Installation Manual

AudioCodes Mediant™ Family of Session Border Controllers (SBC)

Mediant Virtual Edition (VE) SBC

Deployment in Amazon AWS

Version 7.4

audiocodes

Table of Contents

List of Figures

Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from https://www.audiocodes.com/library/technical-documents.

This document is subject to change without notice.

Date Published: November-01-2021

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our website at https://www.audiocodes.com/services-support/maintenance-and-support.

Stay in the Loop with AudioCodes

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

Related Documentation

Manual Name
Mediant Software SBC User's Manual
SBC Series Release Notes

Document Revision Record

LTRT	Description
10867	Initial document release for Version 7.4.
10871	Creating private EC2 updated.

LTRT	Description
10874	CloudFormation template download site; instance type c5.9xlarge and c4.8xlarge; new sections for post-installation configuration and troubleshooting of Mediant VE SBC – PAYG product; miscellaneous
10877	Note added to Deploying Standalone Mediant VE via AWS EC2 Console re adding/removing network interfaces or secondary IP addresses.

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our website at https://online.audiocodes.com/documentation-feedback.

1 Introduction

This document describes deployment of AudioCodes' Mediant Virtual Edition (VE) Session Border Controller (SBC), hereafter referred to as *Mediant VE*, in an Amazon Web Services (AWS) environment.

For detailed instructions on Mediant VE installation in other virtual environments (for example, VMware), refer to the *Mediant VE SBC Installation Manual*.

Note:

- The scope of this document does not fully cover security aspects for deploying the product in the AWS cloud. Security measures should be done in accordance with AWS security policies and recommendations.
- For configuring Mediant VE SBC, refer to the *Mediant Software SBC User's Manual*.

This page is intentionally left blank.

2 Deployment Methods

Mediant VE SBC is available in AWS Marketplace as two different products:

- **Mediant VE Session Border Controller (SBC)**: This product includes a trial license (limited to three SBC sessions) and requires a purchase of production license from AudioCodes.
- **Mediant VE Session Border Controller (SBC) – PAYG**: This product includes a pay-as-you-go license that enables Customers to use the SBC as much as needed and pay for the actual service consumed via their AWS account billing.

Mediant VE SBC supports the following deployment topologies:

- **Standalone topology:** Mediant VE SBC is deployed on a single EC2 instance. Deployment is performed using the AWS EC2 console, as described in Section Deploying Standalone Mediant VE via AWS EC2 Console.
- **High-availability (HA) topology:** Mediant VE SBC is deployed on two EC2 instances, operating in 1+1 Active/Standby mode. Deployment is performed using an AWS CloudFormation template, as described in Section Deploying High-Availability (HA) Mediant VE via CloudFormation Service

Notes:

- The **Mediant VE SBC – PAYG** product supports only Standalone deployment topology (not HA).
- All Mediant VE SBC for AWS products and deployment topologies support only IPv4 addresses (not IPv6).

This page is intentionally left blank.

3 Prerequisites

Prior to deploying Mediant VE SBC on Amazon AWS, make sure that you meet the following prerequisites:

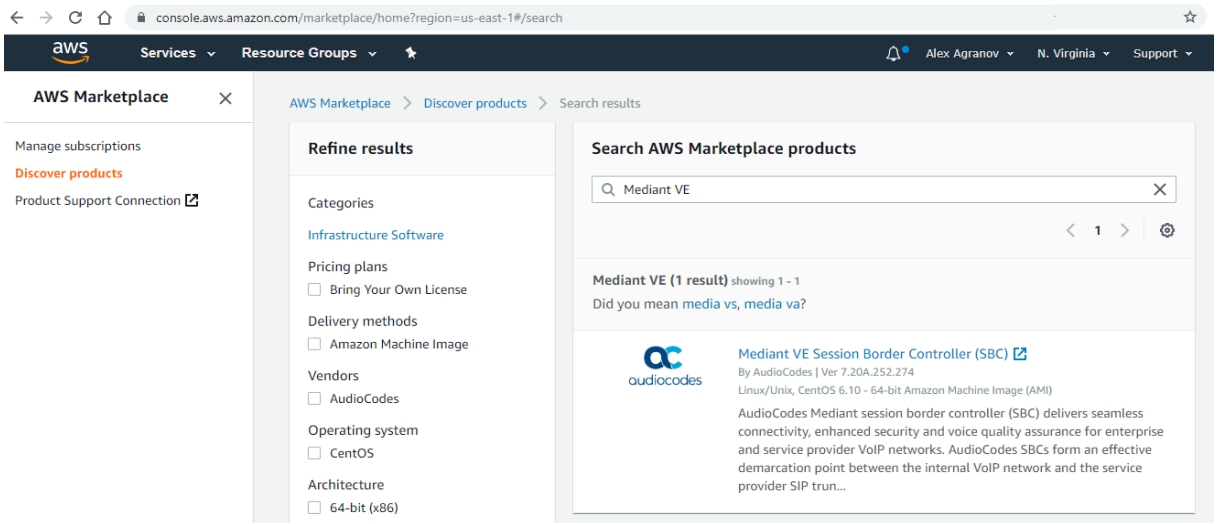
- You have an AWS account. If you don't have an AWS account, you can sign up for one on Amazon's website at http://aws.amazon.com/.
- You have subscribed to the AudioCodes Mediant VE offer in AWS Marketplace. Refer to Section Subscribing to AudioCodes Mediant VE Product in AWS Marketplace for additional information.
- You have created all subnets needed for Mediant VE deployment. Refer to Section Network Prerequisites for additional information.
- **For HA deployment:**
  - If you are going to perform deployment via CloudFormation template, make sure that you have received Mediant VE CloudFormation Template that is distributed as part of *Mediant VE Installation Kit*. Refer to Section CloudFormation Template for Mediant VE HA Deployment for additional information.
  - You have created an Identity and Access Management (IAM) role that enables Mediant VE to manage its network interfaces. Refer to Section IAM Role for Mediant VE HA Deployment for additional information.
  - You have created an HA subnet that is used for internal communication between Mediant VE instances and for accessing the AWS API during the activity switchover. Refer to Section HA Subnet for additional information.

3.1 Subscribing to AudioCodes Mediant VE Product in AWS Marketplace

Prior to deploying the Mediant VE instance, you must subscribe to the AudioCodes Mediant VE product in AWS Marketplace as follows:

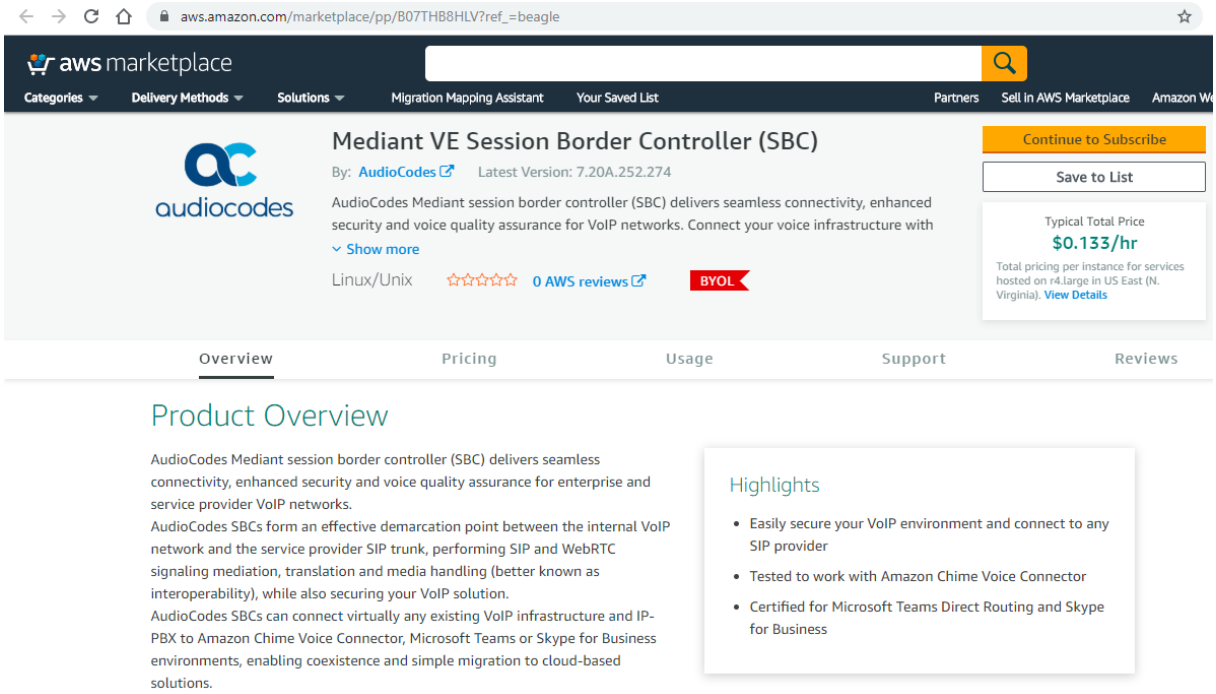
1. Open the AWS Marketplace console at https://console.aws.amazon.com/marketplace.
2. In the **Discover Products** tab, search for the "Mediant VE" product.

Figure 3-1: Searching for Mediant VE Product in the AWS Marketplace



3. Click the **Mediant VE Session Border Controller (SBC)** product.

Figure 3-2: Mediant VE Product in AWS Marketplace



4. Click **Continue to Subscribe** to subscribe to the Mediant VE product.

3.2 CloudFormation Template for Mediant VE HA Deployment

The CloudFormation template for high-availability (HA) Mediant VE deployment is distributed as part of the *Mediant VE Installation Kit*, which can be downloaded from https://services.audiocodes.com/app/answers/detail/a_id/8.

Two CloudFormation templates are included:

- **sbc_ha_cloudformation.txt:** For regular AWS regions
- **sbc_ha_cloudformation_cn.txt:** For AWS China regions, for example, cn-north-1 and cn-northwest-1

3.3 IAM Role for Mediant VE HA Deployment

For HA deployment, the following IAM role must be created prior to deploying the Mediant VE instance. This role ensures that Mediant VE can manage its network interfaces and re-assign IP addresses during a switchover.

Note: IAM Role described below is needed only for HA deployment of Mediant VE, as described in Sections

Deploying High-Availability (HA) Mediant VE via CloudFormation Service and Deploying Mediant VE via Stack Manager. It is not needed for standalone deployment of Mediant VE, as described in Section Deploying Standalone Mediant VE via AWS EC2 Console.

➢ **IAM Role for HA Mediant VE deployment:**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:UnassignPrivateIpAddresses",
                "ec2:AssociateAddress",
                "ec2:DescribeAddresses",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

➢ **To create an IAM Role:**

1. Open the AWS IAM console (https://console.aws.amazon.com/iam).
2. Navigate to the **Policies** screen, and then:
   a. Click **Create**.
   b. Select the **JSON** tab, copy-and-paste the IAM policy rules listed above, and then click **Review policy**.
   c. Enter the IAM policy name (e.g., “SBC_HA”), and then click **Create policy**.
3. Navigate to the **Roles** screen, and then:
   a. Click **Create role**.
   b. Choose **EC2 use case**, and then click **Next: permissions**.
   c. Search for the IAM policy created in the previous step, select it, and then click **Next: tags**.
   d. Click **Next: review**.
   e. Enter the IAM role name (e.g. “SBC_HA”), and then click **Create role**.

3.3.1 IAM Role for Initial Configuration from S3 URL

Mediant VE SBC may be provided with an initial configuration INI file, stored on AWS Simple Storage Service (S3), during its launch. This is done by including the **#s3-url** element in the instance user-data, as described in Automatic Provisioning of Mediant VE-CE SBC via Cloud-Init Configuration Note.

If you use this option, add the following rules to the IAM Role created previously, to enable Mediant VE SBC access to the corresponding S3 bucket (replace “sbc” in the example below with the actual bucket name).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": "arn:aws:s3:::sbc"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::sbc/*"
        }
}
```

3.4 Network Prerequisites

Mediant VE on AWS uses the following subnets:

- **Main Subnet:** Carries management (e.g. HTTP and SSH), signaling (SIP) and media (RTP, RTCP) traffic.
- **Additional Subnets:** Carries signaling (SIP) and media (RTP, RTCP) traffic. These subnets are optional and may be omitted if your network architecture doesn't require them.
- **HA Subnet:** Used for HA deployment only. Carries internal communication between Mediant VE instances. It's also used for accessing the AWS API during the switchover. Refer to Section HA Subnet for detailed instructions on how to correctly create the HA Subnet.

All subnets must reside in the same Availability Zone of the Virtual Private Cloud (VPC) and be created prior to the Mediant VE deployment

Figure 3-2: Network Architecture for Standalone Deployment

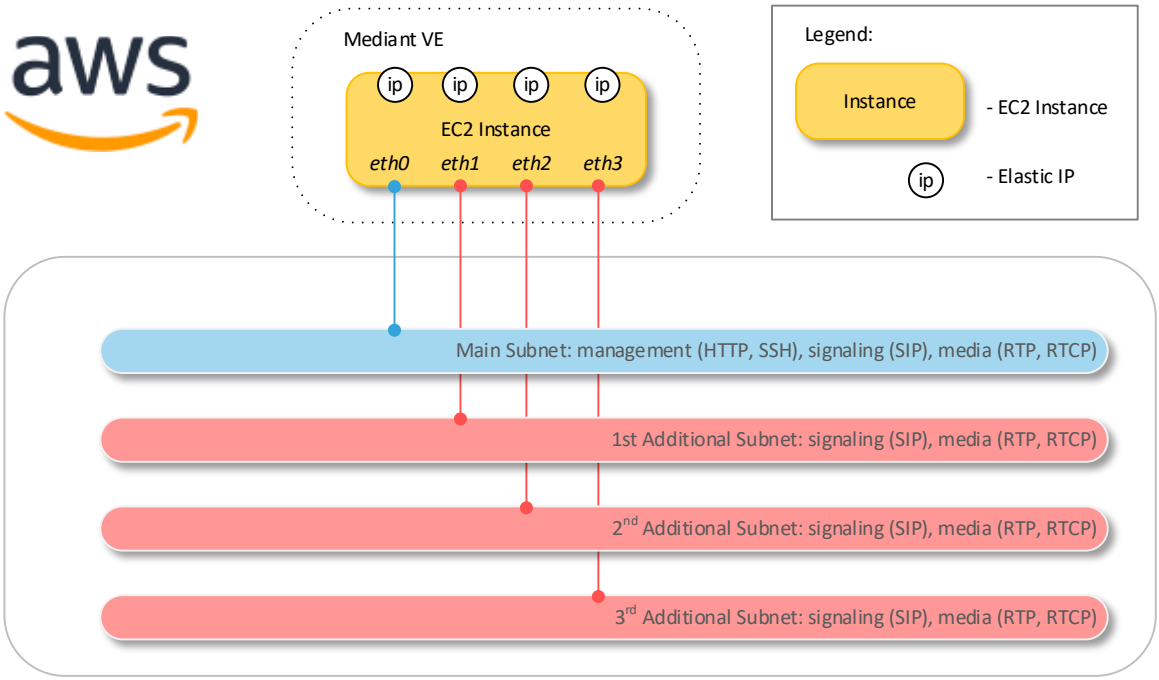
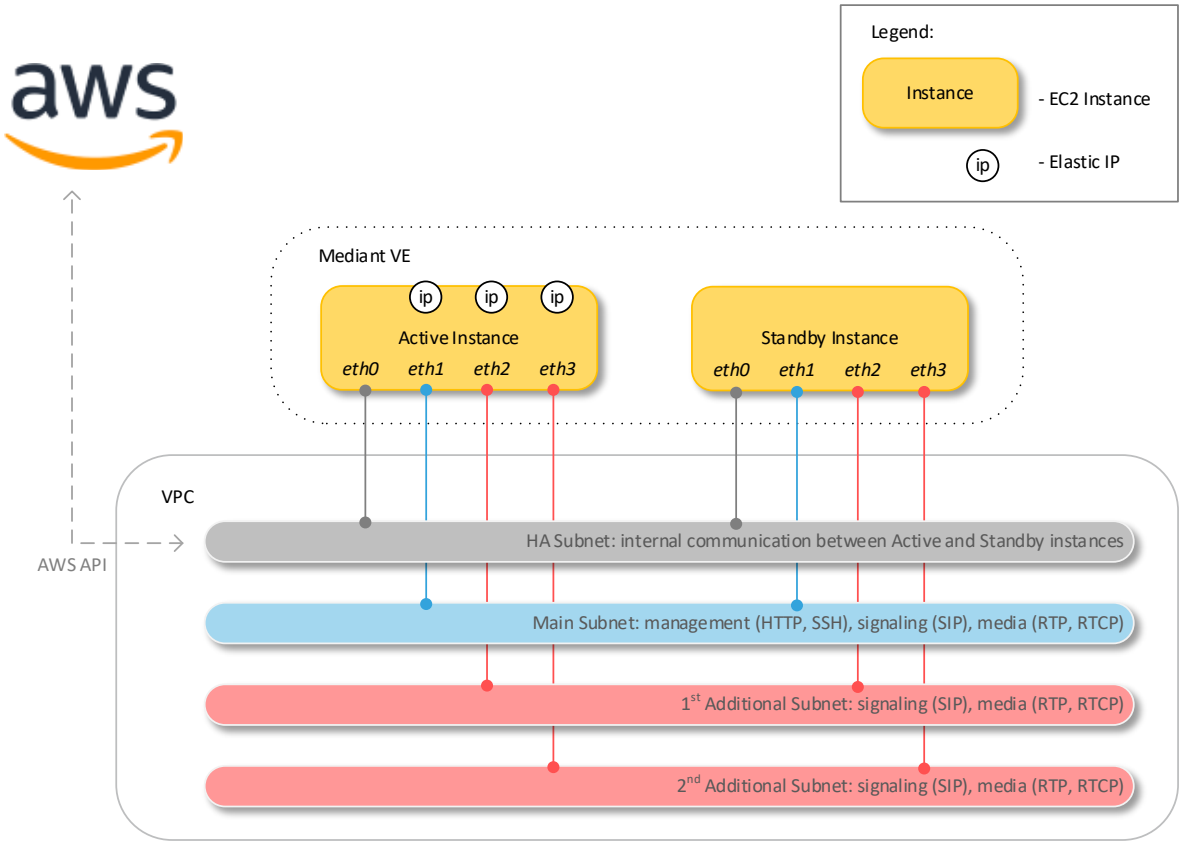


Figure 3-3: Network Architecture for HA Deployment



Mediant VE may communicate with its peers (e.g. IP-PBX or SIP Trunk) via both private and public (Elastic) IP addresses. Use of Elastic IPs is optional and they may be omitted if your network design doesn't require them (i.e., if all communication occurs inside the VPC).

HA deployments operate in 1+1 Active/Standby mode and use "floating" IP addresses, reassigned via the AWS API during activity switchover. Since AWS does not support reassignment of primary IP addresses, Mediant VE never uses them, but uses secondary IP addresses instead (except for the HA subnet).

3.4.1 HA Subnet

The HA subnet is used in high-availability (HA) Mediant VE deployments for the following tasks:

- Internal communication between Mediant VE instances
- Accessing AWS API (for IP address reassignment during activity switchover)

Mediant VE uses private addresses in the HA subnet. Therefore, to enable Mediant VE to access the AWS API via the HA subnet, you must do one of the following:

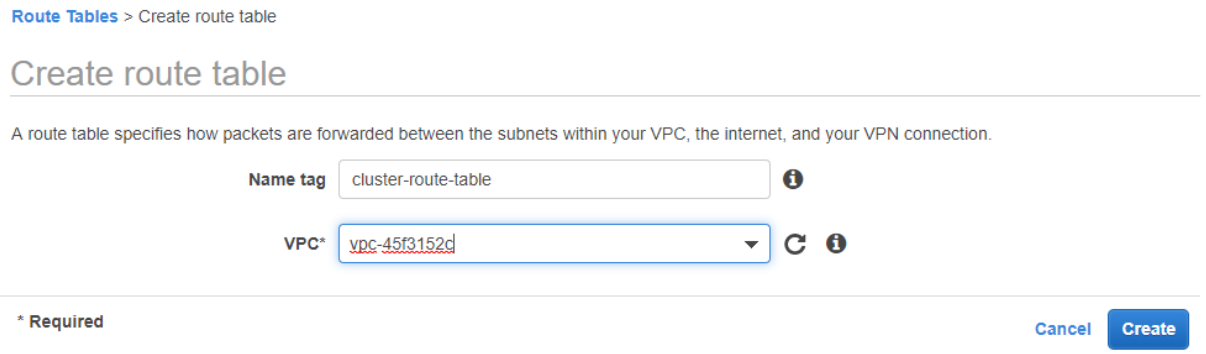
- (Recommended Method) Create a private EC2 endpoint in the HA subnet. This method creates a private AWS API endpoint inside the HA subnet, thereby enabling Mediant VE to access it via the private IP address.
- (Alternative Method) Attach a NAT gateway to the HA subnet. This method uses network address translation (performed by the NAT gateway) to enable access to public AWS API endpoint from Mediant VE SBC's private IP address.

In addition, since the HA subnet carries sensitive information, it is recommended to create a dedicated subnet and protect it from unauthorized access.

➢ **To create the HA subnet:**

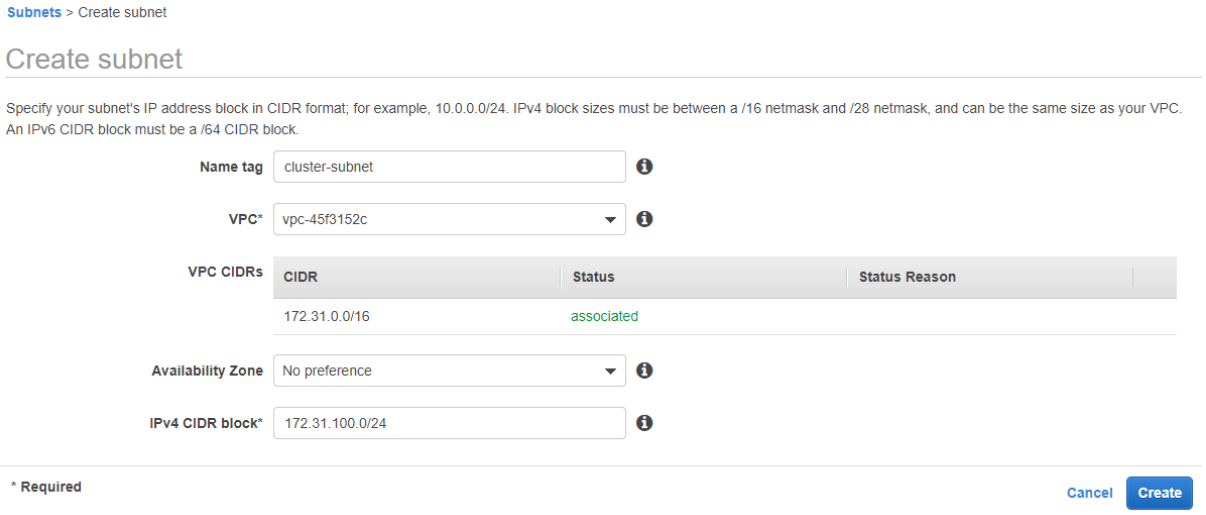
1. Open the AWS VPC management console at https://console.aws.amazon.com/vpc.
2. Open the **Route Tables** page, and then click **Create route table:**
   a. In the 'Name tag' field, enter the new route table name (e.g. 'ha-route-table').
   b. In the 'VPC' drop-down list, select the VPC where Mediant VE will be deployed.
   c. Click **Create** to create the route table.

Figure 3-4: Creating Route Table



3. Open the **Subnets** page, and then click **Create Subnet**.
   a. In the 'Name tag' field, enter the new subnet name (e.g. 'ha-subnet').
   b. From the 'Availability Zone' drop-down list, select the Availability Zone where Mediant VE will be deployed.
   c. In the 'IPv4 CIDR block' field, enter the IPv4 CIDR for the subnet.
   d. Click **Yes, Create** to create the route table.

Figure 3-5: Creating Cluster Subnet

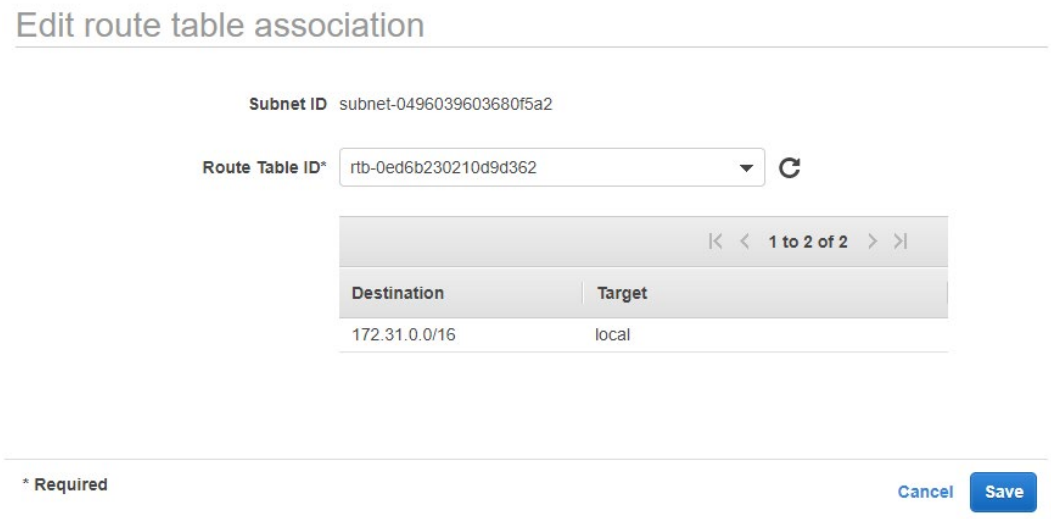


4. Select the created subnet, switch to the **Route Table** tab, and then click **Edit route table association**.

Figure 3-6: Changing Cluster Subnet Route Table

5. Choose the HA route table created in the previous steps, and then click **Save**.

Figure 3-7: Editing Route Table Association



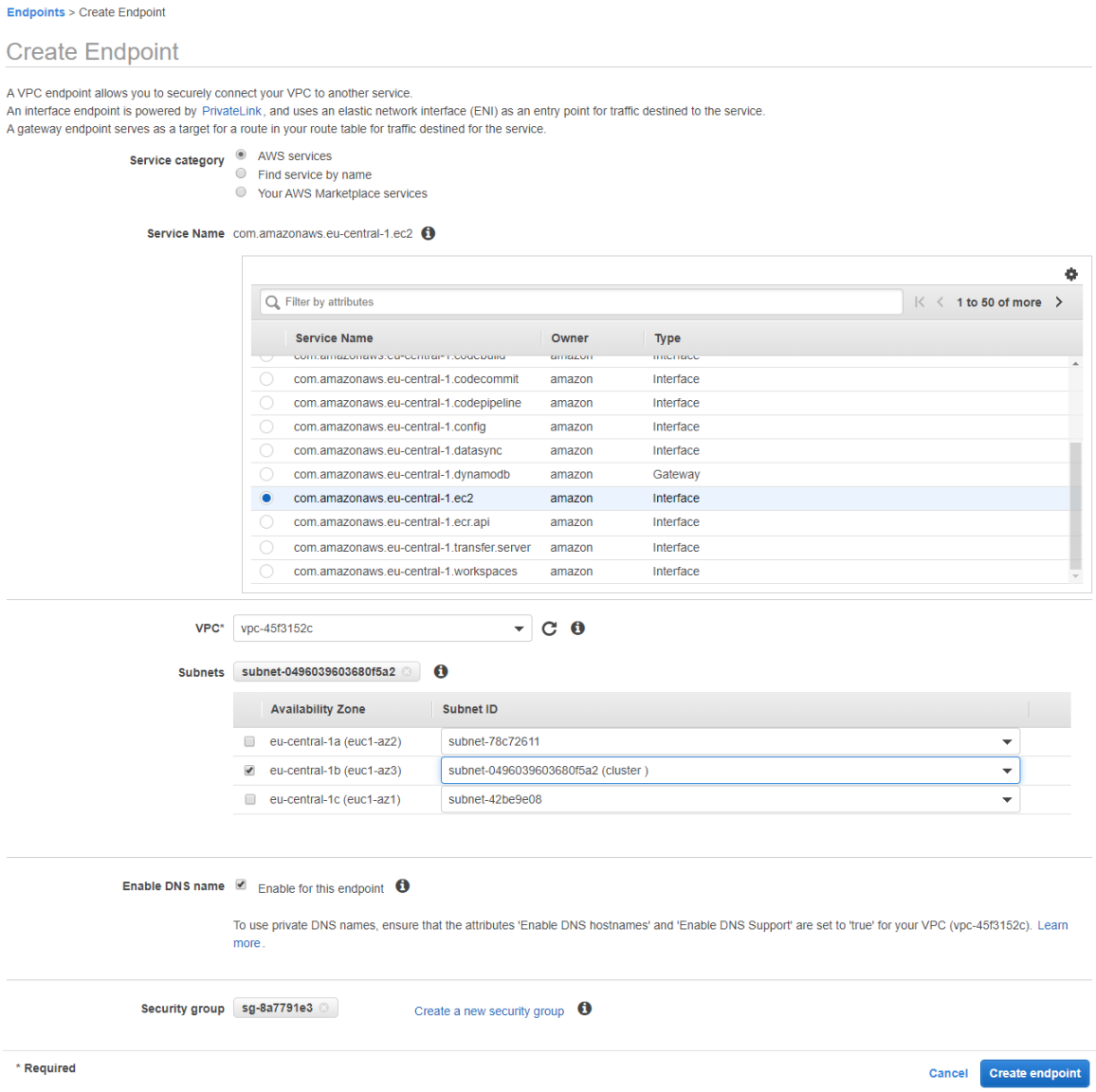
Note: Make sure that the HA subnet has a dedicated route table. Other subnets (i.e., Main subnet and Additional subnets) should be attached to different route table(s), that would typically have the Internet Gateway configured as the default route to ensure proper functionality of Elastic IPs attached to the corresponding network interfaces of EC2 instances .

After you successfully created the HA subnet, you need to enable access to AWS API via it. The recommended method is to create a private EC2 endpoint in the HA subnet.

➢ **To create the private EC2 endpoint in HA subnet:**

1. Open the **Security Groups** page, and then click **Create security group**.
   a. In the 'Security group name' field, enter the security group name (e.g., "Endpoint Security Group").
   b. In the 'VPC' drop-down list, select the VPC where Mediant VE will be deployed.
   c. Under 'Inbound rules', click **Add rule**, and then configure the rule as follows:
      - 'Type': Custom TCP
      - 'Port range': 443
      - 'Source': Anywhere
   d. Click **Create security group** to create the new security group.
2. Open the **Endpoints** page, and then click **Create Endpoint**.
   a. In the 'Service Category' field, select **AWS services**.
   b. In the 'Service Name' field, enter "ec2" in the search box, and then press Enter. Select the EC2 endpoint from the list (e.g., **com.amazonaws.eu-central-1.ec2**).
   c. In the 'VPC' drop-down list, select the VPC where Mediant VE will be deployed.
   d. In the 'Subnets' field, select the HA subnet.
   e. Select the 'Enable DNS name' checkbox.
   f. In the 'Security group' field, remove the default security group and select the 'Endpoint Security Group' that you created in the previous step.
   g. Click **Create Endpoint** to create the new endpoint.

Figure 3-8: Creating Private EC2 Endpoint



An alternative method for enabling access to the AWS API via the HA subnet is by attaching a NAT Gateway to the Cluster subnet.

Note: You don't need to perform the below steps if you created a private EC2 endpoint, as described above.

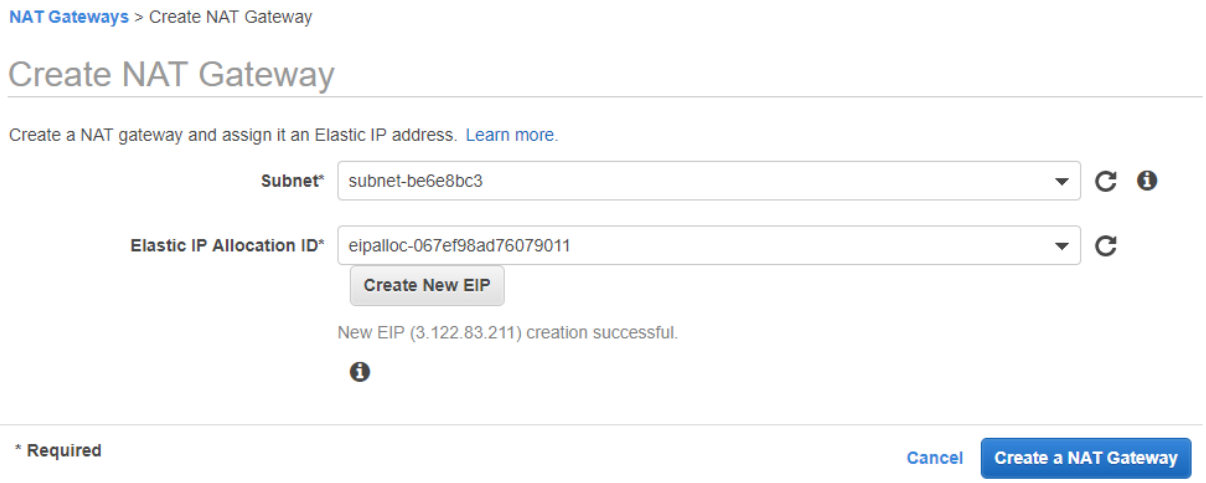
➢ To create NAT Gateway and attach it to the HA subnet:

1. Open the **NAT Gateways** page, and then click **Create NAT Gateway**:
   a. From the 'Subnet' drop-down list, select a subnet that belongs to the same Availability Zone where the HA subnet was created (and where Mediant VE will be deployed) and that has an Internet Gateway attached to it. For example, select **Main Subnet**.

Note: Do not select **HA Subnet** at this stage. The NAT Gateway itself will be configured as a default route in the HA Subnet and therefore, it won't be able to access the Internet from it.

   b. From the 'Elastic IP Allocation ID' drop-down list, select an existing Elastic IP if you have pre-allocated Elastic IPs in your VPC, or click **Create New EIP** to create a new one.
   c. Click **Create a NAT Gateway** to create the NAT gateway.

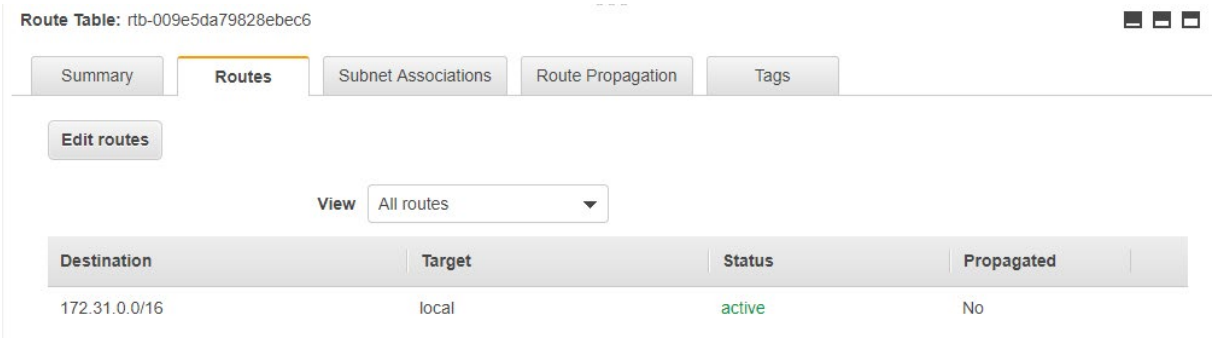
Figure 3-9: Creating NAT Gateway



2. Open the **Route Tables** page, and then select the HA route table created in the previous steps.

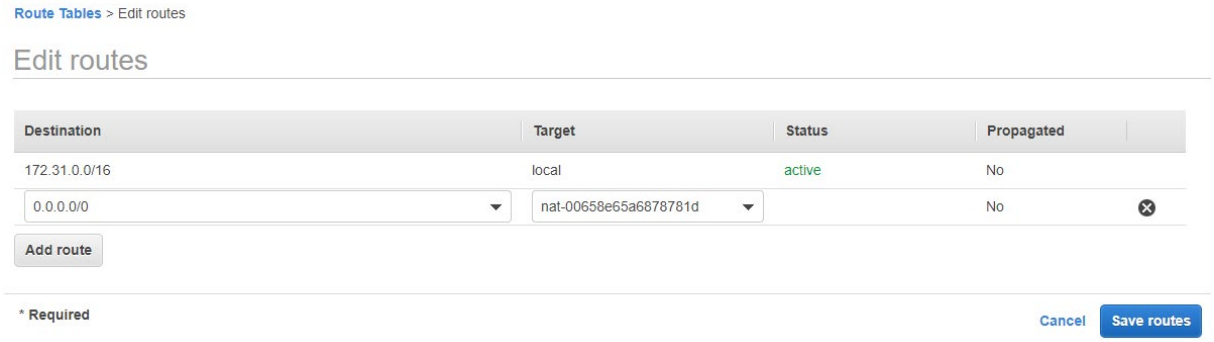
3. Switch to the **Routes** tab, and then click **Edit routes** to edit the routes.

Figure 3-10: Editing Route Table



4. Create the default route entry (0.0.0.0/0) that points to the created NAT gateway, and then click **Save** to save your changes.

Figure 3-11: Creating Default Route



3.5 Instance Type

The following instance types are recommended for Mediant VE SBC deployment:

- For versions from 7.20CO or 7.40A streams based on OS Version 8:
  - **m5.large:** This instance type is recommended for deployments that don't require transcoding and/or other DSP capabilities.
  - **c5.2xlarge** or **c5.9xlarge:** These instance types are recommended for deployments that require transcoding and/or other DSP capabilities.
- For versions from 7.20A stream based on OS Version 6:
  - **r4.large:** This instance type is recommended for deployments that don't require transcoding and/or other DSP capabilities.
  - **c4.2xlarge** or **c4.8xlarge:** These instance types are recommended for deployments that require transcoding and/or other DSP capabilities.

Refer to the SBC Series Release Notes for a complete list of instance types supported by Mediant VE SBC, their capacities and capabilities.

3.6 Automatic Configuration

Mediant VE SBC supports automatic configuration through the **cloud-init** mechanism. For more information, refer to the *Automatic Provisioning of Mediant VE SBC via Cloud-Init Configuration Note*.

4 Deploying Standalone Mediant VE via AWS EC2 Console

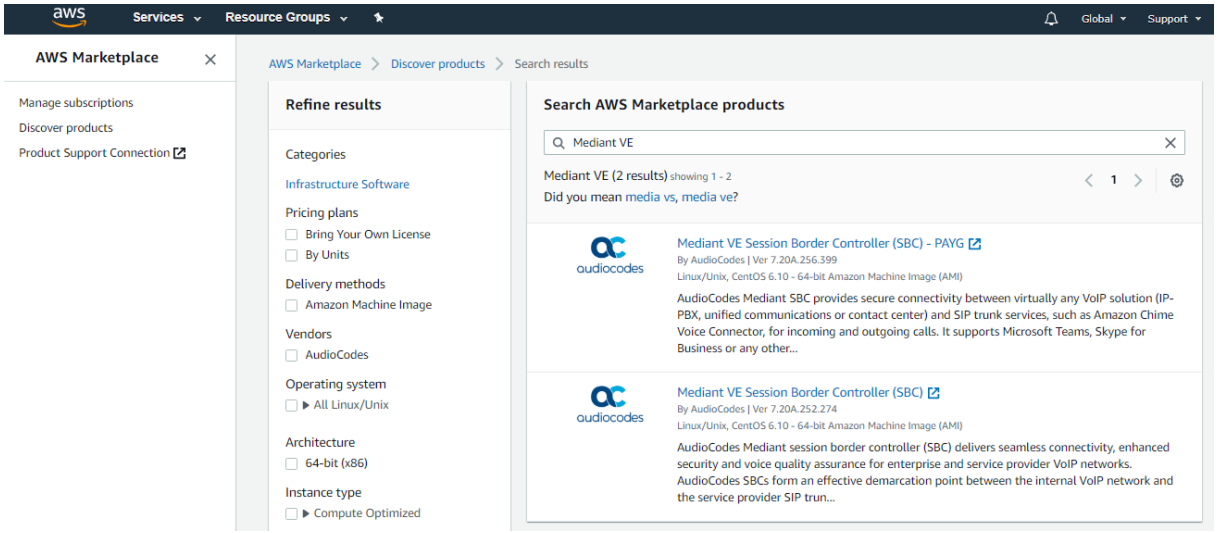
This section describes deployment for a standalone Mediant VE SBC via the AWS EC2 console.

Note: This deployment method is applicable only to standalone (i.e., non-HA) deployments.

➢ **To deploy the standalone Mediant VE SBC instance:**

1. Open the AWS Marketplace console at https://console.aws.amazon.com/marketplace.
2. In the **Discover Products** tab, search for the "Mediant VE" product.

Figure 4-1: Searching for Mediant VE Product in the AWS Marketplace

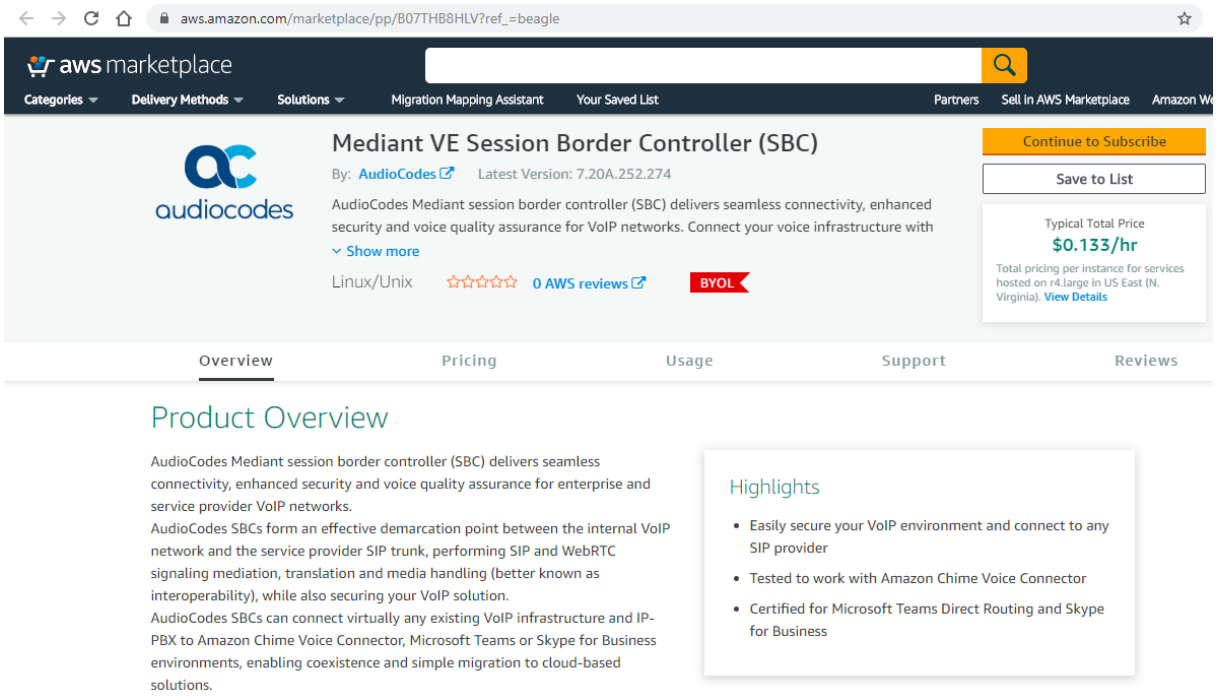


Two products are displayed:

- "Mediant VE Session Border Controller (SBC)": This product includes a trial license (limited to three SBC sessions) and requires a purchase of production license from AudioCodes.
- "Mediant VE Session Border Controller (SBC) – PAYG": This product includes a pay-as-you-go license that enables Customers to use the SBC as much as needed and pay for the actual service consumed via their AWS account billing.

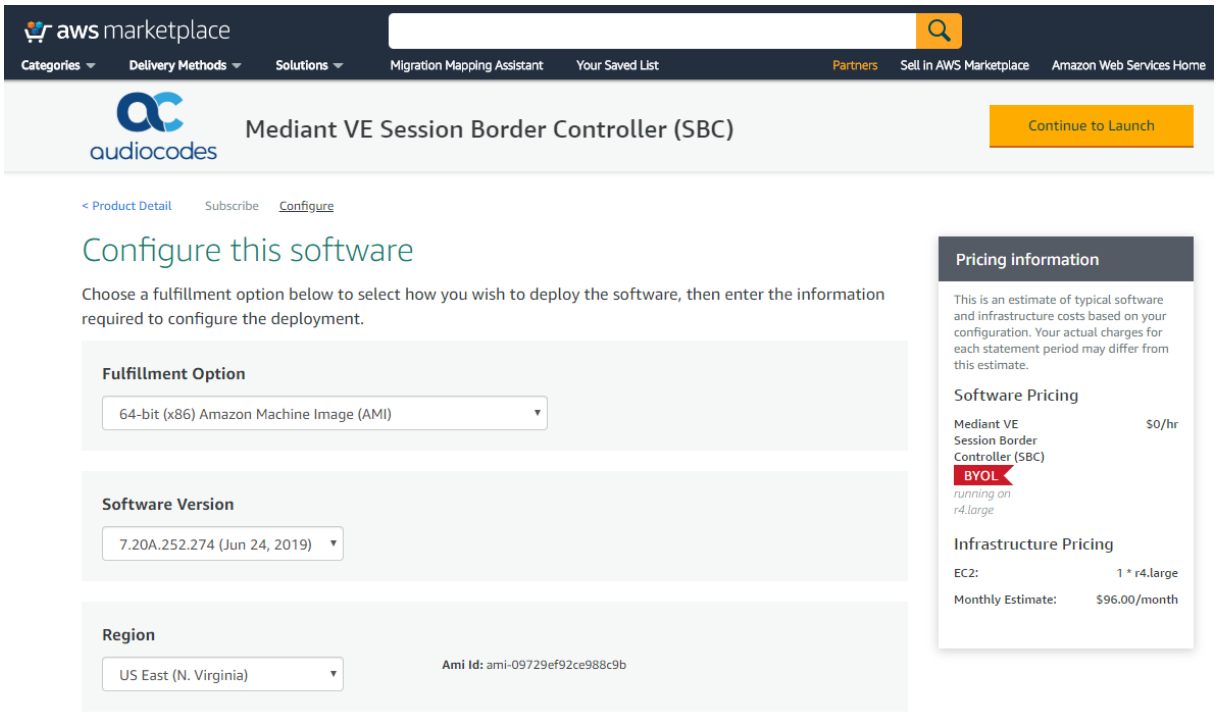
3. Choose the Mediant VE product that matches your licensing needs. For example, choose **Mediant VE Session Border Controller (SBC)** product.

Figure 4-2: Mediant VE Product Page in AWS Marketplace



4. Click **Continue to Subscribe** to subscribe to the Mediant VE SBC product.
5. Click **Continue to Configuration** to proceed with SBC deployment.

Figure 4-3: Mediant VE Configuration Page in AWS Marketplace

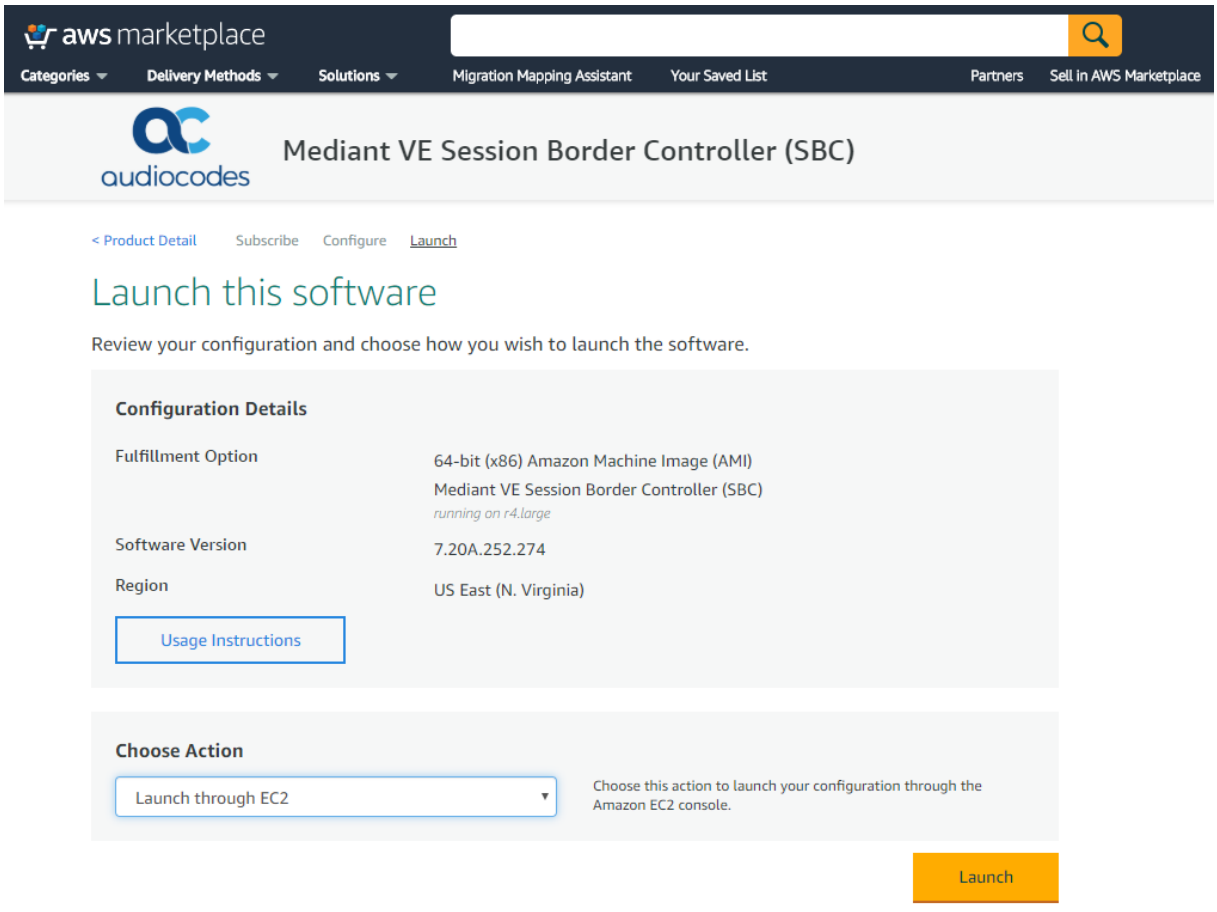


6. Choose the software version that you want to deploy:
   - 7.20A stream is based on OS Version 6.
   - 7.20CO and 7.40A streams are based on OS Version 8 and provide significantly better performance and capacity (refer to the *SBC-Gateway Series Release Notes* for details).
7. Choose the Region where you want to launch the SBC.

Note: For the **Mediant VE SBC – PAYG** product, support is currently provided for installations in US regions only. For support in other regions, please contact us at https://online.audiocodes.com/aws-support-cloud.

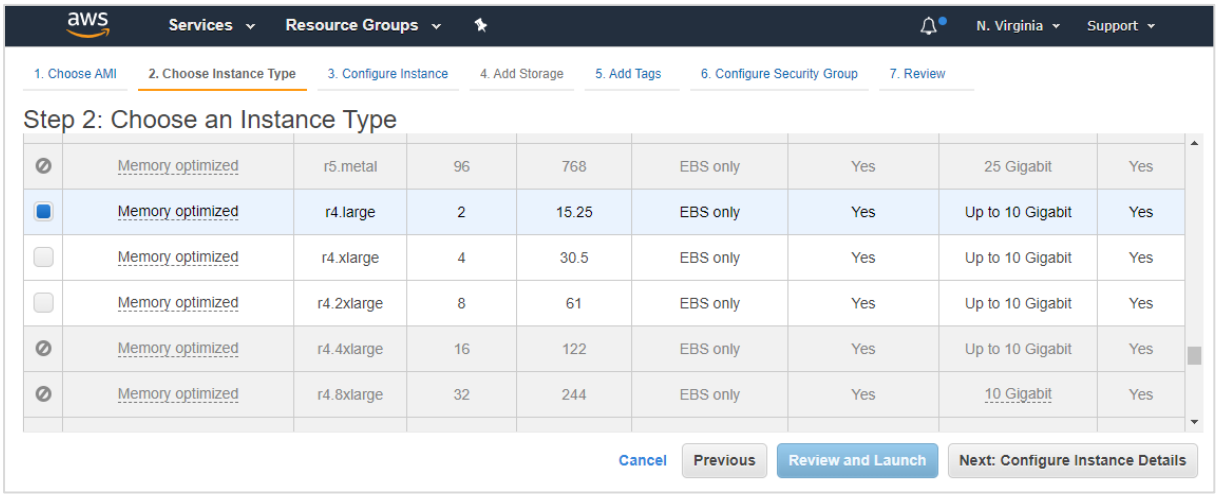
8. Click **Continue to Launch.**

Figure 4-4: Mediant VE Launch Page in AWS Marketplace



9. From the 'Choose Action' drop-down list, select **Launch through EC2**, and then click **Launch**; the Choose Instance Type page appears:

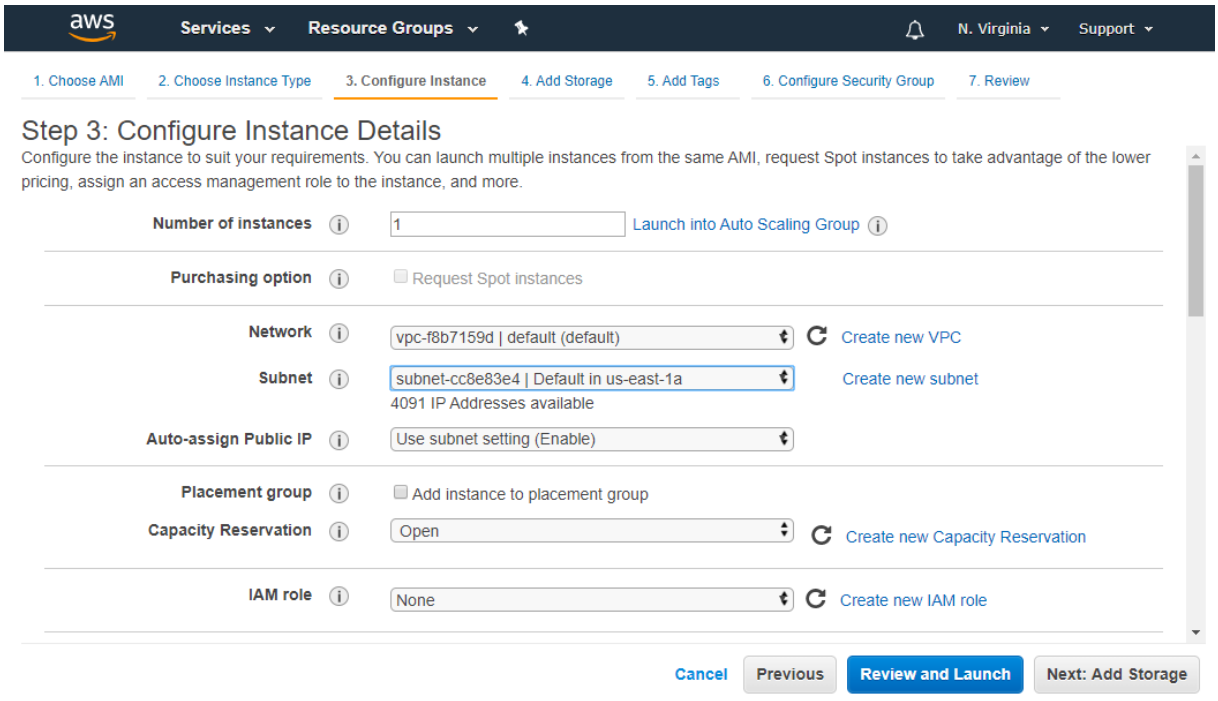
Figure 4-5: Choose Instance Type Page



10. Choose the instance type as follows:
    - If your deployment does not require transcoding and/or other DSP capabilities, choose the **m5.large** instance type for 7.20CO or 7.40A software version or **r4.large** instance type for 7.20A software version.
    - If your deployment requires transcoding and/or other DSP capabilities, choose the **c5.2xlarge / c5.9xlarge** instance type for 7.20CO or 7.40A software version or **c4.2xlarge / c4.8xlarge** instance type for 7.20A software version.

    Refer to the SBC Series Release Notes for a complete list of instance types supported by Mediant VE SBC, their capacities and capabilities.
11. Click **Next**; the Configure Instance page appears:

Figure 4-6: Configure Instance Page



12. Configure network devices and IP addresses:
    - For **Network**, select the VPC where SBC should be deployed.
    - For **Subnet**, select the LAN Subnet. This subnet is used to communicate with the Enterprise IP-PBX and for accessing the SBC management interface (Web or CLI).

- For **IAM role**:
  - If you are deploying the **Mediant VE SBC – PAYG** product, select Automatically create an IAM role with the required permission and the name below, and then enter the IAM role name (e.g., "metering-role").
  - If you are deploying the **Mediant VE SBC** product, leave IAM role empty.

Note: The **Mediant VE SBC – PAYG** product requires an IAM role with the following policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
        "Action": [
                aws-marketplace:MeterUsage
        ],
        "Effect": "Allow",
        "Resource": "*"
        }
     ]
}
```

This role allows Mediant VE SBC PAYG instance to communicate with the AWS Metering API and must be assigned to the launched instance – either automatically (as described above) or manually.

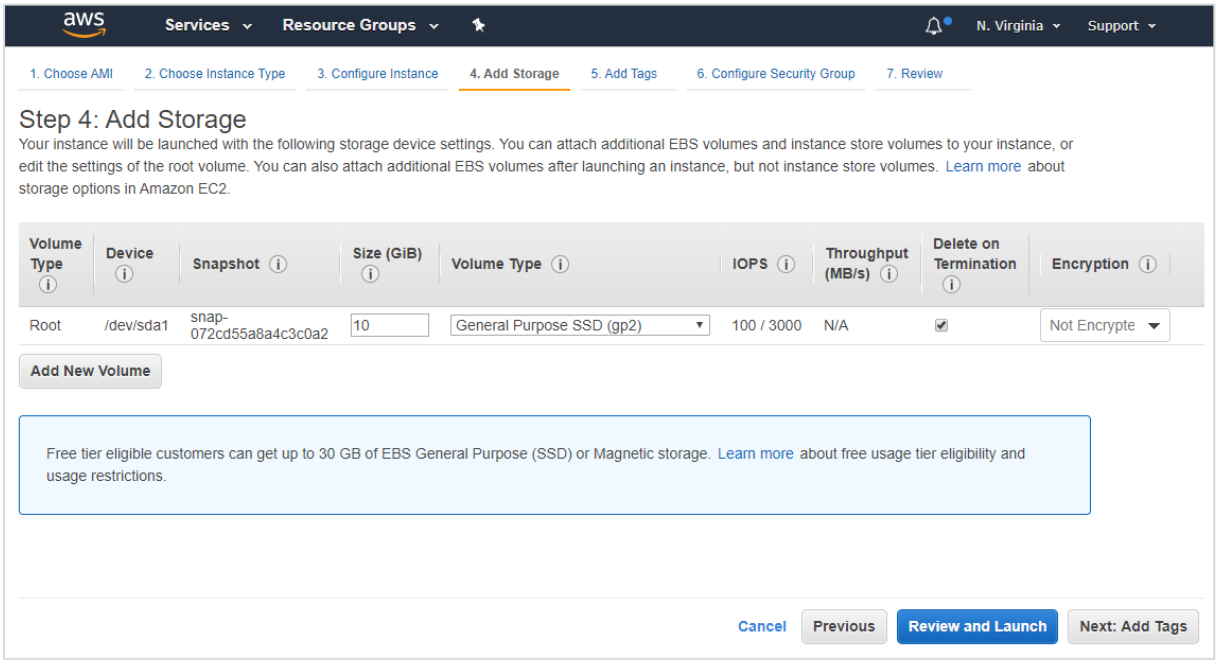
- If you want the deployed instance to have multiple network interfaces, in the **Network Interfaces** section located at the bottom of the page, click **Add Device**, and then select the subnet for the added device (**eth1**).
- If you want the deployed instance to have multiple IP addresses on the same network interface, in the **Network Interfaces** section located at the bottom of the page, click **Add IP**.

Notes:

- If your instance has only one network interface, AWS EC2 may automatically assign a public IP address to the instance. The exact behavior depends on the VPC and/or Subnet configuration. This address however changes if you stop/start the instance and therefore is typically not useful for production environment.
- If you configure multiple network interfaces, AWS EC2 does not automatically assign public IP addresses for the instance.
- To make the Mediant VE SBC instance properly reachable from the Internet, you should assign Elastic IP addresses to it, as described in Section Assigning Elastic IP Addresses to the Instance.
- AWS EC2 Web console supports the configuration of up to two network devices during instance launch. To overcome this limitation and define additional network devices during initial instance launch, consider using AWS EC2 CLI or AWS CloudFormation instead.
- If you need to add/remove network interfaces and/or secondary IP addresses after the initial instance deployment, do this through AWS EC2 management interfaces (i.e., AWS EC2 Web console or AWS EC2 CLI). Mediant VE SBC software automatically detects these changes and updates its networking configuration accordingly.

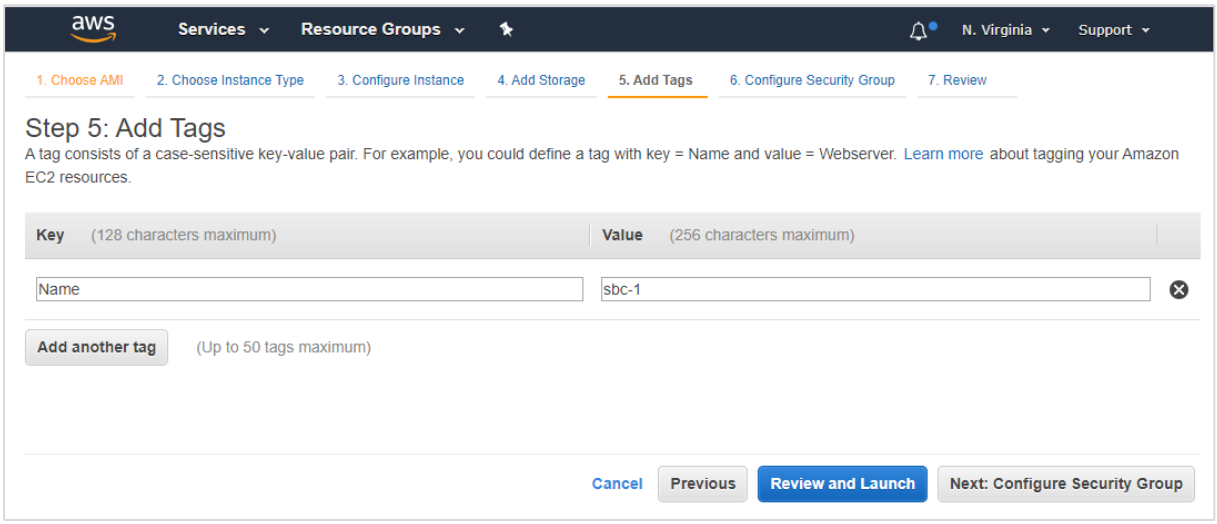
13. Click **Next**; the Add Storage page appears:

Figure 4-7: Add Storage Page



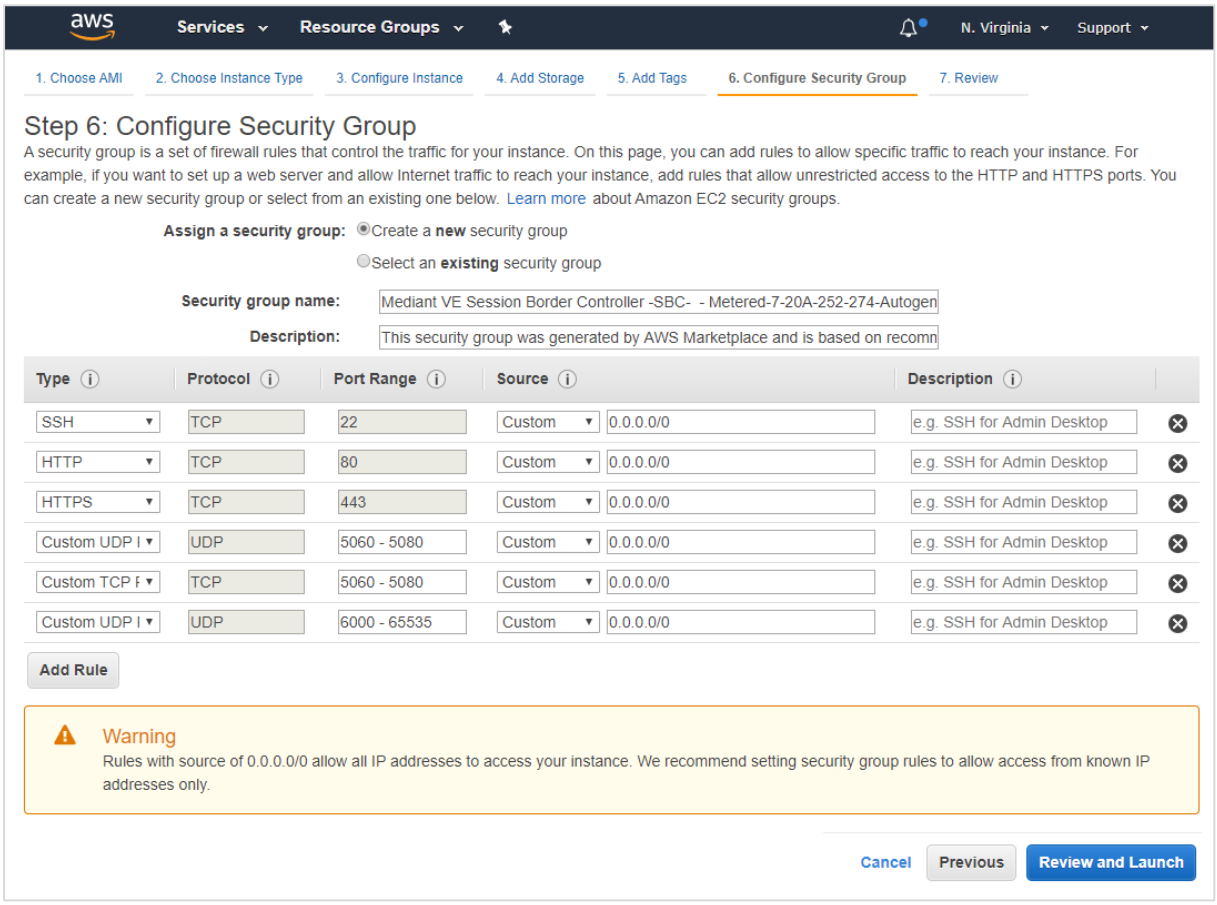
14. From the 'Volume Type' drop-down list, select the required volume of the instance. This setting does not affect SBC performance and may be set to any value.
15. Click **Next**; the Tag Instance page appears:

Figure 4-8: Tag Instance Page



16. In the 'Value' field, enter a name for your instance, and then click **Next**; the Configure Security Group page appears:

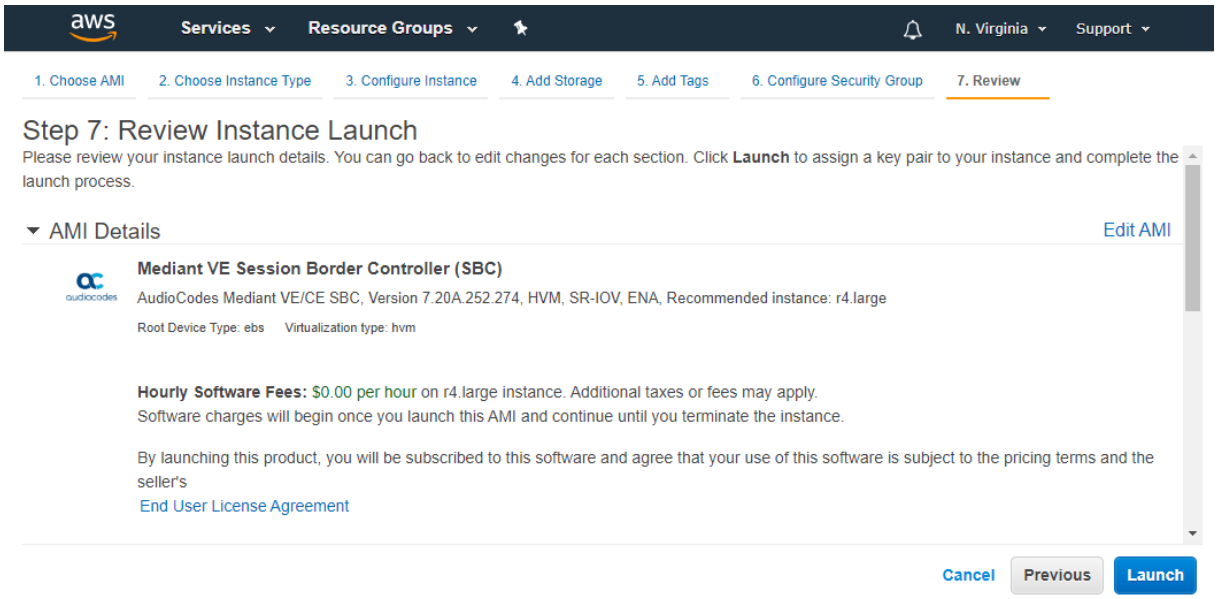
Figure 4-9: Configure Security Group Page



17. Configure firewall rules to allow management (SSH, HTTP, and HTTPS), signaling (SIP) and media (RTP/RTCP) traffic with your instance. Use default rules as a starting point and modify them to match your actual deployment needs.

18. Click **Review and Launch**; the Review page appears displaying a summary of your instance configuration:

Figure 4-10: Review Page



19. Click **Launch**; the Select an existing key pair window appears.
20. Select a key pair to authenticate SSH connection with the SBC instance, click the **I acknowledge** check box, and then click **Launch Instances**.
21. Wait until the new Mediant VE instance is deployed and fully starts (it may take up to 5 minutes). Navigate to the **Instances** page and check the *instance-id* of the deployed instance.
22. Proceed to the next step to assign Elastic IPs to the launched SBC instance.
23. Once you're finished with networking configuration, log in to the deployed instance using the following default credentials:
    - Username: **Admin**
    - Password: ***instance-id***

4.1 Assigning Elastic IP Addresses to the Instance

The AWS EC2 environment assigns "private" IP addresses to the instances running in it. These addresses may be used for communication between the instances running inside the same network (VPC); however, they may not be used to connect to the instance over the Internet.

If the instance has only one network device, AWS EC2 may automatically assign a public IP address to it. The exact behavior depends on the VPC and/or Subnet configuration. This address however is taken from a "shared pool" and changes if you stop/start the instance. Therefore, it is not very useful for production environment.

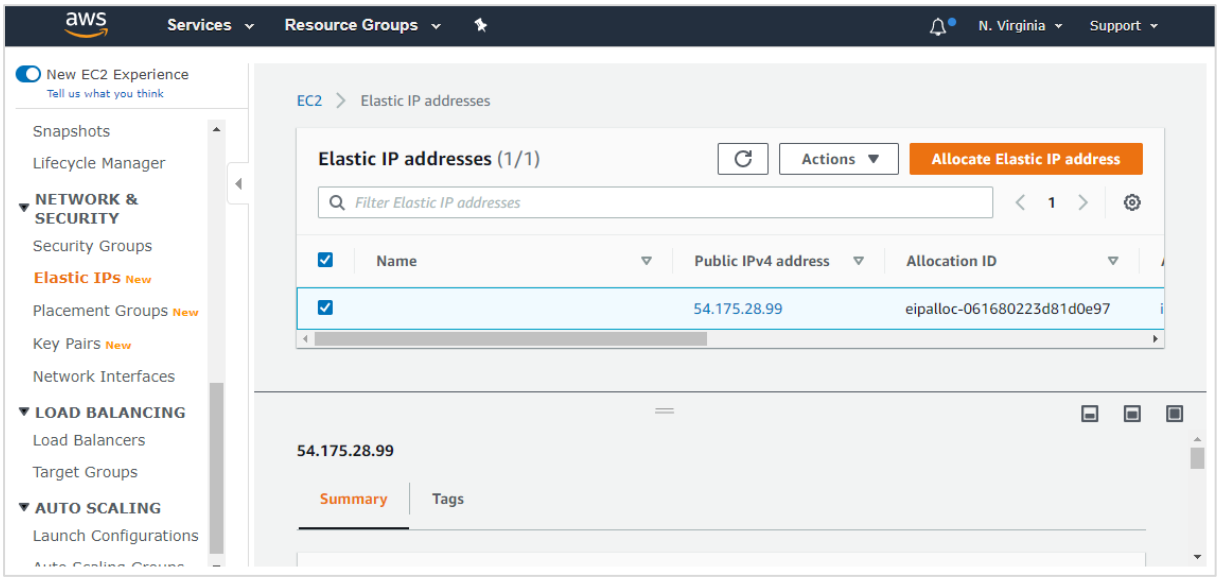
To make SBC properly reachable over the internet, you must allocate Elastic IP addresses and assign them to your instance. Multiple Elastic IP addresses may be assigned to the same AWS EC2 instance, depending on the number of configured private IP addresses.

When an Elastic IP address is associated with the specific instance's private IP address, AWS EC2 environment performs NAT translation by converting elastic IP address to the private IP address, while preserving the port range. If the SBC needs to communicate with a SIP entity using the Elastic IP address, the latter must be configured in the NAT Translation table to ensure proper modification of SIP / SDP messages for NAT traversal.

➢ **To allocate Elastic IP address to SBC instance:**

1. Open the EC2 console at https://console.aws.amazon.com/ec2.
2. Navigate to the **Elastic IPs** page under NETWORK & SECURITY:

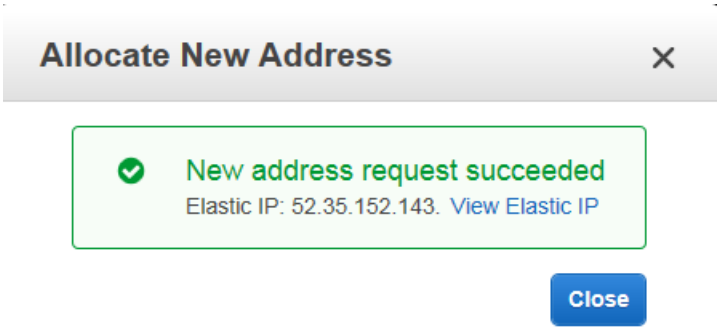
Figure 4-11: Elastic IPs Page



3. Click **Allocate New Address**; a message box appears requesting you to confirm.

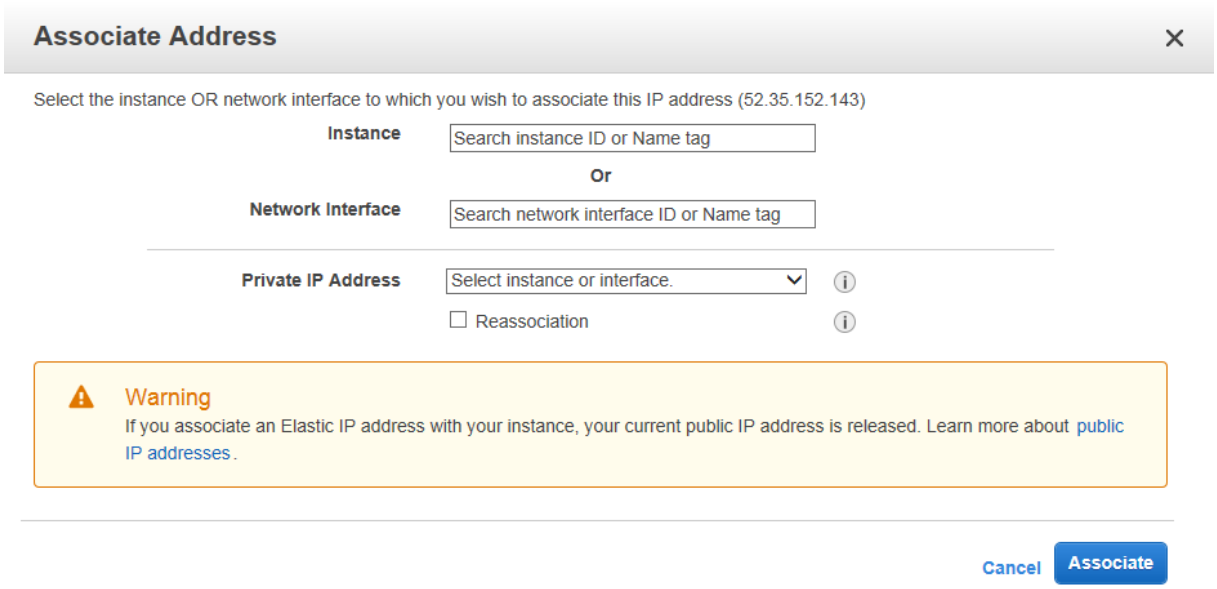
4. Click **Yes, Allocate** to confirm; a message box appears displaying the allocated IP address:

Figure 4-12: Allocated IP Address



5. Click **Close** to close the message box.
6. From the Actions drop-down list, select **Associate Address**.

Figure 4-13: Associate Address Window



7. Select the instance or network interface and private IP address to which you want to associate the Elastic IP address, and then click **Associate**.
8. If you have configured multiple IP addresses and want to make them reachable over the Internet as well, repeat the procedure for additional IP addresses.

4.2 Post-Installation Configuration of Mediant VE SBC – PAYG Product

The "Mediant VE SBC – PAYG" product includes a pay-as-you-go (PAYG) license that requires a persistent connection between the SBC and the AWS Metering API. This connection is performed using public IP addresses. Therefore, you must assign an Elastic IP address to one of the Mediant VE SBC's network interfaces, as described in the previous section. You must also configure the Mediant VE SBC to use this interface, as described below.

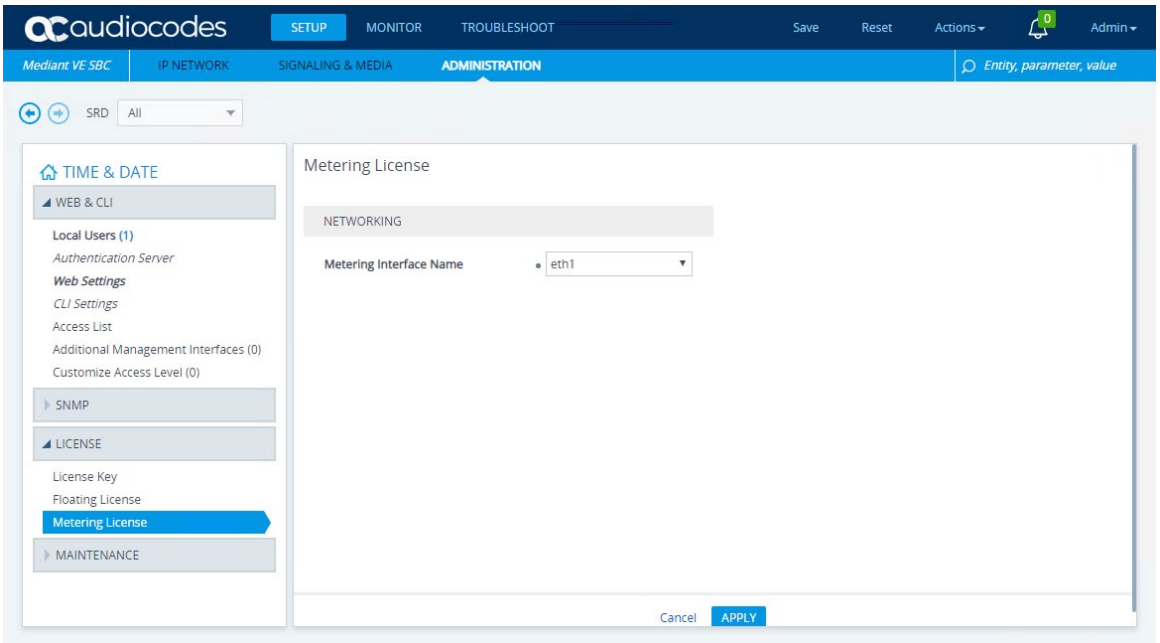
Notes:

- This section is applicable only to the "Mediant VE SBC – PAYG" product that uses the pay-as-you-go (PAYG) license.
- The following procedure is extremely important, as without it the SBC will be unable to communicate with the AWS Metering API and will **seize** its service.

➢ **To perform post-installation configuration of Mediant VE SBC – PAYG product:**

1. Open the SBC Web interface.
2. Log in using default credentials:
   - Username: **Admin**
   - Password: ***instance-id***
3. Navigate to the Metering License page (**ADMINISTRATION** > **LICENSE** > **Metering License**).

Figure 4-14: Metering License Page



4. From the 'Metering Interface Name' drop-down list, select the network interface that has an Elastic IP address attached. This network interface will be used to communicate with the AWS Metering API.
5. Click **Apply** to apply your settings.
6. On the toolbar, click **Save** to save your settings.

4.2.1 Troubleshooting Mediant VE SBC – PAYG Deployment

Mediant VE SBC – PAYG deployment requires persistent connection between the SBC and AWS Metering API. If this connection is unavailable, SBC seizes its operation and raises the "No connection to Metering API" alarm.

SBC contacts the AWS Metering API after the call is completed. Therefore, you will not be able to detect if there is a problem until you have perform a few calls.

Typical reasons that may prevent proper connection between the SBC and the AWS Metering API include the following:

- No "metering" IAM role (with `aws-marketplace:MeterUsage` action) assigned to the SBC instance.
- No Elastic IP address on the network interface used for communication with the AWS Metering API (**ADMINISTRATION** > **LICENSE** > **Metering License**).
- A Network Security Group or some other firewall device is blocking communication between the SBC and the AWS Metering API endpoint (https://metering.marketplace.<region>.amazonaws.com).
- Incorrect UTC time configured on the SBC (**ADMINISTRATION** > **TIME & DATE**).

While troubleshooting, it may be useful to enable the detailed metering logs, by connecting to the SBC's CLI interface and issuing the following commands:

```
enable
    <password> (default: Admin)
debug cloud-license toggle-cl-debug
```

Collect the logged messages via one of the following means:

- Web interface's **TROUBLESHOOT** > **MESSAGE LOG** page
- CLI interface's `debug log` command
- Syslog Viewer utility available at https://tools.audiocodes.com/install/

You may need to wait up to 15 minutes for the metering logs to accumulate after enabling them.

5 Deploying High-Availability (HA) Mediant VE via CloudFormation Service

This section describes deployment of high-availability (HA) Mediant VE that includes two EC2 instances, operating in 1+1 Active/Standby mode. The deployment is performed via the CloudFormation service. The corresponding CloudFormation template is included in the *Mediant VE Installation Kit,* which can be downloaded from https://services.audiocodes.com/app/answers/detail/a_id/8.

Note:

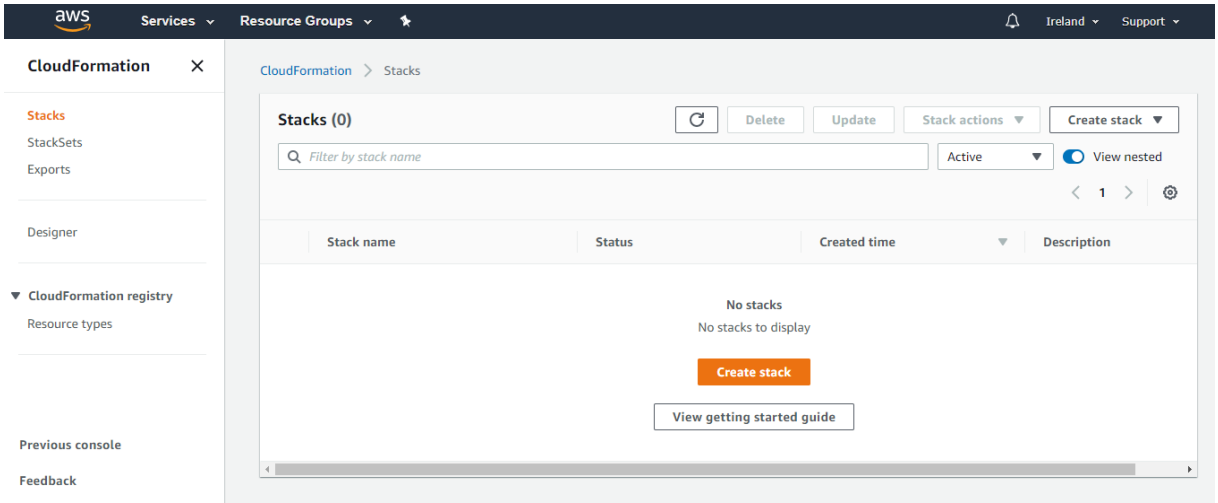
- This deployment method is applicable only to HA (i.e. not standalone) deployments.
- HA deployment is supported only by the **Mediant VE SBC** product (and not by the **Mediant VE SBC – PAYG** product).

The CloudFormation template provided by AudioCodes has certain limitations. For example, it attaches the Elastic IP to the management interface of the deployed Mediant VE instance, but not to the additional interfaces (if used). Customers should use the provided CloudFormation as a reference and modify it to match their deployment needs.

➢ **To deploy high-availability (HA) Mediant VE via AWS CloudFormation service:**

1. Open the CloudFormation console at https://console.aws.amazon.com/cloudformation

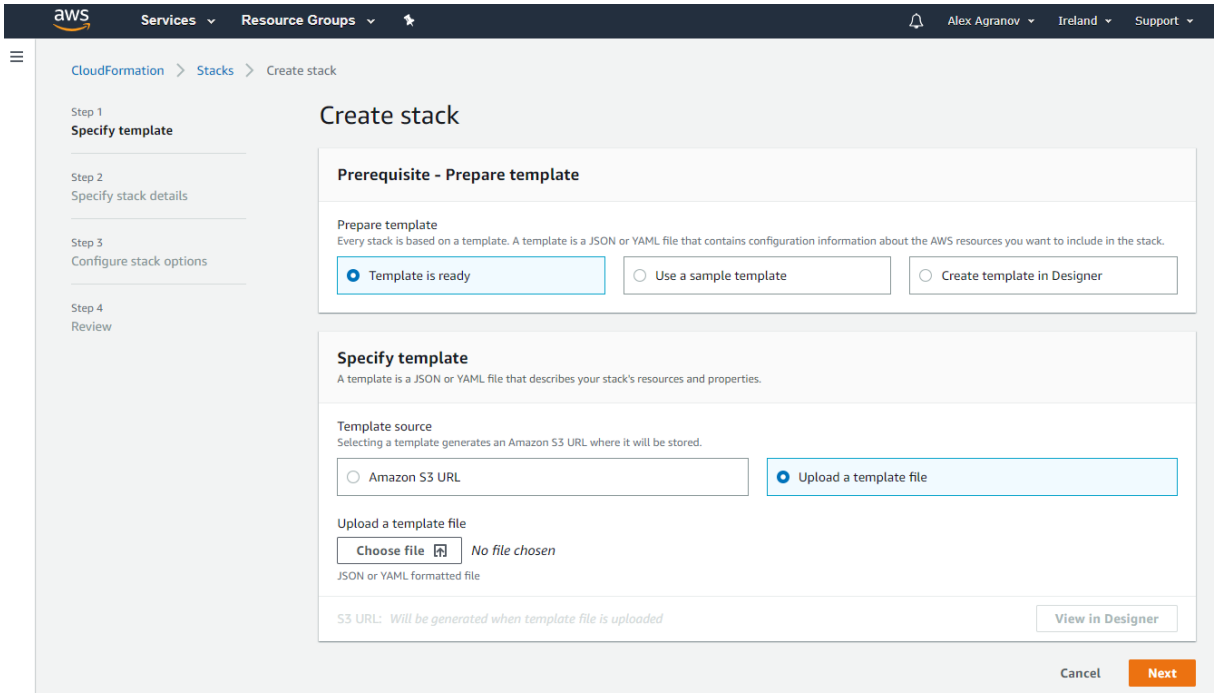
Figure 5-1: CloudFormation Console



2. Select the Region (in the upper right corner) in which to perform the deployment.

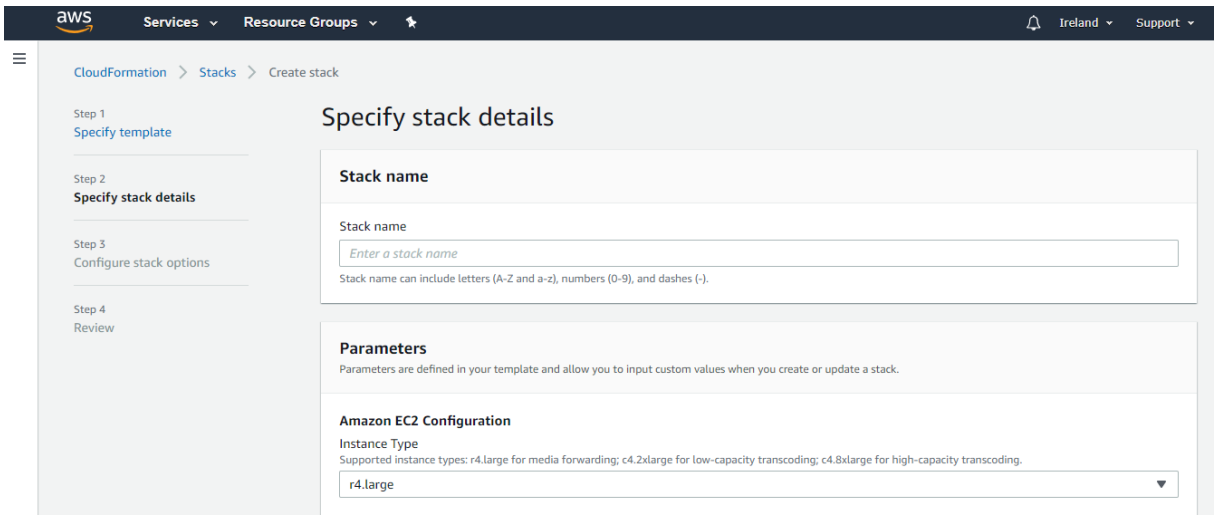
3. Click **Create Stack** to create a new stack, and then select **With new resources (standard)** from the drop-down menu**;** the Create Stack page appears:

Figure 5-2: CloudFormation – Create Stack Page



4. Under the **Specify template** group, select the **Upload a template file**, click **Choose File**, and then select the *Mediant VE HA CloudFormation template* file provided by AudioCodes.
5. Click **Next**; the Specify Stack Details page appears with the fields populated with parameter settings from the template file that you loaded in the previous step:

Figure 5-3: CloudFormation - Specify Details Page (Stack Name)



6. In the **Stack Name** field, type in a meaningful stack name. The stack name is an identifier that helps you find a particular stack from a list of stacks. A stack name can contain only alphanumeric characters (case-sensitive) and hyphens. It must start with an alphabetic character and can't be longer than 128 characters.

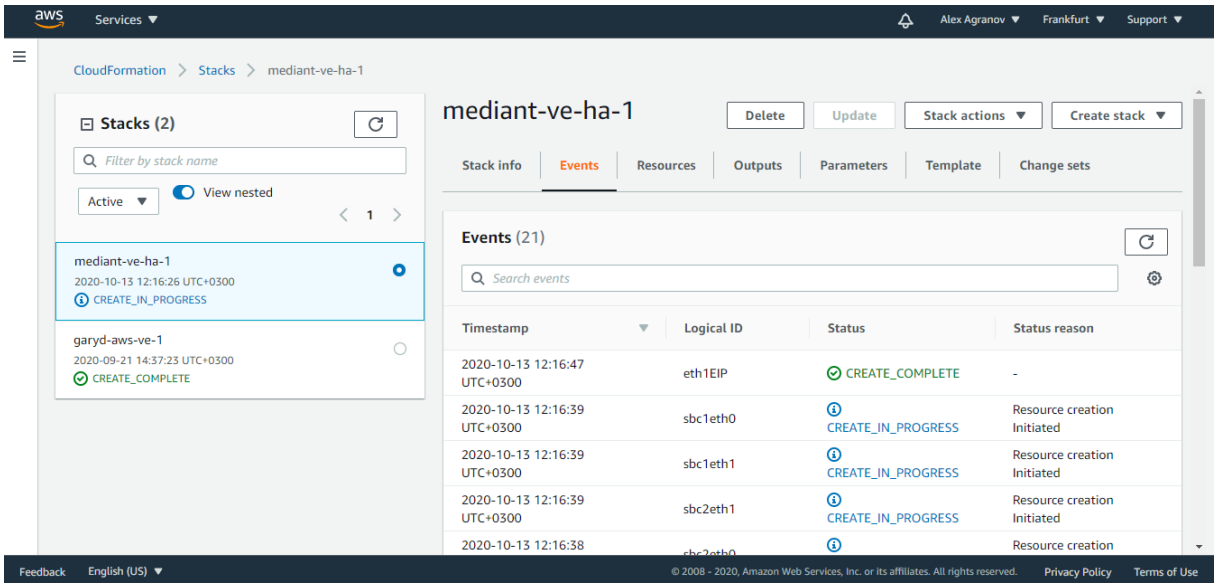
7. Under the **Parameters** section, configure parameters to match the desired stack configuration:
   - Amazon EC2 Configuration:
     - **Instance type:** AWS EC2 instance type for the stack.
     - **Amazon Machine Image (AMI):** Amazon Machine Image (AMI) ID of Mediant VE SBC (check the Mediant VE product in the AWS Marketplace to find AMI ID for the specific region).
     - **IAM Role:** Name of the existing IAM role that enables Mediant VE to manage its network interface, as created in Section IAM Role for Mediant VE HA Deployment.
     - **Key Name:** Name of the existing Key Pair used to secure access to the Mediant VE's SSH interface.
     - **S3 URL of INI Configuration File:** (Optional) Amazon S3 URL of initial Mediant VE configuration file.

Note: If you configure a value for "S3 URL of INI Configuration File", make sure that the IAM role allows access to the corresponding S3 bucket, as described in Section IAM Role for Initial Configuration from S3 URL.

   - Network Configuration:
     - **Which VPC should the SBC be deployed to?** VPC ID of the existing Amazon Virtual Private Cloud (VPC) where Mediant VE should be deployed.
     - **Number or Network Interfaces:** Number of network interfaces to be attached to Mediant VE SBC instances. Minimum number is 2; maximum number depends on the instance type used. Refer to Section Network Prerequisites for details.
     - **HA Subnet:** Subnet ID of existing subnet in your VPC. The subnet is used for internal traffic between two SBC instances and for accessing AWS API. The subnet must have a private EC2 API endpoint or a NAT Gateway set as default route, as described in Section HA Subnet. It is attached to the 1st network interface (eth0).
     - **Main Subnet:** Subnet ID of existing subnet in your VPC. The subnet is used for Management traffic (e.g., for accessing the SBC's Web interface). It may also be used for VoIP traffic (signaling and media). It is attached to the 2nd network interface (eth1).
     - **1st Additional Subnet:** Subnet ID of existing subnet in your VPC. The subnet is used for VoIP traffic (signaling and media). It is attached as the 3rd network interface (eth2). If 'Number of Network Interfaces' is less than 3, set this parameter to the same value as 'Main Subnet'.
     - **2nd Additional Subnet:** Subnet ID of existing subnet in your VPC. The subnet is used for VoIP traffic (signaling and media). It is attached as the 4th network interface (eth3). If 'Number of Network Interfaces' is less than 4, set this parameter to the same value as 'Main Subnet'.
     - **Public IPs**: Select which network interfaces should be assigned with public (Elastic) IP addresses. Keep in mind that for Elastic IPs to operate correctly, corresponding subnets must have an Internet Gateway set as the default route.
8. Click **Next**; the Options page appears. Leave this page at its default settings.

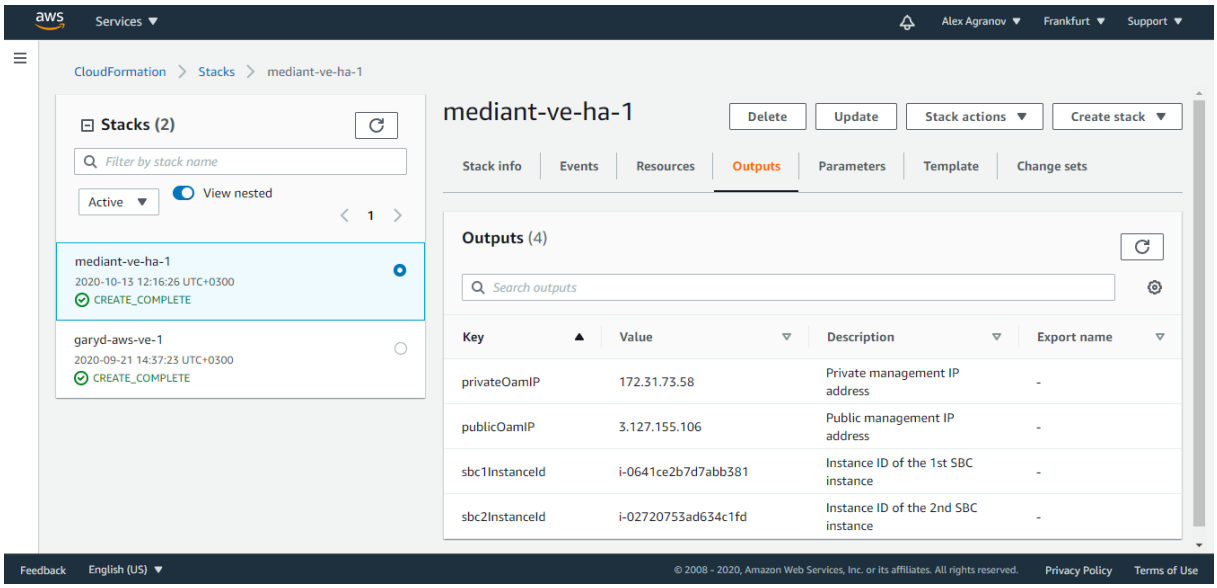
9. Click **Next**; the Review page appears, showing a summary of your stack settings:
10. Click **Create**; CloudFormation starts creating the stack. During stack creation, its state changes to "CREATE_IN_PROGRESS".

Figure 5-4: CloudFormation – Stack Creation Progress



11. Wait until the stack is created and its state changes to "CREATE_COMPLETE". Two SBC instances are created and configured to operate in 1+1 active/standby mode. Their instance-ids, management IPs and default admin credentials are listed in the **Outputs** tab.

Figure 5-5: CloudFormation – Stack Outputs



12. Access the SSH or Web interface of the deployed Mediant VE SBC using the IP address from the **privateOamIP** or **publicOamIP** field, listed in the **Outputs** tab. Use the default admin credentials – from **adminUsername** and **adminPassword** fields – to log in.

Note: If you copy/paste the *instance-id* from the **Outputs** tab, the browser may append a space to the copied value, thus making it invalid. Therefore, it is recommended to type *instance-id* manually.

5.1 Deleting HA Mediant VE Deployment

To delete deployed Mediant VE stack, use **Delete** action from the CloudFormation screen.

6 Deploying Mediant VE via Stack Manager

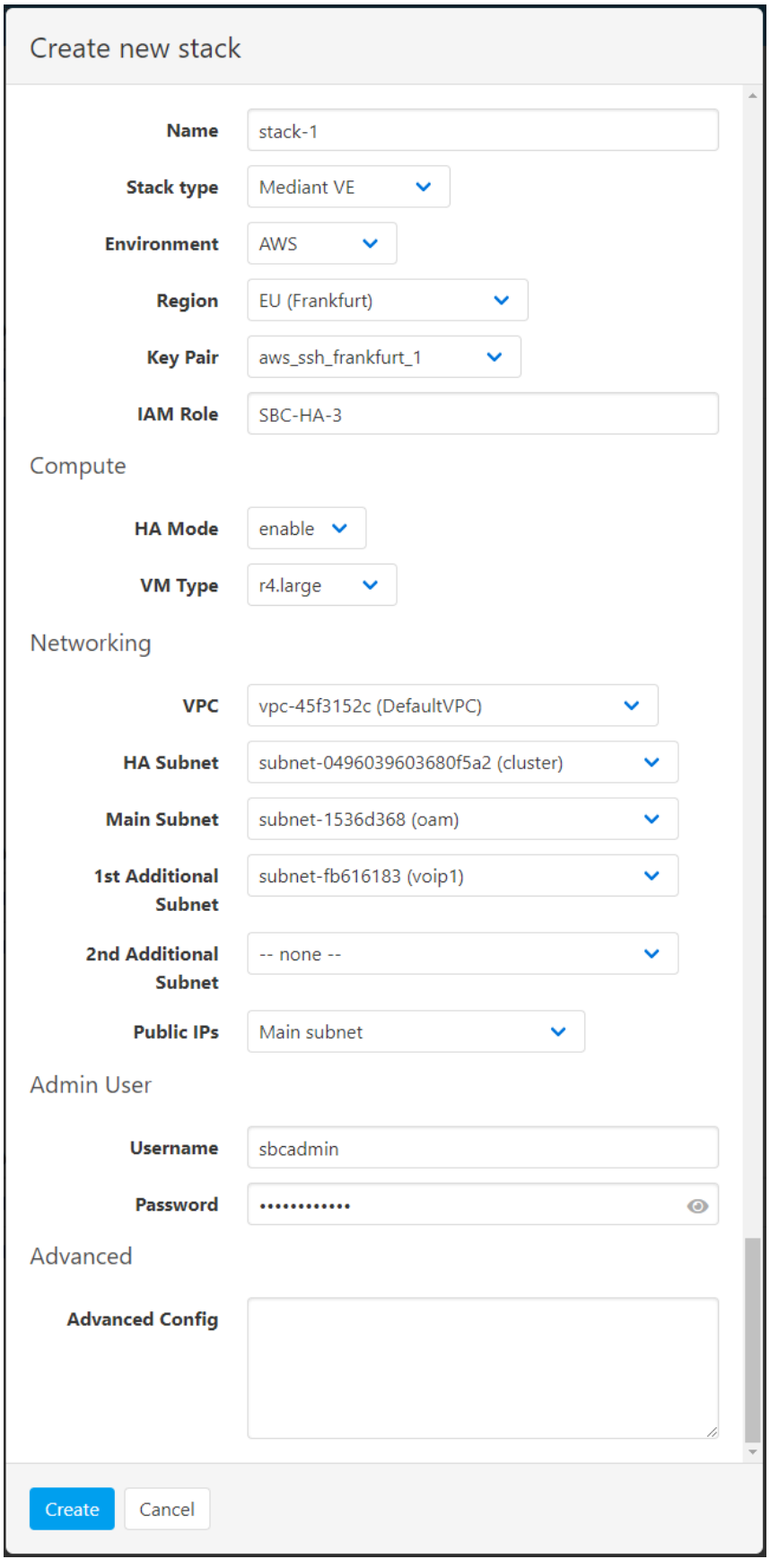
This section describes the deployment of Mediant VE via Stack Manager.

Note: This method is applicable only to the **Mediant VE SBC** product (and not the **Mediant VE SBC – PAYG** product). Both standalone and HA deployment topologies are supported.

➢ **To deploy Mediant VE via Stack Manager:**

1. Install the Stack Manager tool, as described in the *Stack Manager User's Manual*, which you can download from AudioCodes website at https://www.audiocodes.com/library/technical-documents.
2. Create a new Mediant VE stack via Stack Manager's **create** command, as described in the *Stack Manager User's Manual*.

Figure 6-1: Creating New Instance via Stack Manager



6.1 Public IP Addresses

During Mediant VE stack creation, Stack Manager lets you specify which subnets (and corresponding network interfaces) will be assigned with public (Elastic) IP addresses via the **Public IPs** parameter in the **Networking** section.

For each assigned Elastic IP address, Stack Manager creates corresponding entries in the NAT Translation SBC configuration table, thus ensuring that when the SIP application attached to the corresponding private IP addresses communicates with external SIP peers, it essentially does this via the Elastic IP address.

It is also possible to attach multiple Elastic IP addresses to the same network interface. This may be done by configuring the **public_ips** advanced configuration parameter (via **Advanced Config** section).

Note: When the **public_ips** advanced configuration parameter is specified (via **Advanced Config** section), it overrides any value configured via the **Public IPs** parameter in the **Networking** section.

- **public_ips**

  Contains comma-separated list of subnet names (main, additional1, and additional2), which will be assigned with Elastic IP addresses and optionally, with the number of Elastic IP addresses on the corresponding network interface.

  For example:

  ```
  public_ips = main:2,additional1
  ```

  attaches two Elastic IP addresses to the network interface connected to the Main subnet (eth0 for standalone deployment, eth1 for HA deployment) and one Elastic IP address to the network interface connected to the Additional 1 subnet (eth1 for standalone deployment, eth2 for HA deployment).

  When the **public_ips** advanced configuration parameter is specified, Stack Manager automatically creates secondary private IP addresses on the network interfaces that may be required for Elastic IP attachment. The exact behavior depends on the deployment type:

  - Standalone deployments: first Elastic IP address is attached to the primary private IP address. For each additional Elastic IP address, corresponding secondary IP addresses are implicitly created.
  - HA deployments: Elastic IP addresses are always attached to the secondary private IP addresses. For each Elastic IP address, corresponding secondary IP addresses are implicitly created.

6.2 Private IP Addresses

Stack Manager always creates one "operational" private IP address on each network interface. The exact behavior depends on the deployment type:

- **Standalone deployments:** primary IP address is used on each interface
- **HA deployments:** primary IP addresses on eth1, eth2 and eth3 interfaces (connected to Main, 1st and 2nd Additional subnets correspondingly) are not used, because they can't be moved between two Mediant VE instances during activity switchover; instead, secondary IP addresses are created and used.

It is also possible to create multiple "operational" private IP addresses on the same network interface. This may be done by using the **additional_ips** advanced configuration parameter (via **Advanced Config** section).

- **additional_ips**

  Contains a comma-separated list of subnet names (main, additional1, and additional2), which will be assigned with additional private IP addresses and optionally, with the number of additional private IP addresses on the corresponding network interface.

  For example:

  ```
  additional_ips = main,additional1:2
  ```

  creates one additional private IP address on the network interface connected to the Main subnet (eth0 for standalone deployment, eth1 for HA deployment) and two additional private IP addresses on the network interface connected to the Additional 1 subnet (eth1 for standalone deployment, eth2 for HA deployment).

The number of additional private IP addresses specified via the **additional_ips** advanced configuration parameter is added *on top* of any private IP addresses created by Stack Manager by default and/or due to the public (Elastic) IP addresses assigned to the specific network interface.

For example, the following configuration:

```
HA Mode: "enable"
HA Subnet: <ha-subnet-id>
Main Subnet: <main-subnet-id>
1st Additional Subnet: <additional-subnet-id>
Public IPs: "Main subnet"
Advanced Config:
    additional_ips = main,additional1
```

creates the following networking configuration:

- **eth0** – one primary IP addresses (used for internal communication between Mediant VE instances)
- **eth1** – one primary and two secondary IP addresses:
  - Primary IP address is not used because it can't be moved between Mediant VE instances in case of switchover
  - 1st secondary IP address - first "operational" private IP address, created implicitly and assigned with an Elastic IP address (due to the **Public IPs** configuration parameter)
  - 2nd secondary IP address - created due to the **additional_ips** advanced configuration parameter

- **eth2** – one primary and two secondary IP addresses:
  - primary IP address is not used because it can't be moved between Mediant VE instances in case of switchover
  - 1st secondary IP address – first "operational" private IP address, created implicitly
  - 2nd secondary IP address – created due to the **additional_ips** advanced configuration parameter

This page is intentionally left blank.

7 Adjusting Security Groups

When Mediant VE is deployed via the CloudFormation template or Stack Manager, the following security groups are automatically created and assigned to the corresponding network interfaces.

Table 7-1: Inbound Rules for Default Security Groups

Security Group	Subnets	Traffic	Protocol	Port	Source
oamSecurityGroup	Main	SSH	TCP	22	0.0.0.0/0
		HTTP	TCP	80	0.0.0.0/0
		HTTPS	TCP	443	0.0.0.0/0
signalingSecu-rityGroup	Main, 1st Additional, 2nd Additional	SIP over UDP	UDP	5060-5090	0.0.0.0/0
		SIP over TCP/TLS	TCP	5060-5090	0.0.0.0/0
mediaSecurityGroup	Main, 1st Additional, 2nd Additional	RTP, RTCP	UDP	6000-65535	0.0.0.0/0
haSecurityGroup	HA	Internal	UDP	669	haSecurityGroup
		Internal	UDP	680	haSecurityGroup
		Internal	TCP	80	haSecurityGroup
		Internal	TCP	2442	haSecurityGroup

Inbound security rules in the Main and Additional subnets are configured by default to accept traffic from all sources, which constitutes a significant security risk. It is highly recommended to modify them after Mediant VE creation to allow inbound traffic only from specific IP addresses and/or subnets, especially for management traffic.

Inbound security rules in the HA subnet are configured by default to accept traffic from the VMs that belong to the same security group only. Therefore, there is no need to further adjust them.

Outbound security rules in all subnets are configured by default to allow all traffic. You may adjust them as per your needs. If you adjust the outbound rules for HA subnet, make sure that they include the following minimal required rules:

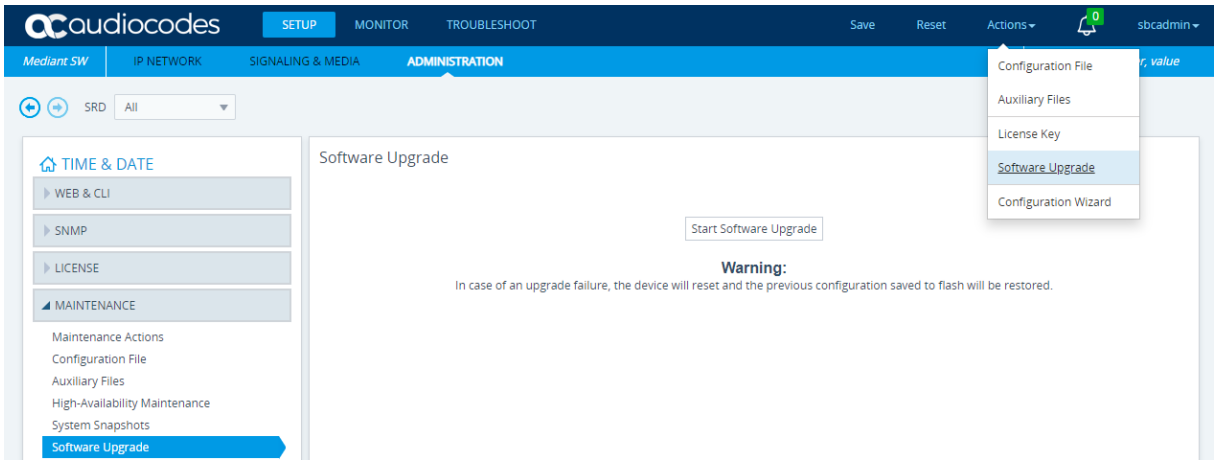
Table 7-2: Minimal Required Outbound Rules for HA Security Group

Type	Protocol	Port Range	Destination	Description
All	All	All	haSecurityGroup	Internal traffic between Mediant VE instances
HTTP	TCP	80	169.254.169.254/32	Communication with EC2 instance meta-data service
HTTPS	TCP	443	A.B.C.D/32	Communication with EC2 API endpoint. Replace A.B.C.D with the actual IP address of the private EC2 endpoint in the HA subnet. If you use a NAT Gateway to access the public EC2 endpoint, replace the destination with 0.0.0.0/0.

8 Upgrading the Software Version

You may upgrade the software version of the deployed Mediant VE software using the software version file (.cmp) through the Web or CLI interface. For example, open the Web interface, and then click **Action > Software Upgrade** on the toolbar to open the Software Upgrade wizard.

Figure 8-1: Opening Web Interface's Software Upgrade Wizard



Upgrading the Mediant VE using the software version file (.cmp) may be performed only within the same OS version stream.

The following streams are available:

- 7.20A stream – based on OS Version 6
- 7.20CO stream – based on OS Version 8
- 7.40A stream – based on OS Version 8

For example, if your Mediant VE is currently running Software Version 7.20A.256.396 (i.e., 7.20A stream, based on OS Version 6), you may use the 7.20A.258.010 .cmp file to upgrade it to a later version (also based on OS Version 6). However, you may not use 7.20CO.258.034 .cmp file to perform a similar upgrade to a version from the 7.20CO stream (based on OS Version 8).

If you want to upgrade Mediant VE deployed with a version from the 7.20A stream (based on OS Version 6) to a version from 7.20CO or 7.40A streams (based on OS Version 8), use one of the following methods:

- **Method 1:** Deploy a new Mediant VE instance using OS Version 8 software image, configure it, and then switch live traffic to the new instance. Refer to Section 8.1 for detailed instructions.
- **Method 2:** Rebuild the existing Mediant VE instance from the new OS Version 8 image. Refer to Section 8.2 for detailed instructions.

Advantages and disadvantages of each method are listed in the following table:

Method	Advantages	Disadvantages
Method 1	▪ If any problems with the new software version (based on OS Version 8) occur, live traffic may be switched back to the old instance, running the old software version. ▪ Traffic may gradually be moved to a new	▪ Requires the use of additional AWS resources for the duration of the upgrade. ▪ Requires a change of IP addresses (both public and private) and therefore, requires reconfiguration of

Method	Advantages	Disadvantages
	instance (assuming that VoIP equipment that sent the traffic towards the SBC supports such functionality), thereby providing better control over the upgrade process and minimizing service downtime.	VoIP equipment that communicates with the SBC. ▪ Requires a new License Key for the new Mediant VE instance.
Method 2	▪ Doesn't require additional AWS resources. ▪ Preserves public and private IP addresses of the deployed SBC instance.	▪ Requires a new License Key after the upgrade (because SBC serial number changes). ▪ Service is unavailable while the instance is rebuilt (typically for 5-10 minutes).

8.1 Method 1 – Side-By-Side Deployment of New Version

This section describes the upgrade of the Mediant VE instance running software version from the 7.20A stream (based on OS Version 6) to a version from the 7.20CO or 7.40A streams (based on OS Version 8) via side-by-side installation of a new Mediant VE instance and gradual migration of live traffic from the old to the new instance.

➢ **To perform upgrade via "side-by-side deployment" method:**

1. Deploy a new Mediant VE instance using OS Version 8 image via one of the following means:
   - For standalone Mediant VE deployment using AWS EC2 console (as described in Section 44), choose version from 7.20CO or 7.40A streams based on OS Version 8
   - For HA Mediant VE deployment using CloudFormation Service (as described in Section 0), choose the AMI ID that corresponds to version from 7.20CO or 7.40A streams based on OS Version 8
   - Using Stack Manager (as described in Section 6), choose **OS Version = 8** during the deployment.

   Connect the new Mediant VE instance to the same VPC and Subnets as the existing Mediant VE instance.
2. Download the configuration file (.ini) from the existing Mediant VE instance (**Actions > Configuration File > Save INI File**).
3. Remove all networking configuration from the downloaded file, using one of the following methods:
   - Using the ini_cleanup.py script from the *Mediant VE Installation Kit, which is* available on www.audiocodes.com portal.

     ```
     # python ini_cleanup.py old.ini new.ini
     ```
   - Manually: Open the file in a text editor (e.g. Notepad++), and then delete the following elements:
     - Configuration tables: PhysicalPortsTable, EtherGroupTable, DeviceTable, InterfaceTable, MtcEntities
     - Configuration parameters: HARemoteAddress, HAUnitIdName, HARemoteUnitIdName, HAPriority, HARemotePriority, HALocalMAC, HARemoteMAC

4. Load the "cleaned up" configuration file to the new Mediant VE instance as an incremental INI file (**SETUP > ADMINISTRATION > MAINTENANCE > Auxiliary Files > INI file (incremental)**).
5. Obtain, activate and apply the license to the new Mediant VE instance, as described in Section 9.1.
6. Switch live traffic from the old Mediant VE instance to the new one. This typically requires a change in the SBC's IP address in the VoIP equipment that communicates with the SBC. Consider performing gradual traffic migration if your VoIP equipment supports it. For example, switch 10% of your live traffic to the new Mediant VE instance first, verify that it is processed as expected, and only then switch the rest of the traffic.
7. After all live traffic is switched to the new Mediant VE instance and service operates normally, delete the old Mediant VE instance.

8.2 Method 2 – Rebuild Existing Mediant VE Instance from New Image

This section describes the upgrade procedure of Mediant VE instance running software version from the 7.20A stream (based on OS Version 6) to a version from the 7.20CO or 7.40A streams (based on OS Version 8) via a rebuild of existing Mediant VE instance from a new image.

The detailed procedure differs depending on the Mediant VE topology (HA or standalone) and deployment method.

8.2.1 Rebuilding Existing Standalone Mediant VE Instance Deployed via AWS EC2 Console from New Image

The described process preserves all IP addresses (private and public) assigned to the Mediant VE instance, as well as most of the SBC configuration. However, the following configuration elements will be lost and must be manually restored afterwards:

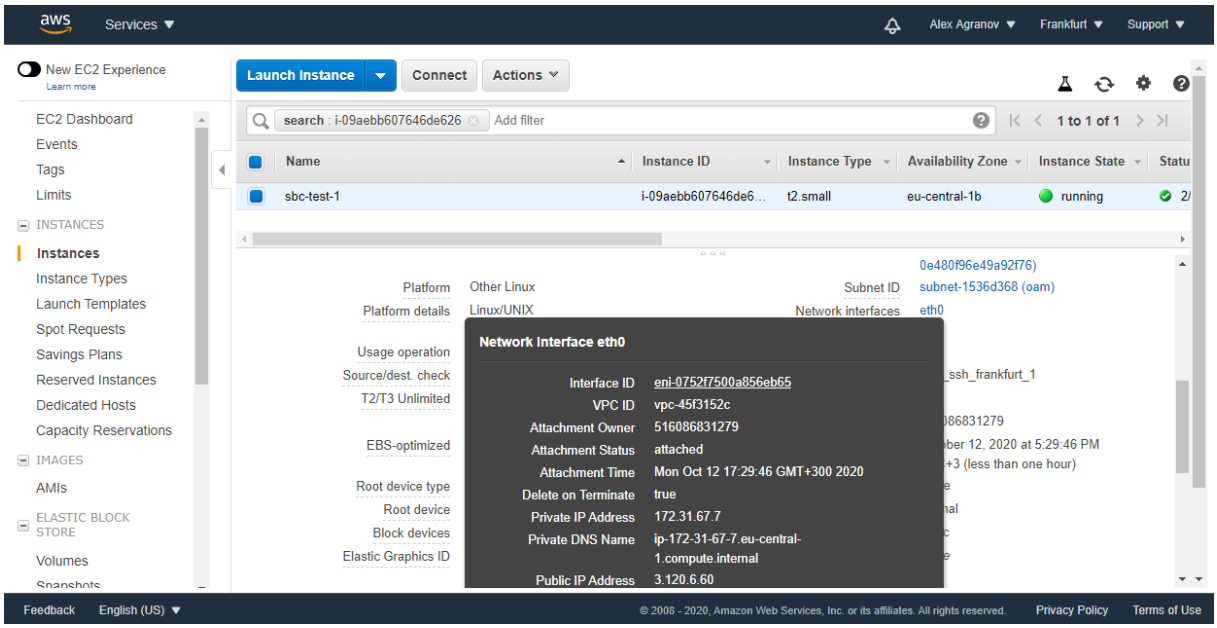
- TLS Contexts configuration (certificates and private keys)
- Auxiliary files (e.g., Pre-recorded Tone files)
- License Keys (because the serial number of rebuilt instances changes)

➢ **To rebuild existing standalone Mediant VE instance deployed via AWS EC2 console from new image:**

1. Download the Configuration Package from the Mediant VE instance: **Actions > Configuration File > Save Configuration Package**.
2. Open the EC2 console at https://console.aws.amazon.com/ec2.
3. Navigate to the **Instances** page, and then locate your Mediant VE instance.

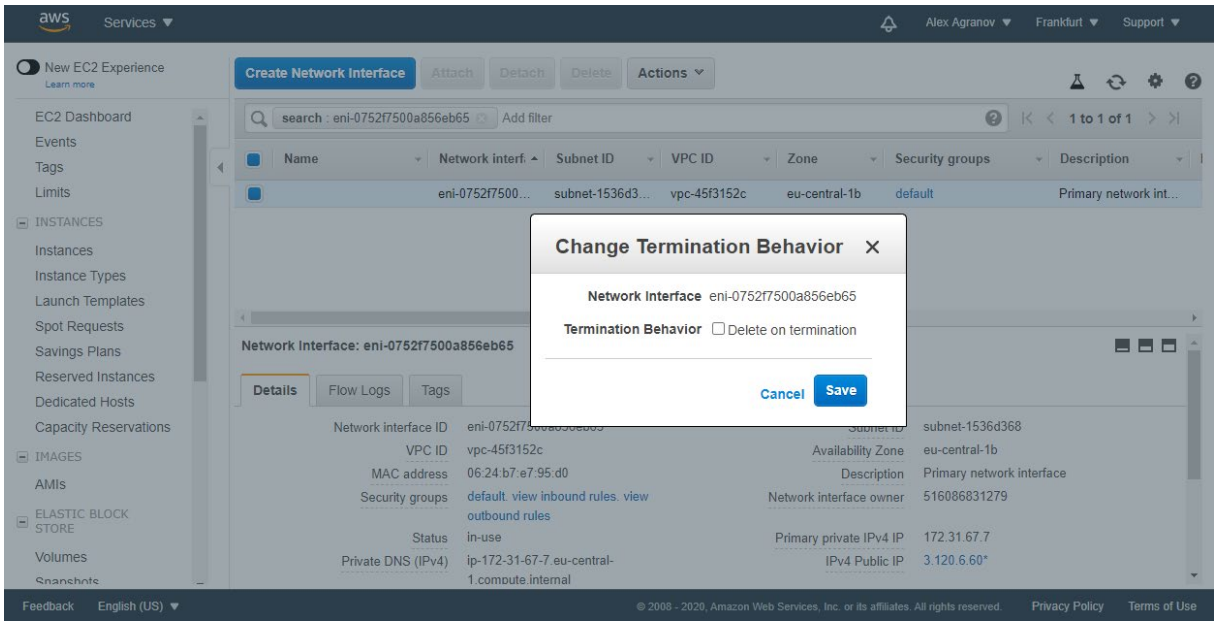
4. Find network interfaces associated with your instance.

Figure 8-2: Finding Network Instances associated with EC2 Instance



5. For each network interface:
   - Navigate to the specific interface in the **Network Interfaces** page.
   - Write down the interface ID (eni-xxxxxxx); you will need it in the next steps.
   - Click **Actions** > **Change Termination Behavior** and clear the 'Delete on termination' check box.

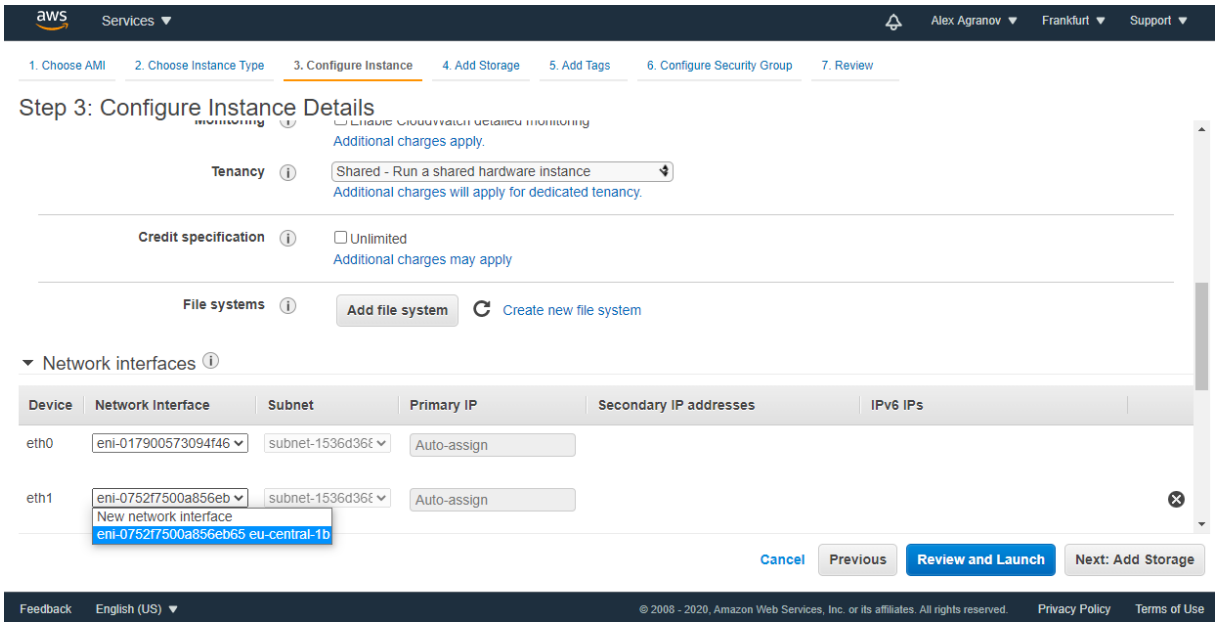
Figure 8-3: Changing Termination Behavior of Network Interface



6. Navigate back to your Mediant VE instance on the **Instances** page.
7. Click **Action > Instance State > Terminate** to terminate the instance. If asked if you want to release Elastic IPs, choose to preserve them.

8. Navigate to the AWS Marketplace at https://console.aws.amazon.com/marketplace and start a new instance deployment, as described in Section 4.
9. Choose a version from the 7.20CO or 7.40A streams, which are based on OS Version 8.
10. In the "Step 3: Configure Instance Details" screen:
    a. Select **VPC** where the old Mediant VE instance was deployed.
    b. Select the **Subnet** that the old Mediant VE instance's 1st network interface was connected to.
    c. Scroll to the bottom of the page.
    d. Under **Network Interfaces**, select an existing network interface that was used by the old Mediant VE instance. If your instance had a second network interface, then add it and choose the corresponding existing network interface.

Figure 8-4: Choosing Existing Network Interfaces during EC2 Instance Creation



11. Proceed with new instance deployment.
12. Wait until the new Mediant VE instance is deployed and fully starts (it may take up to 5 minutes). Navigate to the **Instances** page, and then check the *instance-id* of the deployed instance.
13. Log in to the new Mediant VE instance using the following default credentials:
    - Username: **Admin**
    - Password: *instance-id*
14. Load the Configuration Package file, which was saved in Step 1, back to the device (**Actions > Configuration File > Load Configuration Package**).
15. Restore parts of the Mediant VE configuration that have been lost during the rebuild, namely, TLS Contexts configuration (certificates and private keys) and Auxiliary files.
16. Obtain, activate and apply the license to the new Mediant VE instance, as described in Section 9.

Your Mediant VE is now running the new software version based on OS Version 8 and is fully operational.

8.2.2 Rebuilding Existing High-Availability (HA) Mediant VE Deployed via AWS EC2 Console from New Image

Rebuilding of the existing High-Availability (HA) Mediant VE deployed via AWS EC2 Console using CloudFormation template consists of the following steps:

1. Updating stack with change set #1 that deletes all EC2 instances and related resources.
2. Updating stack with change set #2 that restores all EC2 instances and related resources, using a new image ID (with the new Mediant VE version based on OS Version 8).

The described process preserves all IP addresses (private and public) assigned to the Mediant VE instance, as well as most of the SBC configuration. However, the following configuration elements will be lost and must be manually restored after it:

- TLS Contexts configuration (certificates and private keys)
- Auxiliary files (e.g., Pre-recorded Tone files)
- License Keys (because the serial number of rebuilt instances changes)

➢ **To rebuild existing high-availability (HA) Mediant VE deployed via AWS EC2 console from new image:**

1. Make sure that the 1st SBC instance (SBC-1) is currently active. If not, perform a switchover to make it active.

Note: Secondary IP addresses move during activity switchover. If the 2nd SBC instance is currently active, secondary IP addresses are assigned to it and therefore, stack runtime configuration doesn't match the CloudFormation template. This will result in a failure in the stack update procedure, described below.

2. Download the Configuration Package from the Mediant VE instance (**Actions > Configuration File > Save Configuration Package**).
3. Open the CloudFormation console at https://console.aws.amazon.com/cloudformation.
4. Locate the Mediant VE stack.
5. Switch to the **Template** tab, copy the current stack template to the clipboard and paste it into a new file on your PC. Name the file "mediant-ve.cfn".
6. Create a copy of the file "mediant-ve.cfn" and name it "mediant-ve-reduced.cfn". Edit the copied file "mediant-ve-reduced.cfn" as follows:
   a. Remove the following elements from the **Resources** array:
      - sbc1
      - sbc2
      - sbc1eth2Attachment
      - sbc2eth2Attachment
      - sbc1eth3Attachment
      - sbc2eth3Attachment
      - eth1EIPAssociation
      - recoveryTestAlarmSbc1
      - recoveryTestAlarmSbc2

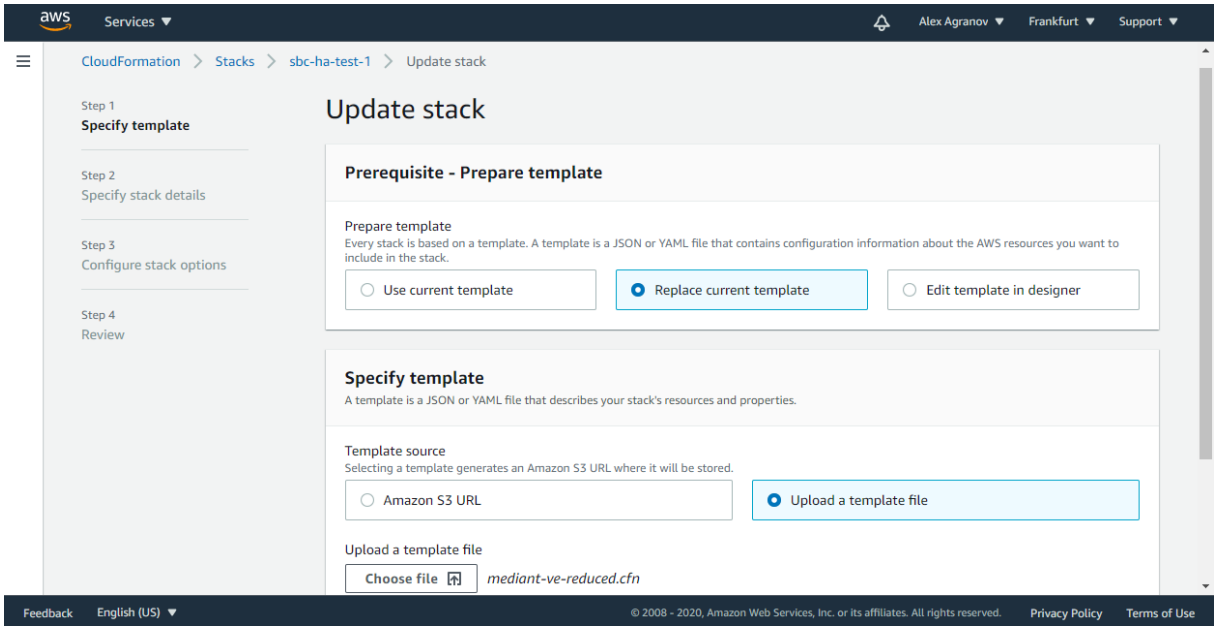
b. Remove the following elements from the **Outputs** array:

- sbc1InstanceId
- sbc2InstanceId

7. In the CloudFormation screen, click **Update**.

8. Choose **Replace current template**, upload the "mediant-ve-reduced.cfn" file from your PC, and then click **Next**.

Figure 8-5: Updating Cloud Formation stack



9. In the subsequent screens, click **Next** to accept default parameters, and then click **Update stack**.

10. While the stack is updated, its state changes to "UPDATE_IN_PROGRESS". Wait until the update is complete and the stack state changes to "UPDATE_COMPLETE".

11. In the CloudFormation screen, click **Update** again.

12. Choose **Replace current template**, upload the "mediant-ve.cfn" file from your PC, and then click **Next**.

13. In the **Specify stack details** screen, modify the **Amazon Machine Image (AMI)** parameter to the value of the AMI that corresponds to a new Mediant VE version (based on OS Version 8). Use AWS Marketplace https://console.aws.amazon.com/marketplace to determine the correct AMI ID that corresponds to the region where Mediant VE is deployed.

14. In the subsequent screens, click **Next** to accept default parameters, and then click **Update stack**.

15. While the stack is updated, its state changes to "UPDATE_IN_PROGRESS". Wait until the update is complete and the stack state changes to "UPDATE_COMPLETE".

16. Log in to the new Mediant VE instance using the default admin credentials – **adminUsername** and **adminPassword** – listed in the **Outputs** tab.

Note: If you copy/paste the *instance-id* from the **Outputs** tab, your browser may append a space to the copied value, thus making it invalid. Therefore, it is recommended to type the *instance-id* manually.

17. Load the Configuration Package file, which you saved in Step 1, back to the device (**Actions > Configuration File > Load Configuration Package**).

18. Restore parts of the Mediant VE configuration that have been lost during the rebuild, namely, TLS Contexts configuration (certificates / private keys) and Auxiliary files.

19. Obtain, activate and apply the license to the new Mediant VE instance, as described in Section 9.

Your Mediant VE is now running the new software version based OS Version 8 and is fully operational.

8.2.3 Rebuilding Existing Mediant VE Deployed via Stack Manager

This chapter describes the upgrade of Mediant VE instance running software version from 7.20A stream (based on OS Version 6) to a version from 7.20CO or 7.40A streams (based on OS Version 8) via a rebuild of existing Mediant VE instance from a new image using the Stack Manager.

The described process preserves all IP addresses (private and public) assigned to the Mediant VE instance, as well as most of the SBC configuration. However, the following configuration elements will be lost and must be manually restored afterwards:

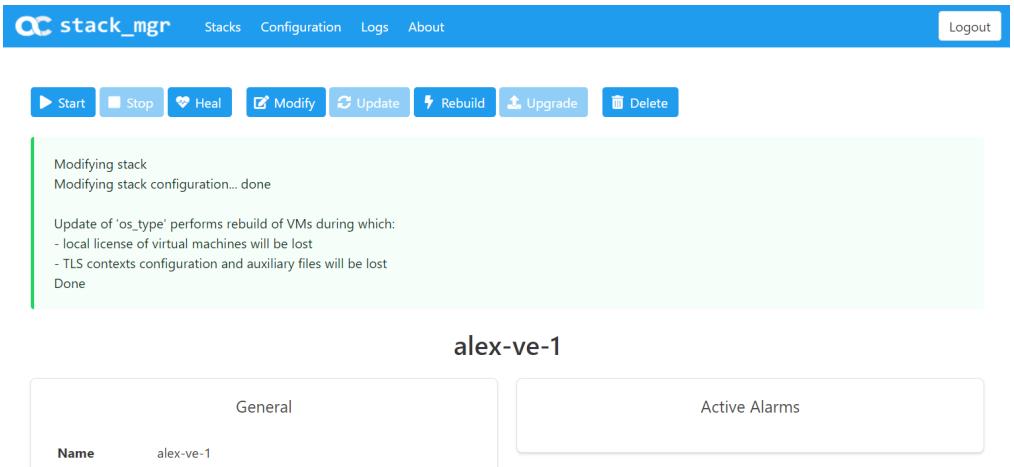
- TLS Contexts configuration (certificates and private keys)
- Auxiliary files (e.g., Pre-recorded Tone files)
- License Keys (because the serial number of rebuilt instances changes)

➢ **To rebuild existing Mediant VE deployed via Stack Manager:**

1. Connect to the Stack Manager Web interface.
2. Click the corresponding stack name.
3. Click **Modify**, and then change the **OS Version** to **8**.
4. Click **Update** to rebuild the stack.
5. Wait for the **Update** operation to complete. The operation typically takes 10-15 minutes, during which all VM instances are rebuilt and service is unavailable. Mediant VE configuration, including private and public IP addresses is preserved.
6. Restore parts of the Mediant VE configuration that have been lost during the rebuild, namely, TLS Contexts configuration (certificates / private keys) and Auxiliary files.
7. Obtain, activate and apply the license to the signaling components, as described in Section 9.

Your Mediant VE is now running the new software version based on OS Version 8 and is fully operational.

Figure 8-6: Upgrading Mediant VE to New Image Based on OS Version 8 via Stack Manager



9 Licensing the Product

Mediant VE SBC is available in AWS Marketplace as two different products:

- **Mediant VE Session Border Controller (SBC)**: This product includes a trial license (see below) and requires purchase of a production license from AudioCodes.
- **Mediant VE Session Border Controller (SBC) – PAYG**: This product includes a pay-as-you-go license that enables Customers to use the SBC as much as needed and pay for the actual service consumed via their AWS account billing.

If you installed the regular (not pay-as-you-go) version of the Mediant VE SBC product, your product includes a trial license that includes the following:

- Three concurrent sessions (signaling and media).
- Three user registrations (far-end users).
- Transcoding capabilities – in order to activate them you need to configure the 'SBC Performance Profile' parameter to **Optimize for Transcoding** (for more information, refer to the *User's Manual*).

Once you are finished evaluating the product you need to obtain, activate and then install the production SBC license.

9.1 Obtaining and Activating a Purchased License Key

Note: This and the following sections are not applicable to **Mediant VE SBC – PAYG** product, which doesn't require any additional license.

For the product to provide you with all your capacity and feature requirements, you need to purchase a new License Key that allows these capabilities. The following procedure describes how to obtain and activate your purchased License Key.

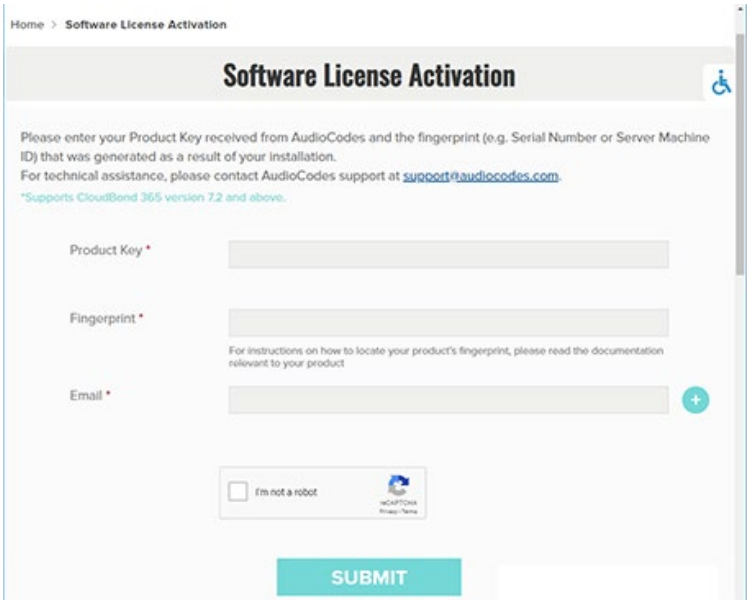
Note:

- License activation is intended **only** for first-time software activation upon product purchase (or if your License Key is "lost", due to whatever reason). For subsequent software feature upgrades, the License Key file is e-mailed to you after your Purchase Order has been processed.
- For HA, each unit has its own Serial Number, Product Key and License Key. Therefore, the instructions in this section must be done for each unit.

➢ **To obtain and activate the License Key:**

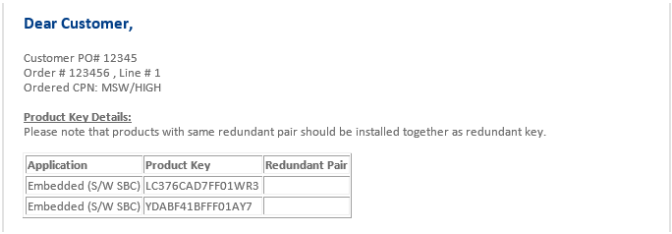
1. Open AudioCodes Web-based Software License Activation tool at https://www.audiocodes.com/swactivation:

Figure 9-1: Software License Activation Tool



2. Enter the following information:
   - **Product Key:** The Product Key identifies your specific Mediant VE SBC purchase for the purpose of subsequent communication with AudioCodes (for example, for support and software upgrades). The Product Key is provided in the Order Confirmation e-mail sent to you by AudioCodes upon your purchase, as shown in the example below:

Figure 9-2: Product Key in Order Confirmation E-mail



Dear Customer,

Customer PO# 12345
Order # 123456 , Line # 1
Ordered CPN: MSW/HIGH

Product Key Details:
Please note that products with same redundant pair should be installed together as redundant key.

Application	Product Key	Redundant Pair
Embedded (S/W SBC)	LC376CAD7FF01WR3	
Embedded (S/W SBC)	YDABF41BFFF01AY7	

Note: For 1+1 High-Availability orders, you are provided with two Product Keys, one for each unit. In such cases, you need to perform license activation twice in order to obtain License Keys for both units.

   - **Fingerprint:** The fingerprint is the Mediant VE SBC's Serial Number. The Serial Number uniquely identifies the software installation. The Serial Number is displayed in the 'Serial Number' field on the Device Information page (**Monitor** menu > **Monitor** menu > **Summary** tab > **Device Information**).
   - **Email:** Provide one or more e-mail addresses to where you want the License Key to be sent.
3. Click **Send** to submit your license activation request.

4. Once AudioCodes processes and completes your license activation, you will receive an e-mail notification with the License Key file attached. Open the file with any text-based program (such as Notepad) and make sure that the serial number ("**S/N**") in the License Key is correct and reflects the Serial Number of your Mediant VE SBC.

Warning: Do not modify the contents of the License Key file.

9.2 Installing the License Key

For installing the License Key on Mediant CE, refer to the *Mediant Software SBC User's Manual*.

Note: The License Key file for HA contains two License Keys - one for the active device and one for the redundant device. Each License Key has a different serial number ("S/N"), which reflects the serial number of each device in the HA system.

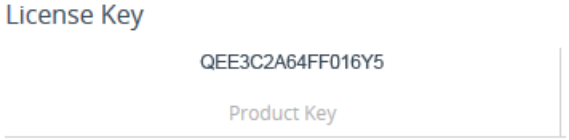
9.3 Product Key

The Product Key identifies a specific purchase of your device installation for the purpose of subsequent communication with AudioCodes (e.g., for support and software upgrades). The Product Key is provided in the order-confirmation email sent to you upon your product purchase and is used for activating your license through AudioCodes Software License Activation tool.

The Product Key is included in the License Key. Once the License Key is installed, you can view the Product Key in the following Web pages:

- License Key page (**Setup** menu > **Administration** tab > **License** folder > **License Key**). The Product Key is displayed in the read-only 'Product Key' field, as shown in the example below:

Figure 9-3: Viewing Product Key

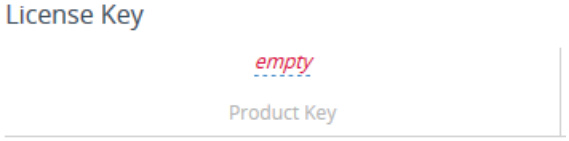


- Device Information page.

If your License Key was purchased in an earlier version (for example, 7.0), the 'Product Key' field may appear empty. In such a scenario, request the Product Key from your AudioCodes sales representative. Once received, do the following:

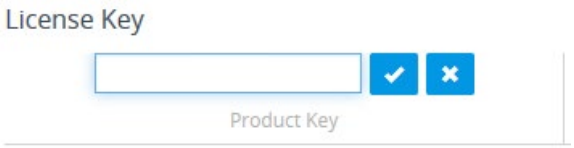
1. Open the License Key page.
2. Locate the Product Key group:

Figure 9-4: Empty Product Key Field



3. Click "empty"; the following appears:

Figure 9-5: Entering Product Key



4. In the field, enter the Product Key, and then click **Submit** (or **Cancel** to discard your entry).

This page is intentionally left blank.

International Headquarters
1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.
200 Cottontail Lane,
Suite A101E,
Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: https://www.audiocodes.com/contact
Website: https://www.audiocodes.com/support
Documentation Feedback: https://online.audiocodes.com/documentation-feedback

Document #: LTRT-10877