Creating and Configuring a Virtual Private Cloud

IndiQus Technologies Pvt. Ltd.

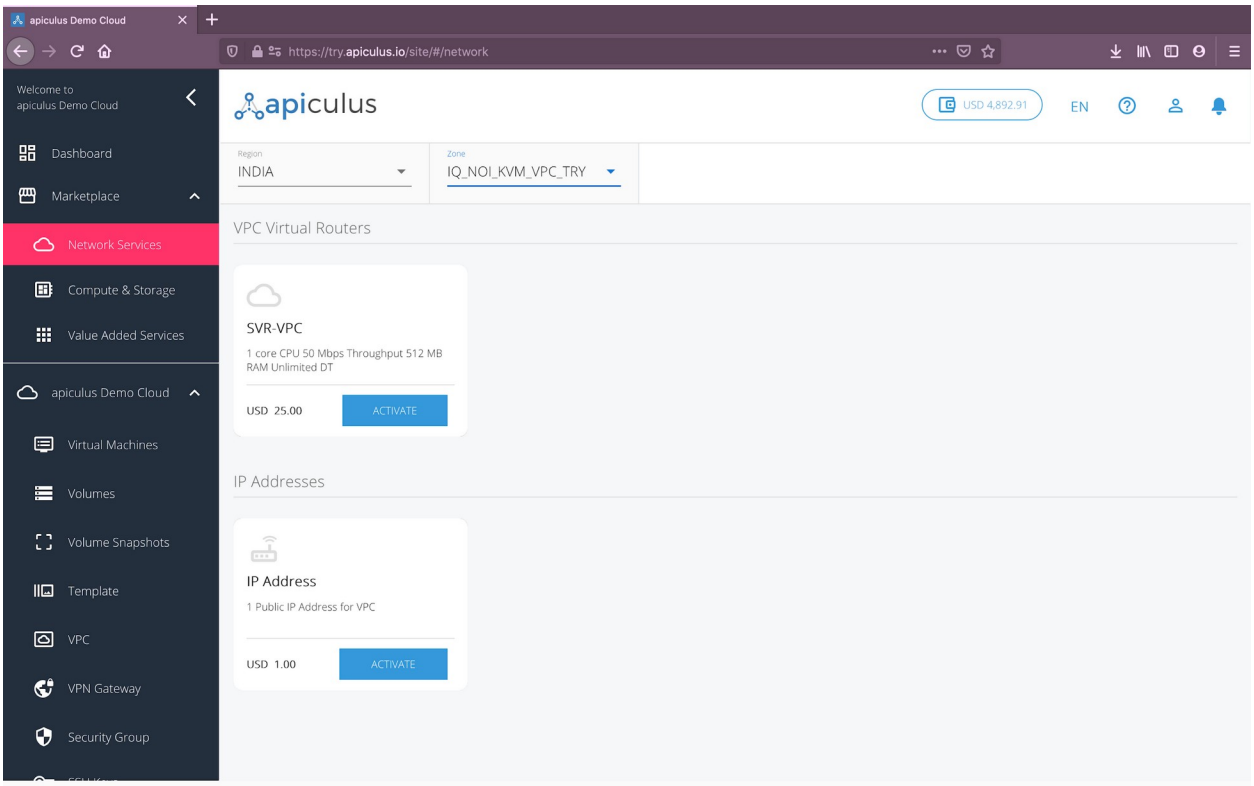
Table of Contents

Purchasing a VPC Virtual Router

To get started with configuring a VPC, you need to first purchase a virtual router from the marketplace. Virtual Routers can be purchased from the **Network Services** section of the marketplace and can be accessed from the **Marketplace** menu on the main navigation panel.

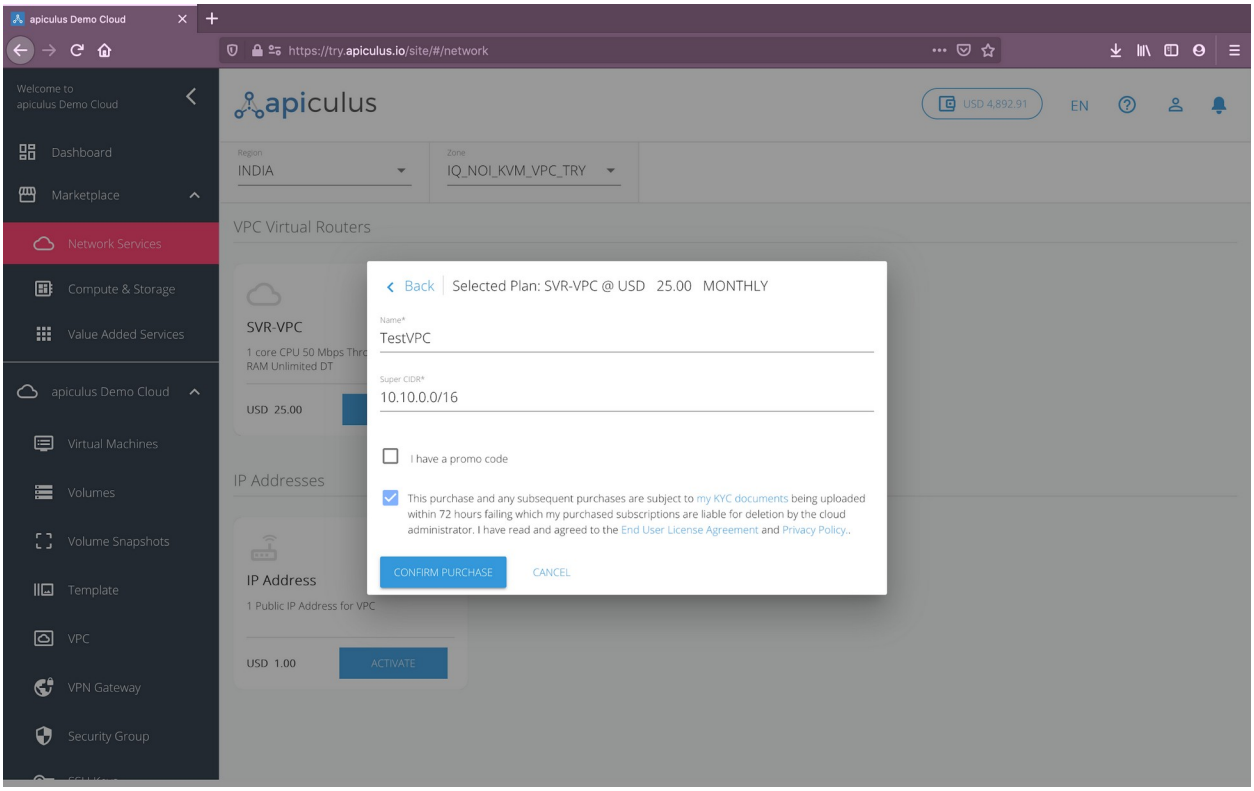
A VPC Virtual Router can be purchased by following these steps:

1. Navigate to **Marketplace** > **Network Services**.
2. Choose the appropriate **region** and **zone** from the dropdown menu on top. *This is needed if there are multiple VPC zones available as part of the public cloud setup.*
3. Select a plan from the options listed under **VPC Virtual Routers**.
4. Alternatively, you can also navigate to the **apiculus Cloud** > **VPC** section on the main navigation panel, select the appropriate **region** and **zone**, and click on the **Buy More** button. This will list all the available options for VPC Virtual Routers.



Once you've chosen the desired plan, you'll be asked for the following details to set up the VPC:

- A **name** for the VPC.
- The **super CIDR** for the internal IP allocation in a x.x.x.x/x format.
- If there are **promo/discount codes** available for this purchase, you'll be shown those options.



Clicking on **Confirm Purchase** with the above information will provision the VPC Virtual Router in your account.

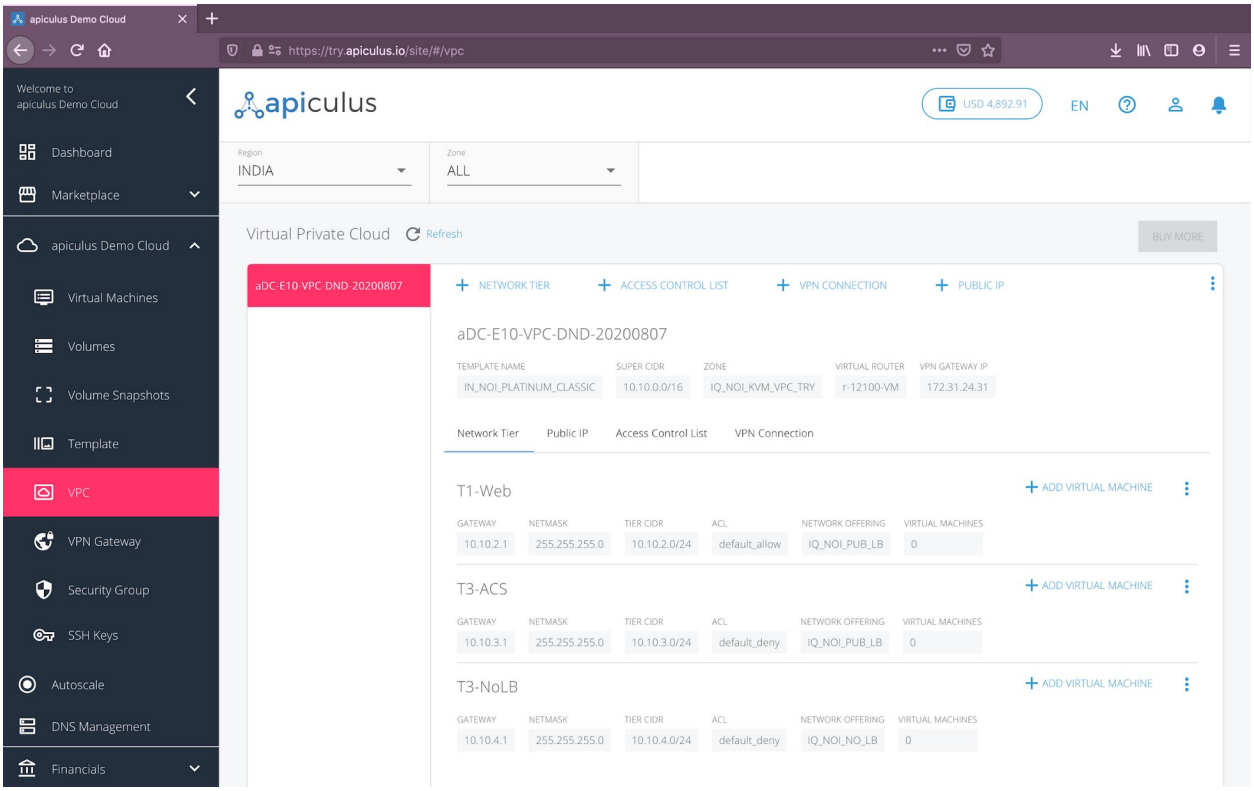
Please note that this might take up to 5-8 minutes. You may use the CloudConsole during this time, but it is advised that you do not refresh the browser window.

Once ready, you'll be notified of this purchase on your email address on record. The newly created VPC can be accessed from **apiculus Cloud > VPC** on the main navigation panel.

To start using the virtual router as a VPC requires basic network configurations to be done. This section describes the steps for the same, and for adding virtual machines to the network.

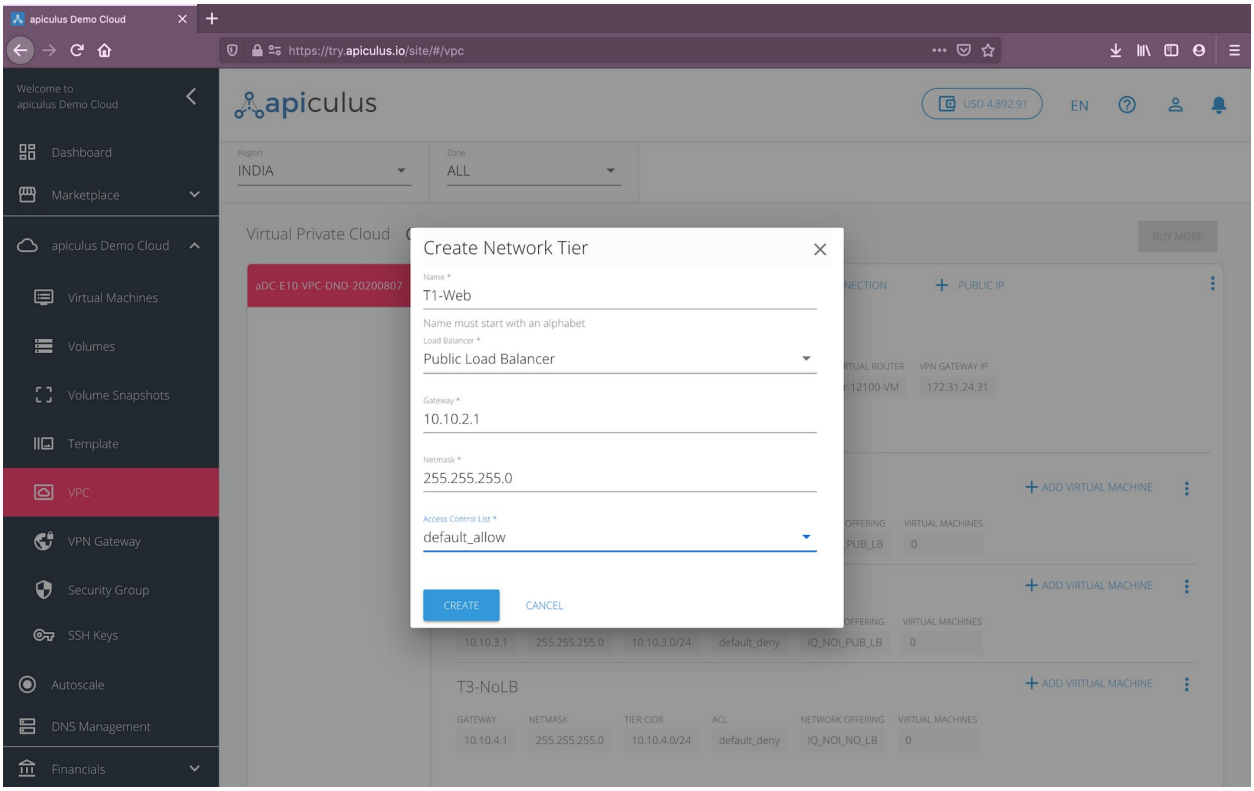
Configuring Tiers and Subnets

VPCs follow the convention of 3-tiered architectures, with web, app and DB tiers forming the norm. You can, however, configure these tiers to suit your application architecture, or just follow the common convention.



To add a tier to your VPC, navigate to the VPC you wish to add the tier to, and click on the **+ Network Tier** option inside the VPC. This will open up a dialog box asking you to provide the following information:

- **Name** of the tier.
- **Load balancing** required on this tier. *Please note that to set up a public load balancer, you need to select **Public LB** on this dropdown. Please also note that there can only be 1 tier of type Public LB in a network.*
- **Gateway** for the subnet. *Please note that this gateway should be consistent with the **Super CIDR** for the VPC.*
- **Subnet mask** for the tier/subnet.
- Default **access control** policy for this tier.

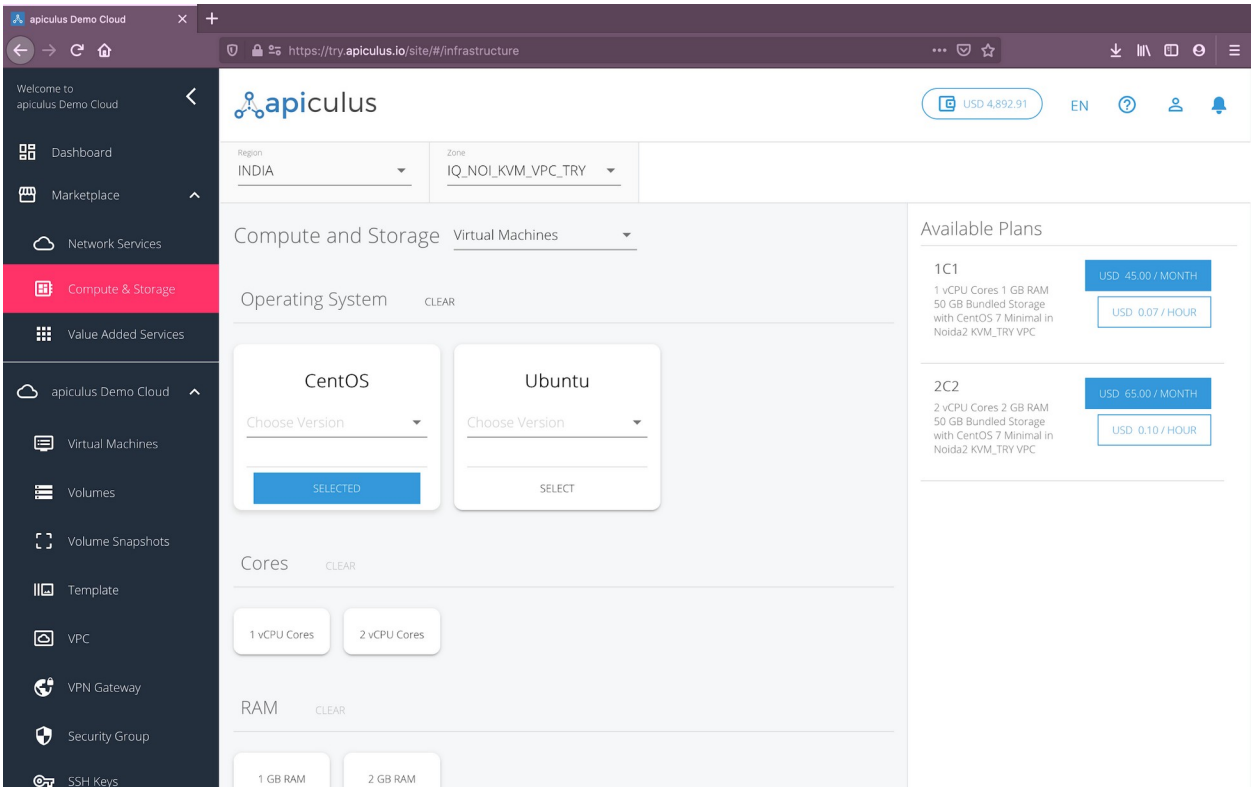


Clicking on **Create** will create the tier or subnet to be used as part of the VPC.

Adding Virtual Machines

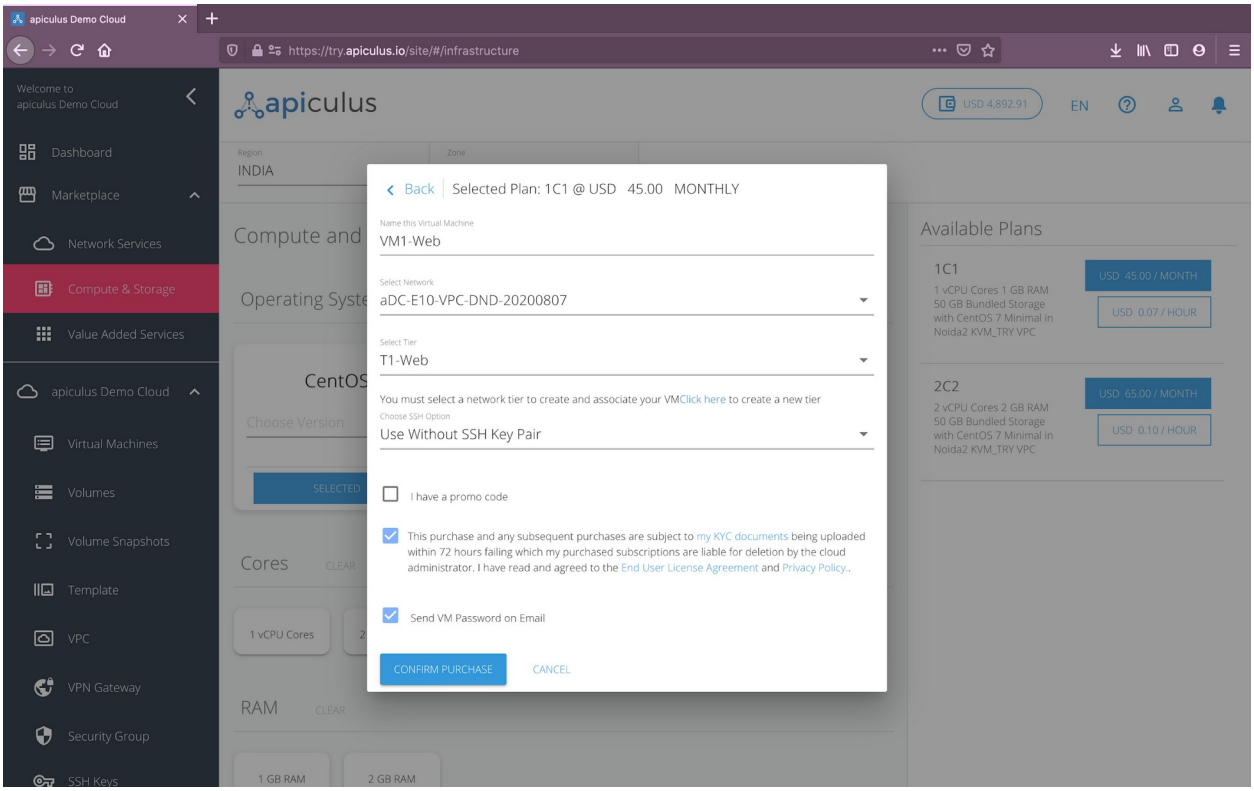
Once you have configured your subnets, you can now start adding virtual machines to these tiers. To add a virtual machine to your VPC, follow these steps:

1. Navigate to **Marketplace** > **Compute and Storage**.
2. Choose the desired configurations for **operating system**, **vCPU**, **RAM** and **root disk**.
3. From the available options shown on the panel on the right-hand side, choose the plan that suits your virtual machine requirements. *Please note that some configurations might not have hourly plans. This is absolutely normal.*
4. Alternatively, you can also navigate to **apiculus Cloud** > **Virtual Machines**, select the appropriate **region** and **zone** from the dropdown menu on top, and click on the **Buy More** button. This will show you a list of all available virtual machine configurations along with their prices.



Once you've chosen the desired plan, you'll be asked for the following details to create the virtual machine:

- **Name** of the virtual machine.
- The **VPC** or **network** for this machine to be a part of.
- The **tier** or **subnet** for this machine to be in.
- Option to use **SSH keys** with the virtual machine. *This option can be accessed later.*
- If there are **promo/discount codes** available for this purchase, you'll be shown those options.
- An option to receive the machine's **password on email**. *This option can be accessed later.*



Clicking on **Confirm Purchase** with the above information will provision the virtual machine inside the chosen VPC in your account.

Please note that this might take up to 5-8 minutes. You may use the CloudConsole during this time, but it is advised that you do not refresh the browser window.

Once ready, you'll be notified of this purchase on your email address on record. The newly created virtual machine can be accessed from **apiculus Cloud > Virtual Machines** on the main navigation panel.

Additionally, you can also navigate to **apiculus Cloud** > **VPC**, into the target VPC, and see the virtual machine count on the tier that you've just added this machine to. In the tier options menu (3 vertical dots, next to the tier name), you can select the **View Attached Virtual Machines** option to see all the virtual machines attached to this tier.

Adding Public IPs

Public IP addresses need to be added to a VPC for a variety of use cases. While all VPC Virtual Routers get their own default bundled public IP address, you need to purchase additional IPs for load balancing, for accessing the contained virtual machines, for static NAT etc.

To add a public IP address to a VPC, follow these steps:

1. Navigate to **Marketplace** > **Network Services**.
2. Choose the appropriate **region** and **zone** from the dropdown menu on top.
3. **Activate** the IP address plan listed under **IP Addresses** in the marketplace.
4. Alternatively, you can also navigate to the **apiculus Cloud** > **VPC** section on the main navigation panel, select the appropriate **region** and **zone**, go to the target VPC, and click on the **+ Public IP** option. This will list all the available options for IP addresses.

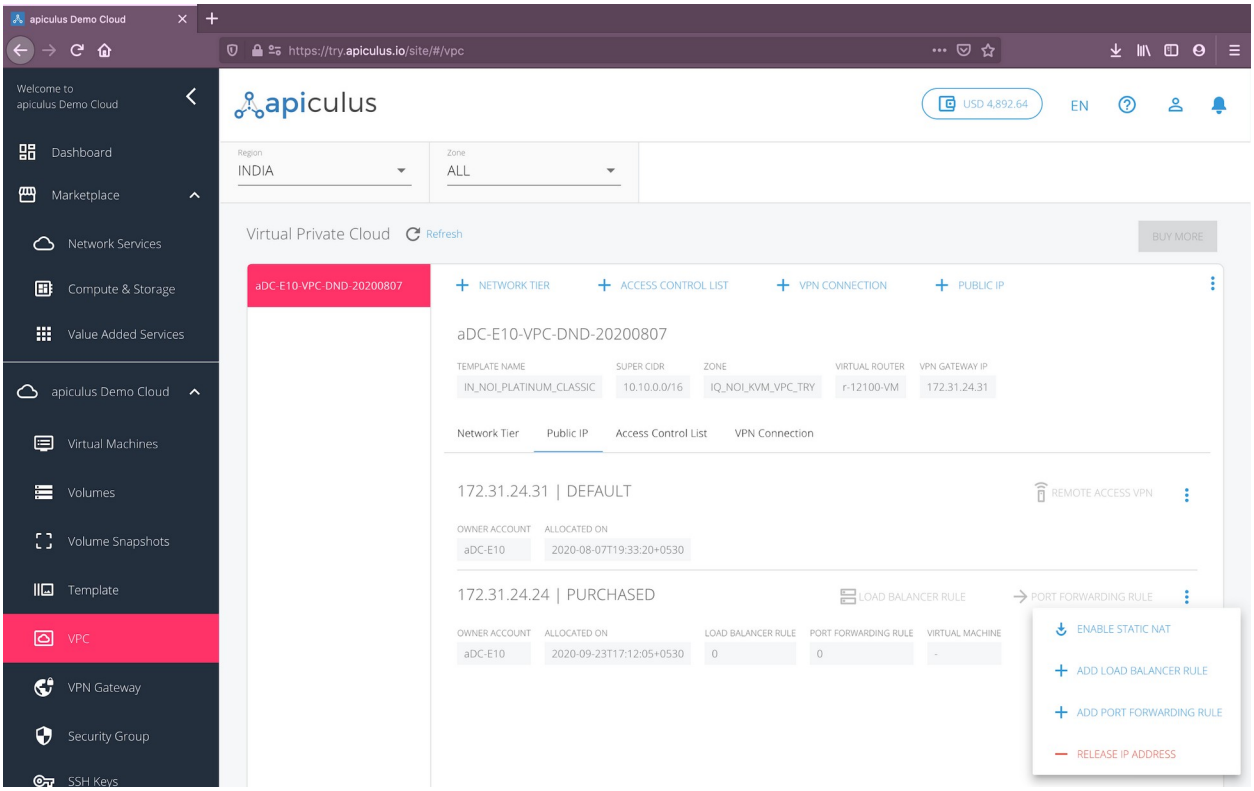
Once you've chosen to activate the public IP address plan, you'll be asked for the following information:

- The **VPC** to use this IP address with.
- If there are **promo/discount codes** available for this purchase, you'll be shown those options.

Clicking on **Confirm Purchase** with the above information will allocate a public IP address inside the chosen VPC in your account.

Please note that this might take up to 5-8 minutes. You may use the CloudConsole during this time, but it is advised that you do not refresh the browser window.

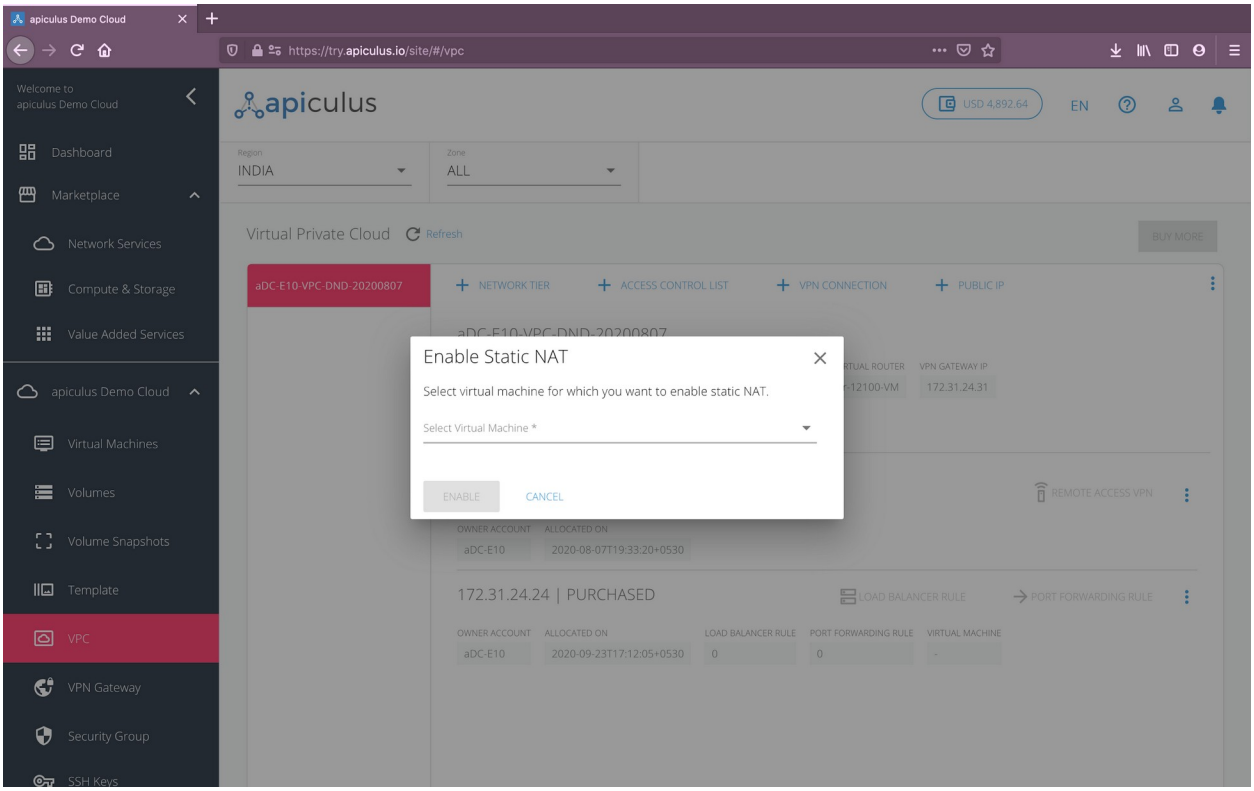
Once ready, you'll be notified of this purchase on your email address on record. The newly allocated IP address can be accessed from **apiculus Cloud** > **VPC** on the main navigation panel, and then going into the target VPC and navigating to the **Public IP** tab next to **Network Tier**.



A public IP address can be used for configuring further access into the VPC, as described in the following subsections, by choosing the options from the IP address menu (3 vertical dots next to the IP address). *Please note that one public IP can only be used with one of the available configurations. To use more than one configuration, you'll need to purchase additional public IP addresses.*

Configuring Static NAT

Choosing the **Enable Static NAT** will allow you to use this public IP as a static translation to any of the contained virtual machines. To use this as a static NAT, choose the virtual machine you want to translate this public IP to in the dialog box that opens and click on **enable**.



To test whether static NAT has been configured correctly, you can use the public IP to SSH into the virtual machine that the IP is NAT-ing to.

Configuring Load Balancing

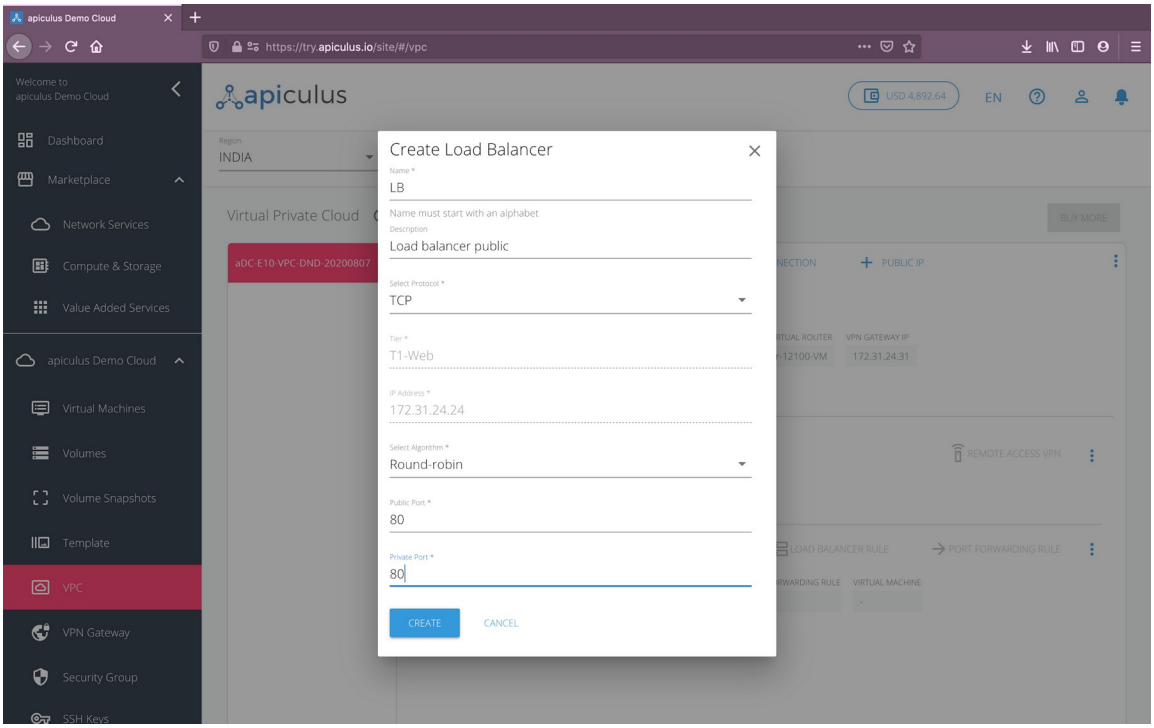
Choosing **+ Add Load Balancer Rule** from the menu will enable this IP address to be used as a load balancer. You'll be asked the following details to first set this up as a load-balancing IP:

- A **name** and **description** for the load balancer rule.
- **Protocol** to use for the load balancer.
- The **load balancing algorithm** to use.
- **Public** and **private** port mapping.

Once the load balancer rule has been created, you can now go into the load balancer and add (or remove) virtual machines to this rule. To do this, follow these steps:

- Click on the **Load Balancer Rule** option next to the IP address listing, which would've got enabled now.
- In the dialog box that opens, click on **Add/Remove Virtual Machines**.

- In the overlay box that opens, you'll be able to see virtual machines that are part of this load balancer, and the machines that are available to be added to this load balancer. Click on add (or remove) and **confirm** to update the load balancer rule.



To test whether the load balancer has been configured correctly, you can log into the virtual machines that are behind this load balancer individually, create an index.html on each virtual machine (with different content), and access the public IP address directly from your browser. If configured correctly, each browser page refresh should take turns in loading the two index.html pages.

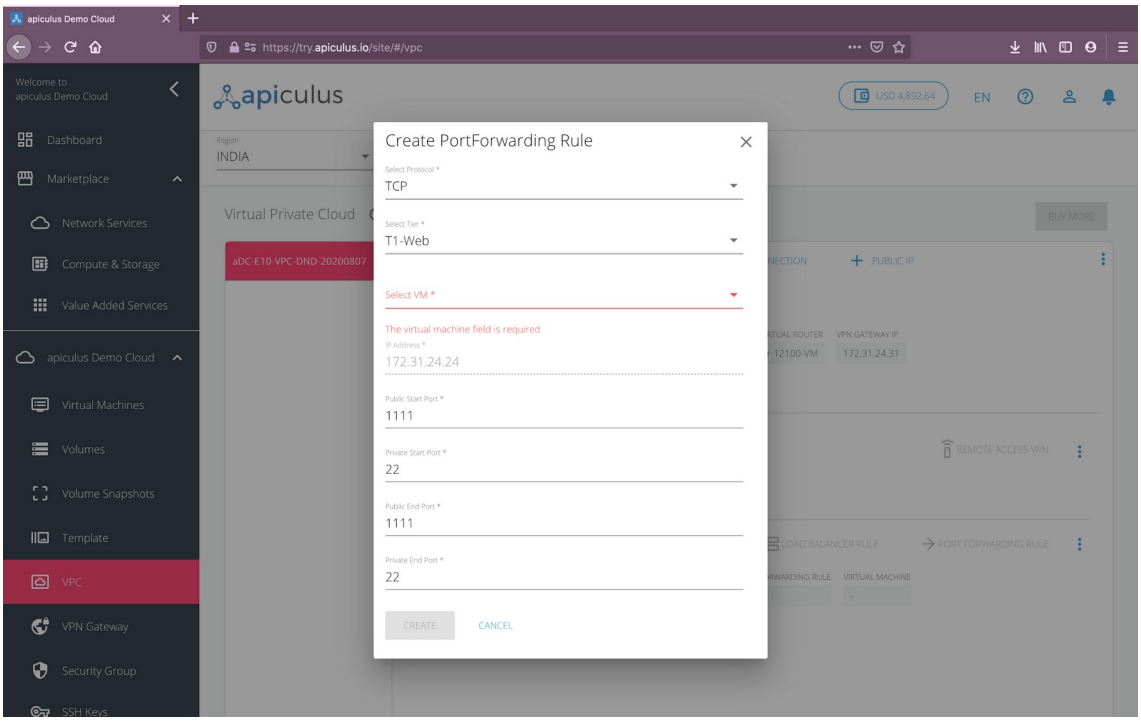
Please note that a load balancer IP rule can only be configured if the tier/subnet type is set up ***Public IP****.*

Configuring Port Forwarding

A port forwarding rule is required for accessing the virtual machines contained in a VPC. Since virtual machines in a VPC only have a private IP address, a public IP address is required for each virtual machine that you want to access from your terminal.

Choosing **+ Add Port Forwarding Rule** from the IP address menu will enable this IP address to be used as a port-forwarding IP. You'll be asked the following details to first set this up as a port-forwarding IP:

- **Protocol** for port-forwarding.
- The **tier** and the **virtual machine** to port-forward to.
- **Public** and **private port** ranges. *Please note that the **end ports** should be equal to or greater than the **start ports**.*



Once the port-forwarding rule has been created, you can now go into the port-fowarding IP address and view details of this rule. To do this, follow these steps:

- Click on the **Port Forwarding Rule** option next to the IP address listing, which would've got enabled now.
- In the dialog box that opens, you can view the virtual machine that this rule has been configured on along with the private and public port range mappings.

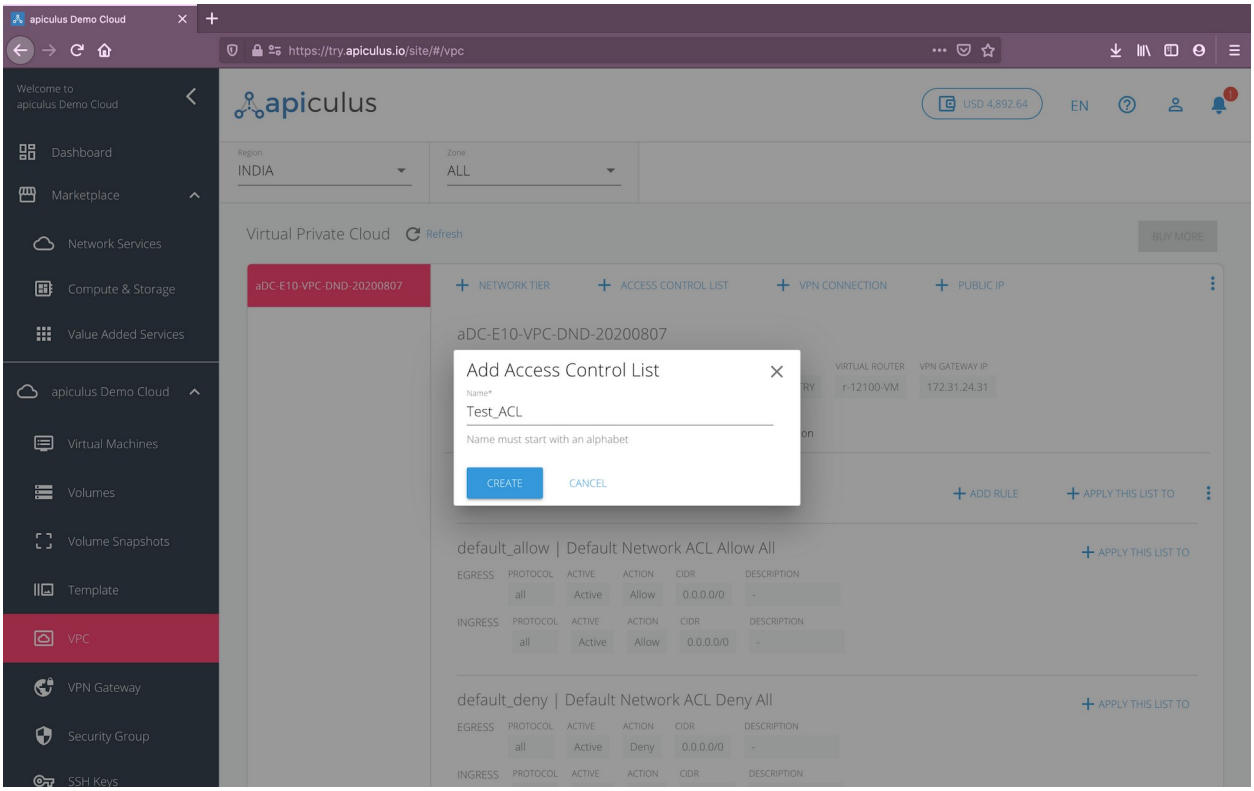
To test whether port-forwarding has been configured correctly, you can use the public IP to SSH into the virtual machine that the IP port-forwards to.

Please note that a port-forwarding IP address can be used to configure multiple port-forwarding access rules but with one virtual machine. To port-forward into a different virtual machine, you'll need to purchase an additional public IP address.

Configuring Access Control Lists

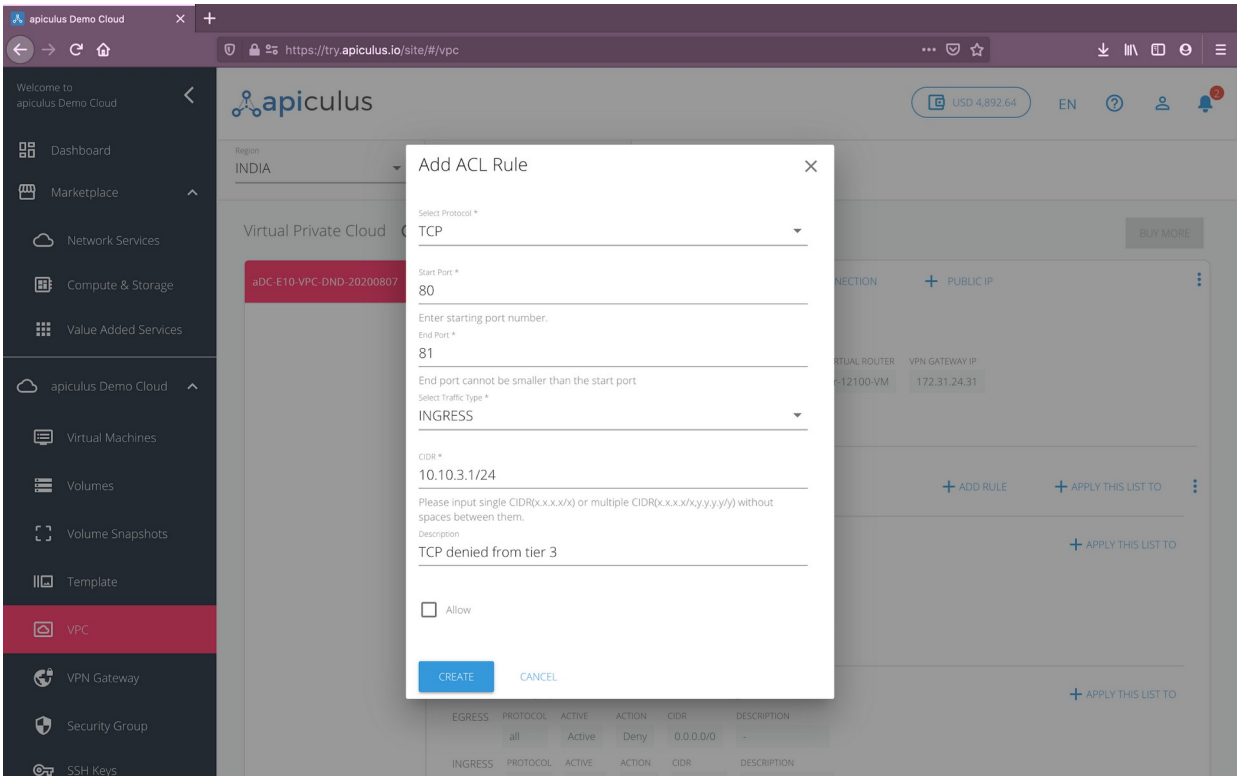
Access control lists let you define policies around inbound and outbound traffic. An access control list is a collection of ingress and egress rules, which specify whether to allow or deny traffic from/to an individual IP or a range of IP addresses.

To create an access control list, navigate to **apiculus Cloud** > **VPC**, go to the target VPC and click on the **+ Access Control List** option on the VPC actions menu. Doing so will ask you to provide a name for the access control list and create an empty list for you to add your custom rules to. *Please note that there are two default access control lists available for all VPCs, which can not be modified.*



Once the empty list has been created, navigate to the **Access Control Lists** tab next to the **Network Tier** and **Public IP** tabs. Follow these steps to add access policies to the access control list:

- Click on the **+ Add Rule** option next to the target access control list name.
- In the dialog box that opens, specify the following:
    - Traffic **protocol**.
    - Traffic **type**.
    - Traffic **source** or **destination**. *This can be a single IP (w.x.y.z), an IP range specified as a CIDR (x.x.x.x/x), or a comma-separated set of CIDR values (x.x.x.x/x, y.y.y.y/y).*
    - A **description** of this rule.
    - Whether this is an **allow** or a **deny** policy.



- Click on **create** to create this policy in the access control list.

Once you've created the policies, you can use the **+ Apply This List To** option to use this access control list with any of the tiers within the VPC.