



Installation Guide (Amazon Web Service Cloud Deployment)

Dialogic[®] BorderNet[™] Session Border Controller (SBC)

Release 3.8.1

June 2019

Table of Contents

1. Introduction
 - 1.1 Purpose of this Document
 - 1.2 Glossary
 - 1.3 Contact Us
2. Overview of Network Topology
 - 2.1 What is AWS?
 - 2.2 Network Topology for Standalone Deployments
 - 2.3 Network Topology for HA Deployments
3. Introduction to AWS GUI
4. AWS Resources Creation
 - 4.1 Regions
 - 4.2 Create a New Virtual Private Cloud (VPC)
 - 4.3 Create New Subnets
 - 4.4 Security Groups
 - 4.4.1 Naming the Security Group
 - 4.4.2 Creating Inbound Rules for the Security Group
 - 4.5 Creating Network Interfaces
 - 4.5.1 Creating Network Interfaces (Standalone Mode)
 - 4.5.2 Creating Network Interfaces (High Availability Mode)
 - 4.6 Creating IGW
 - 4.7 Modify the Route Table
 - 4.8 Allocate Elastic IP Addresses
 - 4.8.1 Standalone Deployment Mode
 - 4.8.2 High Availability Deployment Mode
 - 4.9 EIP to Network Interface Association
 - 4.10 IAM Role
5. BorderNet SBC Installation Steps
6. Attaching Network Interfaces
 - 6.1 Identifying the Instances
 - 6.2 Identifying the New Interfaces
 - 6.3 Attaching the Network Interfaces
7. Adding IP Addresses to Primary Instance
8. Attaching EIPs to Each Instance
9. First Access to the BorderNet SBC
 - 9.1 Locating the Management IP Address
 - 9.1.1 Standalone Instances
 - 9.1.2 HA Instances
 - 9.2 Accessing the GUI
 - 9.3 Deploying your Instance
 - 9.3.1 Standalone Deployment
 - 9.3.2 High Availability Deployment
10. Access the Management GUI

10.1 Standalone Deployments

10.2 HA Deployments

Copyright and Legal Notice

Copyright © 2019 Dialogic Corporation. All Rights Reserved. You may not reproduce this document in whole or in part without permission in writing from Dialogic Corporation at the address provided below.

All contents of this document are furnished for informational use only and are subject to change without notice and do not represent a commitment on the part of Dialogic Corporation and its affiliates or subsidiaries ('Dialogic'). Reasonable effort is made to ensure the accuracy of the information contained in the document. However, Dialogic does not warrant the accuracy of this information and cannot accept responsibility for errors, inaccuracies or omissions that may be contained in this document.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH DIALOGIC® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN A SIGNED AGREEMENT BETWEEN YOU AND DIALOGIC, DIALOGIC ASSUMES NO LIABILITY WHATSOEVER, AND DIALOGIC DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF DIALOGIC PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHT OF A THIRD PARTY.

Dialogic products are not intended for use in certain safety-affecting situations. Please see <http://www.dialogic.com/company/terms-of-use.aspx> for more details.

Due to differing national regulations and approval requirements, certain Dialogic products may be suitable for use only in specific countries, and thus may not function properly in other countries. You are responsible for ensuring that your use of such products occurs only in the countries where such use is suitable. For information on specific products, contact Dialogic Corporation at the address indicated below or on the web at www.dialogic.com.

It is possible that the use or implementation of any one of the concepts, applications, or ideas described in this document, in marketing collateral produced by or on web pages maintained by Dialogic may infringe one or more patents or other intellectual property rights owned by third parties. Dialogic does not provide any intellectual property licenses with the sale of Dialogic products other than a license to use such product in accordance with intellectual property owned or validly licensed by Dialogic and no such licenses are provided except pursuant to a signed agreement with Dialogic. More detailed information about such intellectual property is available from Dialogic's legal department at 3300 Boulevard de la Côte-Vertu, Suite 112, Montreal, Quebec, Canada H4R 1P8. **Dialogic encourages all users of its products to procure all necessary intellectual property licenses required to implement any concepts or applications and does not condone or encourage any intellectual property infringement and disclaims any responsibility related thereto. These intellectual property licenses may differ from country to country and it is the responsibility of those who develop the concepts or applications to be aware of and comply with different national license requirements.**

Dialogic, Dialogic Pro, Veraz, Brooktrout, Diva, BorderNet, PowerMedia, PowerVille, PowerNova, MSaaS, ControlSwitch, I-Gate, Cantata, TruFax, SwitchKit, Eiconcard, NMS Communications, SIPcontrol, Exnet, EXS, Vision, inCloud9, and NaturalAccess, among others as well as related logos, are either registered trademarks or trademarks of Dialogic Corporation and its affiliates or subsidiaries. Dialogic's trademarks may be used publicly only with permission from Dialogic. Such permission may only be granted by Dialogic's legal department at 3300 Boulevard de la Côte-Vertu, Suite 112, Montreal, Quebec, Canada H4R 1P8. Any authorized use of Dialogic's trademarks will be subject to full respect of the trademark guidelines published by Dialogic from time to time and any use of Dialogic's trademarks requires proper acknowledgement.

The names of actual companies and products mentioned herein are the trademarks of their respective owners.

This document discusses one or more open source products, systems and/or releases. Dialogic is not responsible for your decision to use open source in connection with Dialogic products (including without limitation those referred to herein), nor is Dialogic responsible for any present or future effects such usage might have, including without limitation effects on your products, your business, or your intellectual property rights.

Document History

Version #	Version Date	Update Description
1.0	February 2017	Release 3.6.0 - Initial version
1.1	September 2017	Release 3.7.0 -Updated with the HA deployment -Management interface is used also for Utility and HA
1.2	March 2019	Revised version
1.5	April 2019	Some corrections
2.0	May 2019	Edit and update to release 3.8.1

1. Introduction

1.1 Purpose of this Document

This document describes the BorderNet SBC's installation and deployment in the **Amazon Web Services (AWS) Virtual Private Cloud (VPC)**, using **Amazon Elastic Computing Cloud (EC2)** resources and tools.

1.2 Glossary

For the purposes of this document the following abbreviations apply:

Abbreviation	Meaning
AMI	Amazon Machine Image
AWS	Amazon Web Services
AZ	Availability Zones
CIDR	Classless Inter-Domain Routing
EC2	Elastic Computing Cloud
IGW	Internet Gateway
SBC	Session Border Controller
SIP	Session Initiation Protocol
VPC	Virtual Private Cloud
HA	High Availability
EIP	Elastic IP
IAM	Identity and Access Management

1.3 Contact Us

For a list of Dialogic locations and offices, please visit: <https://www.dialogic.com/contact.aspx>.

2. Overview of Network Topology

2.1 What is AWS?

AWS (Amazon Web Services) is a Cloud service belonging to Amazon, which provides services in the form of building blocks. These building blocks can be used to create and deploy any type of application in the Cloud.

These services or building blocks are designed to work with each other resulting in applications which are sophisticated and highly scalable.

2.2 Network Topology for Standalone Deployments

The BorderNet SBC can be deployed within an **Amazon VPC** using the **Amazon EC2 API** and tools, providing VoIP security and transcoding services towards peering entities.

In this scenario, the BorderNet SBC (Standalone or HA) is deployed in a VPC, using the following subnets:

- Management subnet, used to connect the remote users to the SBC's web-based management system, through an **Internet Gateway (IGW)**.
- One or two Private Subnets, used for signaling and media traffic between the BorderNet and two Peering User Agents.

This document describes deployment of the BorderNet SBC in the VPC according to the scenario shown below in Figure 1 (**Standalone** mode) and in Figure 2 (**High Availability** mode).

Different configurations can be implemented to match traffic needs.

In the Standalone mode, there are:

- 1 x Management Interface
- 1 x Public SIP/RTP interface with access to the Internet
- 1 x Private / Home SIP & RTP interface without access to the internet. This interface, is meant to have an internal routing element like the Dialogic ControlSwitch System (UA-B shown in Figure 1).

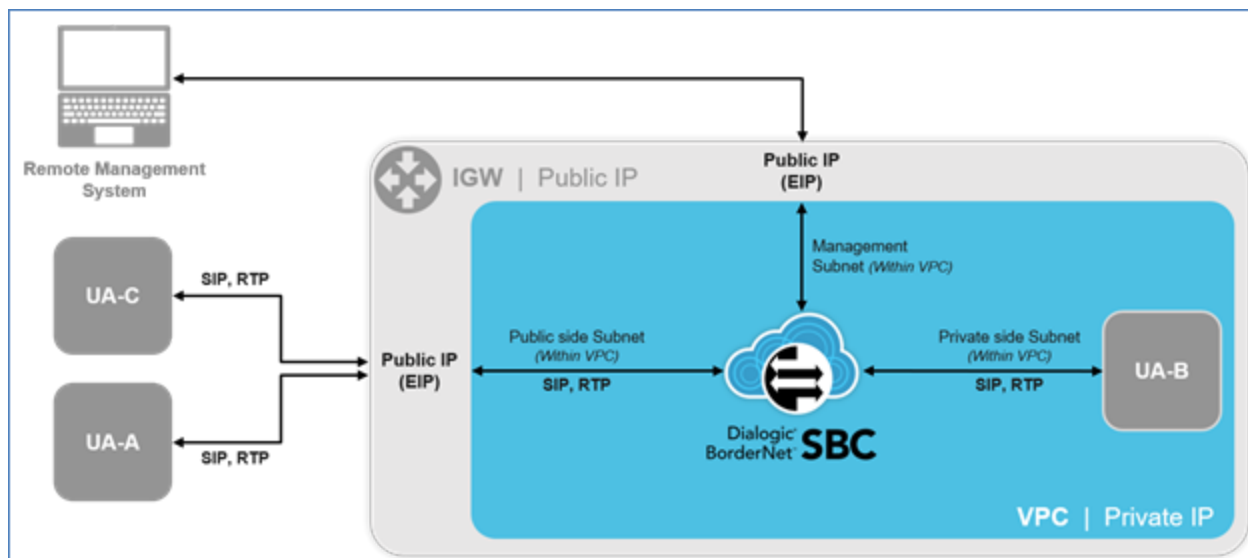


Figure 1: Standalone Network Topology

The UA-A, UA-B, UA-C, can reside in:

- The same VPC as the BorderNet SBC (UA-B is in the same VPC)
- A different VPC within the same region
- A different VPC in a different region. An additional Internet Gateway (IGW) needs to be defined for Internet connectivity.
- Outside of the AWS Cloud.

2.3 Network Topology for HA Deployments

For HA deployments, two BorderNet SBC instances should be defined as two standalone instances, considering the following points:

- Both instances must be from the same instance type.
- Both instances can reside in the same region and on the same VPC or a different VPC.
- The utility IP addresses (secondary IP addresses) during a failover and failback should be declared on both instances.

In this document, the deployment of the BorderNet SBC in HA mode is illustrated in the diagram shown below in Figure 2. Both instances will be installed on the same VPC.

In this scenario, there is a requirement for the set of private IP addresses illustrated below.

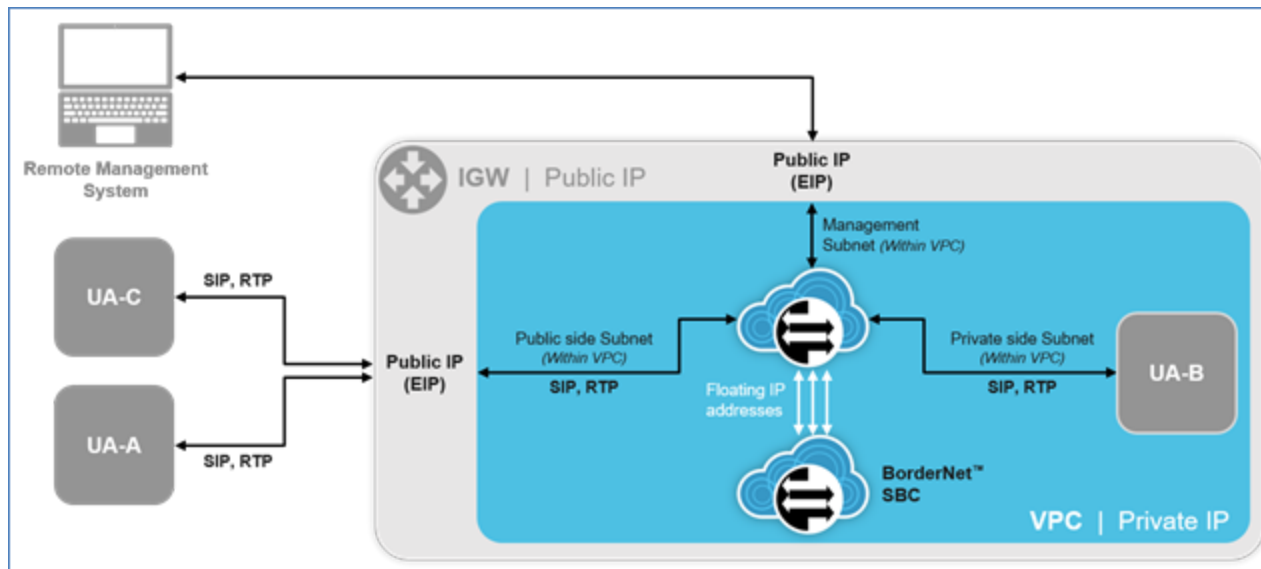


Figure 2: HA Network Topology

In addition to the physical addresses, which are defined per BorderNet SBC, three additional addresses should be defined as the floating addresses:

- for management
- for signaling
- for media

These addresses are defined using the **EC2 Networking à Manage IP Addresses** window, as the **Secondary** addresses. Traffic from UA-A, UA-B and UA-C is directed to the floating addresses.

All the addresses should reside in the same subnet.

Figure 3 provides an example of the floating IP addresses:



Figure 3: Floating IP Addresses for HA (Secondary)

3. Introduction to AWS GUI

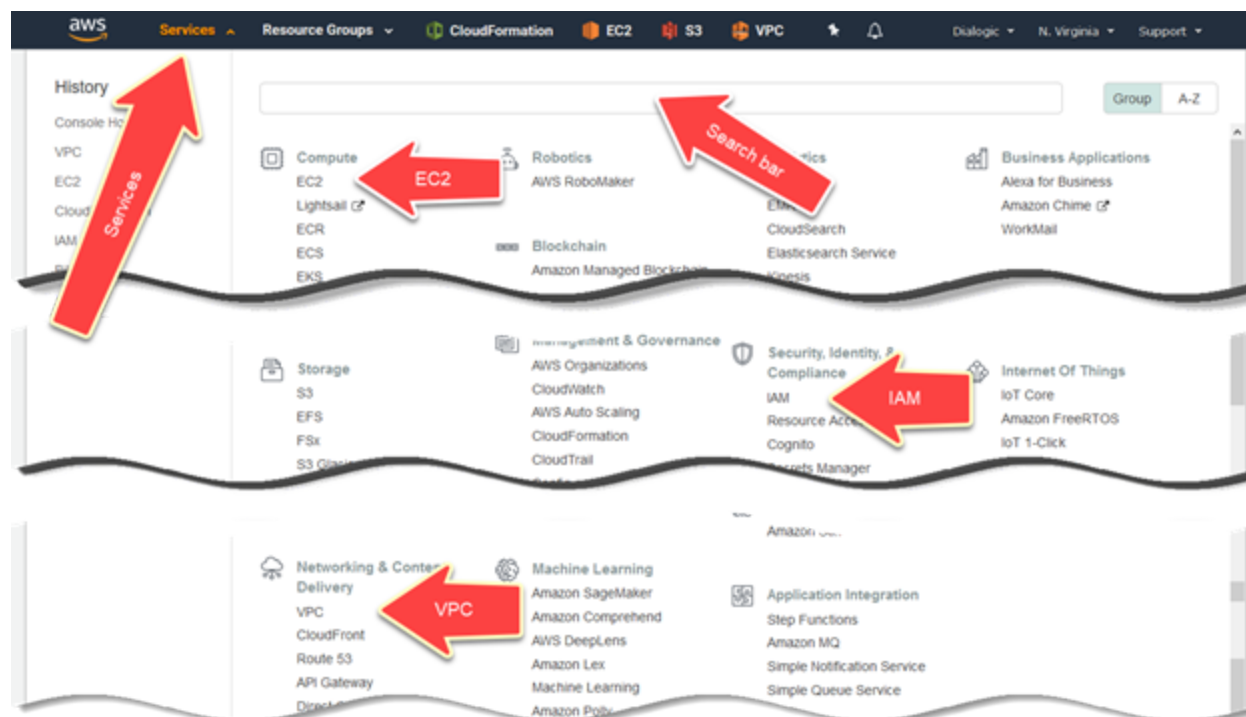
AWS divides its various features as services.

To access the services, click **Services** on the toolbar as shown below.

The following three services are used throughout this guide:

- **EC2** (Elastic Cloud Computing)
- **VPC** (Virtual Private Cloud)
- **IAM** (Identity and Access Management)

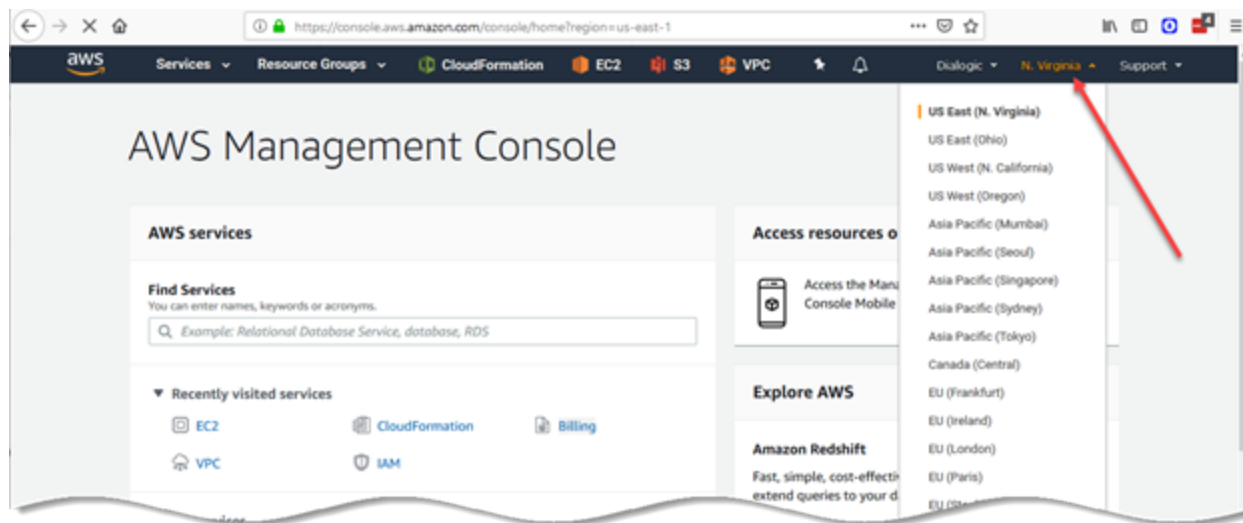
See below the location of each of the 3 services. The search field can also be used to find the service.



4. AWS Resources Creation

4.1 Regions

Select the region to install the BorderNet SBC. For example, US East (N. Virginia) is shown here.

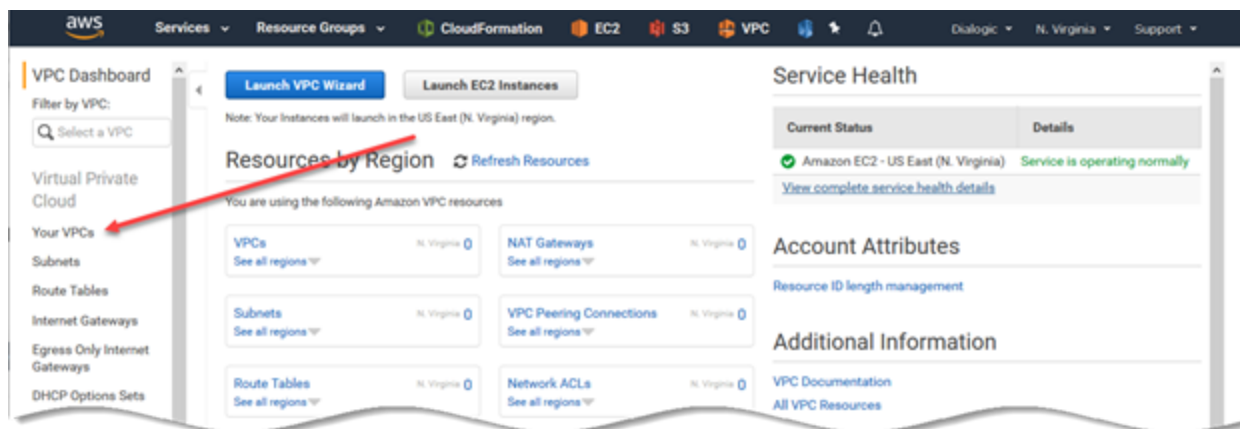


4.2 Create a New Virtual Private Cloud (VPC)

When creating a VPC, a range of IPv4 addresses in the form of a **Classless Inter-Domain Routing (CIDR)** block for the VPC should be created. For example: 192.168.0.0/16.

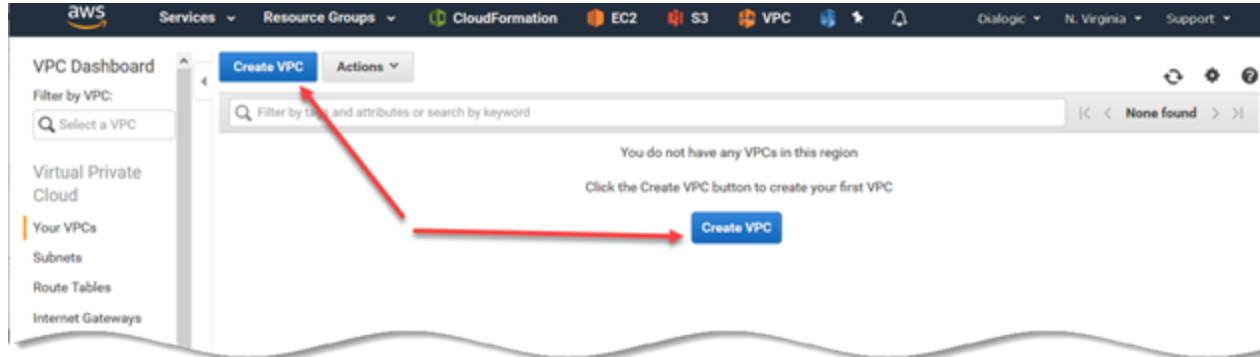
→ To create a new VPC:

1. Click **Services**.
2. Click **VPC** (or use the search bar).
3. Click **Your VPCs** as shown below.



4.

1. Click on the blue **Create VPC** button.



- 2.
3. Enter the **VPC information** as detailed below.
4. The screen below is only a reference sample.
5. Specify the following VPC details as necessary:
6. **Name tag.**
7. **VPC name.** e.g. BorderNet_VPC
8. **IPv4 CIDR block.** Specifies an IPv4 CIDR block for the VPC. It is recommended to specify a CIDR block from the private (non-publicly routable) IP address range as specified in [RFC 1918](#). For example: `192.168.0.0/16`.

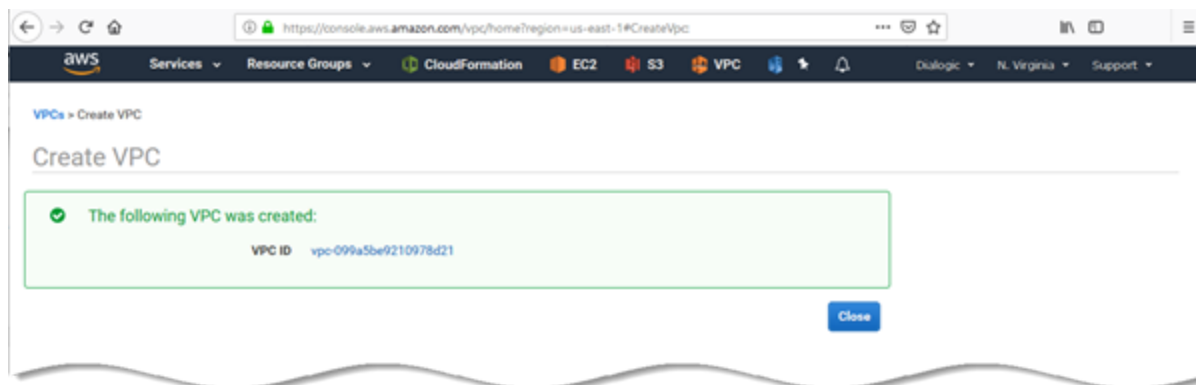
NOTE:

Direct access to the Internet from publicly routable CIDR blocks in a VPC is not supported!

- **IPv6 CIDR block.** Optionally associate an IPv6 CIDR block with your VPC by choosing an Amazon-provided IPv6 CIDR block.
- **Tenancy:** (User commercial choice with Amazon).
- Click on the **Create VPC** button.
- The **Create VPC** window opens.



-
- Once the VPC is created, AWS reports it.
- Click on the blue **Close** button.



4.3 Create New Subnets

When adding a new subnet to the created VPC the **Availability Zone (AZ)** in which you want the subnet to reside can be selected.

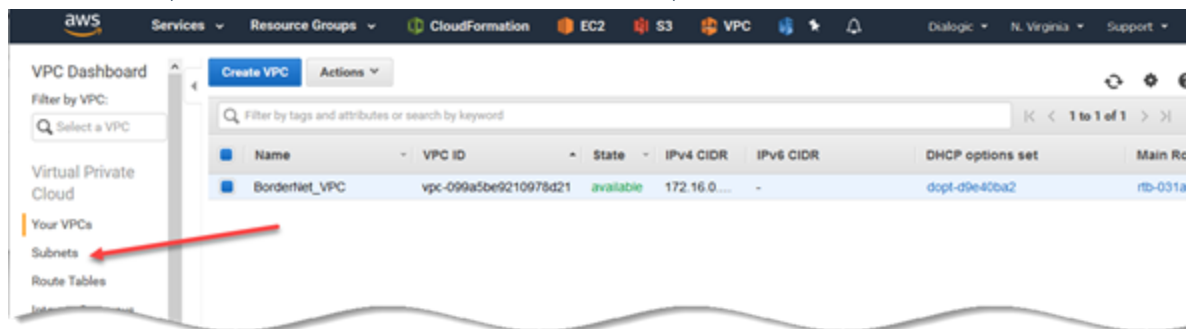
- An IPv4 CIDR block for the subnet from within the range of the created VPC must be specified.
- An IPv6 CIDR block for the subnet can alternately be specified if an IPv6 CIDR block is associated with the created VPC.

In this example, three subnets will be defined.

Type of Traffic	IPv4 CIDR Block	Description
Management	192.168.3.0/24	BorderNet Management
Public	192.168.2.0/24	SIP&RTP traffic - Internet
Private	192.168.1.0/24	SIP & RTP traffic - internal

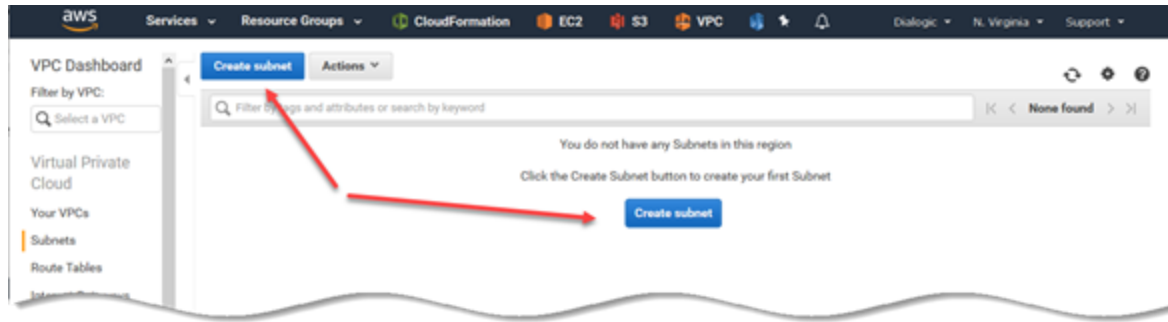
→ To create a new subnet:

1. Select **Subnets** (located at the left-hand sidebar as indicated here).



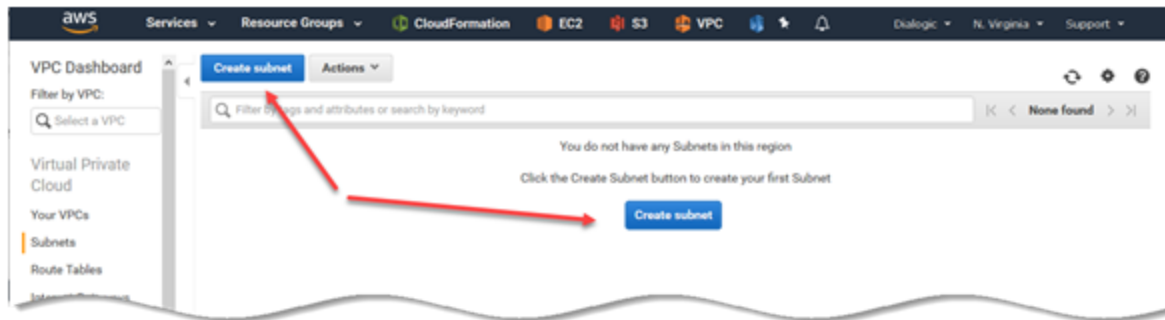
2.

1. Click on one of the blue **Create Subnet** buttons.



2.

3. The **Create Subnet** window opens:



1. Specify the following subnet details as necessary:

2. **Name tag.** Subnet name. e.g. MGMT-Subnet.

3. **VPC:** Select the pre-defined VPC for which the subnet is created, using the drop-down menu.

4. **Availability Zone.** Select an Availability Zone within the selected region.

5. **IPv4 CIDR block:** Specify an IPv4 CIDR block for your subnet. e.g. 172.16.3.0/24.

6. **IPv6 CIDR block:** If an IPv6 CIDR block is associated with your VPC, specify a custom IPv6 CIDR.

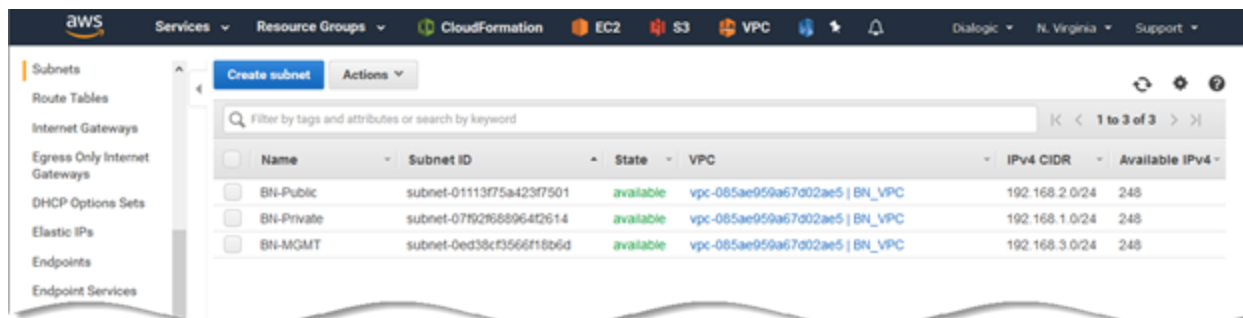
7. Click on the blue **Create** button.

8. Repeat the steps above to create the remaining two subnets - Public and Private Traffic. See the table above.

Note:

This is just an example. Different configurations can be created!

1. When all three subnets are defined the following window opens.



2.

4.4 Security Groups

A **Security Group** acts as a virtual firewall for your instance that controls the incoming and outgoing traffic.

After creating the VPC, a **Security Group** is automatically added. This **Security Group** will be used as the default Security Group changing the entries in the **Inbound Rules** table as follows:

- One entry for HTTPS traffic
- One entry for SSH traffic
- One entry for inter traffic
- One entry for SIP & RTP traffics

Different **Security Groups** can be created depending on the traffic profile and services required. For example, we could define two Security Groups as shown below:

- One Security Group for the Management traffic with a minimum of two open pinholes for HTTPS and SSH (more may be necessary depending on actions/access requirements).
- One Security Group for the other SIP & RTP traffics.

→ To access the Security Group:

1. Select **Services**.
2. Select **VPC**.
3. Select **Security Groups**.
4. Select the existing **Security Group** created by the VPC.

4.4.1 Naming the Security Group

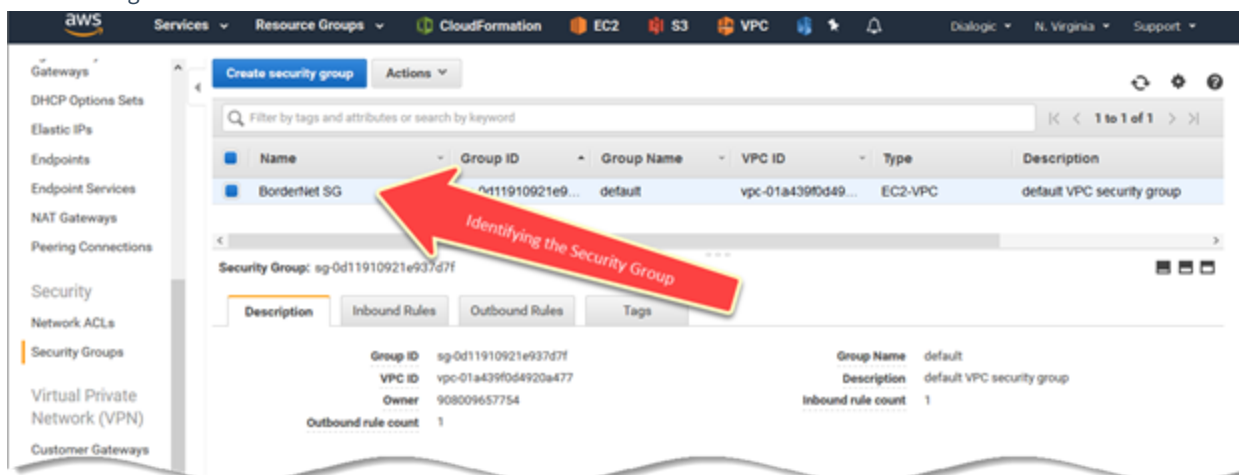
Naming resources is a good practice which assists resource creation and also troubleshooting.

→ To name Security Groups:

1. Place the mouse on the existing row, on the **Name** column. This is an empty field.
2. A pencil icon appears.
3. Click the pencil icon and enter an identifier for this **Security Group**.
4. All entries on the AWS cloud should be identified.

5. For example: **BorderNetSG**.
6. Save the entry.

1. See the image below:



2.

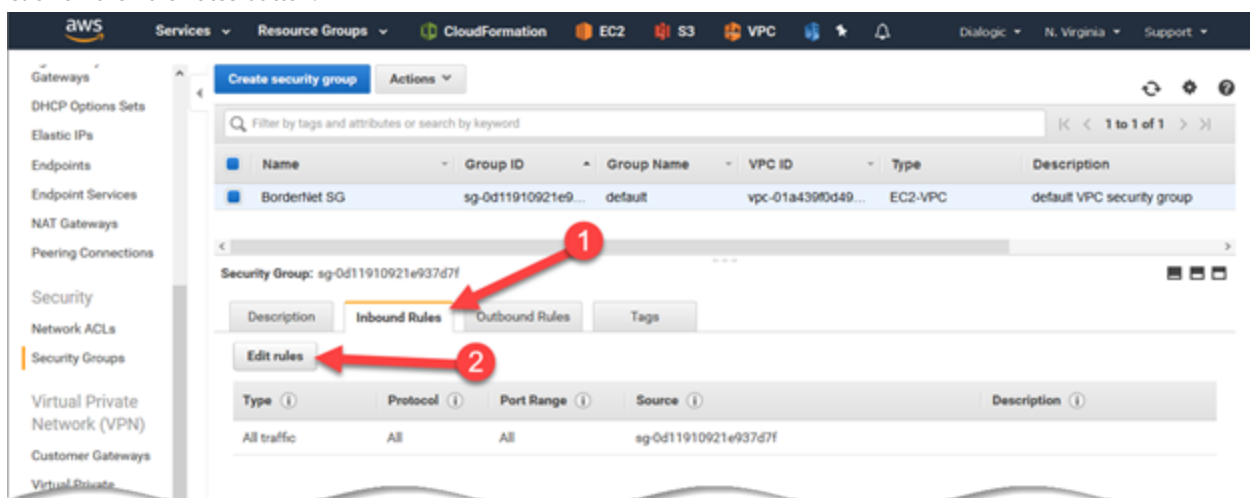
4.4.2 Creating Inbound Rules for the Security Group

Inbound Rules are required to customize the traffic flows allowed through the Security Group. Different inbound or outbound rules can be created to increase security as desired.

For example, we can create the inbound rules as in the matrix below. These rules will be sufficient for the initial configuration.

→ To add Inbound Rules:

1. Click on the **Inbound Rules** tab.
2. Click on the **Edit Rules** button.



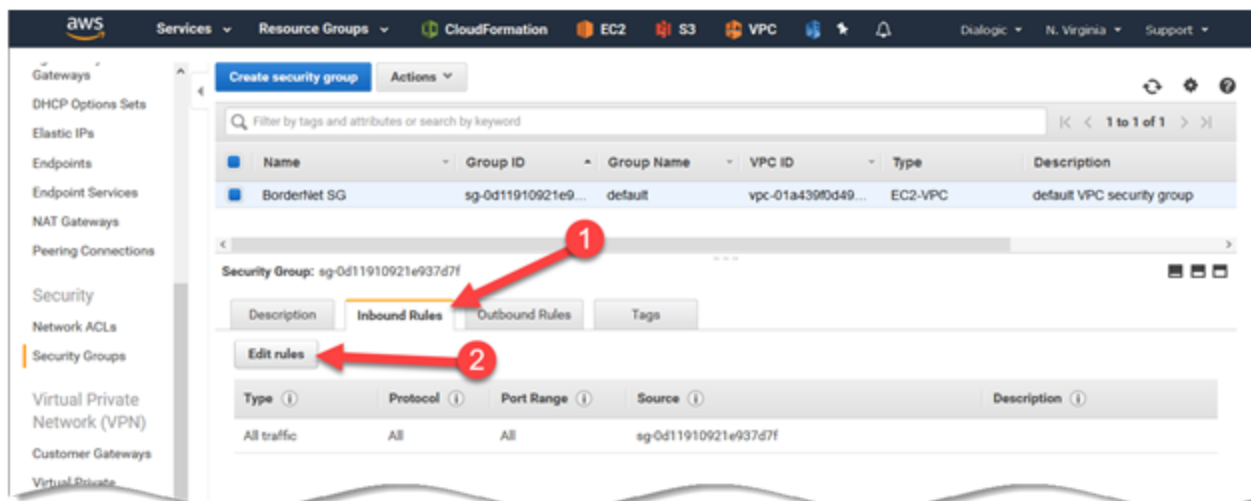
3.

4. On the screen that opens, click on the **Add Rule** button.
5. Leave blank the row **All Traffic**.
6. This entry will permit all traffic internally to the **Security Group**.

1. Click on the **Add Rule** button and proceed adding rules according to the table below.

• Type of Traffic	• Protocol	• Port Range	• Source	• Description
• All traffic	• N/A	• All	• Security Group	• This entry is on the list
• HTTPS	• N/A	• N/A	• Anywhere	• GUI access
• SSH	• N/A	• N/A	• Anywhere	• SSH access for upgrade/maintenance
• Custom TCP Rule	• N/A	• 5060-5070	• Anywhere	• SIP signaling ports
• Custom UDP Rule		• 7000-65000	• Anywhere	• RTP ports

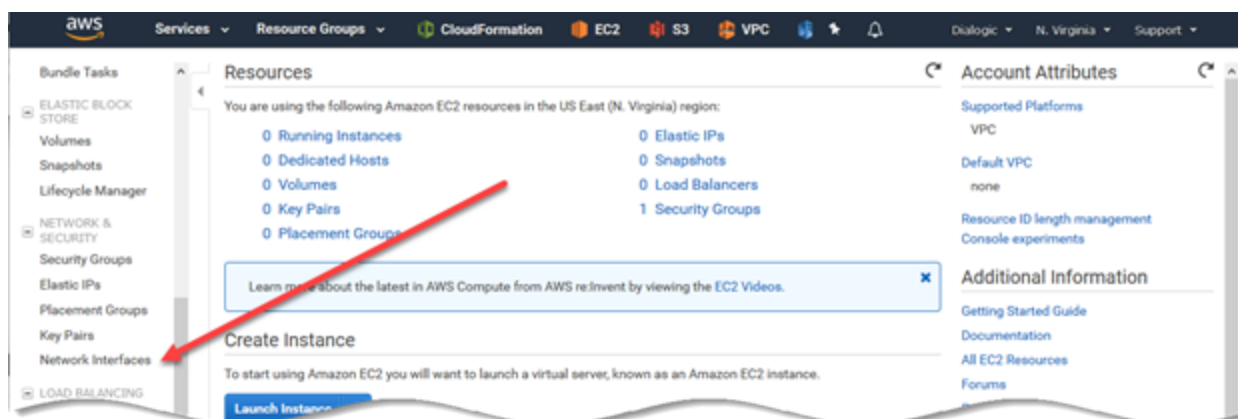
See below the result with all the rules created.



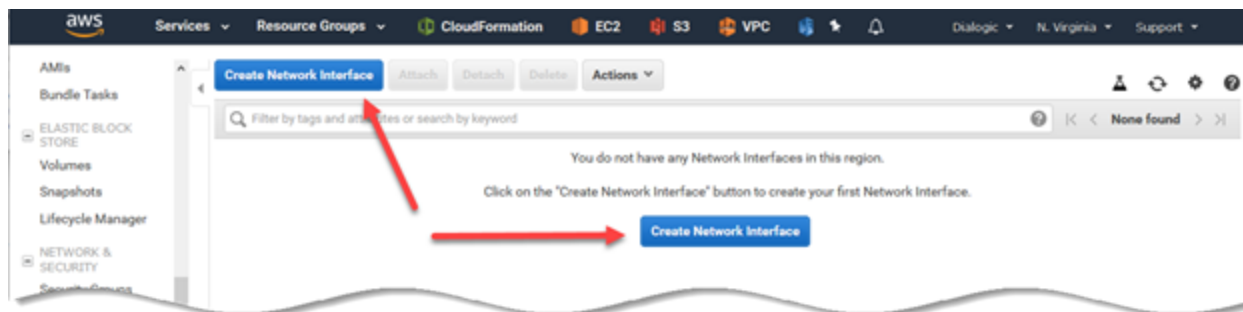
4.5 Creating Network Interfaces

→ To create a Network Interface:

1. Click on **Services > EC2**.
2. On the **EC2** screen click **Network Interfaces** at the left-hand side of the screen (indicated below).



1. Click on one of the blue **Create Network Interface** buttons.



- 2.
3. Follow the instructions below relative to the appropriate deployment mode.

4.5.1 Creating Network Interfaces (Standalone Mode)

To create Network Interfaces in **High Availability** mode proceed straight to [4.5.2](#).

In **Standalone** mode, create three **Network Interfaces** to match the example configuration. Depending on the planned traffic profile different configurations may be created.

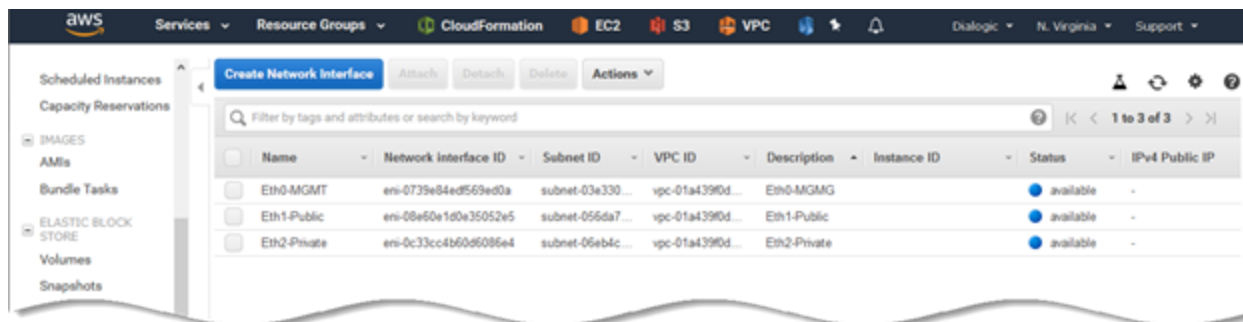
Note

As a reminder of the previous completed configuration steps use the details below for reference.

Description	Type of Traffic	Custom IP	Description
Eth0-MGMT	Management	192.168.3.100	BorderNet Management
Eth1-Public	Public	192.168.2.100	SIP&RTP traffics - external
Eth2-Private	Private	192.168.1.100	SIP&RTP traffics - internal

→ To create a Network Interface in Standalone Deployment Mode:

1. For the configuration example in this guide use the table above as a reference and enter the following information:
2. **Description:** Add a short description.
3. **Subnet:** Select the relevant subnet from the drop-down menu (see table above).
4. **Private IP:** Enter a private IP address in the range of the created subnet. Use the table above. Auto-assign or another IP range (within the subnet) can be used as well.
5. **Security Groups:** Select the Security Group (in this example, there is only one Security Group populating the list).
6. Click on the **Create** button.
7. Name the created **Network Interface**.
8. Repeat the steps above to create the remaining two **Network Interfaces**.
9. The three **Network Interfaces** are now created and identified (see the **Name** column).
10. In the **Status** column, verify that the three **Network Interfaces** are now **available**.



11.

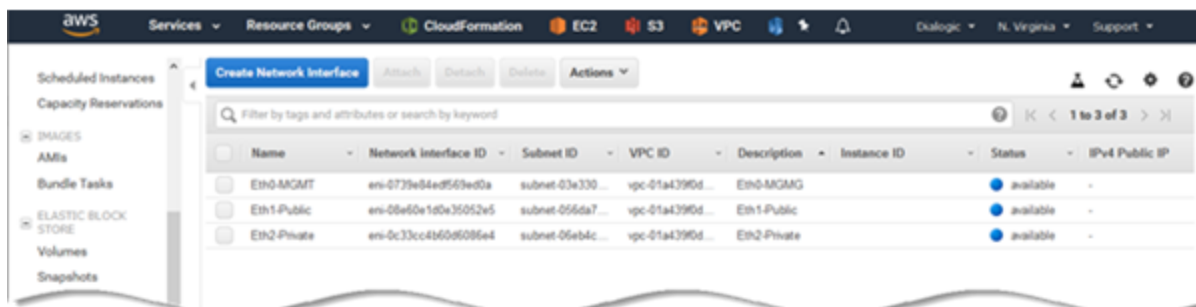
4.5.2 Creating Network Interfaces (High Availability Mode)

Create four **Network Interfaces** to match the example configuration. Depending on the planned traffic profile different configurations may be created.

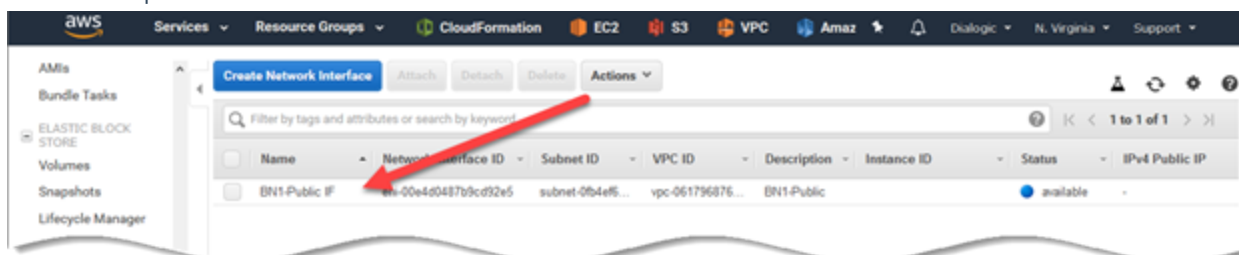
Description	Type of Traffic	Custom IP (auto-assign)	Description
BN1-Public	Public -Primary	192.168.2.101	SIP&RTP traffics - external
BN2-Public	Public-Secondary	192.168.2.102	SIP&RTP traffics - external
BN1-Private	Private-Primary	192.168.1.101	SIP&RTP traffics - internal
BN2-Private	Private-Primary	192.168.1.102	SIP&RTP traffics - internal

→ To create a Network Interface in High Availability Deployment Mode:

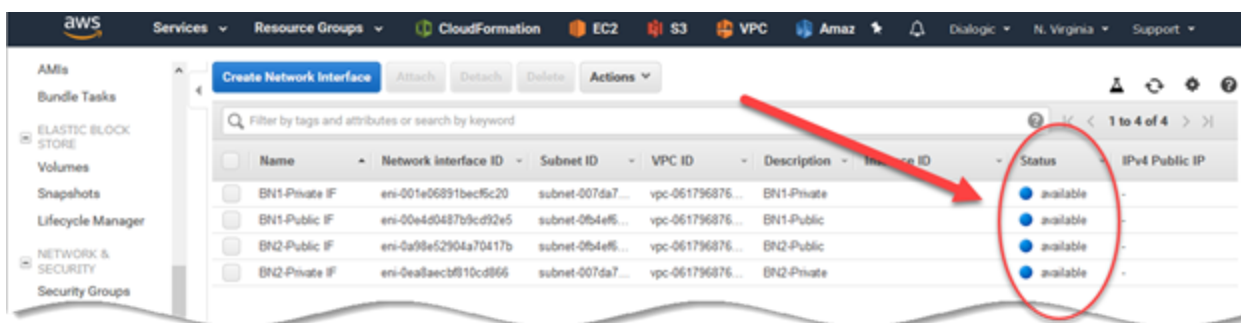
1. For the configuration example in this guide use the table above as a reference and enter the following information:
2. **Description:** Add a short description.
3. **Subnet:** Select the relevant subnet from the drop-down menu (BN-MGMT, BN-Private, BN-Public).
4. **IPv4 Private IP:** Custom
5. **IPv4 address:** Enter the IPv4 address as per the table above.
6. **Security Groups:** Select the Security Group (BorderNet SG).
7. Refer to the screenshot below.



- 8.
9. Click on the **Create** button.
10. The **Network Interface** is unnamed.
11. Name the **Network Interface**.
12. See the example below.



- 13.
14. Repeat the steps above to create the remaining **Network Interfaces** as per the table above.
15. The four **Network Interfaces** are now created and identified (see the **Name** column).
16. In the **Status** column, verify that the four **Network Interfaces** are now **available**.



4.6 Creating IGW

The **IGW (Internet Gateway)** is a VPC component that facilitates communication between instances in your VPC and the internet.

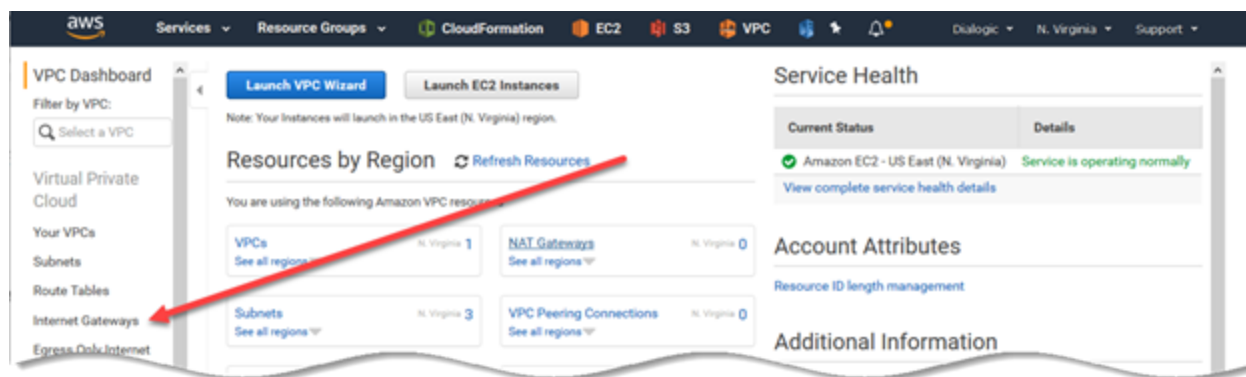
It is necessary to create an IGW for any traffic which arrives from outside to the BorderNet SBC and vice-versa.

→ To create an IGW:

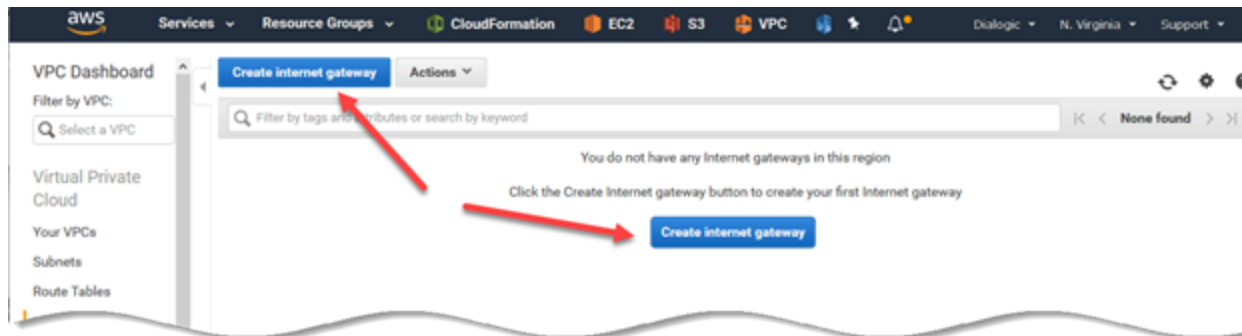
1. Click on **Services > VPC**.



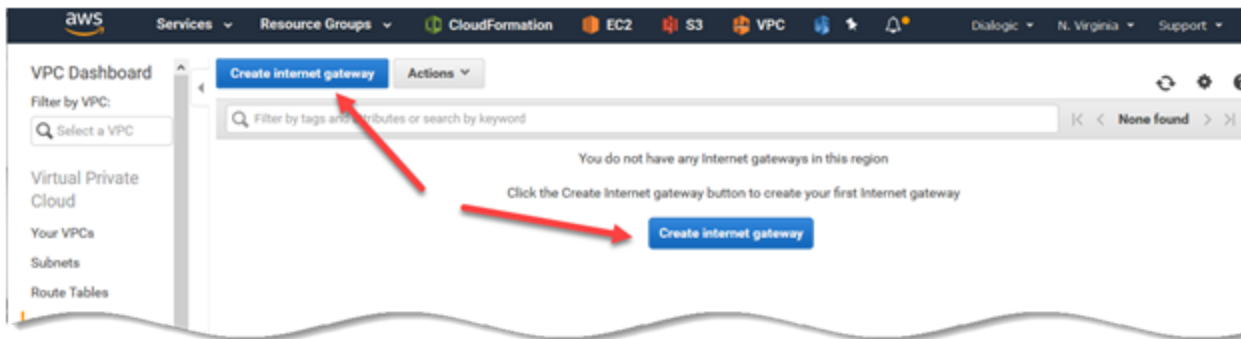
1. In the **Virtual Private Cloud** group click on **Internet Gateways**.



1. Click on one of the blue **Create Internet Gateway** buttons.



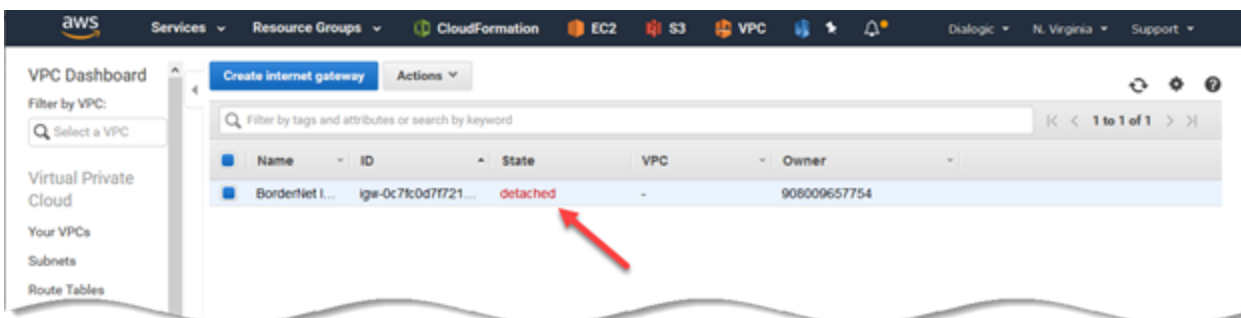
- 2.
3. In the **Create Internet Gateway** window, name the IGW and click on the **Create** button.



1. A message indicating that the **Internet Gateway** has been created will appear.
2. Click on **Close** to proceed to the next step.



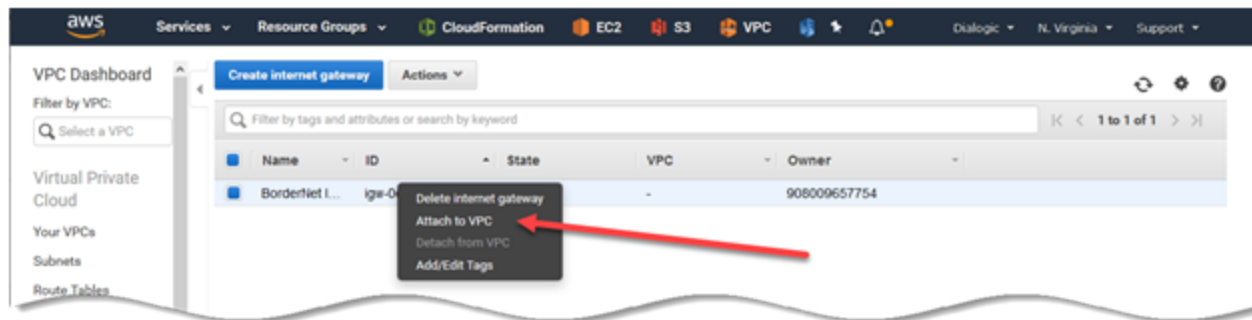
The newly created **Internet Gateway** has a **detached** state as indicated in the screenshot below.



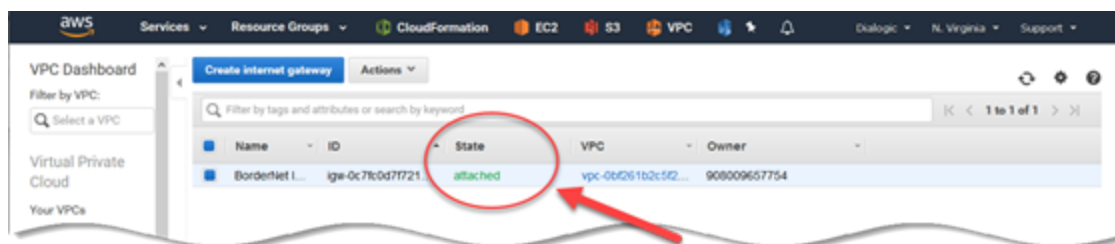
1. To change this state the **Internet Gateway** will be attached to the VPC.
2. Right-click on the IGW row and select **Attach to VPC**.



1. The **Attach to VPC** window opens.



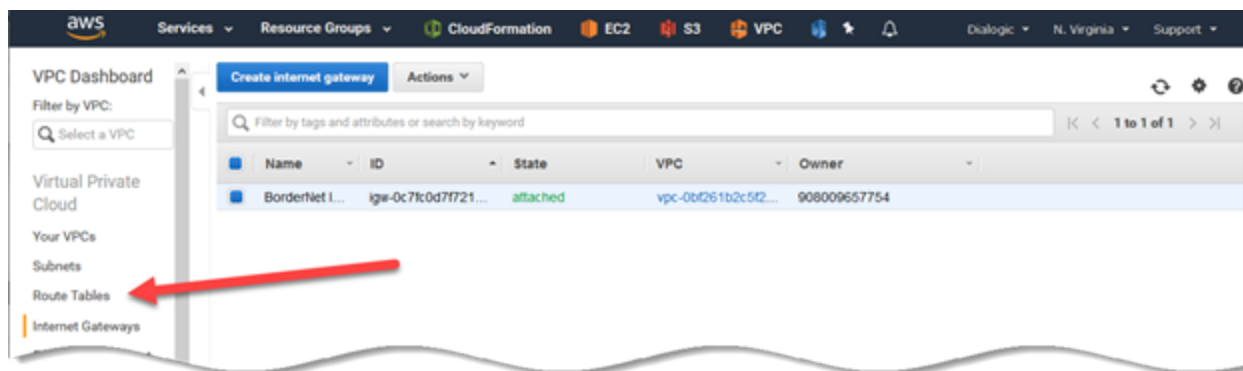
- 2.
3. Select the **VPC** from the drop-down menu and click on the **Attach** button.
4. The **Internet Gateway** state now will be **attached**.
5. The IGW configuration is now complete.



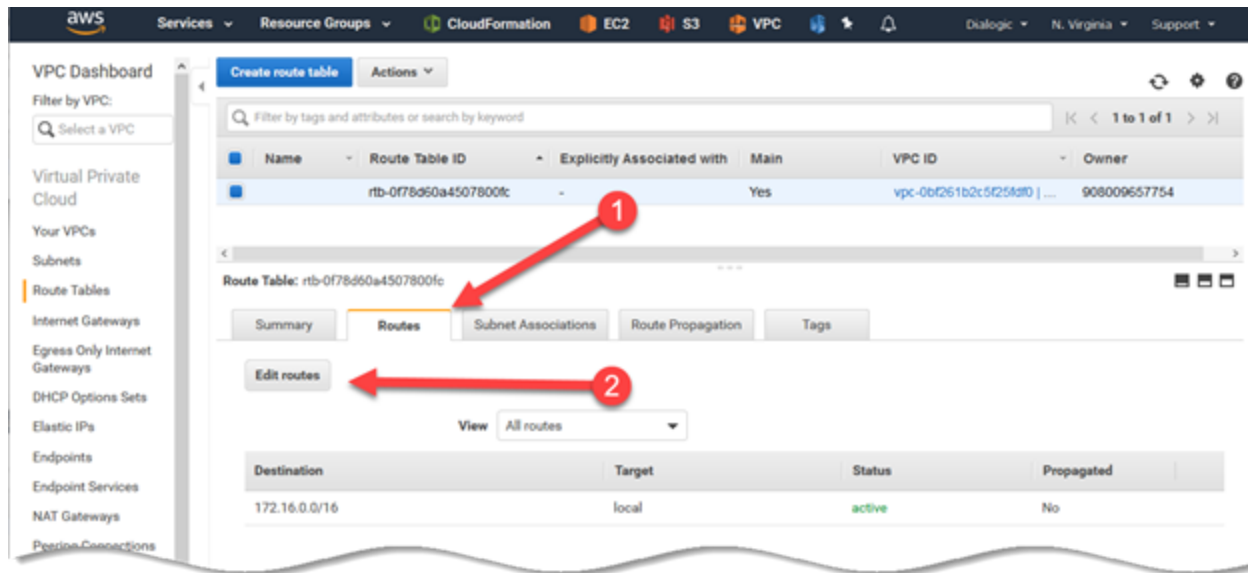
4.7 Modify the Route Table

→ To modify a Route Table:

1. In the **Virtual Private Cloud** group, select **Route Tables**.

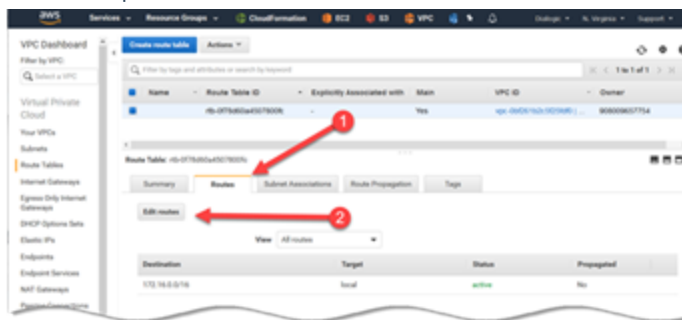


1. The **Route Table** window opens.
2. Select the newly created **Route Table** entry (automatically created upon the creation of the VPC).
3. At the bottom of the screen, select the **Routes** tab and click on **Edit Routes**.



4.

5. The **Edit Routes** window opens.



6.

7. Click on **Add Route**.

8. Enter the destination IP: **0.0.0.0/0**

9. Click on the local drop-down list and select the IGW that has previously been created.

10. Click on the blue **Save Routes** button.

4.8 Allocate Elastic IP Addresses

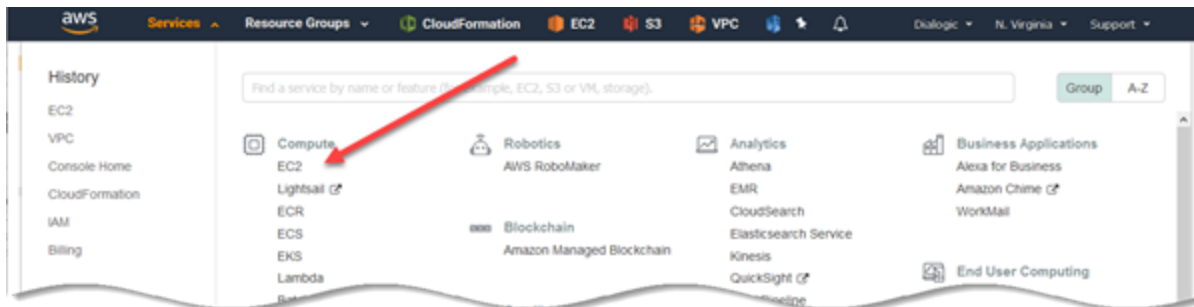
To remotely access the BorderNet SBC for management purposes, both private and public IP addresses should be allocated to it.

The private IP address has already been allocated at the **Network Interfaces** step.

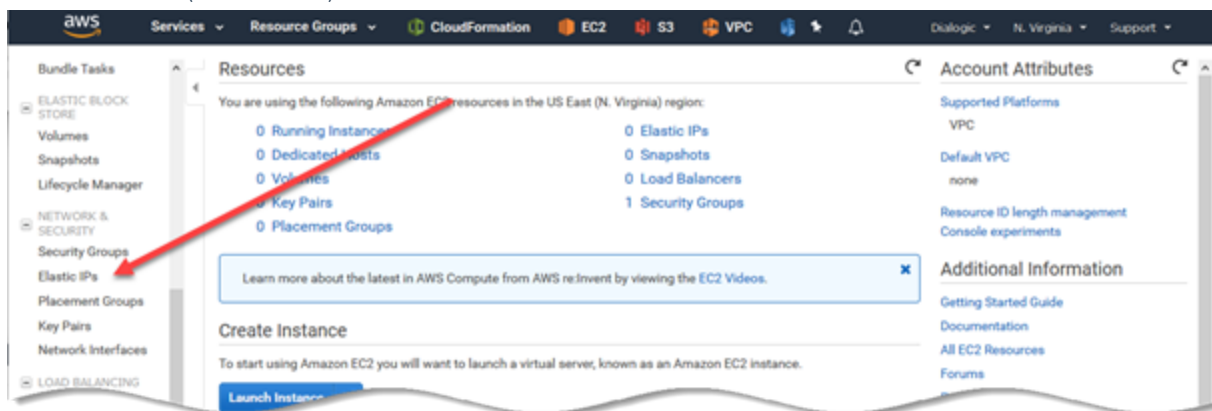
→ To allocate a public IP address:

1. Click on **Services**.

2. Click on **EC2** in the **Compute** group.

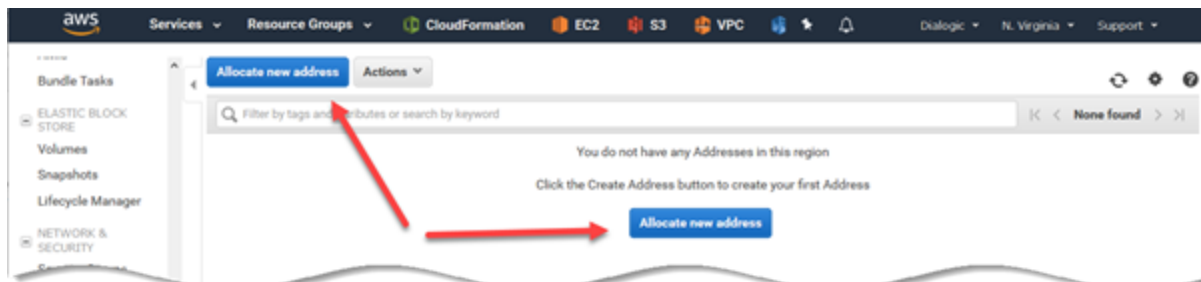


1. Select Elastic IPs (shown below).



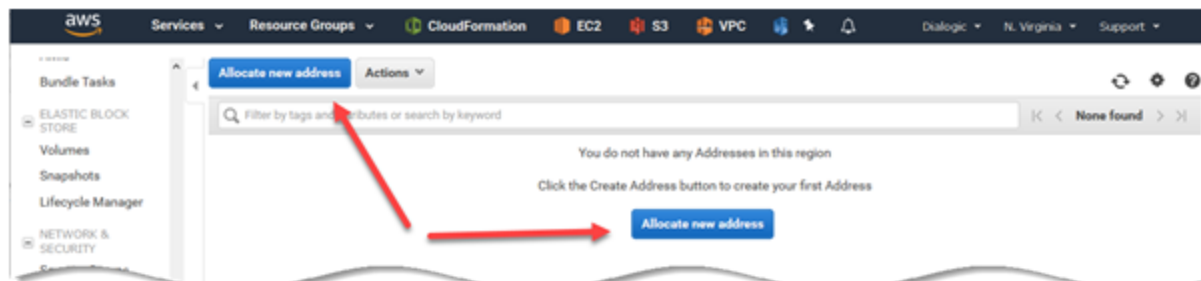
2.

3. Click on one of the blue Allocate new address buttons.



4.

1. The Allocate New Address window opens.



2.

3. In the IPv4 Address Pool field, select either Amazon pool or Owned by me if your company has a public IP address.

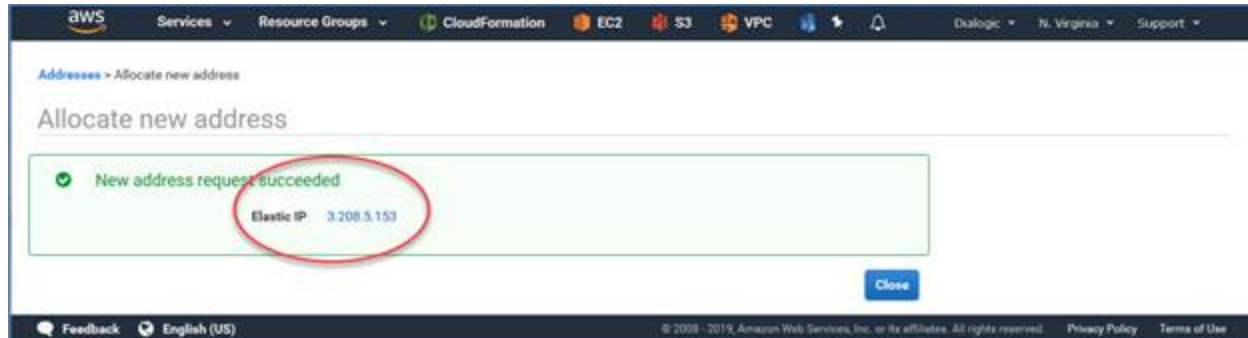
4. Click on the blue Allocate button.

4.8.1 Standalone Deployment Mode

For **High Availability** deployment mode proceed straight to [4.8.2](#).

In **Standalone** deployment mode it is necessary to have two elastic IPs (EIPs) for this example:

- 1 EIP for management
- 1 EIP for traffic from the public internet
- After clicking on the blue **Allocate** button, AWS reports that the new address is allocated and shows the IP address as in the following window.



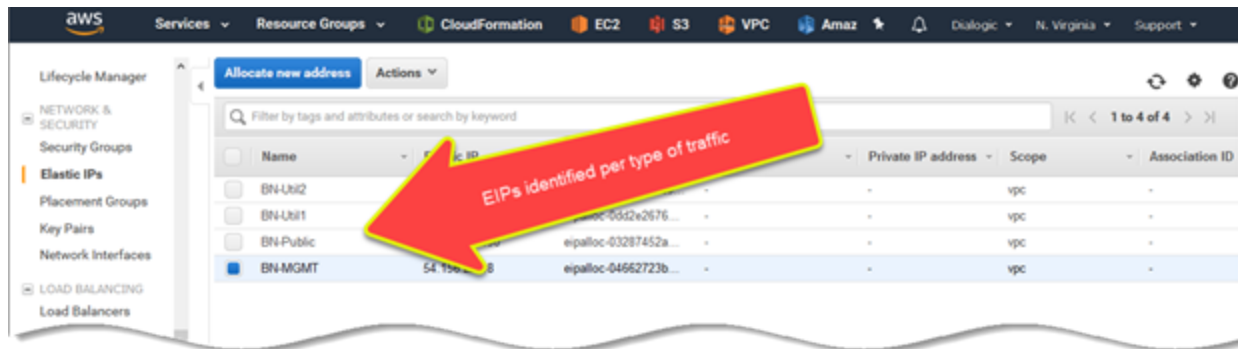
1. Repeat the steps above to create another EIP.
2. Name the EIPs to identify them.



4.8.2 High Availability Deployment Mode

In **High Availability** deployment mode it is necessary to have four elastic IPs (EIPs) for this example:

- 1 x EIP for management (floating)
- 2 x EIPs for utility (1 per instance)
- 1 x EIP for traffic from the public internet
- Name the EIPs to identify the use of the EIP.

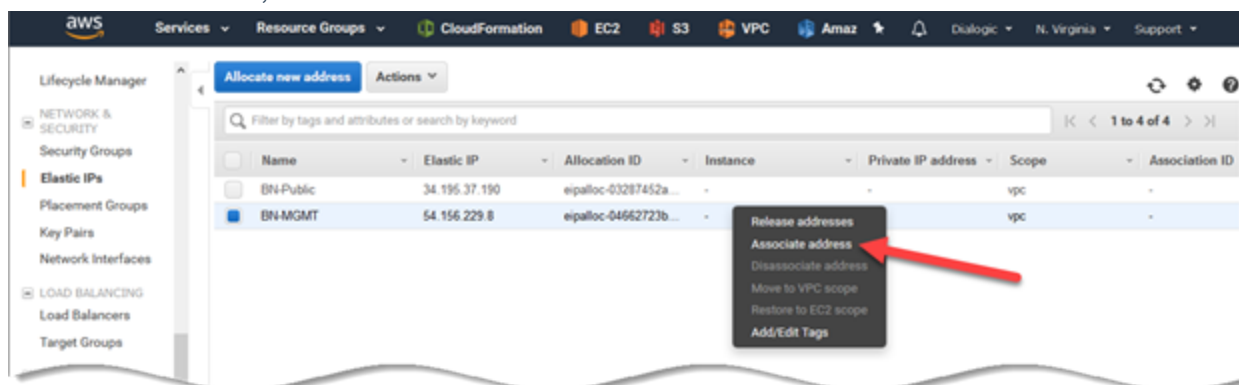


4.9 EIP to Network Interface Association

This facility is available only for Standalone deployments at this stage.

→ To create an EIP to Network Interface Association:

1. Right-click on one of the rows of the created and named EIPs.
2. A pop-up window opens.
3. Select **Associate Address**, as shown below.

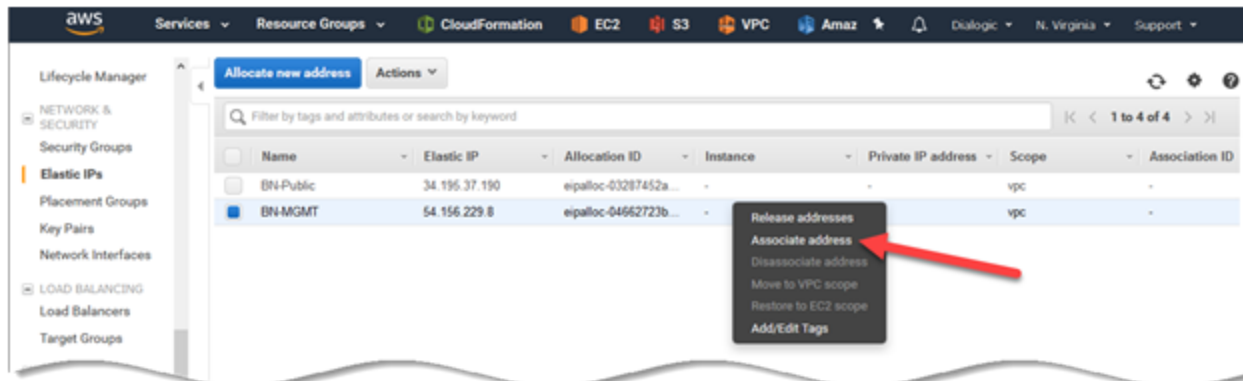


- 4.
5. The **Associate Address** window opens.

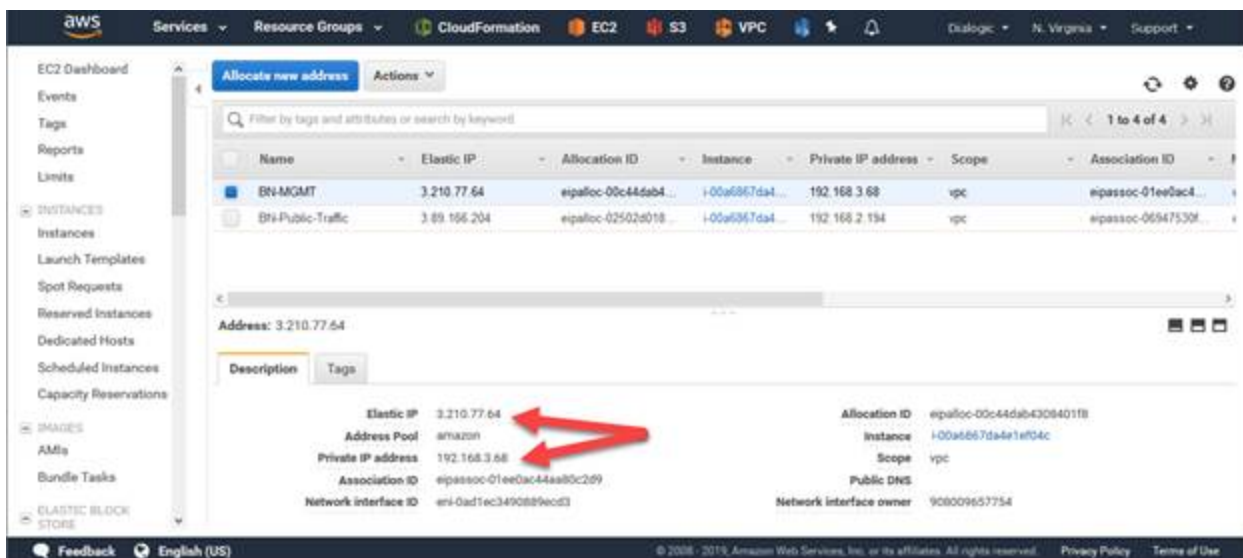
1. Select the following:
 2. **Resource type:** Network Interface.
 3. **Network Interface drop-down field:** Select the Network Interface to associate the EIP to.

Since we have identified the Network Interfaces, it is much easier to associate. See the example below.

- **Private IP:** Click on this field and select the Network Interface IP address to be associated.
- Click on the **Associate** button.
- Repeat the steps above for the Public SIP & RTP traffic.



1. The association of the EIP to the private IP can be seen in the screenshot below.



4.10 IAM Role

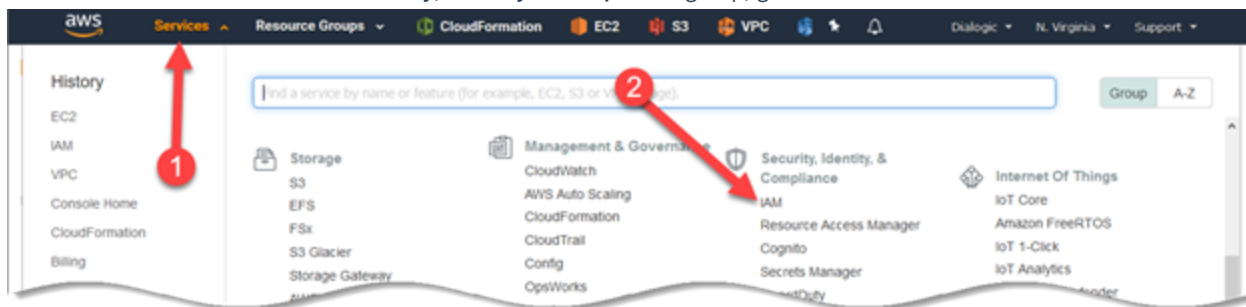
AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources for your users.

Using IAM, AWS users and groups can be created and managed. Users and groups can be assigned permissions to both grant and deny access to specific AWS resources.

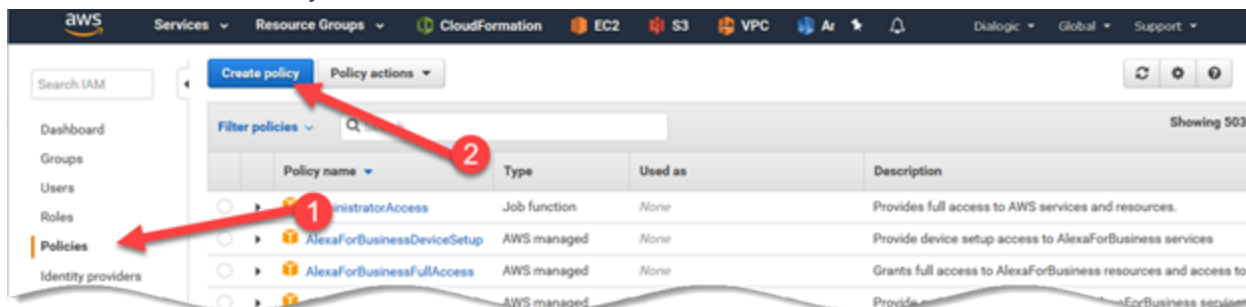
IAM is mandatory for HA deployments and can be used on Standalone deployments as well.

→ To create the IAM role:

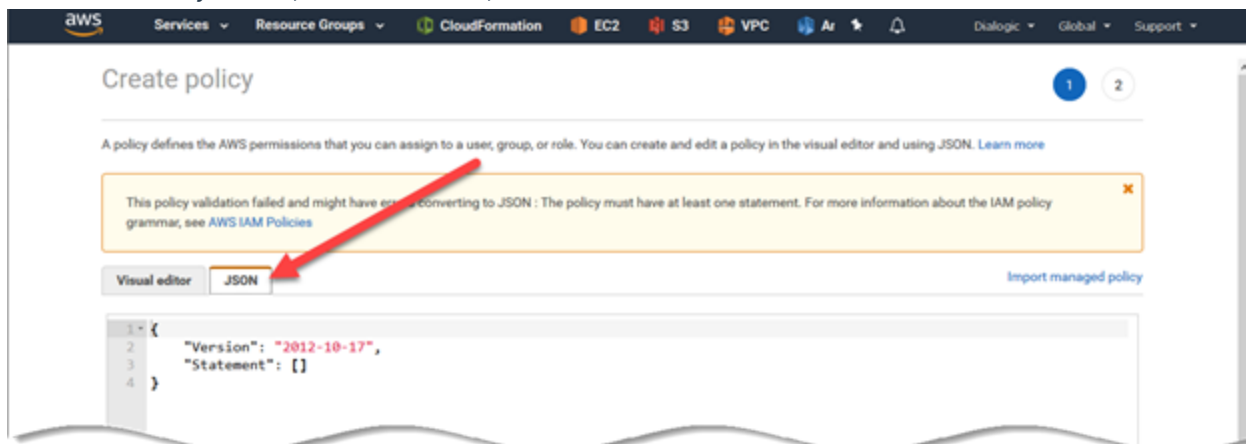
1. In the **Services** section under the **Security, Identity & Compliance** group, go to **IAM**.



- 2.
- 3. In the left-hand sidebar click on **Policies**.
- 4. Click on the blue **Create Policy** button.



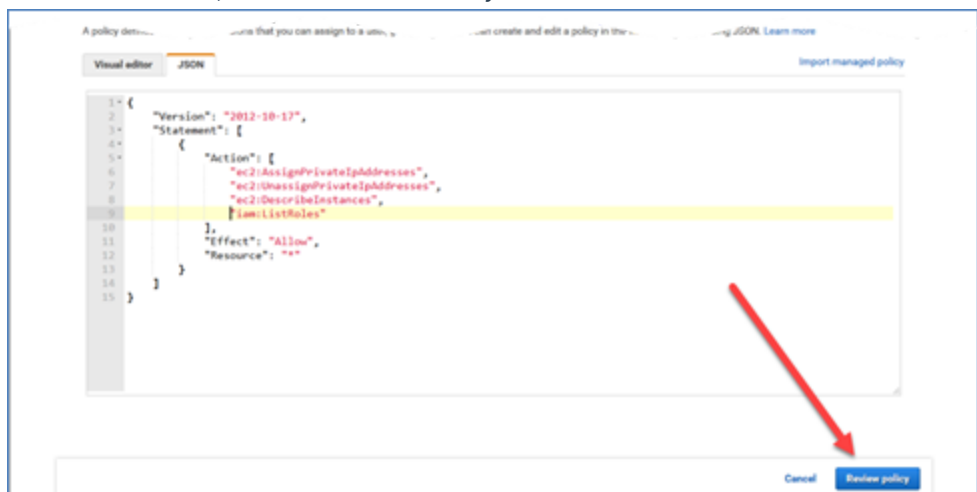
- 5.
- 6. In the **Create Policy** window, **Visual Editor** field, click on the **JSON** tab.



- 7.
- 1. If the **IAM** policy reports any error (see example below), then review each line for any unacceptable character.



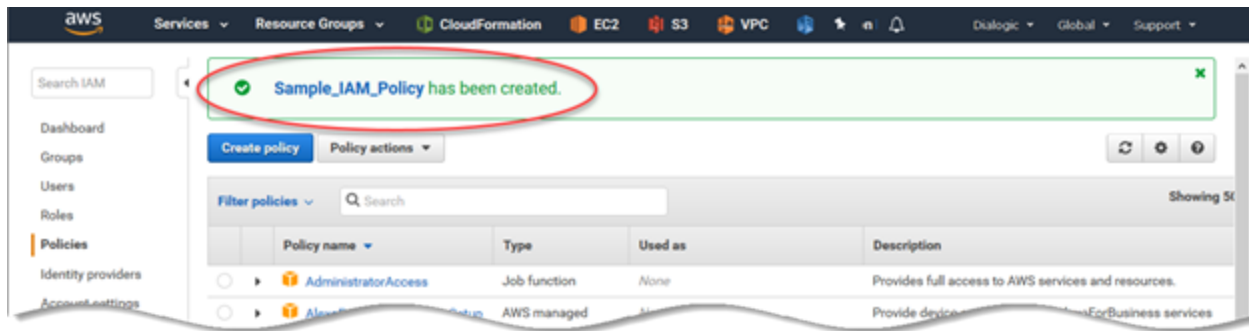
- 2.
- 3. If there are no errors, click on the **Review Policy** button.



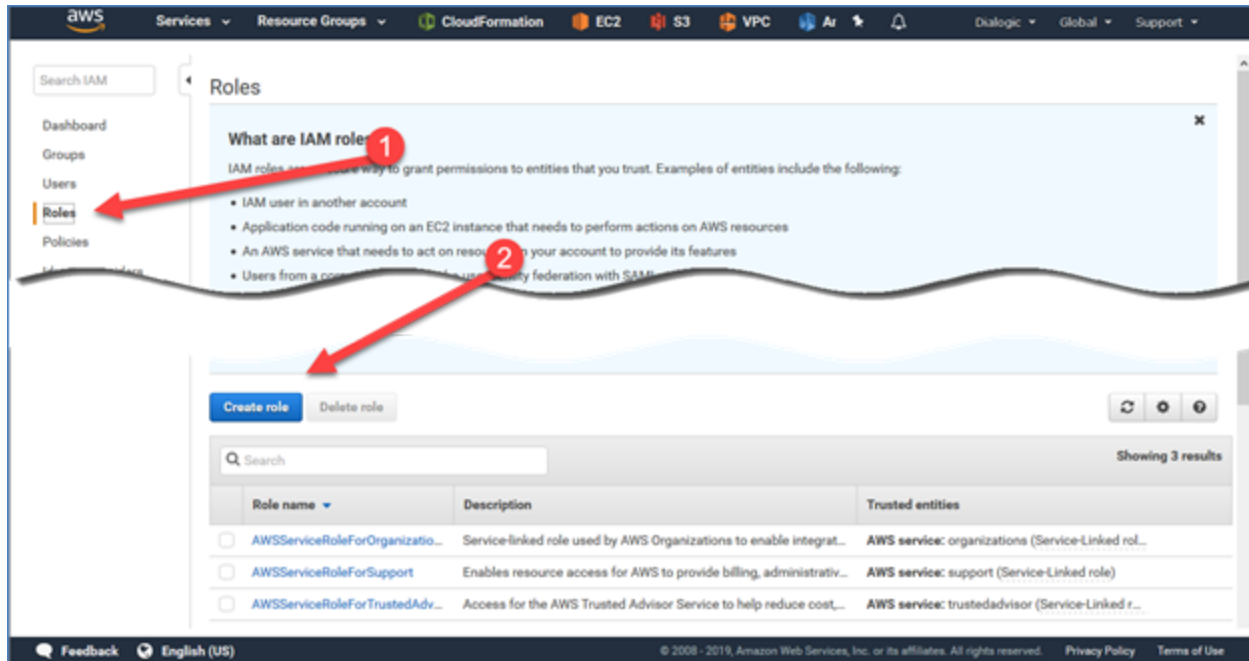
- 4.
- 5. Name the new IAM, and enter a description.
- 6. Click on the blue **Create Policy** button.



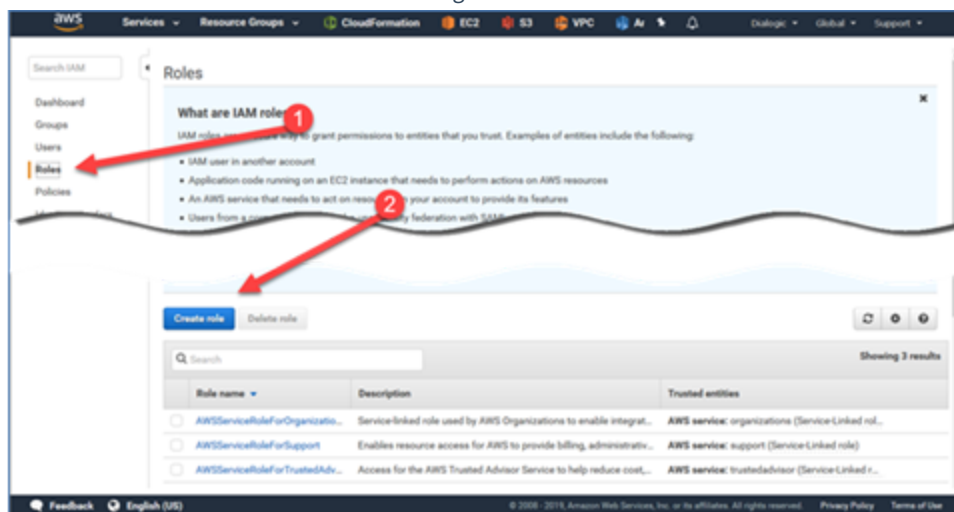
- 7.
- 8. The **Sample_IAM_Policy** is now created.
- 9. This Policy will now be assigned to a **Role**.



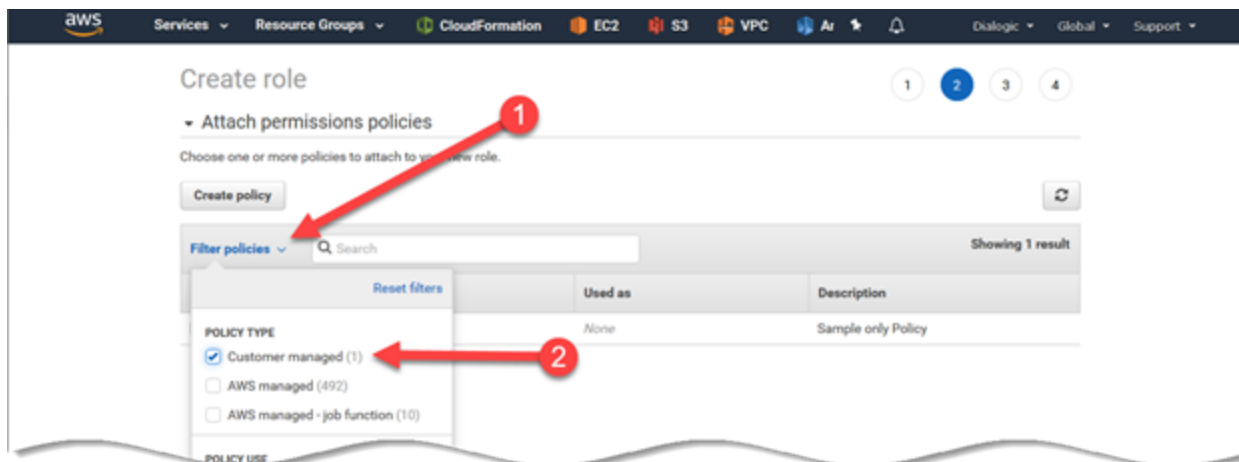
- 10.
11. In the left-hand column of the IAM window click on **Roles**.
12. Click on the blue **Create Role** button.



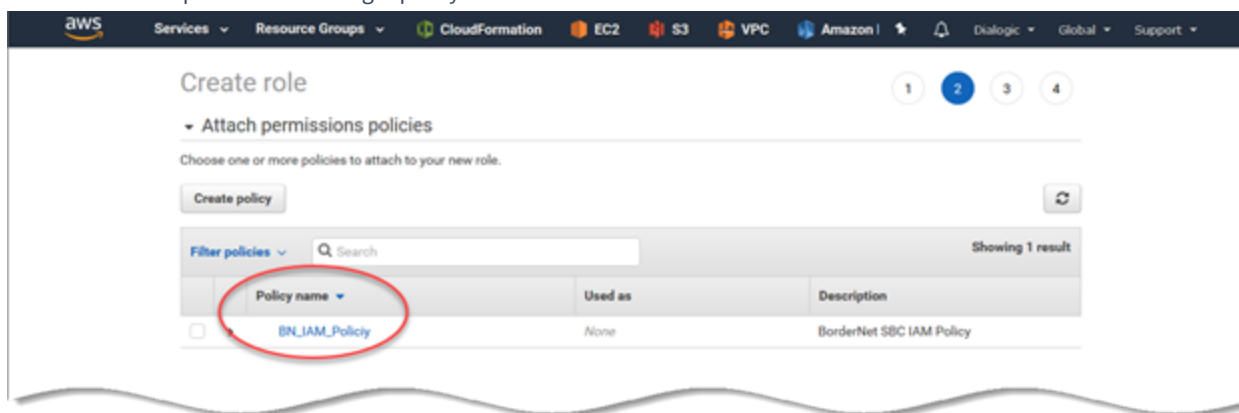
- 13.
14. Click on **AWS service** and then on **EC2** as shown below.
15. Click on the blue **Next: Permissions** button at the lower right-hand side of the window.



- 16.
1. In the **Create Role** window, click on **Filter Policies** (shown below).



- 2.
- 3. In the **Policy Type** group, select **Customer Managed**.
- 4. Click outside the panes and the target policy will be shown as illustrated below.

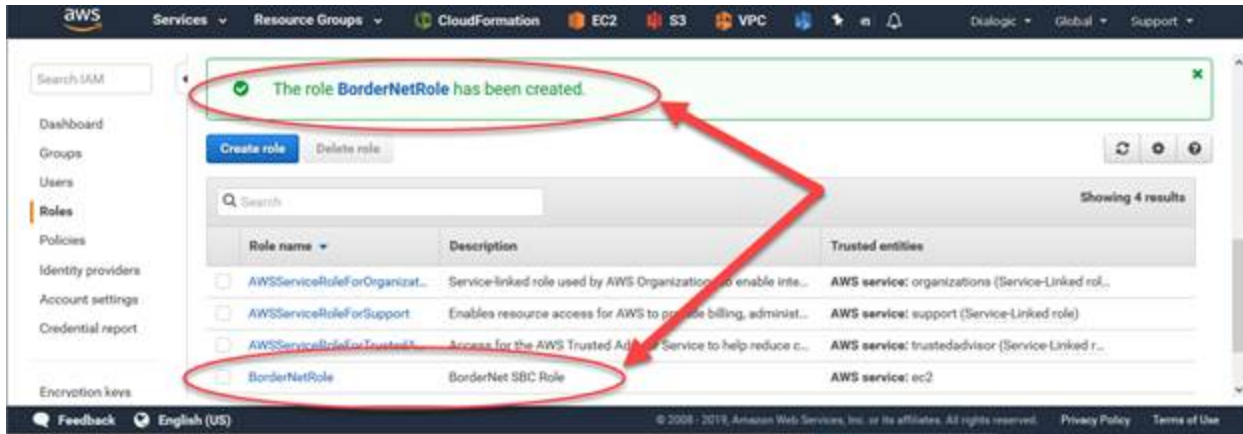


- 5.
- 6. Check that the Policy is visible.
- 7. Click on the blue **Next: Tags** button.
- 8. Tagging will not be performed.
- 9. Click on the blue **Next: Review** button.
- 10. Enter a **Role Name** and a **Role Description**.
- 11. Click on the blue **Create Role** button.



- 12.

1. The new **Role** is now created.

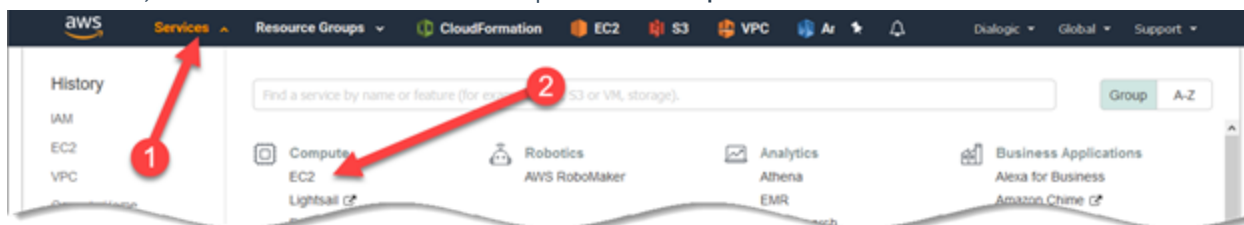


5. BorderNet SBC Installation Steps

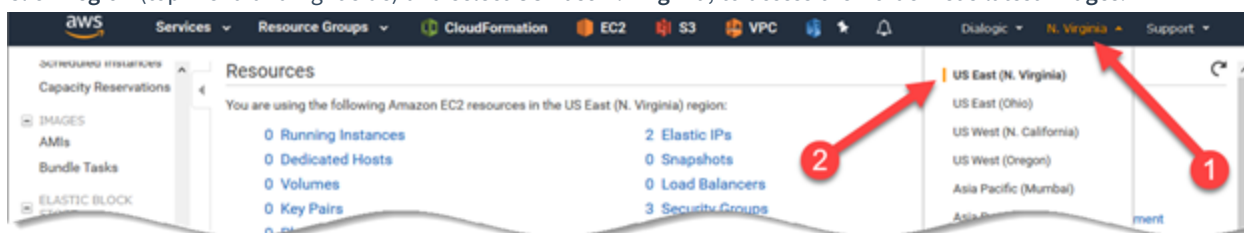
After having successfully configured the AWS resources the next step is to install the BorderNet SBC on the **AWS Cloud**.

→ To install the BorderNet SBC:

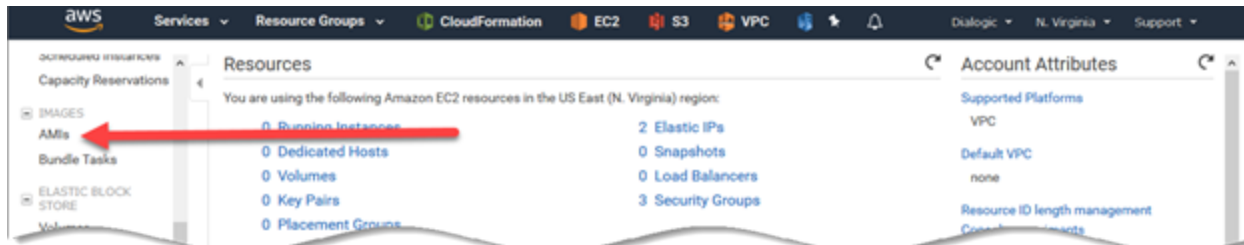
1. Login to your AWS account, if you haven't already done so.
2. In the toolbar, select **Services** and choose the **EC2** option in the **Compute** menu.



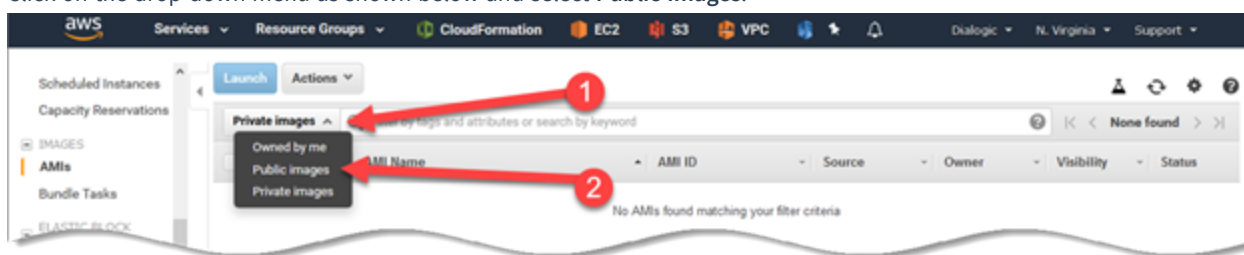
- 3.
4. Each **AWS Data Center** is considered a **Region**, which includes one or more **Availability Zones (AZ)**.
5. Click **Region** (top menu and right side) and select **US East N. Virginia**, to access the BorderNet's latest **Images**.



- 6.
7. Select the **Amazon Machine Images (AMIs)** in the left-hand sidebar.



- 8.
9. Click on the drop-down menu as shown below and select **Public Images**.



- 10.
11. Enter **Bordernet** in the search field and hit enter to locate all BorderNet images.
12. See the example below - this will filter and show all BorderNet SBC images in this region
13. Select the desired image (usually, latest version) and click **Launch**.
14. The **dialogic-bordernet-3.8.0.197** image is selected in this example.

Note:

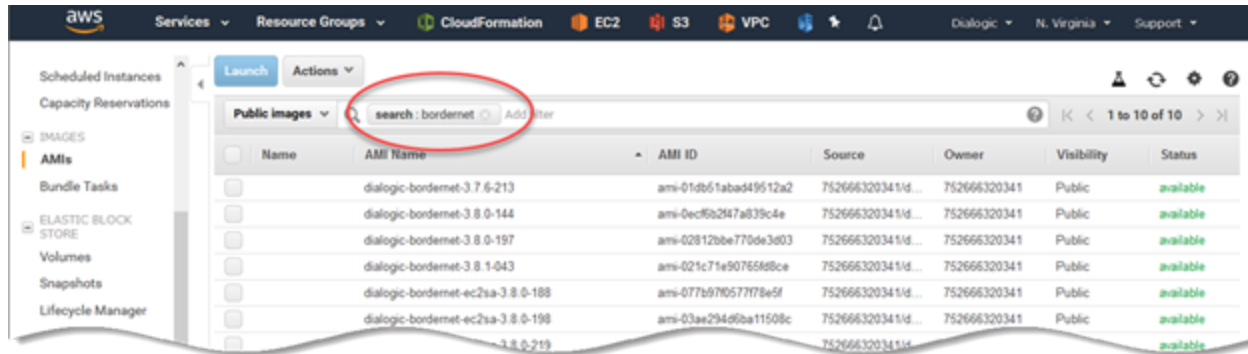
If required, copy the image to your region as follows:

- select the image

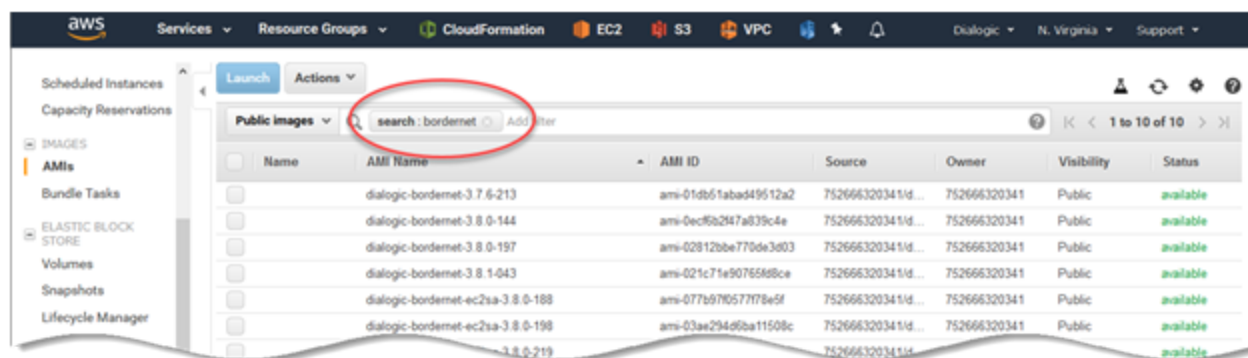
- click on the right button

- choose **Copy AMI**

- in the **Copy AMI** window, select the new destination.



- 1.
2. Select an instance type.
3. This window lists various resources groups (virtual instances of varying CPU, memory, storage and networking capacity combinations) that run the selected BorderNet SBC image.
4. Browse and select the **Compute optimized c4.xlarge** option (4 CPU cores, 7.5 GB, 750 Mbps) for this example.
5. Since the list is very large and in order to locate the correct image, you can use **control+F**.
6. See the screenshot below for reference and click on the **Next Configure Instance Details** button.



7.

8. The **Configure Instance Details** window opens.
9. Configure **Instance Details** (see screenshot on the following page).
10. Enter the following values for the parameters:
11. **Number of Instances**: 1 for Standalone, 2 for HA.
12. **Purchasing option**: Remains unchecked.
13. **Network**: Click on the drop-down list and select the VPC created on AWS resources.
14. **Subnet**: Click on the drop-down list and select the Management subnet created on AWS resources.
15. **Auto-assign Public IP**: Disable.
16. **Placement group**. No placement groups.
17. **Capacity Reservation**: Open.
18. **IAM role**: Select the IAM role created previously: **BorderNetRole**.
19. **CPU options**: None.
20. **Shutdown behavior**. Stop.
21. **Stop - Hibernate behavior**: Unchecked.
22. **Enable termination protection**: Checked (prevents accidental termination of the instance).
23. **Monitoring**. Unchecked.
24. **EBS-optimized instance**: Unchecked.
25. **Tenancy**: User's commercial choice with Amazon.
26. **Elastic Inference**: Unchecked.
27. **Network Interfaces**:
28. For **Standalone** only:

o **On eth0**:

- **Network Interface**: Select the management network interface
- **Subnet**: disabled
- **Primary IP**: disabled

o Click on the **Add device** button.

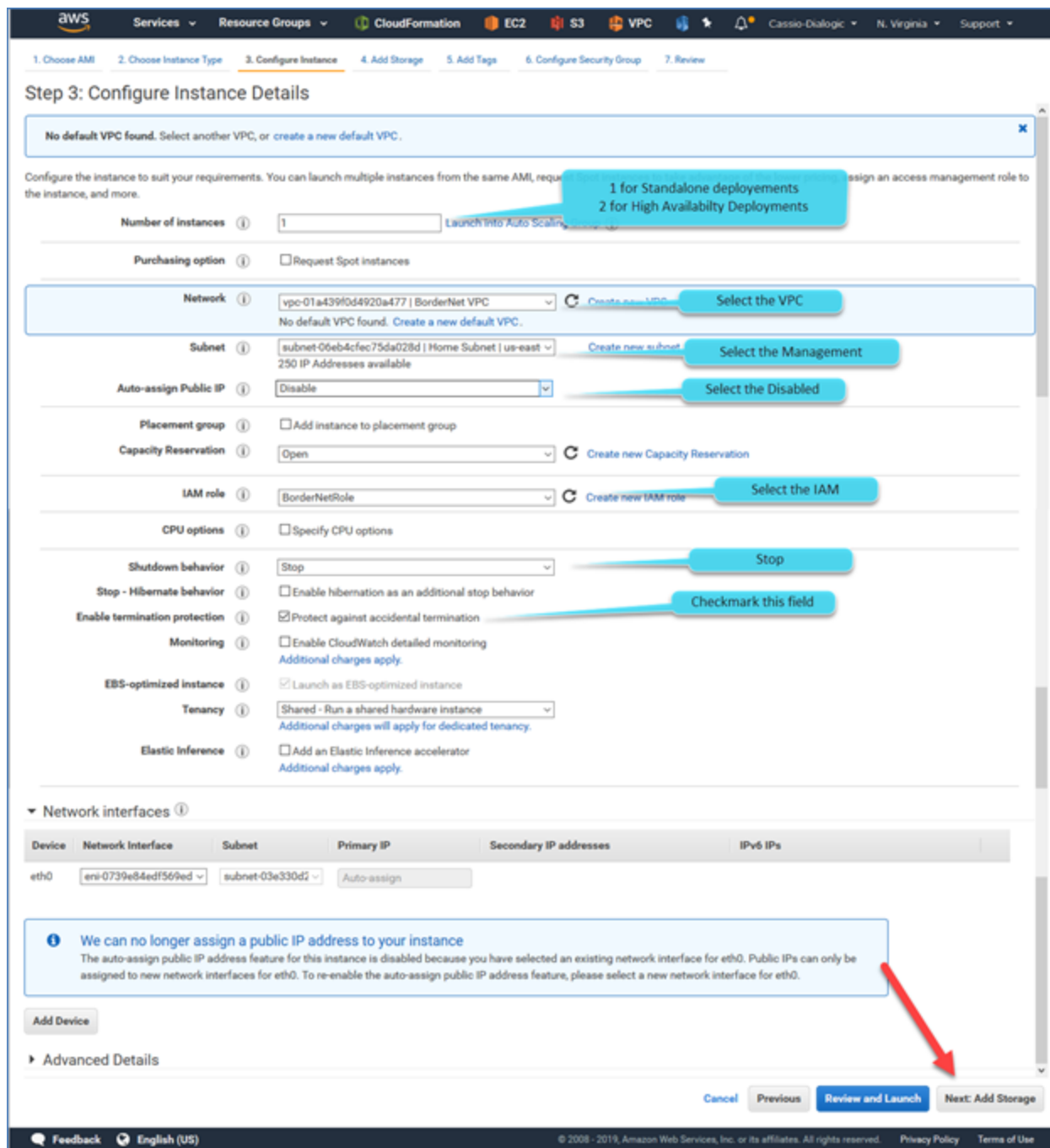
Eth1 interface will be added to the list.

o **On eth1**:

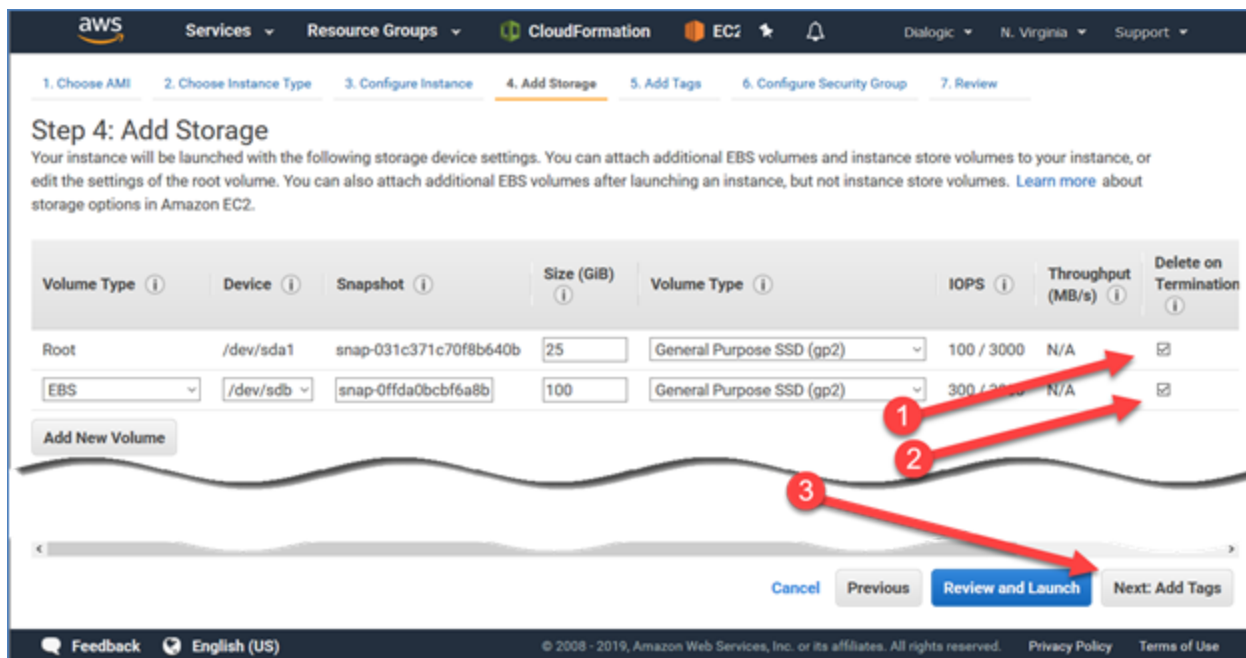
- **Network Interface**: Select the public interface
- **Subnet**: disabled
- **Primary IP**: disabled
- For **High Availability**:

o Leave empty. This will be filled later.

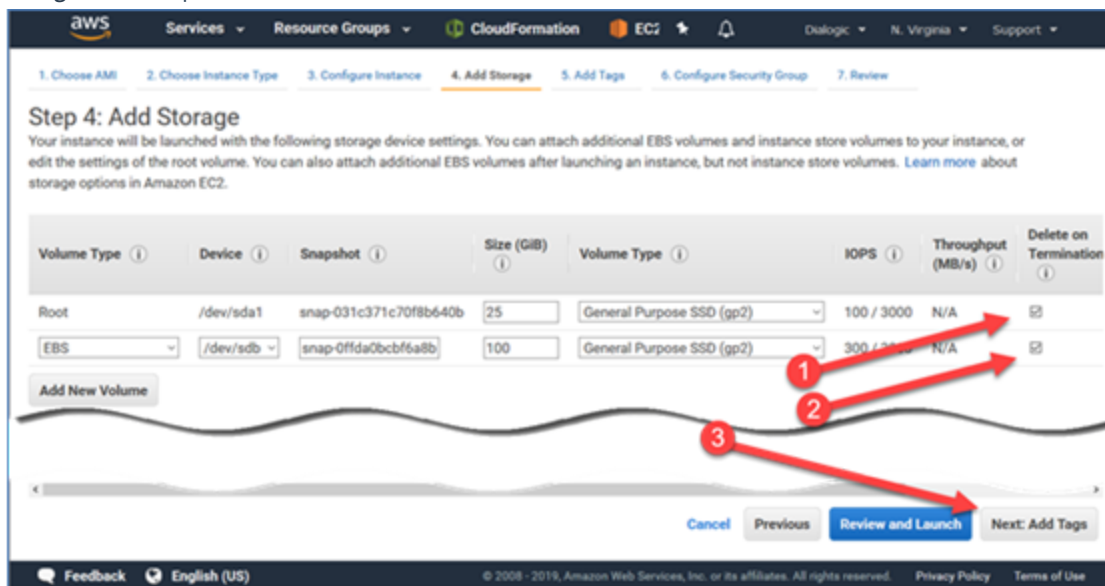
1. Click the **Next:Add Storage** button.



1. The Add Storage window opens.

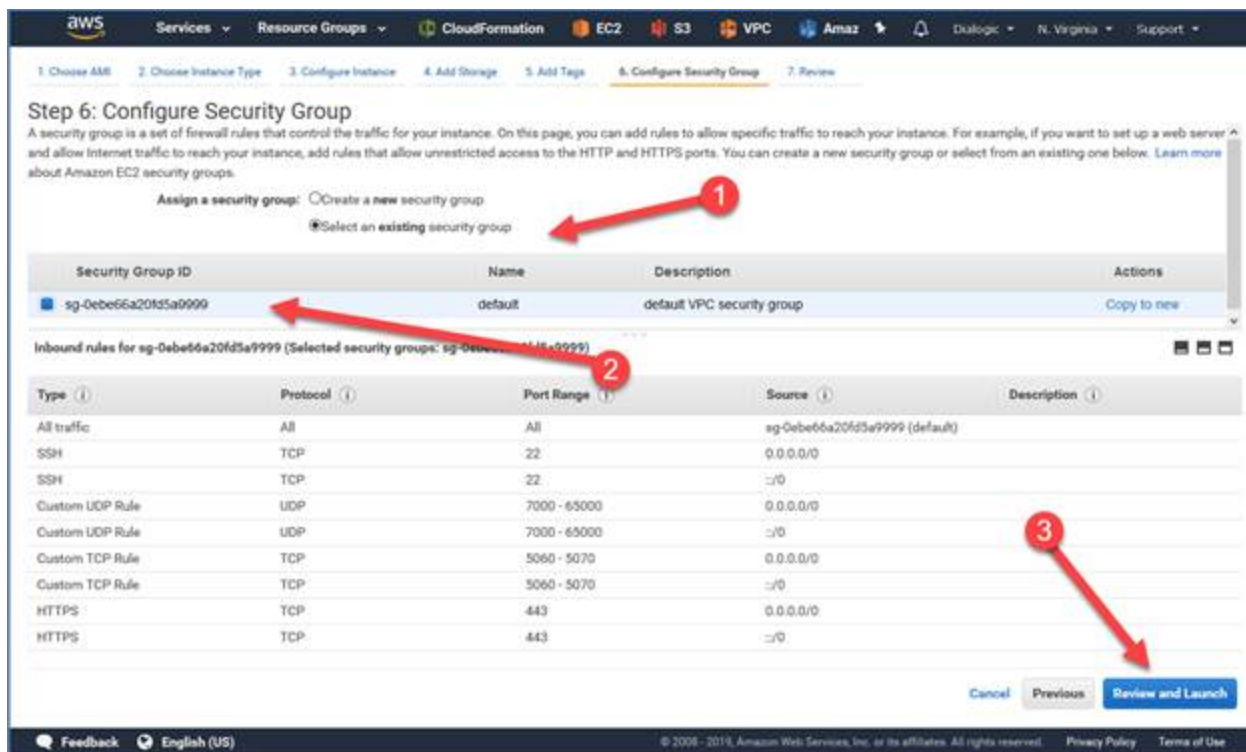


- 2.
3. Check the **Delete on Termination** check-box to remove any leftovers.
4. Click on the blue **Next: Add Tags** button.
5. The **Add Tags** window opens.

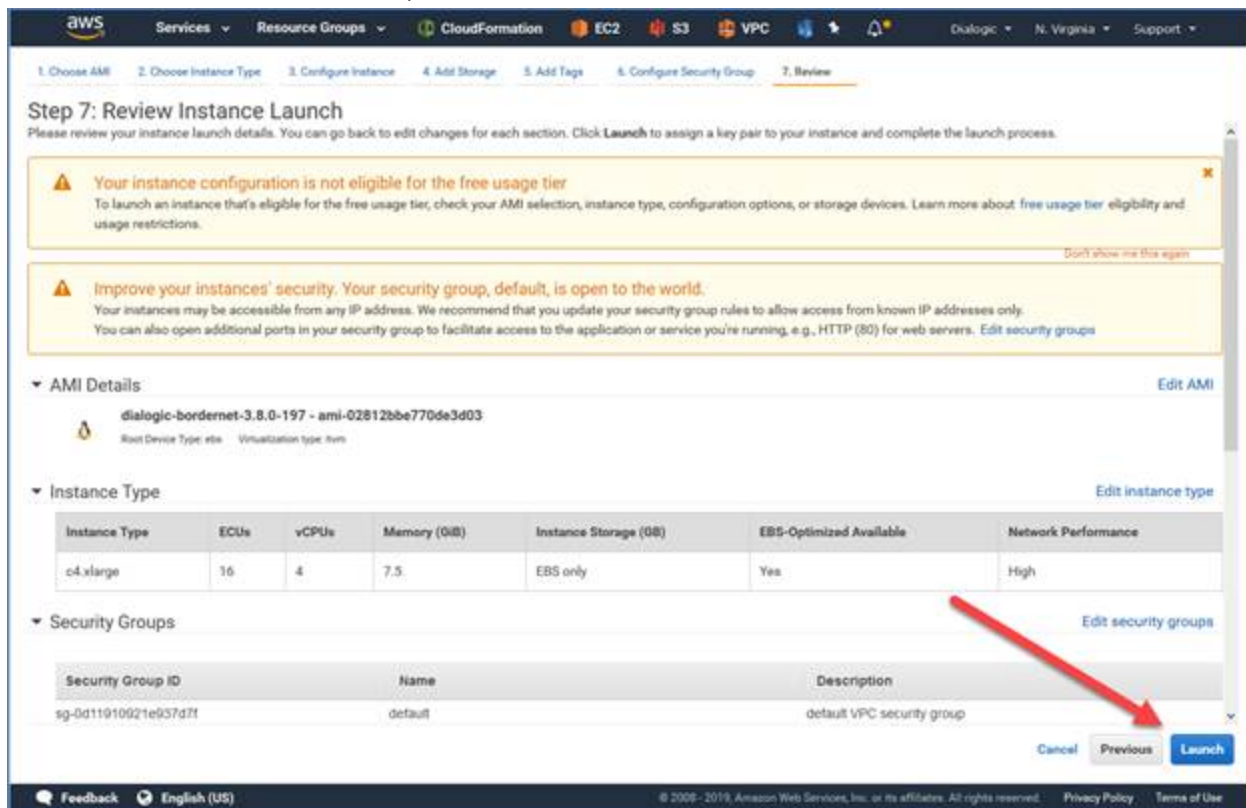


- 6.
7. No actions are required on this screen.
8. Click on the blue **Next: Configure Security Group** button.

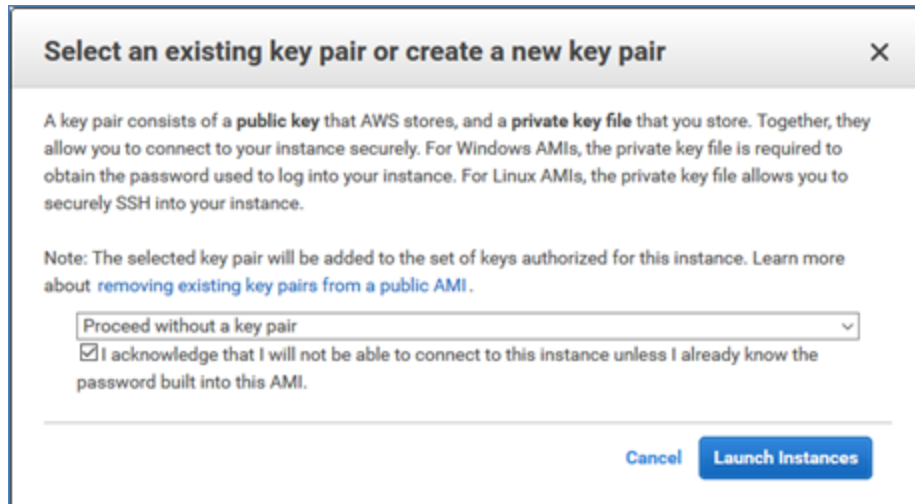
1. The **Configure Security Group** window opens.



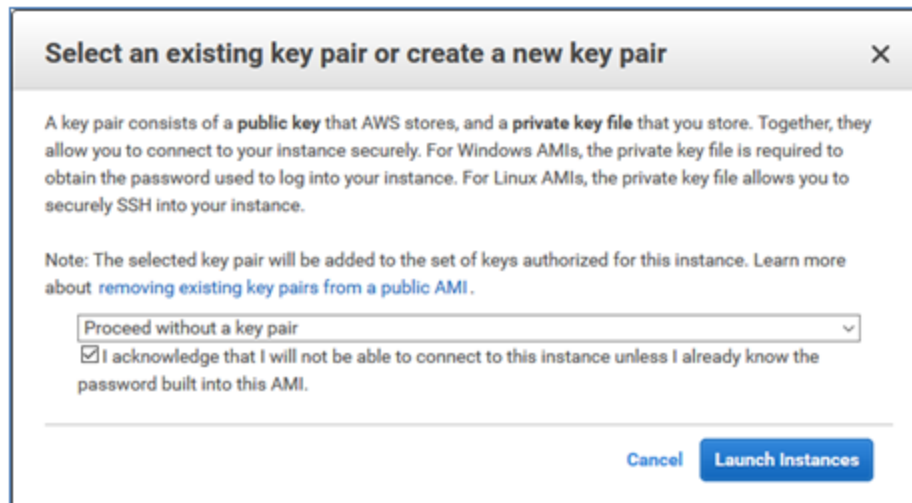
- 2.
3. Select the existing Security Group.
4. Click on the blue Review and Launch button.
5. The Review Instance Launch window opens.



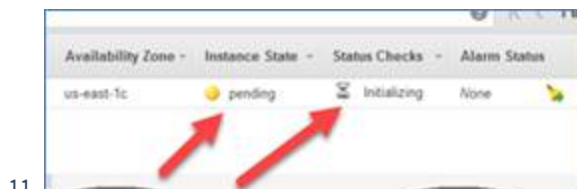
- 6.
1. Assure all configurations were properly completed and click on the blue Launch button.
2. The Select an existing key pair window opens.



- 3.
4. Select **Proceed without a key pair**.
5. Check the acknowledgement clause.
6. Click on the blue **Launch Instances** button.
7. The **Launch Status** window opens.



- 8.
9. The new instance is created.
10. Click on the blue **View Instances** button to follow the deployment.



- 11.

6. Attaching Network Interfaces

This procedure is pertinent to HA deployments only.

For Standalone deployments refer to [First Access](#).

In this step the Public and Private traffic network interfaces will be attached to the BorderNet SBC.

6.1 Identifying the Instances

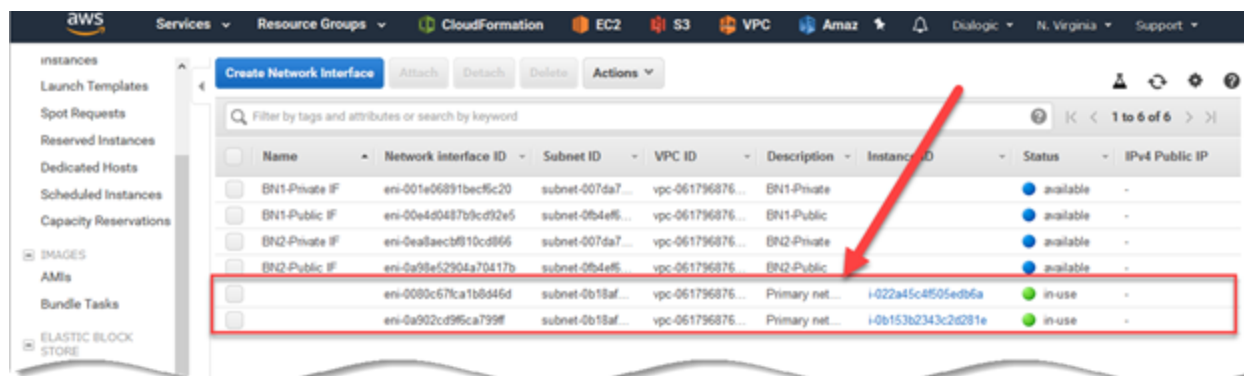
As stated previously, identifying resources is a good practice to follow at this point in the configuration.

→ To identify the instances:

1. Click on **Services > EC2** and select **Instances** in the left-hand sidebar menu.
2. Identify the newly created instances and note that there is no difference between each instance at this point.
3. Make note of the Instance ID for **primary** and **secondary**.
4. These IDs will be used in the following steps.



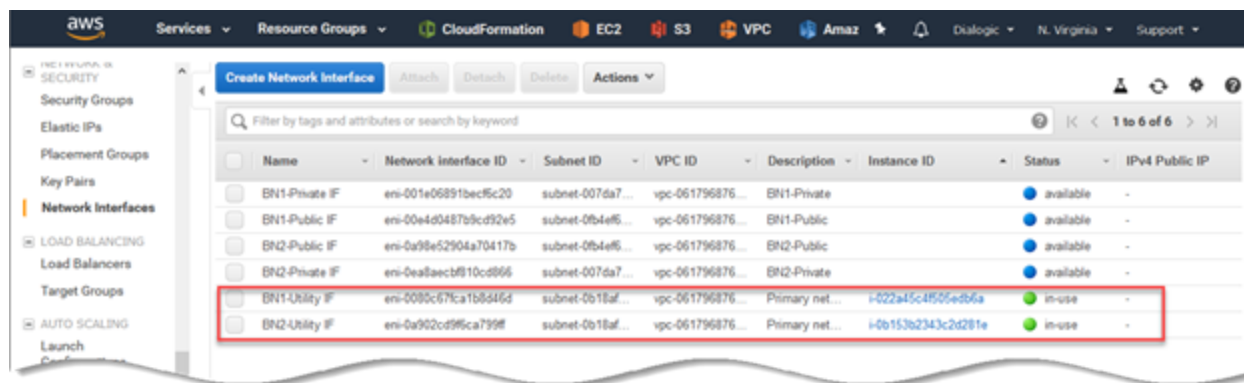
1. Click on **Network Interfaces** (path: **Services > EC2 > Network Interfaces**).
2. Notice that there are two new interfaces on the list.
3. They will be attached to each instance of the BorderNet SBC:



6.2 Identifying the New Interfaces

→ To identify the new interfaces:

1. Identify the two new **Network Interfaces** - the **Utility** and **Management** interfaces.
2. Use the instance ID created previously to determine which **Network Interface** is associated to which instance.
3. See the interfaces identified below.

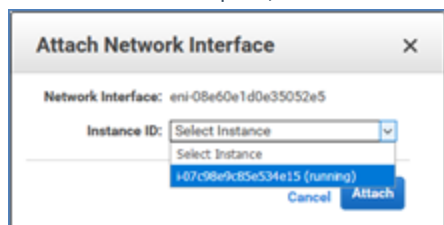


6.3 Attaching the Network Interfaces

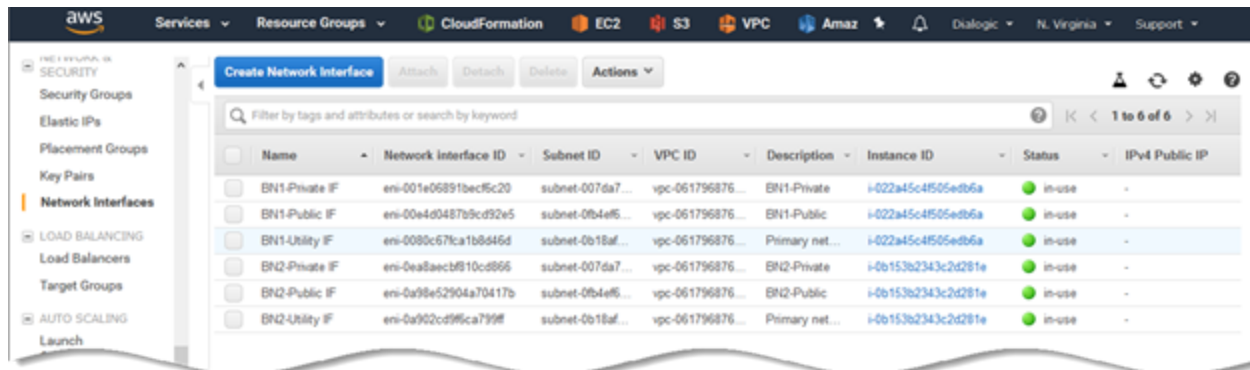
Public and Private interfaces created previously need to be attached to the appropriate instances.

→ To attach the Network Interfaces:

1. Select one of the interfaces.
2. Open the right-click menu of options.
3. Select **Attach**.
4. In the window that opens, select the instance to attach the Network Interface to.



- 5.
6. Click on the blue **Attach** button.
7. Repeat the step for the remaining Network Interfaces.
8. At this point, the Network Interfaces are attached to the respective instance.



9.

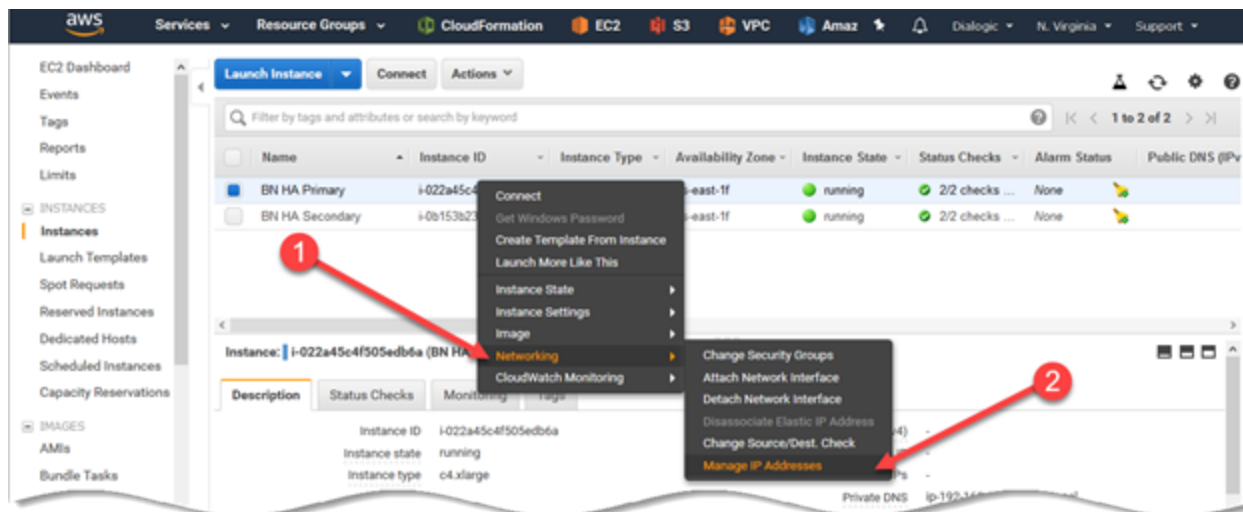
7. Adding IP Addresses to Primary Instance

This procedure is pertinent to HA deployments only.

As machines must be able to switch traffic on failures, additional private IP addresses on the Primary instance are required.

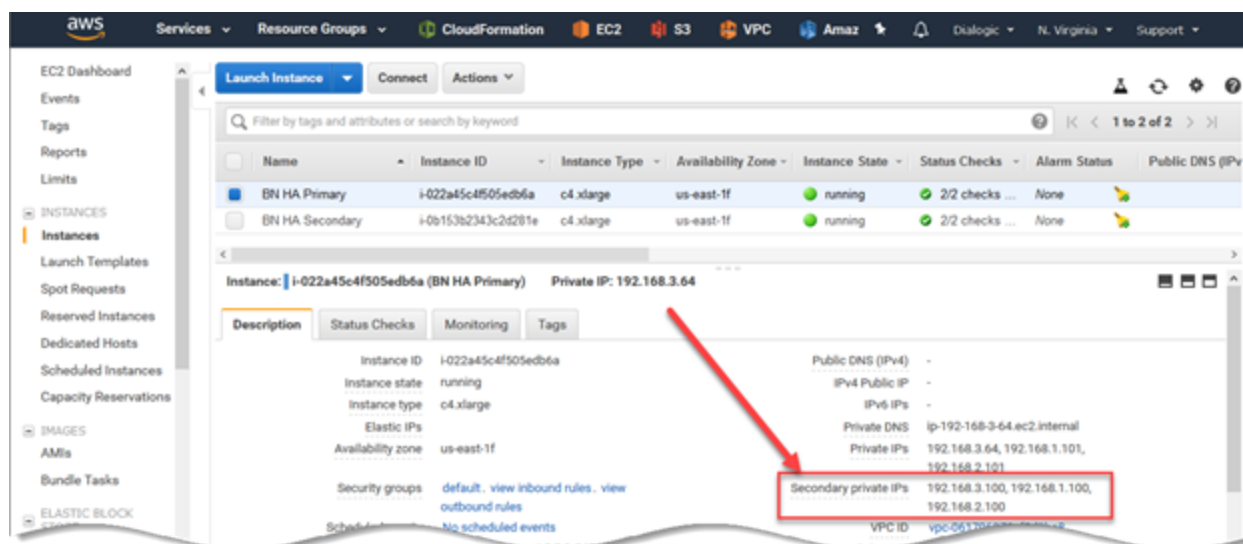
→ To create additional IP addresses:

1. Go to the instances at **Services > EC2 > Instances**.
2. Right-click on the primary instance and select **Networking > Manage IP Addresses**.
3. See below.



- 4.
5. In the **Manage IP Addresses** window that opens, add a new IP address on each eth (0, 1, 2).
- 6.

1. IP addresses can be auto-assigned by AWS or manually entered as follows:
2. Eth0 - 192.168.3.100
3. Eth1 - 192.168.1.100
4. Eth2 - 192.168.2.100
5. Notice the Secondary IPs added to the Primary instance:

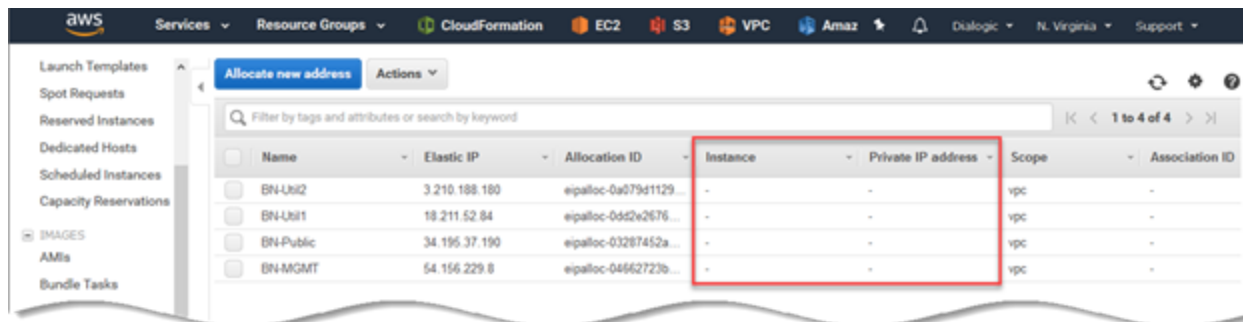


8. Attaching EIPs to Each Instance

This procedure is pertinent to HA deployments only.

→ To associate the EIPs created previously to each instance:

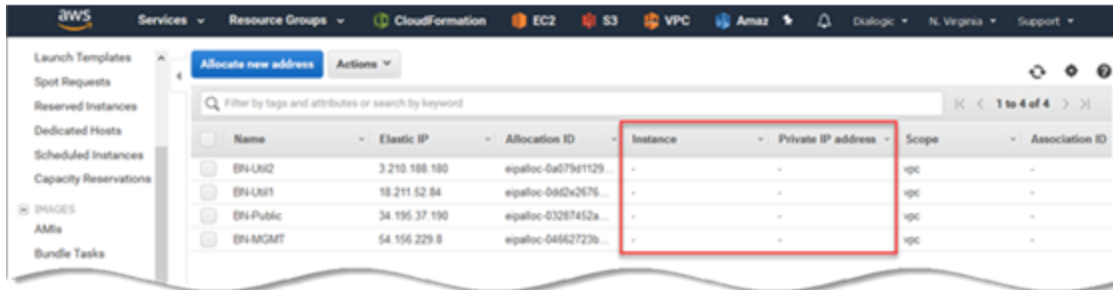
1. In the left-hand sidebar under the **Network & Security** group, click **Elastic IPs**.
2. Notice that the EIPs are not associated to any instance nor do they have Private IPs.



1. Select one of the EIPs in the row.
2. Open the right-click menu and select **Associate**.
3. The **Associate Address** window opens.
4. Use the table below to create the association.

Network Interface	Private IP	Comments
BN1-Utility	192.168.3.100	Management floating IP
BN1-Utility	192.168.3.64	Utility IP to SSH to Primary instance
BN Public	192.168.2.100	Traffic floating IP
BN2-Utility	192.168.3.24	Utility IP to SSH to Secondary instance

1. Click on the blue **Associate** button after each association.
2. See the sample association screen below.



The screenshot shows the AWS console interface for Elastic IP Allocation. The table lists four allocations with columns for Name, Elastic IP, Allocation ID, Instance, Private IP address, Scope, and Association ID. A red box highlights the Instance and Private IP address columns for all rows.

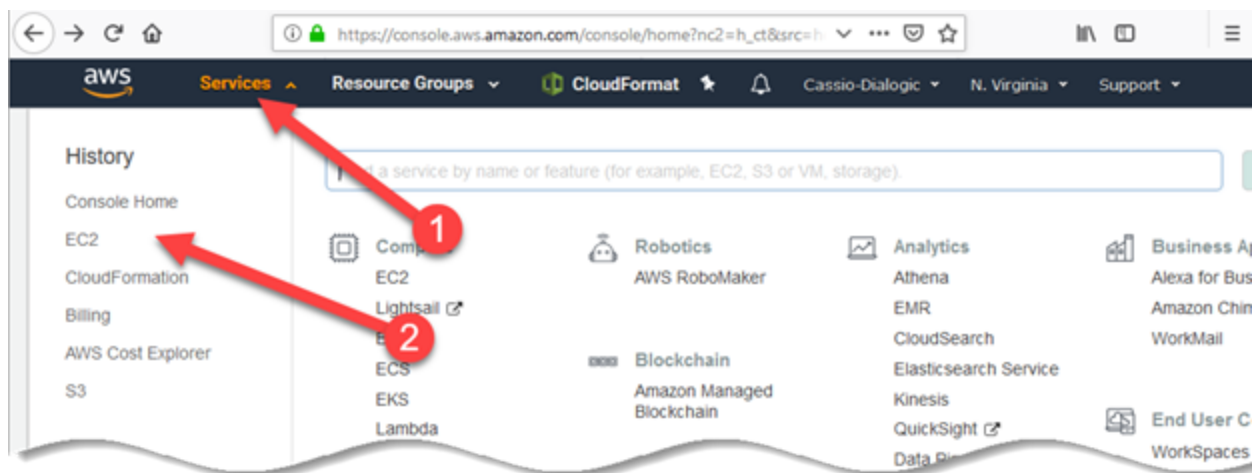
Name	Elastic IP	Allocation ID	Instance	Private IP address	Scope	Association ID
EN-LIN2	3.210.188.180	epalloc-0a079d1129...	-	-	vpc	-
EN-LIN1	10.211.52.84	epalloc-0d62x2676...	-	-	vpc	-
EN-Public	34.195.37.190	epalloc-03287452a...	-	-	vpc	-
EN-MGMT	54.156.229.8	epalloc-04862723b...	-	-	vpc	-

9. First Access to the BorderNet SBC

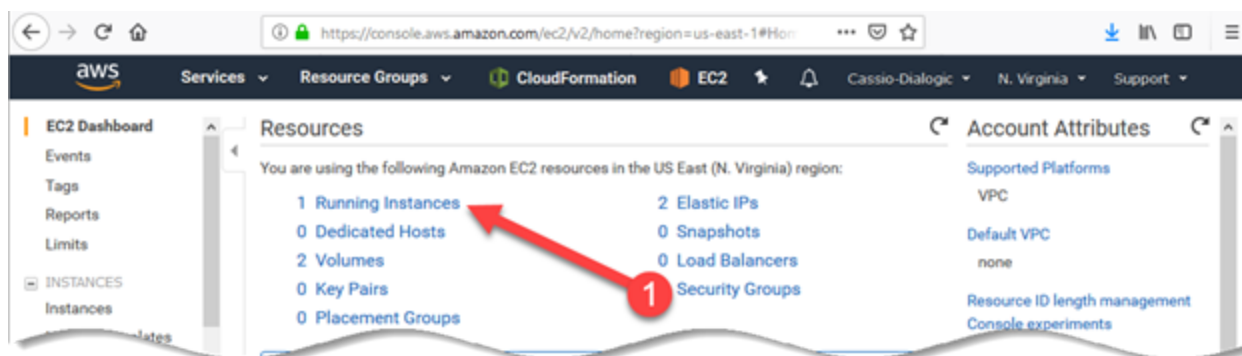
You can now access the BorderNet SBC. The IP address is therefore required. This address is provided by AWS and can be determined by following the steps below.

→ To access the BorderNet SBC:

1. Click **Services > EC2**.



- 2.
3. Click **Running Instances**.



9.1 Locating the Management IP Address

9.1.1 Standalone Instances

On Standalone deployments the Utility and Management IP addresses are the same.

See the screenshot below for further reference.

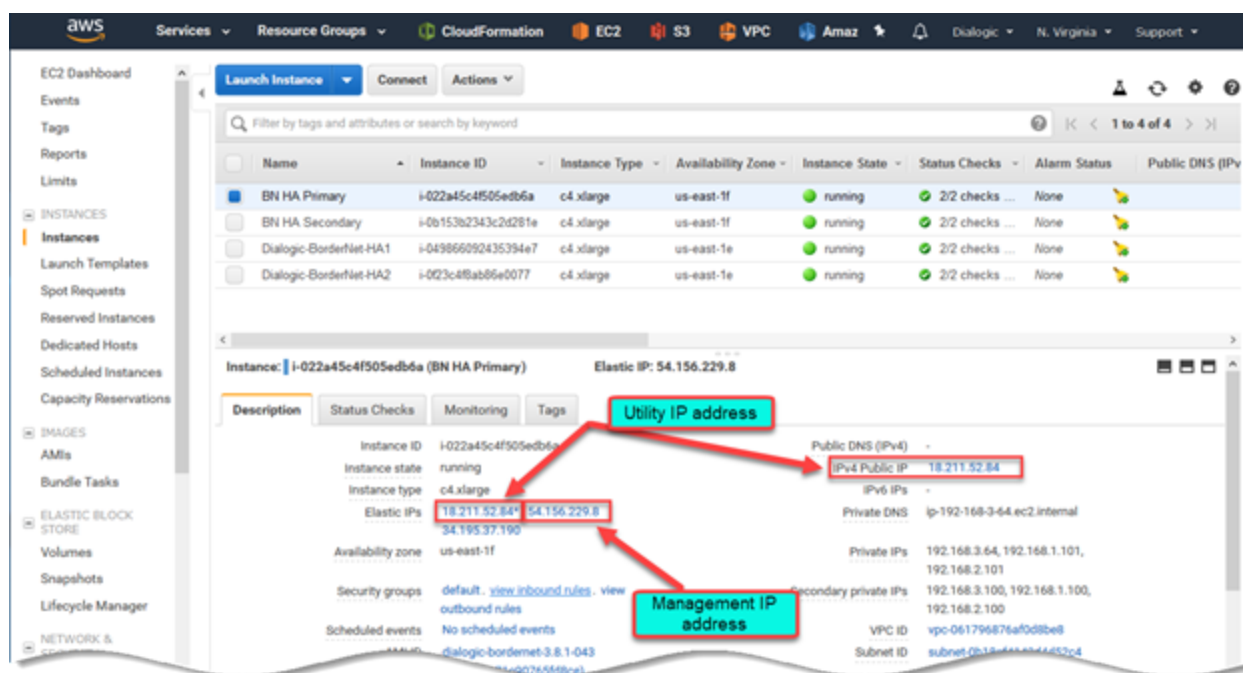
9.1.2 HA Instances

On High Availability deployments there are three EIPs for managing the BorderNet SBC:

- two EIPs are used for the Utilities (one per instance)
- one EIP is used for Management (GUI)

→ To locate the public IP addresses:

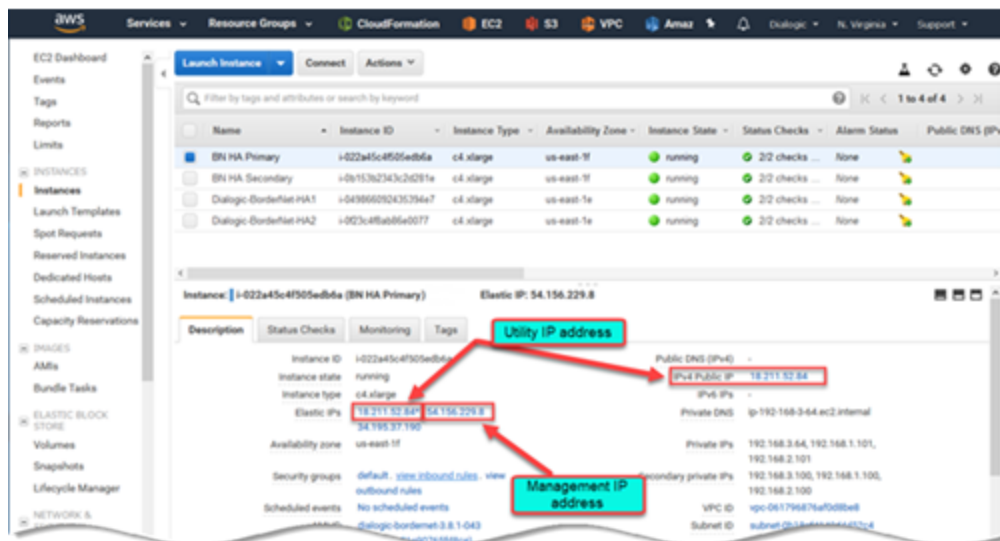
1. Go to the instances at **Services > EC2 > Instances**.
2. Select one of the instances.
3. Notice at the bottom half of the screen - **Elastic IPs** and the **IPv4 Public IP** shown below.
4. The Utility IP address will be presented in both the **Elastic IPs** and the **IPv4 Public IP** fields.
5. Only the active instance will have the Management IP address and the standby instance/platform will only have the Utility IP address.
6. Note and document the Management IP address at this point.



9.2 Accessing the GUI

1. Open your preferred browser.
2. For Standalone deployments, enter the Management/Utility IP address (they are the same for Standalone) using the following format: **https://<BorderNet SBC Management IP address>**.
3. For HA deployments, enter the Utility IP address using the following format: **https://<BorderNet SBC Management IP address>**.
4. The browser may alert to a potential security risk.
5. This is due to the SSL with an unknown certificate.
6. Each browser may show different types of alert screens.

1. For example, when using Firefox, click on **Advanced** and on **Accept the Risk and Continue**.



9.3 Deploying your Instance

Deploying the BorderNet SBC in AWS requires much less information compared to bare metal or other types of virtualized deployments, since most of the IP address are already linked to AWS resources (created in previous steps).

9.3.1 Standalone Deployment

When deploying a Standalone BorderNet SBC, only a hostname is required. All other fields are already filled and cannot be changed.

See the screenshot below:

13. Document the Primary Utility IP address for use later.
14. Proceed to the secondary instance deployment.

→ To deploy the Secondary Instance in HA:

The process to deploy the Secondary platform is similar to the Primary but requires less information.

Select the web browser page that contains the Secondary instance.

1. In the **BorderNet System Deployment** screen select **Secondary Platform**.
2. **Deployment Type:** HA
3. **Designated Role:** Secondary
4. Notice only the Primary platform **Inter-Task** can be added.
5. Enter the Utility private IP address of the Primary platform (documented in the previous step).
6. Document the Secondary **Inter-Task IP** address.
7. This IP address will be used to finish the Primary platform deployment (see below).
8. **DO NOT** click on **Start Deployment** just yet!

1. The **Primary Instance** configuration must be completed first.

Dialogic[®] BorderNet[™] SBC

Welcome to BorderNet SBC (v3.8.1-043) System Deployment

Platform Serial Number : V4284219592
License Request ID : 1E39D3551203F0368F3DA9980F3F4FFF BF5F9F98FEF1FCF3BC91CEA0807BFA9

Provide following information to complete the deployment

Deployment Type : HA
Designated Role : Secondary

Note: Before starting this platform deployment, make sure that primary platform is up and connected to this platform on HA link. Following information is used to connect to primary platform. Make sure to provide correct IP's and netmask.

Inter-Task/HA-Link IP for this platform : 192.168.3.200
Inter-Task/HA-Link Netmask : 24
Inter-Task/HA-Link IP for primary platform :

Start Deployment

→ To Continue Deployment of the Primary Instance

1. Select the **Primary Instance** page in the web browser and complete the missing information (**Utility** and **Inter-Task IP** addresses of the Secondary Instance).
2. They are the same public IP address and can be seen in the screenshot above.
3. Fill in the **Secondary Utility IP** address and **Inter-Task IP** address.
4. Read and confirm that the information entered is correct.
5. Click on the blue **Start Deployment** button.
6. This step takes some time to complete, so wait about three minutes for the Primary Instance deployment to complete.

→ To Continue Deployment of the Secondary Instance

1. The Secondary Platform/Instance screen should be complete.
2. Confirm that the entered **Primary Inter-Task Utility** IP address is correct.
3. Click on the blue **Start Deployment** button.

10. Access the Management GUI

10.1 Standalone Deployments

The same Public IP address can be used for both Management and Utility.

This IP address will also be used to access the GUI.

10.2 HA Deployments

The Public IP address used to deploy the BorderNet SBC in HA mode is the IP address used to populate the Utility IP address fields.

Once the deployment process is complete, the BorderNet SBC can be accessed in HA mode by locating the Public IP address assigned to the **Management** service.

The Public Management IP address was previously determined in step [9.3.2](#) above.

Use **ONLY** this IP address to access the GUI.

END OF DOCUMENT