Mediant Cloud Edition (CE)

Session Border Controller

Version 7.2
# Table of Contents

1 **Introduction** ........................................................................................................................................................................... 9

2 **Installation Prerequisites for Amazon Web Services (AWS) Environment** .......................................................... 11
   2.1 Subscribing to AudioCodes Mediant VE Product in AWS Marketplace .......................................................... 11
   2.2 IAM Role for Mediant CE ....................................................................................................................................................... 12
   2.3 Network Prerequisites .......................................................................................................................................................... 14
      2.3.1 Cluster Subnet ................................................................................................................................................................. 15
   2.4 Instance Types ........................................................................................................................................................................ 19
   2.5 Deployment Topology ......................................................................................................................................................... 19
   2.6 Private IP Addresses ......................................................................................................................................................... 20

3 **Installation Prerequisites for Microsoft Azure Environment** ...................................................................... 21
   3.1 Network Prerequisites .......................................................................................................................................................... 21
   3.2 Subscribing to Mediant VE Offer in Azure Marketplace ............................................................................................... 22
   3.3 Virtual Machine Sizes ......................................................................................................................................................... 25
   3.4 Deployment Topology ......................................................................................................................................................... 26
   3.5 Private IP Addresses ......................................................................................................................................................... 27

4 **Installation Prerequisites for Google Cloud Environment** ................................................................................. 29
   4.1 AudioCodes Mediant CE Image ........................................................................................................................................ 29
   4.2 Network Prerequisites ......................................................................................................................................................... 30
      4.2.1 Firewall Rules ................................................................................................................................................................. 31
   4.3 Machine Types ......................................................................................................................................................................... 32
   4.4 Deployment Topology ......................................................................................................................................................... 33
   4.5 Multiple External IP Addresses ......................................................................................................................................... 34
   4.6 Internal IP Addresses ............................................................................................................................................................ 34

5 **Installation Prerequisites for OpenStack Environment** .............................................................................. 35
   5.1 AudioCodes Mediant CE Image ........................................................................................................................................ 35
   5.2 Network Prerequisites ......................................................................................................................................................... 35
   5.3 Instance Flavors .................................................................................................................................................................... 36

6 **Installation Prerequisites for Non-Cloud Environments (e.g. VMware)** .......................................................... 37
   6.1 Network Prerequisites ......................................................................................................................................................... 37
   6.2 Virtual Machine Types ......................................................................................................................................................... 38

7 **Deploying Mediant CE** ........................................................................................................................................................... 39
   7.1 Deployment via Stack Manager ........................................................................................................................................ 39
      7.1.1 Deployment Troubleshooting ........................................................................................................................................ 39
   7.2 Deployment via Manual Installation and Configuration .................................................................................................. 40

8 **Managing Mediant CE** .......................................................................................................................................................... 49
   8.1 Default Security Rules ............................................................................................................................................................ 49
   8.2 Configuring Non-standard Ports ......................................................................................................................................... 50
      8.2.1 Configuring Non-standard Ports on Azure ................................................................................................................... 50

9 **Licensing Mediant CE** ......................................................................................................................................................... 51
   9.1 Obtaining and Activating a Purchased License Key ...................................................................................................... 51
9.2 Installing the License Key

9.3 Product Key
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-28-2019

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

<table>
<thead>
<tr>
<th>Manual Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mediant Software SBC User's Manual</td>
</tr>
<tr>
<td>SBC-Gateway-MSBR Series Release Notes</td>
</tr>
</tbody>
</table>

Document Revision Record

<table>
<thead>
<tr>
<th>LTRT</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10840</td>
<td>Initial document release for Version 7.2.</td>
</tr>
<tr>
<td>10841</td>
<td>Microsoft Azure added.</td>
</tr>
<tr>
<td>10842</td>
<td>Installation prerequisites for OpenStack</td>
</tr>
<tr>
<td>LTRT</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>10843</td>
<td>Deployment in non-cloud virtual environments; new deployment via manual installation; network prerequisite diagrams updated</td>
</tr>
<tr>
<td>10844</td>
<td>Note removed regarding evaluation for Azure environments.</td>
</tr>
<tr>
<td>10845</td>
<td>Azure HA; Activation License (screenshot)</td>
</tr>
<tr>
<td>10846</td>
<td>Google Cloud platform and miscellaneous updates.</td>
</tr>
<tr>
<td>10847</td>
<td>New section for subscribing Mediant VE in AWS / Azure Marketplace; diagrams updated for network architecture (AWS, Azure / Google Cloud / OpenStack); OAM Subnet changed to Main Subnet; deployment topology updated (AWS / Azure / Google); new sections for private IP addresses (AWS / Azure); section removed – 'Multiple IP Addresses for SC Instances'; new section for installation prerequisites for non-cloud environments; new section for configuring non-standard ports on Azure</td>
</tr>
</tbody>
</table>
1 Introduction

This document describes initial installation of AudioCodes' Mediant Cloud Edition (CE) Session Border Controller (SBC), hereafter referred to as Mediant CE.

Mediant CE is a software-based product that is installed and hosted in a cloud computing environment (see note below).

Mediant CE is composed of two component types:

- **Signaling Component (SC)**: The SC handles all SIP signaling traffic. It also determines which Media Component (see below) handles the specific media traffic, which is based on load balancing between the Media Components.

- **Media Components (MC)**: The MCs handle all media traffic, including transcoding functionality. Up to 21 MCs can be used in the deployed Mediant CE.

Mediant CE provides a unified configuration and management interface, implemented by the SC. This interface provides complete control over all Mediant CE components – both SC and MCs.

Mediant CE supports High Availability (HA), which is implemented by:

- Employing two SC instances that operate in a 1+1 Active/Standby mode and that provide high availability for management and signaling traffic.

- Employing multiple MC instances that operate in an N+1 Active/Active mode and that provide capacity preservation for media traffic.

The Stack Manager tool is provided as part of the solution. It implements complete lifecycle management of the Mediant CE stack, including initial deployment, manual and automatic scaling, healing and service teardown.

The following figure provides an overview of the Mediant CE architecture.
Mediant CE currently supports the following cloud computing platforms:

- Amazon Web Services (AWS)
- Microsoft Azure
- OpenStack
- Google Cloud

You may also deploy Mediant CE in non-cloud virtual environments (e.g., VMware), via manual installation and configuration instructions, provided below. Such deployments don't support the Stack Manager component and certain cluster management features. For example, they don't support automatic scaling.

**Note:**

- Mediant CE deployment in **OpenStack** and **non-cloud virtual environments** is currently available for **evaluation** purposes only.
- The scope of this document does not fully cover security aspects for deploying the product in the cloud. Security measures should be done in accordance with specific cloud security policies and recommendations.
- For configuring Mediant CE, refer to the *Mediant Software SBC User’s Manual*. 
2 Installation Prerequisites for Amazon Web Services (AWS) Environment

Prior to installing Mediant CE in the Amazon Web Services (AWS) environment, 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. For more information, see Section Subscribing to AudioCodes Mediant VE Product in AWS Marketplace on page 11.
- You have created an Identity and Access Management (IAM) role that enables Mediant CE to manage its network interfaces. For more information, see Section IAM Role for Mediant CE on page 12.
- You have created all subnets needed for Mediant CE deployment, including the Cluster subnet with a NAT gateway. For more information, see Section Network Prerequisites on page 14.

2.1 Subscribing to AudioCodes Mediant VE Product in AWS Marketplace

Mediant VE and CE products share the same software image. AudioCodes distributes Mediant VE/CE software images by publishing them in the AWS Marketplace.

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

2. In the Discover Products tab, search for the "Mediant VE" product.
3. Click the Mediant VE Session Border Controller (SBC) product.
4. Click **Continue to Subscribe** to subscribe to the Mediant VE product.

### 2.2 IAM Role for Mediant CE

The following IAM role must be created prior to creating the Mediant CE stack. This role ensures that Mediant CE components can manage their network interfaces and re-assign IP addresses in case of a switchover.

```json
{
    "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:

2. Under Policies, create a new policy as specified above.
3. Under Rules, create a new rule based on the policy created in the previous step.

If you want to perform automatic Mediant CE provisioning using a configuration file stored on the AWS S3 service, add the corresponding statements to the IAM role, for example:

```json
{
    "Effect": "Allow",
    "Action": [
        "s3:ListBucket"
    ],
    "Resource": "arn:aws:s3:::sbc"
},
{
    "Effect": "Allow",
    "Action": [
        "s3:GetObject"
    ],
    "Resource": "arn:aws:s3:::sbc/*"
}
```
2.3 Network Prerequisites

Mediant CE on Amazon Web Services (AWS) uses the following network architecture:

**Figure 2-2: Mediant CE Network Architecture – AWS**

Up to four subnet may be used:

- **Cluster Subnet:** For internal communication between Mediant CE components and for accessing the AWS API; connected to both SC and MC instances as the first network interface (eth0); it must have a NAT gateway attached (for more information, see Section Cluster Subnet on page 15)

- **Main Subnet:** Carries management (HTTP, SSH, etc.), signaling (SIP) and media (RTP, RTCP) traffic; connected to both SC and MC instances as the second network interface (eth1) and to the Stack Manager instance

- **1st and 2nd Additional Subnets:** Carries signaling (SIP) and media (RTP, RTCP) traffic; connected to MC instances as the third and fourth network interfaces (eth2 and eth3) correspondingly; these subnets are optional, as the Main Subnet may carry all types of traffic.

All subnets must reside in the same Availability Zone of the Virtual Private Cloud (VPC). All needed subnets must be created prior to the Mediant CE deployment. During the deployment, Stack Manager creates all relevant Mediant CE components, including SC and MC instances and public IP addresses.
2.3.1 Clustering Subnet

The Clustering Subnet is used for the following tasks:

- Internal communication between Mediant CE components
- Accessing AWS API (for IP address management)

Mediant CE uses private addresses in the Clustering Subnet. Therefore, it is mandatory to attach a NAT gateway to the Clustering Subnet to enable access to AWS API. In addition, since the Clustering Subnet carries sensitive information, it is recommended to create a dedicated subnet and protect it from unauthorized access.

➢ To create the Clustering subnet:

2. 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 Clustering Subnet was created (and where Mediant CE will be deployed) and that has an Internet Gateway attached to it. For example, select **Main Subnet**.

   ![Create NAT Gateway](figure.png)

   **Note:** Do not select **Cluster Subnet** at this stage. The NAT Gateway itself will be configured as a default route in the Clustering 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 2-3: Creating NAT Gateway
3. 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. ‘cluster-route-table’).
   b. In the ‘VPC’ drop-down list, select the VPC where Mediant CE will be deployed.
   c. Click Create to create the route table.

   **Figure 2-4: Creating Route Table**

4. Select the created route table, switch to the **Routes** tab, and then click **Edit routes** to edit the routes.

   **Figure 2-5: Editing Route Table**

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

   **Figure 2-6: Creating Default Route**
6. Open the **Subnets** page, and then click **Create Subnet**.
   a. In the ‘Name tag’ field, enter the new subnet name (e.g. 'cluster-subnet').
   b. From the ‘Availability Zone’ drop-down list, select the Availability Zone where Mediant CE 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 2-7: Creating Cluster Subnet](image)

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

   ![Figure 2-8: Changing Cluster Subnet Route Table](image)
8. Choose the route table created in the previous steps, and then click **Save**.

**Figure 2-9: Editing Route Table Association**

**Note:** Make sure that you modify the routing table so that it's attached **only** to the Cluster Subnet. Other subnets (Main, Signaling1 and Signaling2) should have Internet Gateway configured as the default route; otherwise, you will be unable to communicate with the components deployed in them through the Public IP addresses.
2.4 **Instance Types**

It is recommended to use the following EC2 instance types for Mediant CE components:

- SC instances: r4.2xlarge
- Forwarding MC instances: r4.large
- Transcoding MC instances: c4.4xlarge

2.5 **Deployment Topology**

All Mediant CE components are deployed in a single Availability Zone of an AWS Region.

*Figure 2-10: Mediant CE Deployment Topology (AWS)*

Communication with signaling and media components may be performed via either public or private IP addresses.

IP addresses of active SC instance are moved (using AWS APIs) to the standby SC instance in case of SC switchover.
## 2.6 Private IP Addresses

Default Mediant CE deployment uses public IP addresses on all network interfaces. If you wish to use private IP addresses on some interfaces, modify the following stack configuration parameters (e.g. via Advanced Config section in the Web UI):

- `sc_public_ips`
- `mc_public_ips`

By default these parameters are set to a comma-separated list of all interface names, except eth0. For example, if you connect Mediant CE to four subnets, the parameters are set to "eth1,eth2,eth3".

If you want to use private IP addresses on some subnets, remove corresponding interface names from the list. For example, if you want to use private IP addresses on the 4th subnet (2nd Additional Subnet), set these parameters as follows:

```
sc_public_ips = eth1,eth2
mc_public_ips = eth1,eth2
```
3 Installation Prerequisites for Microsoft Azure Environment

Prior to installing Mediant CE in a Microsoft Azure environment, make sure that you meet the following prerequisites:

- You have a Microsoft Azure account. If you don't have an Azure account, you can sign up for one on Microsoft's website at http://azure.microsoft.com.
- You have subscribed to AudioCodes Mediant VE offer in the Azure Marketplace. For more information, see Subscribing to Mediant VE Offer in Azure Marketplace on page 22.
- You have created all subnets needed for Mediant CE deployment, including the Cluster subnet. For more information, see Section Network Prerequisites on page 21.

3.1 Network Prerequisites

Mediant CE on Microsoft Azure uses the following network architecture:

Figure 3-1: Mediant CE Network Architecture – Azure

Up to four subnet may be used:

- **Cluster Subnet**: For internal communication between Mediant CE components; connected to both SC and MC instances as the first network interface (eth0).
- **Main Subnet**: Carries management (HTTP, SSH, etc.), signaling (SIP) and media (RTP, RTCP) traffic; connected to both SC and MC instances as the second network interface (eth1) and to the Stack Manager instance.
1st and 2nd Additional Subnets: Carries signaling (SIP) and media (RTP, RTCP) traffic; connected to MC instances as the third and fourth network interfaces (eth2 and eth3) correspondingly. These subnets are optional, as the Main Subnet may carry all types of traffic.

All subnets must reside in the same Virtual Network.

All needed subnets must be created prior to the Mediant CE deployment.

During deployment, Stack Manager creates all relevant Mediant CE components, including SC and MC instances, load balancer, and public IP addresses.

3.2 Subscribing to Mediant VE Offer in Azure Marketplace

Mediant VE and CE products share the same software image. AudioCodes distributes Mediant VE/CE software images by publishing them in the Azure Marketplace.

Prior to deploying the Mediant CE you must subscribe to the AudioCodes Mediant VE offer in Azure Marketplace. This is done by deploying a demo instance of Mediant VE product from Azure Marketplace in your subscription. The deployed instance may be deleted immediately after creation.

➢ To deploy a demo instance of Mediant VE product from Azure Marketplace:

2. Navigate to the Azure Marketplace (All services > Marketplace).
3. Search for the product "Mediant VE Session Border Controller (SBC)" published by AudioCodes.
4. Click the **Mediant VE Session Border Controller (SBC)** product; the Mediant VE Product overview screen appears.

**Figure 3-2: Mediant VE SBC Product Overview**

5. Click **Create** to start a new Mediant VE deployment; the Create AudioCodes Mediant VE SBC for Microsoft Azure dialog box appears. The dialog box contains multiple steps. Complete each step according to the description below.
6. In the Basics step, do the following:

**Figure 3-3: Basics Step**

- a. In the 'Virtual Machine name' field, enter a unique name for the new VM.
- b. In the 'Username' field, enter a username – e.g. “sbcadmin”.
- c. For 'Authentication type', select the **Password** option.
- d. In the ‘Password' field, enter a password – e.g. “Admin#123456”.
- e. From the 'Subscription' drop-down list, select a proper subscription for your deployment.
- f. Under 'Resource group', select the **Create new** option and then enter a new Resource Group name for your deployment.
- g. From the 'Location' drop-down list, select a proper location for your deployment.
- h. Click **OK**.

7. In the Virtual Machine Settings and Network Settings steps accept the defaults and click **OK**.

8. In the Buy step, review the Mediant VE SBC terms of use, and then click **OK** to start the virtual machine deployment.
9. Wait until the virtual machine deployment is complete
10. Delete deployed demo instance by deleting the corresponding Resource Group

➢ To delete demo instance of Mediant VE product:
   ▪ Delete the corresponding Resource Group specified during virtual machine creation

### 3.3 Virtual Machine Sizes

It is recommended to use the following VM sizes for Mediant CE components:

- SC instances: Standard_DS3_v2 or Standard_DS4_v2
- Forwarding MC instances: Standard_DS2_v2 or Standard_DS3_v2
- Transcoding MC instances: Standard_DS3_v2 or Standard_DS4_v2
3.4 Deployment Topology

Mediant CE components are deployed across two availability zones of the Azure region.

Figure 3-5: Mediant CE Deployment Topology (Azure)

Azure Load Balancer is used to steer inbound (signaling and management) traffic towards active signaling components. Both public and internal Load Balancers are supported, enabling communication with signaling components via either public or private IP addresses respectively. The following limitations apply:

- When public IP addresses are used, Load Balancer also acts as a NAT gateway for outbound traffic.
- When private IP addresses are used, outbound traffic does not traverse through the Load Balancer. SIP headers (Via and Contact) are used to route responses and subsequent dialogs via the Load Balancer.

<table>
<thead>
<tr>
<th>Active SC</th>
<th>Internal Azure Load Balancer</th>
<th>PBX</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>INVITE ip.src = sc-ip</td>
<td></td>
</tr>
<tr>
<td></td>
<td>sip.via = lb-ip, sip.contact = lb-ip</td>
<td></td>
</tr>
<tr>
<td></td>
<td>200 OK ip.dst = sc-ip</td>
<td>200 OK ip.dst = lb-ip</td>
</tr>
<tr>
<td></td>
<td>BYE ip.dst = sc-ip</td>
<td>BYE ip.dst = lb-ip</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Communication with OVOC must be performed via the public IP address.

Communication with media components is performed via either public or private IP addresses directly attached to them. Corresponding media traffic does not pass through the Load Balancer.

3.5 Private IP Addresses

Default Mediant CE deployment uses public IP addresses on all network interfaces. If you wish to use private IP addresses on some interfaces, modify the following stack configuration parameters (e.g. via Advanced Config section in the Web UI):

- `sc_public_ips`
- `mc_public_ips`

By default these parameters are set to comma-separated list of all interface names, except eth0. For example, if you connect Mediant CE to four subnets, the parameters are set to “eth1,eth2,eth3”.

If you want to use private IP addresses on some subnets, remove corresponding interface names from the list. For example, if you want to use private IP addresses on the 4th subnet (2nd Additional Subnet), set these parameters as follows:

```
sc_public_ips = eth1,eth2
mc_public_ips = eth1,eth2
```

Each SC interface that uses public IP address is attached to the Public Load Balancer. Each SC interface that uses private IP address is attached to the Internal Load Balancer.
This page is intentionally left blank.
4 Installation Prerequisites for Google Cloud Environment

Prior to installing Mediant CE in the Google Cloud environment, make sure that you meet the following prerequisites:

- You have a Google Cloud account. If you don't have a Google Cloud account, you can sign up for one on Google's website at https://cloud.google.com.
- You have uploaded AudioCodes Mediant VE/CE Image to the image repository. For more information, see AudioCodes Mediant CE Image on page 29.
- You have created all subnets needed for Mediant CE deployment, including the Cluster subnet and corresponding Firewall Rules. For more information, see Section Network Prerequisites on page 30.

4.1 AudioCodes Mediant CE Image

To deploy Mediant CE on Google Cloud, you must use the Mediant VE/CE Image for Google Cloud. For more information, go to https://www.audiocodes.com/library/firmware.

To upload Mediant CE image to Google Cloud image repository:

1. Extract the .tar.gz file from the Mediant VE/CE Image for Google Cloud .zip file.
3. Choose an existing bucket or create a new one.
4. Choose an existing folder(s) inside the bucket or create a new one if needed.
5. Click Upload files, and then select the Mediant VE/CE image for the Google Cloud .tar.gz file.
6. Wait until the upload completes.
8. Click Create Image.
9. Enter an image name.
10. Specify the source as the Cloud Storage file, and then choose the .tar.gz file that you uploaded in previous steps.
11. Specify the additional properties for your image (e.g. family or description).
12. Click Create to create the image.
4.2 Network Prerequisites

Mediant CE on Google Cloud uses the following network architecture:

![Figure 4-1: Mediant CE Network Architecture – Google Cloud](image)

Up to four subnet may be used:

- **Cluster Subnet**: For internal communication between Mediant CE components; connected to both SC and MC instances as the second network interface (eth1).
- **Main Subnet**: Carries management (HTTP, SSH, etc.), signaling (SIP) and media (RTP, RTCP) traffic; connected to both SC and MC instances as the first network interface (eth0) and to the Stack Manager instance.
- **1st and 2nd Additional Subnets**: Carries media (RTP, RTCP) traffic; connected to MC instances as the third and fourth network interfaces (eth2 and eth3) correspondingly. These subnets are optional, as the Main Subnet may carry all types of traffic.

Subnets may reside in the same or different Virtual Networks. However, for security reasons it is recommended to separate the Cluster subnet from the other subnets and use a dedicated Virtual Network for it.

All needed subnets must be created prior to the Mediant CE deployment.

During deployment, Stack Manager creates all relevant Mediant CE components, including SC and MC instances, load balancer and external IP addresses.

Communication with SCs (management and signaling traffic) must be performed via the IP addresses attached to the Load Balancer. Most setups use a single external IP address attached to the Network Load Balancer for this purpose. Refer to the next chapter for additional configuration options.

Communication with MCs (media traffic) may be done via either internal or external IP addresses attached directly to each MC instance.
4.2.1 Firewall Rules

On the Google Cloud platform, firewall rules are configured at network level rather than at the instance / network interface level. Therefore, you must manually configure them prior to the first Mediant CE deployment, as described below.

To simplify firewall rules configuration, Stack Manager assigns network tags to all created Mediant CE components. The following tags are created by default and may be customized by changing the `sc_tags` and `mc_tags` parameters in the stack configuration file.

- Signaling Components: `sbc`, `sc`
- Media Components: `sbc`, `mc`

The following firewall rules must be created for successful Mediant CE deployment:

<table>
<thead>
<tr>
<th>Subnet</th>
<th>Name</th>
<th>Protocol</th>
<th>Port</th>
<th>Description</th>
<th>Target Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster</td>
<td>udp-669</td>
<td>UDP</td>
<td>669</td>
<td>Internal communication between SC and MC instances</td>
<td>sbc</td>
</tr>
<tr>
<td></td>
<td>udp-680</td>
<td>UDP</td>
<td>680</td>
<td>Internal communication between SC and MC instances</td>
<td>sbc</td>
</tr>
<tr>
<td></td>
<td>http</td>
<td>TCP</td>
<td>80</td>
<td>Internal communication between SC and MC instances</td>
<td>sbc</td>
</tr>
<tr>
<td></td>
<td>tcp-2424</td>
<td>TCP</td>
<td>2424</td>
<td>Internal communication between SC and MC instances</td>
<td>sbc</td>
</tr>
<tr>
<td></td>
<td>tcp-2442</td>
<td>TCP</td>
<td>2442</td>
<td>Internal communication between SC and MC instances</td>
<td>sbc</td>
</tr>
<tr>
<td></td>
<td>udp-925</td>
<td>UDP</td>
<td>925</td>
<td>Internal communication between SC and MC instances</td>
<td>sbc</td>
</tr>
<tr>
<td></td>
<td>udp-3900</td>
<td>UDP</td>
<td>3900</td>
<td>Internal communication between SC and MC instances</td>
<td>sbc</td>
</tr>
<tr>
<td>Main</td>
<td>ssh</td>
<td>TCP</td>
<td>22</td>
<td>CLI management interface on active SC instance</td>
<td>sc</td>
</tr>
<tr>
<td></td>
<td>http</td>
<td>TCP</td>
<td>80</td>
<td>Web management interface on active SC instance</td>
<td>sc</td>
</tr>
<tr>
<td></td>
<td>https</td>
<td>TCP</td>
<td>443</td>
<td>Secure Web management interface on active SC instance</td>
<td>sc</td>
</tr>
<tr>
<td></td>
<td>sip-udp</td>
<td>UDP</td>
<td>5060-5090</td>
<td>SIP signaling traffic on active SC instance</td>
<td>sc</td>
</tr>
<tr>
<td></td>
<td>sip-tcp</td>
<td>TCP</td>
<td>5060-5090</td>
<td>SIP signaling traffic on active SC instance</td>
<td>sc</td>
</tr>
<tr>
<td></td>
<td>media</td>
<td>UDP</td>
<td>6000-65535</td>
<td>RTP media traffic on MC instances</td>
<td>mc</td>
</tr>
</tbody>
</table>
### Additional Subnets

<table>
<thead>
<tr>
<th>Subnet</th>
<th>Name</th>
<th>Protocol</th>
<th>Port</th>
<th>Description</th>
<th>Target Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>sip-udp</td>
<td>UDP</td>
<td>5060-5090</td>
<td>SIP signaling traffic on active SC instance</td>
<td>sc</td>
<td></td>
</tr>
<tr>
<td>sip-tcp</td>
<td>TCP</td>
<td>5060-5090</td>
<td>SIP signaling traffic on active SC instance</td>
<td>sc</td>
<td></td>
</tr>
<tr>
<td>media</td>
<td>UDP</td>
<td>6000-65535</td>
<td>RTP media traffic on MC instances</td>
<td>mc</td>
<td></td>
</tr>
</tbody>
</table>

➢ **To create Firewall Rules:**

1. In the Google Cloud Platform Console, go to the VPC Network > Firewall Rules page [https://console.cloud.google.com/networking/firewalls](https://console.cloud.google.com/networking/firewalls).
2. Click **Create Firewall Rule** to create a new firewall rule.
3. Create firewall rules as per the table above:
   - Direction of traffic: Ingress
   - Action on match: Allow
   - Targets: Specified target tags
   - Tag name: `<tag>`
   - Source filter: IP ranges
   - Source IP ranges: 0.0.0.0/0
   - Protocols and ports: Specified protocol and ports
     - `<protocol>`: `<ports>`

### 4.3 Machine Types

It is recommended to use the following machine types for Mediant CE components:

- SC instances: `n1-standard-4` or `n1-standard-8`
- Forwarding MC instances: `n1-standard-2` or `n1-standard-4`
- Transcoding MC instances: `n1-standard-8` or `n1-standard-16`
4.4 Deployment Topology

Mediant CE components are deployed across two availability zones of the Google Cloud region.

Figure 4-2: Mediant CE Deployment Topology (Google)

Communication with SCs is performed via the IP addresses attached to Google Load Balancer. The Load Balancer steers inbound (signaling and management) traffic towards the active SC. It is recommended to use external IP addresses when communicating with SCs. Google Load Balancer doesn’t perform NAT translation and forwards traffic without modifying the IP packet’s destination address. Therefore, all IP addresses attached to the Load Balancer should be configured as virtual IP addresses in both SC instances and be used for all applications (e.g. SIP Interfaces).

Since Google Load Balancer supports only the primary network interface (eth0), SCs may be connected to the Main Subnet only. Additional Subnets 1 and 2 are used for MCs only. Communication with MCs is performed via IP addresses (external or internal) directly attached to them. Corresponding media traffic does not pass through any Load Balancer.
4.5 Multiple External IP Addresses

Default Mediant CE deployment uses a single external IP address to communicate with SC instances. This IP address is attached to the Network Load Balancer that steers traffic towards the active SC instance.

You may define additional external IP addresses to communicate with SC instances, by configuring the following stack configuration parameter (e.g. via Advanced Config section in the Web interface):

- **sc_public_ips**
  
  You may set this parameter to "eth0:<num>", where <num> is the total value of external IP addresses to be created. For example, this configuration,

  \[ sc_public_ips = eth0:2 \]

  creates two external IP addresses and corresponding Forwarding Rules. This enables signaling (SIP) traffic to be sent towards SC instances via two distinct IP addresses. Note that management (HTTP, SSH, etc.) traffic is always sent to the 1st external IP address and therefore, this IP address should be used for communication with OVOC.

4.6 Internal IP Addresses

Default Mediant CE deployment uses external IP addresses on all network interfaces. If you wish to use internal IP addresses on some interfaces, modify the following stack configuration parameters (e.g. via Advanced Config section in the Web UI):

- **mc_public_ips**
  
  By default, this parameter is set to a comma-separated list of all interface names, except eth1. For example, if you connect Mediant CE to four subnets, the parameter is set to "eth0,eth2,eth3".

  If you want to use internal IP addresses on some subnets, remove corresponding interface names from the list. For example, if you want to use internal IP addresses on the 4th subnet (2nd Additional Subnet), set this parameter as follows:

  \[ mc_public_ips = eth0,eth2 \]

- **sc_additional_ips**
  
  If you want to use internal IP addresses to communicate with SCs, set this parameter to "eth0:<num>", where <num> is the total value of internal IP address pairs to be created. For example, this configuration,

  \[ sc_additional_ips = eth0:1 \]

  creates an Internal Load Balancer and a pair of internal IP addresses. One of these IP addresses is used for forwarding UDP traffic (SIP over UDP) to the active SC instance and another one for TCP traffic (SIP over TCP or TLS).

**Note:** Use of internal IP addresses (and Internal Load Balancer) for communication with SC instances is an experimental feature and is not recommended for production environment.
5 Installation Prerequisites for OpenStack Environment

Prior to installing Mediant CE in the OpenStack environment, make sure that you meet the following prerequisites:

- You have uploaded AudioCodes Mediant VE/CE Image to the image repository. For more information, see Section AudioCodes Mediant CE Image on page 35.
- You have created all subnets needed for Mediant CE deployment, including the Cluster subnet. For more information, see Section Network Prerequisites on page 35.

5.1 AudioCodes Mediant CE Image

To deploy Mediant CE on OpenStack, you must use the Mediant VE/CE QCOW2 Image for KVM/OpenStack. For more information, go to https://www.audiocodes.com/library/firmware. Upload the image to OpenStack image repository, using the following command:

```bash
# openstack image create --disk-format qcow2 --container-format bare --public --file ./sbc-F7.20A.202.204.qcow2 sbc-F7.20A.202.204
```

5.2 Network Prerequisites

Mediant CE on OpenStack uses the following network architecture:

Figure 5-1: Mediant CE Network Architecture – OpenStack
Up to four subnet may be used:

- **Cluster Subnet**: For internal communication between Mediant CE components; connected to both SC and MC instances as the first network interface (eth0).

- **Main Subnet**: Carries management (HTTP, SSH, etc.), signaling (SIP) and media (RTP, RTCP) traffic; connected to both SC and MC instances as the second network interface (eth1) and to the Stack Manager instance.

- **1st and 2nd Additional Subnets**: Carries signaling (SIP) and media (RTP, RTCP) traffic; connected to MC instances as the third and fourth network interfaces (eth2 and eth3) correspondingly. These subnets are optional, as the Main Subnet may carry all types of traffic.

All needed subnets must be created prior to Mediant CE deployment.

### 5.3 Instance Flavors

It is recommended to use the following instance flavors for Mediant CE components:

- SC instances: 4 vCPU (non-hyperthreaded), 32GB RAM
- Forwarding MC instances: 1 vCPU (non-hyperthreaded), 4GB RAM
- Transcoding MC instances: 8 vCPU (non-hyperthreaded), 8GB RAM
6 Installation Prerequisites for Non-Cloud Environments (e.g. VMware)

Prior to installing Mediant CE in a non-cloud environment (e.g. VMware), make sure that you meet the following prerequisites:

- You have AudioCodes Mediant VE/CE Image for your environment (e.g. OVF image for VMware). Images can be downloaded from AudioCodes website at https://www.audiocodes.com/library/firmware.
- All subnets needed for Mediant CE deployment are available, including the Cluster subnet. For more information, see the following section.

6.1 Network Prerequisites

Mediant CE in non-cloud environments (e.g. VMware) uses the following network architecture:

Figure 6-1: Mediant CE Network Architecture – Non-Cloud Environments (e.g., VMware)

Up to four subnets may be used:

- **Cluster Subnet**: For internal communication between Mediant CE components.
- **Main Subnet**: Carries management (HTTP, SSH, etc.), signaling (SIP), and media (RTP, RTCP) traffic.
- **1st and 2nd Additional Subnets**: Carries signaling (SIP) and media (RTP, RTCP) traffic. These subnets are optional because the Main Subnet may carry all types of traffic.

The 1st network interface (eth0) is typically connected to the Main Subnet. The last network interface is typically connected to the Cluster Subnet.
6.2 Virtual Machine Types

It is recommended to use the following virtual machine types for Mediant CE components:

- SC instances: 4 vCPU (non-hyperthreaded), 32GB RAM
- Forwarding MC instances: 1 vCPU (non-hyperthreaded), 4GB RAM
- Transcoding MC instances: 8 vCPU (non-hyperthreaded), 8GB RAM
7 Deploying Mediant CE

This chapter describes Mediant CE deployment.

7.1 Deployment via Stack Manager

Deployment of Mediant CE is performed using the Stack Manager tool. This deployment method features:

- Simplified Mediant CE deployment, ensuring all needed resources are properly created and configured
- Resizing and adjustment of Mediant CE resources to actual service needs – both manual and automatic
- Complete Mediant CE lifecycle, including update of Mediant CE network topology, software upgrade of all its components, north-bound API for integration with orchestration tools and others
- Simplified Mediant CE termination, ensuring all resources corresponding to the Mediant CE are properly removed

➢ To deploy Mediant CE:

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 CE stack via Stack Manager’s create command, as described in the Stack Manager User's Manual.

7.1.1 Deployment Troubleshooting

Stack Manager uses cloud-native orchestration engines to perform deployment:

- AWS: Cloud Formation templates
- Azure: Azure Resource Manager (ARM) templates
- OpenStack: Heat templates
- Google: Deployment Manager templates

If Mediant CE deployment fails and the error description provided by Stack Manager is not detailed enough, refer to the corresponding orchestration engine’s detailed logs for additional information.
### 7.2 Deployment via Manual Installation and Configuration

This deployment method enables Mediant CE deployment in non-cloud virtualized environments (e.g., VMware). All needed resources (e.g., subnets and virtual machines) must be manually created and properly configured by the operator, as described below.

As this deployment method doesn’t include a “management component”, automatic scaling is not supported. Manual scaling may be done by creating and configuring additional resources, but it is considerably more complicated than when using Stack Manager.

**Note:** For supported cloud environments, you should deploy Mediant CE using the Stack Manager tool, as described previously.

The following instructions describe the following Mediant CE deployment example:

**Figure 7-1: Sample Mediant CE Deployment In VMware**

The deployment consists of:
- Two signaling components: sc-1 and sc-2
- Three media components: mc-1, mc-2, and mc-3
- Private subnet, which is used for management (e.g., SSH and HTTP), signaling (SIP), and media (RTP) traffic
- Public subnet, which is used for signaling (SIP) and media (RTP) traffic
- Cluster subnet, which is used for internal communication between Mediant CE components
To deploy Mediant CE:

1. Create virtual machines for all Mediant CE components.

2. Connect all virtual machines to the subnets:
   - eth0 (1st network port) – private subnet
   - eth1 (2nd network port) – public subnet
   - eth2 (3rd network port) – cluster subnet

3. Configure IP addresses on the 1st signaling component (sc-1):
   - eth0 – Application Type is O+C+M
   - eth1 – Application Type is C+M
   - eth2 – Application Type is Maintenance (HA)

4. Configure IP addresses on the 2nd signaling component (sc-2):
   - eth0 – Application Type is O+C+M
   - eth2 – Application Type is Maintenance (HA)

5. Configure IP addresses on the media component (mc-1, mc-2, and mc-3):
   - eth0 – Application Type is O+C+M
   - eth1 – Application Type is C+M
   - eth2 – Application Type is Cluster

6. Configure HA connection between signaling components:
   a. On the 1st signaling component (sc-1):
      a. Open the HA Settings page (Setup menu > IP Network tab > Core Entities folder > HA Settings).
      b. Configure the 'HA Remote Address' parameter to the Maintenance IP address (eth2) of the 2nd signaling component (sc-2).
      c. Save the configuration.
   b. On the 2nd signaling component (sc-2):
      a. Open HA Settings page (Setup menu > IP Network tab > Core Entities folder > HA Settings).
      b. Configure the 'HA Remote Address' parameter to the Maintenance IP address (eth2) of the 1st signaling component (sc-1).
      c. Save the configuration.
   c. Reset the 1st signaling component and wait until it boots up.
   d. Reset the 2nd signaling component. When the reset completes, the 2nd signaling component establishes HA connection with the 1st signaling component and loses all its networking configuration, except for the Maintenance IP address. Therefore, you will be unable to access its Web interface. Instead, you should check its status on the Monitor page on the Web interface of the 1st signaling component.
e. Wait until the HA connection between signaling components is fully established and Monitor page shows the 'HA Status' as "Operational" and both Active and Redundant devices are visible.

Figure 7-2: HA Connection Between Signaling Components
7. Add the cluster IP address to the signaling components:
   a. On the 1st signaling component (sc-1), open the Interfaces table (Setup menu > IP Network tab > Core Entities folder > IP Interfaces).
   b. Add an additional (secondary) IP address to the VLAN that is attached to the 3rd network interface (eth3).
   c. Configure the ‘Application Type’ parameter to Cluster for this additional IP address.

Figure 7-3: Network Configuration on Signaling Components

8. Configure signaling components to operate in Media Cluster mode:
   a. On the 1st signaling component (sc-1), open the Cluster Manager Settings page (Setup menu > IP Network tab > Media Cluster folder > Cluster Manager Settings).
      ♦ Configure the 'Cluster Mode' parameter to Media Cluster.
      ♦ Configure the 'Device Role' parameter to Signaling Component.
   b. Save the configuration.
   c. Reset the device to activate the new operation mode.

9. Configure media components (mc-1, mc-2, mc-3) to operate in Media Cluster mode:
   a. On each media component (mc-1, mc-2, mc-3), open the Cluster Manager Settings page (Setup menu > IP Network tab > Media Cluster folder > Cluster Manager Settings).
      ♦ Configure the 'Cluster Mode' parameter to Media Cluster.
      ♦ Configure the 'Device Role' parameter to Media Component.
b. Refresh the navigation menu, by clicking the browser's **Reload** button or using the Ctrl+R shortcut key.

c. Open the **MC Settings** page (Setup menu > IP Network tab > Media Cluster folder > MC Settings).
   - Configure the 'Cluster Manager IP Address' parameter to the Cluster IP address of the signaling component (added in Step 7).
   - Configure the 'Media Component Profile' parameter to match the intended operational mode of the media components.

d. Save the configuration.

e. Reset the device to activate the new configuration.

10. Configure signaling components to operate with media components:
   a. On the 1st signaling component (sc-1), open the Media Components page (Setup menu > IP Network tab > Media Cluster folder > Media Components).
   b. Click **New** to add new media component entry.
   c. Configure the media component name and corresponding OAM IP address (assigned to eth0 interface).
   d. Repeat the above steps for all media components.
   e. Save the configuration.
   f. Wait until the **Status** of all media components displays "Connected".

**Figure 7-4: Media Components Configuration and Status Table**

11. Configure Remote Media Interfaces on signaling components:
   a. On the 1st signaling component (sc-1), open the Remote Media Interfaces page (Setup menu > Signaling & Media tab > Core Entities folder > Remote Media Interfaces).
   b. Click **New** to add a new Remote Media Interface.
   c. Enter the name of the network interface on Media Components that is capable of handling media traffic (e.g., "eth0" or "eth1" in our example).
   d. Repeat the above steps for all network interfaces on the Media Components that are capable of handling media traffic.
   e. Verify that the 'Number of MCs' for each configured interface matches the actual number of Media Components (three in our example).
12. Update Media Realms configuration on signaling components:
   a. On the 1st signaling component (sc-1), open the Media Realms page (Setup menu > Signaling & Media tab > Core Entities folder > Media Realms).
   b. Click Edit to edit the default Media Realm.
   c. Configure Remote IPv4 Interface Name to reference one of the Media Component’s network interfaces, configured as Remote Media Interfaces in Step 12.
All traffic associated with this Media Realm will be sent/received via the corresponding network interface on one of the Media Components. If you need to define additional Media Realms, configure them in a similar manner. In other words, configure **Remote IPv4 Interface Name** or **Remote IPv6 Interface Name** to associate the Media Realm with the corresponding network interface on one of the Media Components. Mediant CE automatically distributes calls across available Media Components, choosing the proper network interface and port range as configured for the Media Realm.

**Figure 7-6: Media Realms Configuration**

13. If one of your subnets resides behind NAT device, configure NAT translation as follows:

   For each Media Component (mc-1, mc-2, and mc-3):
   a. Open the NAT Translation page (**Setup** menu > **IP Network** tab > **Core Entities** folder > **NAT Translation**).
   b. Click **New** to create a new NAT Translation rule, and then configure it as follows:
      - Configure the 'Source Interface' parameter to reference the corresponding network interface (e.g. eth1).
      - Configure the 'Source Start Port' parameter to 1.
      - Configure the 'Source End Port' parameter to 65535.
      - Configure the 'Target IP Address' parameter to match the public IP address of the NAT device (e.g., 10.6.2.101).
      - Configure the 'Target Start Port' parameter to 1.
      - Configure the 'Target End Port' parameter to 65535.
   c. Reset the Media Component to activate the new configuration.
   d. Repeat the above steps for all Media Components.
On the 1st signaling component (sc-1):

a. Open the Media Components page (Setup menu > IP Network tab > Media Cluster folder > Media Components).

b. For each entry that corresponds to the specific Media Component, click the Network Interfaces link at the bottom of the page, and then verify that the Public IP Address is properly detected for relevant interfaces.

Figure 7-7: Verifying Public IP Address of the Media Component

14. Open the NAT Translation page (Setup menu > IP Network tab > Core Entities folder > NAT Translation).
15. Click **New** to create a new NAT Translation rule, and then configure it as follows:

- Leave the 'Source Interface' parameter empty.
- Configure the 'Remote Interface Name' parameter to reference the corresponding Media Component's network interface (e.g., eth1).
- Configure the 'Source Start Port' parameter to **1**.
- Configure the 'Source End Port' parameter to **65535**.
- Configure the 'Target IP Mode' parameter to **Automatic**.
- Configure the 'Target Start Port' parameter to **1**.
- Configure the 'Target End Port' parameter to **65535**.

Mediant CE will automatically perform NAT Translation, using the Public IP address of the Media Component that handles the specific call.

16. Your basic Mediant CE configuration is complete. You should now configure the SIP application, as described in the *Mediant VE/CE User's Manual* and perform some basic calls to verify correct system operation.
8 Managing Mediant CE

Mediant CE management is performed through the Web, CLI, and REST management interfaces provided by the active SC component. These management interfaces are accessible as follows:

- Azure: via “eth1” private or public IP address assigned to the Azure Load Balancer
- Google: via the primary External IP address assigned to the Network Load Balancer
- AWS, OpenStack and other environments: via “eth1” private or public IP addresses assigned to the active signaling component

All Mediant CE management operations are performed through the above described management interface. There is no need to access management interfaces on other components (e.g., on media components) and such access is blocked by default security rules.

8.1 Default Security Rules

Note: This section is not applicable to Google Cloud environment where Firewall Rules are defined at subnet level and are not managed by Stack Manager.

Mediant CE deployment creates security rules that enable only relevant traffic for each component and subnet. These security rules are assigned to network interfaces on both signaling and media components.

<table>
<thead>
<tr>
<th>Component</th>
<th>Traffic</th>
<th>Subnet</th>
<th>Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signaling Component (SC)</td>
<td>SSH</td>
<td>Main</td>
<td>TCP</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>HTTP</td>
<td>Main</td>
<td>TCP</td>
<td>80</td>
</tr>
<tr>
<td></td>
<td>HTTPS</td>
<td>Main</td>
<td>TCP</td>
<td>443</td>
</tr>
<tr>
<td>SIP over UDP</td>
<td>• Main</td>
<td></td>
<td>UDP</td>
<td>5060-5090</td>
</tr>
<tr>
<td></td>
<td>• Signaling1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Signaling2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIP over TCP/TLS</td>
<td>• Main</td>
<td></td>
<td>TCP</td>
<td>5060-5090</td>
</tr>
<tr>
<td></td>
<td>• Signaling1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Signaling2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media Component (MC)</td>
<td>RTP, RTCP</td>
<td>• Main</td>
<td>UDP</td>
<td>6000-65535</td>
</tr>
<tr>
<td></td>
<td>• Media1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Media2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Security rules in the Main Subnet are configured by default to accept management traffic (SSH, HTTP, and HTTPS) from all sources, which constitutes a significant security risk. It is highly recommended to modify them after Mediant CE creation to allow only specific IP addresses / subnets to access Mediant CE management interfaces.
8.2 Configuring Non-standard Ports

When adding non-standard management or signaling ports to the Mediant CE configuration (e.g., allowing SIP traffic on port 5160), the following changes must be also implemented:

- Corresponding security group / firewall rules must be updated to allow traffic on the specific port.
- For environments that use Load Balancer (Azure or Google), load balancing rules must be updated to pass traffic on the specific port.

8.2.1 Configuring Non-standard Ports on Azure

For Mediant CE deployments on Azure performed using Stack Manager Version 1.7.4 or later, the above-described changes should be implemented via Stack Manager's "modify" command. Modify the following parameters:

- SC Management Ports
- SC Signaling Ports

Parameters contain a comma-separated list of ports and corresponding transport protocols, for example, "22/tcp,80/tcp,443/tcp,161/udp".

After modifying the parameters, run the "update" command to apply the changes.

For Mediant CE deployments on Azure performed using a Stack Manager version earlier than Version 1.7.4, the above-described changes must be implemented manually through the Azure Portal / PowerShell / CLI. However, to update load balancing rules you need to use Azure PowerShell or CLI, because these rules must have outbound SNAT disabled and currently (as of November 2019) such configuration is not supported by Azure's portal.

For example, to add a load balancing rule on port 5160 for UDP traffic, use the following commands:

```
$stackName = "ce-ha1"
$iface = "eth1"
$port = 5160
$proto = "Udp"
$name = $iface + "-" + $port + "-" + $proto.ToLower()
$rgName = $stackName + "-sc"
$lbName = $stackName + "-lb"
$idx = [int]$iface.Substring($iface.Length-1) - 1

$lb = Get-AzureRmLoadBalancer -ResourceGroupName $rgName ` -Name $lbName
Set-AzureRmLoadBalancer -LoadBalancer $lb
```
9 Licensing Mediant CE

Once you have successfully installed Mediant CE, you need to obtain, activate and then install the License Key.

**Note:** Licensing is applicable only to SCs; MCs do not require licensing.

9.1 Obtaining and Activating a Purchased License Key

For Mediant CE to provide you with all the required capacity and features, you need to obtain and activate a License Key which enables these capabilities.

**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 Mediant CE with two SC instances, each SC instance has its own Serial Number, Product Key and License Key. Therefore, the instructions in this section must be done per SC instance.

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


![Figure 9-1: Software License Activation Tool](image-url)
2. Enter the following information:

- **Product Key:** The Product Key identifies your specific Mediant CE 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:

  ![Product Key Example](image)

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

  Dear Customer,

  Customer: POM 12630
  Order: 12630_A_L1E 11
  Ordered CP: MDE16484

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

<table>
<thead>
<tr>
<th>Application</th>
<th>Product Key</th>
<th>Redundant Pair</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded (S/W 18C)</td>
<td>1C5792ADB2FB43450018080</td>
<td></td>
</tr>
<tr>
<td>Embedded (S/W 18C)</td>
<td>1C5792ADB2FB43450018057</td>
<td></td>
</tr>
</tbody>
</table>

  **Note:** For Mediant CE orders with two SC instances, you are provided with two Product Keys, one for each SC instance. In such cases, you need to perform license activation twice to obtain License Keys for both SC instances.

- **Fingerprint:** The fingerprint is the Mediant CE’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 **Submit** to send 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 SC instance.

  **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 Mediant CE with two SC instances must contain two License Keys - one for the active SC instance and one for the redundant SC instance. Each License Key has a different serial number ("S/N"), which reflects the serial number of each SC instance.
9.3 **Product Key**

The Product Key identifies a specific purchase of your Mediant CE deployment 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 > Maintenance 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](image)

- 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](image)

3. Click "empty"; the following appears:

   ![Figure 9-5: Entering Product Key](image)

4. In the field, enter the Product Key, and then click **Submit** (or **Cancel** to discard your entry).
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/corporate/offices-worldwide
Website: https://www.audiocodes.com/

©2019 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VolPerfect, VolPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice, AudioCodes Meeting Insights, AudioCodes Room Experience and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-10847