NE-ONE™

AWS Installation Guide

Revision 3

Reproduction

Warranty

All information is believed to be true and correct at time of print. Information in this document is subject to change without notice and does not represent a commitment on the part of Calnex.

Calnex makes no warranties, expressed or implied of any kind with regards to this material or its products, including the implied warranties of merchantability and fitness for a particular purpose.

Calnex shall not be liable for errors contained herein or for incidental or consequential damage in connection with the furnishing, performance or use of this material or supplied products.

Please note: there are no internal serviceable parts in any equipment supplied by Calnex. Opening the hardware voids all warranties.

Trademarks

Calnex NE-ONE is a registered trademark of Calnex. Other trademarks are the property of their respective owners.

Table of Contents

This page is intentionally left blank.

CHAPTER 1 ABOUT THIS TECHNICAL PUBLICATION

1. INTRODUCTION

This Installation Guide describes how to install and configure the NE-ONE Cloud Appliance on the Amazon Web Services (AWS) cloud computing platform, and is intended for administrator users with knowledge of AWS.

2. ASSOCIATED DOCUMENTS

This Installation Guide refers to the *NE-ONE User and Administration Guide*.

3. DOCUMENTATION CONVENTIONS

The following conventions are used in the text of this document to distinguish particular types of information:

3-1. Special emphasis in text

The following table shows the types of emphasis used to distinguish particular elements in the text of this document:

Font Convention	Identifies
Bold	Graphical user interface (GUI) elements such as buttons, tiles, panels, menu items, fields, radio buttons, check boxes, etc. Command names, variable values, field values and executables.
Italic	Document names, external references to other documents, internal references and hyper links.
`Monospace`	File names, pathnames, variable names, File contents, program output, code examples, and command line interface (CLI) examples / syntax.
`Monospace bold`	Commands and text that users are instructed to enter at the keyboard.

3-2. User interface conventions

The following conventions are used:

- All button options are represented with the word on the button in bold font.
  For example, the Next button is represented as **Next**.
  All menu options are represented with the option name in bold. For example, the Connect option is represented as **Connect**.
- When an instruction to select a menu option is given, the path to the menu option is represented with the menu options in bold typeface and each level separated by a greater than symbol (>).
  For example, to select the Open command from the File menu you will be instructed to select the **File > Open** command.

3-3. Entering and typing

Depending on the situation, you may be instructed to type or enter a command or string of text. When you are required to press the return key after typing a command or string of text, the actual command or string of text is prefixed by enter or entering. For example, in a command line interface (CLI) you are instructed as follows:

Change to the `temp` directory by entering:

```
cd temp
```

In some cases you are not required to press the return key after typing a command or string of text, for example:

- field entries in a graphical user interface (GUI)
- typing a menu option in a CLI which does not require you to press the return key.

In these cases you are instructed to type the appropriate command or string of text. For example, to specify your name in a GUI field you are instructed as follows:

Type your first name in the **First Name** field.

3-4. Mouse Buttons

It is assumed that the left mouse button is the primary one.

3-5. Definition of Notices and Notes

! Notice:

Used for instructions to the user to prevent damage to property.

Note:

Used to draw attention to information that is important for the user to know.

4. CONTACT INFORMATION

If you need to contact Calnex regarding the installation or use of the NE-ONE, please do so using the following channels:

Postal Address	Calnex Solutions plc Oracle Campus Linlithgow West Lothian EH49 7LR United Kingdom
Telephone (Calnex EMEA and other regions)	+44 (0)1799 252 200
Telephone (Calnex Americas)	+1 888-448-4366
Global support email	support@ne-one.com
Website	http://www.ne-one.com

CHAPTER 2 INSTALLATION

The instructions in this chapter describe how to create and configure the NE-ONE Cloud Appliance using the AWS Virtual Private Cloud (VPC), the EC2 Amazon Elastic Compute Cloud instance, and the Amazon Machine Image (AMI).

Note:
For brevity the term "NE-ONE Cloud Appliance" is referred to as NE-ONE in the rest of this chapter.

1. PREREQUISITES

For the NE-ONE to function as expected, the following AWS services are required:

- A VPC.
- At least 3 Subnets (i.e. a Subnet for the NE-ONE's Management port, and a Subnet for each of the licensed hardware ports on the NE-ONE).

Note:
The number of Subnets you require vary according to the number of licensed ports you have with your NE-ONE. For example, an NE-ONE with four licensed hardware ports will require 5 Subnets (i.e. one Subnet for the Management port, and one Subnet for each of the licensed hardware ports).

- Either an Internet Gateway or VPN access into your VPC.
- Security Groups configured to allow the relevant connections to the NE-ONE.

The procedures in the sections below describe the configuration of these required services along with the NE-ONE.

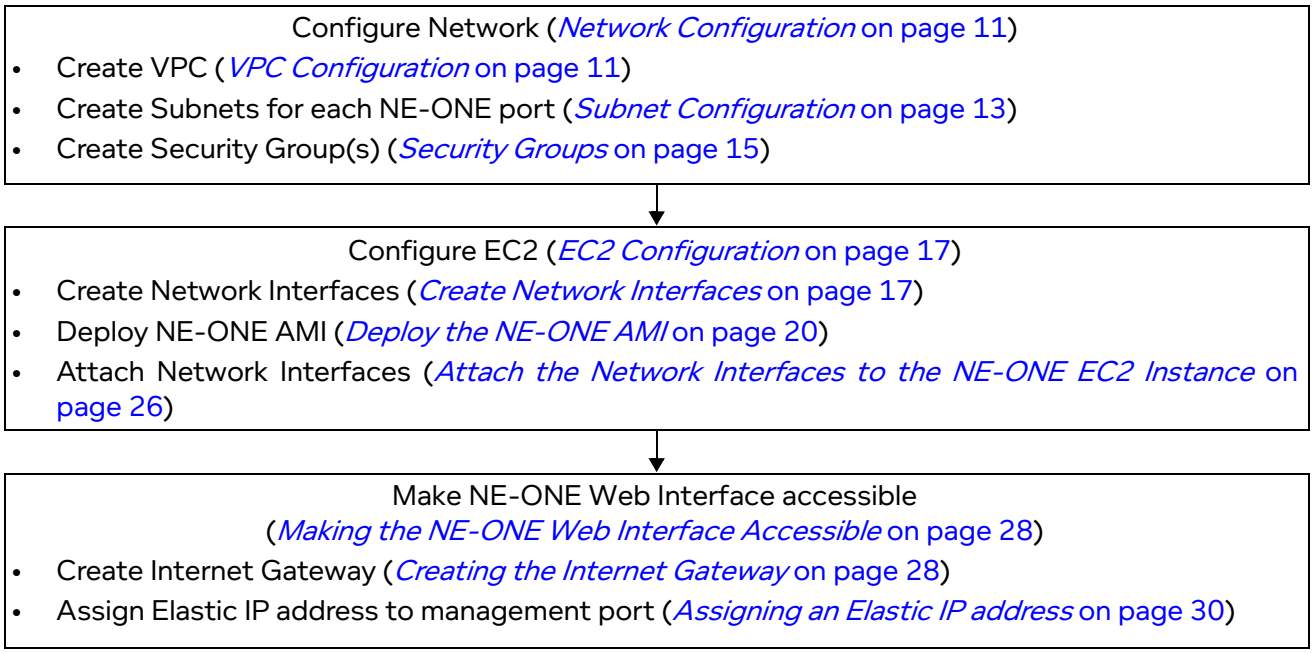
Note:
All of the procedures in the sections below assume that you are logged in to AWS.

Note:
All of the procedures in the sections below assume that you have the **New EC2 Experience** and **New VPC Experience** switches activated within AWS.

1-1. Installation Overview

Illustration 1 provides the installation overview of the NE-ONE on AWS, highlighting the order in which you must undertake the different installation procedures. In order to understand the context of the installation of the NE-ONE on AWS, also review the example functional overview in *NE-ONE Functional Overview* on page 8.

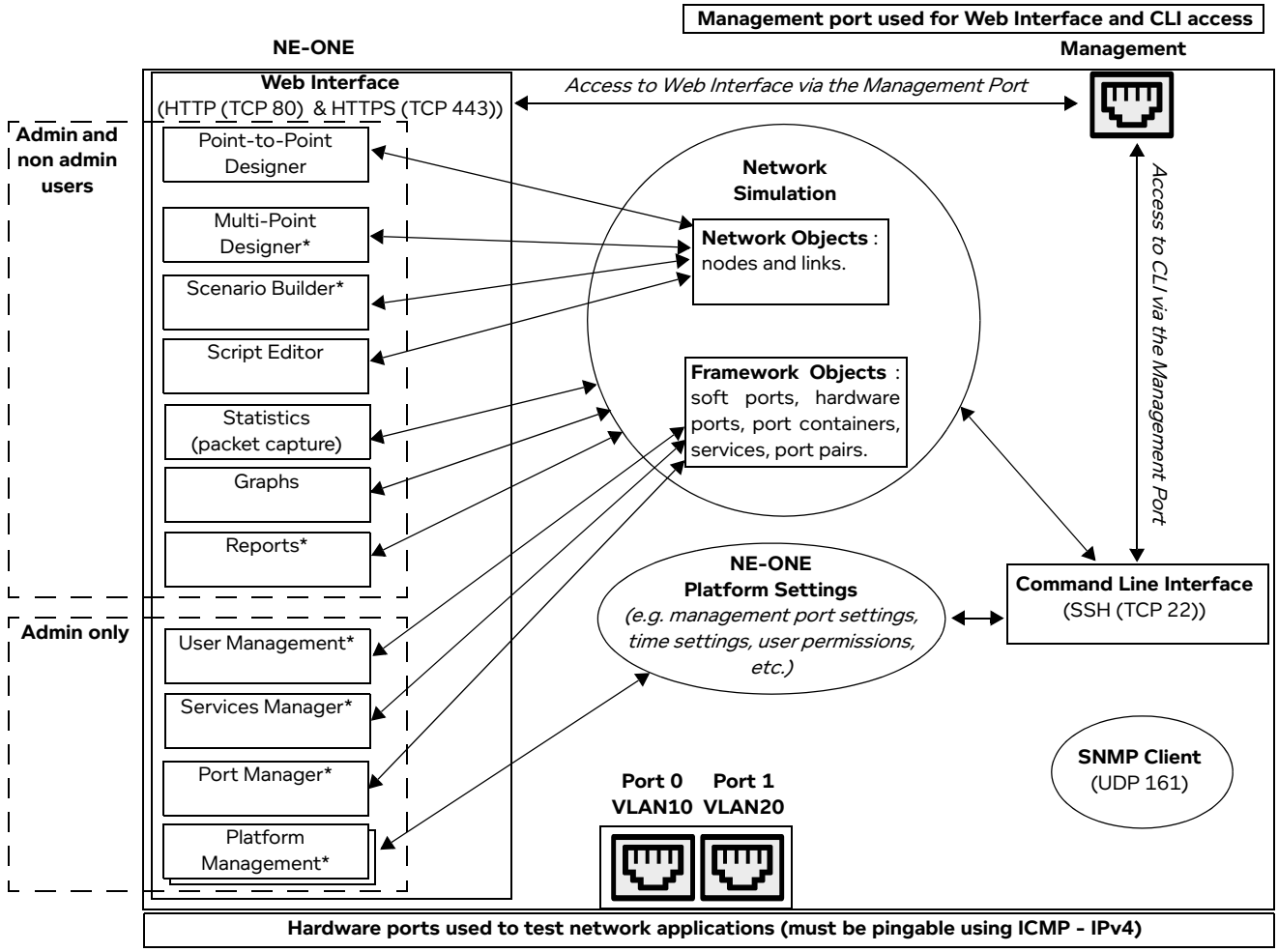
ILLUSTRATION 1 - INSTALLATION OVERVIEW



1-2. NE-ONE Functional Overview

Illustration 2 shows a high-level functional overview of the NE-ONE. The NE-ONE has a powerful and intuitive Web Interface with different pages, allowing admin users to administer all aspects of the NE-ONE, and allowing non-admin users to create and run Software Defined Test Networks (SDTNs) for network application testing purposes.

ILLUSTRATION 2 - HIGH-LEVEL FUNCTIONAL OVERVIEW OF THE NE-ONE



Note:

Traffic cannot pass between the management port and hardware ports.

Note:

The asterisk (*) in *Illustration 2* indicates that some or all of the Web Interface is associated with a premium feature. For more information about the NE-ONE Web Interface, refer to the *NE-ONE User and Administration Guide*.

In the example of *Illustration 2*, two hardware ports are licensed. In this example, for the installation sections below):

- The two hardware ports will have Subnets called VLAN10 (IPv4 CIDR Block: 10.0.10.0/24 Subnet) and VLAN20 (IPv4 CIDR Block: 10.0.20.0/24 Subnet) created, respectively.
- The Management port will be have a Subnet called Management (IPv4 CIDR Block: 10.0.100.0/24 Subnet) created.
- A Security Group and applied to the Network Interfaces will be set up allowing the following traffic to pass
  - HTTP - this will be used by the NE-ONE Web Interface
  - HTTPS - this will be used by the NE-ONE Web Interface
  - Custom UDP - 161 - this will be used by the NE-ONE SNMP Client
  - SSH -this will be used by the NE-ONE Command Line Interface

  - All ICMP - IPv4 - this allows you to ping all the hardware ports on the NE-ONE
- The two hardware ports will have Network Interfaces created for them, will be named Port 0 and Port 1, and will have the Security Group applied to them.

Note:
If the license for your NE-ONE has more than two licensed hardware ports, you must create Subnets and Network Interfaces for each of the licensed hardware ports.

Note:
By default the EC2 already has one default Network Interface automatically created for it, whose description is called the **Primary network interface**. This Network Interface will not be changed in our example, and is used for the Management port of the NE-ONE.

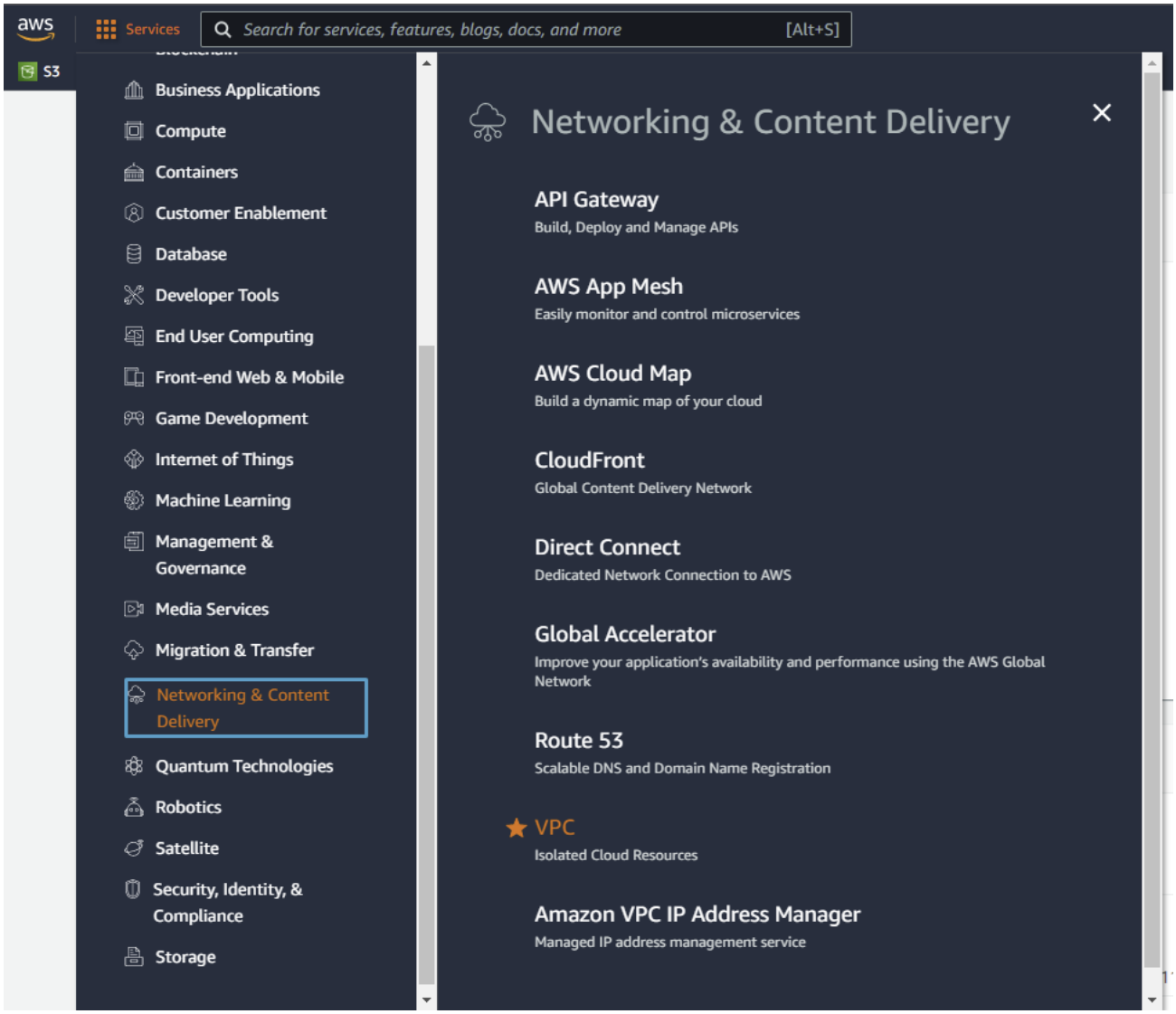
2. NETWORK CONFIGURATION

You may already have your AWS network configured. However, Calnex recommend that you still follow this section to ensure your current AWS network configuration is compatible with the NE-ONE.

2-1. VPC Configuration

The first element required as part of the installation for NE-ONE in AWS is to create a VPC in which to contain all parts of your test environment.

1. Click the **Services** drop-down menu.
2. From the variety of different services provided, select **VPC** from within the **Networking & Content Delivery**.

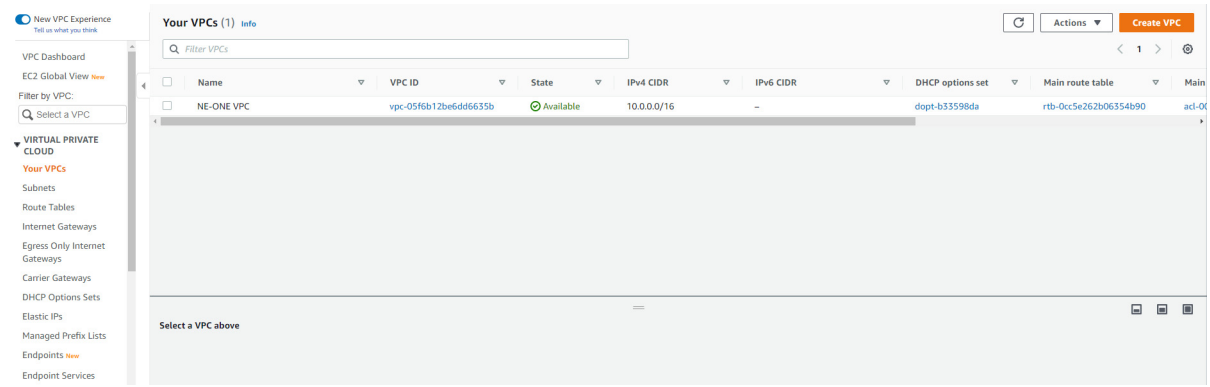


Note:

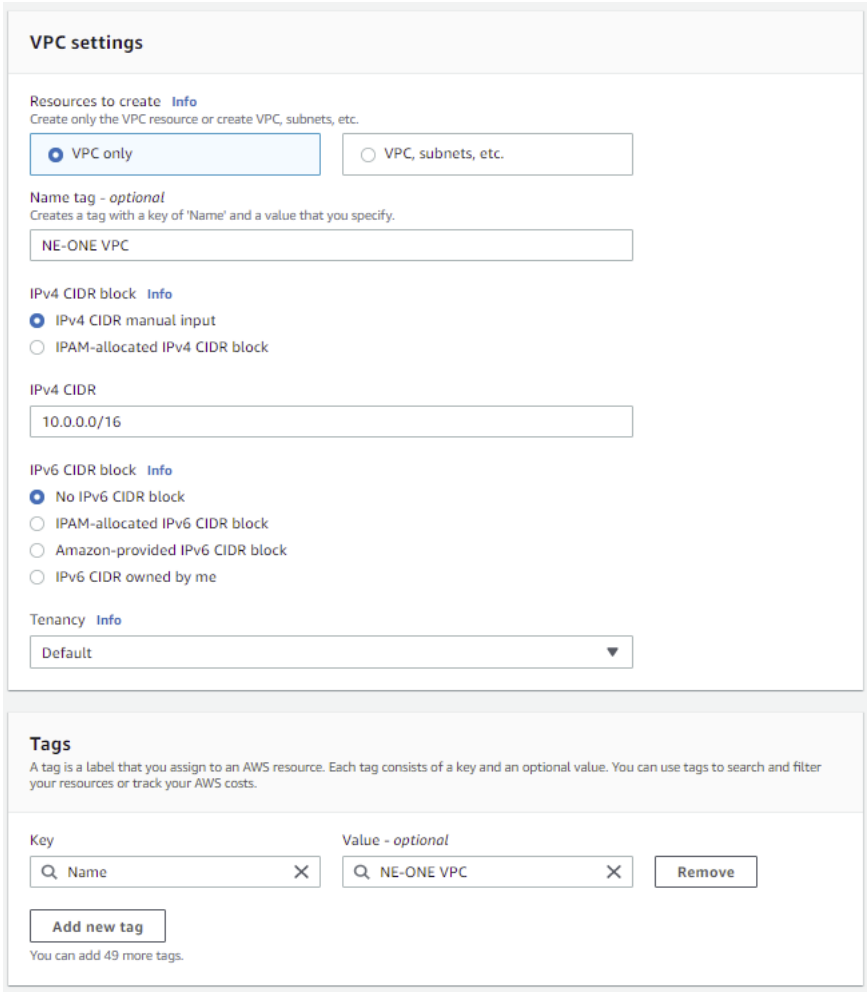
You can search for **VPC** either by finding it under the **Networking & Content Delivery** category or by using the search bar.

On the left hand side of the screen is a sidebar, which allows you to navigate around the VPC service screen.

3. On the **VPC** sidebar click on **Your VPCs**.



4. Click on the **Create VPC** button in the top right of the AWS interface to launch the Create VPC wizard.
5. From the **VPC settings** page that appears, do the following:



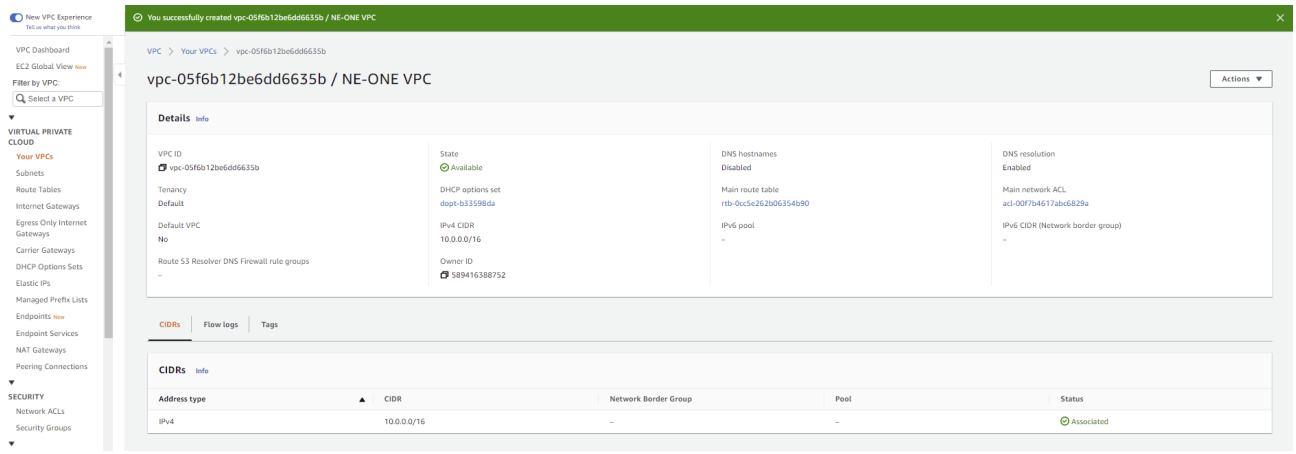
- Ensure that the default **VPC only** radio button is enabled.
- In the **Name tag** field, type an appropriate name. In our example, type **`NE-ONE VPC`**, although any recognizable name can be used.
- Leave the default **IPv4 CIDR manual input** radio button selected, and specify an appropriate private IP address range in the **IPv4 CIDR** field. In our example, **`10.0.0.0/16`** is used in the **IPv4**

CIDR field for the VPC address range, however any private IP address range can be used.

- Leave the default **IPv6 CIDR block** radio button selected.
- Leave the **Tenancy** drop-down field set to **Default**.

6. Click **Create VPC** to create the VPC.

   The VPC is created and you are automatically taken to the **VPC overview** page for the newly created VPC.



Once the VPC is created, configure the Subnets according to *Subnet Configuration*.

2-2. Subnet Configuration

Once a VPC is created according to *VPC Configuration*, you can create the Subnets used as part of the environment as described below.

You must specify the different Subnets that will be used by the NE-ONE, including a Management Subnet along with a Subnet for each Network Interface you want to use for the hardware ports on the NE-ONE.

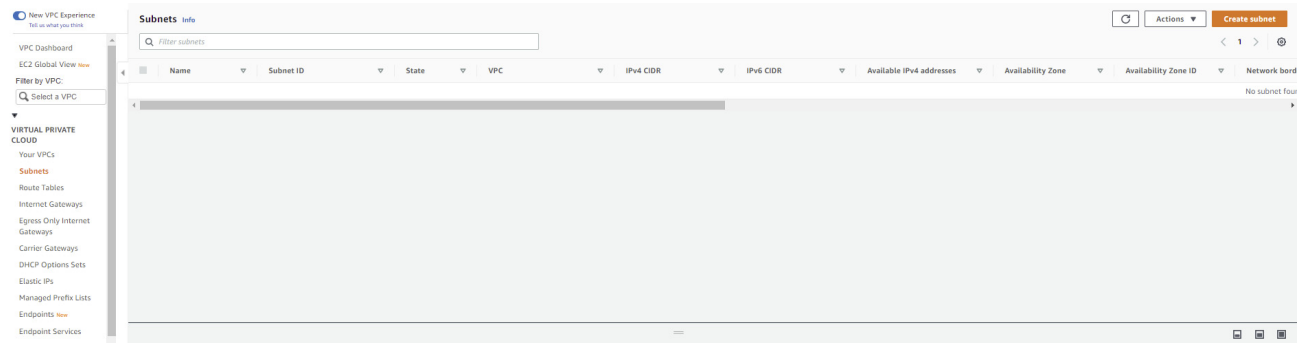
In the example below, the following three Subnets are created:

- Management
  IPv4 CIDR Block: 10.0.100.0/24
- VLAN10
  IPv4 CIDR Block: 10.0.10.0/24
- VLAN20
  IPv4 CIDR Block: 10.0.20.0/24

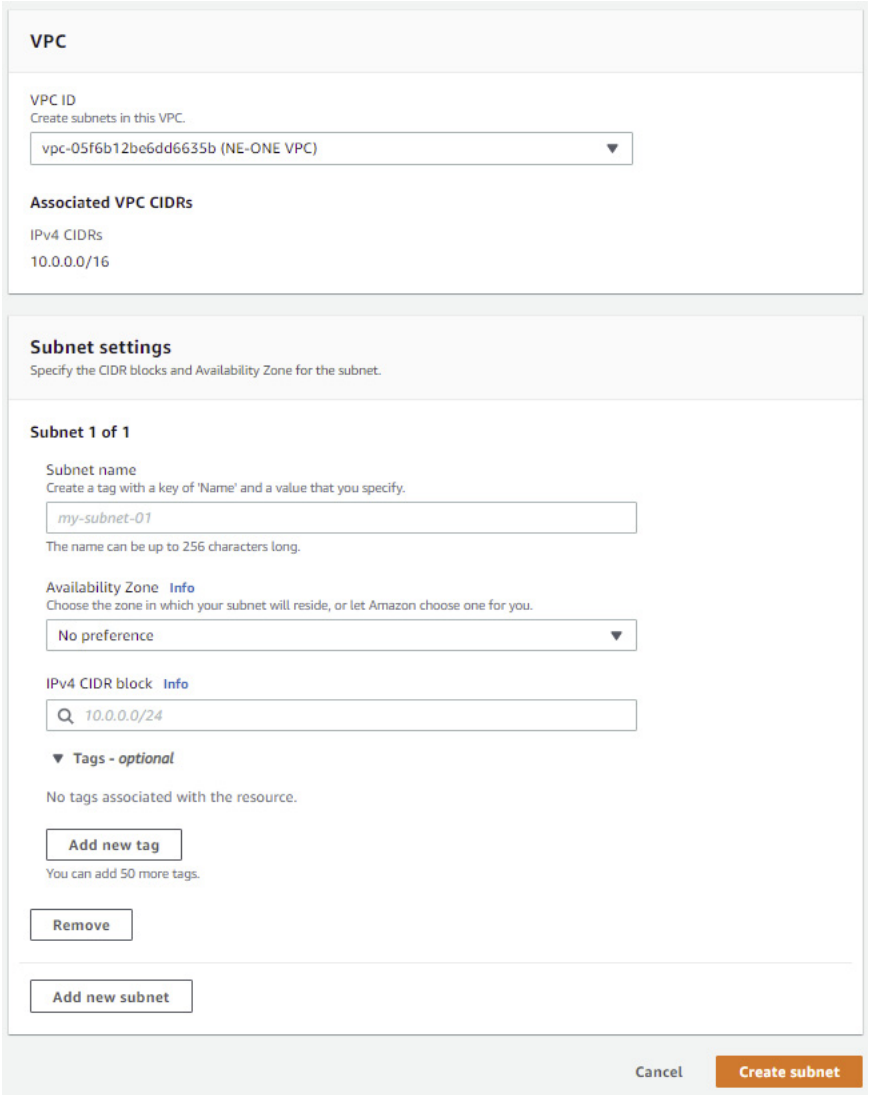
Note:
The IP range of these Subnets must be found within the VPC's range and not overlap.

Note:
Availability zones can be left default to be automatically assigned or assigned manually.

1. Click **Subnets** from within the sidebar.



2. Click the **Create subnet** button to launch the Subnet Creation Wizard.



3. From the Subnet Creation Wizard that appears, ensure that the correct VPC ID is selected (i.e. the VPC ID will contain the name that you created in *VPC Configuration* (in our example, NE-ONE VPC)), then click the **Add new subnet** button twice to create two addition Subnets in addition to the initial sole Subnet. Three Subnets will now exist within the **Subnet settings** section.
4. From the Subnet creation wizard that appears, in the **Subnet settings** section, do the following:

a. In the **Subnet 1 of 3** section, **Subnet name** field, type **`Management`** for the Subnet name.
b. In the **Subnet 1 of 3** section, **IPv4 CIDR block** field, type **`10.0.100.0/24`** for the Management's Subnet.
c. In the **Subnet 2 of 3** section, **Subnet name** field, type **`VLAN10`** for the Subnet name.
d. In the **Subnet 2 of 3** section, **IPv4 CIDR block** field, type **`10.0.10.0/24`** for the VLAN10's Subnet.
e. In the **Subnet 3 of 3** section, **Subnet name** field, type **`VLAN20`** for the Subnet name.
f. In the **Subnet 3 of 3** section, **IPv4 CIDR block** field, type **`10.0.20.0/24`** for the VLAN20's Subnet.

5. Click the **Create subnet** button to create the three Subnets that you defined in step 4.

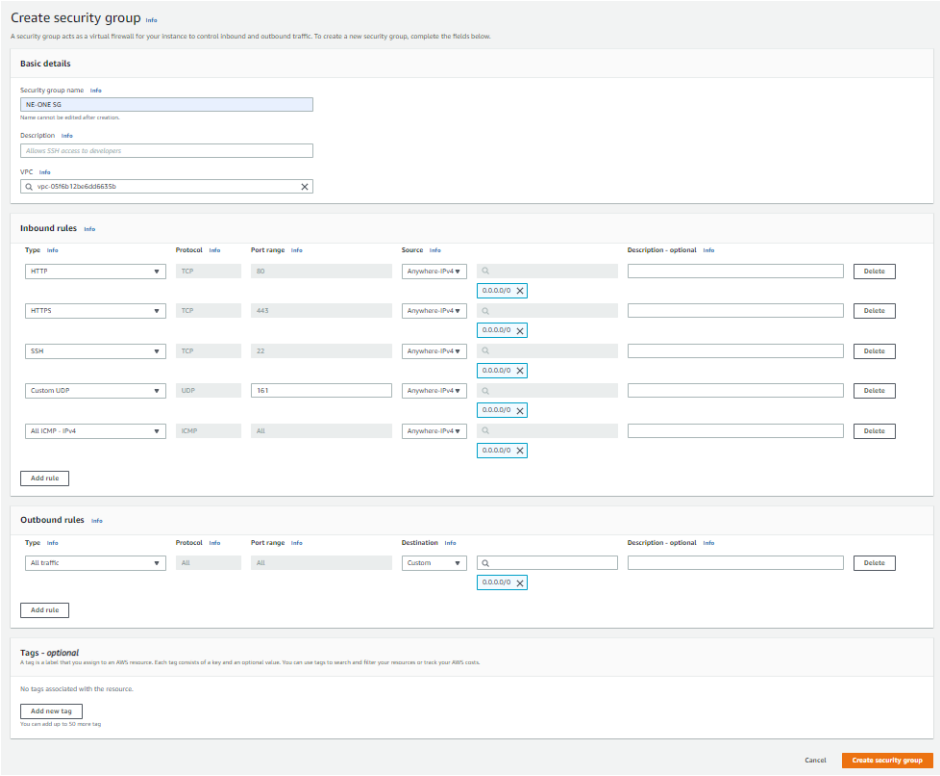
2-3. Security Groups

By default, all traffic is blocked on a VPC (i.e. there are no inbound rules defined), and no traffic can pass until you create a Security Group with appropriate inbound rules allowing appropriate NE-ONE related traffic to pass.

At this point we would be able to go and connect to any appliances in the VPC, however even though the networking is established, you must alter the security rules to allow traffic into the VPC. You can do this by going into **Security Groups** and assigning rules as required, for this we are going to allow global access into all ports.

This first Security Group will act as the main Security Group for the NE-ONE's Management port. This is how we connect to the NE-ONE via SSH as well as the Web Interface.

1. Click **Security Groups** in the sidebar, then click the **Create security group** button.
   The **Create security group** page appears.



2. Give the security group a recognizable name and a description to match the purpose, as follows:

a. In the **Security group name** field, type an appropriate security group name (e.g. in our example, type **`NE-ONE SG`**).
b. In the **Description** field, type an appropriate description (e.g. in our example, type **`Allows access to NE-ONE`**).

3. Under **Inbound Rules**, click the **Add rule** button for each of the inbound rule types that you want to add, and add the following inbound rules:
   - HTTP - this will be used by the NE-ONE Web Interface
   - HTTPS - this will be used by the NE-ONE Web Interface
   - Custom UDP - 161 - this will be used by the NE-ONE SNMP Client
   - SSH -this will be used by the NE-ONE Command Line Interface
   - All ICMP - IPv4 - this allows you to ping all the test interfaces (test ports) on the NE-ONE
4. Under **Outbound Rules**, leave the default values (i.e. **Type** set to **All traffic**, and **Destination** set to **Custom**).
5. Once you have finished creating all the inbound rules, click **Create security group**.

Note:
For the source, in our example above, we have used 0.0.0.0/0 to allow traffic of these types from all sources. If you want to limit access to the NE-ONE to specific IP address ranges, use those ranges instead.

Note:
These are the minimum requirements for the NE-ONE to function, however certain functionalities within the GUI may require further ports to be added. Documentation on this can be found within the product or by contacting support@ne-one.com.

Note:
For Network Interfaces other than the management interface on the NE-ONE, the Inbound Rules will depend on the types of traffic you are sending to the NE-ONE. Enabling ICMP - IPv4 will allow you to ping those interfaces.

Note:
Calnex recommend setting up additional security groups for these other Network Interfaces to limit the types of traffic that can access them, but for this example we will use the same (first) Security Group for simplicity.

3. EC2 CONFIGURATION

3-1. Create Network Interfaces

The next step is to configure the Network Interfaces, which will allow you to connect to the NE-ONE along with connecting your other applications for testing.

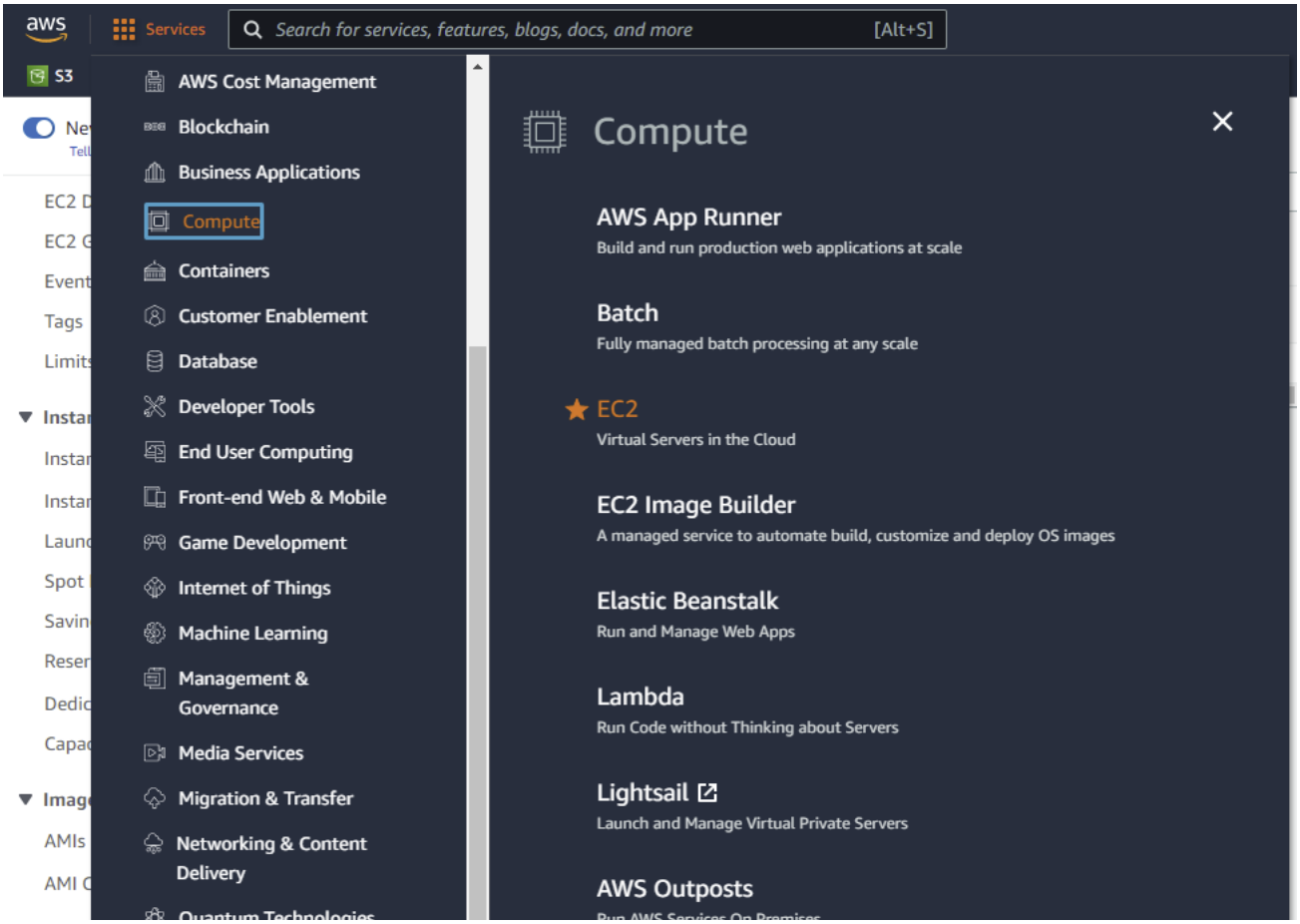
You must create a Network Interface for each Subnet that you previously created in *Subnet Configuration* on page 13, other than the Management Subnet, giving it a recognizable name and assigning it the Security Group that you previously created in *Security Groups* on page 15.

In the example below, the following Network Interfaces are created:

- Port 0
  Subnet : VLAN10
  Security Group : NE-ONE SG
- Port 1
  Subnet : VLAN20
  Security Group : NE-ONE SG

To do this, perform the following steps:

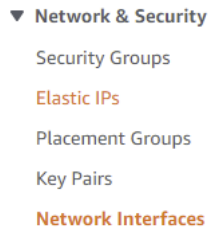
1. Click the **Services** drop-down menu.
2. From the variety of different services provided, select **EC2** from within the **Compute** category.



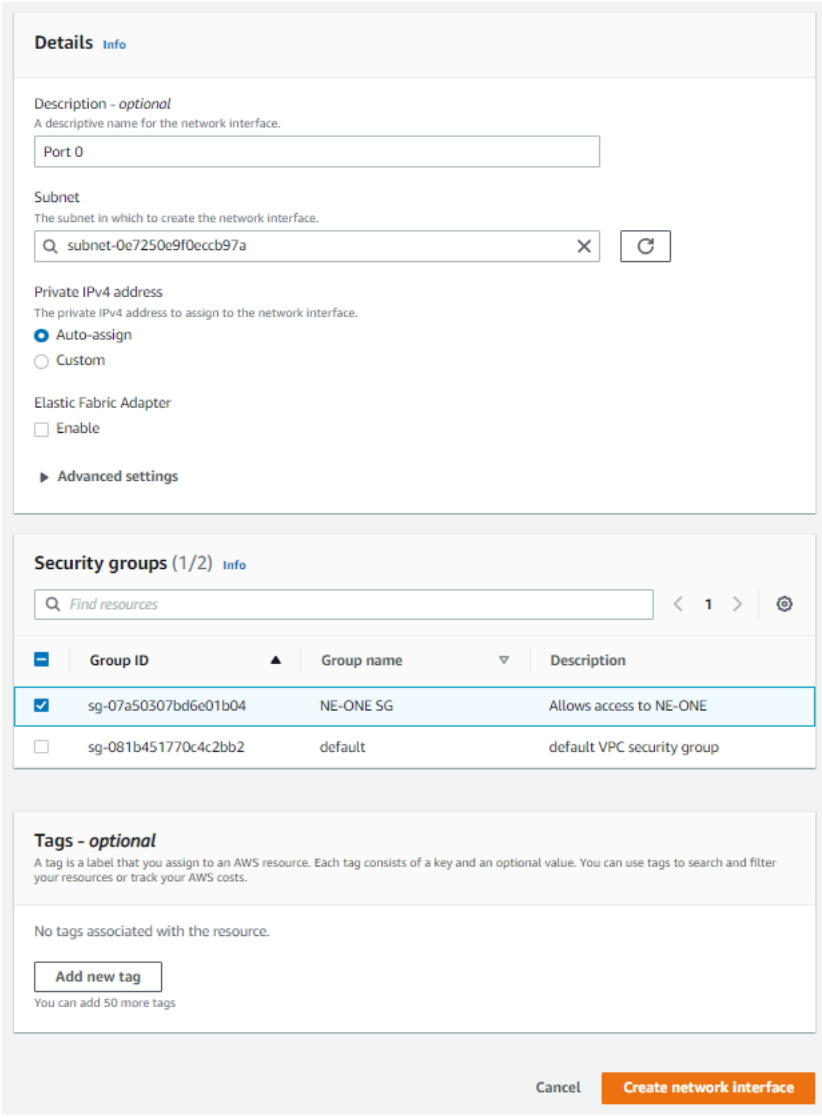
Note:

You can search for **EC2** either by finding it under the **Compute** category or by using the search bar.

3. From the **EC2** sidebar, click on **Network Interfaces** under **Network and Security**.



4. For each of the Network Interfaces that you want to create, click on **Create Network Interface**, then do the following in the **Network Interface Creation Wizard** that appears:



   a. In the **Description** field, type an appropriate description. For consistency with the hardware versions of the NE-ONE and the terms used within the documentation, Calnex recommend that you use Port 0, Port 1, etc.

      In our example, type Port 0 for the Subnet VLAN10 you previously created in *Subnet Configuration* on page 13.

      In our example, type Port 1 for the Subnet VLAN20 you previously created in *Subnet*

Configuration on page 13.

b. In the **Subnet** field, type the appropriate Subnet name to search for and select the Subnet that you previously created in *Subnet Configuration* on page 13.

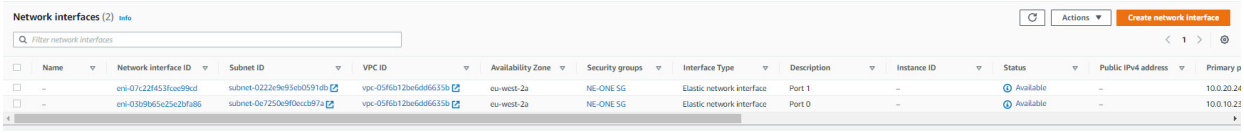
In our example, for the Port 0 description, search for and select the Subnet VLAN10.

In our example, for the Port 1 description, search for and select the Subnet VLAN20.

c. In the **Security groups** area, tick the check box associated with the NE-ONE SG Security Group that you previously created in *Security Groups* on page 15.

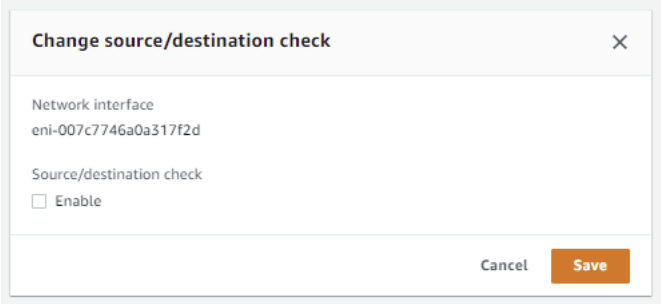
d. Click **Create network interface**.

The newly created Network Interface gets added to the EC2 within the **Network Interfaces** area under **Network and Security**.



5. In order for the newly created Network Interface to pass packets over the NE-ONE, you must disable source/destination checking. To disable source/destination checking, do the following for each of the newly created Network Interfaces:

a. Select the newly created Network Interface, click on **Actions** in the top right, and select **Change source/dest. check**.



b. From the **Change source/destination check** dialog box that appears, untick the **Enable** check box.

c. Click **Save**.

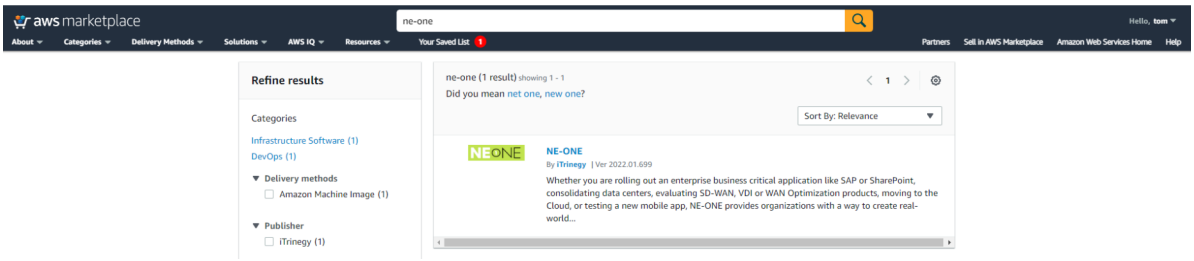
The Network Interfaces are now set up, and you are ready to deploy the NE-ONE AMI.

3-2. Deploy the NE-ONE AMI

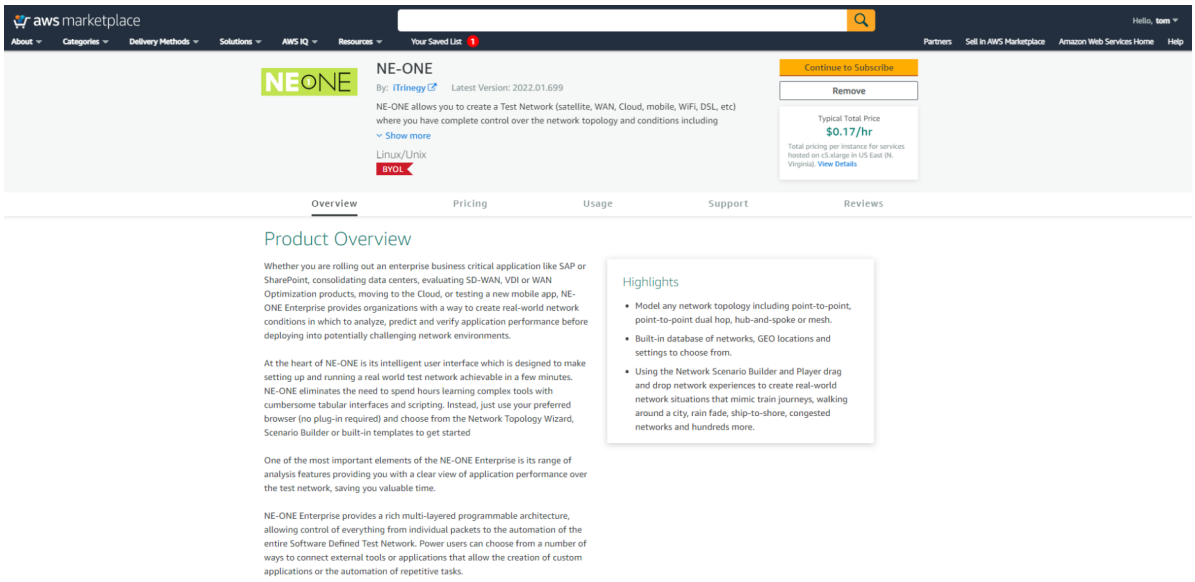
Now that the VPC has been set up with all the appropriate Subnets, Network Interfaces, and Security Groups, you must deploy the NE-ONE AMI on to them, using the steps described below.

1. Go to the AWS Market Place (*https://aws.amazon.com/marketplace*), and in the search bar, search for **NE-ONE**.

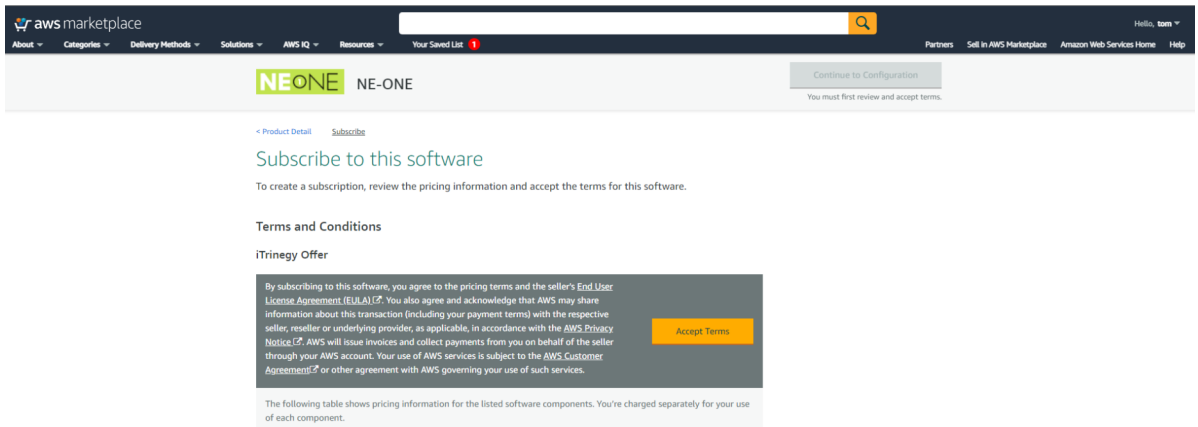
2. From the results that appear, click on the **NE-ONE** link.



3. From the **Product Overview** page that appears, click **Continue to Subscribe**.

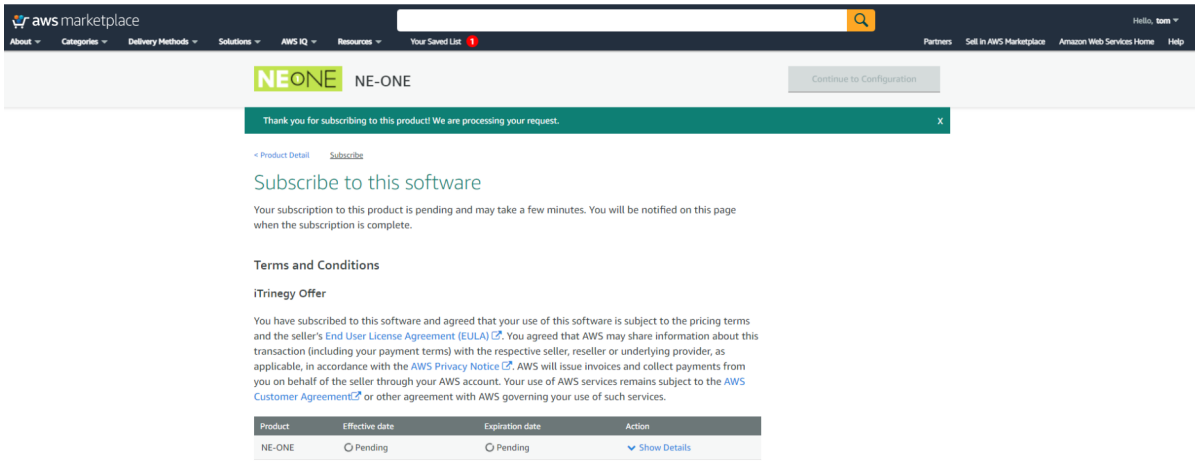


4. From the **Subscribe to this software** page that appears, click **Accept Terms**.

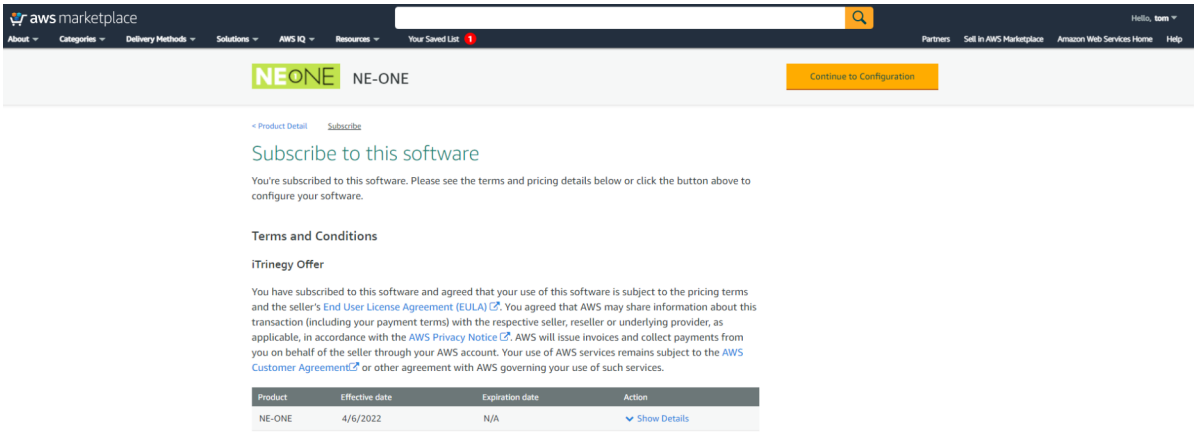


While the subscription is being processed, the **Continue to Configuration** button remains grayed

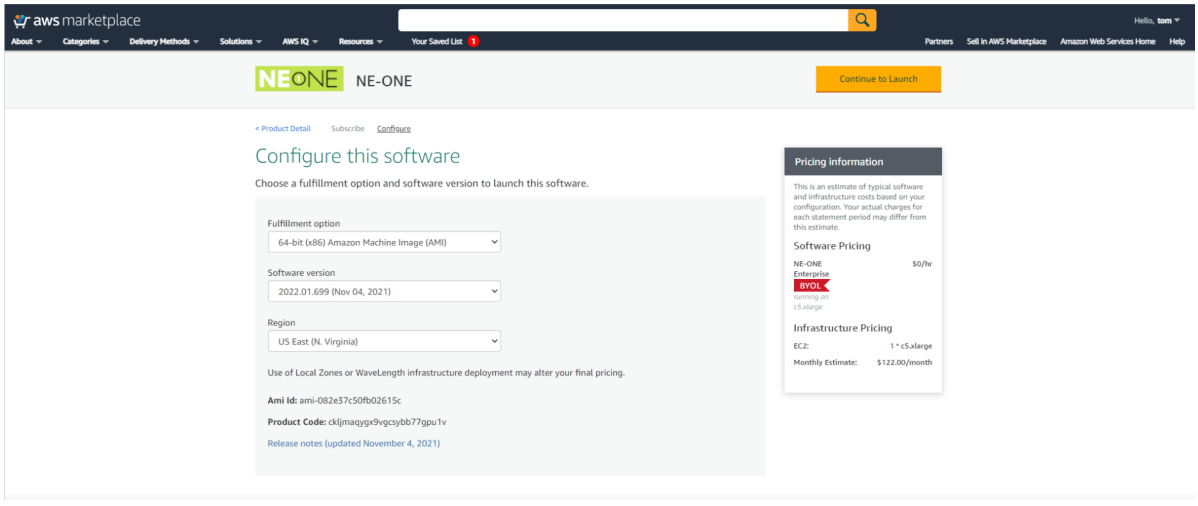
out and the **Effective date** and **Expiration date** show the **Pending** status.



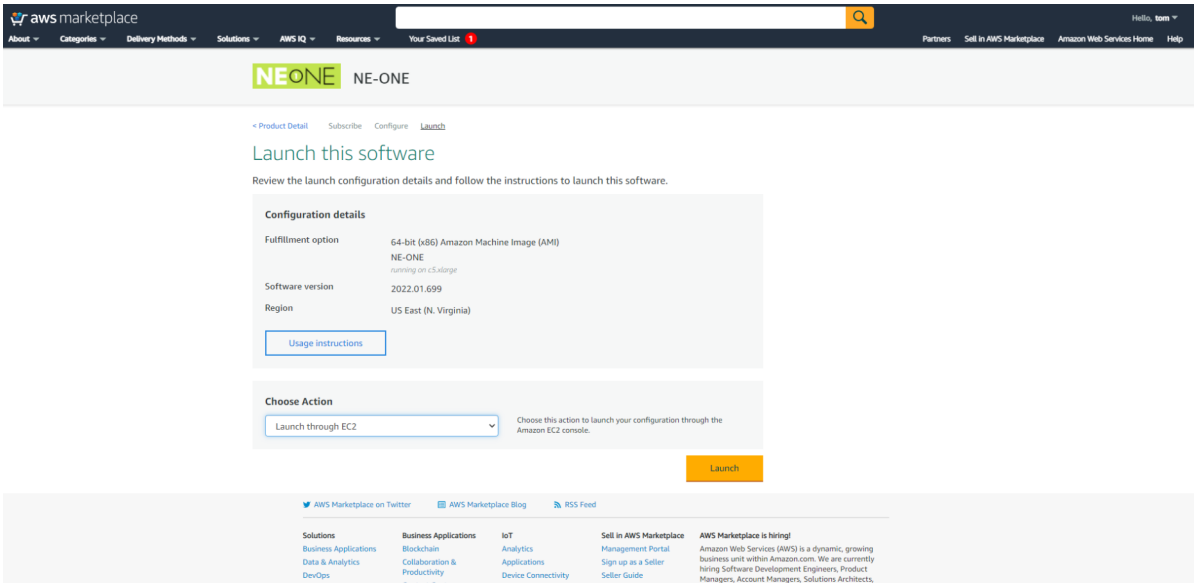
5. Once the subscription has been processed, click **Continue to Configuration**.



6. From the **Configure this software** page that appears, do the following:
   a. Leave the default **Fulfillment option** set to **64-bit (x86) Amazon Machine Image (AMI)**.
   b. Leave the default **Software version** set to the latest version.
   c. Select an appropriate region from the **Region** drop-down field.
   d. Click **Continue to Launch**.

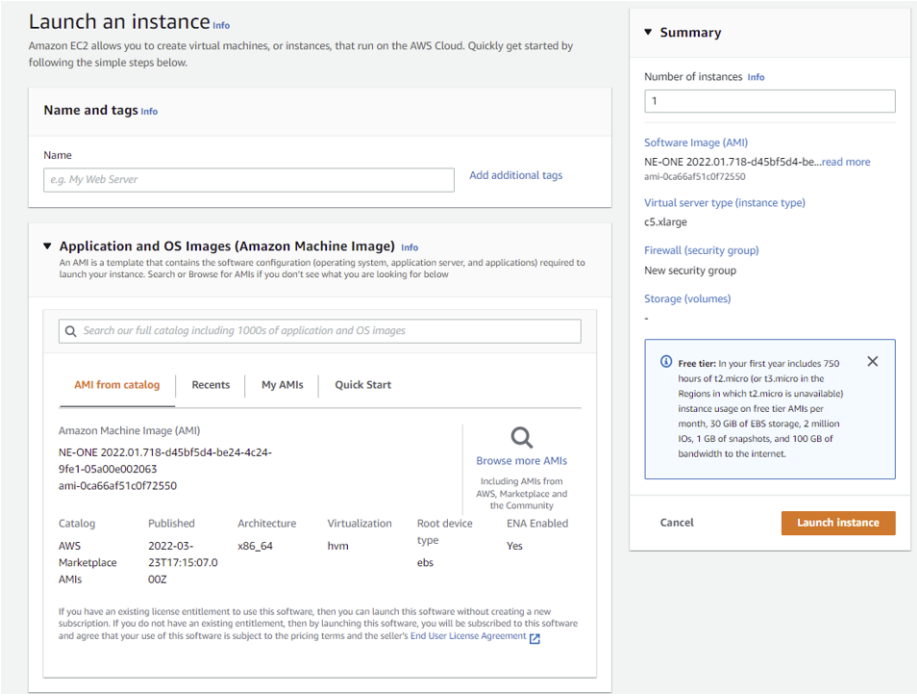


7. From the **Launch this software** page that appears, select **Launch through EC2** from the **Choose Action** drop-down field, then click **Launch**.



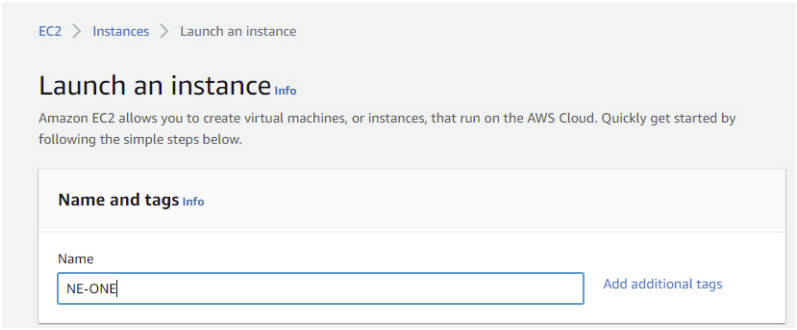
A **Launch an instance** page appears, containing the following:

- A fixed **Summary** area on the right containing the summary of the EC2 instance that is being created with a **Launch instance** button.
- A scrollable area on the left containing different expandable areas, some of which you need to configure, will some of which you can leave set to the default values.

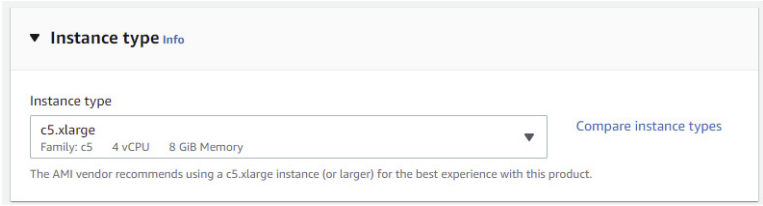


8. From the **Launch an instance** page that appears, do the following:

a. Scroll down to the **Name and tags** area, and type a desired name (e.g. **`NE-ONE`**) in the **Name** field.

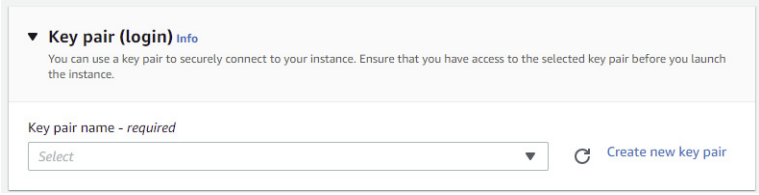


b. Scroll down to and expand the **Instance type** area, and select **c5.xlarge** from the **Instance type** drop-down field.

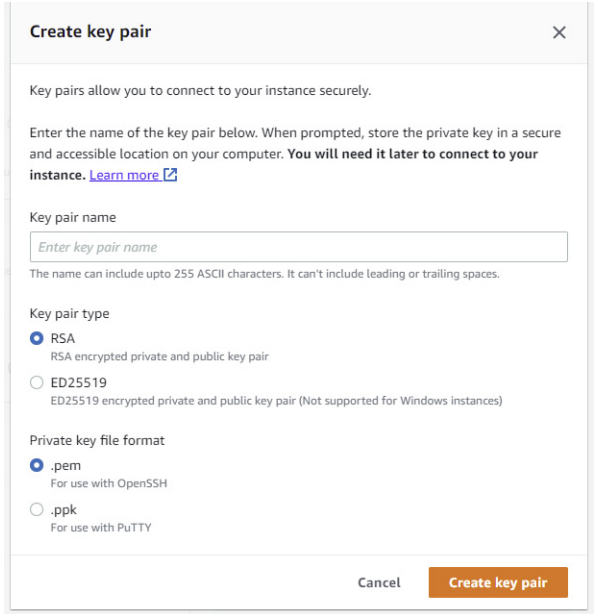


c. From the **Select an existing key pair or create a new key pair** dialog box that appears, either select **Create a new key pair** or use a key you currently have access to.

d. Scroll down to and expand the **Key pair (login)** area, then click the **Create new key pair** link.



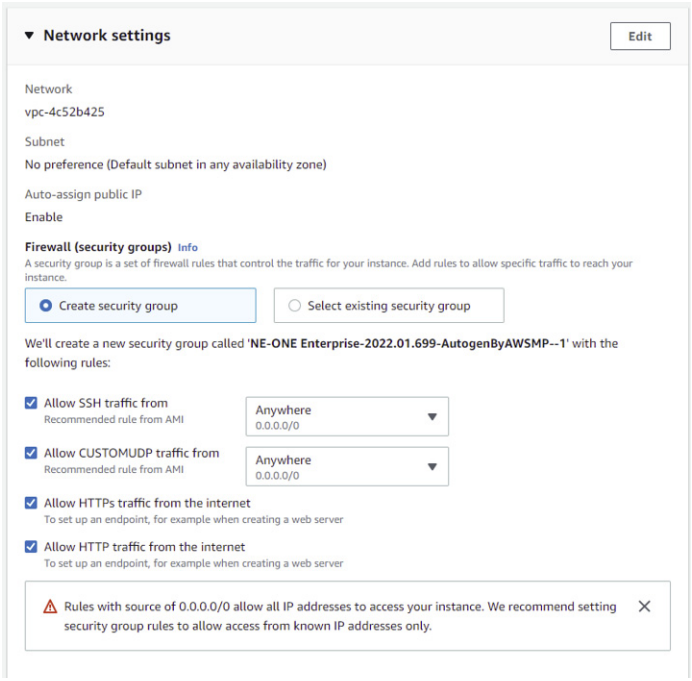
e. From the **Create key pair** dialog box that appears, type a desired key pair name (e.g. **`NE-ONE`**) in the **Key pair name** field, leave the **Key pair type** radio button set to **RSA**, leave the **Private key file format** radio button set to **.pem**, then click the **Create key pair** button.



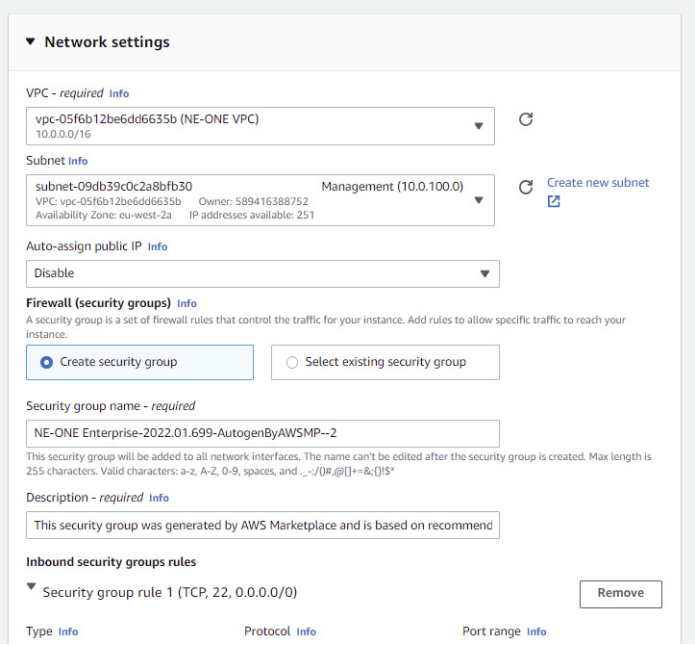
The **Create key pair** dialog box closes, and you are returned to the **Create key pair** dialog area of the **Launch an instance** page, which is now has the **Key pair name** drop-down field populated with the key pair you just created.

f. Scroll down to and expand the **Network settings** area.

The **Network settings** area expands, with an **Edit** button at the top right.



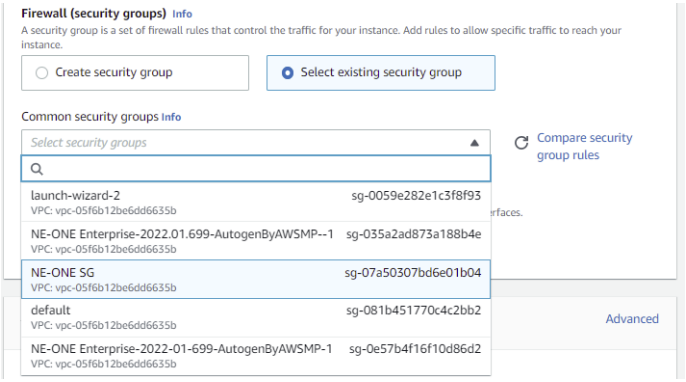
g. In the expanded **Network settings** area, click the **Edit** button, then do the following:



In the **VPC - required** drop-down field, select the VPC that you previously created in *VPC Configuration* on page 11.

In the **Subnet** drop-down field, select the Management Subnet you previously created in *Subnet Configuration* on page 13.

h. In the expanded **Network settings** area, enable the **Select existing security group** radio button, then select the NE-ONE SG Security Group that you previously created in *Security Groups* on page 15.



i. Leave the default settings unchanged in the other **Application and OS Images (Amazon Machine Image)**, **Configure storage** and **Advanced details** areas of the **Launch an instance** page.

j. In the **Summary** area click the **Launch instance** button.

The NE-ONE EC2 instance is now running on the AMI, and will become on-line.

3-3. Attach the Network Interfaces to the NE-ONE EC2 Instance

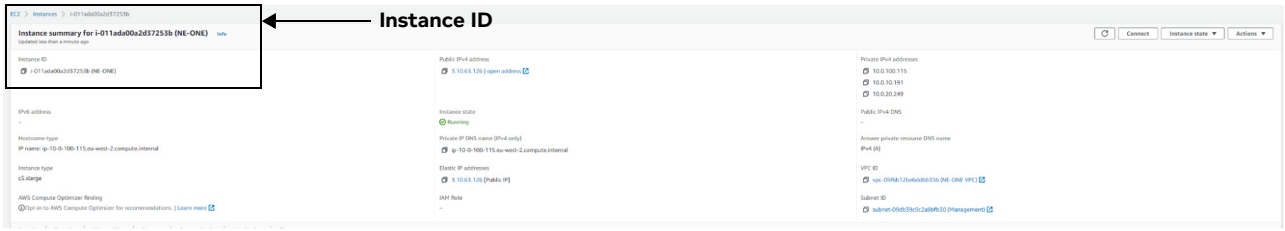
Once the NE-ONE EC2 instance has come on-line, you must attach all of the previously created Network Interfaces to the NE-ONE EC2 instance. Use the following steps to connect all of the previously created Network Interfaces to the running NE-ONE EC2 instance.

Note:
This procedure only needs to be done once. The only reason you need to re-do the steps below is if the Network Interfaces you created get removed. In which case, you would re-create the Network Interfaces and attach them again.

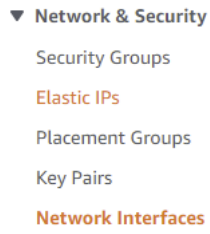
1. Click the **Services** drop-down menu.
2. From the variety of different services provided, select **EC2** from within the **Compute** category.

Note:
You can search for **EC2** either by finding it under the **Compute** category or by using the search bar.

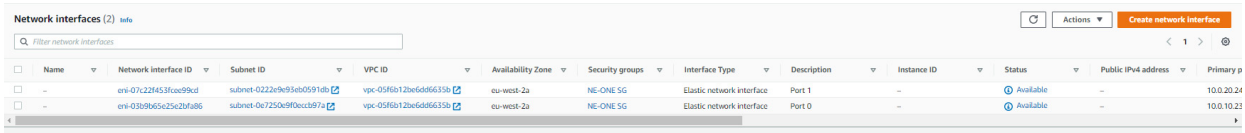
3. From the **EC2** sidebar, select **Instances**.



4. Note down the Instance ID of the NE-ONE EC2 instance, as you will need this when attaching the Network Interfaces.
5. From the **EC2** sidebar, click on **Network Interfaces** under **Network and Security**.

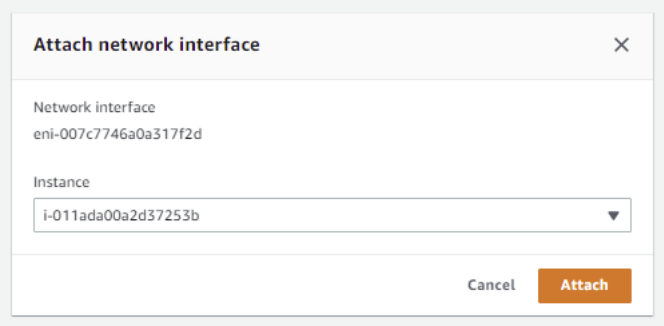


A list of Network Interfaces appear, from within the **Network Interfaces** area under **Network and Security**.



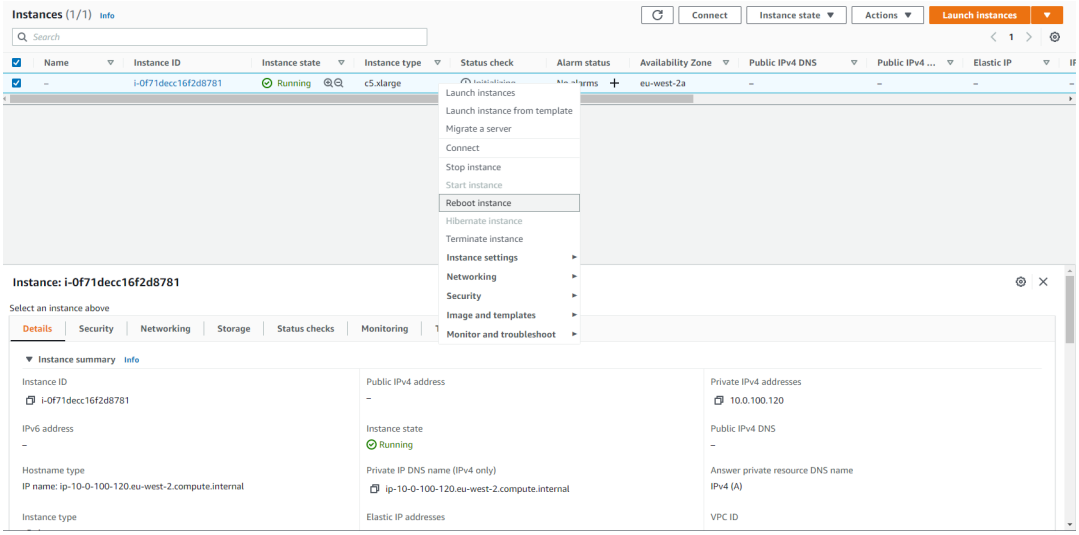
6. From the list of Network Interfaces appear, do the following for each of the Network Interfaces that you need to attach to the NE-ONE EC2 instance:
   a. Select the appropriate Network Interface from the list.

b. Click on **Actions** and then **Attach**.



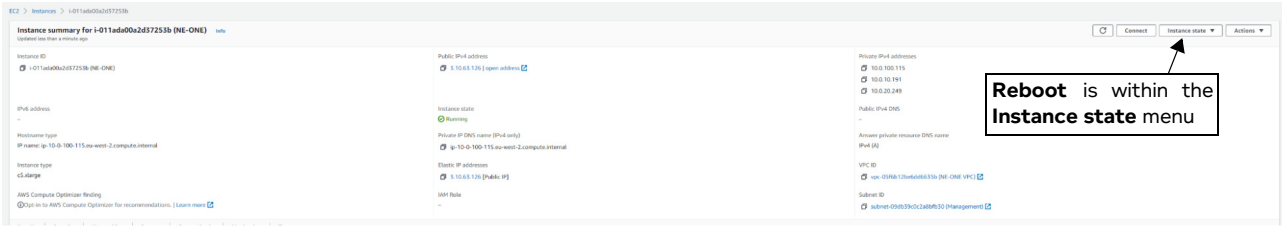
c. Select the NE-ONE EC2 instance that you identified in step 4, and click **Attach**.

7. Once all of the necessary Network Interfaces are attached the NE-ONE EC2 instance, you need to reboot the NE-ONE EC2 instance in order to bring the attached Network Interfaces on-line. To do this navigate back to your instances (i.e. **EC** sidebar > **Instances**), right click on the NE-ONE EC2 instance and select **Reboot Instance** and then click **Reboot**.



Note:

You can also reboot the NE-ONE EC2 instance, by clicking on the NE-ONE EC2 instance (i.e. drilling down one extra level within the AWS interface) and select **Reboot** from the **Instance state** menu.



Once the NE-ONE EC2 instance is rebooted after attaching the Network Interfaces, the NE-ONE is on-line and ready for use. You must now make the NE-ONE Web Interface accessible using the steps described in *Making the NE-ONE Web Interface Accessible*.

4. MAKING THE NE-ONE WEB INTERFACE ACCESSIBLE

Once the NE-ONE is on-line and ready for use, you must use one of the following methods to make the Web Interface accessible:

- Attach the Management Subnet to an Internet Gateway and set up routing to allow external traffic to connect over the Internet.
- Use the AWS VPN
- Create a Jump Host instance in the same VPC

Note:

In this Installation Guide we will create an Internet Gateway and configure the routing to allow connecting to the Web Interface over the Internet. The use of an AWS VPN and creating a Jump Host instance are beyond the scope of this Installation Guide. For more information on using an AWS VPN or creating a Jump Host instance, contact Calnex Support, or your Support Representative.

4-1. Creating the Internet Gateway

Use the following steps to create an Internet Gateway and configure the routing to allow connecting to the Web Interface over the Internet:

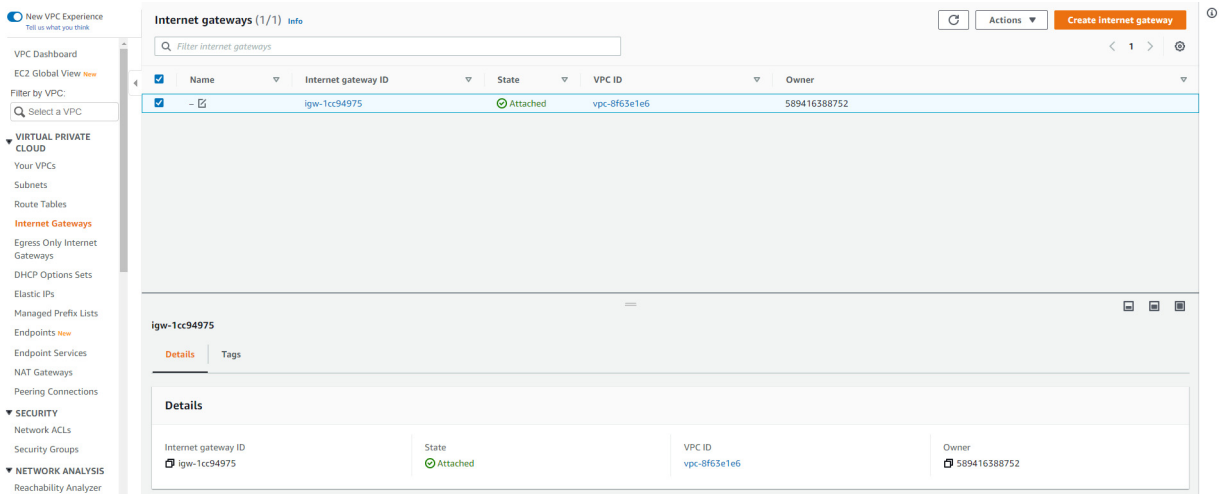
1. Click the **Services** drop-down menu.
2. From the variety of different services provided, select **VPC** from within the **Networking & Content Delivery**.

Note:

You can search for **VPC** either by finding it under the **Networking & Content Delivery** category or by using the search bar.

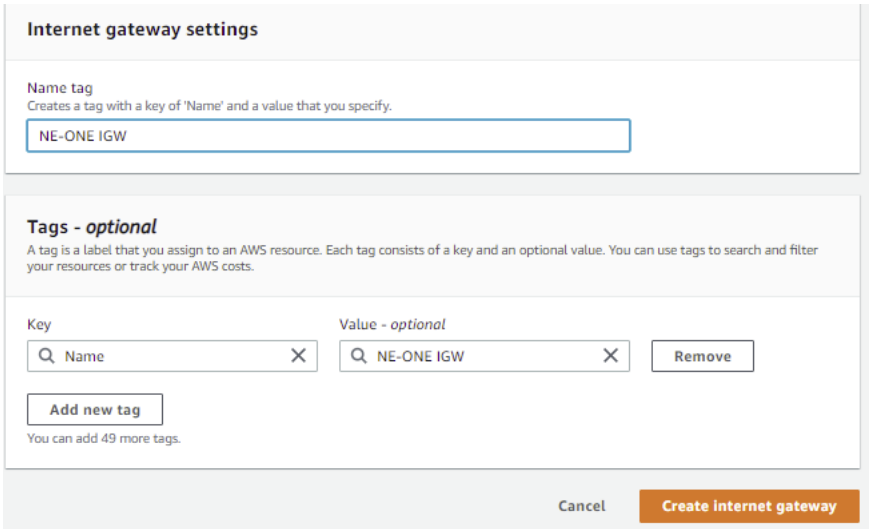
On the left hand side of the screen is a sidebar, which allows you to navigate around the VPC service screen.

3. On the **VPC** sidebar, click on **Internet Gateways**.

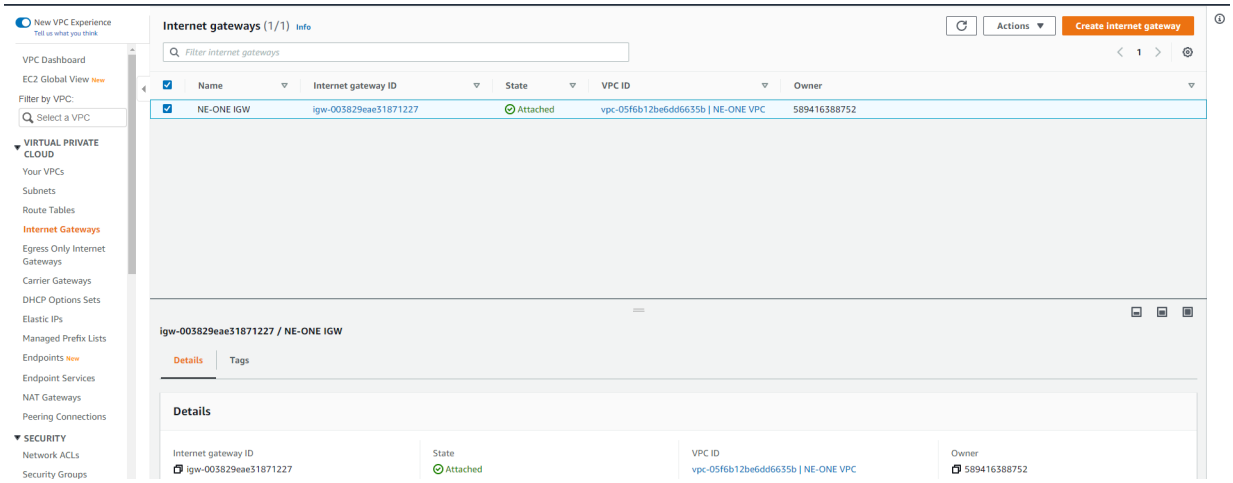


4. Click on **Create Internet Gateway**.
5. From the **Internet gateway settings page** that appears, specify the Internet Gateway name tag in

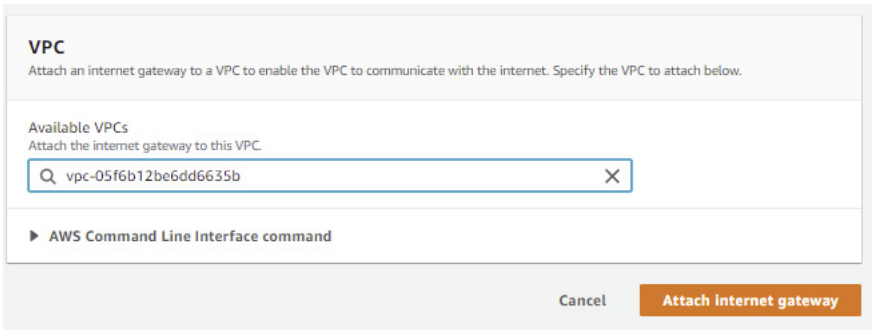
the Name tag field (e.g. **NE-ONE IGW**) and click **Create internet gateway**.



The newly created Internet Gateway is created and listed the **Internet gateways** area of the AWS interface.

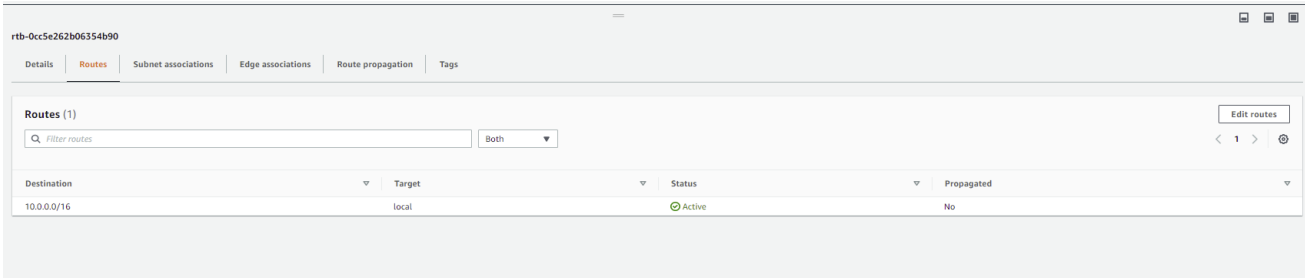


6. Once the Internet Gateway has been created, select it and select **Actions** and then **Attach to VPC**.
7. From the **VPC** dialog box that appears, select the VPC you created previously in *VPC Configuration* on page 11 and the click **Attach internet gateway**.

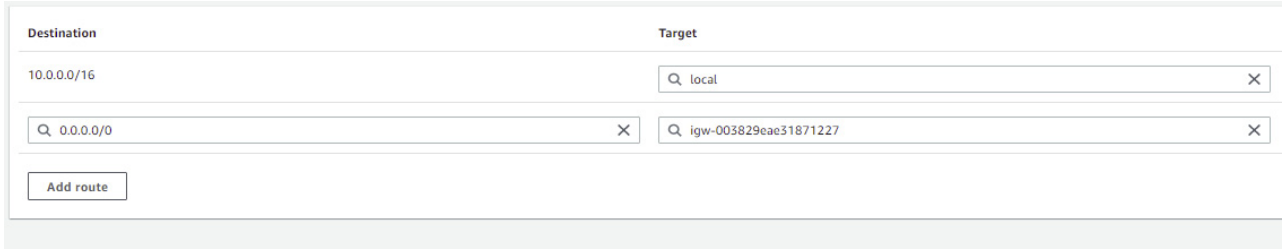


8. Navigate to **Route Tables** on the **VPC** sidebar, and select the existing route table.

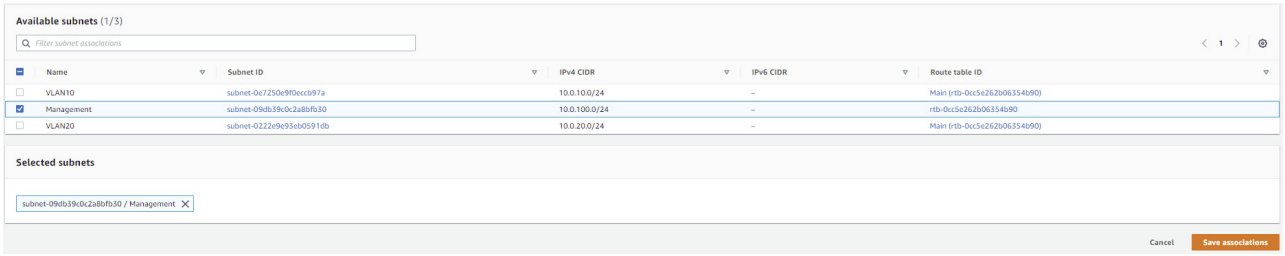
9. In the bottom window, select **Routes** and then **Edit Routes**.



10. Click **Add Route**, select **0.0.0.0/0** as the **Destination** and then the Internet Gateway that you created in step 5 as the **Target**. Then click **Save Changes**.



11. In the bottom window, select **Subnet associations**, and then **Edit subnet associations**.
12. From the **Available subnets** page that appears, tick the check box associated with the Management Subnet you previously created in *Subnet Configuration* on page 13.



13. Click **Save associations**.

4-2. Assigning an Elastic IP address

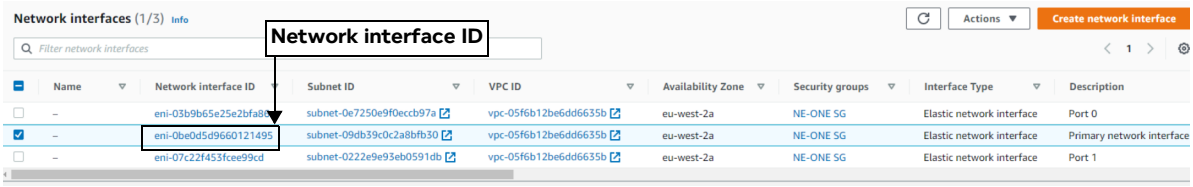
1. Click the **Services** drop-down menu.
2. From the variety of different services provided, select **EC2** from within the **Compute** category.

Note:
You can search for **EC2** either by finding it under the **Compute** category or by using the search bar.

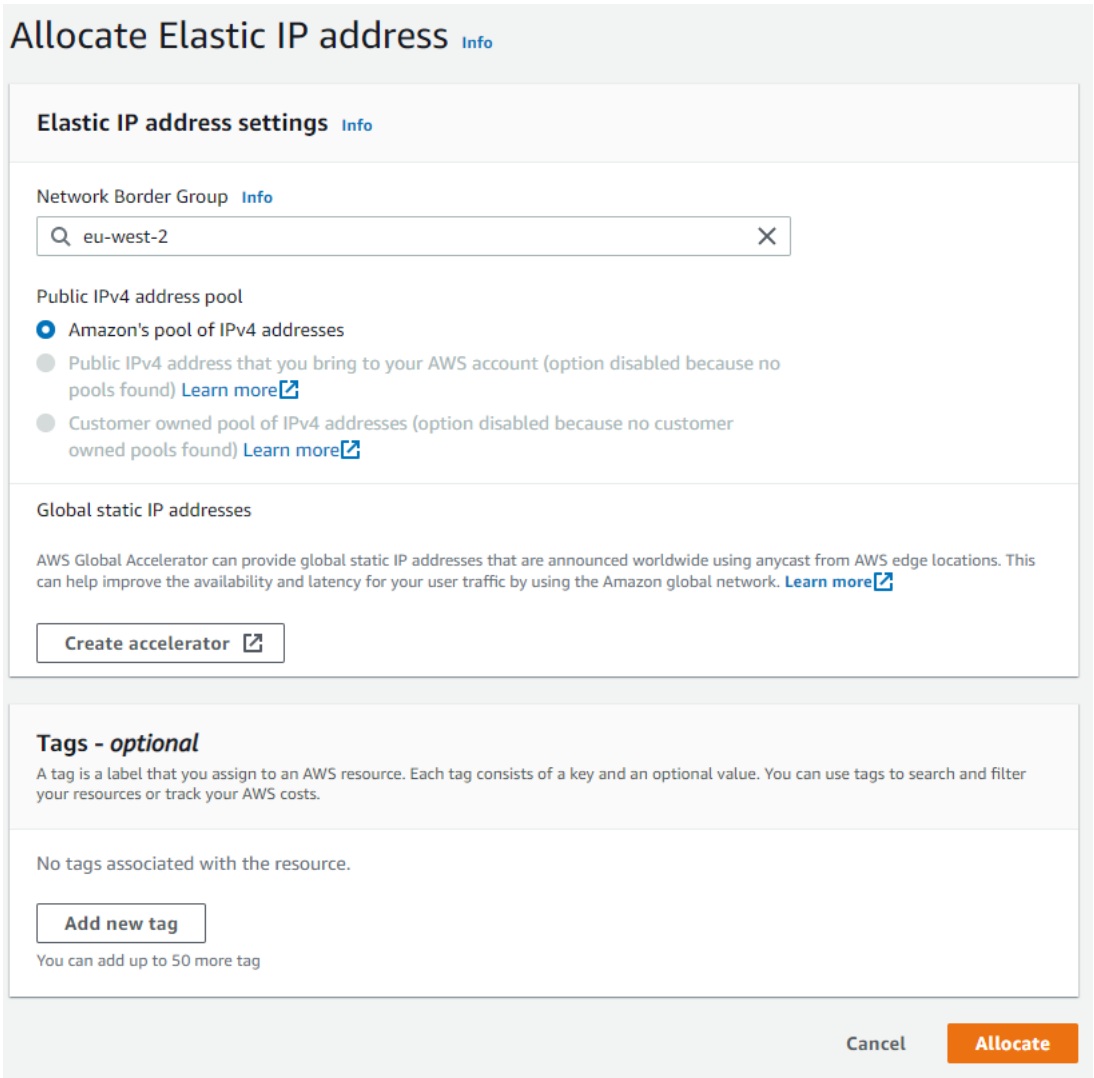
3. From the **EC2** sidebar, click on **Network Interfaces** under **Network and Security**.

4. Note down the Network interface ID of the management port (it will be of the format eni-NNNNN,

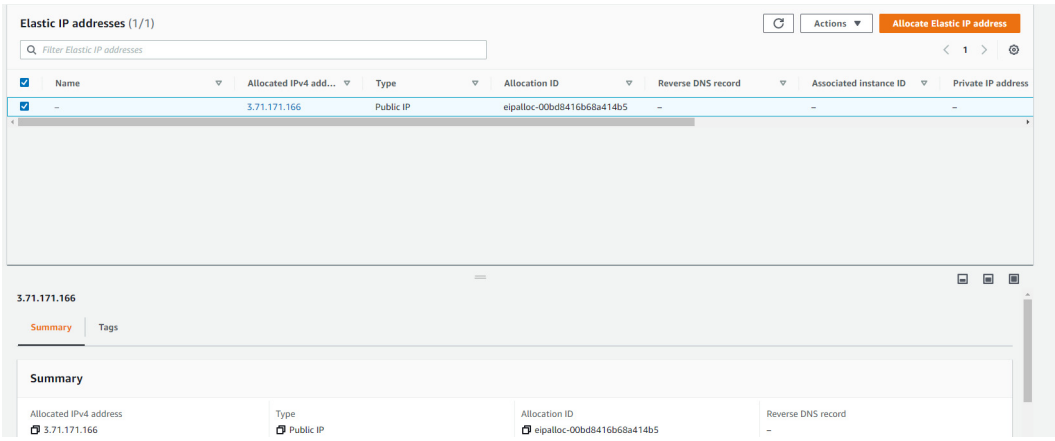
and have the default description **Primary network interface**).



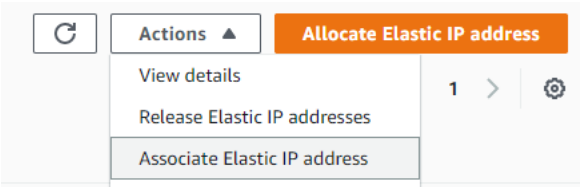
5. From the **EC2** sidebar, click on **Elastic IPs** under **Network and Security**, and then click **Allocate Elastic IP address**.
6. From the **Allocate Elastic IP address** dialog box that appears, leave the settings as default and click **Allocate**.



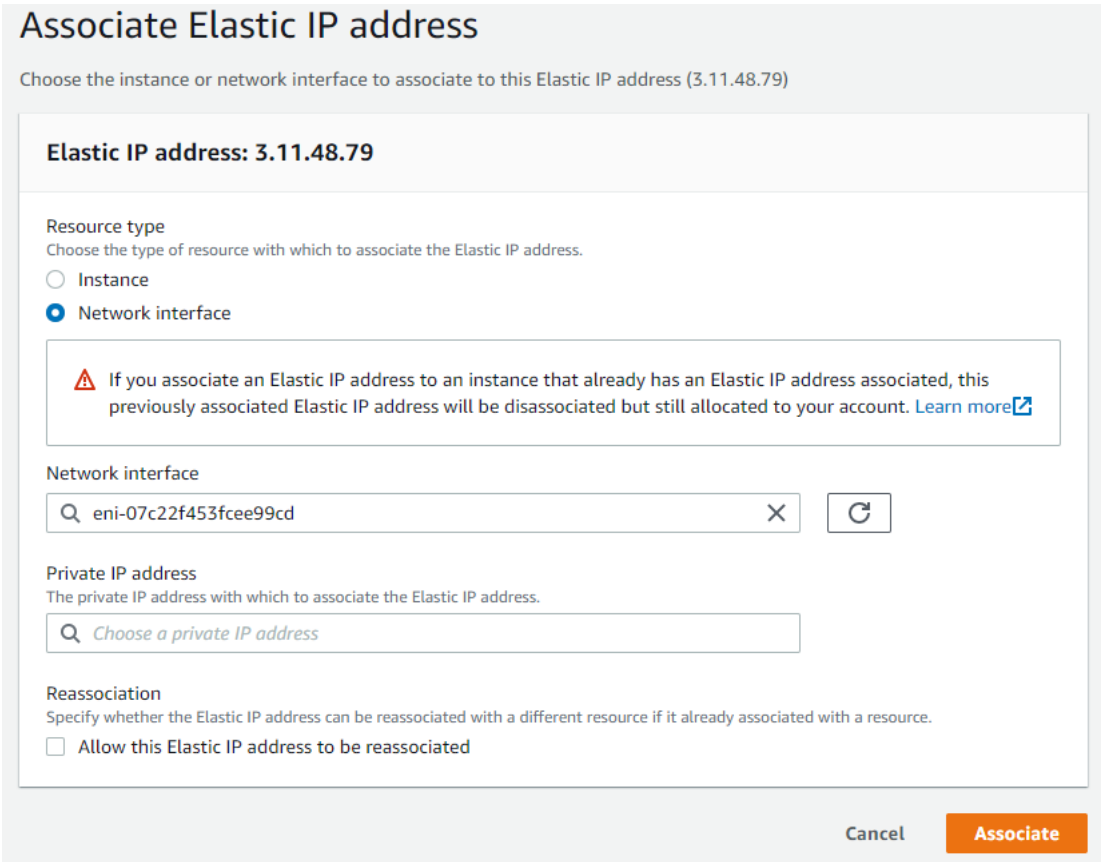
A newly created elastic IP address appears in the **Elastic IP addresses** area of the AWS interface.



7. Select the newly created elastic IP address, click on **Actions** and then **Associate Elastic IP address**.



8. In the **Associate Elastic IP address** dialog box that appears, do the following:
   a. Select **Network Interface** as the **Resource type**.
   b. In the **Network interface** field, type the Network Interface ID you noted down during step 4.
   c. Click **Associate**.



9. Navigating back to the instances (**EC2** sidebar > **Instances**), the NE-ONE instance will now have an Elastic IP assigned, which can now be used to connect to the NE-ONE Web Interface.

Note:
The changes to the NE-ONE instance take immediate effect. You do not need to reboot the NE-ONE instance.

Note:
The default login for the NE-ONE Web Interface will be admin for the username, along with your Instance ID for the password. Upon logging in to the Web Interface for the first time, you will be prompted to specify a new password.

Note:
From the NE-ONE Web Interface you can now apply the license key supplied to you by Calnex Support or your Support Representative. For more information how to use the NE-ONE Web Interface and licensing the NE-ONE Web Interface, refer to the *NE-ONE User and Administration Guide*.

This page is intentionally left blank.

Revision History

Date	Reference	Reason for change
30/03/2022	Revision 1	Initial 2022 Release.
06/04/2022	Revision 2	Minor updates
24/06/2022	Revision 3	Updates for Calnex re-branding and AWS interface changes.

User Feedback

To help us continually improve the quality of this Technical Publication, we appreciate your input. Please answer the following questions, and fax or mail the completed questionnaire back to the address noted in *Contact Information on page 6*.

1. Is this Technical Publication easy to use?

2. Is the information presented in a clear and logical way?

3. Is the information accurate?

4. Would you like to see instructions for any additional procedures? Please list them in the space below.

5. Is there something you do not like about this Technical Publication ?

www.calnexsol.com