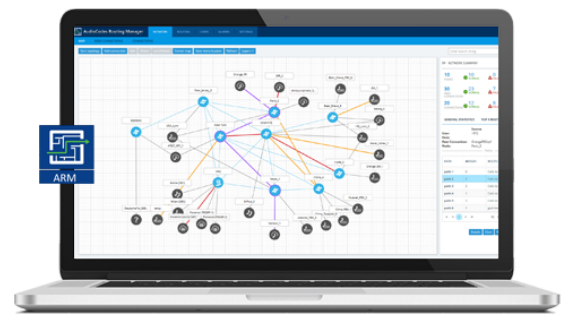


AudioCodes Routing Manager (ARM)

Version 8.8



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: September-25-2019

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>.

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>.

Stay in the Loop with AudioCodes



Related Documentation

Document Name
ARM User's Manual
ARM Release Notes

Document Revision Record

LTRT	Description
41840	Initial document release.
41841	Removed content corresponding to software modifications
41842	Fix. Requirements, Adding New VM, Deploying New VM, Deploying the Router OVF File
41843	Fix. Service Network Reboot. New: Changing an Existing Configurator's IP.
41844	New content. OVA.
41845	Licensing
41846	[v7.2] Modified router definition. Added 'Performing an Online Software Upgrade'. Added 'ARM Datacenter Recovery Procedure'.
41847	[v7.4] New screenshots. CPU: 2 cores. OVA note. Host machines HA.
41848	DNS support
41849	New RAM Storage requirements
41850	Licensing license policy Online Software Upgrade CentODS6.9 tar.gz VM memory 8 GB
41851	RAM: 10GB p/VM > 8GB p/VM; Storage: 100 GB p/VM > 40GB p/VM
41852	License page. Upgrade. OS upgrade.
41853	Hyper-V VMWare
41854	CPU: 2 cores per VM for Router VMs / 4 cores per VM for Configurator VM
41855	AWS. Network Bandwidth. Hyper-V requirements. VMWare requirements. Deploying ARM AMIs on AWS. Upgrade.
41856	Azure support
41857	Replaced unavailability on Microsoft's Azure Marketplace with availability
41858	AWS requirement: m4.xlarge instance type for Configurator and m4.large instance type for Router

Table of Contents

1	Introduction	1
	Intended Audience	1
	VMWare	1
	Hyper-V	1
	Amazon Web Services	1
	Microsoft Azure	1
	About the ARM	1
	Architecture	2
	Requirements	2
	Network Bandwidth	2
	AWS	2
	Azure	2
	Hyper-V	2
	VMWare	3
	VMware Terms	3
2	Installing the ARM	5
	Deploying a New VM	5
	Deploying the ARM's OVA File on VMWare	5
	Deploying the ARM's VHD File on Microsoft Hyper-V	9
	Deploying the ARM's AMIs on AWS	15
	Deploying the ARM from Microsoft's Azure Marketplace	19
	Logging	26
	Deploying the ARM through the PowerShell CLI	27
	Installing the Azure PowerShell CLI	27
	Deploying the ARM Environment - ARM Configurator	27
	Deploying the ARM Environment - ARM Routers	29
	Deleting the ARM Deployed through the PowerShell CLI	32
3	Performing Initial Configuration	33
	Configure a Static IP Address and Hostname for the VM	33
	Licensing	37
	Changing an Existing Configurator's IP Address	38
	Defining Routing Servers	38
4	Network Guidelines: ARM in the Public Cloud	41
	Introduction	41
	Public or Private IPs	41
	Private IP	41
	Public IP / FQDN	41
	Moving from Private IPs to Public IPs	42
	Security Group Configuration	45
	LDAP Server / Active Directory	46
	LDAP Server in the Cloud or Mirrored to the Cloud	46
	LDAP On-Premises	46

ARM GUI	46
SSH Client	46
Configurator to Router	46
Nodes (SBC or Media Gateways)	47
On-Premises Nodes using Public IPs	47
Cloud SBCs in same VPC, or VPN between SBCs and ARM	47
NTP Server	47
SNMP Traps	47
Accessing Security Group Configuration	47
On Microsoft Azure	47
On AWS	48
5 Performing an Online Software Upgrade	50
Preparing for the Upgrade	50
Performing the Upgrade	51
Troubleshooting	55
6 Backing up / Restoring ARM Software	56
Backup Types	56
Performing a Manual Backup	56
Restoring ARM Software	57
7 High Availability (HA)	58
Overview	58
Requirements for a vSphere HA Cluster	58
Distributing ARM VMs in an HA Cluster	59
VM UUID	59
ARM Datacenter Recovery Procedure	59
Preparation	60
Change Automatic Backup to an Hourly Backup	60
Prepare a Redundant Configurator	60
Recovering from Datacenter Failure	60

1 Introduction

This guide shows how to install the AudioCodes Routing Manager (ARM) in an enterprise's Virtual Machine (VM) environment.

Intended Audience

The guide is intended for IT managers in enterprises that already have VMware vSphere Hypervisor (ESXi) or Microsoft Hyper-V deployed in their networks for IT purposes, or have a public cloud account on Amazon Web Services or Microsoft Azure.

VMWare

For ARM deployments on VMWare, follow the instructions in this document but skip the documentation relating to Hyper-V.

Hyper-V

For ARM deployments on Microsoft Hyper-V, follow the instructions in this manual but replace references to 'VMWare vSphere' with 'Microsoft Hyper-V'. The installation files for the ARM Configurator and Router VMs are in VHD rather than OVA format. Note that during VM deployment in Hyper-V, you need to supply the VM settings. For more information about Hyper-V, see the [Microsoft Hyper-V Server 2016 Manual](#).

Amazon Web Services

For ARM deployments on Amazon Web Services (AWS) EC2 (Elastic Compute Cloud), follow the instructions in this manual but replace references to 'VMWare vSphere' with 'AWS console'.

Rather than the installation files for the ARM Configurator and Router, the templates for ARM instances are published as AMI (Amazon Machine Images). Note that during AMI deployment, you need to supply the instance settings. For more information about AWS EC2, see [AWS EC2 documentation](#).

Microsoft Azure

ARM can be deployed from Microsoft Azure Marketplace. For more information about deploying the ARM from Azure Marketplace, see [Deploying the ARM from Microsoft's Azure Marketplace](#) on page 19. For more information about Microsoft Azure, see [Microsoft Azure documentation](#).

About the ARM

The ARM is a LINUX-based, software-only, telephony management product which expedites and streamlines IP telephony routing for enterprises that have multiple globally distributed branches. The ARM determines the quickest, least expensive, and best call quality routes in packet networks.

Routing data, previously located on the SBC, Unified Communications (UC) application (e.g., Microsoft's Skype for Business), or Media Gateway, is now located on the ARM, which functions with an ARM server. If an enterprise has an SBC in every branch, a single ARM, deployed in the enterprise's HQ, can route all calls in the globally distributed corporate network to PSTN, the local provider, enterprise headquarters, or to the IP network.

Routing rules, configured by the IT manager in the ARM's Routing Table, perform the routing.

If an enterprise has only one or two branches, its IT manager can easily independently implement maintenance changes. In globally distributed enterprises, IT managers until now had to laboriously implement changes multiple times, per branch. With the ARM, however, IT managers implement changes only once, saving enterprises significant labor and time resources and costs.

Architecture

The ARM currently contains two modules:

- Topology Manager (a.k.a. Configurator). This module determines
 - network topology
 - what hardware and software is installed
 - best route to take in terms of cost, call quality, voice quality, and/or user priority
- Routing Manager.
 - Operates together with the Topology Manager (Configurator)
 - Commands the nodes (gateways and SBCs) in the network what route to take, which it receives from the Topology Manager

The number of modules are managed by processes running on LINUX. The processes run independently of one another.

Requirements

Network Bandwidth

The minimum bandwidth requirements per 100 CAPS of expected capacity are:

- Between ARM router and configurator: 300 Kilobytes per second or 2.5 mbps
- Between ARM router and the nodes: 5 Megabytes per second or 40 mbps

AWS

Installation of the ARM on AWS requires:

- An AWS account with sufficient permissions to deploy instances and define the necessary IAM roles
- Access from your organization's network to AWS domain (SSH, HTTPS)
- m4.xlarge instance type for Configurator and m4.large instance type for Router

Azure

Installation of the ARM on Azure requires:

- An Azure account with sufficient permissions to deploy VMs
- Access from your organization's network to Azure domain (SSH, HTTPS)
- D4s_v3 instance for Configurator and D2s_v3 instances for Routers

Hyper-V

Installation of the ARM on Hyper-V requires the following:

- Microsoft Server 2016 and up
- At least two host machines for high availability (HA)
- 64-bit host machines
- Redundant host, on a redundant network connection, and power supply
- RAM: 8 GB per Router VM, and 16 GB per configurator VM

- CPU: 2 cores (64 bit) per VM for Router VMs, and 4 cores per VM for Configurator VM
- Storage: 40 GB per VM (for HA explained in [Requirements for a vSphere HA Cluster](#) on page 58)
- VM requirements for ARM Configurator and ARM Routers are the same
- A minimum of three VMs, i.e., One Configurator and at least two Routers - see [Requirements for a vSphere HA Cluster](#) on page 58



ARM VHD images are provided with Linux integration services for Hyper-V version 4.2.

VMWare

Installation of the ARM on VMWare requires the following:

- VMware vSphere Hypervisor (ESXi) version 5.5 and up
- At least two host machines for high availability (HA)
- 64-bit host machines
- Redundant host, on a redundant network connection, and power supply
- VMware vCenter Server version 5.5
- RAM: 8 GB per Router VM, and 16 GB per configurator VM
- CPU: 2 cores (64 bit) per VM for Router VMs, and 4 cores per VM for Configurator VM
- Storage: 40 GB per VM (for HA explained in [Requirements for a vSphere HA Cluster](#) on page 58)
- VM requirements for ARM Configurator and ARM Routers are the same
- A minimum of three VMs, i.e., One Configurator and at least two Routers - see [Requirements for a vSphere HA Cluster](#) on page 58



ARM OVA images are provided with VMWare Tools 5.5. However, the ARM supports later versions of VMWare Tools as well. If an ARM customer runs the VMWare environment with later version, it's recommended they upgrade the ARM images at the Guest level from vSphere Client menu: **Guest > Install/Upgrade VMware Tools**.

VMware Terms

VMware's software package 'vSphere' contains the following components:

- ESXi server
- vSphere client
- vCenter server

Table 1-1: vSphere Software Package

Component	Description
ESXi server	This is the virtualization server. It's the most important component. It's a type 1 hypervisor. All VMs or Guest OSs, including the ARM, are installed on it.
vCenter server	Similar to vSphere client but with more power. It's a centralized management application that lets you centrally manage VMs and ESXi hosts. To install, manage and access the virtual servers located above the ESXi server, you'll need vSphere client or vCenter.

Component	Description
vSphere client	Used to access vCenter server and ultimately manage ESXi server. It lets administrators connect to ESXi server and access or manage VMs. It's installed on the client machine, e.g., the IT manager's laptop, from where it's used to connect to ESXi server and perform management tasks. To install, manage and access the virtual servers located above ESXi server, you'll need vSphere client or vCenter.



The physical servers are 'Host 1'. A hypervisor is installed on each. Each mediates between the hardware and the VMs the resources required: memory, CPU, storage, and to give a VM to each.

2 Installing the ARM

The ARM can be installed on VMWare, Microsoft Hyper-V, Azure or AWS. Installing the ARM adds another VM to the enterprise customer's environment. AudioCodes supplies enterprise customers with an OVA template/image. The enterprise customer deploys the OVA in their existing virtual environment.



- Screenshots shown here are of the Configurator (Topology Manager) OVA deployment.
- Screenshots of the Router OVA deployment are identical, only 'router' is indicated instead of 'configurator'.
- The 'Router' VM must be deployed at least twice, for HA purposes (see [Requirements for a vSphere HA Cluster](#) on page 58 for detailed information).

Deploying a New VM

In a VM environment, vCenter server is used to load and deploy the following new VMs:

- ARM Configurator
- ARM Router

AudioCodes supplies two OVA files for them:

- Configurator OVA file. Only one is deployed.
- Router OVA file. Many can be deployed, for example, if there are 1000 nodes and the network is congested with heavy traffic. Initially, two are deployed for HA in an Active-Active configuration (not Active-Standby).

Deploying the ARM's OVA File on VMWare

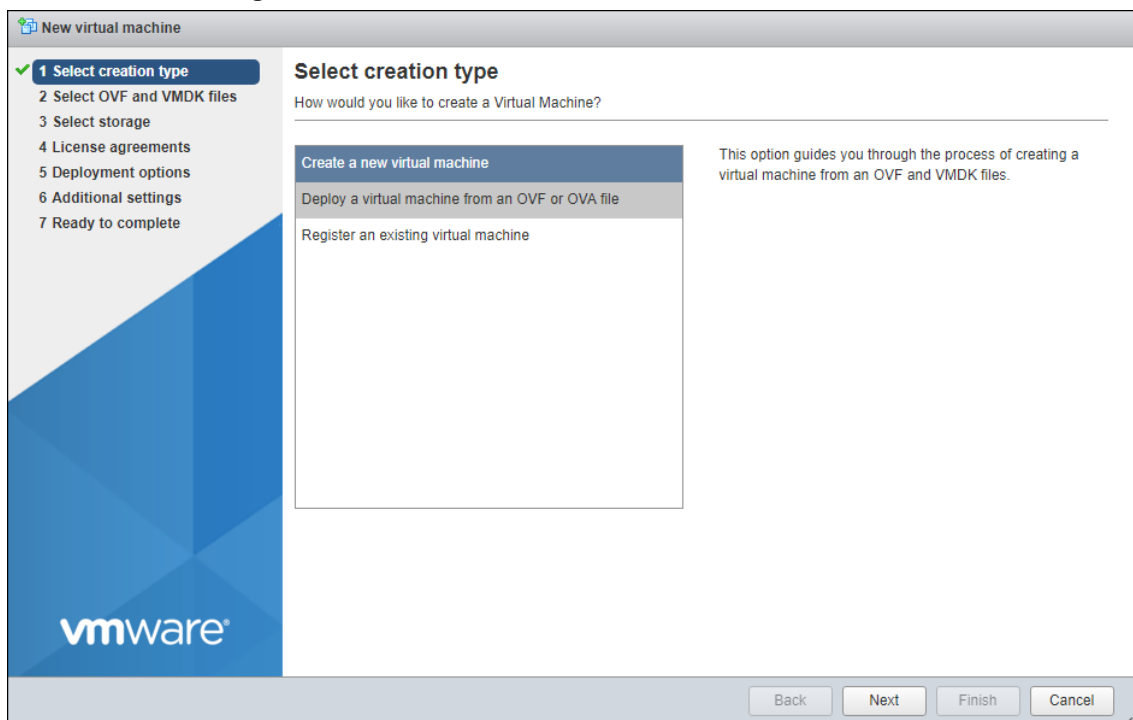
IT managers can deploy the ARM on a VMware server such as the ESXi. To do so, IT managers must create a Virtual Machine from the OVA file distributed by AudioCodes.

➤ **To deploy the OVA file:**

1. From your internet browser, access the VMware ESXi server as shown below.

Figure 2-1: VMWare ESXi - Log in

2. Enter the User name and Password and click **Log in**.

Figure 2-2: Create a new virtual machine

3. Choose **Host**, select **Deploy a virtual machine from an OVF or OVA file** and then click **Next**.

Figure 2-3: VM Name and select OVA file

New virtual machine - ARM_Configurator

1 Select creation type
2 Select OVF and VMDK files
 3 Select storage
 4 License agreements
 5 Deployment options
 6 Additional settings
 7 Ready to complete

Select OVF and VMDK files

Select the OVF and VMDK files or OVA for the VM you would like to deploy

Enter a name for the virtual machine.

ARM_Configurator

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

Click to select files or drag/drop

Back Next Finish Cancel

4. Enter a name for the virtual machine, e.g., ARM_Configurator, and then click **Click to select files or drag/drop** to navigate to the ARM OVA file.

Figure 2-4: Select storage

New virtual machine - ARM_Configurator

1 Select creation type
 2 Select OVF and VMDK files
3 Select storage
 4 License agreements
 5 Deployment options
 6 Additional settings
 7 Ready to complete

Select storage

Select the datastore in which to store the configuration and disk files.

The following datastores are accessible from the destination resource that you selected. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
datastore1	1.63 TB	1.2 TB	VMFS6	Supported	Single

1 items

Back Next Finish Cancel

5. Click **Next**.

Figure 2-5: Deployment options

The screenshot shows the 'New virtual machine - ARM_Configurator' wizard. On the left, a progress bar indicates five steps: 1. Select creation type, 2. Select OVF and VMDK files, 3. Select storage, 4. Deployment options (highlighted), and 5. Ready to complete. The main area is titled 'Deployment options' and contains a table with the following settings:

Select deployment options	
Network mappings	VM Network (dropdown menu)
Disk provisioning	<input checked="" type="radio"/> Thin <input type="radio"/> Thick
Power on automatically	<input checked="" type="checkbox"/>

At the bottom right, there are four buttons: 'Back', 'Next' (highlighted), 'Finish', and 'Cancel'.

6. Click **Next**.

Figure 2-6: Ready to complete

The screenshot shows the 'New virtual machine - ARM_Configurator' wizard at the 'Ready to complete' step. The progress bar on the left now highlights step 5. The main area is titled 'Ready to complete' and contains a table summarizing the settings:

Review your settings selection before finishing the wizard	
Product	ARM-Conf_8.6.19
VM Name	ARM_Configurator
Disks	ARM-Conf_8.6.19-disk1.vmdk
Datastore	datastore1
Provisioning type	Thin
Network mappings	VM Network: VM Network
Guest OS Name	Unknown

Below the table, there is a yellow warning icon and the text: 'Do not refresh your browser while this VM is being deployed.' At the bottom right, there are four buttons: 'Back', 'Next', 'Finish' (highlighted), and 'Cancel'.

7. Click **Finish**.

Figure 2-7: Host - Disk Format

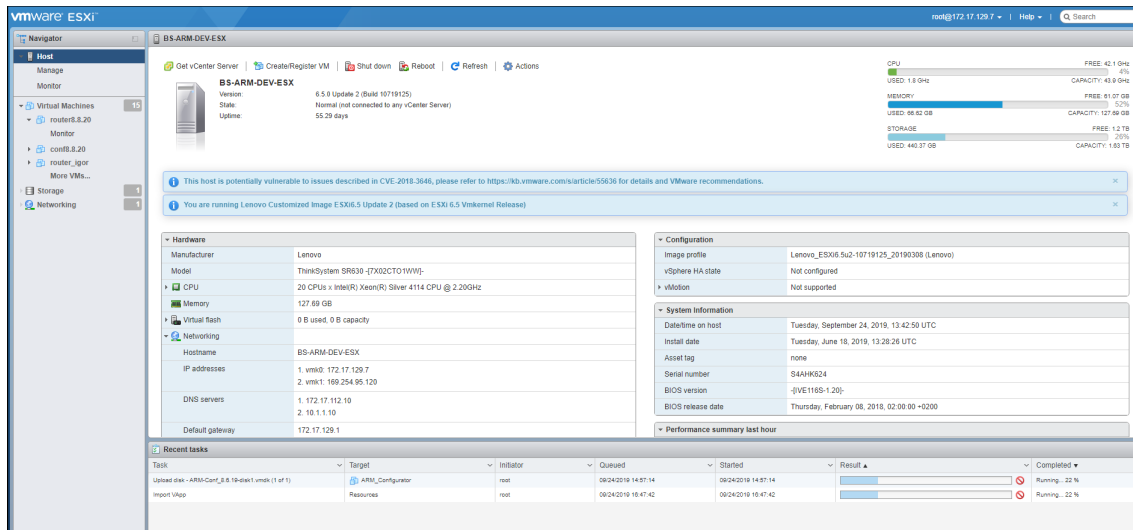
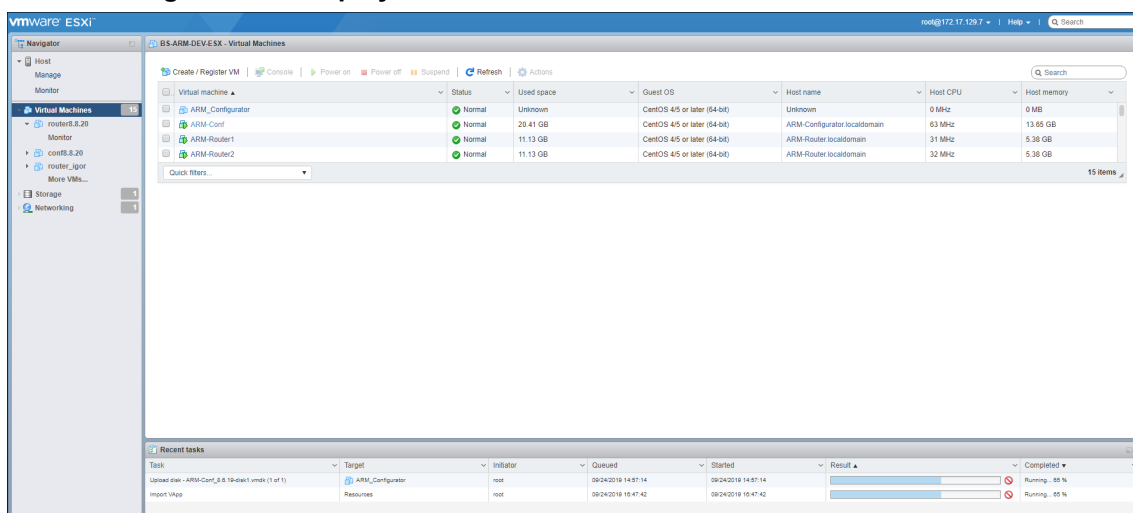


Figure 2-8: Deployment Information - Virtual Machines



Deploying the ARM's VHD File on Microsoft Hyper-V

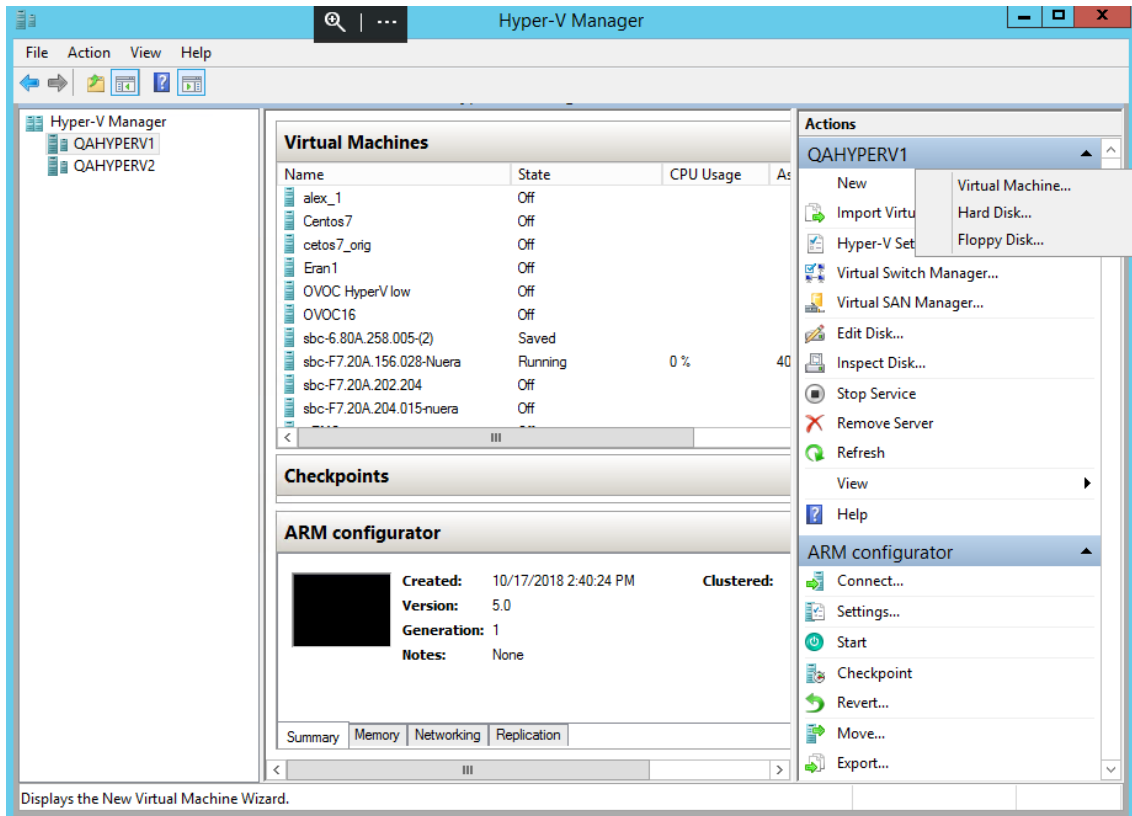
The ARM's VHD file must be deployed on Microsoft's Hyper-V.

➤ Before deploying the ARM's VHD file:

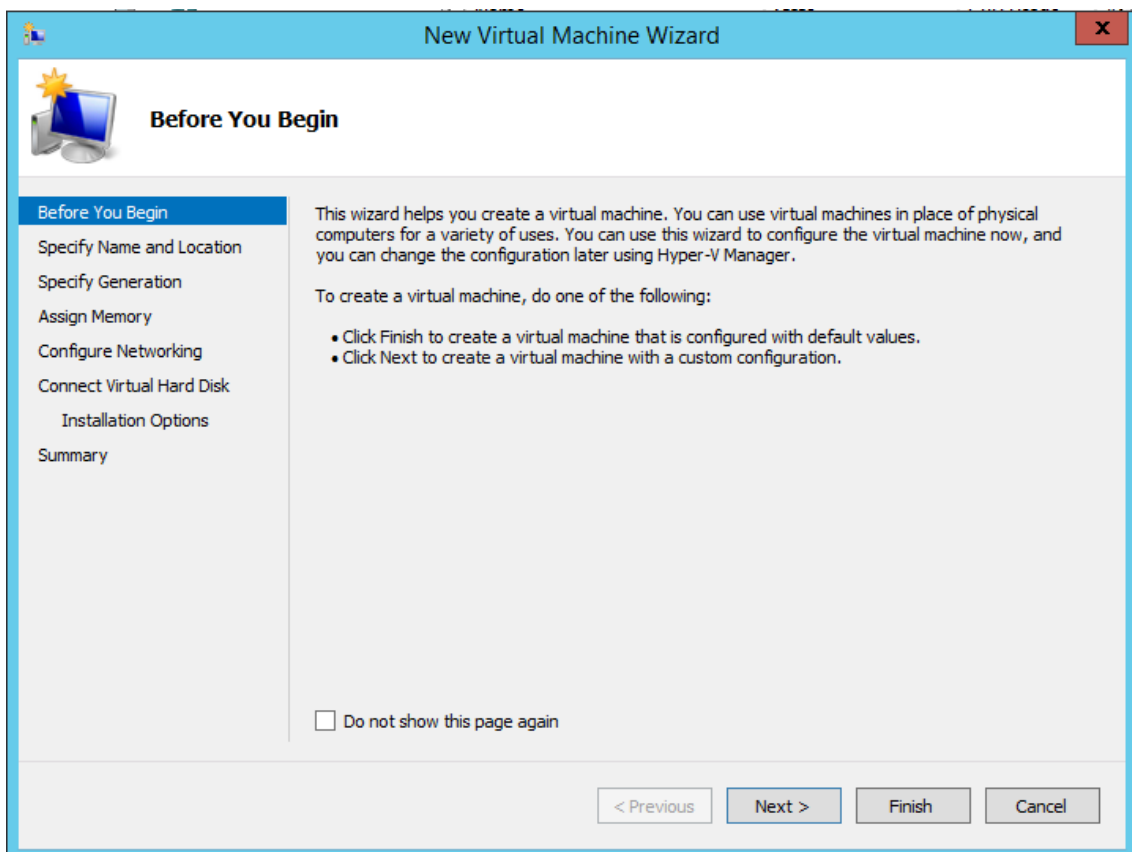
1. Obtain the VHD file for the ARM Configurator and ARM Router for the version you want to install.
2. Copy the VHD files to the VHD storage location on your Hyper-V host; create a separate copy of the VHD file for each VM.

➤ To deploy the ARM's VHD file:

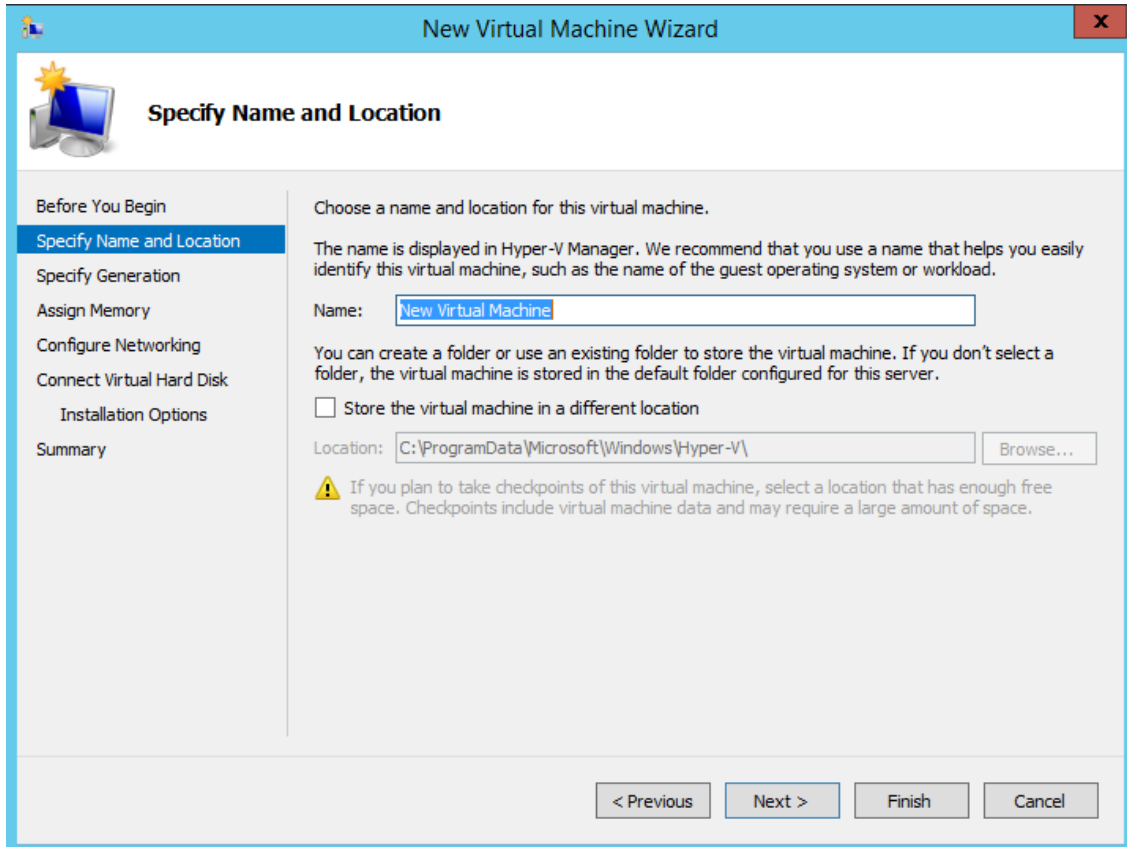
1. Start Hyper-V Manager.
2. Click **New > Virtual Machine**.

Figure 2-9: New > Virtual Machine

3. Click **Next**.

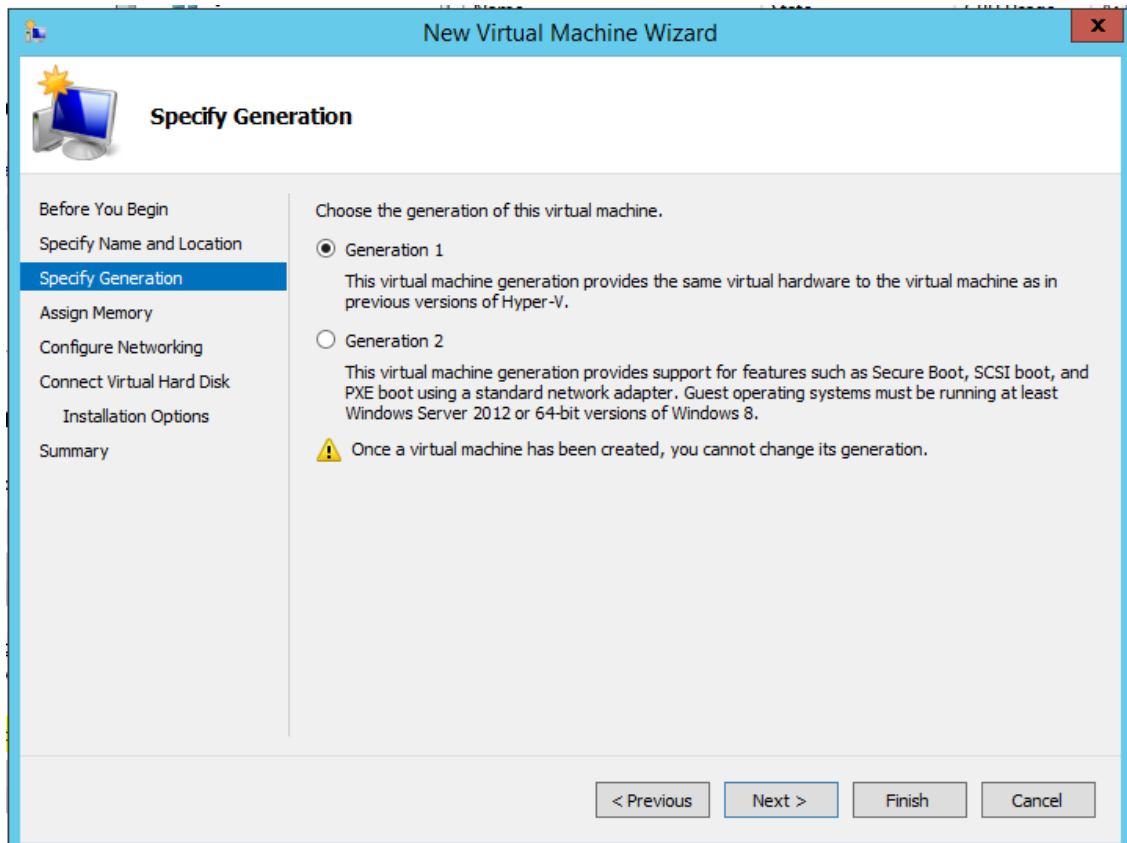
Figure 2-10: New Virtual Machine Wizard

4. Give the VM a name and click **Next**.

Figure 2-11: New Virtual Machine Wizard: Specify a Name

The screenshot shows the 'New Virtual Machine Wizard' window, specifically the 'Specify Name and Location' step. The left sidebar contains a list of steps: 'Before You Begin', 'Specify Name and Location' (highlighted), 'Specify Generation', 'Assign Memory', 'Configure Networking', 'Connect Virtual Hard Disk', 'Installation Options', and 'Summary'. The main area has a title 'Specify Name and Location' and a sub-header 'Choose a name and location for this virtual machine.' Below this, it says 'The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.' There is a text box for 'Name' containing 'New Virtual Machine'. Below that, it says 'You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.' There is a checkbox for 'Store the virtual machine in a different location' which is unchecked. Below that is a text box for 'Location' containing 'C:\ProgramData\Microsoft\Windows\Hyper-V\' and a 'Browse...' button. A warning icon and text state: 'If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.' At the bottom are buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'.

5. Select **generation 1** and click **Next**.

Figure 2-12: New Virtual Machine Wizard: Select 'Generation 1'

The screenshot shows the 'New Virtual Machine Wizard' window, specifically the 'Specify Generation' step. The left sidebar contains a list of steps: 'Before You Begin', 'Specify Name and Location', 'Specify Generation' (highlighted), 'Assign Memory', 'Configure Networking', 'Connect Virtual Hard Disk', 'Installation Options', and 'Summary'. The main area has a title 'Specify Generation' and a sub-header 'Choose the generation of this virtual machine.' Below this, there are two radio button options: 'Generation 1' (selected) and 'Generation 2'. Under 'Generation 1', it says 'This virtual machine generation provides the same virtual hardware to the virtual machine as in previous versions of Hyper-V.' Under 'Generation 2', it says 'This virtual machine generation provides support for features such as Secure Boot, SCSI boot, and PXE boot using a standard network adapter. Guest operating systems must be running at least Windows Server 2012 or 64-bit versions of Windows 8.' A warning icon and text state: 'Once a virtual machine has been created, you cannot change its generation.' At the bottom are buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'.

6. Allocate 16000 MB for the ARM Configurator VM and 8000 MB for the ARM Router VM and click **Next**.

Figure 2-13: New Virtual Machine Wizard (for ARM Configurator): Allocate 16000 MB

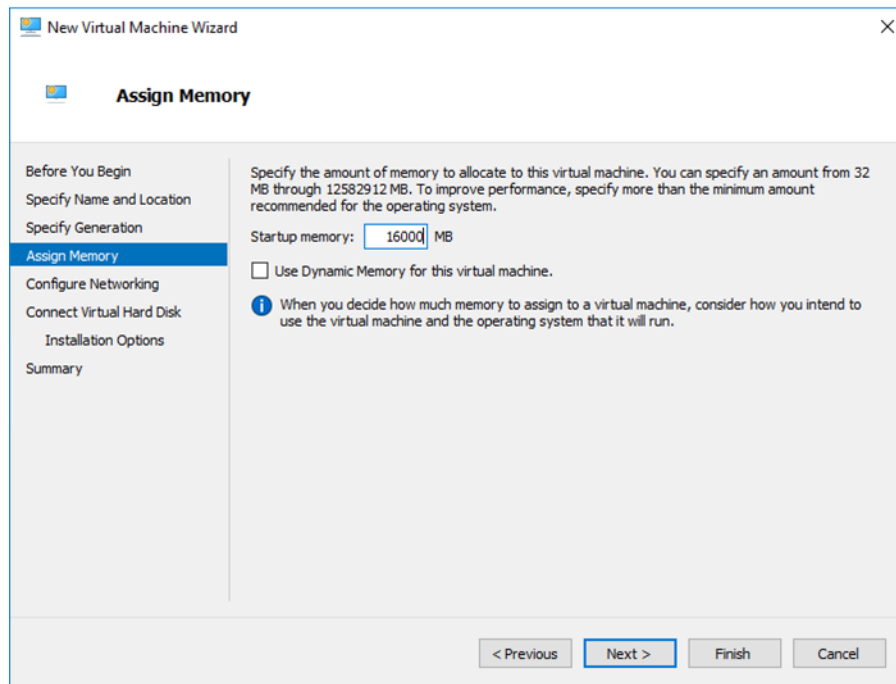
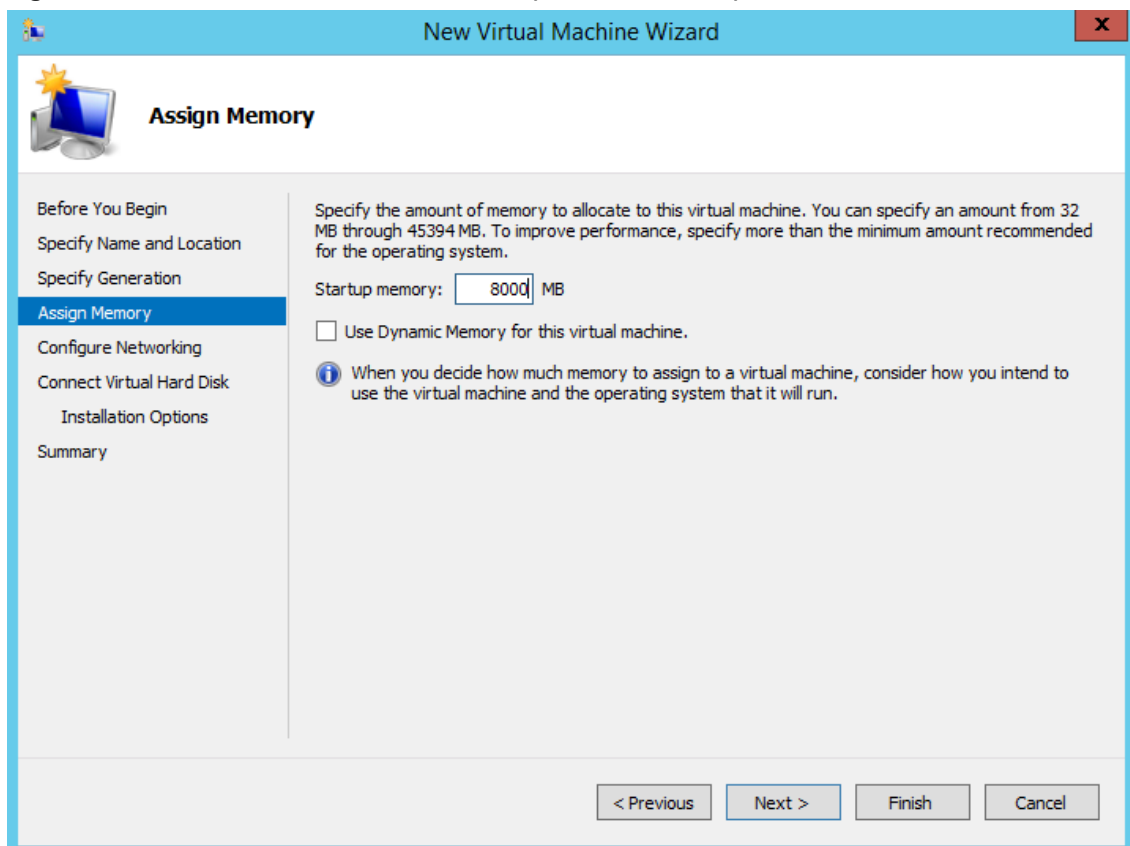
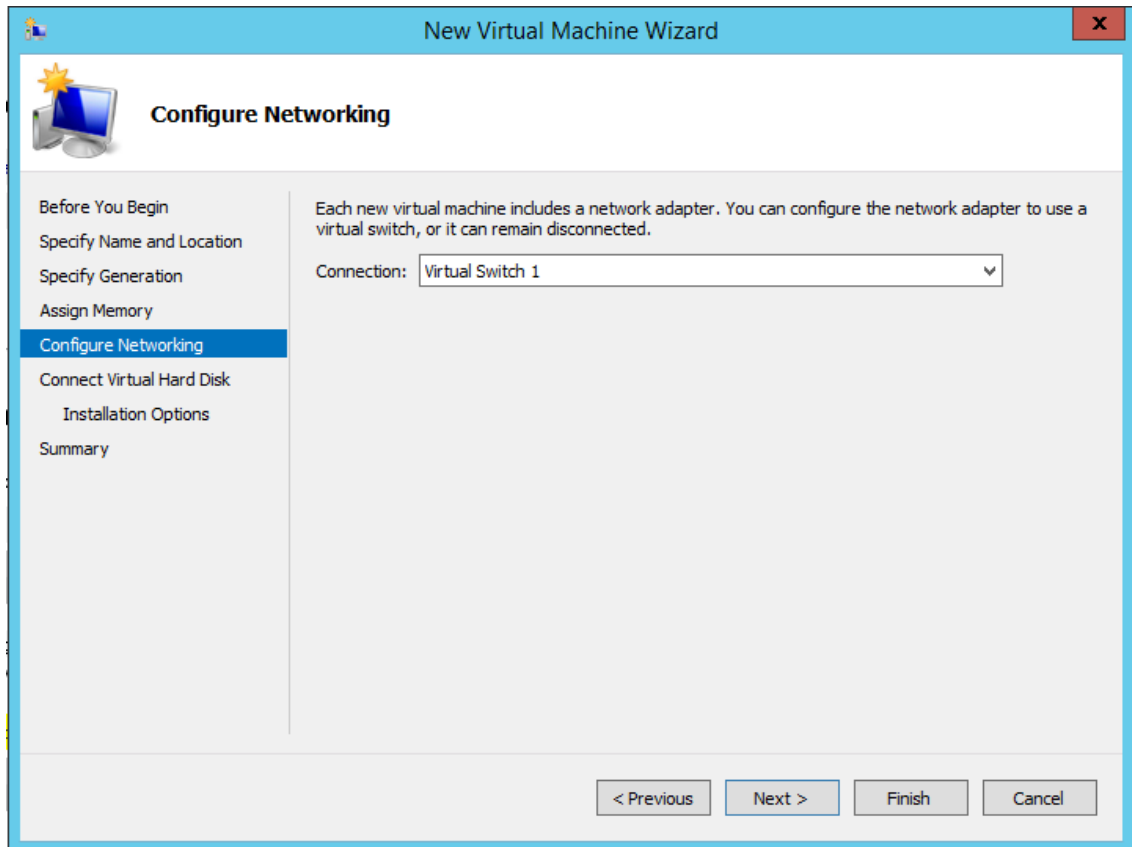


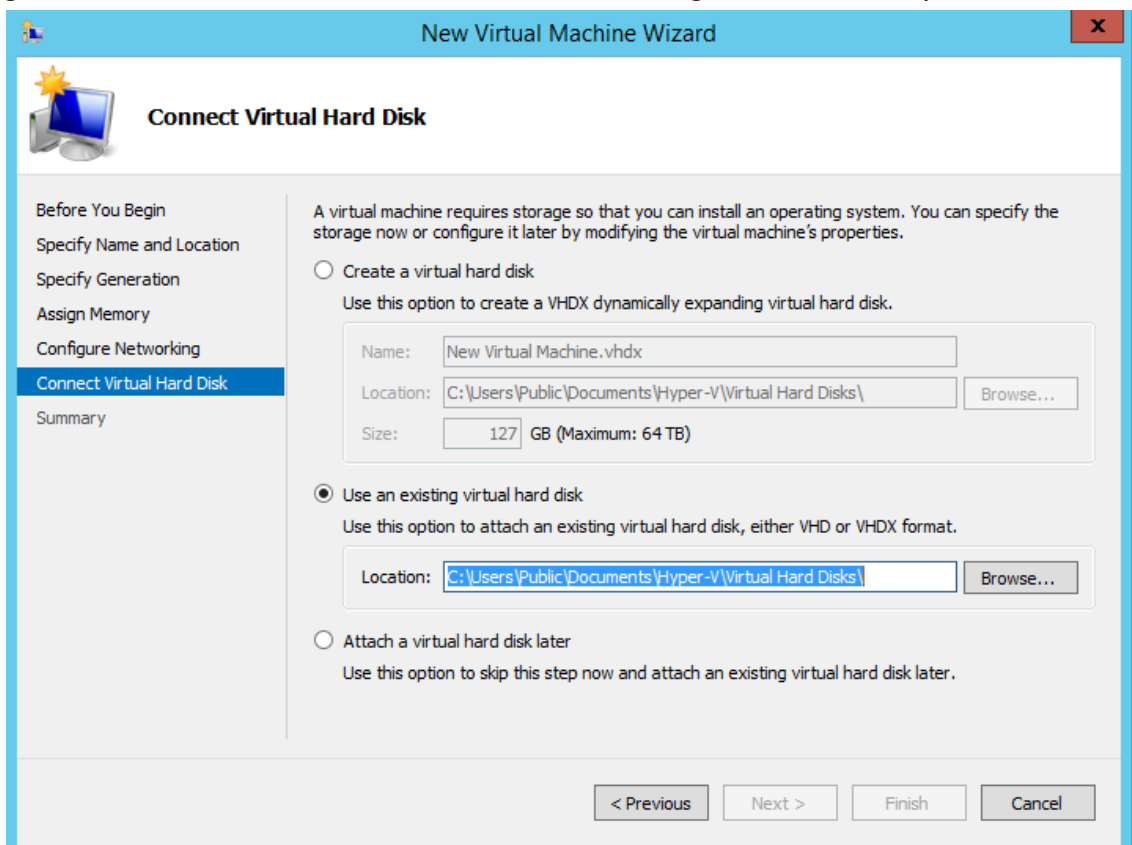
Figure 2-14: New Virtual Machine Wizard (for ARM Router): Allocate 8000 MB



7. Select a virtual switch and click **Next**.

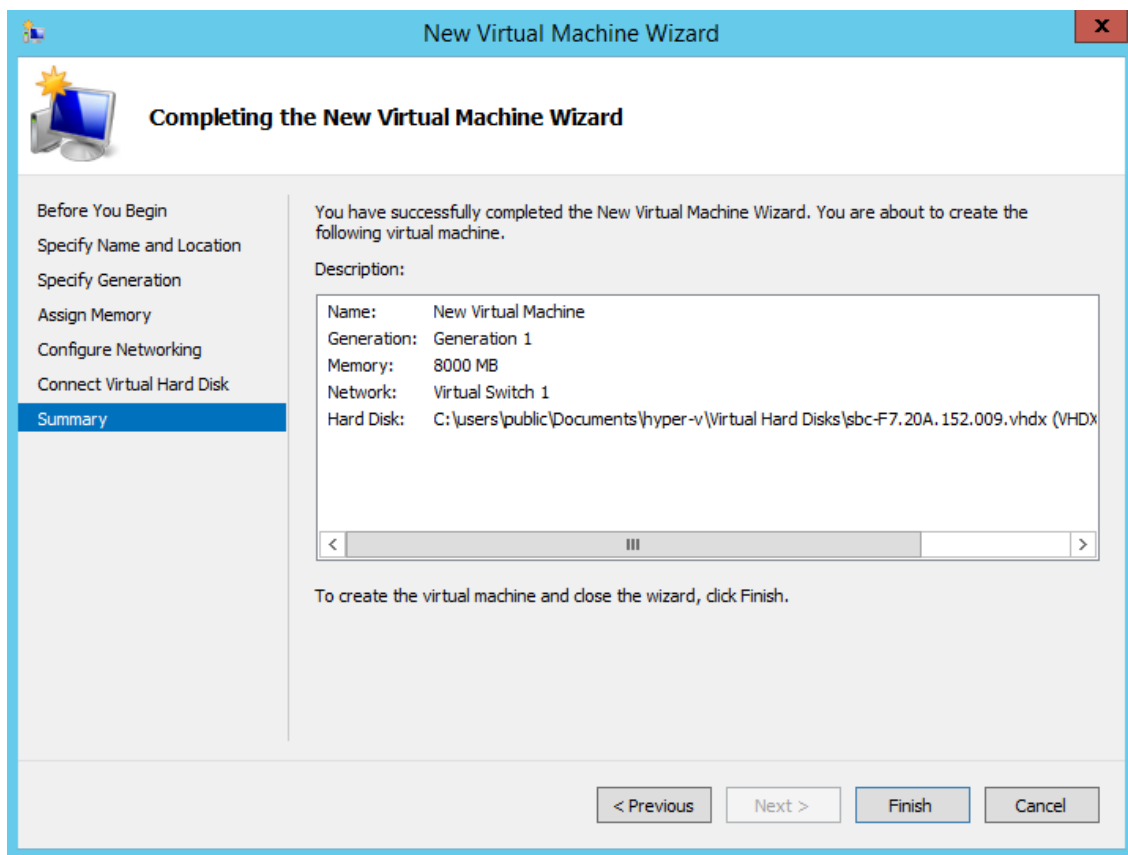
Figure 2-15: New Virtual Machine Wizard: Selecting a Virtual Switch

8. Select the **Use an existing virtual hard disk** option, click **Browse** and select the VHD file, and click **Next**.

Figure 2-16: New Virtual Machine Wizard: Use an existing virtual hard disk | VHD

9. Display the **Summary** describing the virtual machine and click **Finish**.

Figure 2-17: Summary

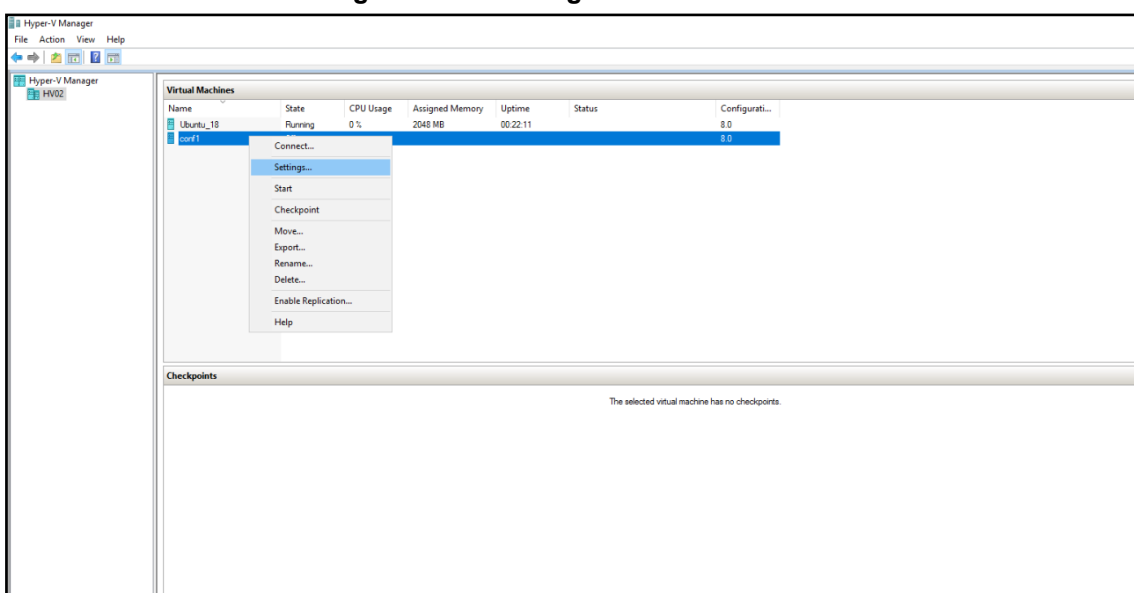


You now need to change the number of CPU cores to **2** in the ARM Router and **4** in the ARM Configurator, for each VM.

➤ **To change the number of CPU cores for each VM:**

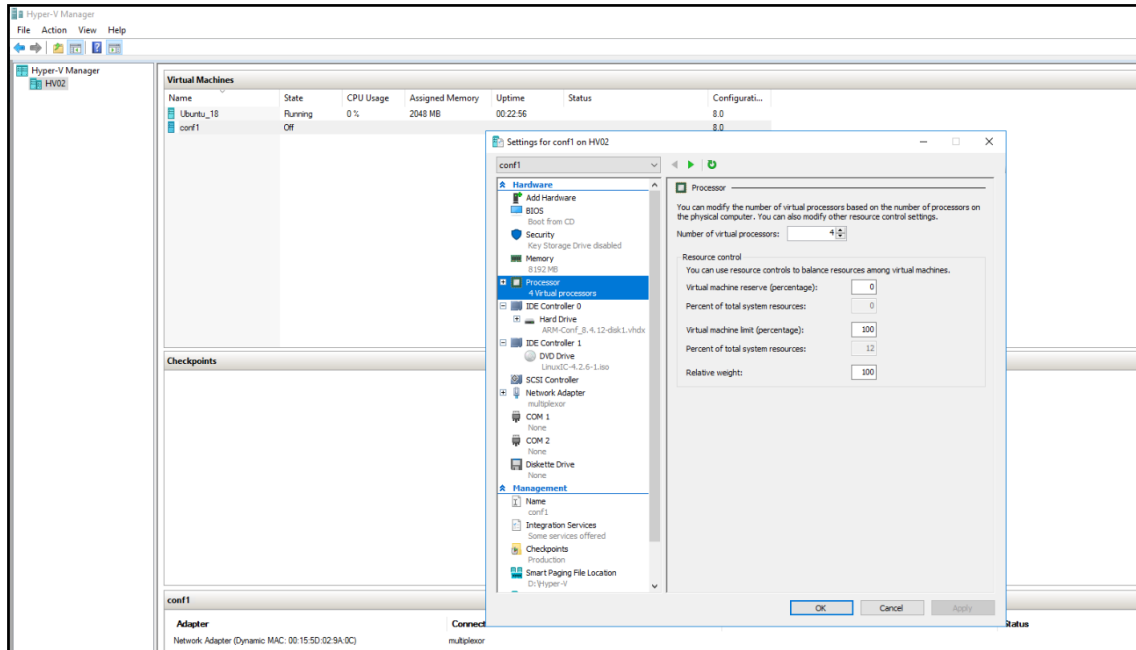
1. In Hyper-V Manager, right-click the VM and from the pop-up menu select **Settings**.

Figure 2-18: Settings



2. Click **Processor** and configure 'Number of virtual processors' to **4** for the Configurator VM, and to **2** for the Router VMs.

Figure 2-19: Processor



3. Click **OK**.

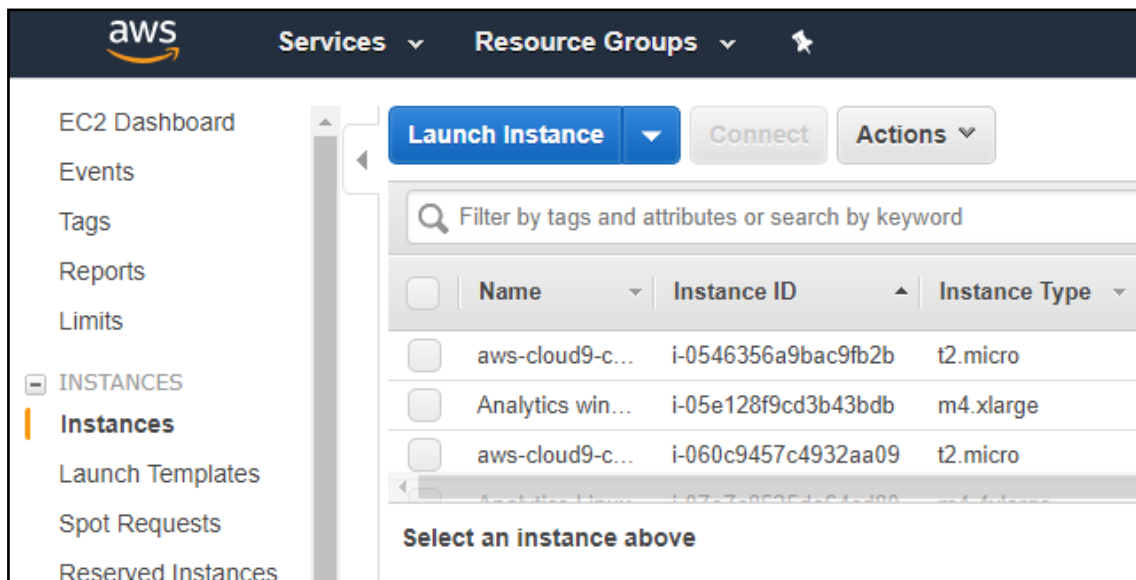
Deploying the ARM's AMIs on AWS

IT managers can deploy the ARM's AMIs (Amazon Machine Images) on Amazon Web Services (AWS).

➤ To deploy the ARM's AMIs on AWS:

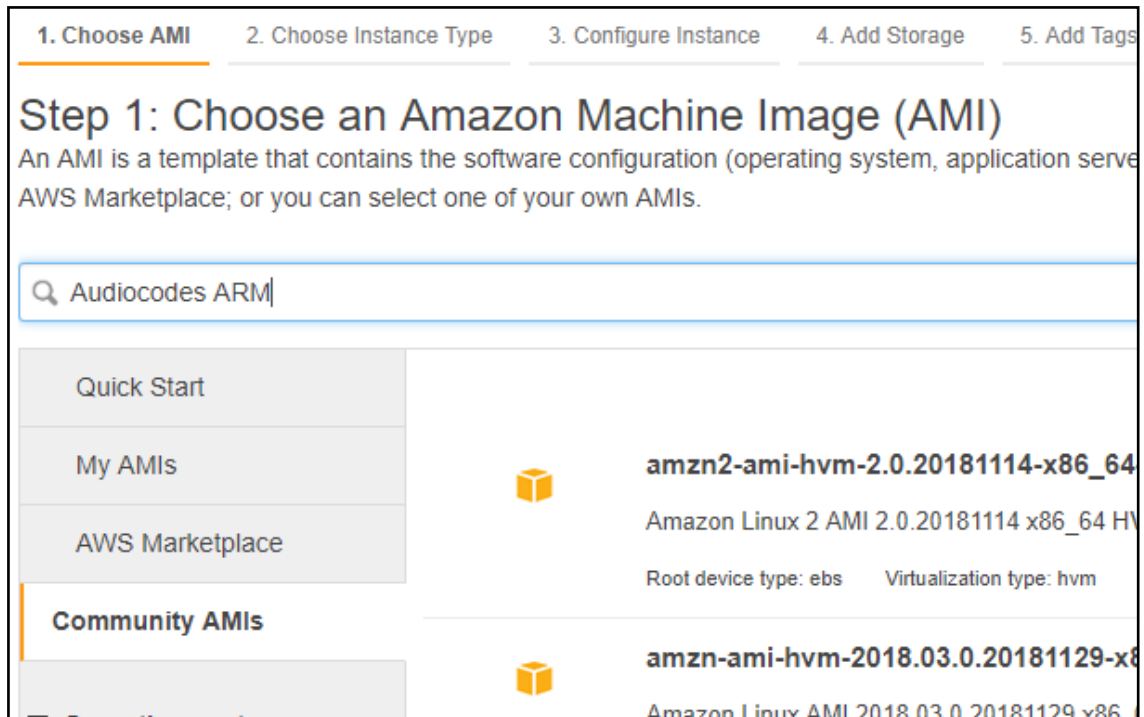
1. In the AWS console EC2, go to **Instances** and click **Launch Instance**.

Figure 2-20: Launch Instance



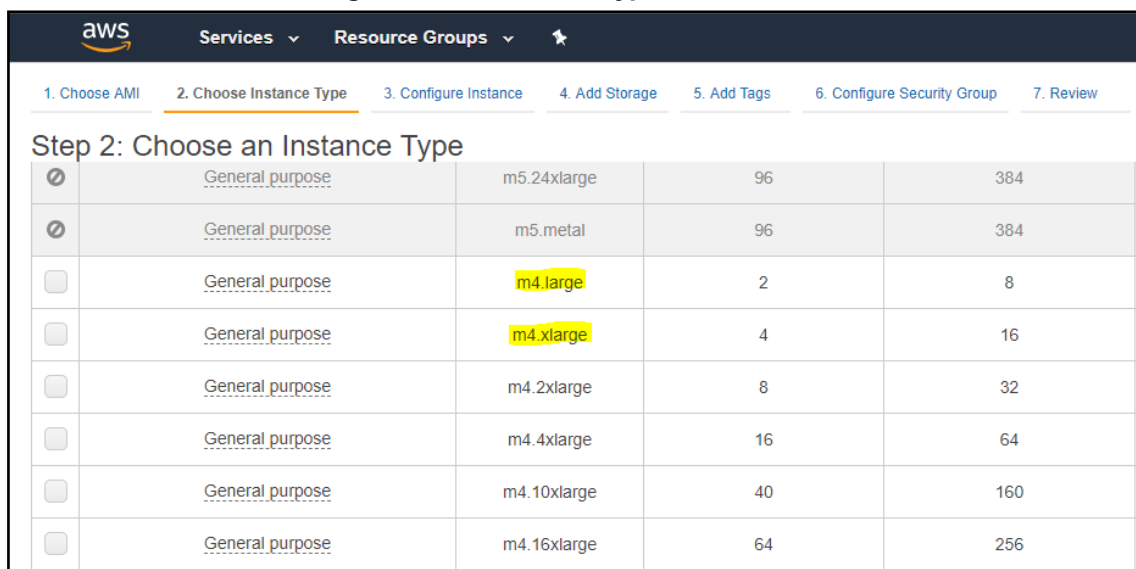
2. Go to the **Community AMIs** tab and in the 'Search' field, enter **Audiocodes ARM**.

Figure 2-21: Community AMIs



3. Select the **ARM configurator** and then the **ARM router** of the correct version.
4. Select **Instance Type**: For Router, select **m4.large** and for configurator, select **m4.xlarge**.

Figure 2-22: Instance Type



5. Select the correct IAM role, network and subnet to suit your network environment and AWS account environment (for more information, see the *AWS documentation*), and then click **Next** three times.

Figure 2-23: Configure Instance Details

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

pricing, assign an access management role to the instance, and more.

Number of instances ⓘ 1 [Launch into Auto Scaling Group](#) ⓘ

Purchasing option ⓘ ☐ Request Spot instances

Network ⓘ vpc-b12d03d8 | c1m (default) [Create new VPC](#)

Subnet ⓘ No preference (default subnet in any Availability Zone) [Create new subnet](#)

Auto-assign Public IP ⓘ Use subnet setting

Placement group ⓘ ☐ Add instance to placement group.

Capacity Reservation ⓘ Open [Create new Capacity Reservation](#)

IAM role ⓘ None [Create new IAM role](#)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

6. Create or select the security group to suit your network environment (for more information, see the *AWS documentation*).

Figure 2-24: Security Group

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☐ Create a new security group ☒ Select an existing security group

Security Group ID	Name	Description
sg-c7e58eac	1-Click SQL Server 2016 Web Edition on Windows 2016-SQL Server 2014 WE Win2016V1-0-7-AutoGenByAWSMP	This security group was generated by AWS Marketplace and is based on recom
sg-b1d41bdb	aws-cloud9-clm-0523b021d2814f31990559e2d22c64c0-InstanceSecurityGroup-10HWL4TUI2U71	Security group for AWS Cloud9 environment aws-cloud9-clm-0523b021d2814f3
sg-d9af81b2	aws-cloud9-clm-11f4ba733e504919a00b7516e4937d2-InstanceSecurityGroup-3S963K0U51ES	Security group for AWS Cloud9 environment aws-cloud9-clm-11f4ba733e504919
sg-3b2a0753	aws-cloud9-clm-1dc4fd0407c341d8ad38c94b193247d9-InstanceSecurityGroup-1UWV4P0LKB96G	Security group for AWS Cloud9 environment aws-cloud9-clm-1dc4fd0407c341d
sg-c39ba2a8	aws-cloud9-Nati-CLM-9f605ac92ad642e4b81578786c1a76ea-InstanceSecurityGroup-FYMEQA828GK	Security group for AWS Cloud9 environment aws-cloud9-Nati-CLM-9f605ac92ac

Inbound rules for sg-b7d57cdf (Selected security groups: sg-b7d57cdf)

Type	Protocol	Port Range	Source	Description
All traffic	All	All	37.142.12.66/32	
All traffic	All	All	195.189.193.1/32	
All traffic	All	All	52.15.247.160/27	
All traffic	All	All	52.15.193.255/32	

[Cancel](#) [Previous](#) [Review and Launch](#)

7. Click **Review and launch**.



All VMs should be in the same virtual private cloud (VPC) and in the same subnet. All VMs should be in a security group that allows all

- outgoing traffic
- incoming traffic from inside the VPC
- incoming SSH, HTTP, HTTPS from any of the enterprise's subnets



Online upgrade of the ARM on AWS is performed in the same way as on VMWare.

➤ To set up High Availability:

Configure auto-recovery in case hardware failure occurs:

1. In the AWS console, go to **EC2** and then **Instances**.

2. Select your ARM VM Instance.
3. Go to the **Status Checks** tab.
4. Click **Create Status Check**.

Figure 2-25: Create Status Check

The screenshot shows the AWS Management Console interface for an EC2 instance. The left sidebar contains navigation links for EC2 Dashboard, Events, Tags, Reports, Limits, INSTANCES, Launch Templates, Spot Requests, Reserved Instances, Dedicated Hosts, Capacity Reservations, IMAGES, AMIs, Bundle Tasks, ELASTIC BLOCK STORE, Volumes, Snapshots, and Lifecycle Manager. The main content area displays a table of instances. The instance 'aws-cloud9-c...' with ID 'i-099cfa673e5239364' is selected. Below the table, the 'Status Checks' tab is active, showing options to 'Create Status Check Alarm' and 'Create Status Check Alarm'. The 'System Status Checks' section indicates that these checks monitor the AWS systems required to use this instance and ensure they are functioning properly.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Stat
aws-cloud9-c...	i-0546356a9bac9fb2b	t2.micro	us-east-2b	stopped		None
Analytics win...	i-05e128f9cd3b43bdb	m4.xlarge	us-east-2b	stopped		None
aws-cloud9-c...	i-060c9457c4932aa09	t2.micro	us-east-2b	stopped		None
Analytics Linux	i-07e7c8525da64cd80	m4.4xlarge	us-east-2b	stopped		None
aws-cloud9-c...	i-099cfa673e5239364	t2.micro	us-east-2c	stopped		None
ubuntu	i-0a3163e59da1117fe	t2.micro	us-east-2a	running	2/2 checks ...	None

Instance: **i-099cfa673e5239364** (aws-cloud9-Nati-CLM-9f605ac92ad642e4b81578786c1a76ea) Private IP: 172.31.35.54

Buttons: **Description**, **Status Checks**, **Monitoring**, **Tags**

Text: Status checks detect problems that may impair this instance from running your applications. [Learn more](#) about status checks.

Button: **Create Status Check Alarm**

Section: **System Status Checks** ⓘ

Text: These checks monitor the AWS systems required to use this instance and ensure they are functioning properly.

Section: **Instance Status Checks** ⓘ

Text: These checks monitor your software and network connectivity.

5. Select the **Take the action** option and then select **Recover this instance**.

Figure 2-26: Take the action > Recover this instance

The screenshot shows the 'Create Alarm' dialog box. It includes a title bar 'Create Alarm' with a close button. The main content area explains that CloudWatch alarms can be used to receive notifications when metric data reaches a defined level. It prompts the user to choose whom to notify and when the notification should be sent. The 'Send a notification to' field is set to 'No SNS topics found...' with a 'create topic' link. The 'Take the action' section has four radio buttons: 'Recover this instance' (selected), 'Stop this instance', 'Terminate this instance', and 'Reboot this instance'. The 'Whenever' section is set to 'Status Check Failed (System)' and 'Is: Failing'. The 'For at least' section is set to '2 consecutive period(s) of 1 Minute'. The 'Name of alarm' field is 'awsec2-i-0a3163e59da1117fe-High-Status-Check'. On the right, there is a graph titled 'Status Check Failed (System) Count' showing a single data point for instance 'i-0a3163e59da1117fe' at a count of 1. The bottom right has 'Cancel' and 'Create Alarm' buttons.

Create Alarm [X]

You can use CloudWatch alarms to be notified automatically whenever metric data reaches a level you define.

To edit an alarm, first choose whom to notify and then define when the notification should be sent.

☒ **Send a notification to:** No SNS topics found... [create topic](#)

☒ **Take the action:**

- ☒ Recover this instance ⓘ
- ☐ Stop this instance ⓘ
- ☐ Terminate this instance ⓘ
- ☐ Reboot this instance ⓘ

Whenever: Status Check Failed (System)

Is: Failing

For at least: 2 consecutive period(s) of 1 Minute

Name of alarm: awsec2-i-0a3163e59da1117fe-High-Status-Check

Status Check Failed (System) Count

Graph showing a single data point for instance i-0a3163e59da1117fe at a count of 1.

Buttons: **Cancel**, **Create Alarm**

6. Click **Create Alarm**.
- Configure auto-reboot in case VM failure occurs:
7. In the AWS console, go to **EC2** and then **Instances**.
8. Select your ARM VM Instance.
9. Go to the **Status Checks** tab.
10. Click **Create Status Check**.

Figure 2-27: Create Status Check

The screenshot shows the AWS Management Console interface. On the left is a navigation menu with categories like EC2 Dashboard, INSTANCES, IMAGES, and ELASTIC BLOCK STORE. The main area displays a table of EC2 instances. One instance, 'aws-cloud9-...', is selected. Below the table, the 'Status Checks' tab is active, showing a 'Create Status Check Alarm' button and information about system and instance status checks.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status
aws-cloud9-c...	i-0546356a9bac9fb2b	t2.micro	us-east-2b	stopped		None
Analytics win...	i-05e128f9cd3b43bdb	m4.xlarge	us-east-2b	stopped		None
aws-cloud9-c...	i-060c9457c4932aa09	t2.micro	us-east-2b	stopped		None
Analytics Linux	i-07e7c8525da64cd80	m4.4xlarge	us-east-2b	stopped		None
aws-cloud9-...	i-099cfa673e5239364	t2.micro	us-east-2c	stopped		None
ubuntu	i-0a3163e59da1117fe	t2.micro	us-east-2a	running	2/2 checks ...	None

Instance: **i-099cfa673e5239364 (aws-cloud9-Nati-CLM-9f605ac92ad642e4b81578786c1a76ea)** Private IP: 172.31.35.54

Buttons: Description, **Status Checks**, Monitoring, Tags

Status checks detect problems that may impair this instance from running your applications. [Learn more](#) about status checks.

Create Status Check Alarm

System Status Checks ⓘ Instance Status Checks ⓘ

These checks monitor the AWS systems required to use this instance and ensure they are functioning properly. These checks monitor your software and network connectivity.

11. Select the **Take the action** option and then select **Reboot this instance**.

12. From the 'Whenever' dropdown, select **Status Check Failed (Instance)**.

Figure 2-28: Create Status Check

The screenshot shows the 'Create Alarm' dialog in AWS CloudWatch. It includes fields for notification, action, and alarm configuration. The 'Take the action' section has 'Reboot this instance' selected. The 'Whenever' dropdown is set to 'Status Check Failed (Any)'. A graph on the right shows the 'Status Check Failed (Any) Count' over time.

Create Alarm

You can use CloudWatch alarms to be notified automatically whenever metric data reaches a level you define.

To edit an alarm, first choose whom to notify and then define when the notification should be sent.

☒ **Send a notification to:** No SNS topics found... [create topic](#)

☒ **Take the action:**

- ☐ Recover this instance ⓘ
- ☐ Stop this instance ⓘ
- ☐ Terminate this instance ⓘ
- ☒ **Reboot this instance ⓘ**

AWS will use the existing Service Linked Role to perform this EC2 action. [Learn more.](#)

AWSServiceRoleForCloudWatchEvents (show IAM policy document)

Whenever: Status Check Failed (Any) ⓘ

Is: Falling

For at least: 2 consecutive period(s) of 1 Minute ⓘ

Name of alarm: awsec2-i-0a3163e59da1117fe-Status-Check-Failed

[Cancel](#) [Create Alarm](#)

Status Check Failed (Any) Count

Graph showing the count of status check failures over time for instance i-0a3163e59da1117fe. The count is 0 for most of the time, with a peak of 1 at 10:00 and 12:00.

13. Click **Create Alarm**.



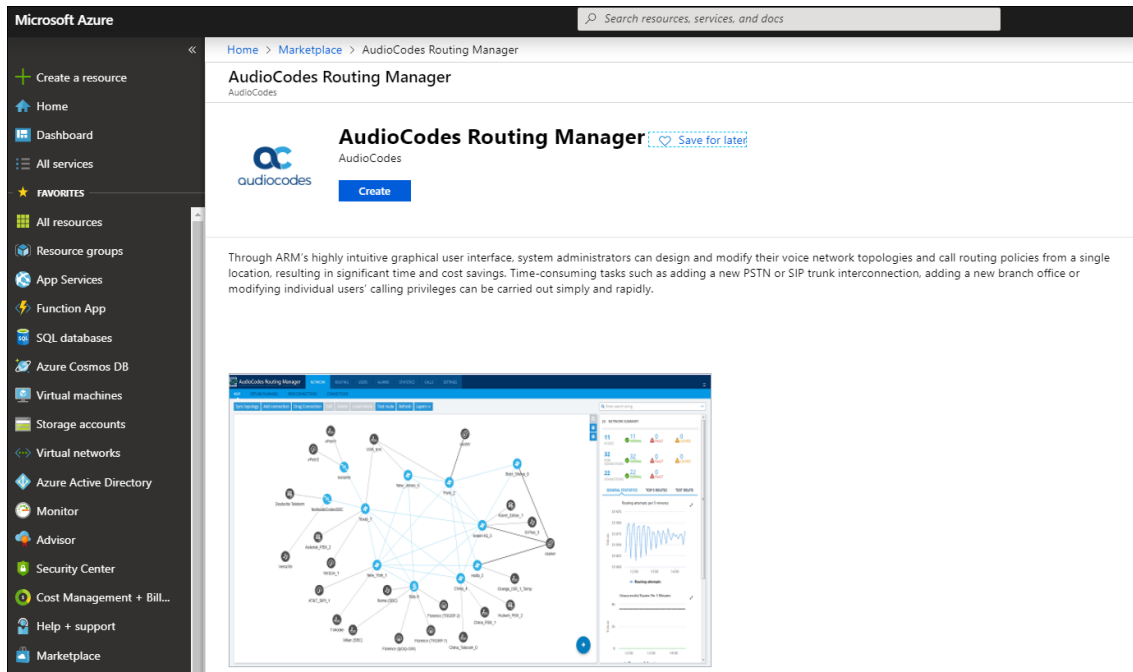
The preceding procedure must be performed for all ARM VM instances.

Deploying the ARM from Microsoft's Azure Marketplace

Network administrators can deploy the ARM from Microsoft's Azure Marketplace. Before deployment, make sure your network meets the requirements detailed in [Azure](#) on page 2.

➤ To deploy the ARM from Microsoft's Azure Marketplace:

1. In your browser, navigate to Microsoft Azure Marketplace and then search for 'AudioCodes Routing Manager'.

Figure 2-29: Microsoft Azure Marketplace - AudioCodes Routing Manager

2. Click the **Create** button. An installation wizard is displayed.

Figure 2-30: Create ARM (1) Basics

Home > Marketplace > AudioCodes Routing Manager > Create AudioCodes Routing Manager > Basics

Create AudioCodes Routing ...

- 1 Basics** > Configure basic settings
- 2 Configurator Settings > Configure virtual machine settings
- 3 First Router Settings > Configure first router settings
- 4 Second Router Settings > Configure second router settings
- 5 Summary > AudioCodes Routing Manager
- 6 Buy >

Basics

* Configurator Virtual Machine name ⓘ
arm-configurator

* User Name ⓘ
arm ✓

* Authentication type ⓘ
☒ Password
 ☐ SSH public key

* Password ⓘ
..... ✓

* Confirm password
..... ✓

Subscription
SBC Lab ▼

* Resource group ⓘ
 (New) arm-europe ▼
[Create new](#)

* Location
(Europe) West Europe ▼

OK

- Configure Step 1, basic settings. Define the name of the Configurator VM **arm-configurator** as shown in the preceding figure. Use the **i** (information) icon for clarification. This VM is one of two routers that must be defined: ARM Configurator and ARM Router.
- Define the name of the Configurator VM user, **arm**, as shown in the preceding figure. Use the **i** (information) icon for clarification.
- For 'Authentication type', select the **SSH public key** option. Use the **i** (information) icon for clarification.
- In the 'Password' and 'Confirm Password' fields, enter the generated RSA SSH key password. Use the **i** (information) icon for clarification.
- From the 'Subscription' drop-down, select **SBC Lab**.
- From the 'Resource Group' drop-down, select the group relevant to you or click **Create new** and define a new one. Use the **i** (information) icon for clarification.

9. From the 'Location' drop-down, select the location relevant to you.
10. Click **OK**.

Figure 2-31: Create ARM (2) Configure virtual machine settings

Home > Marketplace > AudioCodes Routing Manager > Create AudioCodes Routing Manager > Configurator Settings

Create AudioCodes Routing ... ×

Configurator Settings □ ×

- 1 Basics Done ✓
- 2 **Configurator Settings** >
Configure virtual machine settings
- 3 First Router Settings >
Configure first router settings
- 4 Second Router Settings >
Configure second router settings
- 5 Summary >
AudioCodes Routing Manager
- 6 Buy >

* Configurator Virtual machine size ⓘ
1x Standard D4 v3
 4 vcpus, 16 GiB memory
[Change size](#)

* Configurator Public IP Address ⓘ >
 (new) arm-configurator-ip

* Configurator Public DNS Prefix ⓘ
 arm-configurator-e2456e0d85 ✓
 westeurope.cloudapp.azure.com

* Virtual network ⓘ >
 (new) VirtualNetwork

* Subnets ⓘ >
 Review subnet configuration

OK

11. In Step 2 in the wizard, click **Change size** and select **D2s_v3** for Router VMs and **D4s_v3** for Configurator VMs. Use the **i** (information) icon for clarification.
12. Configure the **Configurator Public IP Address**, **Configurator Public DNS Prefix**, **Virtual Network** and **Subnet** according to your organization's network and click **OK**. Use the **i** (information) icon for clarification.



- By default, the ARM uses private IPs but network administrators can opt to change to public IPs. See [Moving from Private IPs to Public IPs](#) on page 42 for more information.
- All VMs should be in the same virtual network and in the same subnet. All VMs should be in a security group that allows all
 - ✓ outgoing traffic
 - ✓ incoming traffic from inside the VPC
 - ✓ incoming SSH, HTTP, HTTPS from any of the enterprise's subnets

Figure 2-32: Create ARM (3) First Router Settings

Home > Marketplace > AudioCodes Routing Manager > Create AudioCodes Routing Manager > First Router Settings

Create AudioCodes Routing ...

- 1 Basics Done ✓
- 2 Configurator Settings Done ✓
- 3 First Router Settings Configure first router settings >
- 4 Second Router Settings Configure second router settings >
- 5 Summary AudioCodes Routing Manager >
- 6 Buy >

First Router Settings

- * First Router Virtual Machine name ⓘ
- * Routers Virtual machine size ⓘ
1x Standard D2 v3
 2 vcpus, 8 GiB memory
[Change size](#)
- * First Router Public IP Address ⓘ >
 (new) router1-ip
- * First Router Public DNS Prefix ⓘ
 ✓
 westeurope.cloudapp.azure.com

OK

13. Define the settings of the first router. Use the i (information) icon for clarifications. Click **OK**.

Figure 2-33: Create ARM (4) Second Router Settings

Home > Marketplace > AudioCodes Routing Manager > Create AudioCodes Routing Manager > Second Router Settings

Create AudioCodes Routing ...

- 1 Basics Done ✓
- 2 Configurator Settings Done ✓
- 3 First Router Settings Done ✓
- 4 Second Router Settings** > Configure second router settings
- 5 Summary > AudioCodes Routing Manager
- 6 Buy >

Second Router Settings

- * Second Router Virtual Machine name ⓘ
- * Second Router Public IP Address ⓘ >
(new) router2-ip
- * Second Router Public DNS Prefix ⓘ
 ✓
westeurope.cloudapp.azure.com

OK

14. Define the settings of the second router. Use the **i** (information) icon for clarifications. Click **OK**.

Figure 2-34: Create ARM (5) Summary

Home > Marketplace > AudioCodes Routing Manager > Create AudioCodes Routing Manager > Summary

Create AudioCodes Routing ...

- 1 Basics Done ✓
- 2 Configurator Settings Done ✓
- 3 First Router Settings Done ✓
- 4 Second Router Settings Done ✓
- 5 Summary AudioCodes Routing Manager >
- 6 Buy >

Summary

Validation passed

Basics	
Subscription	SBC Lab
Resource group	arm-europe
Location	(Europe) West Europe
Configurator Virtual Machine...	
User Name	arm-configurator
Password	*****
Configurator Settings	
Configurator Virtual machine...	Standard D4 v3
Configurator Public IP Address	arm-configurator-ip
Configurator Public DNS Prefix	arm-configurator-e2456e0d85
Virtual network	VirtualNetwork
Subnet	Subnet-1
Subnet address prefix	10.13.0.0/24
First Router Settings	
First Router Virtual Machine ...	router1
Routers Virtual machine size	Standard D2 v3
First Router Public IP Address	router1-ip
First Router Public DNS Prefix	router1-5f65ab96b7
Second Router Settings	
Second Router Virtual Machi...	router2
Second Router Public IP Add...	router2-ip
Second Router Public DNS P...	router2-fa6142ea2a

OK [Download template and parameters](#)

15. Make sure all settings are correct and then click **OK**.



ARM HA (High Availability) is enabled on Azure by default. No additional settings need to be configured.

Figure 2-35: Create ARM (6) Buy

Home > Marketplace > AudioCodes Routing Manager > Create AudioCodes Routing Manager > Create

Create AudioCodes Routing ...

- 1 Basics Done ✓
- 2 Configurator Settings Done ✓
- 3 First Router Settings Done ✓
- 4 Second Router Settings Done ✓
- 5 Summary AudioCodes Routing Manager ✓
- 6 Buy >

Create

AudioCodes Routing Manager
by AudioCodes
[Terms of use](#) | [privacy policy](#)

Deploying this template will result in various actions being performed, which may include the deployment of one or more Azure resources or Marketplace offerings and/or transmission of the information you provided as part of the deployment process to one or more parties, as specified in the template. You are responsible for reviewing the text of the template to determine which actions will be performed and which resources or offerings will be deployed, and for locating and reviewing the pricing and legal terms associated with those resources or offerings.

The legal terms associated with any Marketplace offering may be found in the Azure portal. For pricing information and to determine which offerings may be purchased using monetary commitment funds or subscription credits, please contact your reseller. If any Microsoft products are included in a Marketplace offering (e.g., Windows Server or SQL Server), such products are licensed by Microsoft and not by any third party.

Template deployment is intended for advanced users only. If you are uncertain which actions will be performed by this template, which resources or offerings will be deployed, or what prices or legal terms pertain to those resources or offerings, do not deploy this template.

Terms of use

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) provided above as well as the legal terms and privacy statement(s) associated with each Marketplace offering that will be deployed using this template, if any; and (b) agree that Microsoft may share my contact information and transaction details with any third-party sellers of the offering(s). Microsoft assumes no responsibility for any actions performed by third-party templates and does not provide rights for third-party products or services. See the [Azure Marketplace Terms](#) for additional terms.

☒ I give Microsoft permission to use and share my contact information so that Microsoft or the Provider can contact me regarding this product and related products.

Name:

Create

16. Select the terms permission option and then click **Create**.



Online upgrade of the ARM on Azure is performed in the same way as on VMWare.

Logging

Network administrators can perform logging for debugging and data mining purposes.



Applies only when the ARM is deployed from Microsoft's Azure Marketplace.

- Logging can be performed using Microsoft Azure's 'Serial Console'.
 - You can use root + password.
- Logging can be performed using SSH.
 - Root login is blocked remotely.
 - Use user+password which is configured when creating the VMs.
 - You can then switch to root user with the command "sudo -i" ..

Deploying the ARM through the PowerShell CLI

Enterprise network administrators and ITSP operators can deploy a standalone ARM through the Azure PowerShell CLI. This deployment method provides maximum flexibility and is therefore most suited for advanced Azure users who want to exercise full control over their deployment.

Here's the procedure you need to follow to deploy the ARM through the PowerShell CLI:

1. Install the Azure PowerShell CLI (see [Installing the Azure PowerShell CLI](#) below)
2. Deploy the ARM environment:
 - ARM Configurator (see [Deploying the ARM Environment - ARM Configurator](#) below)
 - ARM Routers (see [Deploying the ARM Environment - ARM Routers](#) on page 29)
3. Delete the ARM if necessary (see [Deleting the ARM Deployed through the PowerShell CLI](#) on page 32)

Installing the Azure PowerShell CLI

Before you can use the Azure PowerShell CLI to deploy the ARM, you need to install it.

➤ To install the Azure PowerShell CLI:

1. Run PowerShell with Administrator privileges.
2. Use the following commands to install the Azure PowerShell CLI:

```
Install-Module PowerShellGet -Force
Install-Module -Name AzureRM -AllowClobber
```

Deploying the ARM Environment - ARM Configurator

After installing the Azure PowerShell CLI as shown in [Installing the Azure PowerShell CLI](#) above, you can deploy the ARM environment, namely, the ARM Configurator and the ARM Routers.

Here's how to deploy the ARM Configurator.

➤ To deploy the ARM Configurator:

1. Run PowerShell with Administrator privileges.
2. Set the correct execution policy:

```
Set-ExecutionPolicy remoteSigned
```

3. Sign in to your Azure account:

```
Login-AzureRmAccount
```

4. Select the appropriate subscription if multiple subscriptions exist:

```
Select-AzureRmSubscription -SubscriptionName "<Name>"
```

5. Get the parameters of the preconfigured virtual network and subnet:

```
$VNetResourceGroupName = "ArmCliResourceGroup"
$VNetName = "ArmCliVNetName"
$SubnetName = "ArmCliSubnetName"
$MyNSG = "arm-nsg"
$VNet = Get-AzureRMVirtualNetwork -Name $VNetName
-ResourceGroupName $VNetResourceGroupName
```



```
$Subnet = Get-AzureRMVirtualNetworkSubnetConfig
-Name $SubnetName -VirtualNetwork $VNet
```

6. Create a new Resource Group:

```
$ArmName = "armsolution"
$Location = "WestEurope"
$ResourceGroupName = $ArmName + "-rg"
$ArmResourceGroup = New-AzureRmResourceGroup
-Name $ResourceGroupName -Location $Location
```

7. Create a new Configurator Virtual Machine configuration:

```
$VMConfiguratorName = $ArmName + "-configurator"
$VMConfiguratorSize = "Standard_D4s_v3"
$ConfiguratorVM = New-AzureRMVMConfig
-VMName $VMConfiguratorName
-VMSize $VMConfiguratorSize
```

8. Create a new public IP address:

```
$randomDnsPrefix = -join ((97..122) | Get-Random -Count 10 | % {[char]$_})
$dnsPrefix = $ArmName + "-" + $randomDnsPrefix + "-configurator"
$ConfiguratorPublicIPName = $VMConfiguratorName + "-PublicIP"
$ConfiguratorPublicIP = New-AzureRmPublicIpAddress -Name
$ConfiguratorPublicIPName -ResourceGroupName
$ResourceGroupName -DomainNameLabel $dnsPrefix
-Location $Location -AllocationMethod Static -Sku Standard
```

9. Create the first Network Interface:

```
$InterfaceName = $VMConfiguratorName + "-ni"
$Interface = New-AzureRmNetworkInterface -Name $InterfaceName
-ResourceGroupName $ResourceGroupName -Location $Location
-SubnetId $Subnet.id -PublicIpAddressId
$ConfiguratorPublicIP.id
Add-AzureRmVMNetworkInterface -VM $ConfiguratorVM
-Id $Interface.id -Primary
```

10. Set an existing Network Security Group (NSG):

```
$nic = Get-AzureRmNetworkInterface -ResourceGroupName
$ResourceGroupName -Name $InterfaceName
$nsg = Get-AzureRmNetworkSecurityGroup -ResourceGroupName
$VNetResourceGroupName -Name $MyNSG
$nic.NetworkSecurityGroup = $nsg
$nic | Set-AzureRmNetworkInterface
```

11. Configure the source image:

```
Set-AzureRmVMSourceImage -VM $ConfiguratorVM
-PublisherName audiocodes -Offer audiocodesarmforazure
-Skus audiocodes_arm_for_azure_sku_configurator
-Version latest
Set-AzureRmVMPlan -VM $ConfiguratorVM
```

```
-Name audiocodes_arm_for_azure_sku_configurator
-Publisher audiocodes -Product audiocodesarmforazure
```

12. Configure the managed disk:

```
$DiskSize = "40"
$DiskName = $VMConfiguratorName + "-Disk"
Set-AzureRmVMOSDisk -VM $ConfiguratorVM -Name $DiskName
-DiskSizeInGB $DiskSize -CreateOption fromImage -Linux
```

13. Configure the Admin User credentials:

```
$AdminUsername = "arm"
$AdminPassword = "Admin#123456"
$Credential = New-Object PSCredential $AdminUsername,
($AdminPassword | ConvertTo-SecureString -AsPlainText -Force)
Set-AzureRmVMOperatingSystem -VM $ConfiguratorVM -Linux
-ComputerName $VMConfiguratorName -Credential $Credential
```

14. Create the new Virtual Machine:

```
New-AzureRMVM -ResourceGroupName $ResourceGroupName
-Location $Location -VM $ConfiguratorVM
```

15. Find the public IP address of the new Configurator instance:

```
Get-AzureRmPublicIpAddress -Name $ConfiguratorPublicIPName
-ResourceGroupName $ResourceGroupName
```

16. Use this IP address to connect to the Configurator management interface through the Web interface or SSH.

Deploying the ARM Environment - ARM Routers

After installing the Azure PowerShell CLI as shown in [Installing the Azure PowerShell CLI](#) on page 27, you can deploy the ARM environment, namely, the ARM Configurator as shown in [Deploying the ARM Environment - ARM Configurator](#) on page 27 and the ARM Routers. Here's how to deploy the ARM Routers.

➤ To deploy the ARM Routers:

1. Run PowerShell with Administrator privileges. Skip to step 7 if you just created the ARM Configurator (using the same PowerShell window).
2. Set the correct execution policy:

```
Set-ExecutionPolicy remoteSigned
```

3. Sign in to your Azure account:

```
Login-AzureRmAccount
```

4. Select the appropriate subscription if multiple subscriptions exist:

```
Select-AzureRmSubscription -SubscriptionName "<Name>"
```

5. Get the parameters of the **preconfigured** virtual network and subnet:

```
$VNetResourceGroupName = "ArmCliResourceGroup"
$VNetName = "ArmCliVNetName"
$SubnetName = "ArmCliSubnetName"
$MyNSG = "arm-nsg"
$VNet = Get-AzureRMVirtualNetwork -Name $VNetName
-ResourceGroupName $VNetResourceGroupName
$Subnet = Get-AzureRMVirtualNetworkSubnetConfig
-Name $SubnetName -VirtualNetwork $VNet
```

6. Get the Resource Group:

```
$ArmName = "armsolution"
$Location = "WestEurope"
$ResourceGroupName = $ArmName + "-rg"
$ArmResourceGroup = Get-AzureRmResourceGroup
-Name $ResourceGroupName -Location $Location
```

7. Create a new Availability Set:

```
$RouterAvailabilitySetName = $ResourceGroupName + "-as"
```

For the first Router:

```
$AvailabilitySetObj = New-AzureRmAvailabilitySet -ResourceGroupName
$ResourceGroupName -Name $RouterAvailabilitySetName -Location $Location
-Sku Aligned -PlatformFaultDomainCount 2 -PlatformUpdateDomainCount 5
```

For all the remaining Routers:

```
$AvailabilitySetObj = Get-AzureRmAvailabilitySet
-ResourceGroupName $ResourceGroupName
-Name $RouterAvailabilitySetName
```

8. Create the new Router Virtual Machine configuration:

```
$VMRouterNumber = "1" // or 2 ....
$VMRouterName = $ArmName + "-router-" + $VMRouterNumber
$VMRouterSize = "Standard_D2s_v3"
$RouterVM = New-AzureRMVMConfig
-VMName $VMRouterName
-VMSize $VMRouterSize
```

9. Create the new public IP address:

```
$randomDnsPrefix = -join ((97..122) | Get-Random -Count 10 | % {[char]$_})
$dnsPrefix = $ArmName + "-" + $randomDnsPrefix + "-router-" + $VMRouterNumber
$RouterPublicIPName = $VMRouterName + "-PublicIP"
$RouterPublicIP = New-AzureRmPublicIpAddress -Name
$RouterPublicIPName -ResourceGroupName
$ResourceGroupName -DomainNameLabel $dnsPrefix
-Location $Location -AllocationMethod Static -Sku Standard
```

10. Create the first network interface:

```
$InterfaceName = $VMRouterName + "-ni"
$Interface = New-AzureRmNetworkInterface -Name $InterfaceName
-ResourceGroupName $ResourceGroupName -Location $Location
-SubnetId $Subnet.id -PublicIpAddressId
$RouterPublicIP.id
Add-AzureRmVMNetworkInterface -VM $RouterVM
-Id $Interface.Id -Primary
```

11. Set an existing NSG:

```
$nic = Get-AzureRmNetworkInterface -ResourceGroupName
$ResourceGroupName -Name $InterfaceName
$nsg=Get-AzureRmNetworkSecurityGroup -ResourceGroupName
$VNetResourceGroupName -Name $MyNSG
$nic.NetworkSecurityGroup = $nsg
$nic | Set-AzureRmNetworkInterface
```

12. Configure the source image:

```
Set-AzureRmVMSourceImage -VM $RouterVM
-PublisherName audiocodes -Offer audiocodesarmforazure
-Skus audiocodes_arm_for_azure_sku_router
-Version latest
Set-AzureRmVMPlan -VM $RouterVM
-Name audiocodes_arm_for_azure_sku_router
-Publisher audiocodes -Product audiocodesarmforazure
```

13. Configure the managed disk:

```
$DiskSize = "40"
$DiskName = $VMRouterName + "-Disk"
Set-AzureRmVMOSDisk -VM $RouterVM -Name $DiskName
-DiskSizeInGB $DiskSize -CreateOption fromImage -Linux
```

14. Configure the Admin User credentials:

```
$AdminUsername = "arm"
$AdminPassword = "Admin#123456"
$Credential = New-Object PSCredential $AdminUsername,
($AdminPassword | ConvertTo-SecureString -AsPlainText -Force)
Set-AzureRmVMOperatingSystem -VM $RouterVM -Linux
-ComputerName $VMRouterName -Credential $Credential
```

15. Create the new Virtual Machine:

```
New-AzureRMVM -ResourceGroupName $ResourceGroupName
-Location $Location -VM $RouterVM
```

16. Find the public IP address of the new Mediant VE instance:

```
Get-AzureRmPublicIpAddress -Name $RouterPublicIPName
-ResourceGroupName $ResourceGroupName
```

17. Use this IP address to connect to the Router management interface through the Web interface or SSH.

Deleting the ARM Deployed through the PowerShell CLI

After deploying the ARM through the PowerShell CLI, you can opt to delete it if necessary.

- To delete the ARM deployed through the PowerShell CLI, simply delete the corresponding Resource Group:

```
Remove-AzureRmResourceGroup -Name $ResourceGroupName
```

3 Performing Initial Configuration

IT managers can perform initial configuration via an SSH connection to the Configurator VM and to the Router VM.

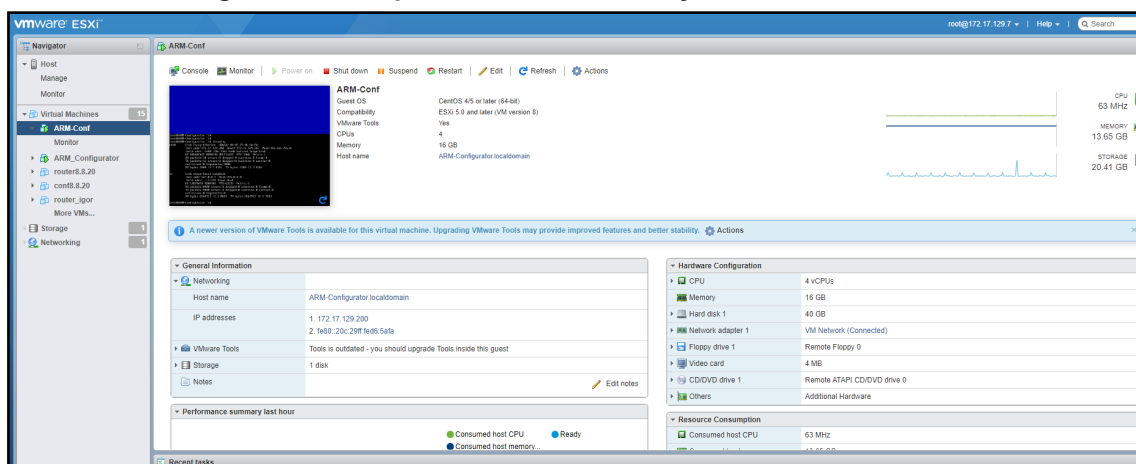
Initial configuration involves configuration of a static IP address and hostname for the VM.

Configure a Static IP Address and Hostname for the VM

The newly deployed VM (Topology Manager VM or Routing Manager VM) is by default configured with DHCP client enabled, so if your network includes a DHCP server, the VM will be configured with a dynamic IP address when powering up.

View the VM's IP address in the VSphere client's Summary screen.

Figure 3-1: VSphere Client's Summary Screen



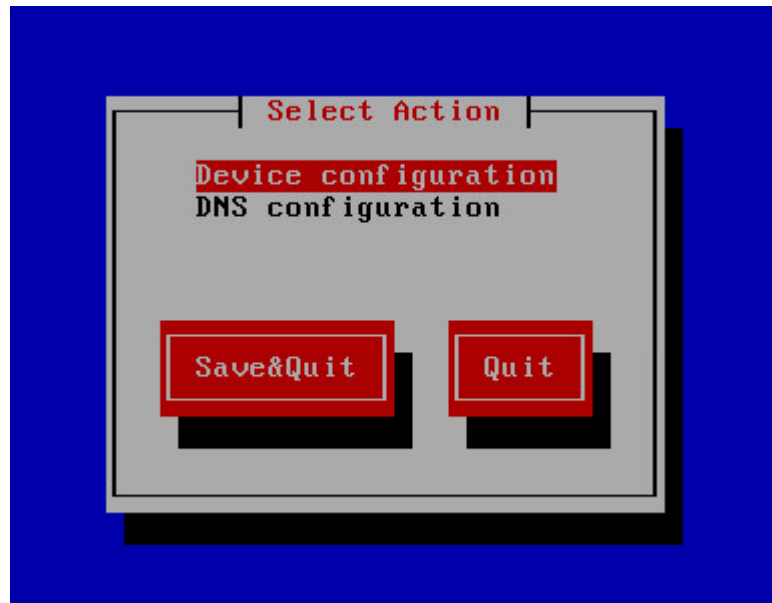
➤ To configure a static IP address and hostname for the VM:

1. Access the VM via either
 - a. SSH, the dynamic IP address of the VM, described above.
 - b. VMware virtual console
2. Log in to the VM: define **root** for username and **password** for password.
3. Run this command:

```
system-config-network-tui
```

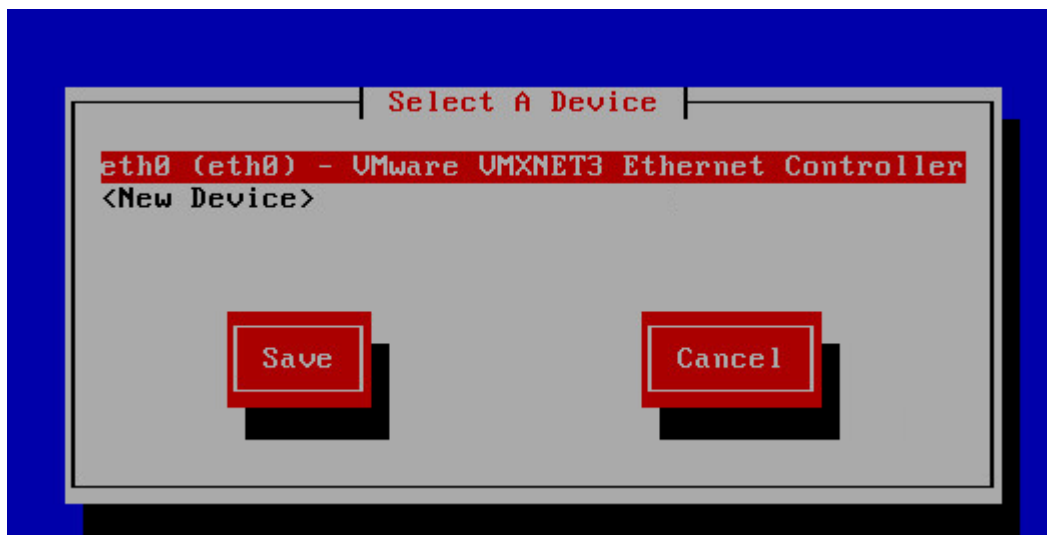
4. You're prompted for a Text User Interface.
5. Select **Device Configuration**.

Figure 3-2: Device Configuration



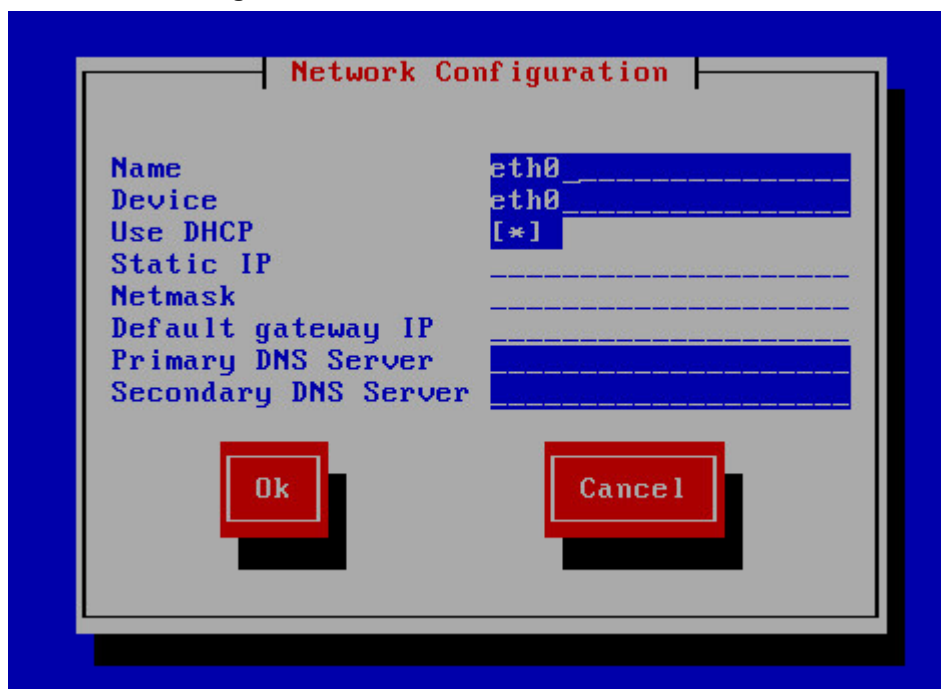
6. Select **eth0**.

Figure 3-3: eth0



7. Change to static IP address: use the Tab key to navigate between fields and the space key to select. Enter a new static IP address, Netmask, Default Gateway, and DNS Servers.

Figure 3-4: Static IP Address

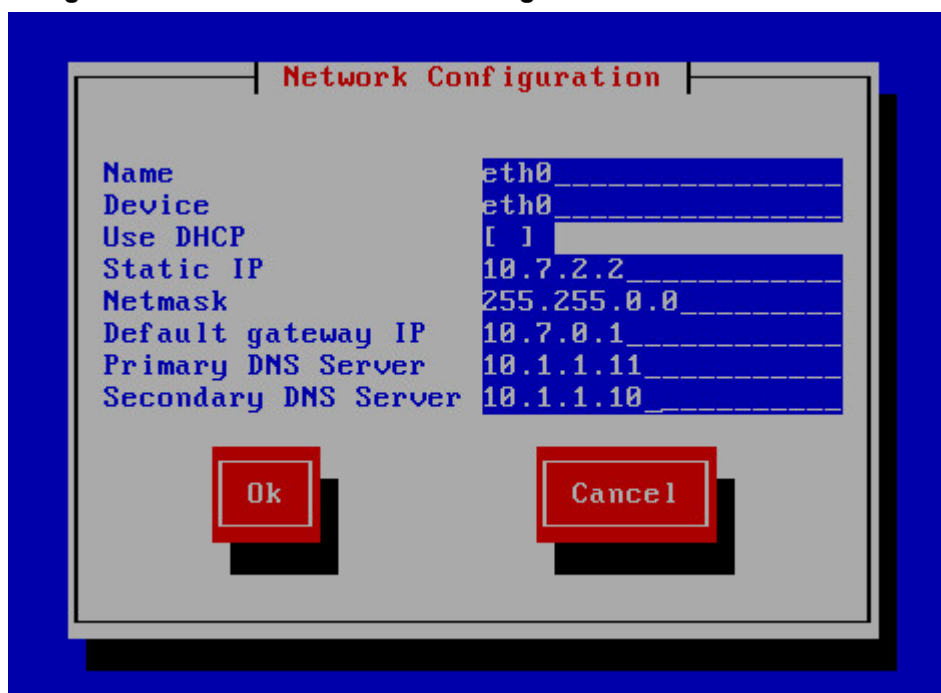


The image shows a 'Network Configuration' dialog box with a blue border. Inside, there is a list of configuration options on the left and corresponding input fields on the right. The options are: Name, Device, Use DHCP, Static IP, Netmask, Default gateway IP, Primary DNS Server, and Secondary DNS Server. The input fields are: 'eth0' for Name and Device, '[*]' for Use DHCP, and empty fields for Static IP, Netmask, Default gateway IP, Primary DNS Server, and Secondary DNS Server. At the bottom, there are two red buttons: 'Ok' and 'Cancel'.

Field	Value
Name	eth0
Device	eth0
Use DHCP	[*]
Static IP	
Netmask	
Default gateway IP	
Primary DNS Server	
Secondary DNS Server	

Use the following figure as a configuration reference.

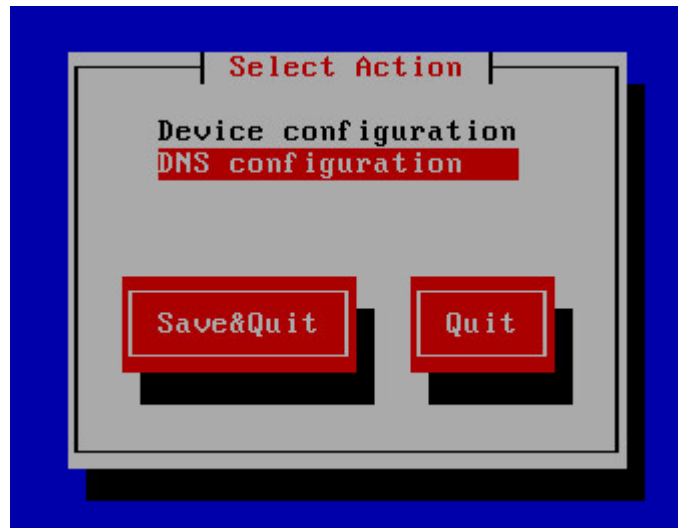
Figure 3-5: Static IP Address – Configuration Reference



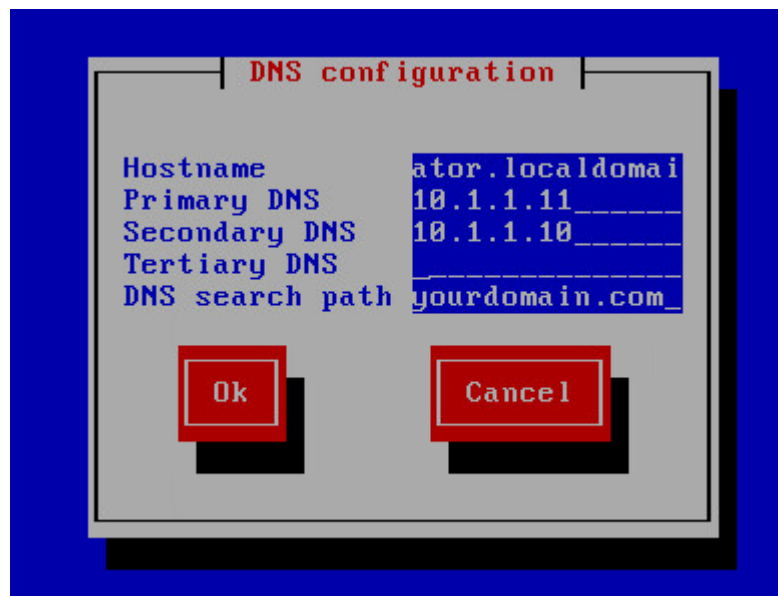
The image shows a 'Network Configuration' dialog box with a blue border. Inside, there is a list of configuration options on the left and corresponding input fields on the right. The options are: Name, Device, Use DHCP, Static IP, Netmask, Default gateway IP, Primary DNS Server, and Secondary DNS Server. The input fields are: 'eth0' for Name and Device, '[1]' for Use DHCP, '10.7.2.2' for Static IP, '255.255.0.0' for Netmask, '10.7.0.1' for Default gateway IP, '10.1.1.11' for Primary DNS Server, and '10.1.1.10' for Secondary DNS Server. At the bottom, there are two red buttons: 'Ok' and 'Cancel'.

Field	Value
Name	eth0
Device	eth0
Use DHCP	[1]
Static IP	10.7.2.2
Netmask	255.255.0.0
Default gateway IP	10.7.0.1
Primary DNS Server	10.1.1.11
Secondary DNS Server	10.1.1.10

8. Select **OK** and then in the next screen, select **Save**.
9. Select DNS Configuration.

Table 3-1: DNS Configuration

10. Enter a new hostname, for example, **ARM-Router1.yourdomain.com**
Default hostnames:
 - **ARM-Configurator.localdomain** for the Topology Manager VM
 - **ARM-Router.localdomain** for the Routing Manager VM
11. Make sure all other DNS fields are configured correctly.

Figure 3-6: DNS Configuration

12. Select **OK** and then in the next screen, select **Save&Quit** to exit the Text User Interface.
13. Enter the command

```
hostname <your new hostname>
```

14. For example:

```
hostname ARM-Router1.yourdomain.com
```



The next step disconnects your SSH connection to this VM. You'll need to reconnect later to the new static IP address.

15. For the changes to take effect, reboot the VM:

```
reboot
```

16. Wait for the machine to come up after the reboot, and then reopen the SSH session/console.

17. Verify the new hostname; enter these commands:

```
# hostname  
# dnsdomainname
```

Licensing

The ARM must be licensed with a valid license for the product to become fully operational. License policy is based on a detailed breakdown for the ARM license model, including the following aspects of ARM functionality and capacity:

- Expiration Date
- Number of Sessions
- Number of Users
- Number of Routing Rules
- Tune Based Routing (can be either enabled or disabled)
- Quality Based Routing (can be either enabled or disabled)
- Test Route (can be either enabled or disabled)
- Network Planner (can be either enabled or disabled)
- Policy Studio (can be either enabled or disabled)

Information about the license applied to your ARM can be viewed in the ARM GUI's 'License Details' page (**Settings > License**) (see the *User's Manual* for more information).

➤ To activate a license:

1. Run the ARM GUI. Log in using the default username **Operator** and password **Operator** and then open the License page (**Settings** menu > **Administration** > **License** tab) shown in the following figure.

Figure 3-7: License

2. Select and copy the 'Machine ID' shown in red in the preceding figure.
3. Activate the product through the AudioCodes License Activation tool at <https://www.audiocodes.com/swactivation>. You'll need your Product Key and the Server Machine ID for the activation process. An email will subsequently be sent to you with your Product License.
4. Copy and paste the Product License string that AudioCodes sends you into the 'License Key' field, indicated in blue in the preceding figure, and then click **Submit**; the number of sessions purchased and the license expiry date are displayed.
5. Make sure the license details (the number of sessions purchased and the license's expiry date) are those that you purchased.

Changing an Existing Configurator's IP Address



When changing the IP address of an existing configurator that has existing routers configured, the existing routers will not move to the new configurator's IP address. You need to remove the existing routers and then add them again, as shown in [Defining Routing Servers](#) below.

Defining Routing Servers

You need to define Routing Servers in the ARM GUI. Before doing so, it's recommended to see *Getting Acquainted with the ARM GUI* in the *ARM User's Manual*.

➤ To define a Routing Server:

1. In the ARM GUI, open the Routing Servers page (**Settings > Routing Servers > Servers**).

Figure 3-8: Routing Servers

SERVERS		Routing servers					
GROUPS		Add Edit Delete Lock/Unlock Refresh					
		STATUS	ADMINISTRATIVE STATE	NAME	ADDRESS	PORT	NODE PROTOCOL
		✓	🔒	router2	172.17.129.32	443	https
		✓	🔒	router1	172.17.129.31	443	https
		Nodes: Israel-HQ_3, New_Jersey_6, China_4, New_York_1, Paris_2, Beer_Sheva_8, Haifa_5, Italy_9, Texas_7					
		Nodes: Israel-HQ_3, Beer_Sheva_8, Italy_9, China_4, Paris_2, Haifa_5, New_York_1, New_Jersey_6, Texas_7					

2. Click **Add**.

Figure 3-9: Add Server

ADD SERVER

Name *

Address *

Port

443

Protocol

https

Credentials ▼

OK

Close

3. Configure the Routing Server VM to connect to the device.
4. Point the Routing Server to the VM's IP address or Host name.

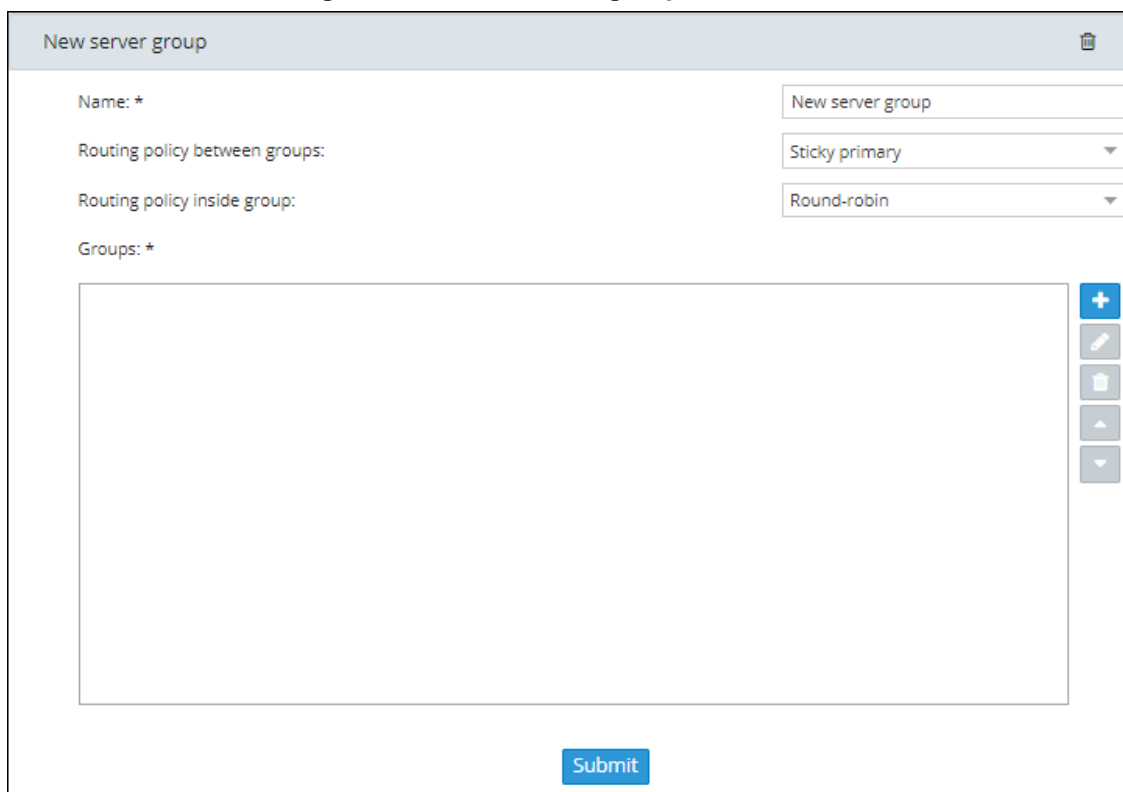
➤ **To define a Routing Server Group:**

1. In the ARM GUI, open the Routing Servers page (**Settings > Routing Servers**) and then click **Groups**.

Figure 3-10: Routing Server Groups

SERVERS		Routing server groups	
GROUPS		Add Refresh	
		group of node New_York_1	🗑️ ▼
		group of node New_Jersey_6	🗑️ ▼
		router1	🗑️ ▼

2. Click **Add**.

Figure 3-11: New server group

The screenshot shows a web-based configuration interface for creating a new server group. The window has a title bar 'New server group' with a close button. The main area contains several fields and a list container. The 'Name' field is required (marked with an asterisk) and contains the text 'New server group'. The 'Routing policy between groups' dropdown is set to 'Sticky primary'. The 'Routing policy inside group' dropdown is set to 'Round-robin'. The 'Groups' field is also required (marked with an asterisk) and contains an empty list. To the right of the list is a vertical toolbar with five icons: a blue plus sign, a pencil, a trash can, an up arrow, and a down arrow. A blue 'Submit' button is located at the bottom right of the form.

New server group

Name: * New server group

Routing policy between groups: Sticky primary

Routing policy inside group: Round-robin

Groups: *

Submit

3. Click  to select Routing Servers to add to the group.

4 Network Guidelines: ARM in the Public Cloud

Introduction

The ARM comprises two components:

- Configurator – a single Virtual Machine (VM)
- Router – a number load shared VMs

The ARM requires the following network connectivity:

- HTTPS between the configurator and all the routers
- Java Message Service (JMS) between the configurator and the routers
- NTP between the configurator and the routers
- Incoming HTTPS on an external IP address on the configurator for access to the GUI
- Incoming SSH on an external IP address on all ARM VMs for access to the command line for collecting logs, upgrade and backup and restore, etc.
- HTTPS between the configurator and the nodes
- HTTPS between the routers and the nodes
- LDAP between the configurator and the organization's Active Directory
- NTP between the configurator and an NTP server
- Outgoing SNMP traps to network management server

Public or Private IPs

There are two main ways to configure your network:

- Using private IPs: There is a VPN between all of your local networks, and the cloud network, or all of the network elements (ARM VMs, SBCs, etc.) are in the cloud, in the same VPC.
- Using public IPs or FQDN to connect over the internet: There are network elements that are on-premises, and there is no VPN connection between them and the VPC.

Private IP

Each VM gets a private IP from the cloud provider. Use the ARM router's private IP when configuring the ARM routers in the ARM routers table. Use the SBC's private IP when adding an SBC in the ARM network view. Follow the instructions in [Security Group Configuration](#) on page 45.

Public IP / FQDN

Obtain a permanent (elastic) external IP address for each VM. Use the ARM router's public IP or FQND when configuring the ARM routers in the ARM routers table. Use the SBC's public IP or FQND when adding an SBC in the ARM network view.

➤ To configure:

1. In the ARM GUI, open the Security page (**Settings > Administration > Security**).

Figure 4-1: Security

Navigation	Section	Field	Value	
LICENSE SECURITY OPERATORS NODE CREDENTIALS ROUTER CREDENTIALS CONFIGURATOR CREDENTIALS LDAP AUTHENTICATION RADIUS AUTHENTICATION REMOTE MANAGER CERTIFICATES	SECURITY	Session timeout (hours):	2	
		Inactivity period (minutes):	120	
		http/https enabled:	<input checked="" type="checkbox"/>	
	* These changes will take place after logout			
	ARM CONFIGURATION	ARM IP Address	172.17.133.7	
		ARM Hostname	arm7.corp.audiocodes.com	
		Communication method	Hostname Based	
	CERTIFICATE VERIFICATION	Verify certificate when ARM performs https requests	<input type="checkbox"/>	

2. Paste the FQND of the ARM configurator in the 'ARM Hostname' field under the ARM Configuration page section.
3. Set the 'Communication method' to **Hostname Based**.

Moving from Private IPs to Public IPs

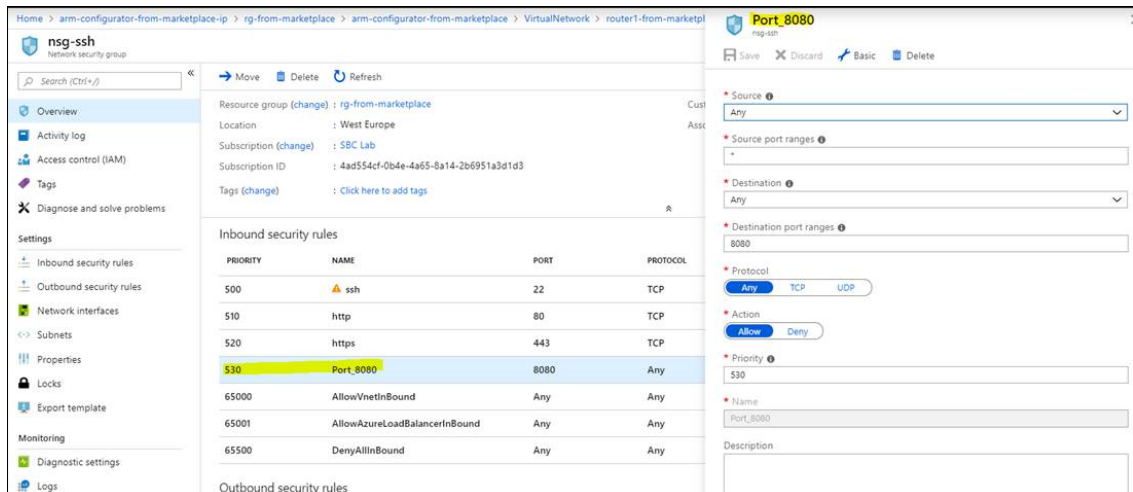


Applies only to the ARM in Microsoft's Azure Marketplace.

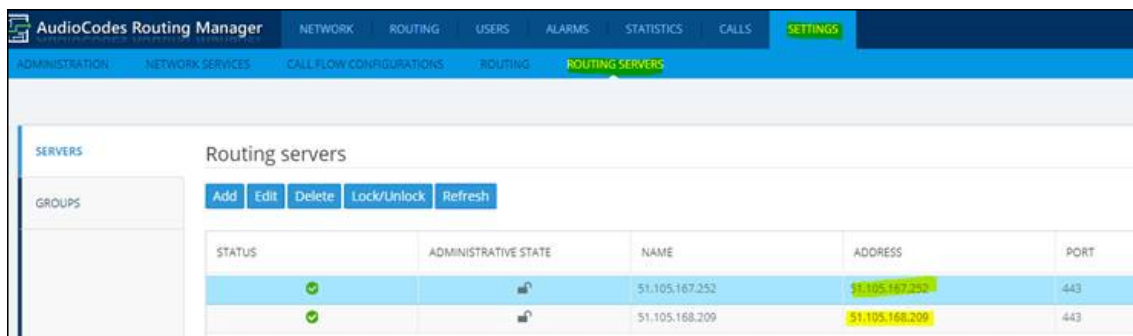
In Microsoft's Azure Marketplace, the ARM by default uses private IPs but network administrators can opt to move to public IPs.

➤ To move to public IPs:

1. In Microsoft's Azure Marketplace, add to 'Network security group' for incoming port 8080.

Figure 4-2: Microsoft's Azure Marketplace 'Network security group'

2. In the ARM GUI, open the 'Routing servers' page (**Settings > Routing Servers > Servers**) and configure routers with a Public IP address/ DNS name.

Figure 4-3: Routing servers page

3. In the 'Security' page of the ARM, configure the parameter 'ARM Hostname' to the Configurator **Public IP address / DNS name** and 'Communication method' to **Hostname Based**.

Figure 4-4: Security page

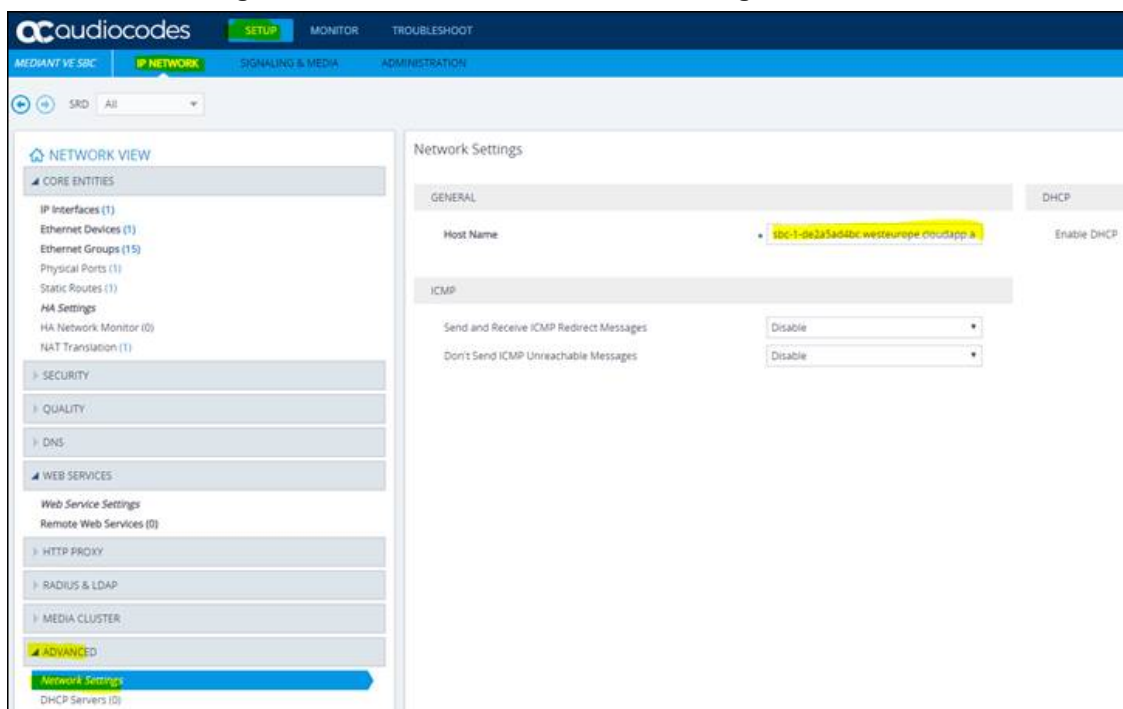
The screenshot shows the 'Security' page in the AudioCodes Routing Manager. The left sidebar contains a menu with 'SECURITY' highlighted. The main content area is divided into three sections: 'SECURITY', 'ARM CONFIGURATION', and 'CERTIFICATE VERIFICATION'. In the 'SECURITY' section, 'Session timeout (hours)' and 'Inactivity period (minutes)' are both set to '5', and 'http/https enabled' is checked. A note states '* These changes will take place after logout'. The 'ARM CONFIGURATION' section shows 'ARM IP Address' as '10.6.0.4', 'ARM Hostname' as '51.105.163.52', and 'Communication method' as 'Hostname Based'. The 'CERTIFICATE VERIFICATION' section has two unchecked checkboxes for verifying certificates. A 'Submit' button is located at the bottom right.

- When adding a node, select **Hostname** in the Add Node screen in the ARM GUI.

Figure 4-5: Hostname in the Add Node screen

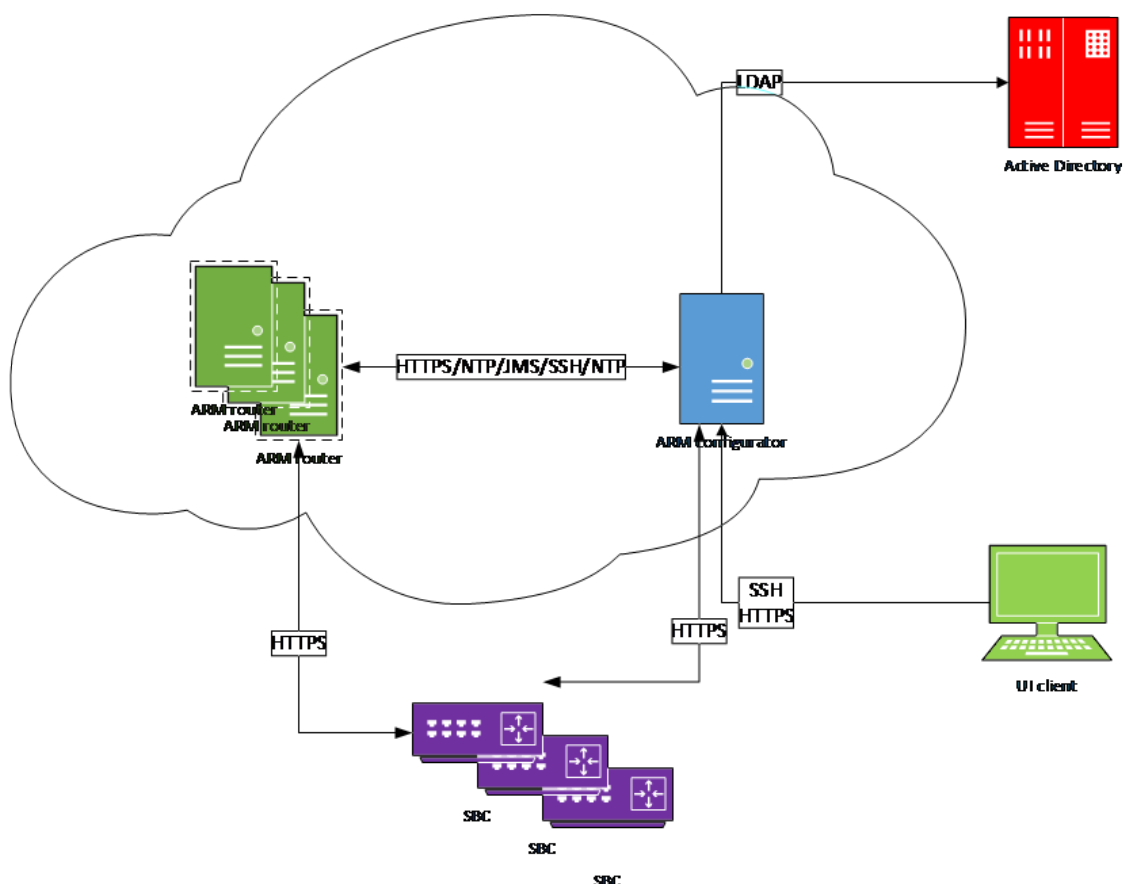
The screenshot shows the 'ADD NODE' dialog box. It has fields for 'Name' (sbc-1), 'Address' (sbc-1-de2a5ad4bc.wi), and 'Protocol' (HTTP). Below these fields is a 'Credentials' dropdown menu. At the bottom are 'OK' and 'Cancel' buttons. The 'IP Address' radio button is selected, and the 'Hostname' radio button is also selected.

- In the device's Web interface, configure the Network Settings page using the figure below as a reference.

Figure 4-6: Web Interface Network Settings

Security Group Configuration

Use the following figure as reference.

Table 4-1: Security Group Configuration

LDAP Server / Active Directory

The ARM can connect to an LDAP server to synchronize with the organization's users database or to authenticate the ARM GUI user. If either of these features are required, then an LDAP connection between the ARM configurator and the LDAP server is required. The LDAP server can be on-premises in the customer's network, mirrored to the cloud, or entirely in the cloud.

LDAP Server in the Cloud or Mirrored to the Cloud

The ARM configurator and the LDAP server must be in the same security group and the security group must have a rule allowing incoming and outgoing LDAP traffic (port 389) or LDAPS (port 636) inside the security group, or the two security groups must allow for LDAP traffic between them.

LDAP On-Premises

A VPN connection must be established between the ARM configurator in the cloud and the LDAP server in the customer's network.

ARM GUI

To access the ARM GUI from a web browser, the browser must have HTTPS access (port 443) to the ARM configurator's external IP address.

The ARM configurator's security group must have a rule allowing incoming HTTPS port 443 from the external IP address of the computer on which the browser is running.

SSH Client

SSH access may sometimes be needed to access the VM's Linux shell to collect logs, execute backup and restore and upgrade the ARM software, etc.

The security group of all ARM VMs must have a rule allowing incoming SSH port 22 from the external IP address of the computer on which the SSH client is running.

Configurator to Router

Between the configurator and router there must be two-way HTTPS traffic, JMS/NTP access from router to configurator, and SSH access from configurator to router.

Add the following rules to the configurator's security group:

- allow all outgoing traffic to the router's security group, or the router's public IP address if using public IPs
- allow incoming HTTPS port 443 from the router's security group, or the router's public IP address if using public IPs
- allow incoming TCP port 8080 for JMS from the router's security group, or the router's public IP address if using public IPs
- allow incoming UDP port 123 for NTP from the router's security group, or the router's public IP address if using public IPs

Add the following rules to the router's security group:

- allow all outgoing traffic to the configurator's security group, or the configurator's FQDN if using public IPs
- allow incoming HTTPS port 443 from the configurator's security group, or the configurator's FQDN if using public IPs
- allow incoming SSH port 22 from the configurator's security group, or the configurator's FQDN if using public IPs

Nodes (SBC or Media Gateways)

ARM configurator and routers must have two-way HTTPS traffic with the nodes.

On-Premises Nodes using Public IPs

On-premises SBCs are normally located in the organization's DMZ. They must have HTTPS port 443 open towards the subnets of the relevant cloud service. Additionally, the configurator and routers must allow HTTPS traffic to the external IP addresses of the nodes.

Add a rule to the security groups of the ARM configurator and routers to allow all outgoing traffic to the external IP addresses of the nodes.

Add a rule to the security groups of the configurator and routers to allow incoming HTTPS port 443 from the external IP address of the nodes.

Cloud SBCs in same VPC, or VPN between SBCs and ARM

Add the following rules to the security groups of the ARM configurator and router, and to the security group of the SBCs:

- allow all outgoing traffic to the other two security groups
- Allow incoming HTTPS port 443 from the other two security groups

NTP Server

The ARM configurator must have access to an NTP server.

Add a rule to the configurator's security group, allowing outgoing traffic to UDP port 123 to the external IP address of the NTP server.

SNMP Traps

The ARM can optionally send SNMP traps to an external network management server. To allow this feature, a rule must be added to the configurator's security group allowing outgoing UDP port 161 to the external IP address of the network management server.

Accessing Security Group Configuration

On Microsoft Azure

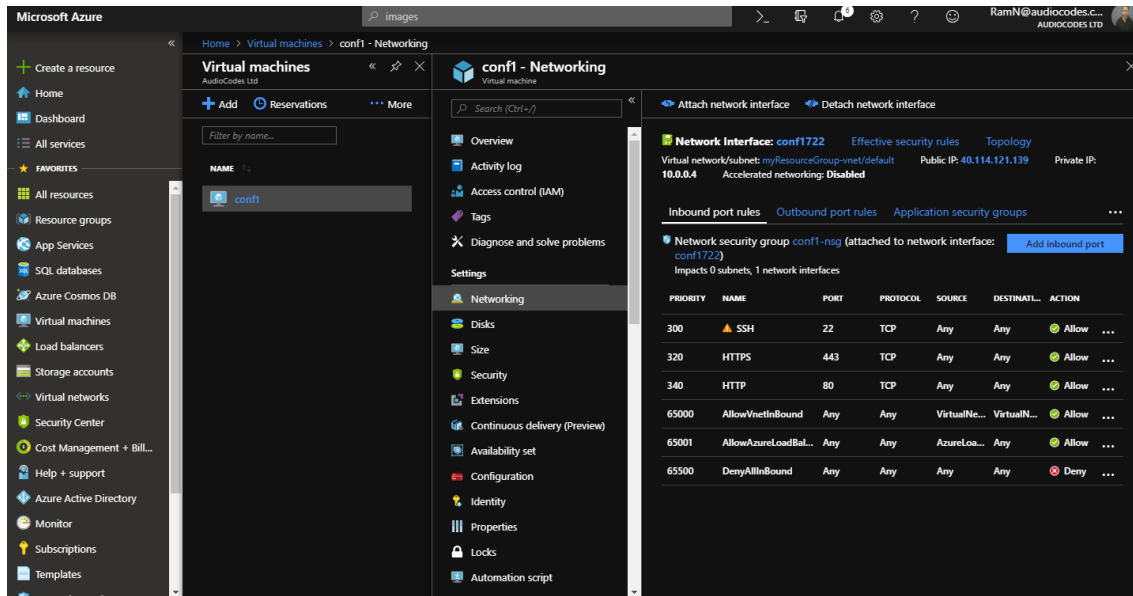
Go to **Virtual machines**, click the VM and then **Networking**.

For inbound rule, select the **Inbound port rules** and click **Add inbound port**.

For outbound rule, select the **Outbound port rules** and click **Add outbound port**.

Configure source, source port ranges, destination, destination port ranges, protocol, action and name, and click **Add**.

Table 4-2: Security Group Configuration

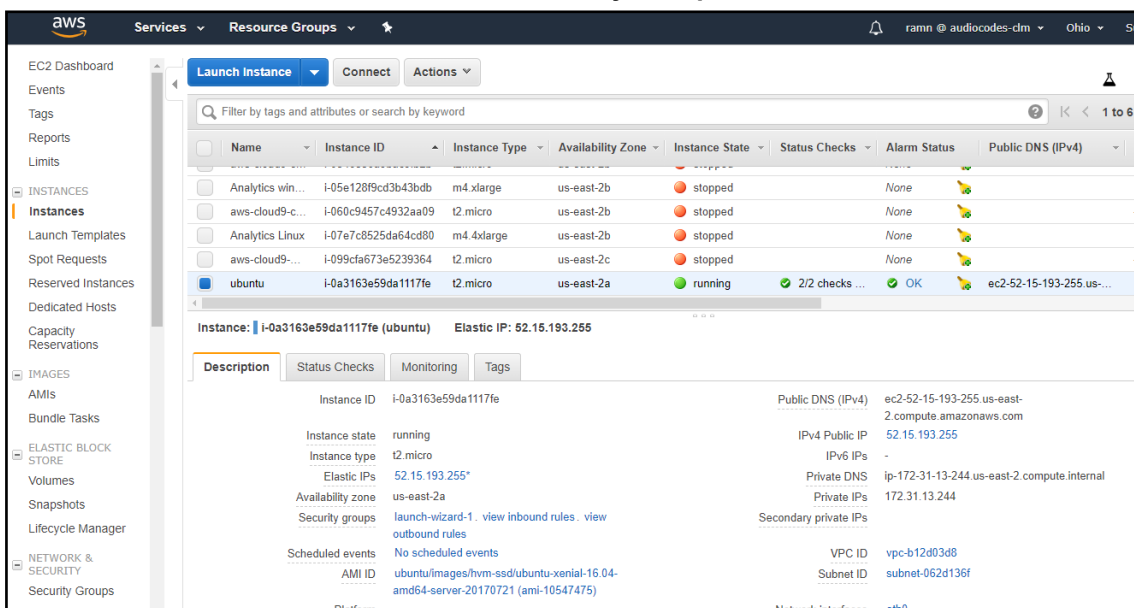


On AWS

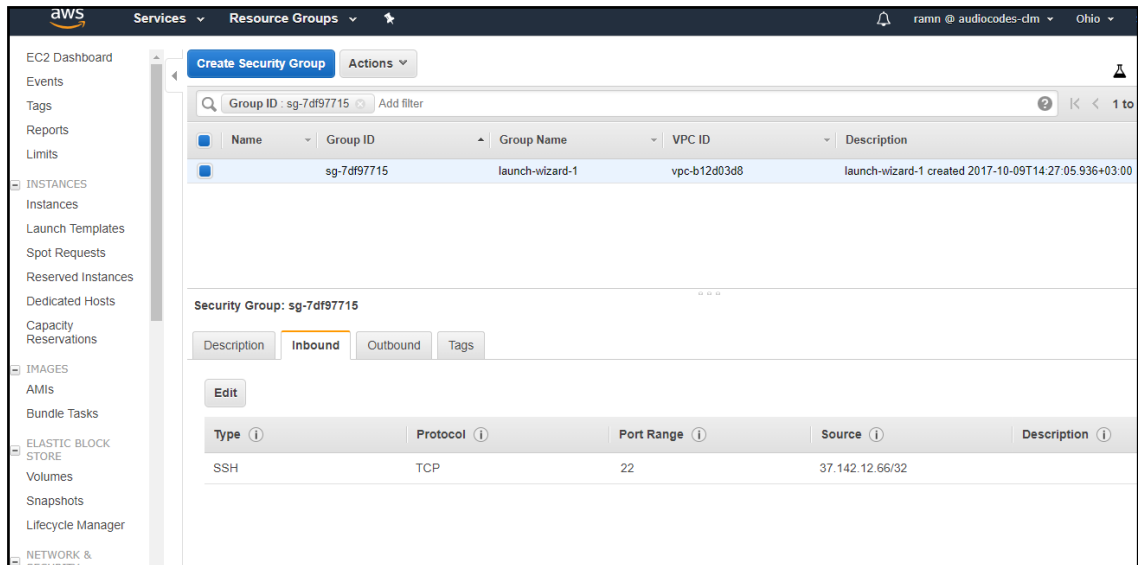
➤ To configure:

1. In the AWS console EC2, go to **Instances**, click the instance and then under the **Description** tab, click the security group.

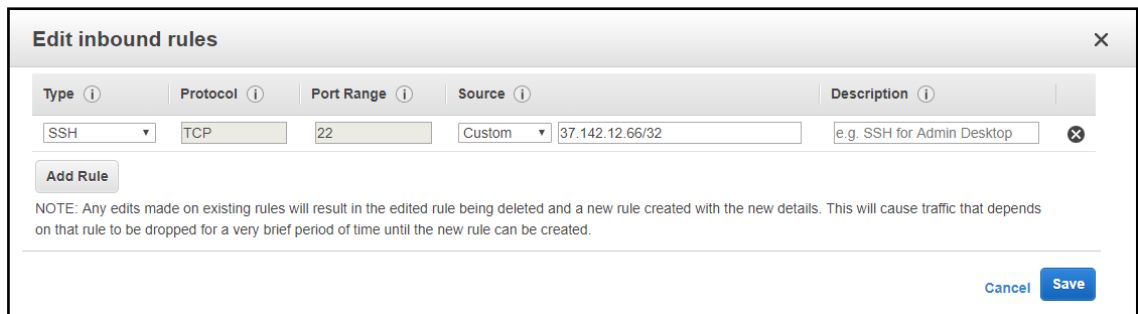
Table 4-3: AWS – Security Group



2. For the inbound rule, select the **Inbound** tab and for the outbound rule, select the **Outbound** tab and then click **Edit**.

Table 4-4: AWS – Inbound | Outbound Rule - Edit

3. Click **Add Rule**.

Table 4-5: AWS – Add Rule

4. Configure 'Type', 'Protocol', 'Port Range', 'Source' and then click **Save**.

5 Performing an Online Software Upgrade

IT managers can install a new software version on an existing ARM installation. The online upgrade replaces the software version on all ARM components. All existing configuration is preserved. Only one router is down at a time. Routers can operate temporarily without the configurator, so there is no downtime, and minimal effect on the ARM. After the initial user input collection, the upgrade continues, and completes without user interaction.

The upgrade automatically performs all of the following on the configurator:

- Unpacks the software archive file and validates readiness for upgrade
- Stops the configurator
- Converts the database to the new version schema
- Installs the new software on the configurator
- Updates the operating system of the configurator if necessary
- Validates the successful upgrade of the configurator
- Copies the relevant files to the routers
- Installs and verifies new software on the routers, one by one
- Updates the operating system of the routers if necessary

Preparing for the Upgrade

You need to prepare for the upgrade.

➤ **To prepare for the upgrade:**

1. Make sure your network is stable.
2. Make sure the ARM is available.
3. Make sure all routers are in service (green).
4. Obtain the root user password for all virtual machines.
5. Obtain the upgrade tar.gz archive file for the version you want to upgrade to.
6. Copy the tar.gz files to the configurator using SFTP (SSH File Transfer Protocol).
7. Choose a time with low call traffic.



The following steps are for upgrades from ARM Version 8.4 or earlier. If you're upgrading from ARM Version 8.6 or later, you can skip it.

8. Copy the file **cent88update-repo.tar.gz** from the same location where you obtained the upgrade tar.gz file, and copy it to the '/root' directory on the ARM configurator. This file contains Linux security updates. Note that this upgrade will take longer, due to the Linux update.
9. Perform the following actions for the Configurator VM only (this step is necessary because as of Version 8.4, the ARM Configurator requires four CPU cores while Version 8.2 only required two, and as of version 8.6, the ARM Configurator requires 16 GB of RAM while version 8.4 required only 8 GB):
 - a. In vSphere client, right-click the VM and select **Power > Power off**
 - b. Right-click the VM and select **Edit settings > Hardware > CPUs**, and then change the number of cores per socket to 4 (if it is not already set to 4).
 - c. Right-click the VM and select **Edit settings > Hardware > Memory**, and then change the memory size to 16 GB.
 - d. Right-click the VM and select **Power > Power on**.

- e. Wait for the VM to boot up and then check in the GUI that all routers are available.



The next step is for ARM router upgrades from ARM Version 7.8 or earlier. If you're upgrading from ARM Version 8.0 or later, you can skip it.

10. This step is necessary because as of Version 8.0, the ARM router requires a RAM memory allocation of 8 GB, while Version 7.8 only required 4 GB.
Perform the actions below for each ARM router:



There will be no loss of service so long as you perform this action separately for each VM and wait for the current VM to be up and available before moving on to the next.

- a. In vSphere client, right-click the VM and select **power>power off**
- b. Right-click the VM and select **edit settings>Hardware>Memory**, and then change the memory size to 8 GB.
- c. Right-click the VM and select **power>power on**
- d. Wait for the VM to go up and then check in the GUI that all routers are available.
- e. Move on to the next VM.

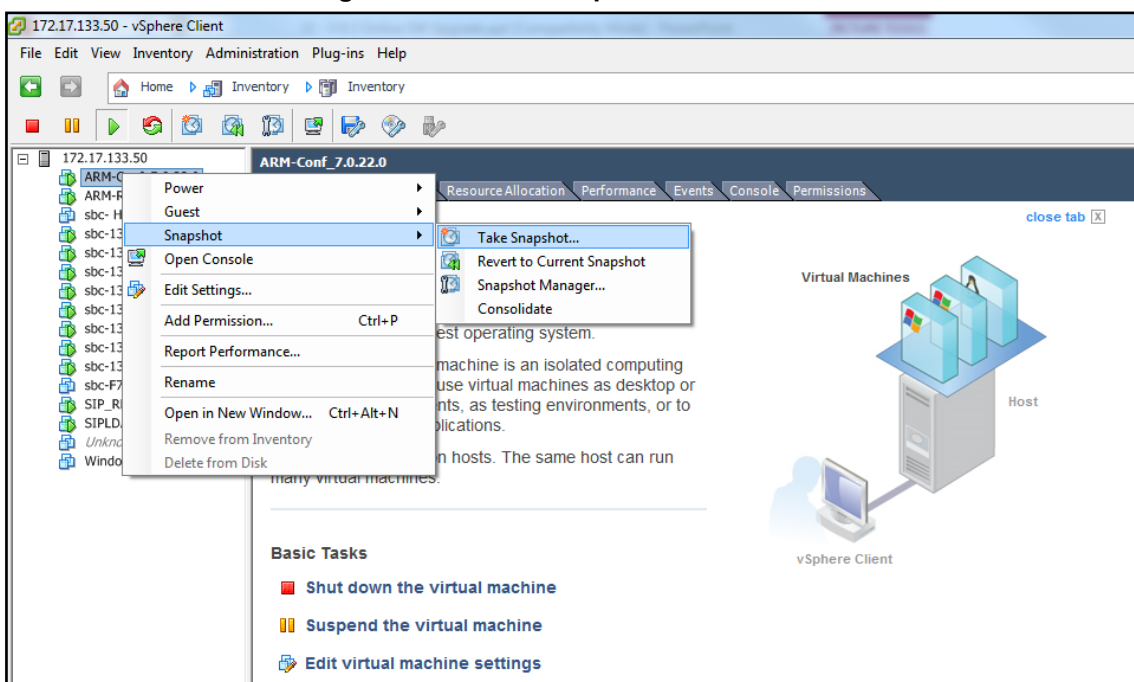
Performing the Upgrade

You're now ready to perform the upgrade.

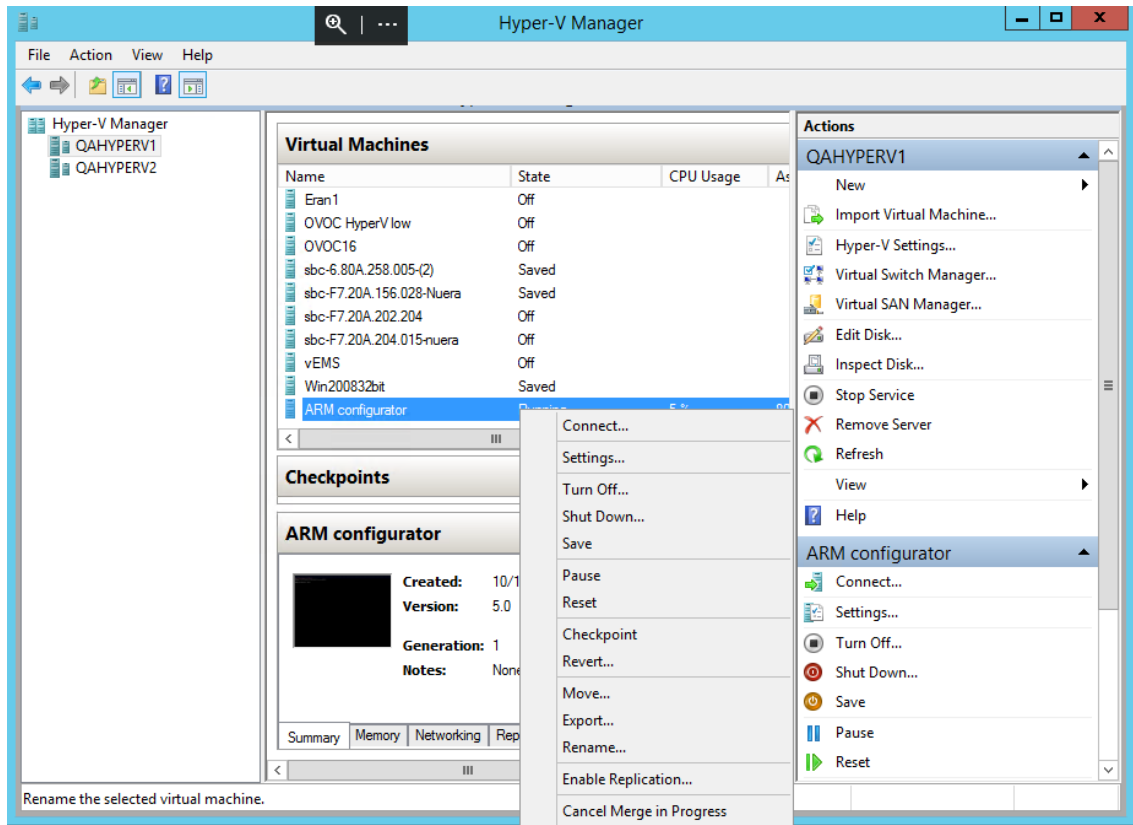
➤ To perform the upgrade:

1. Perform a virtual machine snapshot of the configurator and all of the routers:
 - a. If you're on VMWare: In the vSphere client, right-click the virtual machine and select **Snapshot > Take Snapshot**.

Figure 5-1: Take Snapshot



- b. If you're on Hyper-V: In Hyper-V Manager, right-click the virtual machine and select **Checkpoint**.

Figure 5-2: Hyper-V Manager: Select 'Checkpoint' from VM's Right-Click Menu

- c. Log into the configurator using SSH.
- d. Execute the following command:

```
upgrade_arm <path to the upgrade archive file/filename>
```

- e. Answer **y** to the following questions:

Figure 5-3: Answer 'y' to the Questions

```
*****
**      Audiocodes Routing Manager - Online Software Upgrade      **
**                                                                 **
*****
About to perform upgrade from 7.0.28.0 to 7.0.29.0. Are you sure? (y/[n]):
y
Did you perform a virtual machine snapshot of every ARM component virtual machine (Configurator and Routers)? (y/[n]):
y
```

- f. On the first upgrade, you will be prompted to enter each of the router's root user password (the configurator root user fingerprint is stored in the router so router password entry is not needed on future upgrades).
- g. Wait for the notification **ARM has been successfully upgraded to...**

Figure 5-4: ARM has been successfully upgraded to...

```

check_routers:
router1 router8.corp.audiocodes.com
SSH connection with router router1 is successful

copy_files_to_routers

copy_files_to_router_router1 (router8.corp.audiocodes.com)
copying backup.pl to router8.corp.audiocodes.com
copying restore.pl to router8.corp.audiocodes.com
copying log_color.pl to router8.corp.audiocodes.com
copying log.pl to router8.corp.audiocodes.com
copying watchdog.pl to router8.corp.audiocodes.com
copying upgrade.pl to router8.corp.audiocodes.com
copying cli.pl to router8.corp.audiocodes.com
copying log to router8.corp.audiocodes.com
copying cli to router8.corp.audiocodes.com
copying tomcat to router8.corp.audiocodes.com
copying sshd_config to router8.corp.audiocodes.com
copying java.security to router8.corp.audiocodes.com
copying RoutingManager.war to router8.corp.audiocodes.com
copying arm-cdr-util.jar to router8.corp.audiocodes.com
copying apache-tomcat-9.0.8.tar to router8.corp.audiocodes.com
copying ComponentVersions.txt to router8.corp.audiocodes.com
copying centosupdate-repo.tar.gz to router8.corp.audiocodes.com

stop_tomcat
tomcat is down

backup
backup is complete. Backup file is /home/backup/backup_172.17.133.7_1807011228_8.0.20.tar.gz

upgrade_tomcat

convert_database
executing conversion scripts:
8.2.1.sql
8.2.3.sql
8.2.4.sql
8.2.5.sql
8.2.8.sql

copy_WARs_to_webapps
Delete /opt/tomcat/webapps/ARM.war
Move ARM.war to /opt/tomcat/webapps/ARM.war

convert_config_files

install_os_patches
This can take a while. Please be patient....
[ ***** ]
Done installing os patches

start_tomcat
waiting for tomcat to finish coming up...
tomcat finished coming up

upgrade_router

upgrade_router_router1 (router8.corp.audiocodes.com)
old version: 8.0.20
old version BUILD: 20 MAJOR: 8 MINOR: 0 IS_PATCH: 0
new version: 8.2.9
new version BUILD: 9 MAJOR: 8 MINOR: 2 IS_PATCH: 0

stop_tomcat
tomcat is down

backup
backup is complete. Backup file is /home/backup/backup_172.17.133.8_1807011235_8.0.20.tar.gz

upgrade_tomcat

copy_WARs_to_webapps
Delete /opt/tomcat/webapps/RoutingManager.war
Move RoutingManager.war to /opt/tomcat/webapps/RoutingManager.war

convert_config_files

install_os_patches
This can take a while. Please be patient....
[ ***** ]
Done installing os patches

start_tomcat
waiting for tomcat to finish coming up...
tomcat finished coming up
router upgrade script done
Rebooting router...
Successfully upgraded router router1
Upgrade script finished successfully

*****
* ARM has been successfully upgraded to 8.2.9 *
*****
The upgrade is complete. For OS upgrade to take effect, this configurator must be restarted (the routers have already been rebooted). Press enter to reboot this configurator

```



For the OS upgrade to take effect, the Configurator must be restarted at the end of the upgrade. Press **Enter** to reboot the Configurator.

- h. If you are installing on AWS: In the AWS console EC2, go to **Instances**. Right-click your instance, click **Image** and then **Create Image**.

Figure 5-5: AWS - Create Image

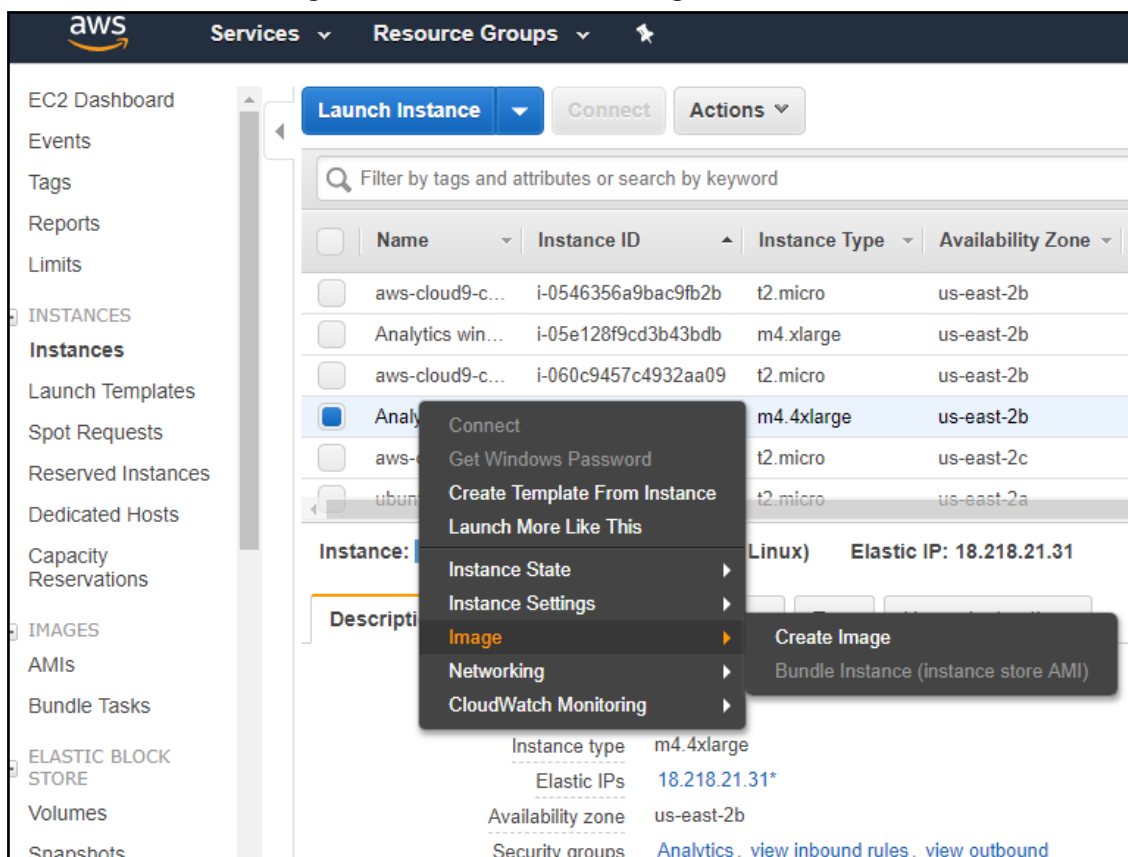
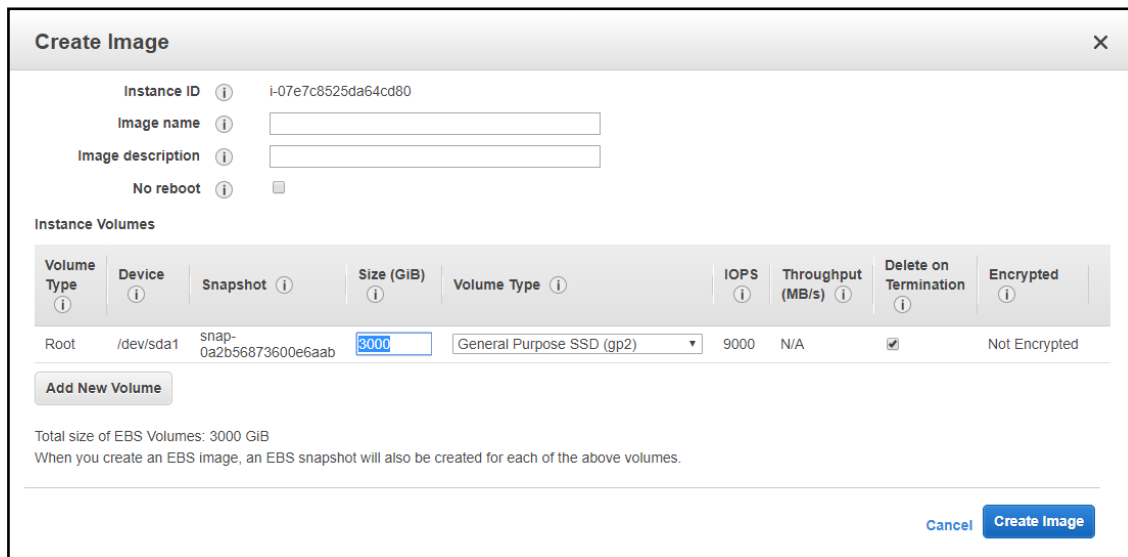


Figure 5-6: AWS – Image Settings



Troubleshooting

If the upgrade fails:

- If the failure occurs during a router upgrade, you'll view this message:

```
Upgrade of router router1 failed

*****
* This upgrade is now paused. Please press Enter to retry the upgrade of this router. *
* If the problem persists, please contact Audiocodes support *
*****
```

- In this case, press Enter to retry the upgrade of this router and continue the upgrade. If the problem persists, leave the upgrade at its current state and contact AudioCodes support. Alternately, revert the upgrade as described in the following paragraph.
- If the upgrade does not allow retry or the failure is consistent or you decided to revert to the previous version:
Copy the file **/home/upgrade/upgrade.log** from all ARM Virtual Machines to your computer and then revert to the pre-upgrade snapshot in VMware vSphere client.

If the upgrade is successful but the ARM is not performing flawlessly in the new version:

1. Log into the ARM Configurator virtual machine via SSH and type the command:

```
logCollect
```

2. Copy the created **tar.gz** file to your computer and then revert to the pre-upgrade snapshot in the VMware vSphere client.
- If the upgrade was interrupted by a network disconnect or by a failure of the SSH client machine, you can attempt to continue the upgrade by running the same command again; the upgrade will attempt to continue from where it left off. If this is unsuccessful, revert to the previous version as described in the previous paragraph.

6 Backing up / Restoring ARM Software

The backup feature collects software, configuration and log files to enable you to restore the ARM server to its previous state.

You should back up the ARM software

- before risky changes
- after changing the ARM configuration

Backup Types

Two backup types are supported:

- Periodic Backup
 - Applies only to the Topology Manager VM
 - Stores backup files in */home/backup/periodic* and does not include the log files
 - The directory stores up to 10 files, deleting the oldest file before creating a new one.
- Manual Backup
 - Applies to the Routing Manager VM *and* to the Topology Manager VM
 - Stores backup files in */home/backup*.

Performing a Manual Backup

You can perform a manual backup.

➤ To perform a manual backup:

1. Log in to the VM (Topology Manager or Routing Manager) using ssh with user 'root'.
2. Execute the command:

```
backup_arm
```

The backup utility prompts:

```
Include log files? (y/[n]):
```

3. Answer **yes** to include all log files in the backup file.

The backup utility prompts:

```
Include all software files? ([y]/n):
```

4. Answer **no** to exclude software files from the backup file. This will make the backup smaller but will not allow rollback of changes in the tomcat directory or version changes.

The backup feature creates a backup file and prompts:

```
>>> collecting arm DB ...
>>> Creating tar archive...
.....
>>> Compress tar file...
```

```
Completed backup. Backup file is
/home/backup/backup_<ip address>_<date and time>_<version>.tar.gz
```

Checksum file is
/home/backup/backup_<ip address>_<date and time>_<version>.sfv

A text file with the same name as the backup file but with suffix “sfv” (Simple File Verification) is created, containing the CRC32 checksum of the *tar.gz* file.

The restore process checks that the checksum matches the *tar.gz* file before running.

Restoring ARM Software

You can restore ARM software.

➤ To restore ARM software:

1. Log in to the VM (Topology Manager or Routing Manager) using ssh with user ‘root’.
2. Execute the command:

```
restore_arm_backup <backup file name>
```

The restore feature prompts you to confirm:

WARNING! You are now going to restore a backup of the ARM server. ARM server will now stop, and all configuration, database and software files will be overrun. Are you sure you want to restore this backup? [Yes/No] (No):

The restore feature prompts you to confirm start:

Restore is done. ARM server will now start. Press Enter to continue:

7 High Availability (HA)

Overview

ARM HA is based on VMware HA which [per VMware documentation] is a viable virtualization solution for environments that can tolerate brief interruptions of service and potential loss of transactions serviced at the time of failure. VMware HA strives to minimize downtime and deliver service continuity by restarting a VM on a different host if the initial host fails, or on the same host if application failure occurs.

Both ARM VM modules, Topology Manager *and* Routing Manager, provide availability capabilities, but the HA concept differs for each module.

Topology Manager runs over only one VM. If the host fails, the Topology VM is restarted on another host by the VMware HA feature. Down time is equal to VM restart time, acceptable for the Topology Manager module because real time routing is unaffected.

The Routing Manager module runs in Active-Active mode: a few router VMs can run simultaneously, providing not only HA (no down time) if one of them goes down but also scalability by adapting to traffic capacity.

For more information on VMware HA capabilities and configuration, see [vSphere 5.5 Availability](#).

vSphere HA provides HA for VMs by pooling the VMs and the hosts they reside on into a cluster. Hosts in the cluster are monitored and if a failure occurs, the VMs on a failed host restart on alternate hosts.

VM Monitoring restarts individual VMs if their VMware Tools heartbeats are not received within a set time.

Requirements for a vSphere HA Cluster

Consult the checklist below before setting up a vSphere HA cluster. For more information, see *Best Practices for Networking* or *Creating a vSphere HA Cluster* in [vSphere 5.5 Availability](#).

- All hosts must be licensed for vSphere HA.
- You need at least two hosts in the cluster.
- All hosts need to be configured with static IP addresses. If you are using DHCP, make sure that the address for each host persists across reboots.
- There should be at least one management network in common among all hosts and best practice is to have at least two. VMkernel network with the **Management Traffic** checkbox enabled. See *Best Practices for Networking* in [vSphere 5.5 Availability](#).
- To ensure that any VM can run on any host in the cluster, all hosts should have access to the same VM networks and datastores. Similarly, VMs must be located on shared, not local, storage otherwise they cannot be failed over if a host fails.



vSphere HA uses datastore heartbeating to distinguish between partitioned, isolated, and failed hosts. Accordingly, if there are some datastores that are more reliable in your environment, configure vSphere HA to give preference to them.

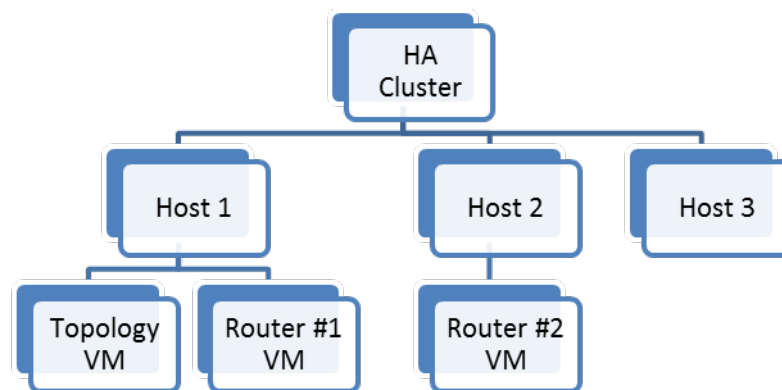
- For VM Monitoring to function, VMware tools must be installed. The provided ARM VM includes VMware tools software.
- vSphere HA supports both IPv4 and IPv6. A cluster that mixes the use of both of these protocol versions, however, is more likely to result in a network partition.

Distributing ARM VMs in an HA Cluster

To achieve best HA performance for ARM VMs in the VMware HA environment, locate the Topology Manager and Routing Manager VMs among the hosts in the HA cluster like this:

- Deploy the Topology Manager VM on only one VM. It can be located on any host in the HA cluster according to VMware administrator preference, depending on environment resources.
- When the ARM setup includes only one Routing Manager VM, it necessarily means that if there's a failure of the host or Routing Manager VM, the routing service will be unavailable until the Routing Manager VM finishes restarting on the current host or on a different host. So for the routing service to stay up continuously, at least two Routing Manager VMs must be deployed, each on a different host in the HA cluster.

Figure 7-1: HA Cluster Schema Example



In the above example, if Host 1 fails, VMware HA restarts the Topology VM on Host 2 or Host 3, and restarts Router #1 VM on Host 2 or Host 3.

Meanwhile, Router #2 VM preserves the routing service.

After this HA process, all three VMs may be located on Host 2 only. It's inadvisable to maintain all VMs on a single host because if a failure occurs on Host 2, *both* Router VMs will restart and the routing service will be unavailable during the restart.

A preferable option is to set Router #1 VM to restart on Host 3 if failure occurs, or, if the HA cluster contains only two hosts (Host 1 and Host 2), to restore Host 1 and move Router #1 VM back to its original location.

VM UUID

Each VM has a universal unique identifier (UUID). The UUID is generated when you initially power on the VM.

The software licenses of the ARM Topology Manager VM and Routing Manager VM are linked to the VM UUID, so each VM's UUID must be kept else a new license must be issued for the VM.

If you do not move or copy the VM to another location, the UUID remains constant. When you power on a VM that was moved or copied to a new location, you are prompted to specify whether you moved or copied the VM. If you indicate that you copied it, it receives a new UUID.

A VM can be configured to keep the same UUID (see [Vmware Documentation](#)).

ARM Datacenter Recovery Procedure

Read the following to learn how to prepare for and recover from a datacenter failure.

ARM comprises a single configurator virtual machine and two or more router virtual machines. The routers operate as stateless load sharing. If the routers are distributed among multiple datacenters and one datacenter fails, ARM traffic is automatically diverted to the other routers.

The ARM configurator is a single VM. High Availability is achieved by using VMWare's HA functionality. If the active VMWare host fails, a stand-by host comes up with the same ARM configurator.

If datacenter failure occurs, it is assumed that the ARM configurator will be non-operational since both the active and standby VMWare host are non-operational. In this case, a procedure is required to recover the ARM configurator in a different datacenter.

When a configurator is down, the routers continue to operate using the last known configuration. This means that ARM call routing functionality will continue even though the configurator is down. Restoring the configurator is important for allowing configuration changes, alarms, GUI, user management, etc. Also, if a router must be restarted, it would need to reload the configuration from the configurator.

Preparation

Change Automatic Backup to an Hourly Backup

The ARM automatically performs a periodic backup of the configurator. The default period is 24 hours, keeping the last 10 backups. To change this to an hourly backup, login to the LINUX shell via SSH as user root, and type the following command:

```
mv /etc/cron.daily/dailybackup /etc/cron.hourly/hourlybackup
```

This will perform a backup every hour and keep the last 10 backups. The backups are stored in the folder **/home/backup/periodic**

Each backup file is accompanied by a corresponding sfv (checksum) file. It is recommended to pull the latest backup file with its corresponding sfv file once an hour from the configurator, and store it in the standby datacenter. This can be done using scp.

Prepare a Redundant Configurator

You need to prepare a redundant configurator.

➤ To prepare a redundant configurator:

1. In the standby datacenter, install a separate ARM configurator with the same software version as the active configurator. Besides setting the virtual machine's IP address, do not configure anything on this ARM.
2. From the GUI, obtain the machine ID and send it to AudioCodes in order to receive a license for this ARM. Load it to this configurator.
3. Switch off the virtual machine so that it will not take up any resources of the host.



If you perform an upgrade of your main ARM, perform the same upgrade on the standby ARM. You can perform the upgrade before the recovery if you don't now.

Recovering from Datacenter Failure

You need to prepare a redundant configurator.

➤ To prepare a redundant configurator:

1. Turn on the configurator virtual machine in the standby datacenter.
2. Copy the latest ARM configurator backup file with its corresponding sfv file to the new configurator.

3. Log in to the LINUX shell via SSH, and type the command:

```
restore_arm_backup --datacenter_recovery <backup filename>
```

The script keeps the existing software license on the device.

4. Wait for the configurator to be up and running. Make sure it's up by logging in to the GUI.



The routers and nodes are at this point not connected to the new IP address of the configurator. They will appear read in the network view and in the routing server table.

5. To fix this, type the following command in the LINUX shell:

```
configurator_publish_ip_change.pl
```

The script prompts for the HTTP credentials. Enter the same credentials you use for logging into the GUI. The output of the command will be 'All routers and nodes were successfully moved to the new configurator IP address'.

6. After a few minutes, the configurator will be connected and synced with all of the routers and nodes and the ARM will be fully functional.
7. If some of the nodes or routing servers fail to move to the new configurator IP address, they will be listed in the command output.

If a node fails to move, manually change the configurator IP in the node by logging into the node's Web interface. Go to **Services > HTTP Services > HTTP Remote Services > ARMTopology > HTTP Remote Hosts > ARMTopology > Edit**, and set the new IP Address.

If a router fails to move, check if it's running and connected. If it's not, bring it up and run the following command again:

```
configurator_publish_ip_change.pl
```

If it's up, restart it by logging into its shell via SSH, and type the command:

```
service tomcat restart
```

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/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, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice 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-41858

