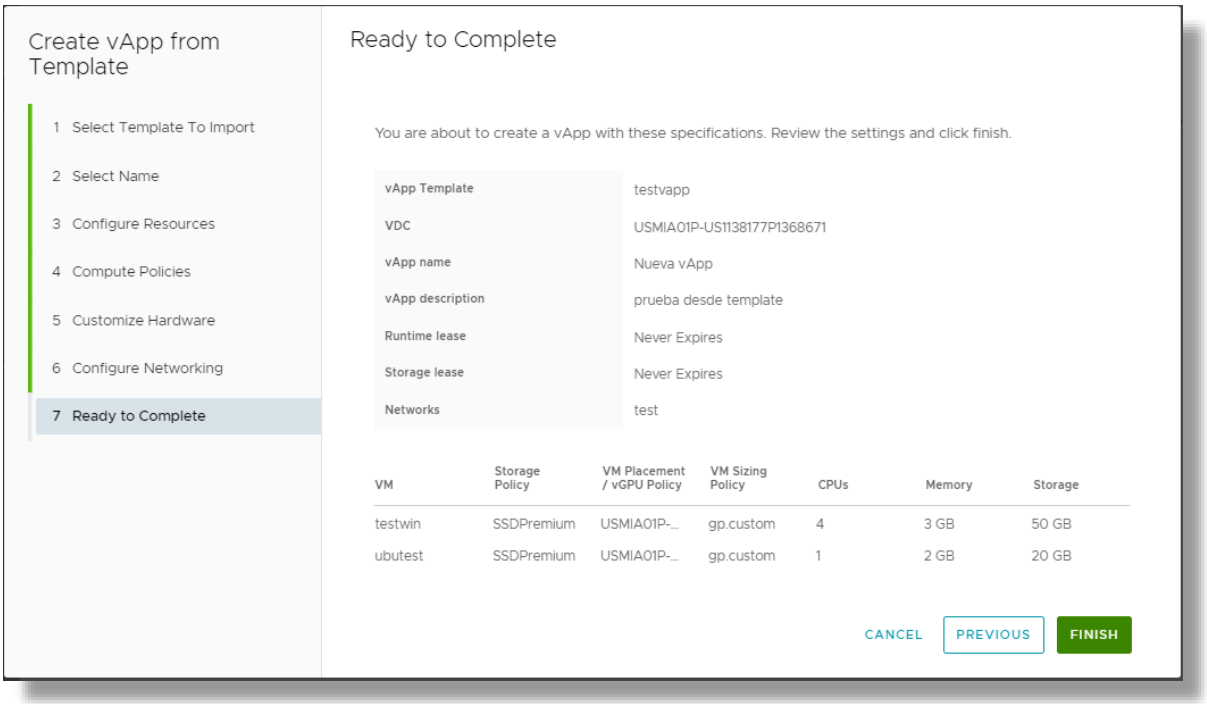
9. in the "Customize Hardware " section the storage distribution per virtual machine is displayed



10. In the "Network Configuration" section, enter the network to which you want to associate the NICs of the Virtual Machines, by default the VLAN that the source virtual machines are assigned is pre-selected, click on next.



11. Finally, a summary will be displayed with the configuration of the vApp to be created, click on Finish.

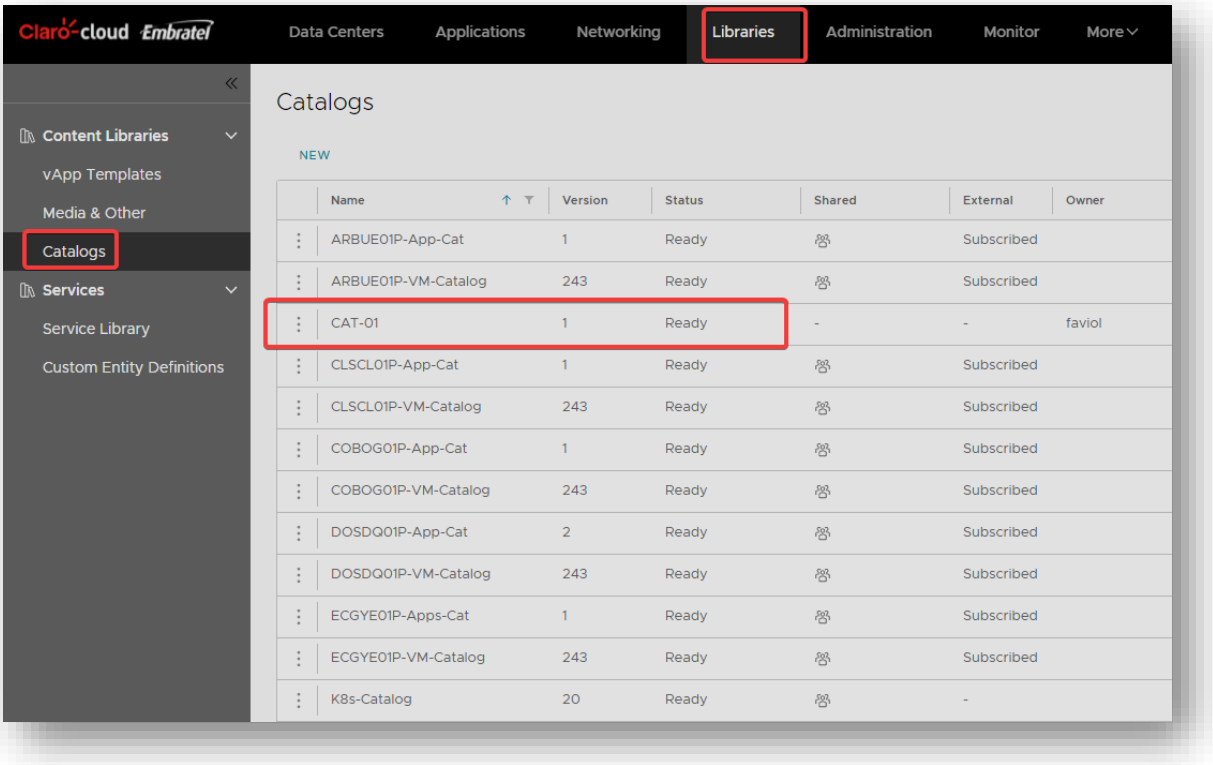


Share a catalog

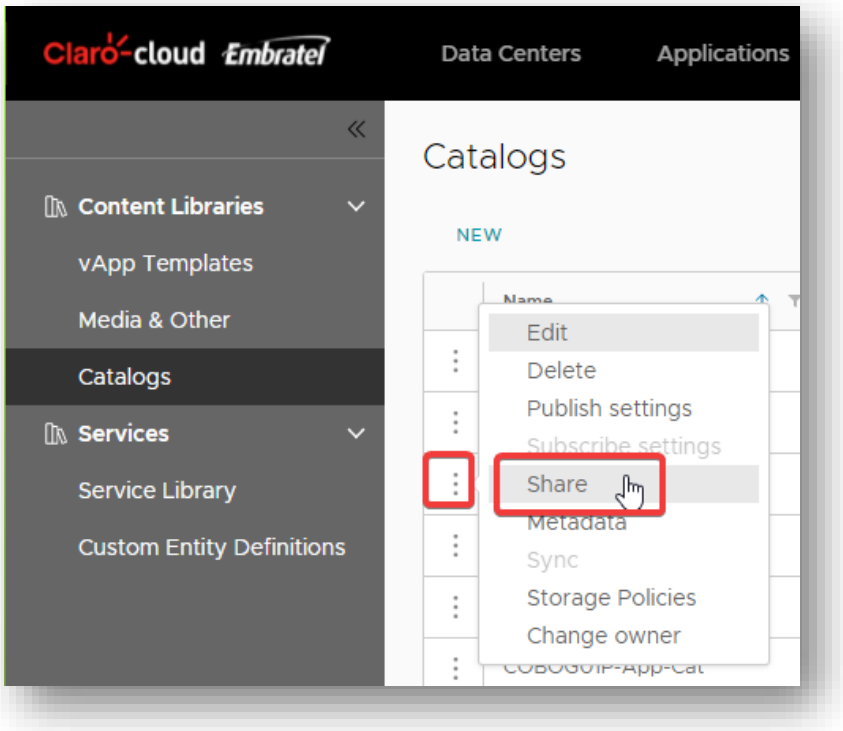
You can share a catalog with all members of the organization or with someone in particular. This requires being the owner of the catalog and having the appropriate permissions.

Below are the steps to follow to perform this process:

1. On the main menu, click Libraries, select catalogs in the left pane, and then select the catalog you want to share.

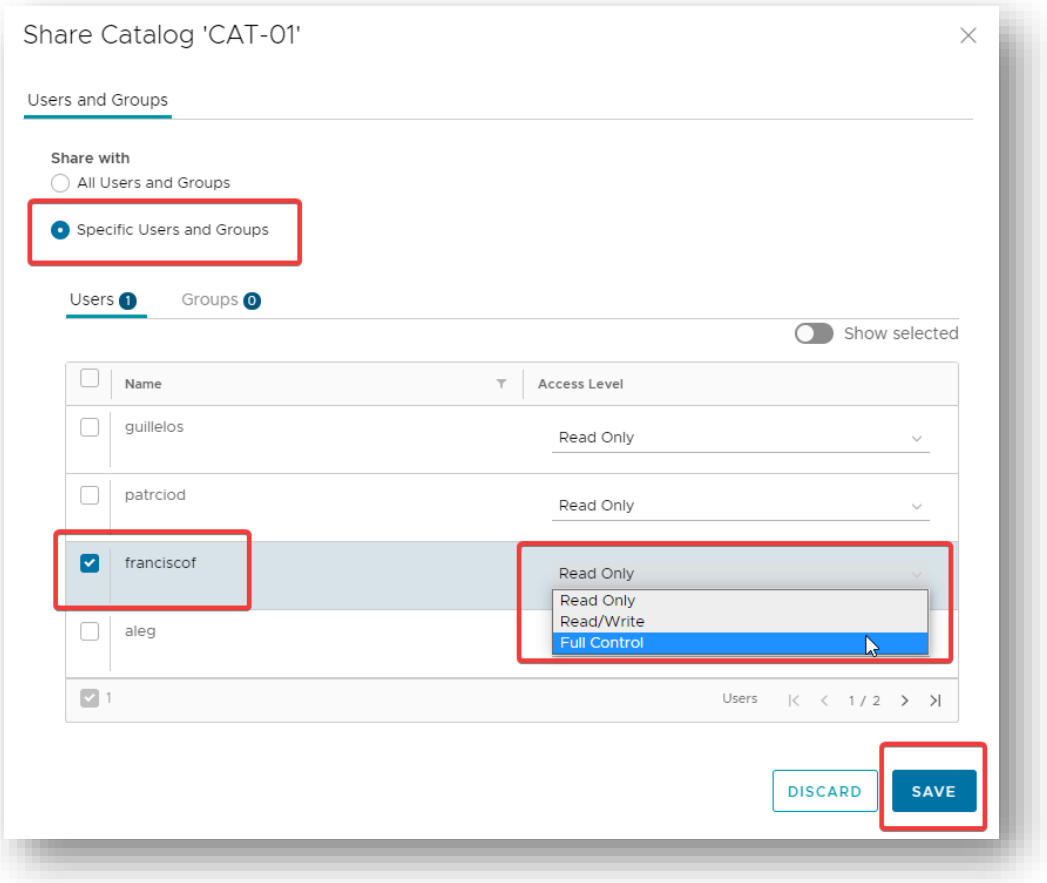


2. Select "Share" from the 3-dots menu



3. The following form will appear, select if you want to share with all users and groups or a specific member. You can also set the permission level assigned to the catalog. At the end of clicking on "Save"

    - Read-only
    - Read/ Write
    - Full Control

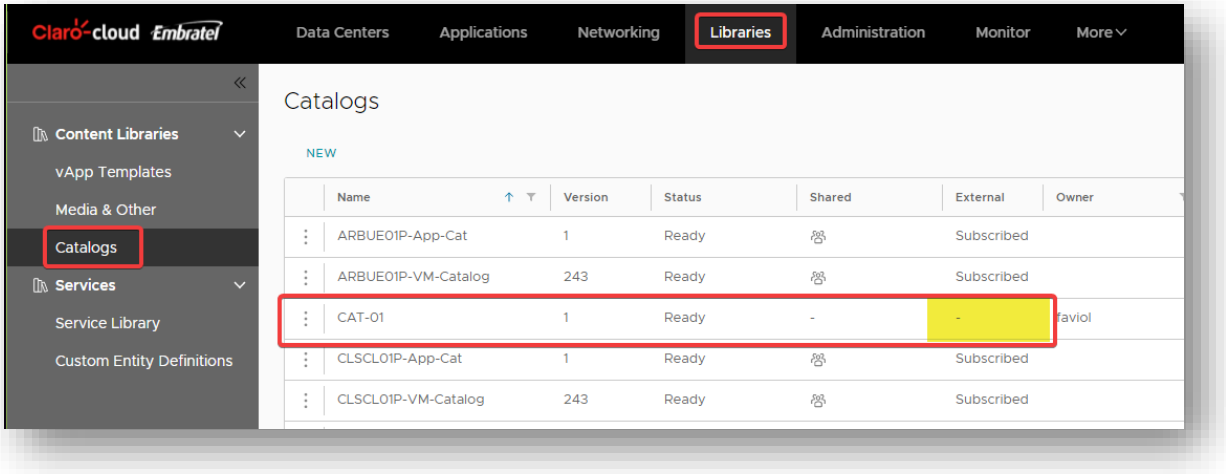


Delete a catalog

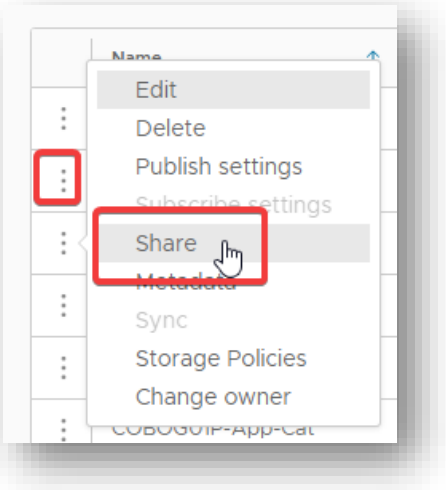
In the event that you need to delete any catalogs from your organization, follow these steps:

> **Important:**
>
> - If there is a template or media in the catalog, you must move these items to another catalog before deleting it.
> - Public catalogs added by default cannot be deleted

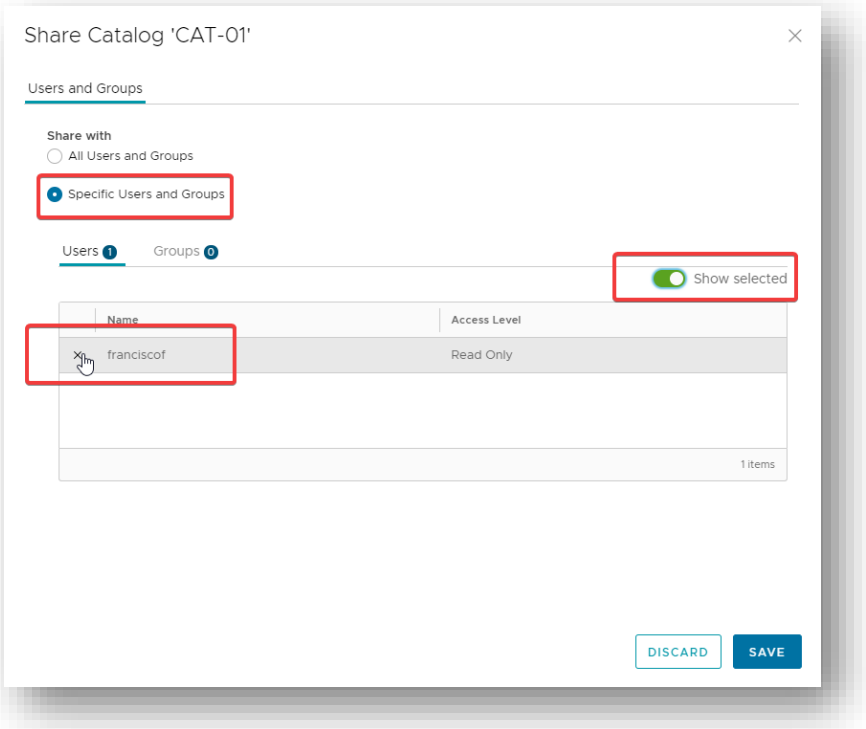
1. On the main menu click Libraries, then click Catalogs and verify that the catalog is not shared.



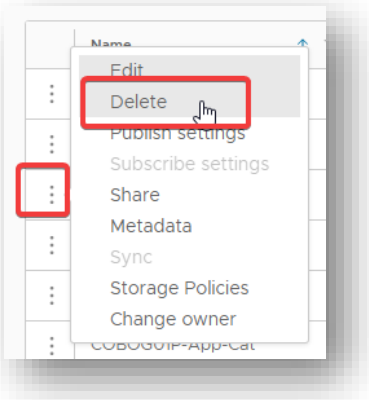
2. If the catalog is shared, select the "Share" option to be able to remove permissions from shared users

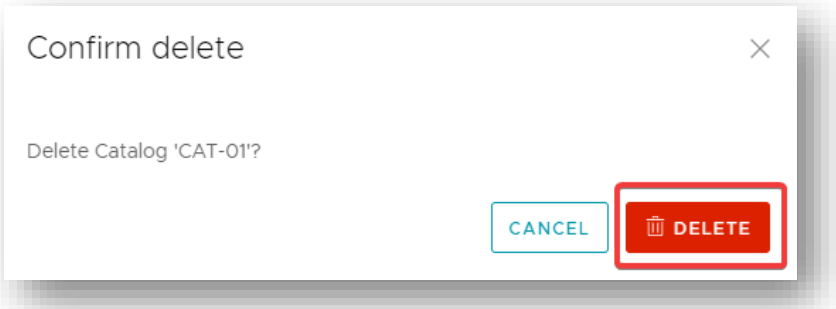


3. Select the Show Selection button to the right, to determine which user or group has permissions, click the "X" to remove, and then click "Save".



4. Once confirmed that the catalog is not shared, click on the 3-dot menu and click "Delete"





9. Create a Kubernetes cluster

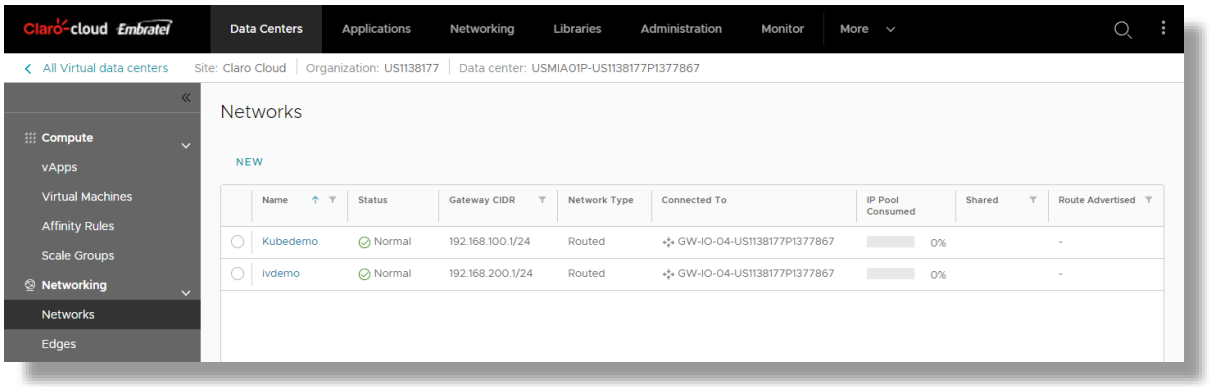
In this section you will find instructions for deploying Kubernetes clusters based on a VMware Tanzu Kubernetes Grid. If you do not have the plugin active, it is necessary to contact Claro Cloud technical support to enable it.

Prerequisites for installing a Kubernetes cluster

To create a Kubernetes cluster, you must pre-deploy the following:

Before you start the cluster provisioning process, it is important to implement the following steps:

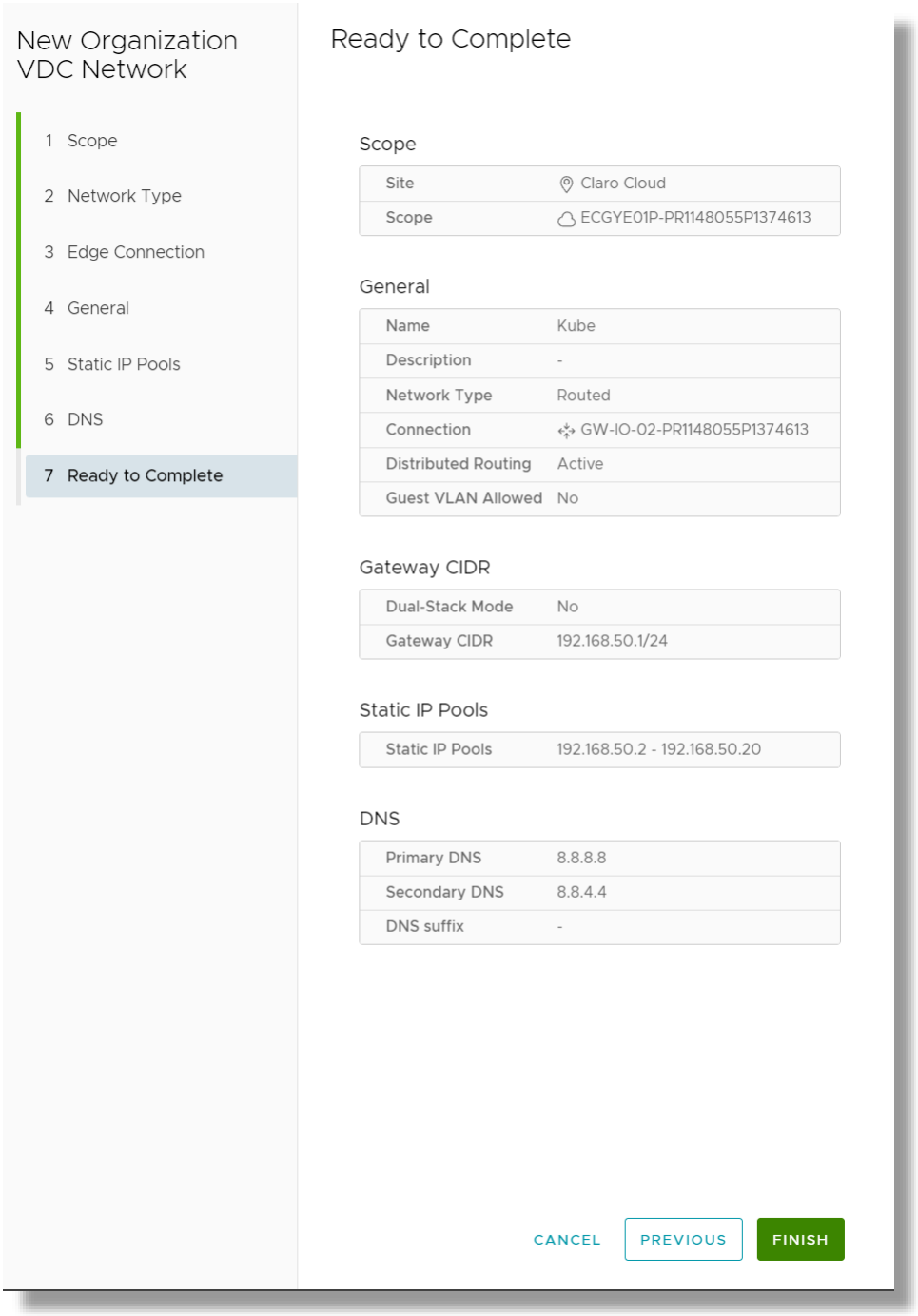
1. It is necessary to configure an additional "Routed" type network, with which the cluster and its nodes will be linked. Important, this network must have access to the Internet and the network name must not match any of the existing networks.
   1.1. Within the Data Center control panel, go to the Networks section, click on the "New" button



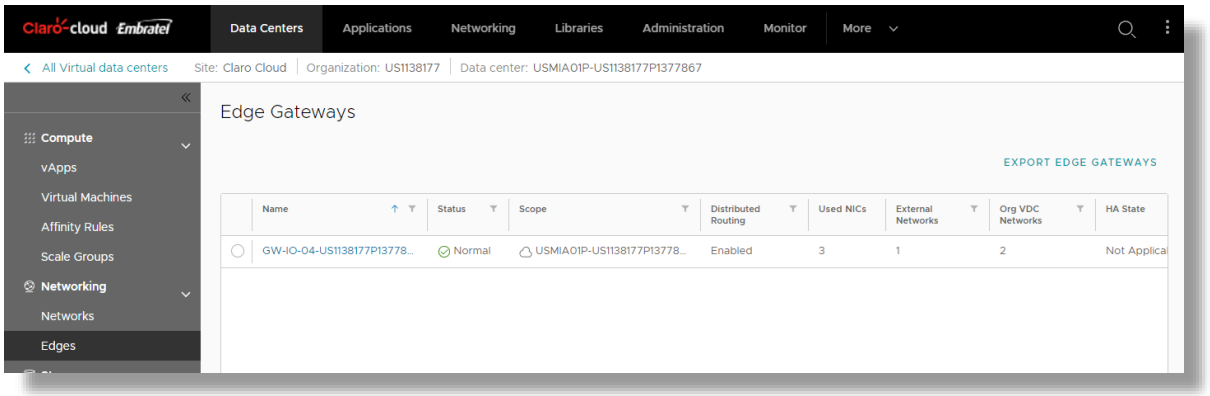
   1.2. Enter the following parameters

Item	Description
Scope	1. Select Organization Data Center 2. Select the Data Center where your Cluster will be provisioned
Network Type	Select "Routed"
Edge Connection	1. Select the Edge Gateway where the network will be created, this Edge must be hosted in the Data Center you previously chose 2. Leave "Guest VLAN Allowed" off
General	1. Enter the name of the network, **it must be different from any existing network** 2. Optionally enter a short description 3. Keep "Dual-Stack Mode" off 4. Enter an IP and network mask, which will serve as a Gateway within the network, e.g. 192.168. 50.1/24
Static IP Pool	Enter the static IP group to be assigned within the network, e.g. 192.168.50.2 – 192.168.50.20

DNS	Mandatorily, it is necessary to enter the primary and secondary DNS, in case of not having a specific service enter the following parameters: 1. Primary DNS: 8.8.8.8 2. Secondary DNS: 8.8.4.4 3. DNS suffix: leave blank

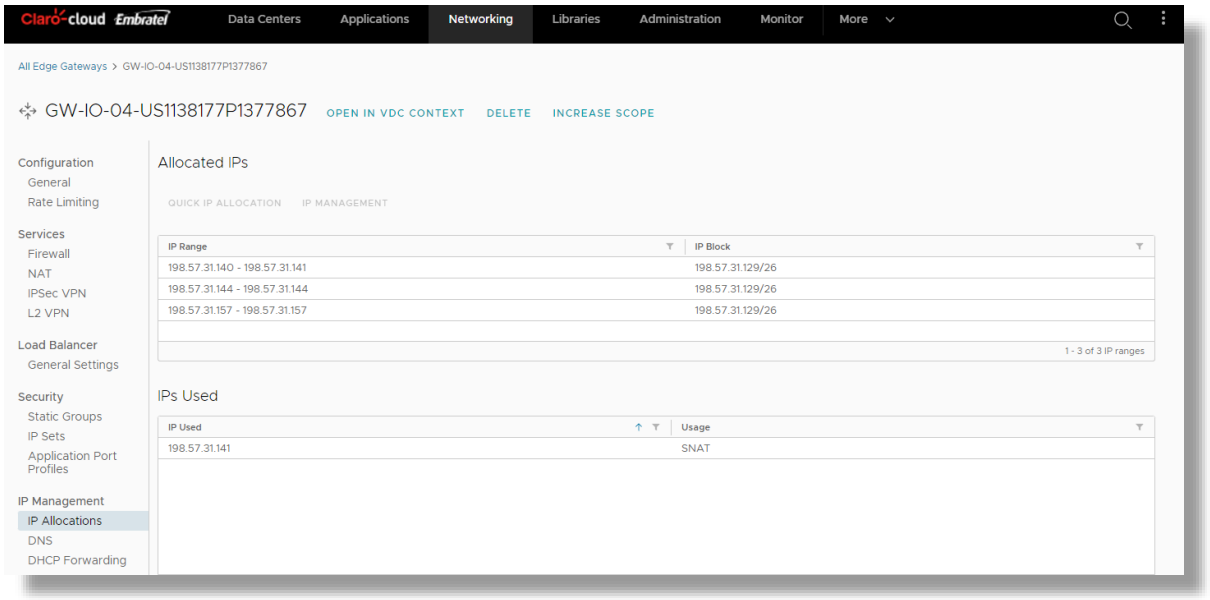


2. It is necessary to have at least 3 free public IPs, this because to validate the availability of your IPs follow the following steps:
   2.1. Enter the Networking section, click on the "Edge Gateways" section and select the Edge instance of the Data Center where you want to install the cluster

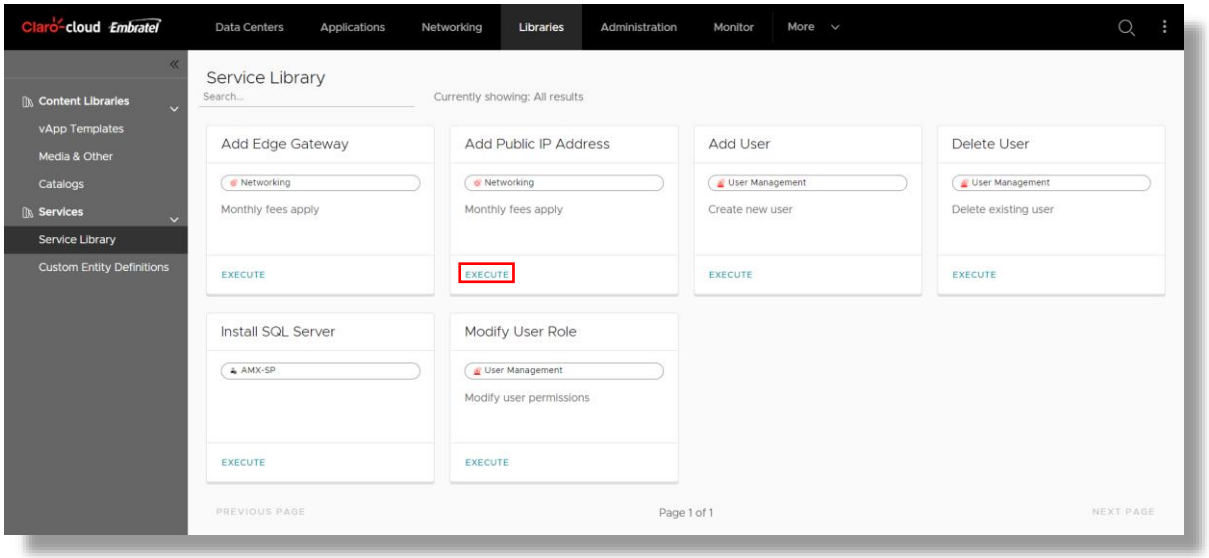


   2.2. By clicking on the IP "Allocation" option in the "IP Management" section, the following information will be displayed:

Item	Description
Allocated IPs	this section lists all public IPs hosted on your edge instance
IPs Used	this section shows which public IPs are in use and what task it is being used for



   2.3. If you do not have unused public IPs, enter the "Libraries" section and click on the "Service Libraries" option, in the box that says "Add Public IP Address" by clicking on the "Execute" button

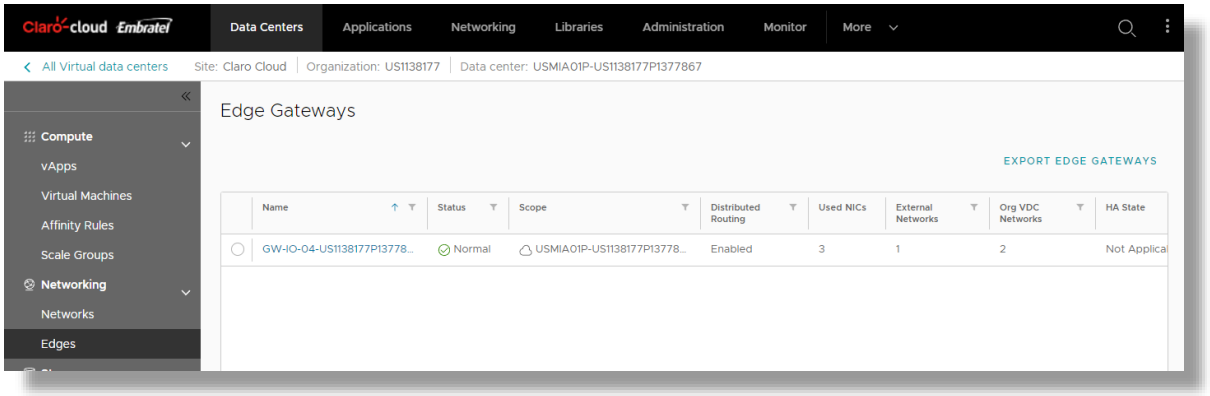


2.4. A box will open where you must enter the Edge Gateway to which you want to add new IPs and the number of Public IPs you want to add (at least 2, one IP will be occupied for the configuration of an SNAT and the second is required to be left free to associate it with the cluster during the provisioning process)

> **Important:** For each cluster that you want to configure, you must have a public IP available

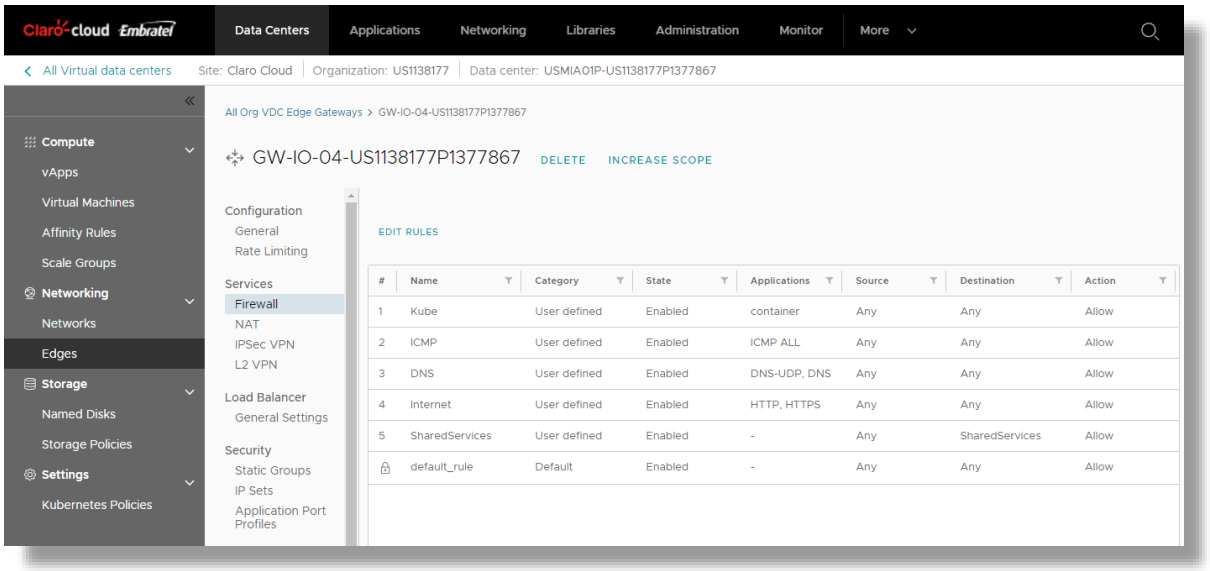
3. Enable firewall rules to allow traffic to the created network (step 1) to the Internet through ports 443, 80, and 6443.

3.1. Go to Data Center, click on the "Edge Gateways" section and select the Edge instance of the Data Center where you want to install the cluster



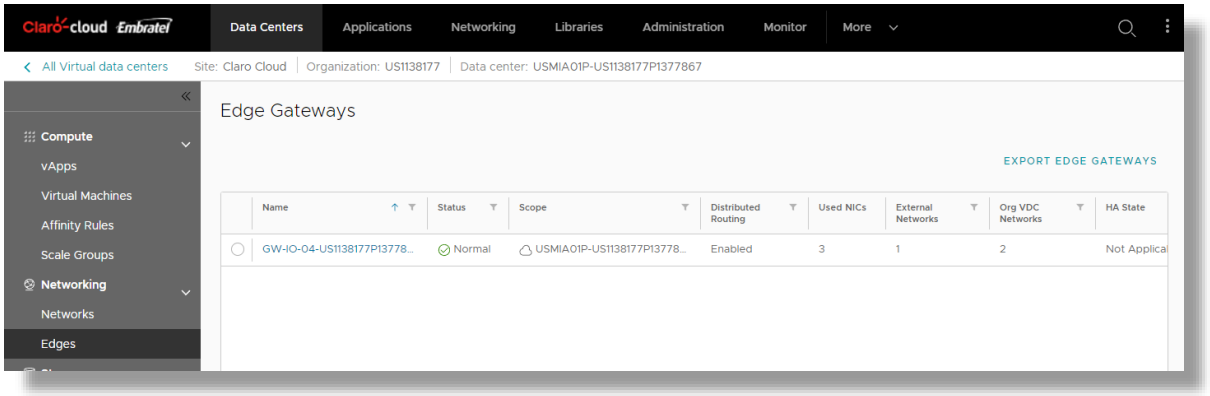
3.2. Select the option of "Firewall" and click on the "Edit Rules" button, add a policy where traffic is allowed through ports 443, 80 and 6443, for more details on how to configure a firewall rule see the following section "Configuring Firewall rules"

> **Note:** It is advisable to have the following protocols enabled: DNS, ICMP

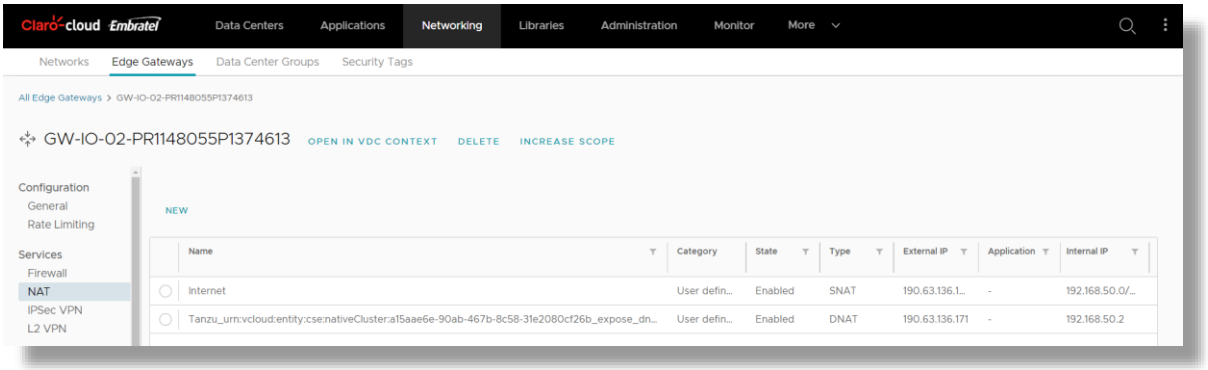


> **Important:** Ports are listed as applications, so port 443 is categorized as HTTPS, port 80 as HTTP and port 6443 as it is not a known port, it is necessary to configure a new profile, see the section "Configuration of application port profiles"

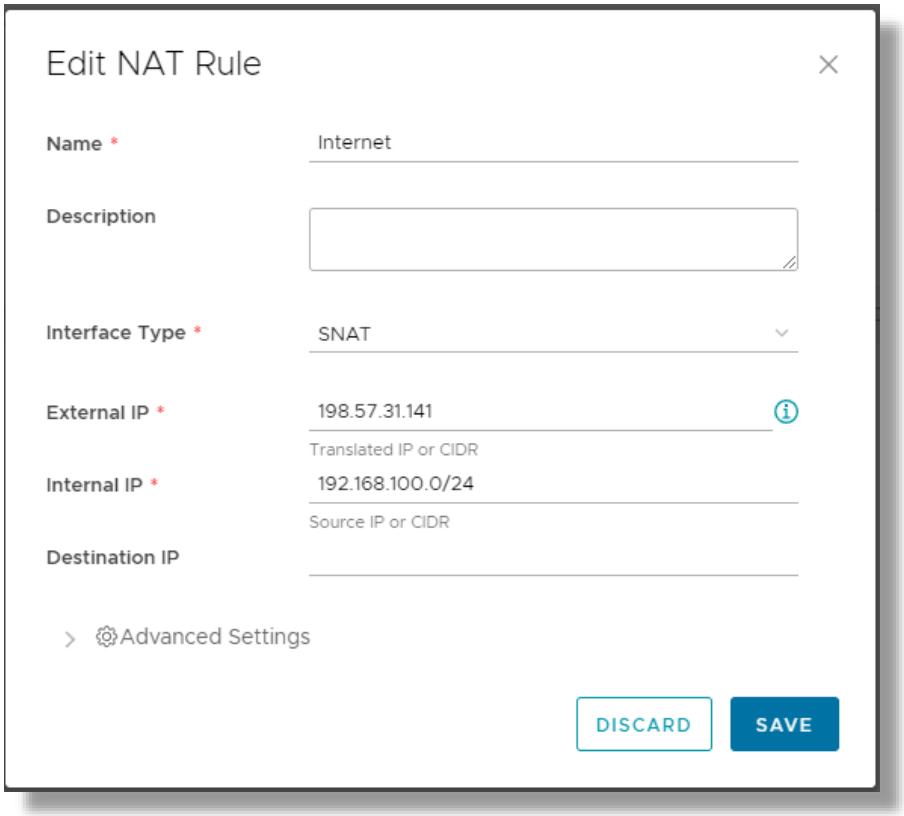
4. Enable SNAT rule to allow traffic to the Internet, it is important to consider that it is not possible to use 0.0.0.0/0 as an internal network, it is necessary to enter the segment of the specific VLAN.
   4.1. Go to Data Center, click on the "Edge Gateways" section and select the Edge instance of the Data Center where you want to install the cluster



4.2. Select the option of "NAT" and click on the "New" button

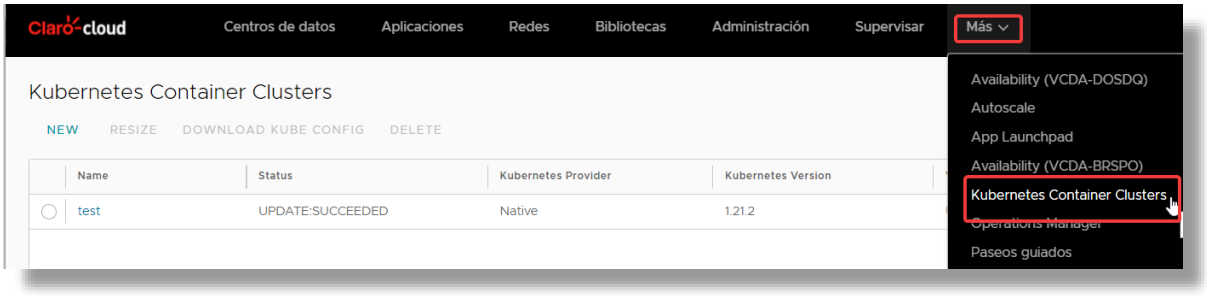


4.3. Add a rule of type SNAT, where the External IP parameter is the public IP to be assigned to the cluster, the Internal IP must be the segment of the routed VLAN that will be destined for the cluster configuration.

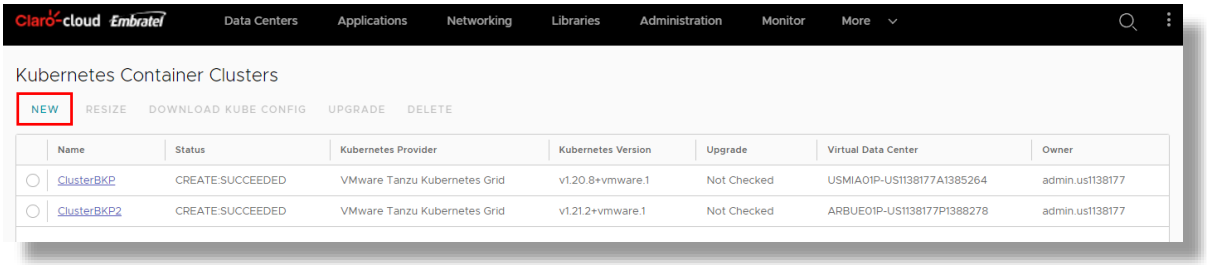


Create a Kubernetes cluster

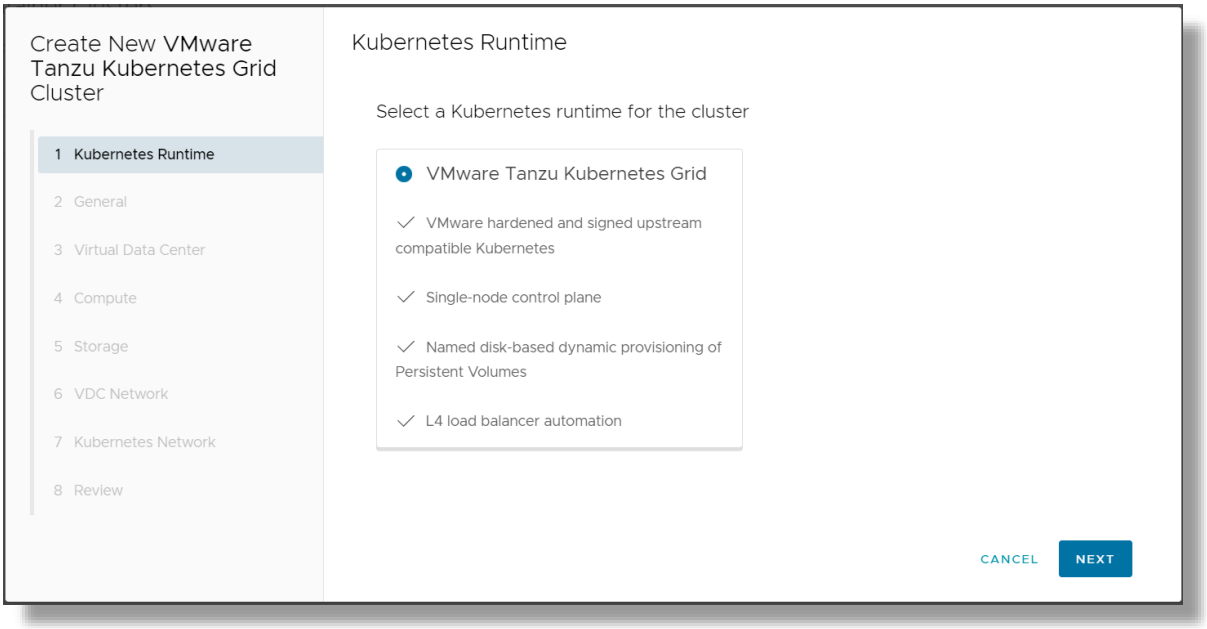
1. In the main menu, select the "More" option, in the submenu choose the option "Kubernetes Container Cluster"



2. To start deploying a new cluster click "New"



3. The following screen will be displayed, click on "Next" to start the configuration

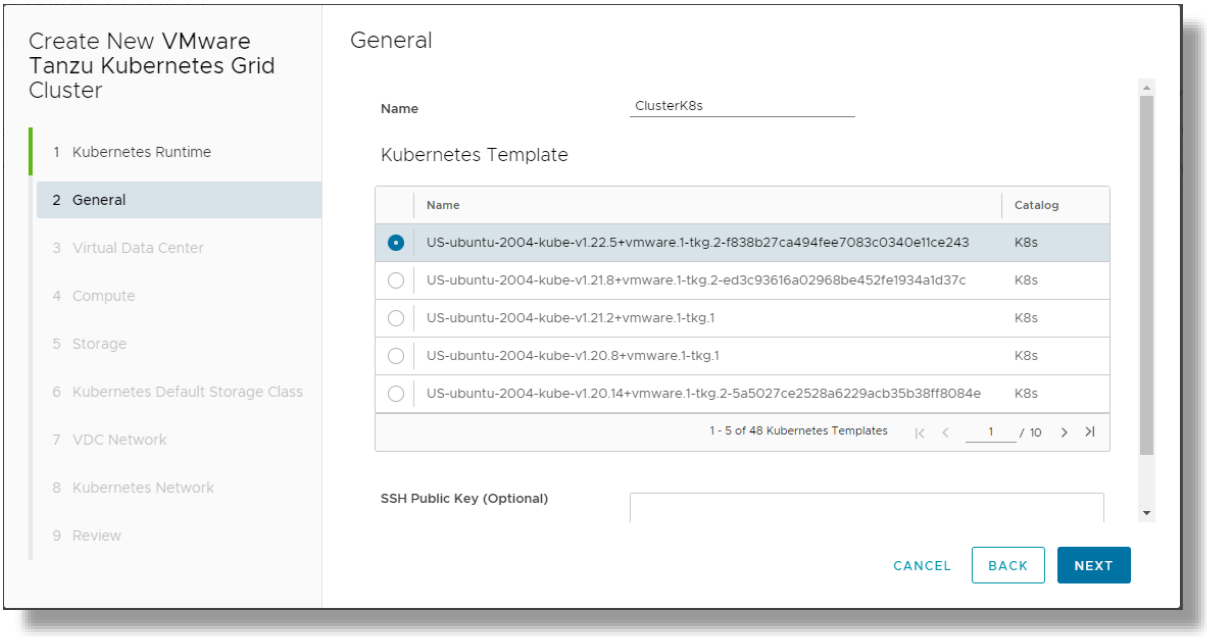


Important: The base configuration of a VMware Tanzu Kubernetes Grid Cluster through the control panel can only have 1 Master node and "N" number of Workers nodes.

It is possible to add more master nodes through APIs

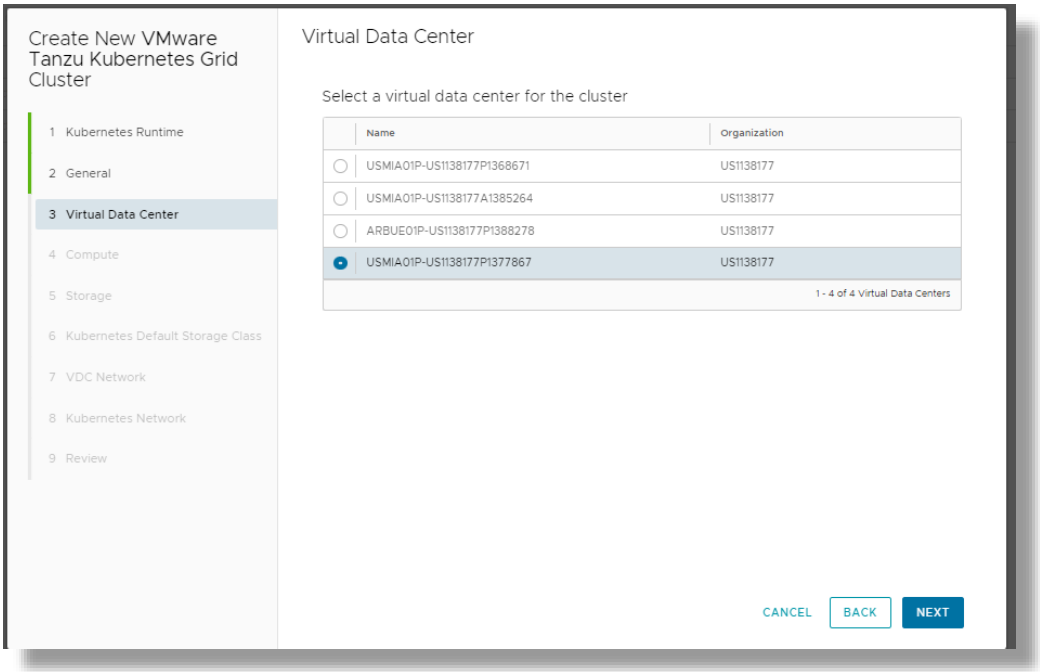
4. In the General section, you must specify the cluster name and operating system version with which all nodes within the cluster will be deployed. At the end of clicking on "Next"

Important: The **template** to be selected **must belong to the same country where your Data Center is hosted**. At the beginning of the name of each template you have a prefix of each country



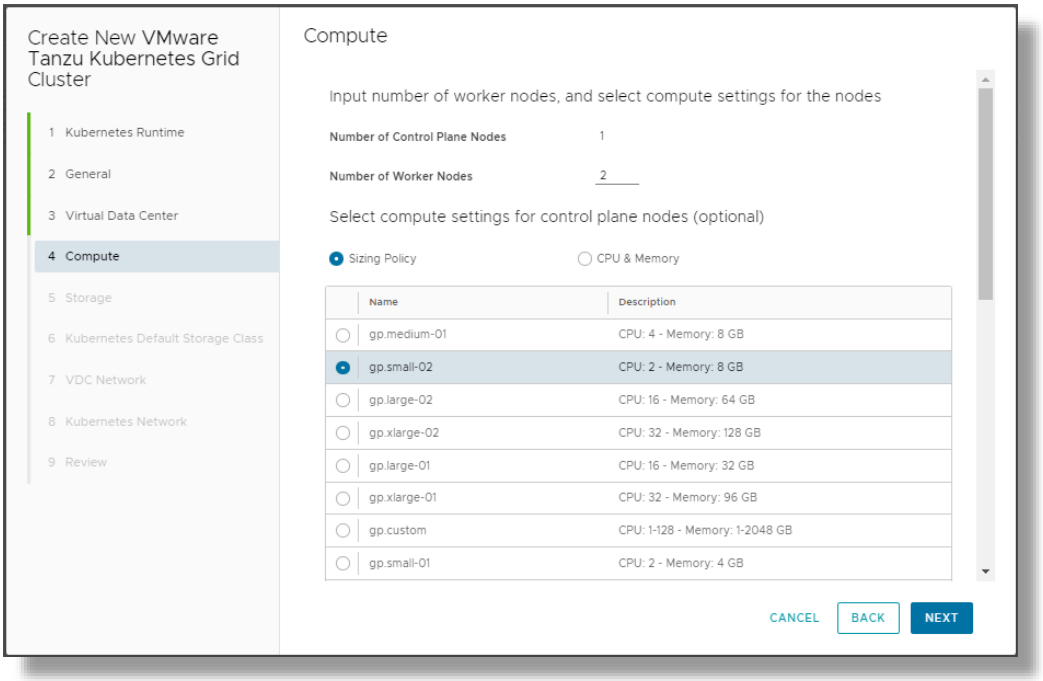
Note: In the "Name" column you can see the Kube version integrated into the template.

5. Select the Data Center where the cluster will be deployed, click on "Next"



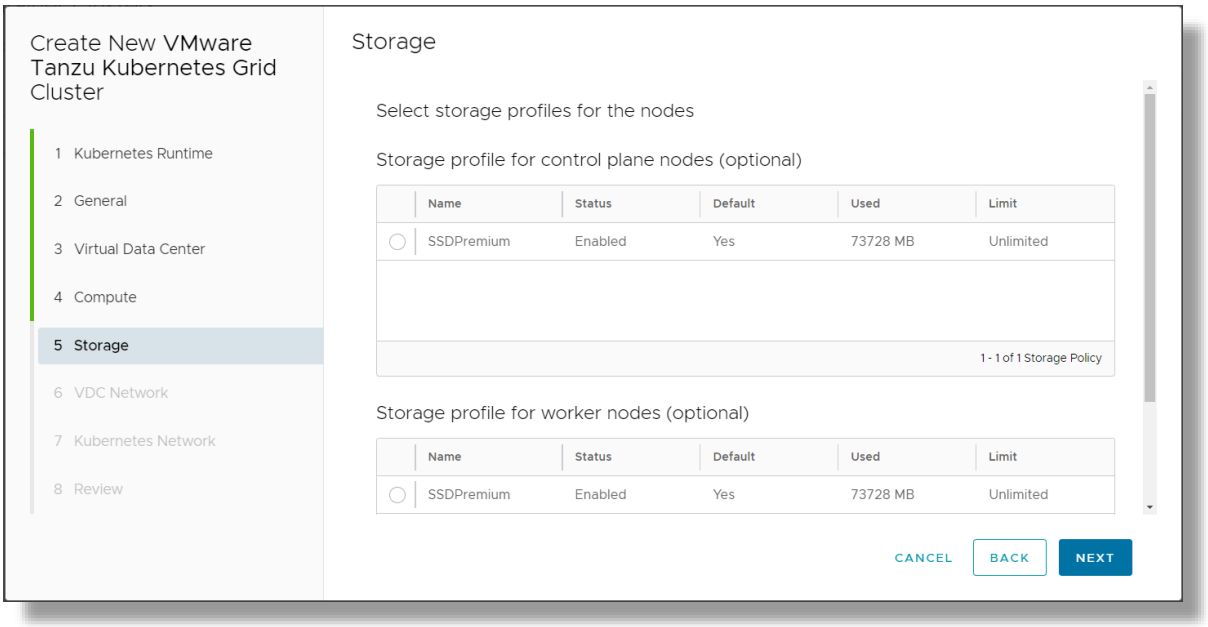
6. Define the number of worker nodes that will be provisioned within the cluster, as well as the size of both Control Plane and Workers nodes. At the end of clicking Next

Important: Node sizes should not be less than 2 vCPUs and 4 GB RAM



Note: Workers nodes are created the same size, we can vary the size within the cluster creation process

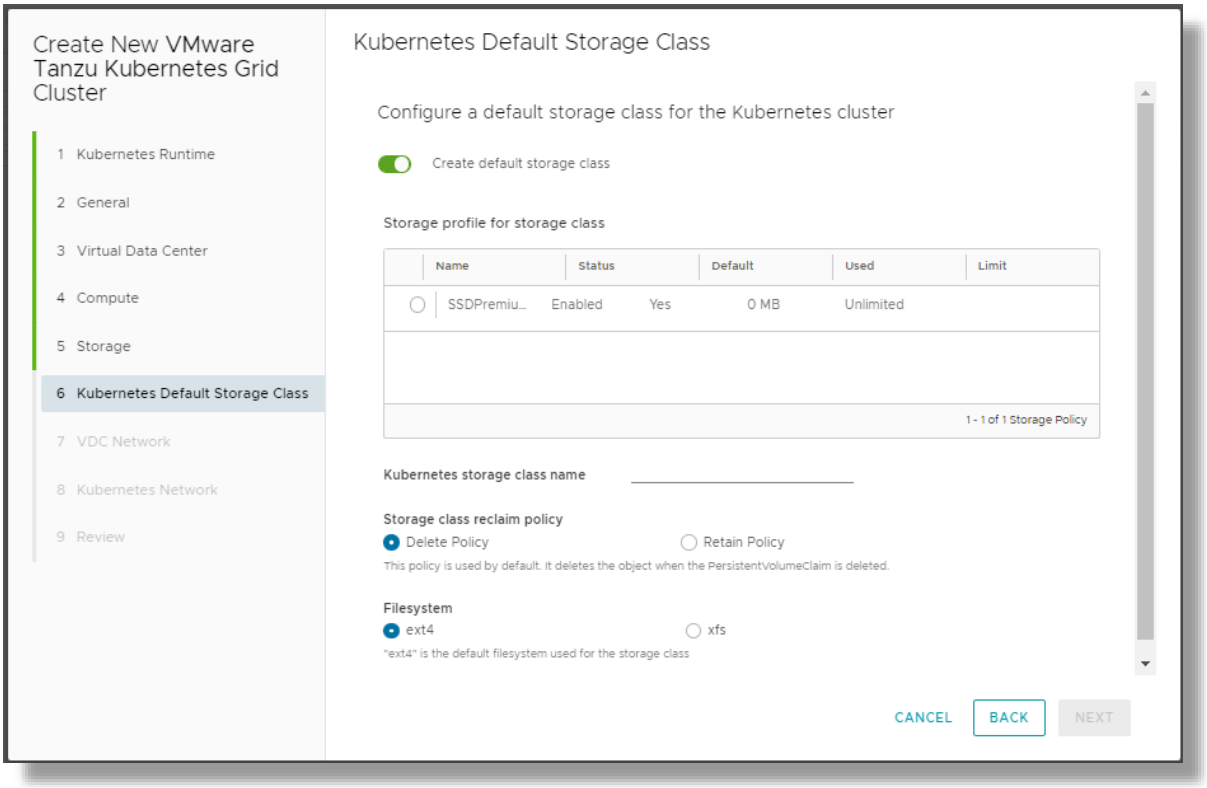
7. Enterprise Claro Cloud has high-performance SSD disks, so it will assign this storage policy by default. At the end of clicking on "Next"



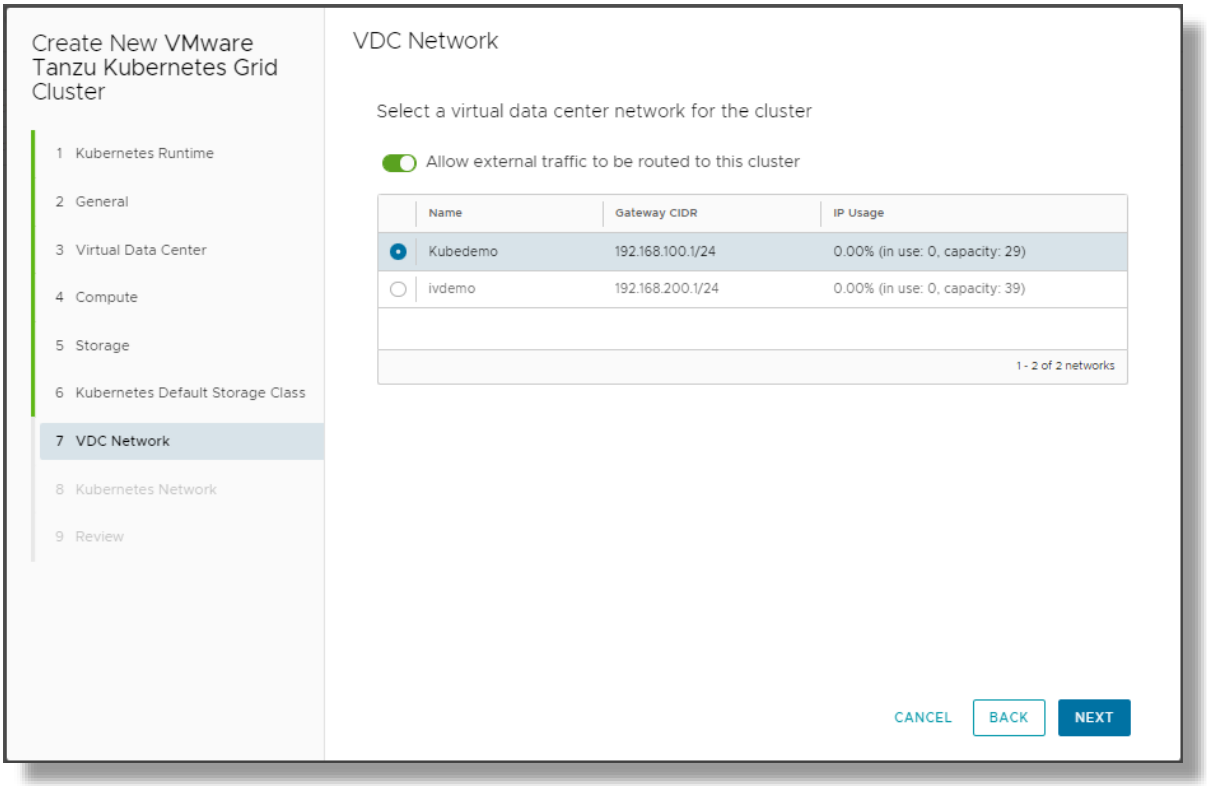
8. In "Kubernetes Default Storage Class" section, enter the following. At the end of clicking on "Next"

Item	Description
Storage profile for storage class	Select Premium SSD

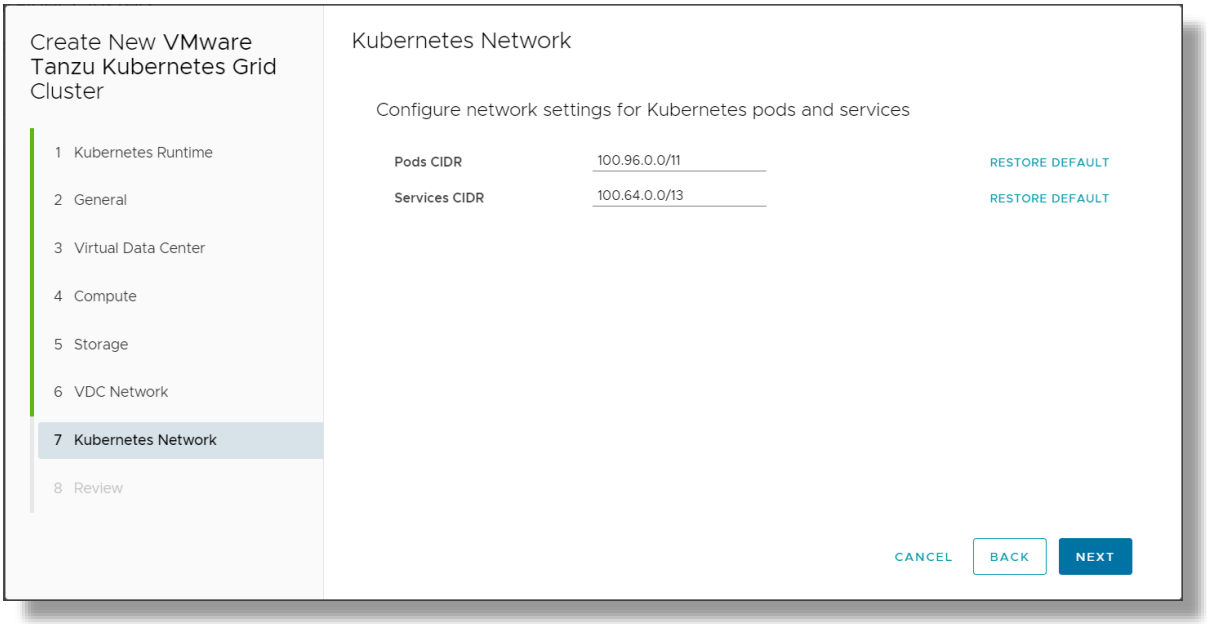
Kubernetes storage class name	Enter the name of the storage class
Storage class reclaim policy	• Delete Policy – During the cluster erasure process, storage is included • Retain Policy – If a cluster is allocated separate disks, it does not delete any volumes at the time of deleting the cluster Recommendation keep "Delete Policy" selected
Filesystem	Select format type



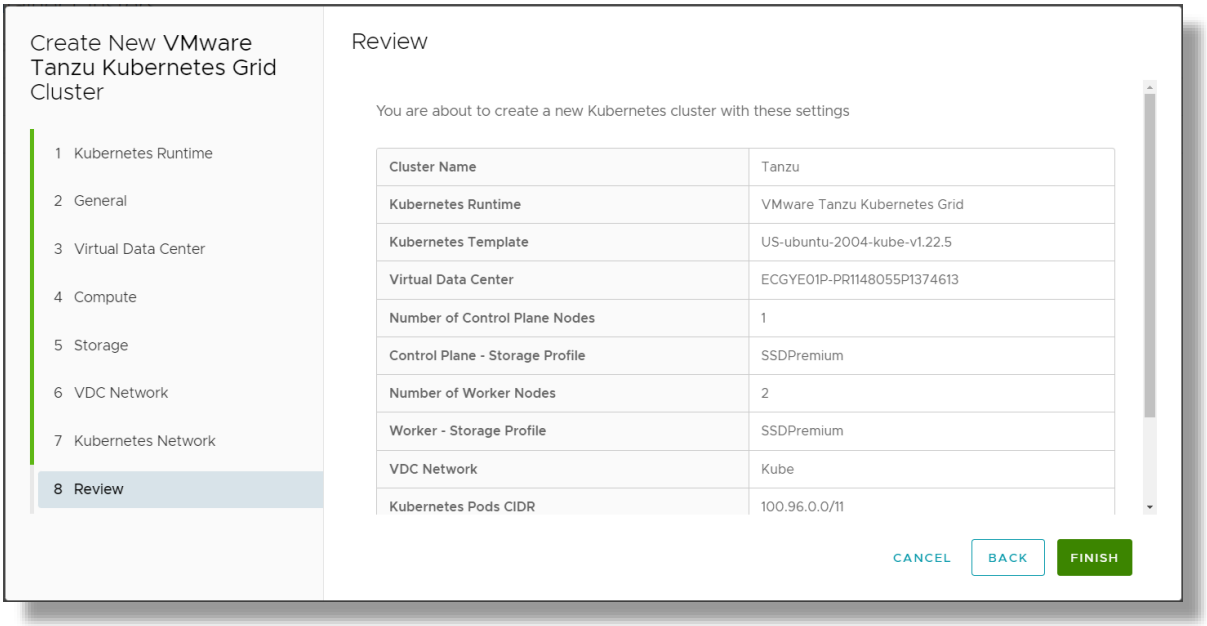
9. Select the network previously created at the beginning of this process, as the main feature, this network must have output to the Internet. At the end of clicking on "Next"



10. The internal networks that will be assigned to the cluster will be displayed, keep the default parameters.

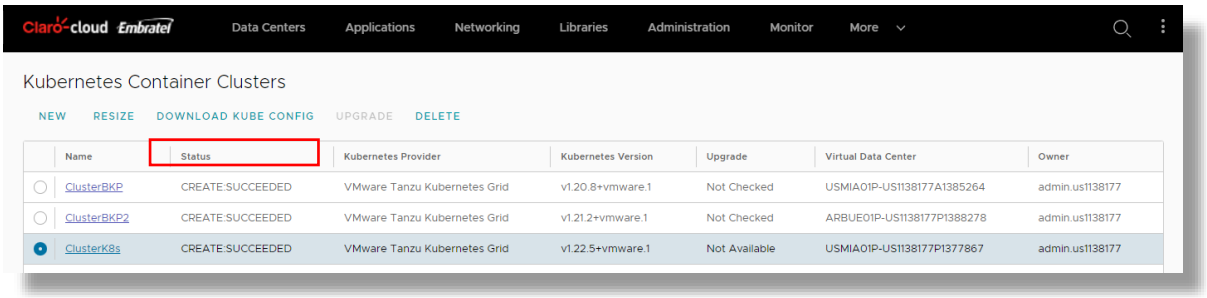


11. A summary with the cluster configuration will be displayed by clicking on "Finish"



Kubernetes Cluster Access

1. Once the creation process is finished, select your cluster and click on "Download Kube Config", this file contains the necessary information for you to enter your cluster.

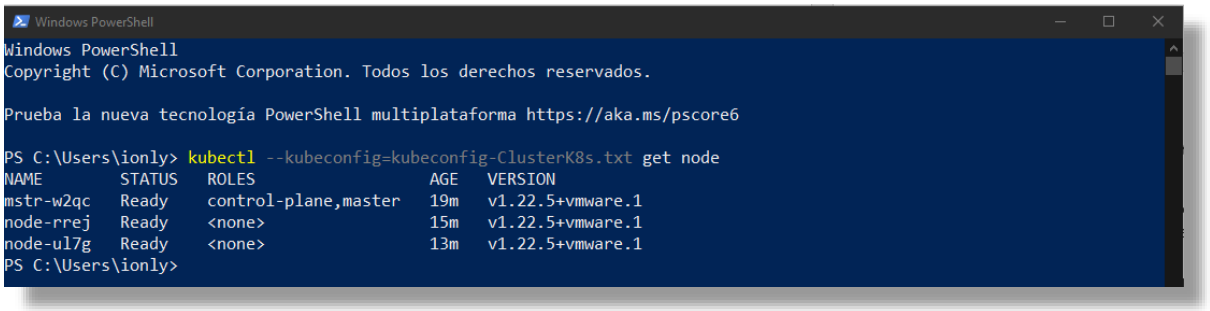


2. It is necessary to download the Kubectl package to your computer, then links to the installation process according to each operating system:

- Windows - https://kubernetes.io/docs/tasks/tools/install-kubectl-windows/
- MacOS - https://kubernetes.io/docs/tasks/tools/install-kubectl-macos/
- Linux - https://kubernetes.io/docs/tasks/tools/install-kubectl-linux/

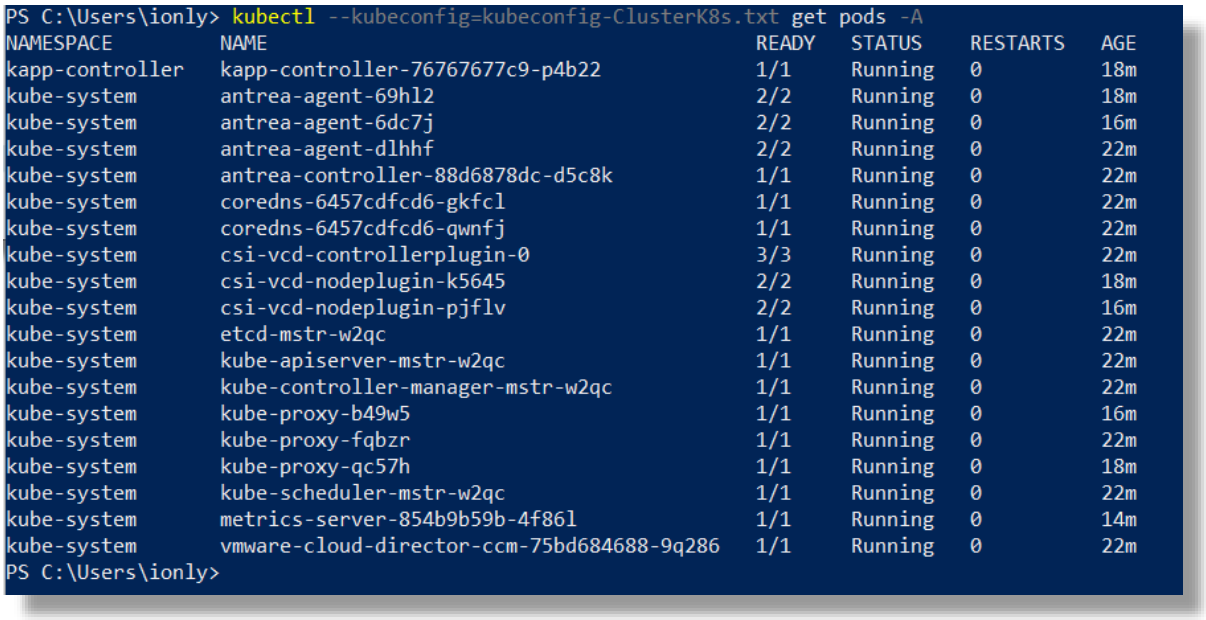
2.1 Once Kubectl is installed, the client will be able to enter through the Kubeconfig file, to validate the nodes of its cluster and excute the command

Kubectl --kubeconfig=< Name_of _the _downloaded_file.txt> get node



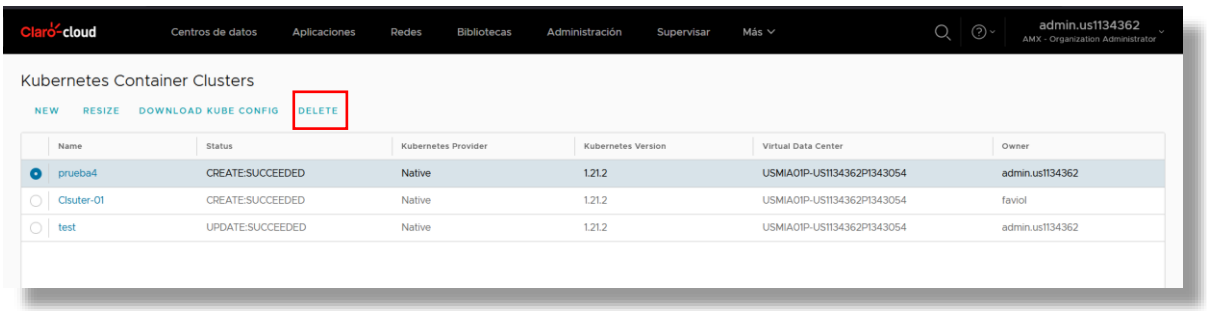
2.2 To display the status of your pods, run the command

Kubectl --kubeconfig=< Name_of _the _downloaded_file.txt > get pods

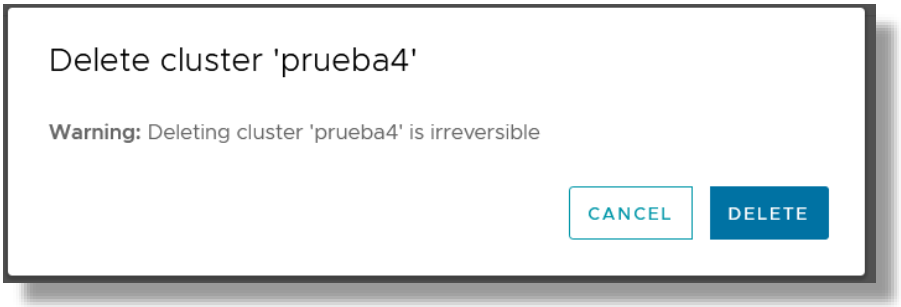


Delete a Kubernetes cluster

1. To delete the cluster, just select the cluster to delete and click "Delete"



2. Confirm the deletion, click on "Delete"

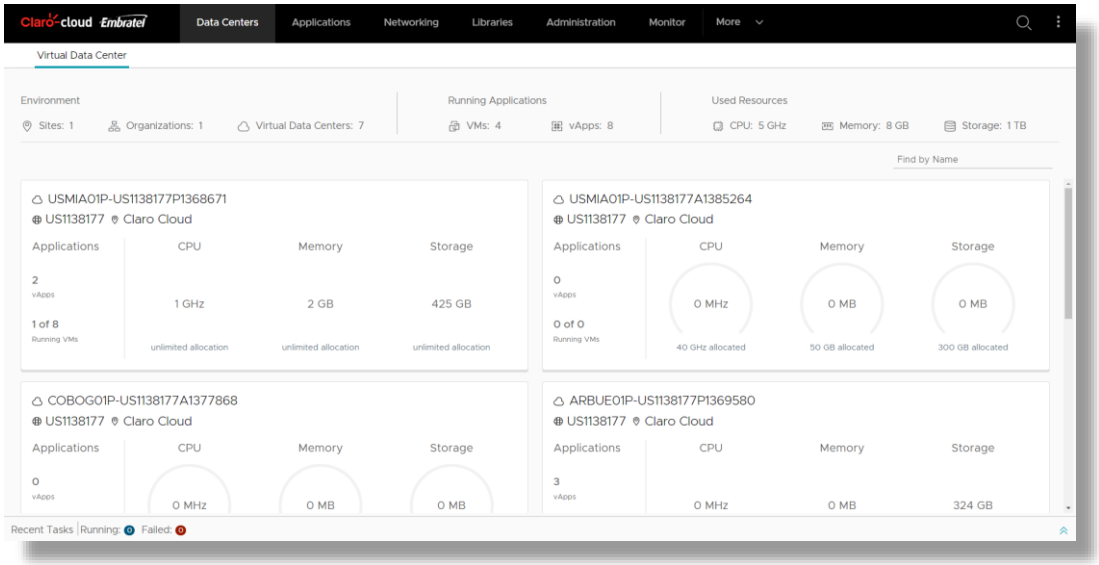


10. Scale Groups (automatic horizontal scaling)

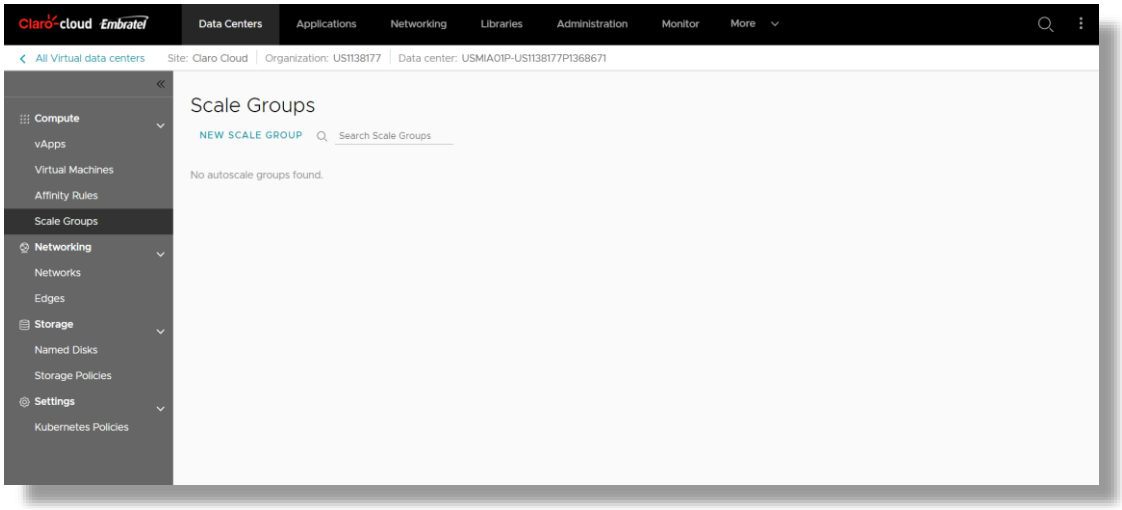
This section will show you the process for configuring scale-out, which will allow you to mitigate workload loads on your infrastructure by automatically adding virtual machines as your application requires.

> **Important:** It is important to ensure that the application is adapted and optimized to support automatic scaling.
>
> Additionally, if you want to implement scaling on an already provisioned machine, it is necessary to first create a template. (see how to create a template)

1. Select "Data Center" from the main menu, choose the Data Center where automatic scaling is required.

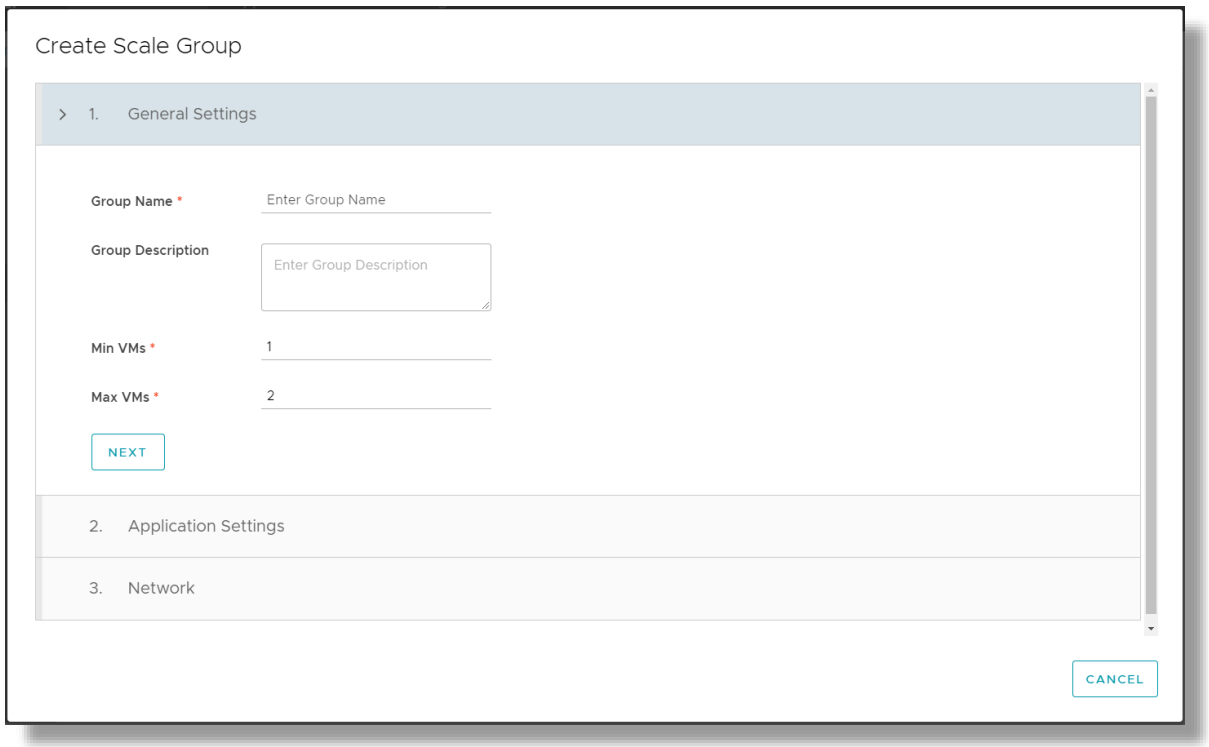


2. Choose "Scale Groups" in the secondary menu within the Data Center, click on "New Scale Group"



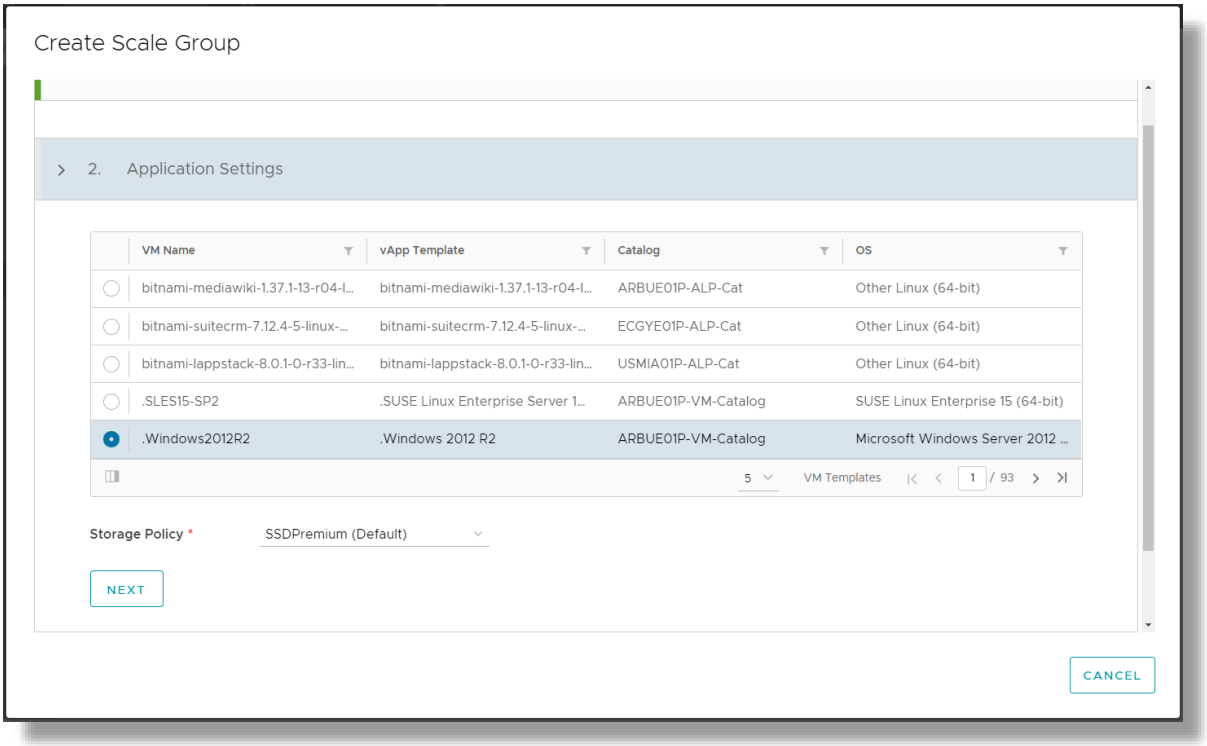
3. The following General Settings screen will open where you must enter the following information, at the end of clicking on "Next"

Item	Description
Group Name	Enter the name of the scale group
Group Description	Optionally enter a short description of the scala group
Min VMs	Enter the minimum number of VMs your scale group can have.
Max VMs	Enter the maximum number of VMs your scale group can have.



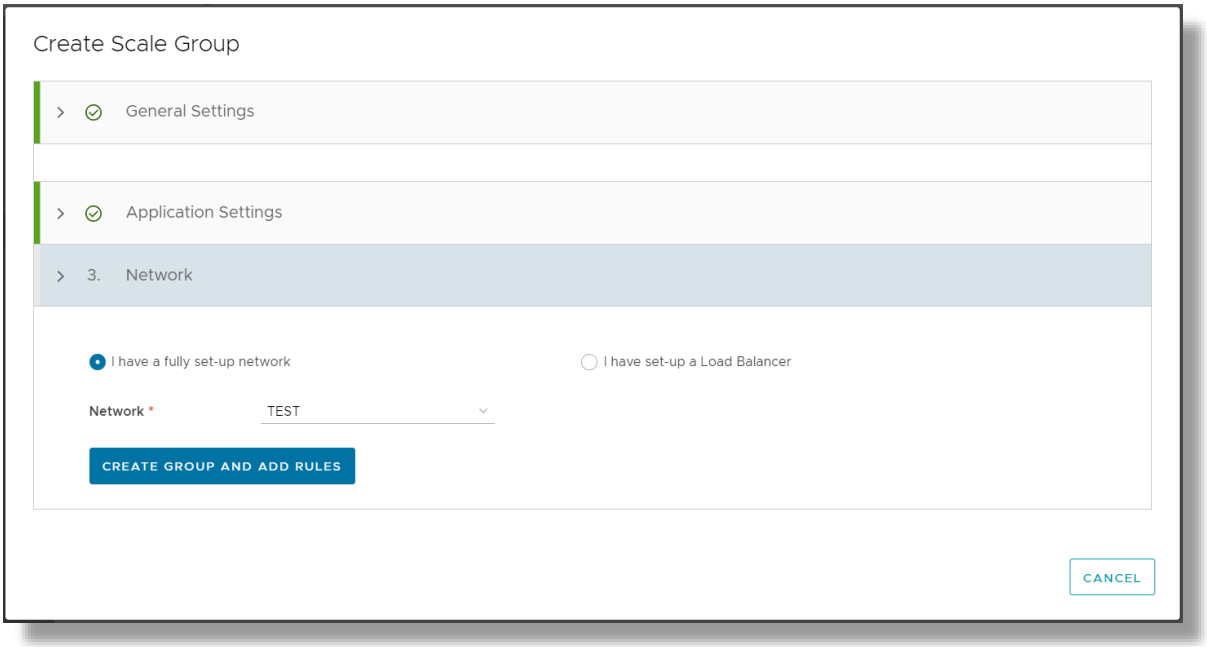
4. In the Application Settings section enter the following information, at the end of clicking on "Next"

Item	Description
Template	Select the template that the group will take as a reference to create the new nodes. Remembering that the new nodes are a faithful copy of the base template.
Storage Policy	Select the type of storage to be allocated to the new virtual machines (only SSD storage is currently available)

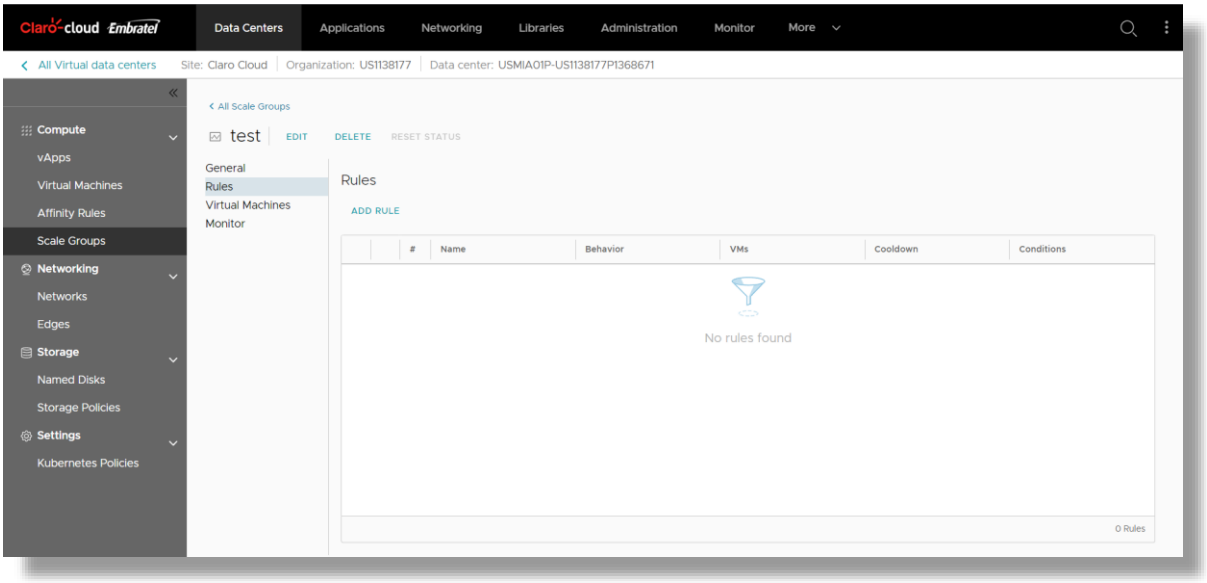


5. In the Network section choose the means by which you will link the VMs within the scale group, when you finish clicking on "Create group and add rules"

Item	Description
I have a fully set-up network	Select the network within the data center to which the scale group will be linked.
I have set-up a Load Balancer	If you have the Load Balancing service, you can link your scale group through a balancing pool, just enter: • Network CIDR – IP of the gateway within the balancing pool • Edge Gateway – The Edge gateway where the balancing service is hosted. • Server group – Select the balancing pool to which you want to link the scale group



6. Once the Scale Group is created, the following screen will open where you can create your scaling rules, by clicking on "Add rule"

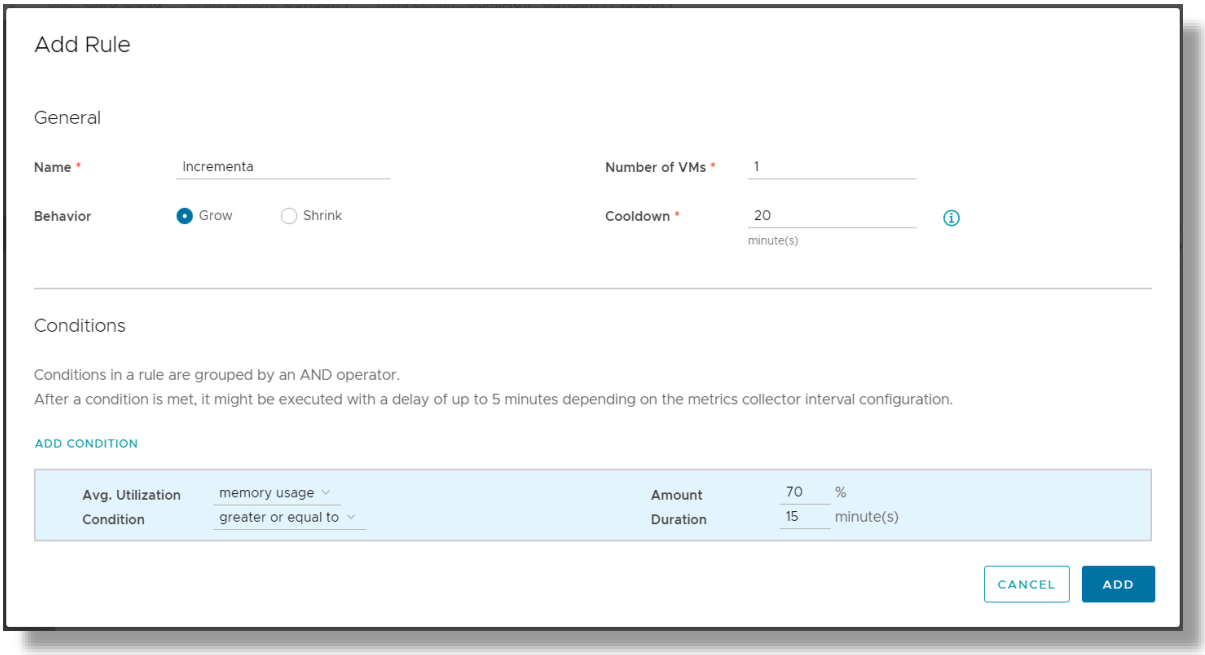


7. The next screen will open where you will have to enter the following information, at the end of clicking on "ADD"

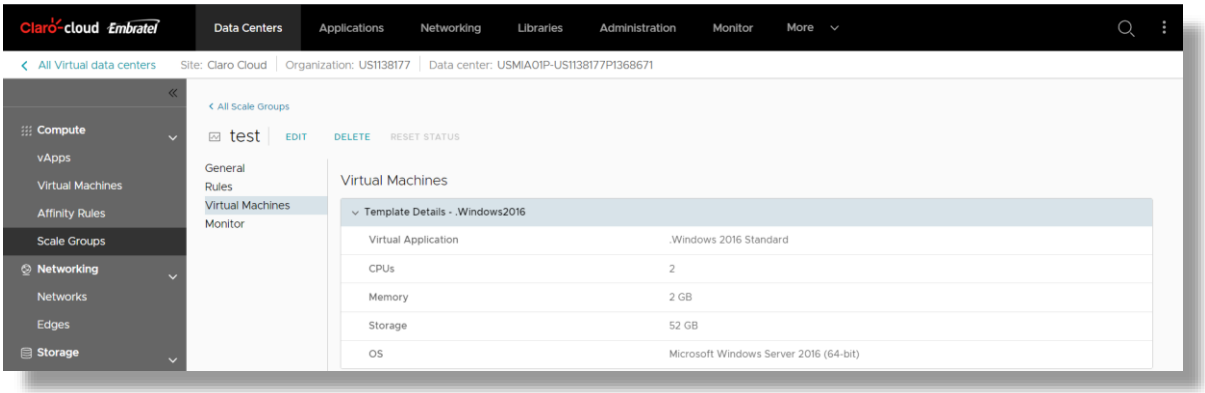
> **Note:** You will be able to enter the number of policies and conditions required by your application

Item	Description
Name	Enter the name of the rule to be created.

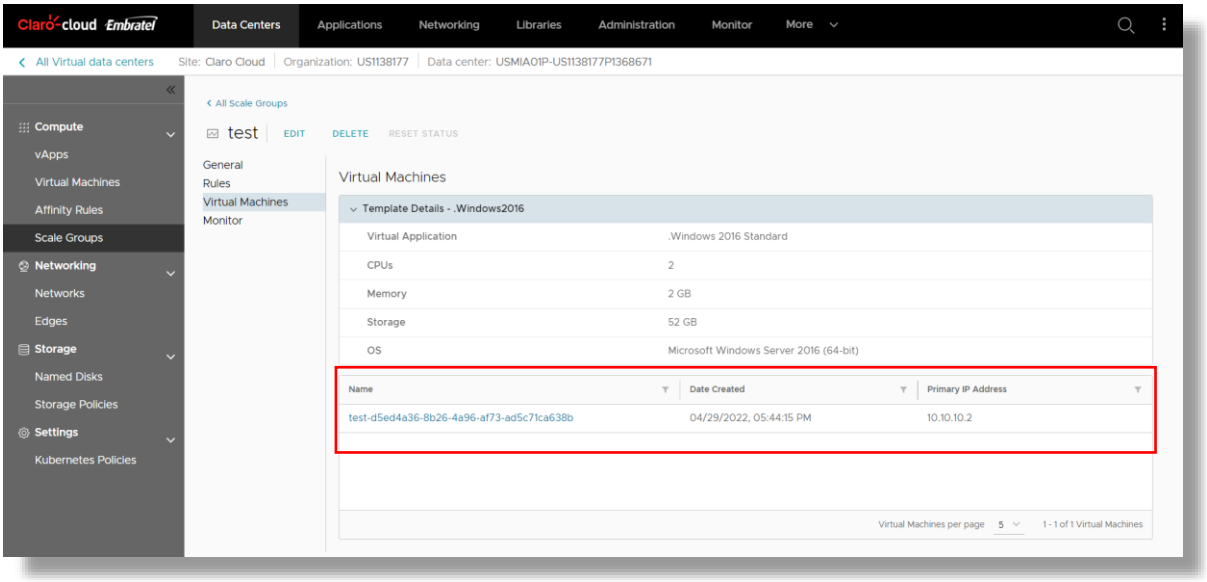
Number of VMs	Enter the number of VMs you want to create and/or delete when scaling goes live.
Behavior	Select the action you want to apply when scaling: Grow or Shrink.
Cooldown	Define the time in minutes it will take for the platform to assess whether any policies are being met.
Avg. Utilization	Choose the virtual machine component(s) to evaluate.
Condition	Choose the condition that must be met for scaling to be activated.
Amount	Enter the percentage of usage to be met for the condition to be met.
Duration	Enter the time you require the condition to be met in minutes



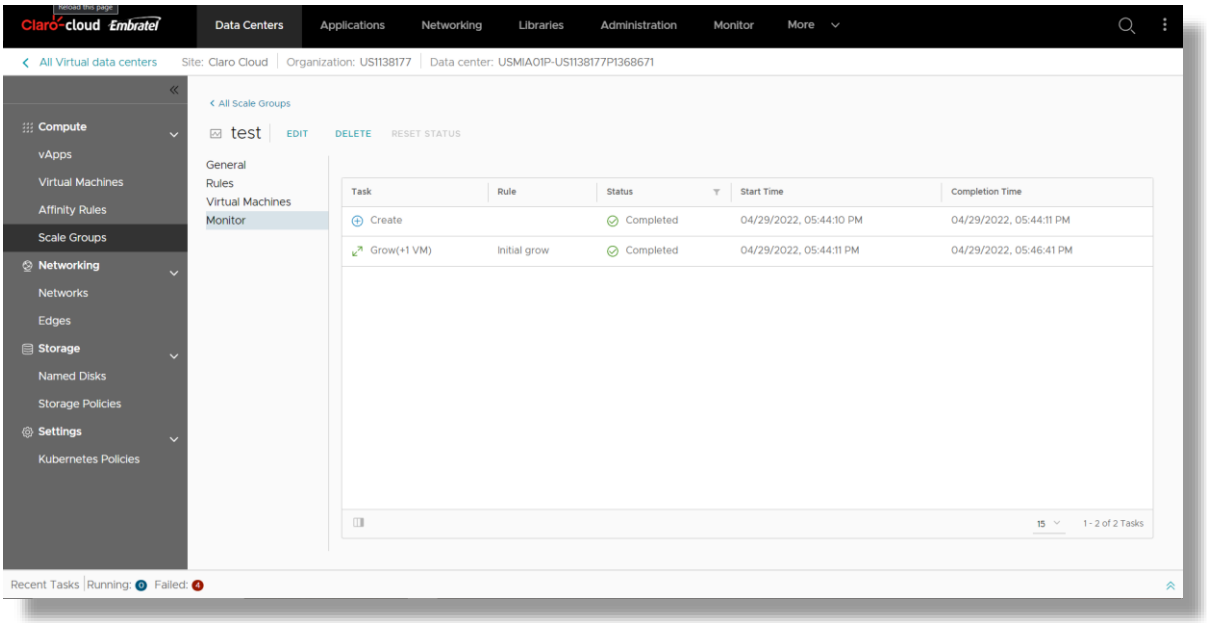
8. For the visualization of the virtual machines within the click scale group in the "Virtual Machines" section, here you can see the main features of the template with which the virtual machines will be created automatically.



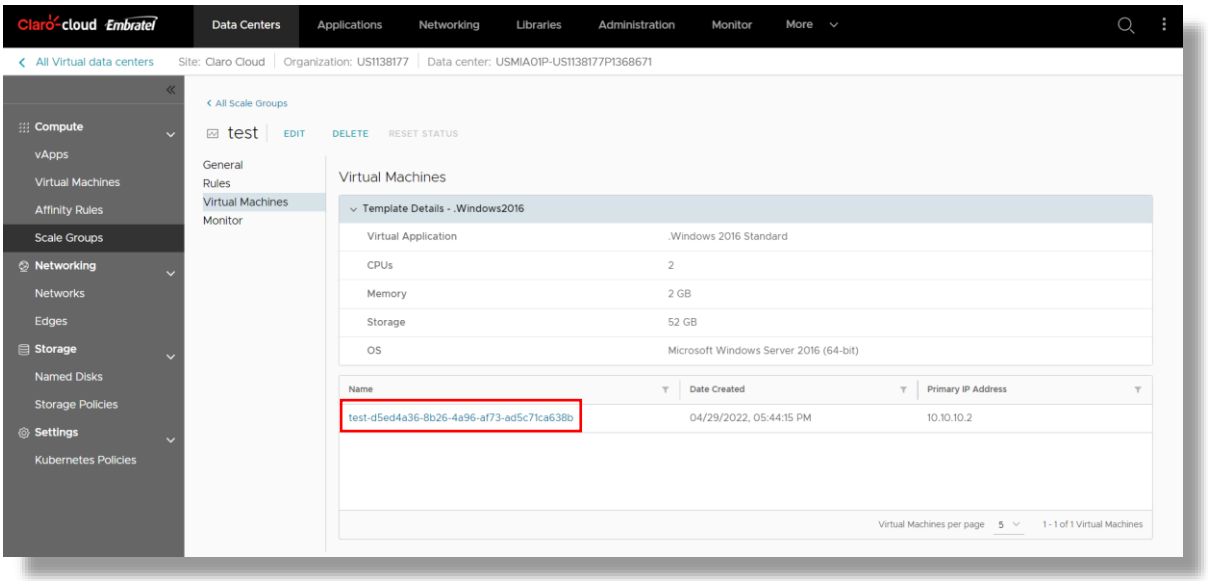
9. Likewise, you can view the complete list of virtual machines provisioned at the moment, by default when creating the group the first virtual machine in the group is automatically provisioned.



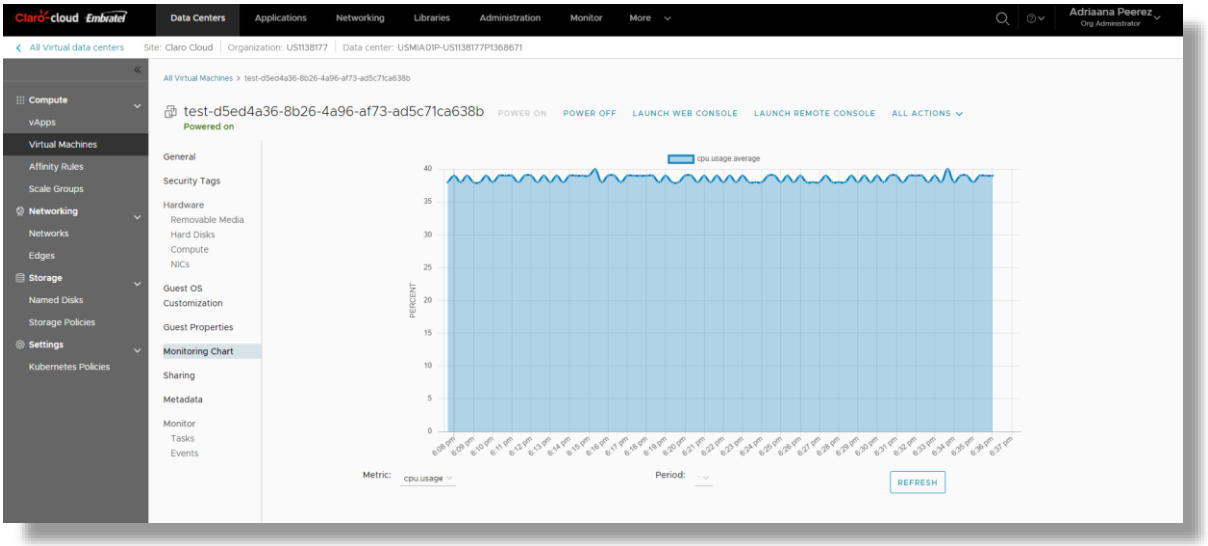
10. In the Monitor section, you can view each action executed in the group, the applied rule, the status of the task, the date it was executed, and the date the task ended are recorded.



11. You will be able to monitor the consumption of each resource in your virtual machines through the usage board, enter the "Virtual machines" section by clicking on the name of the VM



12. The next screen will open, click on the "Monitor Chart" option, select the metric and the period you want to view and click on "Refresh"



11. User and role management

In this section you can manage access to your organization. Enterprise Claro Cloud allows you to manage, create, and delete users in addition to having predefined roles that will help you with the management of your services properly.

Available user roles

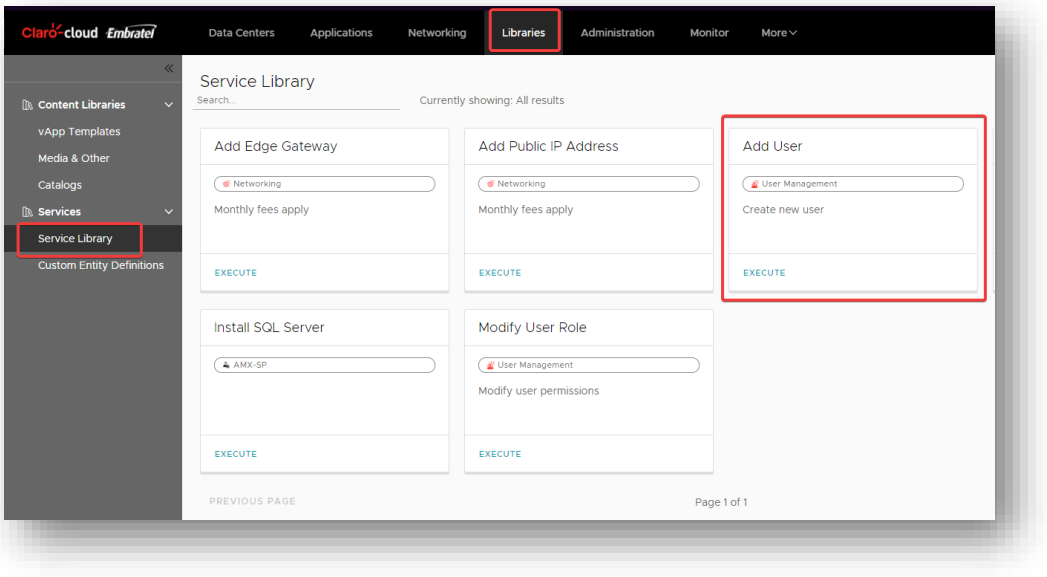
Role	Description
Administrator	Can contract, modify, and cancel VDC on-Demand and Resource Pool subscriptions in countries with available compute regions. You have access only to the Claro Cloud Administration console
Organization Administrator	Can purchase new services through the self-service portal (e.g. Virtual Machines, IP's, Edges). In addition, this role can create modify and delete resources instances networks within a vdc and private catalogs. Has access to administrative and billing information. Can create, manage, and modify users and roles in your organization.
Technical Administrator	Can create instances, applications, and manage deployed IaaS resources, as well as be able to configure networks within a VDC. Role cannot: purchase additional resources within the self-service portal, change administrative information, modify resource limits, change roles, or add additional users.
Compute Administrator	Can create new instances within a Virtual Data Center, and you can manage and modify existing instances.
Network Administrator	Can manage functionality within T1 Edge Gateway instances, such as creating new VLANs, managing and creating Firewall and NAT rules, generating IPSec and L2 VPN connections.
Staff-Read Only	Can view instance configuration parameters, network, and monitor status. Role cannot generate new instances, delete or change instance configuration parameters, or perform administrative tasks.

Create a user

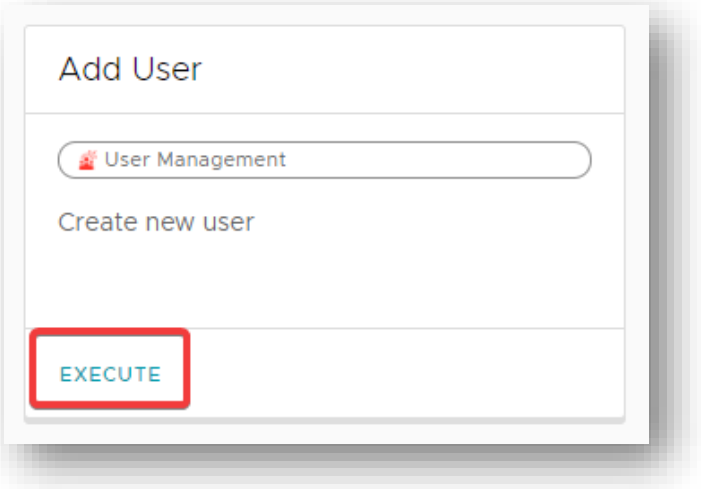
To create users within the Claro Cloud platform, perform the following process

> **Note:** This action can only be performed by an Organization Administrator

1. Select "Libraries" from the main menu, from the left menu select "Service Library"

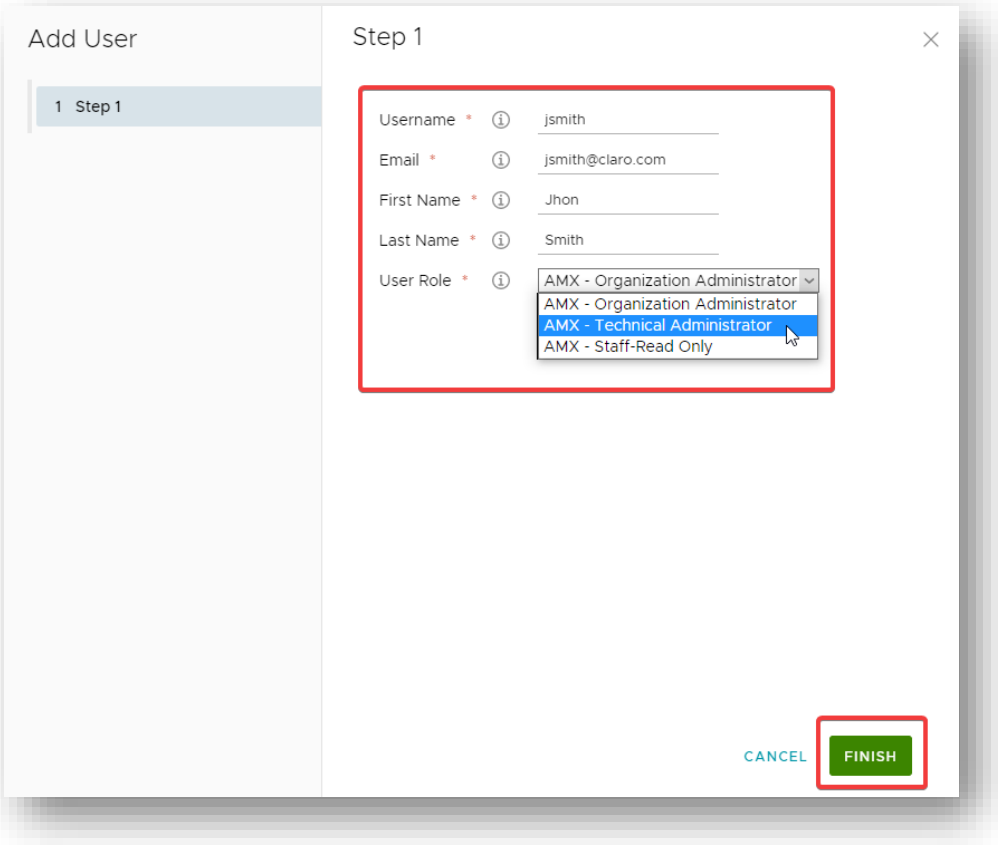


2. Locate the "Add User" box and click the "Execute" button



3. The next screen will be displayed, enter the required information. At the end of clicking on "Finish"

Item	Description
Username	User Name
Email	User email, it is possible to assign more than one user the same email
First Name	First name
Last Name	Surname
User Role	Role within the organization

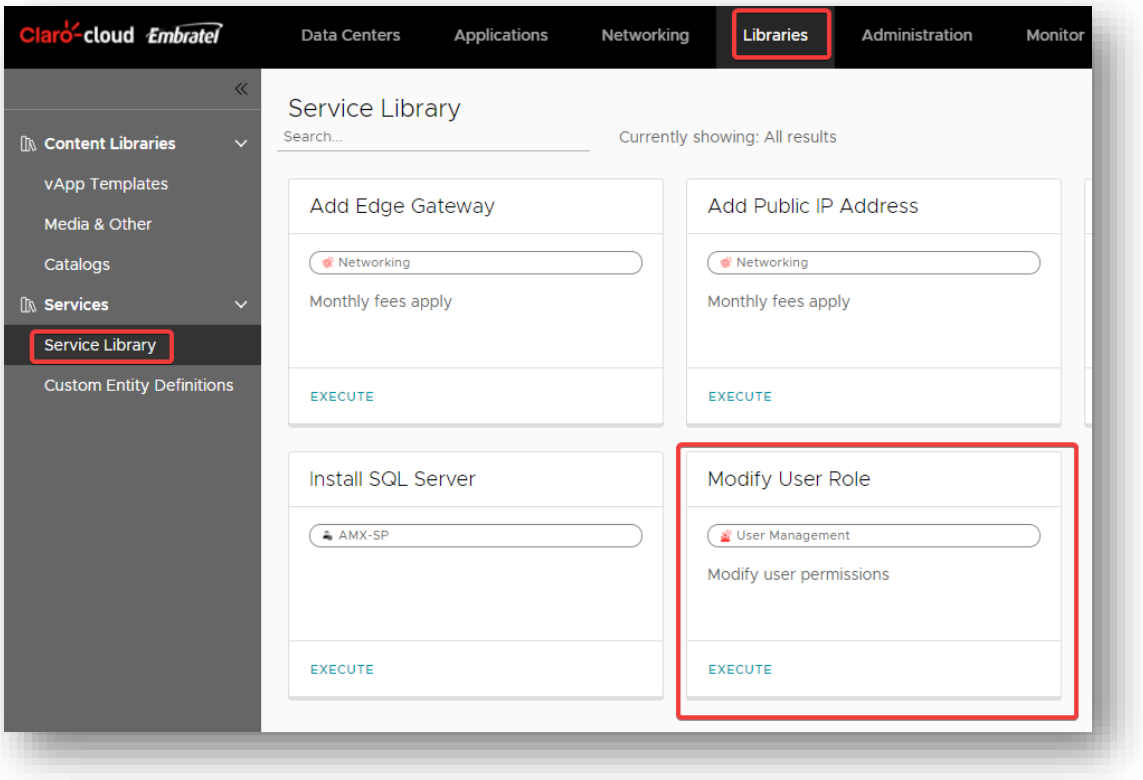


Modify a user's role

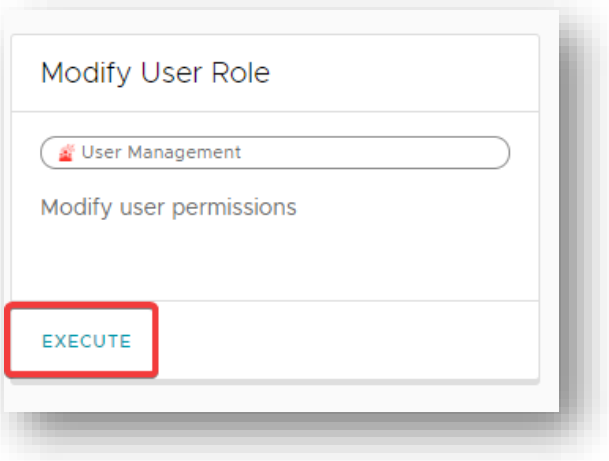
You can modify a user role that was previously assigned to a created user

> **Note:** this action can only be performed by an Organization Administrator

1. Select "Libraries" from the main menu, from the left menu select "Service Library"

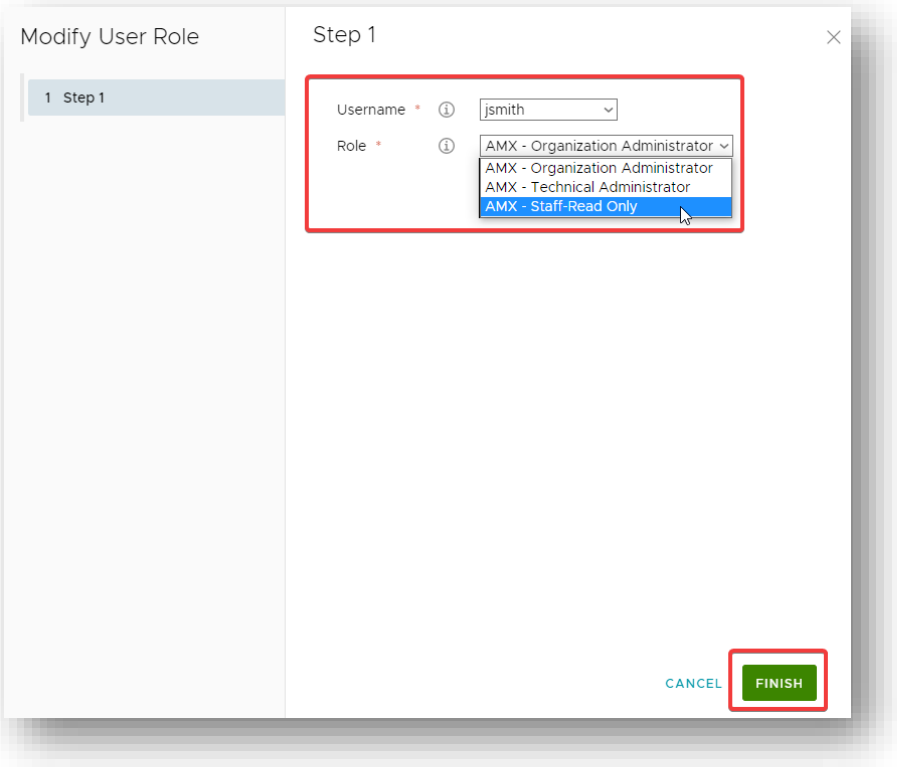


2. Locate the "Modify User Role" box and click the "Execute" button



3. The next screen will be displayed, enter the required information. At the end of clicking on "Finish"

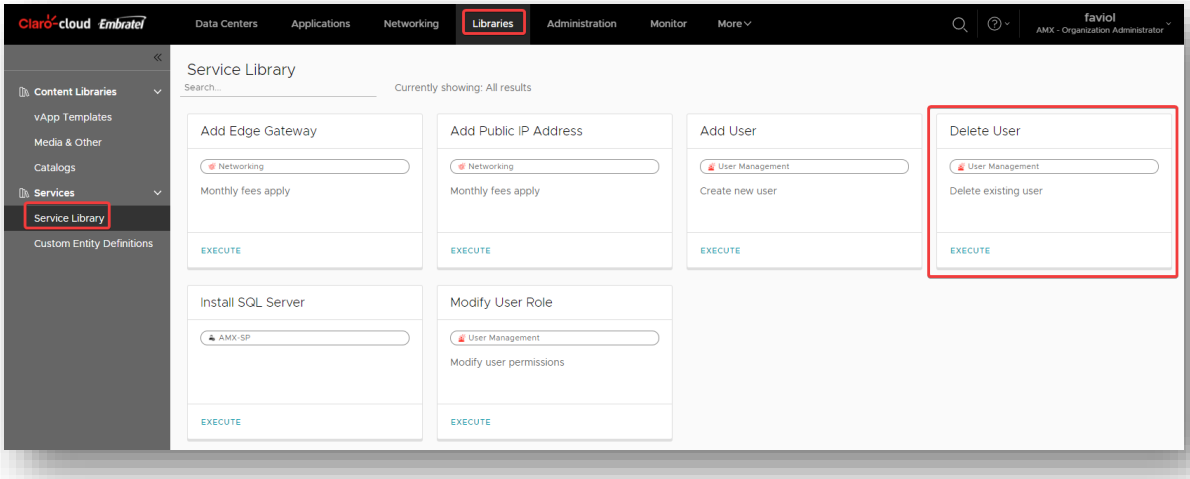
Item	Description
Username	Lists users created in your organization
Role	New role to assign



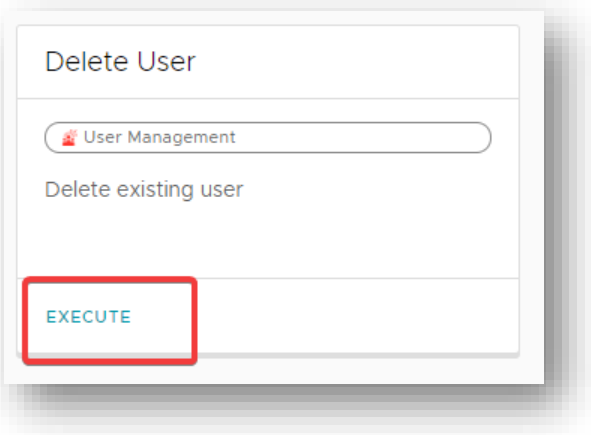
Delete a user

> **Note:** This action can only be performed by an Organization Administrator

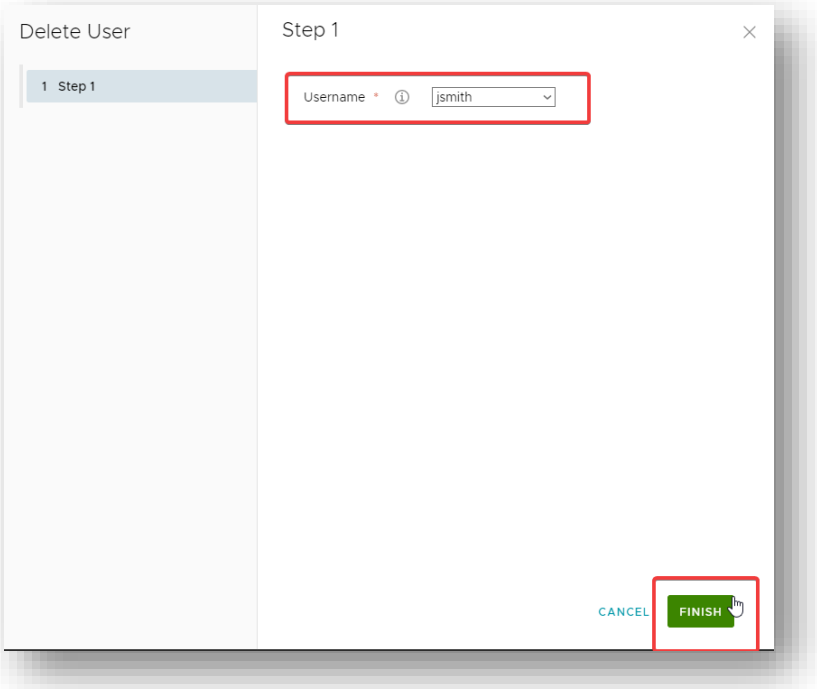
1. Select "Libraries" from the main menu, from the left menu select "Service Library"



2. Locate the "Delete User" box and click the "Execute" button



3. The following screen will be displayed, where the active users in the organization will be listed, select the user to delete, click on "Finish"

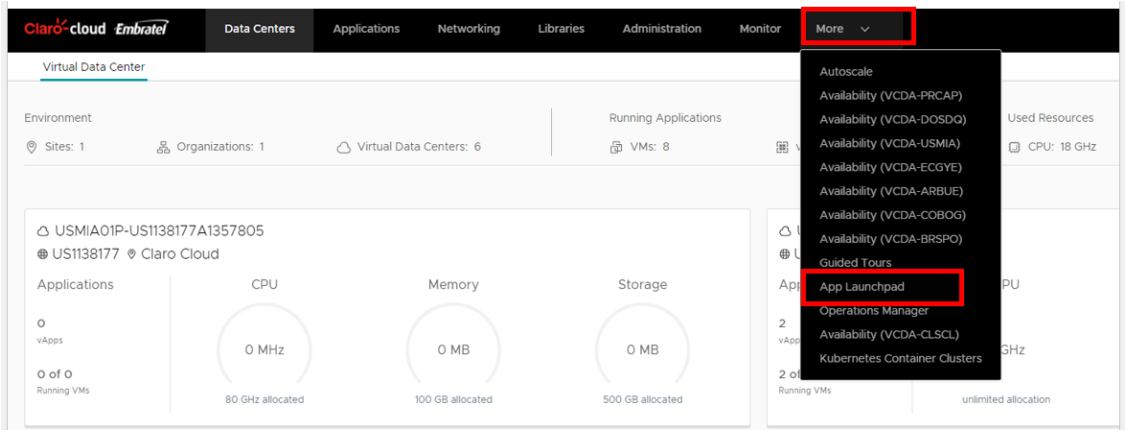


11. Application Catalog in Enterprise Claro Cloud

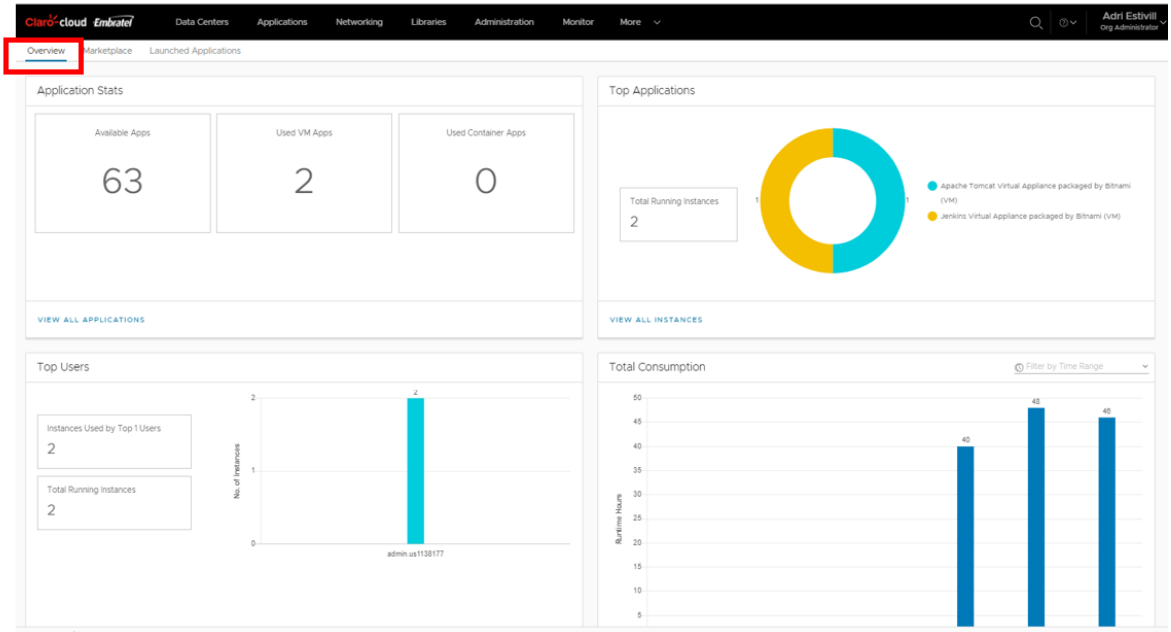
Enterprise Claro Cloud offers you a catalog of open source applications that you can use to deploy virtual machines directly in your Organization's Data Centers.

Process to enter the catalog

1. In the main menu select "More", in the submenu click on "App Launchpad".

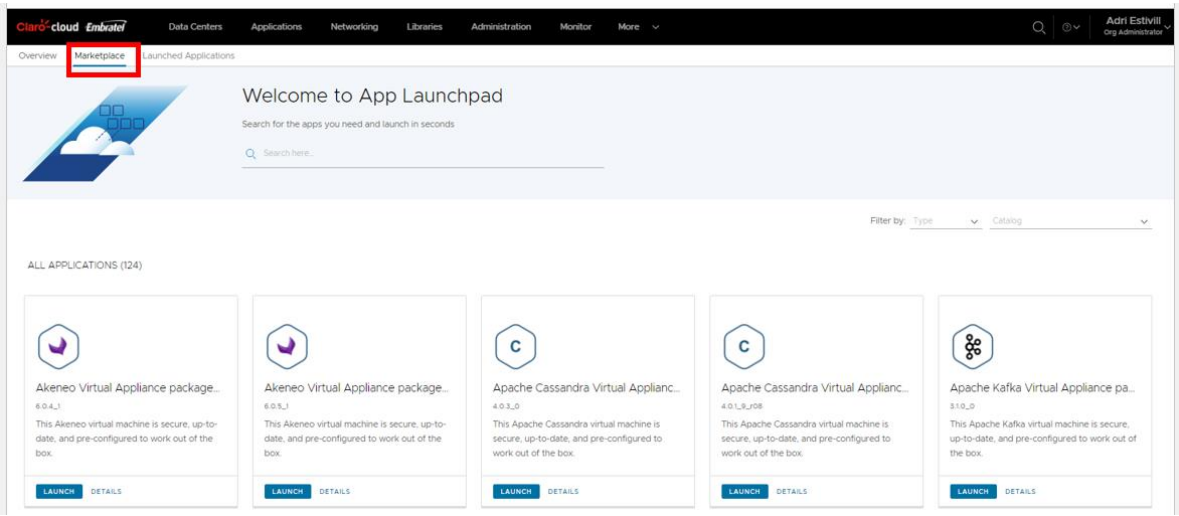


2. The following screen will be displayed, where you can view an overview of the applications that are deployed in the organization

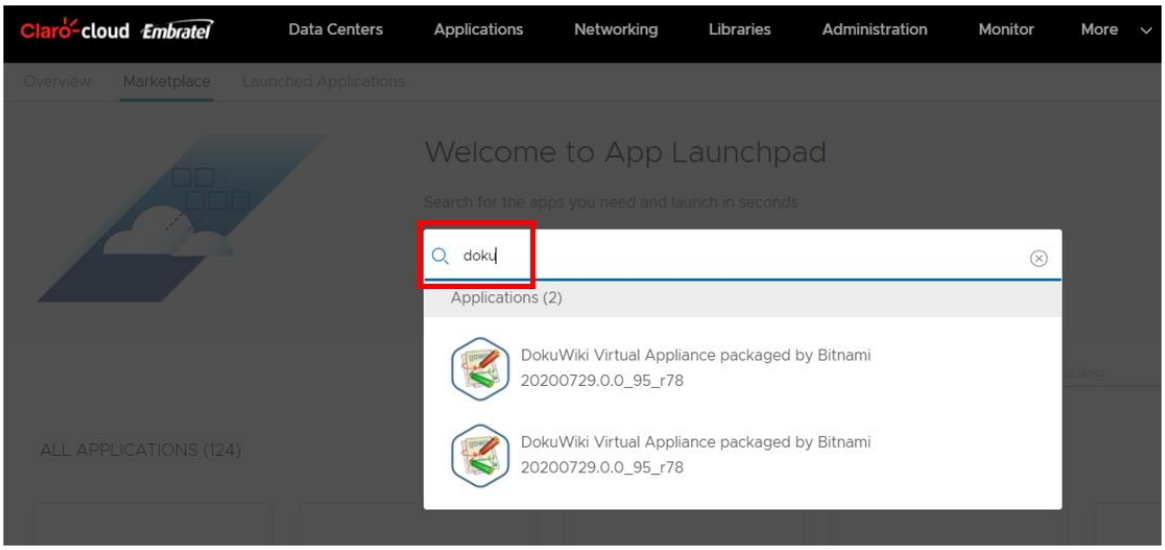


3. Select the Marketplace option to deploy the application catalog

4. In case you have contracted infrastructure in more than one computing region, it is advisable to filter the catalog in the region you want to provision

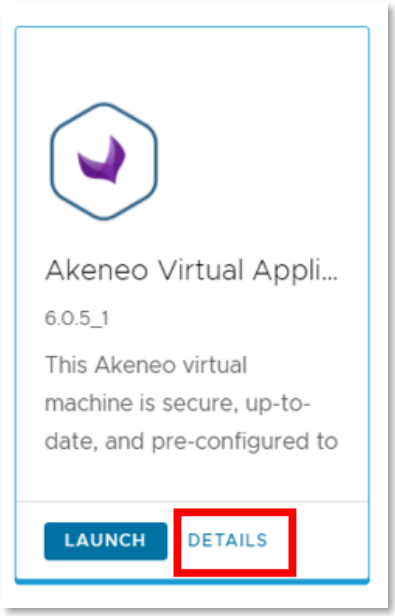


5. You can use the built-in search engine to find a particular application.

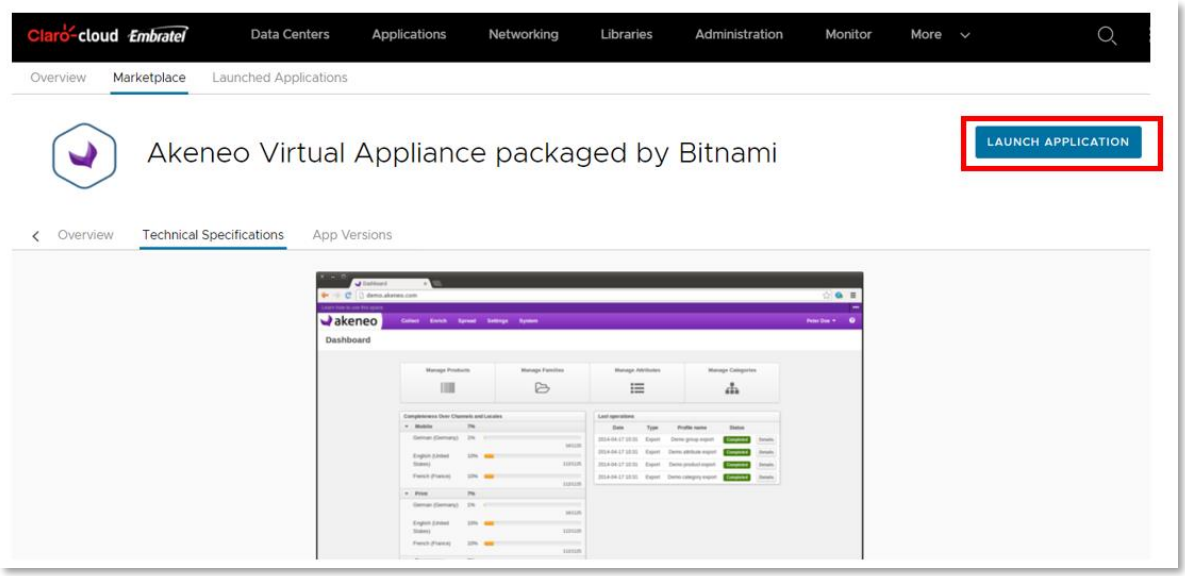


Creating an application

1. Find and select the application to deploy, click on "Details" then select it.



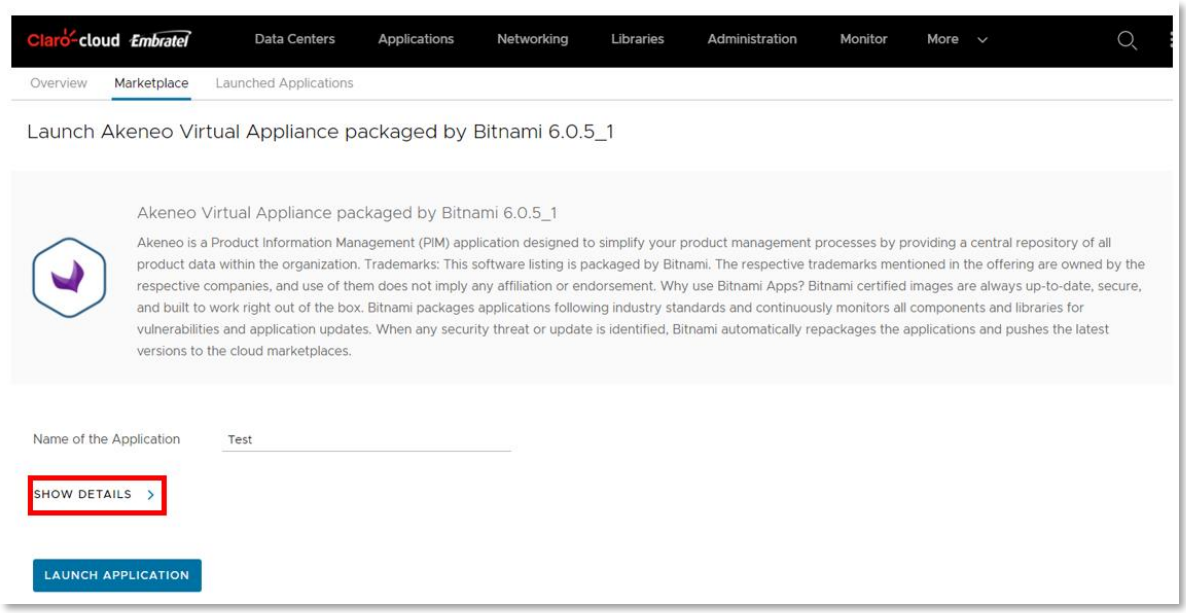
2. The following screen will be displayed to show you the overview of the application, versions, and technical specifications. To start the implementation click "Launch Application"

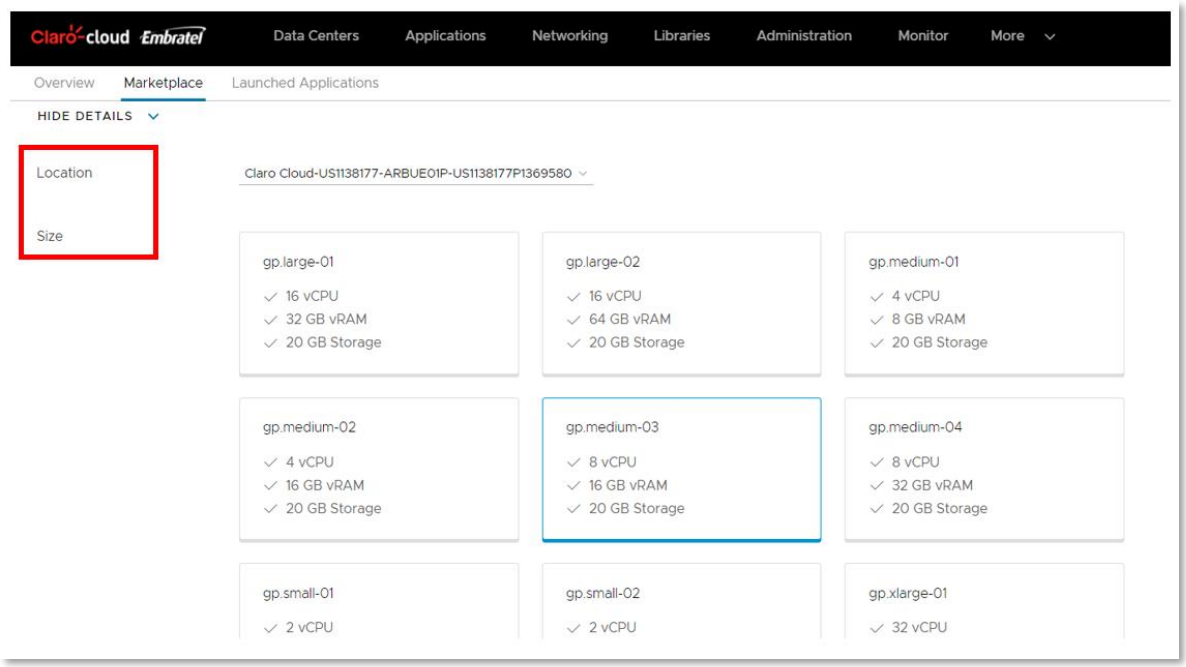


3. The following screen will be displayed, first you must enter the name to define the hostname of the virtual machine to be deployed. After clicking show details to display the rest of the parameters to configure.

Item	Description
Location	Select the Data Center where you want to deploy your application

Size	Define the size of the virtual machine where the application will be installed
IP address	Define the internal or external IP address to assign

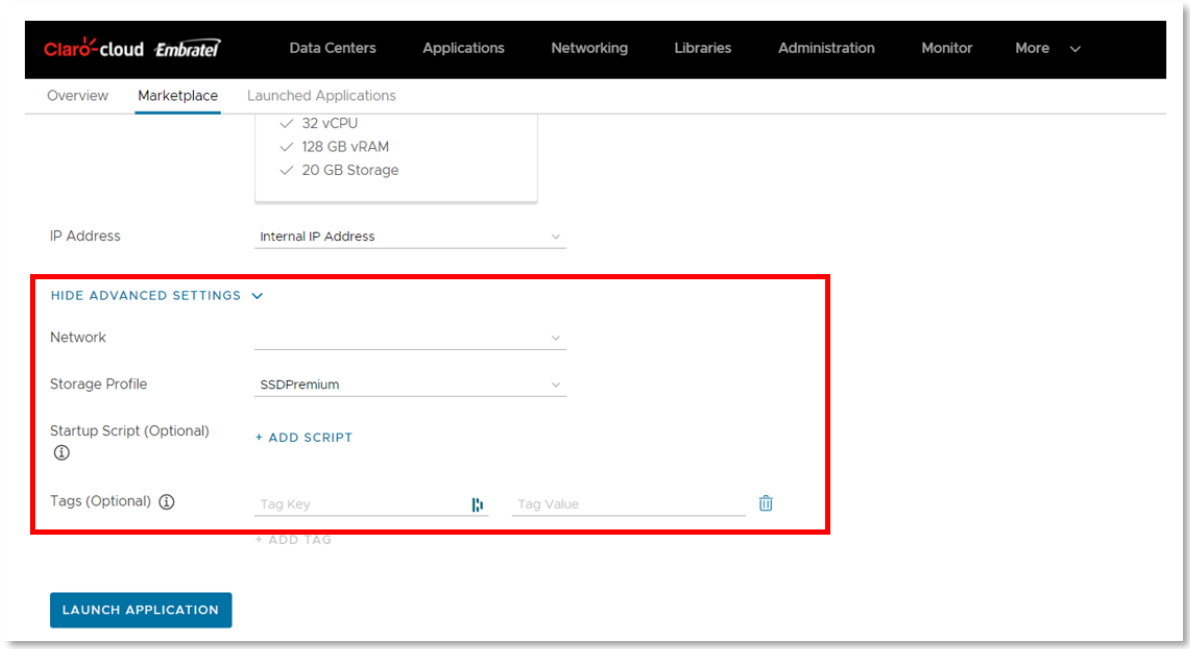




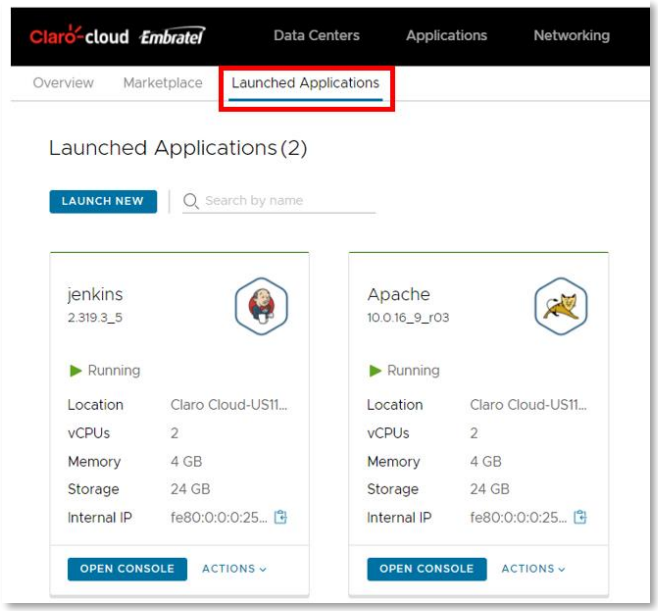
4. Optionally, you can click Advanced Settings to define the following parameters. When finished, click "Start Application"

Item	Description

Network	Select an existing network from the previously chosen Data Center
Storage Profile	Type of storage, as the only option Enterprise Claro Cloud has SSD disks
Startup script	You can load a customization script into a virtual machine. The script runs before and after guest customization when you deploy a virtual machine based on an application template.
Tags	User-defined tags are useful when adding additional properties to your application.



5. Upon completion of provisioning, you will be able to view your application from the "My Applications" option or directly in the selected Data Center



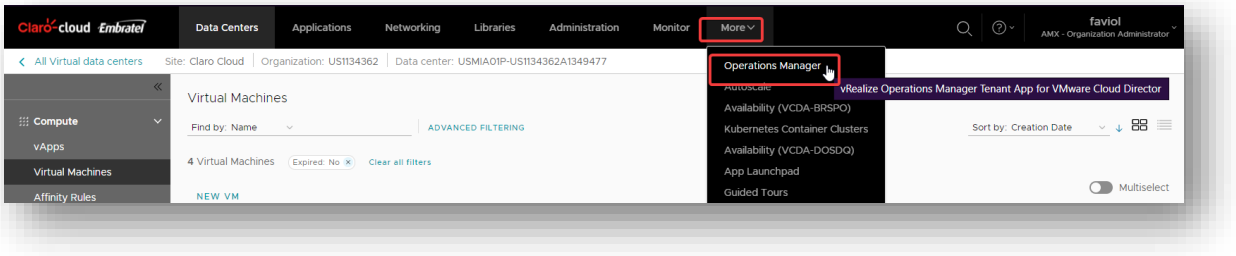
6. To access your application see the First access to a virtual machine section
7. To be able to reset your password the Reset password section by default

12. Monitoring

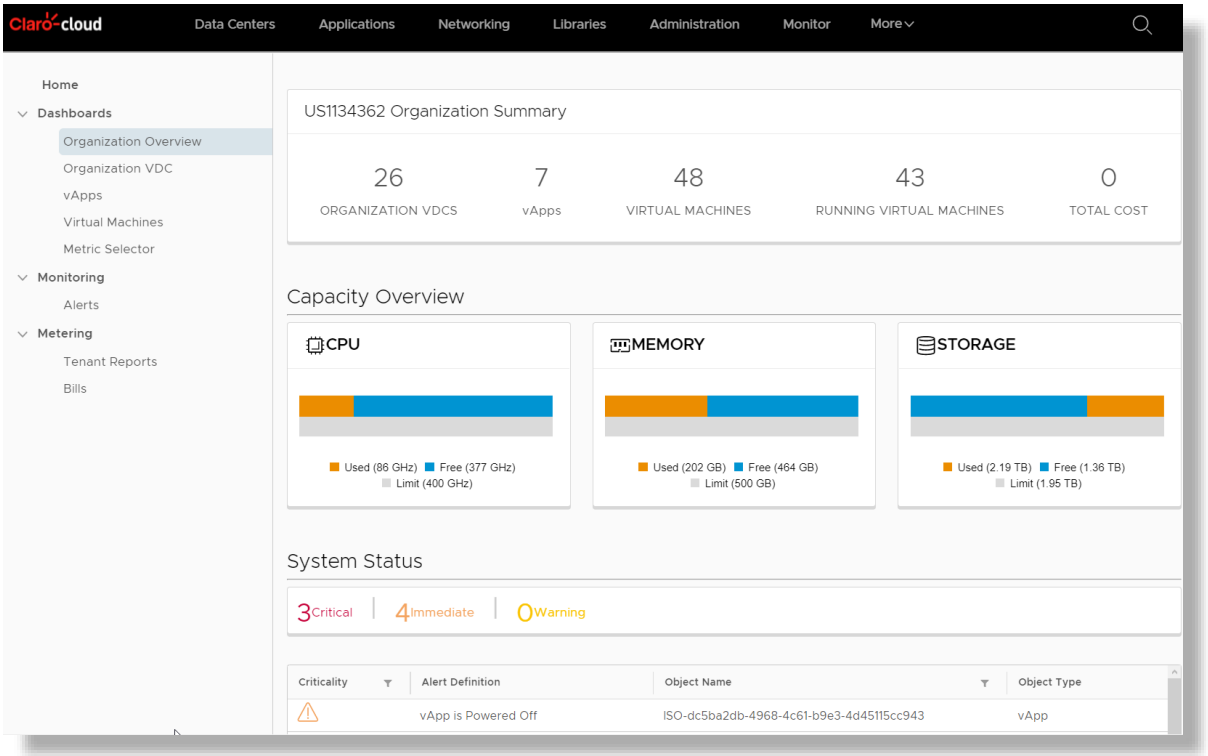
Enterprise Claro Cloud has a section where you can visualize metrics of consumption, health, and general platform behavior.

To enter this module follow the steps

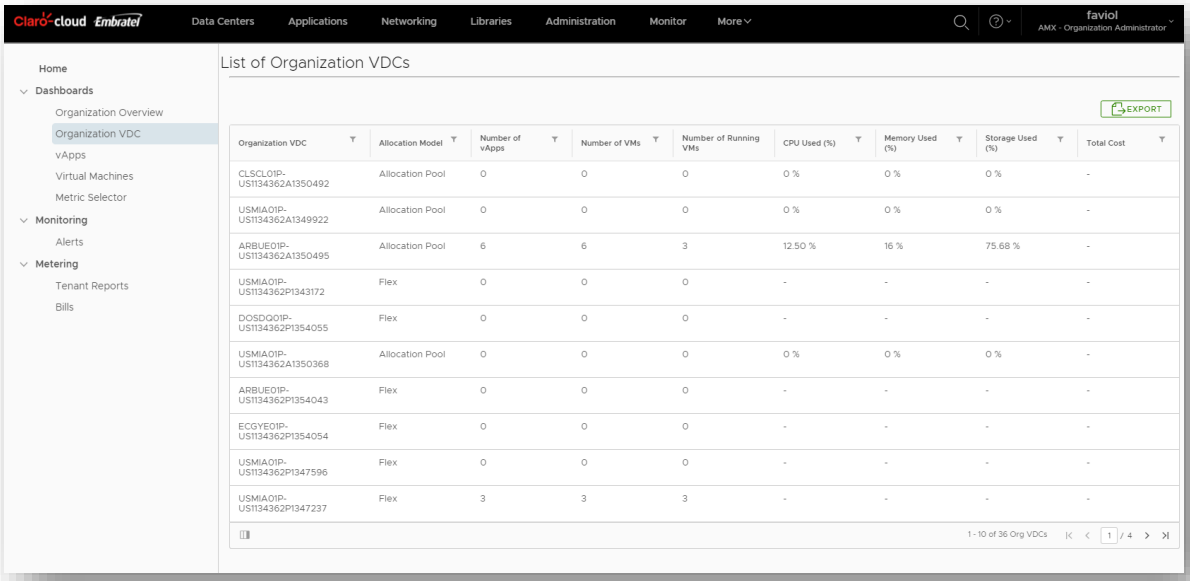
1. From the main menu, select More, and then select the Operations Manager option.



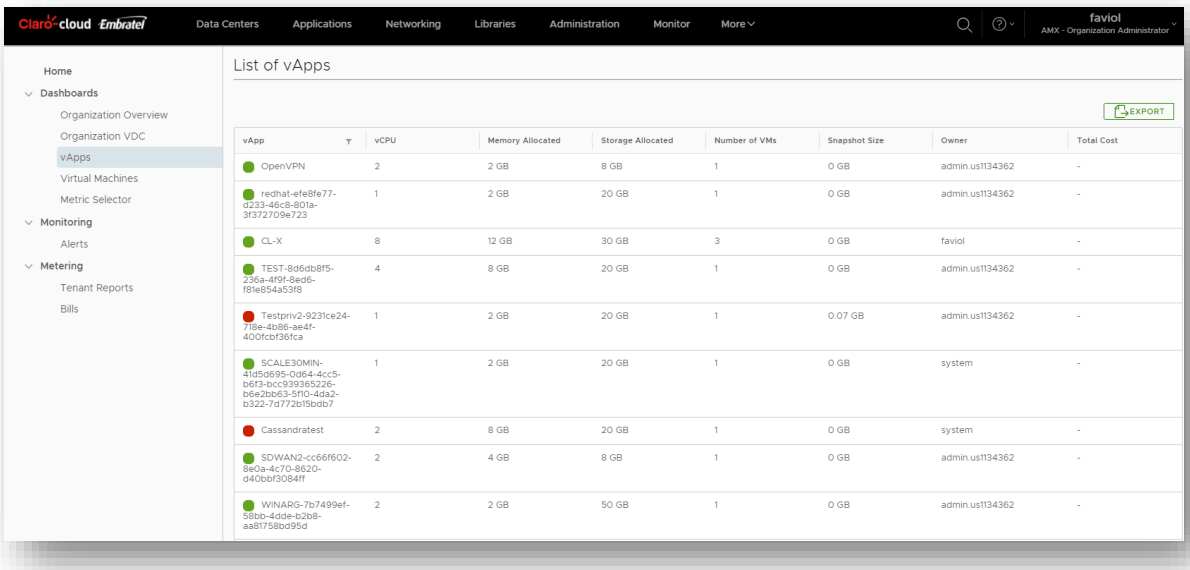
2. Within the Operation Manager menu there will be a menu on the left which offers options where you can review a summary of your Organization, as well as the resources provisioned and consumed for CPU, Memory, and Storage.



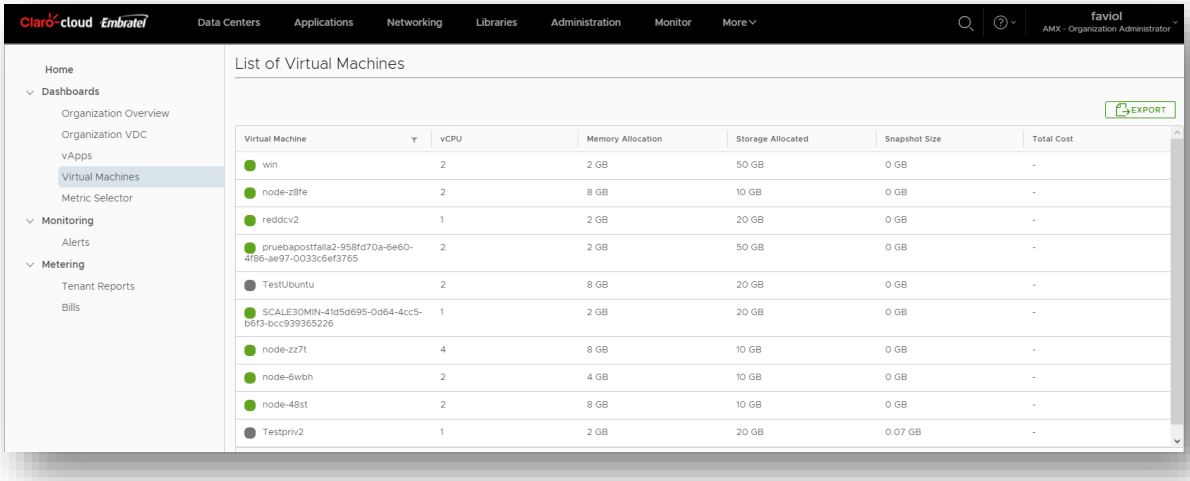
3. In the Organization VDC section you can see the list of your VDCs. For each of them you can see the type of VDC, the number of vApps that it contains, the number of virtual machines that it groups and how many of them are running. You'll also be able to validate the percentage of CPU used, along with memory and storage. Finally, the total cost for each VDC is observed.



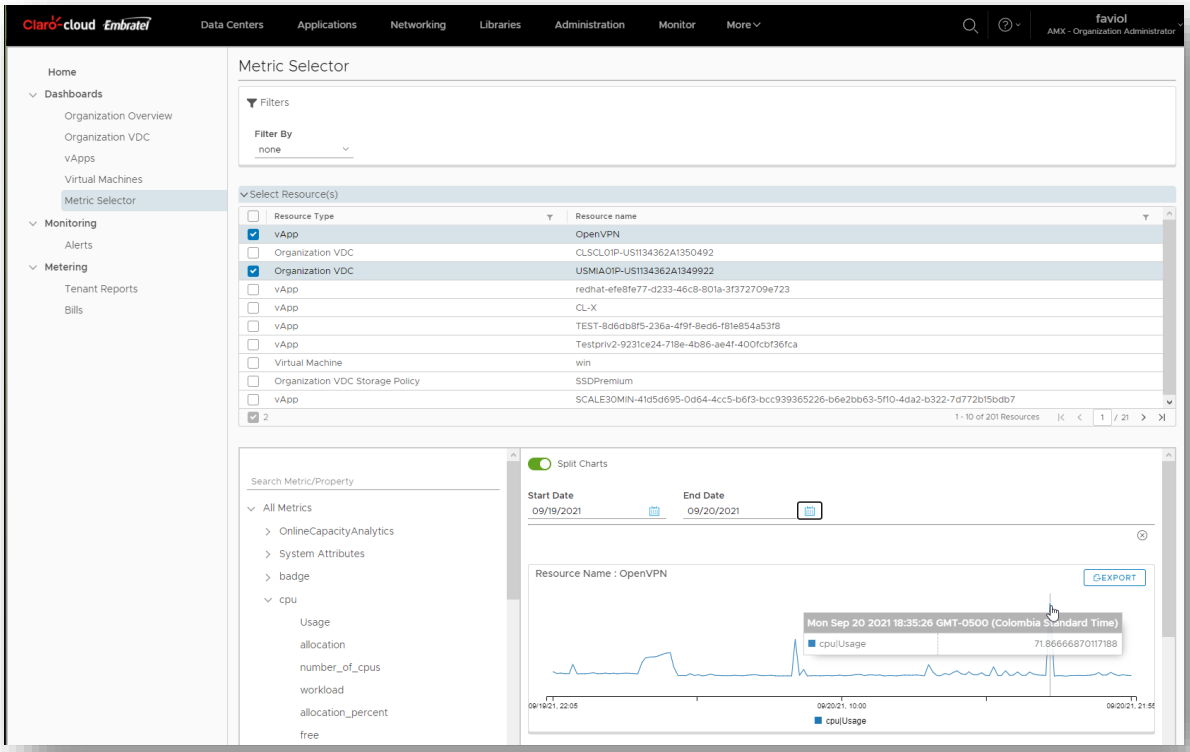
4. The vApps section will show the list of vApps with the resources used (vCPU, Memory, and Storage), as well as the number of VMs that it has.



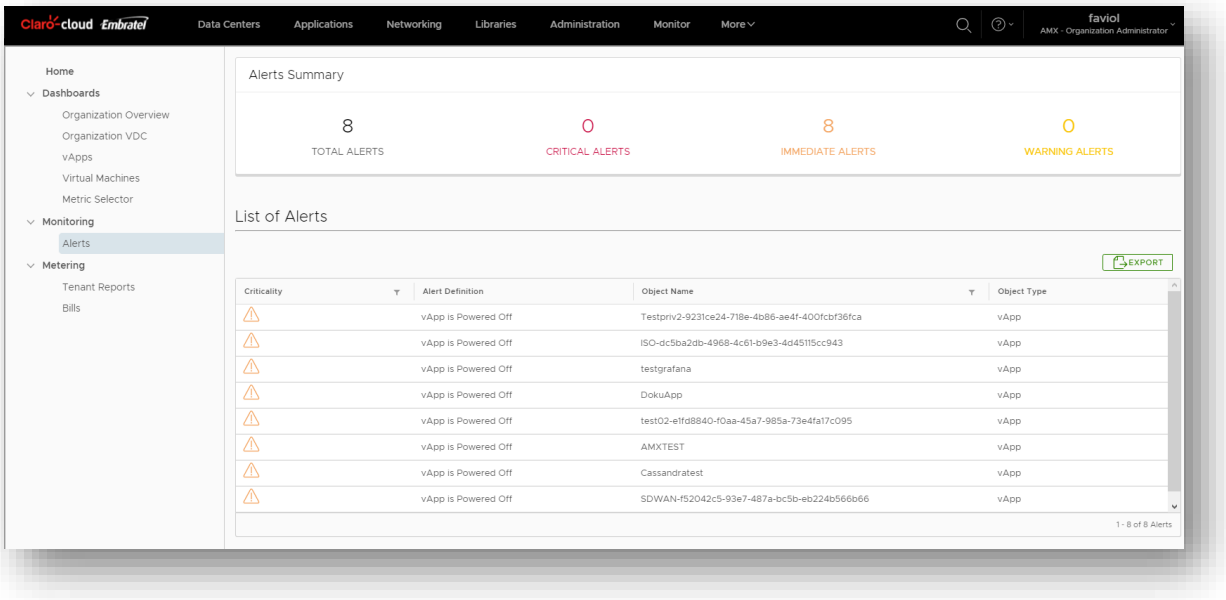
5. In the Virtual Machines section it will show you the list of virtual machines along with their vCPU, Memory and Storage resources. You can also view the Snapshot size, if any, and the total cost.



6. In the Metric Selector section you can opt for different parameters that will help you create personalized dashboards of the different contracted services, to be able to visualize the use in periods of time.

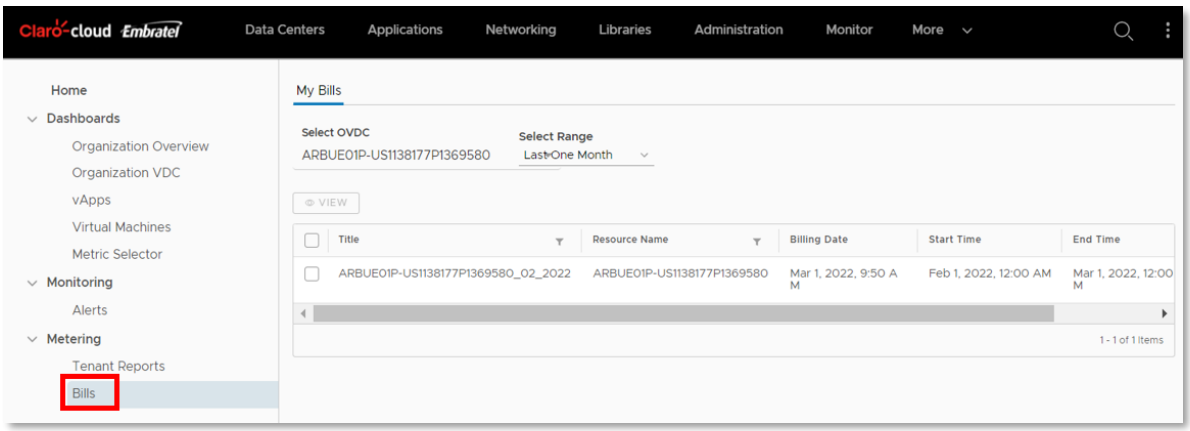


7. In the Alerts section it will show you a summary of important events to validate, where you can also observe the criticality and the services that could have a problem or incident.



8. In the Bills section, you can view detailed consumption reports by Data Center, which contain the details of the contracted services that will be included in your billing

> **Important:** For Data Centers in Resource Pool scheme, computing resources (vCPU, RAM and Storage) will not be displayed, these will be detailed in your Claro Cloud invoice.
>
> The reports will be generated according to your Claro Cloud billing cycle



13. APIs

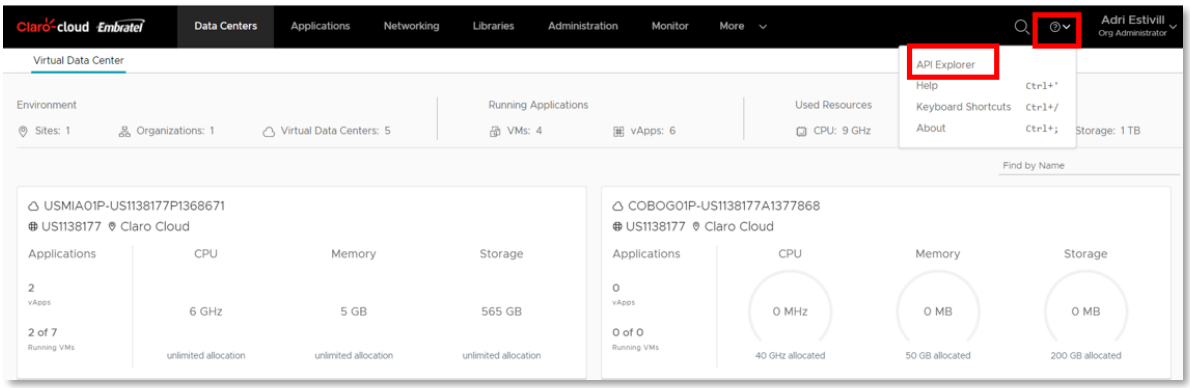
Enterprise Claro Cloud offers you the ability to manage your service through Restful APIs. For more information, go to https://developer.vmware.com/apis/1196/vmware-cloud-director)

Below are the different methods to access this functionality.

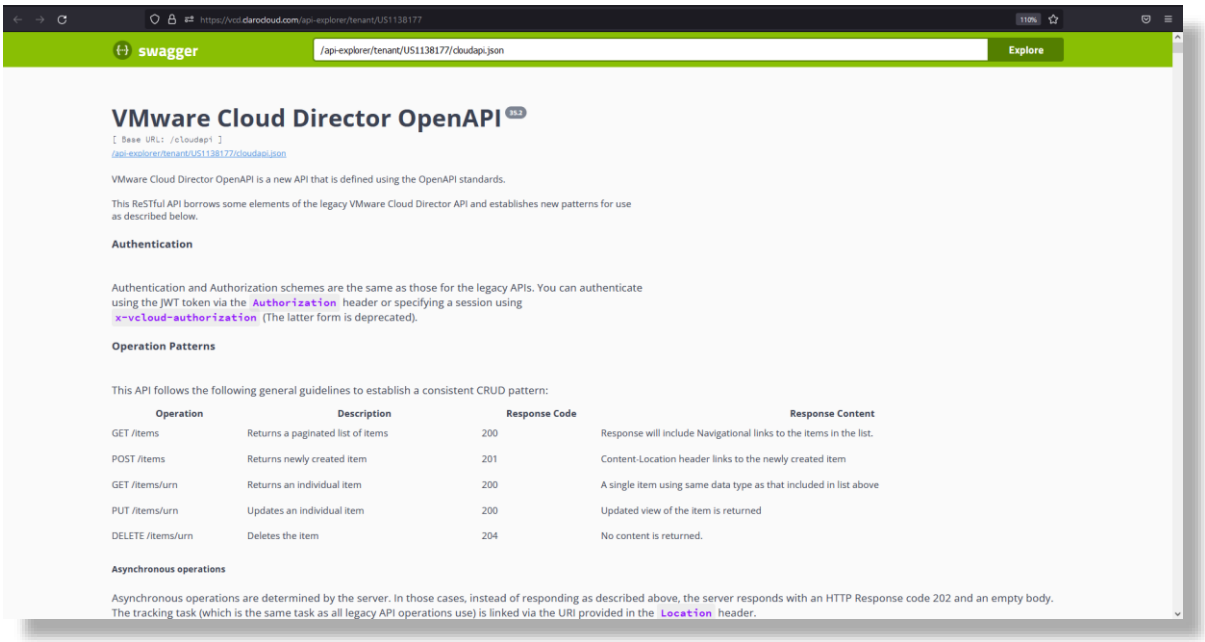
Direct access via control panel (Swagger)

Through its self-service panel you will be able to access an interface where you can use APIs without downloading additional software,

1. From the main menu, select the help icon (?) and then the "API Explorer" option.



2. The following web page will open, where you can run Restful API calls, without the need to install additional software



> **Note:** No registration or login is required, the platform automatic links your organization and user

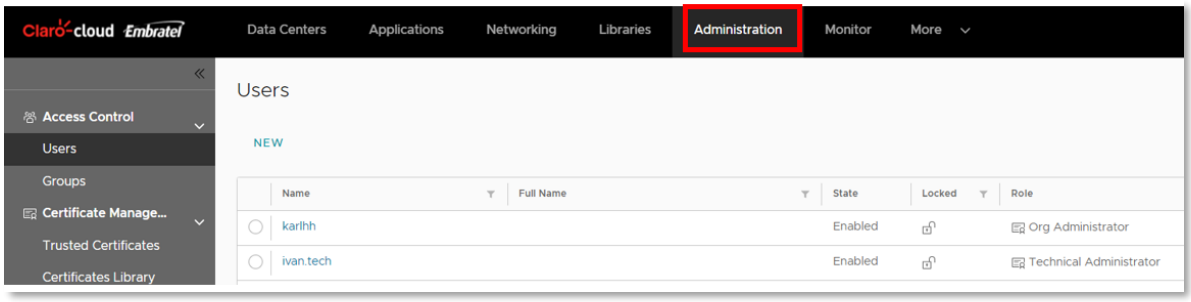
Administration through Terraform Provider

One of methods of administration and access to your service that Enterprise Claro Cloud makes available to you is Terraform Provider, which allows you to manage, implement and access your services through code.

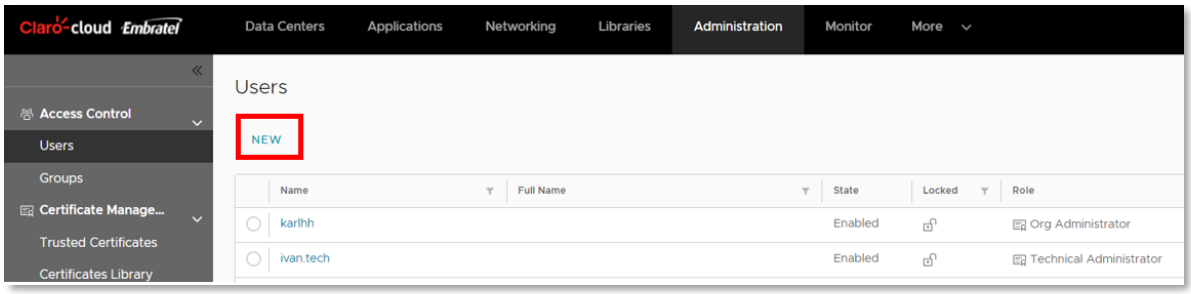
For more information, go to https://registry.terraform.io/providers/vmware/vcd/latest/docs

It is necessary to create an additional user in order to be able to enter your service through Terraform, perform the following steps.

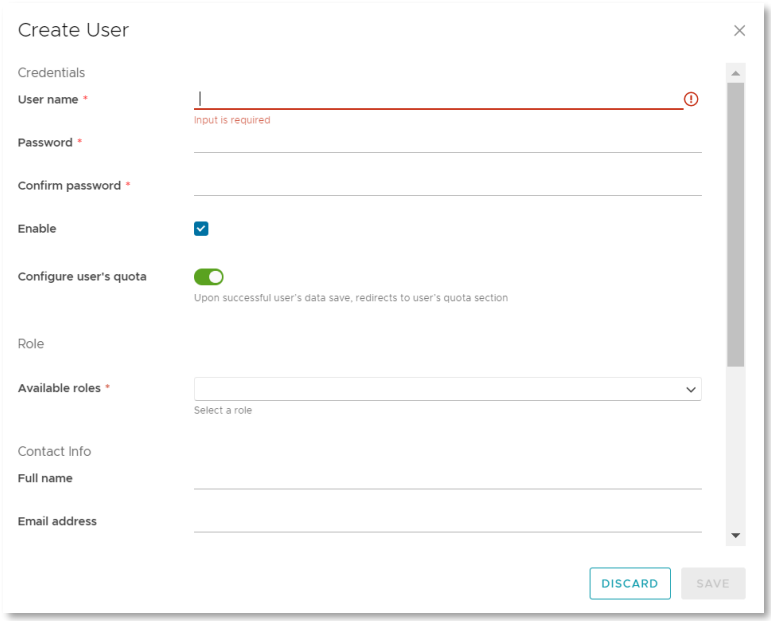
1. From the main menu, select Administration



2. Click "New"



3. The next screen will open and enter the following information, when finished click "Save"



Item	Description
User name	Enter user name
Password	Define a password. It is recommended to include at least one capital letter a number and a special character
Enable	Keep this option on
Configure user's quota	Enables user resource limits
Available features	Select the user role to assign it is recommended to assign an Organization Administrator
Full name	Enter your full name
E-mail address	Please enter a valid email account
Phone Number	Enter a contact phone number
ID	(optional) Enter your ID number
Quota of all VMs	The maximum number of virtual machines in vApps that an organization member can store in an undeployed state.
Running VM quota	The maximum number of virtual machines that a member of this organization can deploy simultaneously.

14. Glossary

App Launchpad

It is a VMware Cloud Director service extension that service providers can use to create and publish application catalogs ready for deployment. Users of the leasing service can then deploy the applications with a single click.

App Launchpad supports the use of applications from the Bitnami App Catalog that is available on the VMware Marketplace.

Load Balancer / Load Balancer

It is one of the features included in Claro Cloud with the power of the new AVI Networks component, which allows load balancing or applications with different algorithms for applications that are running on several virtual machines by exposing a VIP (Virtual IP).

Distributed Firewall

The distributed firewall allows you to segment virtual datacenter entities in your organization, such as virtual machines, based on the attributes and names of the virtual machines. NSX software provides distributed firewall capability in the vCloud Director environment.

Kubernetes Cluster

This cluster is a complete distribution of the open source Kubernetes container orchestration platform compiled, signed, and supported by VMware. This is a cluster instance integrated with vCloud Director that is CSE (Container Service Extension) enabled.

Private and public IP range

The main differences between public IP and private IP is that the former is accessible from the Internet and the latter is not, and that the former is assigned to the internet endpoint and access (the router) and the latter to the devices connected to that endpoint.

T1 Edge Gateway

It is an NSX service which in turn supports network services such as Routing, VPN (IPSec, L2), Load Balancing, DHCP.

Coat

It is a logical organization within vCloud Director that allows you to operate virtual infrastructure with its different compute, network and storage components.

vCloud Director

Cloud service delivery platform developed by VMware, allows to operate infrastructure efficiently and elastically

Virtual Firewall

It is a firewall integrated into a fully virtualized environment, allows you to perform traditional and advanced filtering functions when integrated with other components

VM

Initials corresponding to virtual machines for its acronym in English

VMware Cloud Availability

VMware product used for replication and disaster recovery

VPN IPSEC

Connection between two sites that you make using the concept of tunnel or secure network on another network that is not, for example, a secure connection on the Internet, the basis of its operation corresponds to two systems at the ends that are responsible for encrypting the message in the middle and encapsulating the useful information. This is achieved with different algorithms, protocols and in some cases, with digital certificates. For the VMware platform this system is managed by the Edge Gateway

VPN L2

An L2 or Layer 2 VPN is a type of VPN where data links are virtualized to simulate a local network over geographically remote sites where data service providers are not involved in IP routing and control of this depends on the client completely.

VXLAN

It is one of the network encapsulation protocols that allows to solve the limitations of traditional VLANs, among which are the number of networks and the reuse of addressing in environments where thousands of machines are used typically in virtualized environments. The basic operation corresponds to an increase in information from the TCP/IP packet header which carries additional information that is processed in the VTEPs which are responsible for encapsulating and de-encapsulating the useful information. MTU greater than 1600 must be enabled to support VXLAN protocol