Installation Manual

One Voice Operations Center

AudioCodes Routing Manager (ARM)

Version 9.4

audiocodes

Notice

Date Published: April-07-2021

WEEE EU Directive

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

Customer Support

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

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
41859	Report log files. Username. Password. Upgrade. UNIX shell.

LTRT	Description
42161	Storage. Router memory: 16 GB (instead of 8 GB) if >1m users. Configuring a static IP address and hostname for the VM. 'Number of standard security queries (per month)'. Online Software Upgrade. New CentOS8.
42162	Syntax fixes.

Table of Contents

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 22. 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
  - hardware and software 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 Router VM and 80 GB per Configurator VM (for HA, see Requirements for a vSphere HA Cluster on page 80
- A minimum of three VMs, i.e., One Configurator and at least two Routers - see Requirements for a vSphere HA Cluster on page 80

VMWare

Installation of the ARM on VMWare requires the following:

- VMware vSphere Hypervisor (ESXi) version 6.5 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
- 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 Router VM, and 80 GB per Configurator VM (for HA explained in Requirements for a vSphere HA Cluster on page 80
- A minimum of three VMs, i.e., One Configurator and at least two Routers - see Requirements for a vSphere HA Cluster on page 80

ARM OVA images are provided with VMWare Tools 6.5. 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
- 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.

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.

- An operator who manages more than 1 million users will have to deploy ARM Routers with extended memory – 16 GB (instead of the standard 8 GB). A high number of users requires more memory for using ARM Routers maps for real-time user-based routing.
- The ARM Routers memory extension should be applied at a VM level prior to applying a Feature Key with an extended number of users.
- In the case of adding a new ARM Router to the ARM with an extended number of users (more than 1 million), the Router's VM should have 16 GB memory.

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 80 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.

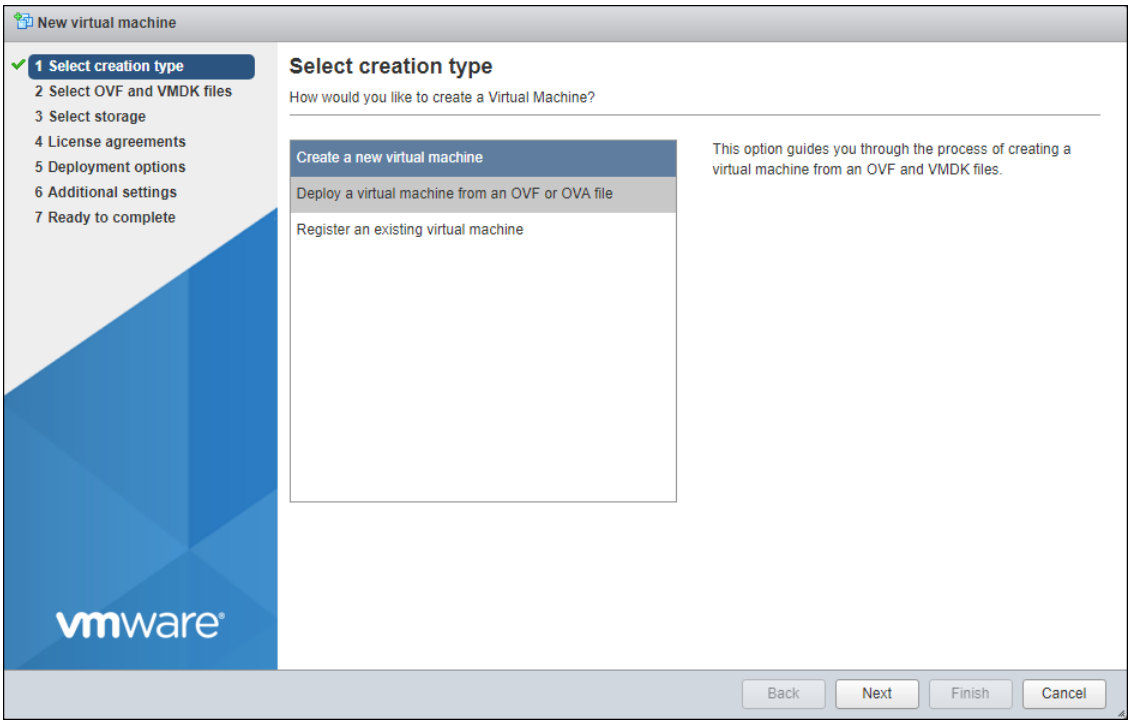
➢ **To deploy the OVA file:**

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

Figure 2-1: VMWare ESXi - Log in

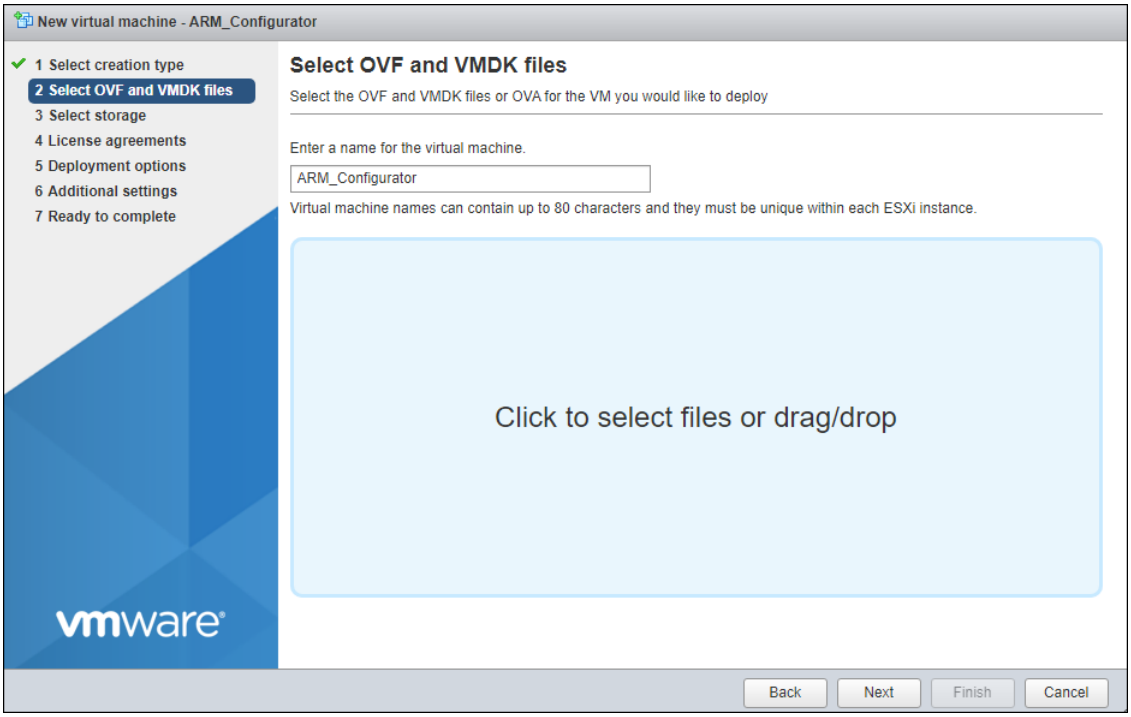
2. Enter the User name and Password and click **Log in**.

Figure 2-2: Create a new virtual machine



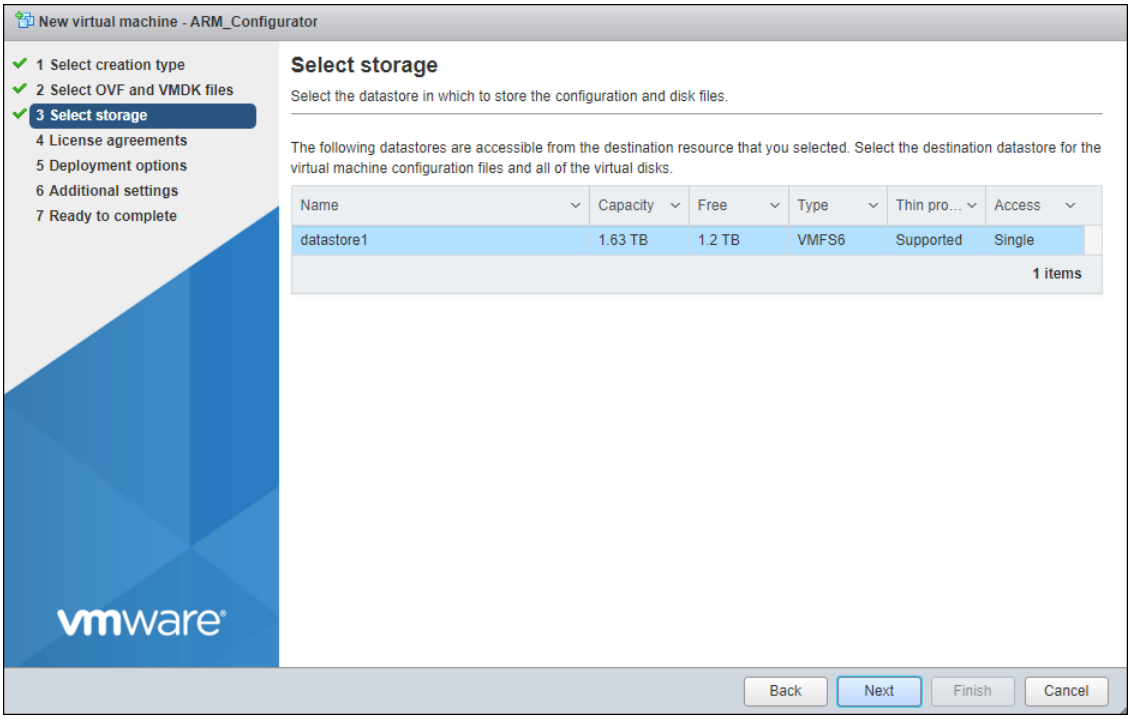
3. Select **Deploy a virtual machine from an OVF or OVA file** and then click **Next**.

Figure 2-3: Define VM Name and Select OVA File



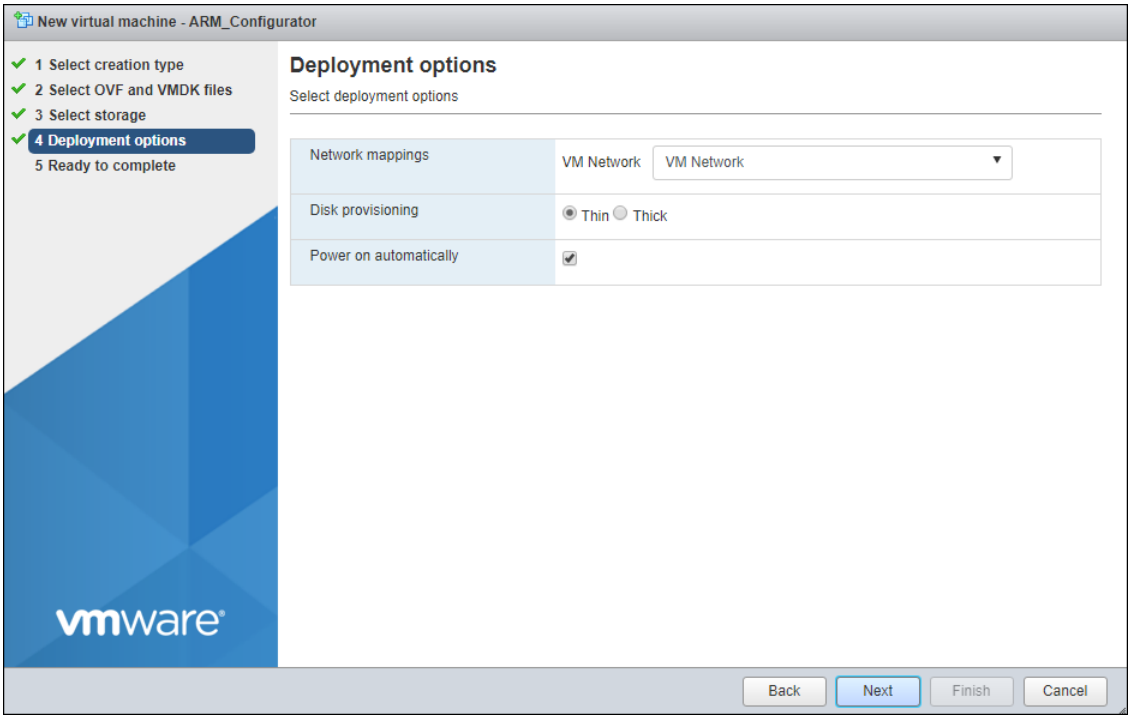
4. Enter a name for the virtual machine, e.g., ARM_Configurator, and then click **Click to select files or drag/drop** to navigate to the ARM OVA file.

Figure 2-4: Select storage



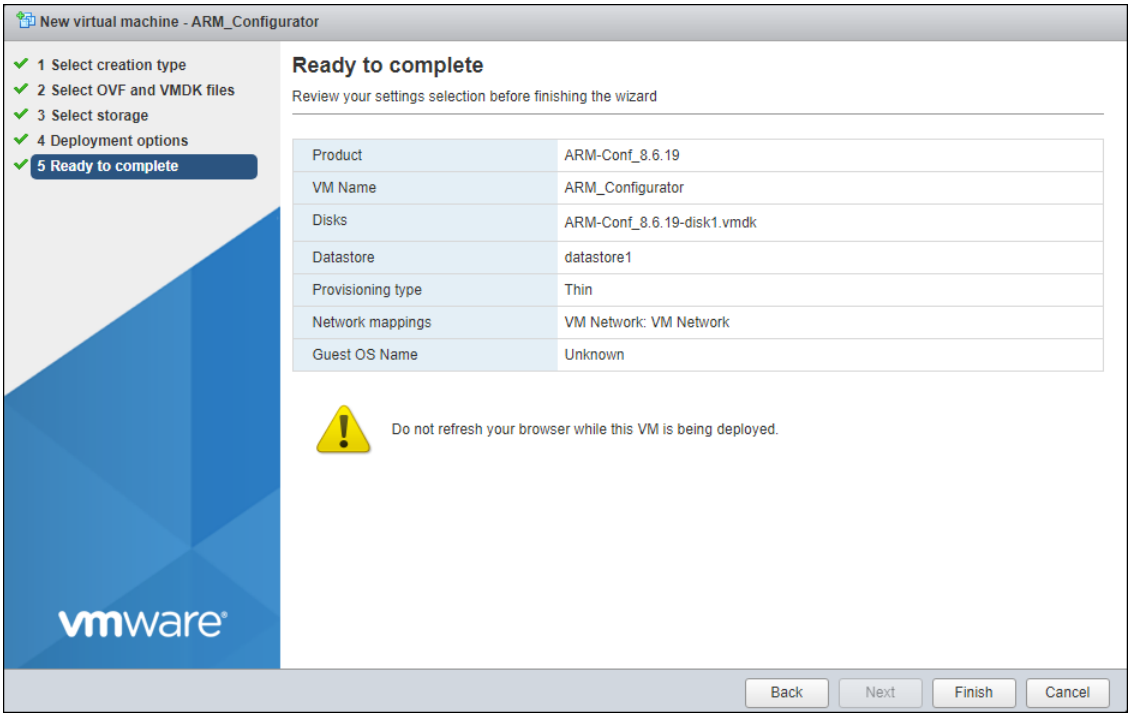
5. Click **Next**.

Figure 2-5: Deployment options



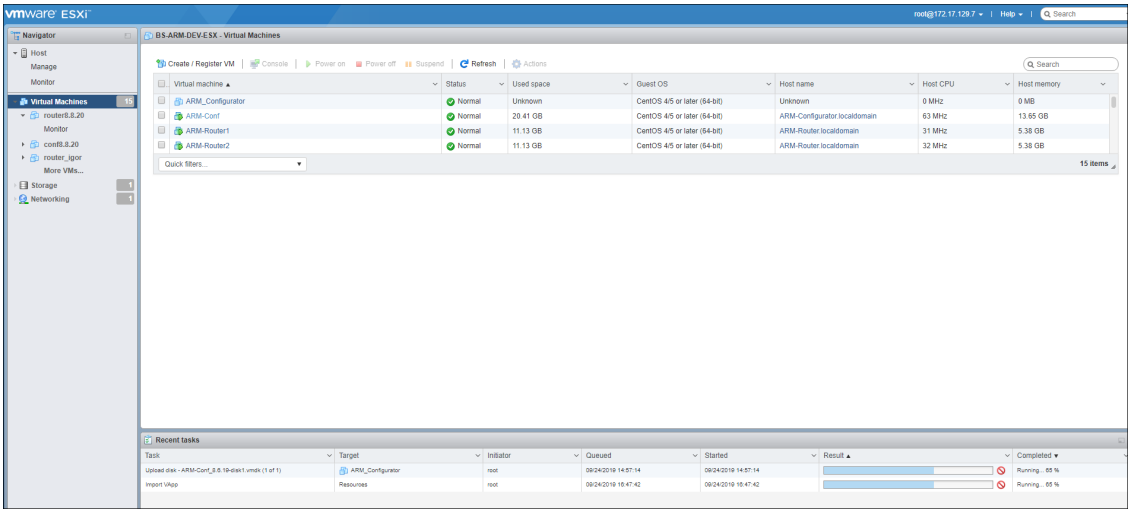
6. Choose the necessary network and then click **Next**.

Figure 2-6: Ready to complete



7. Click **Finish**.

Figure 2-7: OVA File Installation Progress



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

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

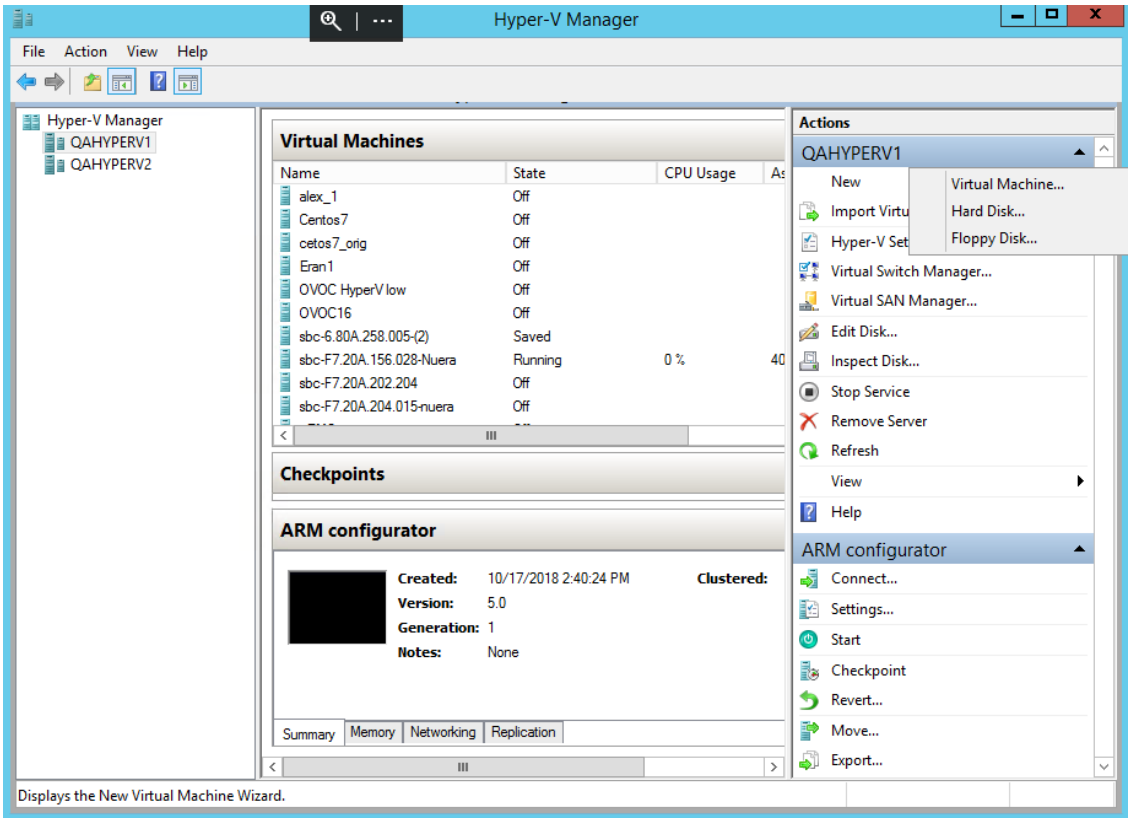
➢ Before deploying the ARM's VHD file:

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:

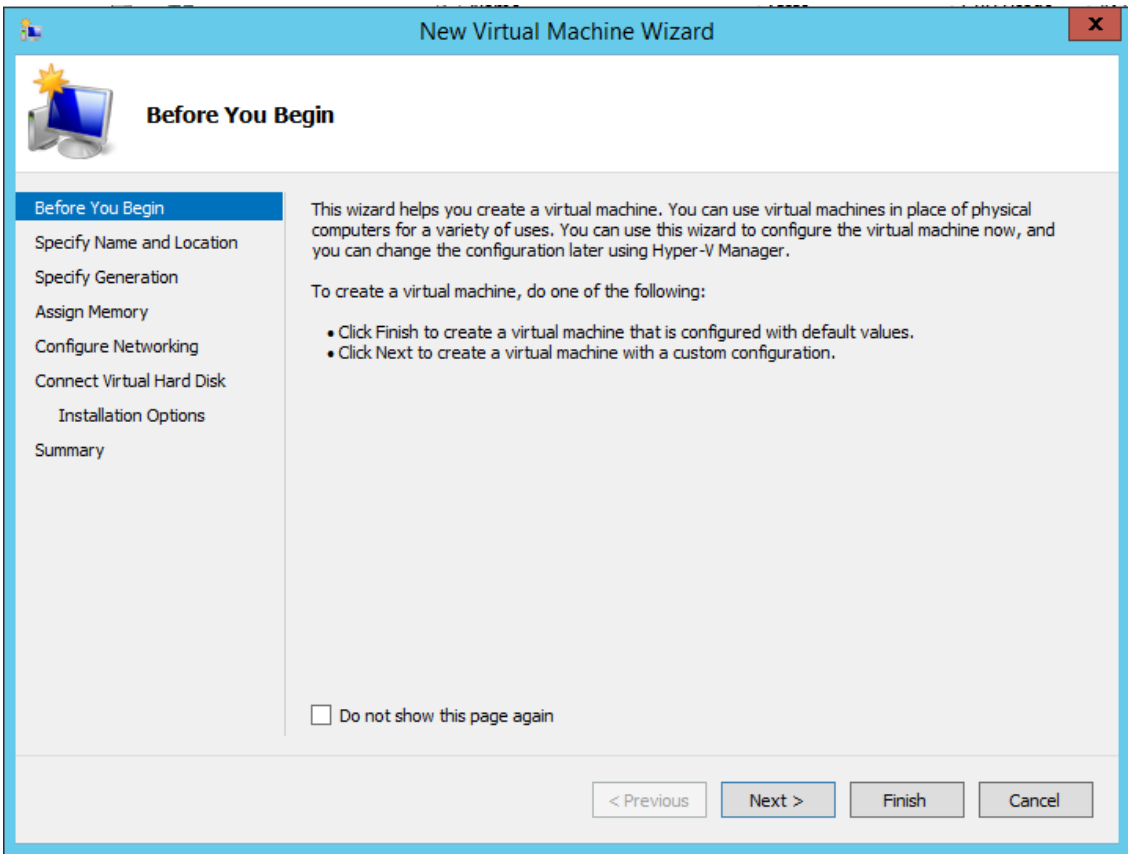
1. Start Hyper-V Manager.
2. Click **New** > **Virtual Machine**.

Figure 2-8: New > Virtual Machine



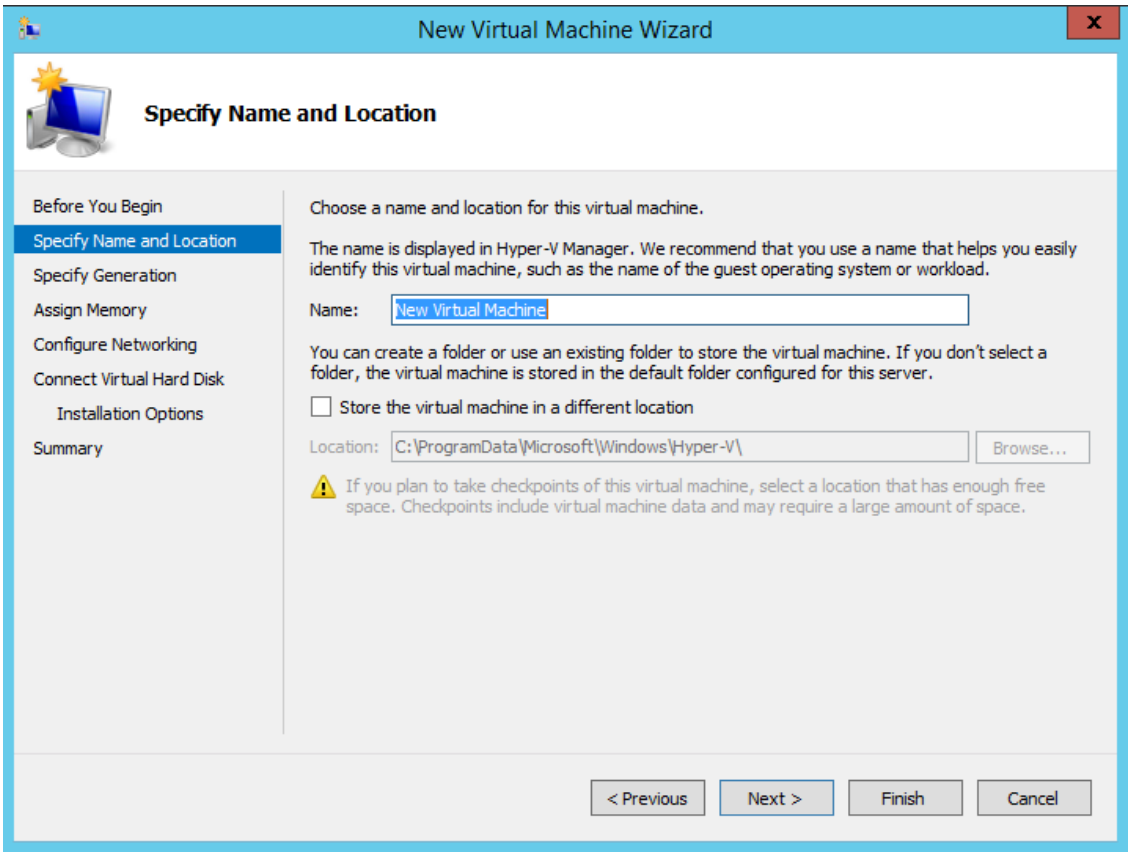
3. Click **Next**.

Figure 2-9: New Virtual Machine Wizard



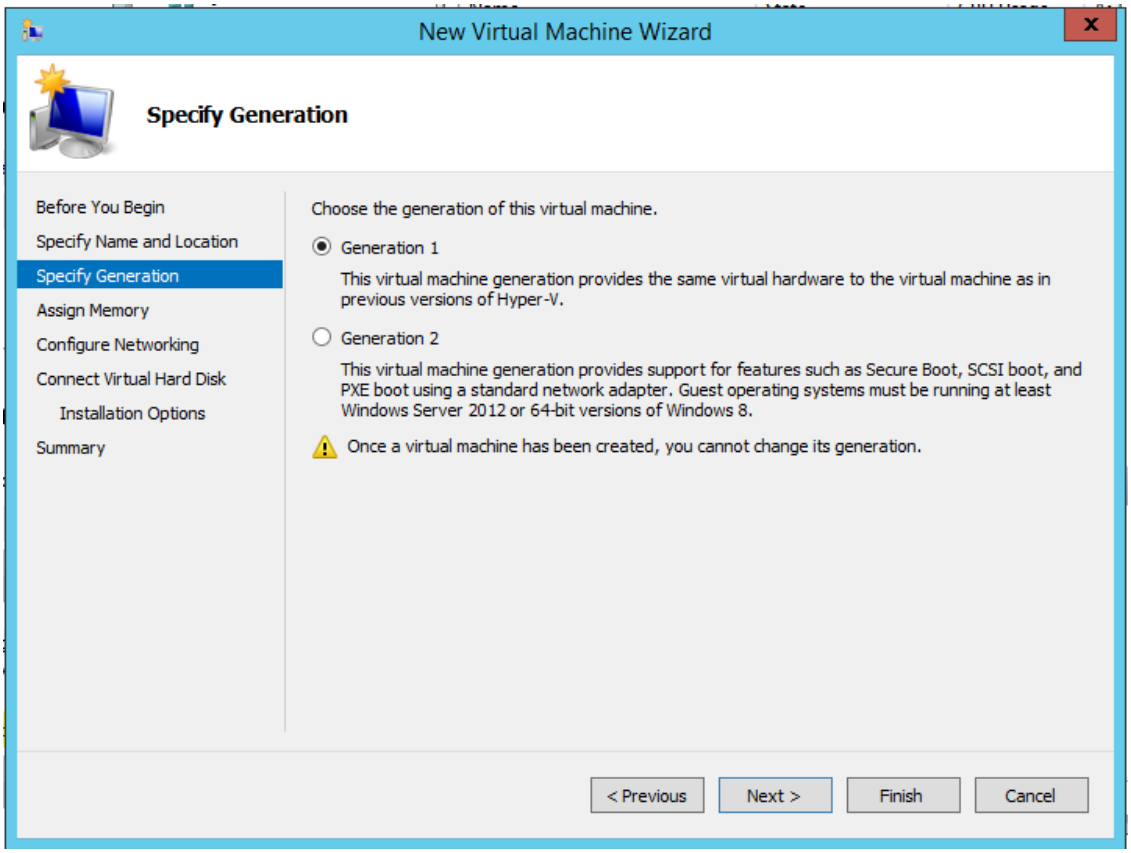
4. Give the VM a name and click **Next**.

Figure 2-10: New Virtual Machine Wizard: Specify a Name



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

Figure 2-11: New Virtual Machine Wizard: Select 'Generation 1'



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

Figure 2-12: New Virtual Machine Wizard (for ARM Configurator): Allocate 16000 MB

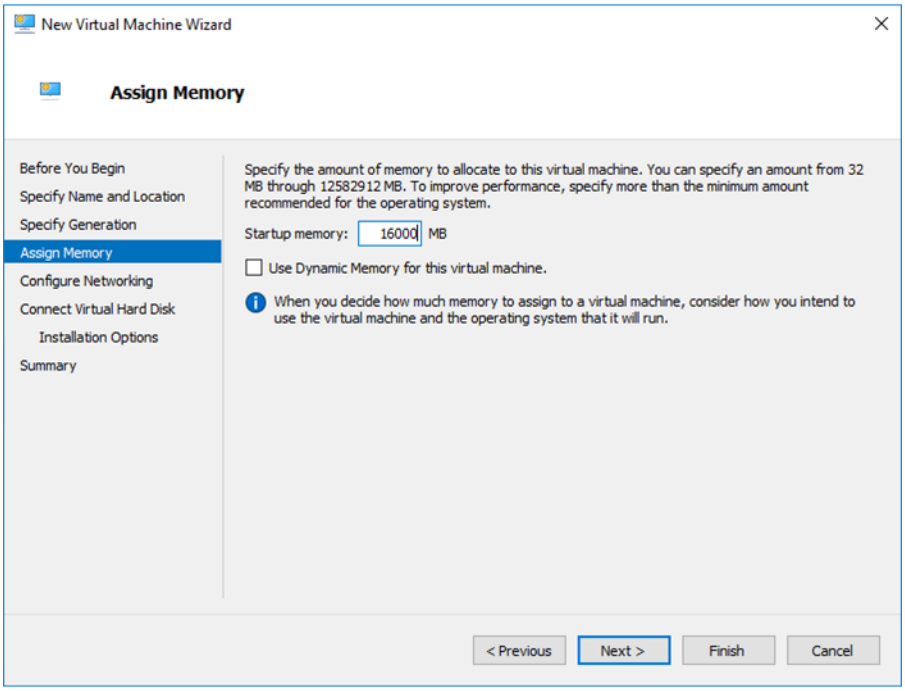
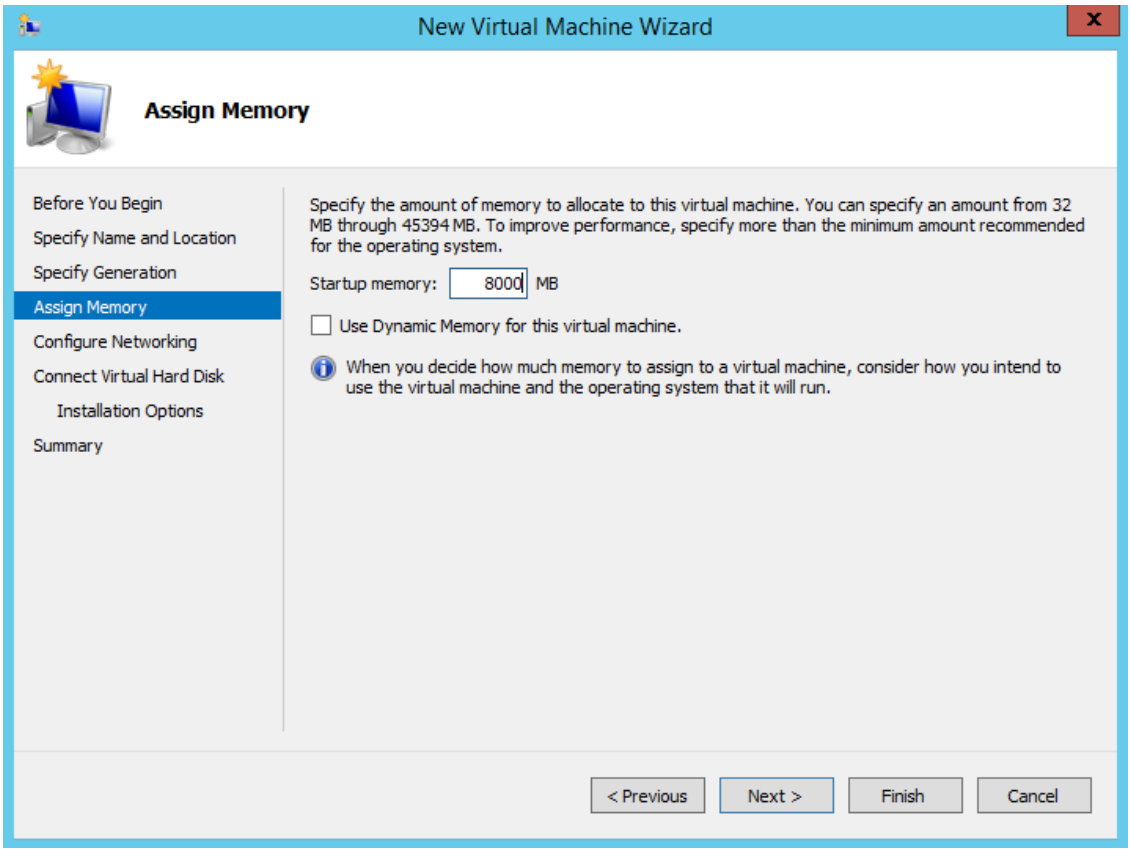
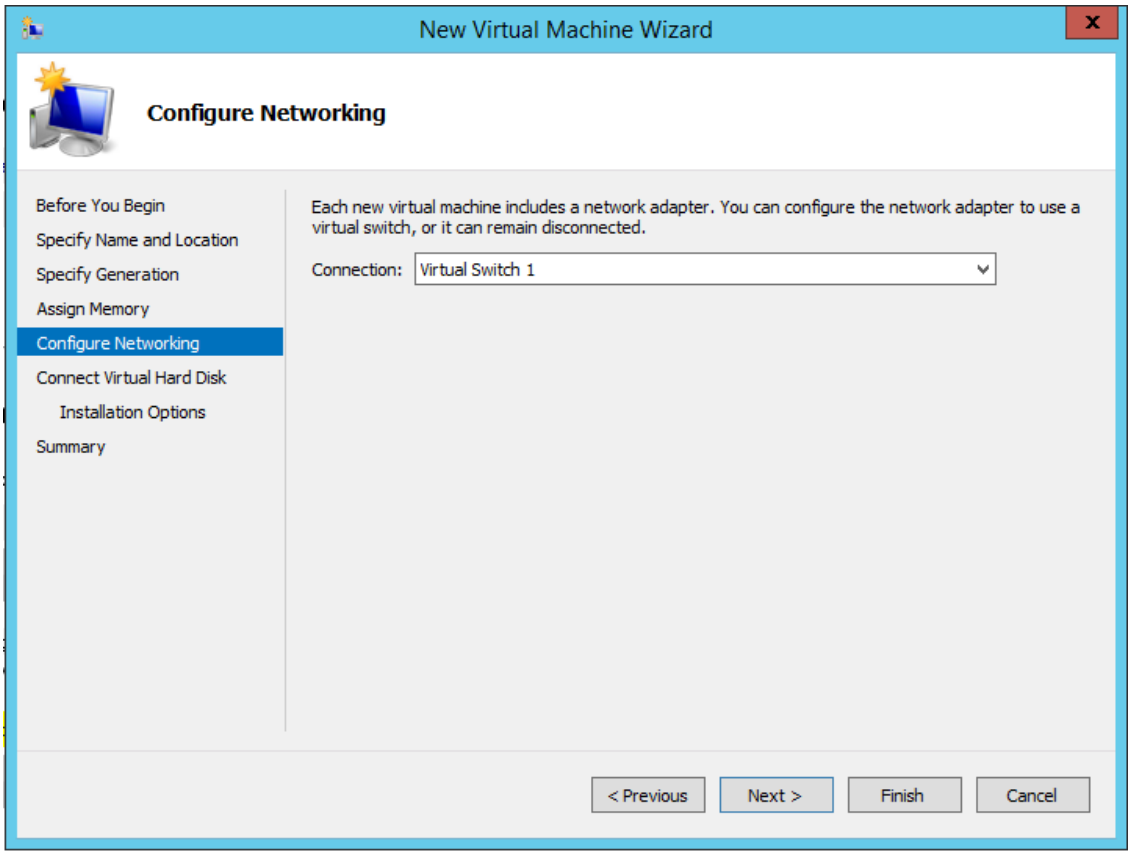


Figure 2-13: New Virtual Machine Wizard (for ARM Router): Allocate 8000 MB



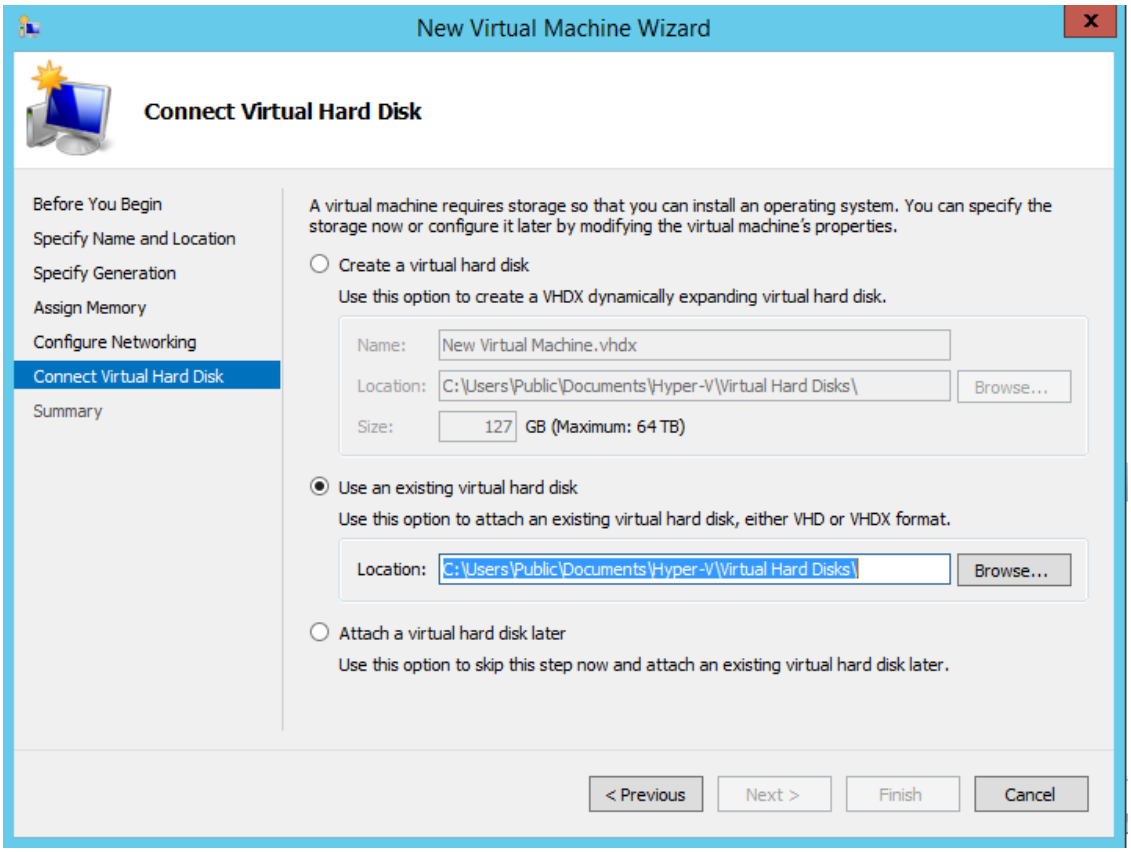
7. Select a virtual switch and click **Next**.

Figure 2-14: New Virtual Machine Wizard: Selecting a Virtual Switch



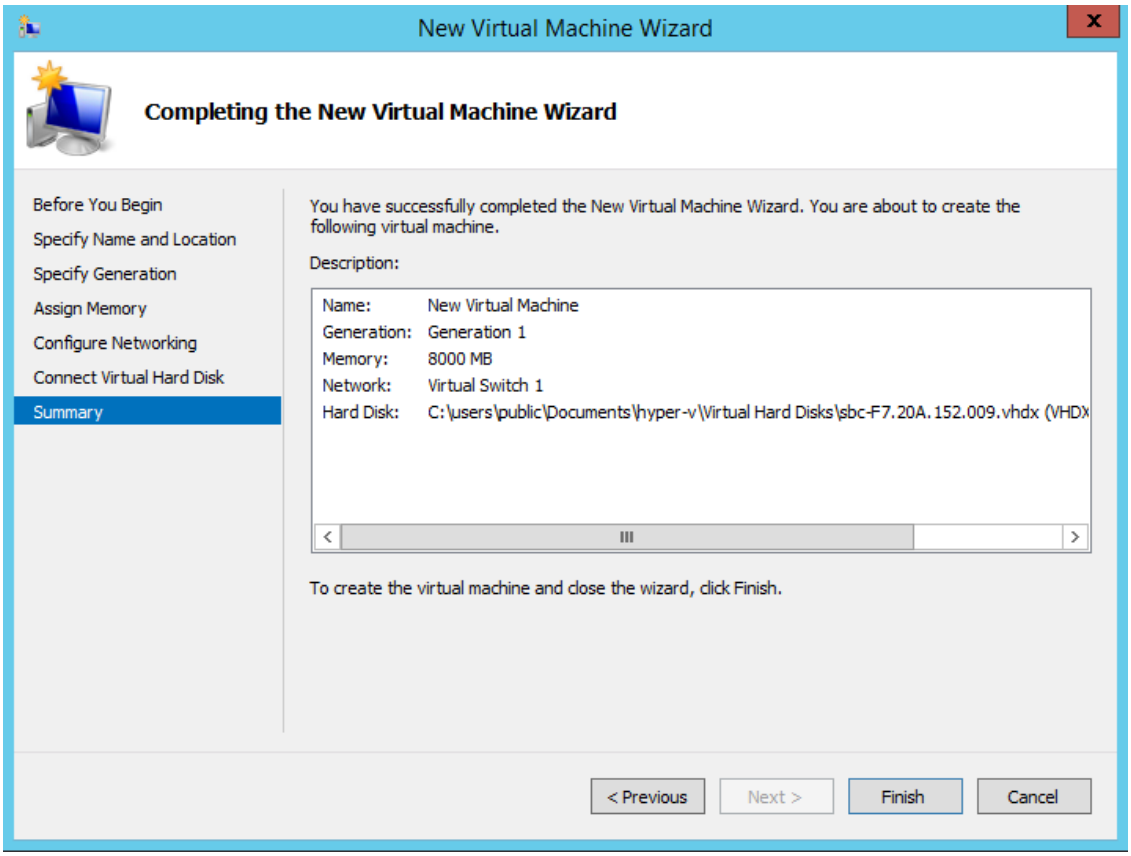
8. Select the **Use an existing virtual hard disk** option, click **Browse** and select the VHD file, and click **Next**.

Figure 2-15: New Virtual Machine Wizard: Use an existing virtual hard disk | VHD



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

Figure 2-16: Summary

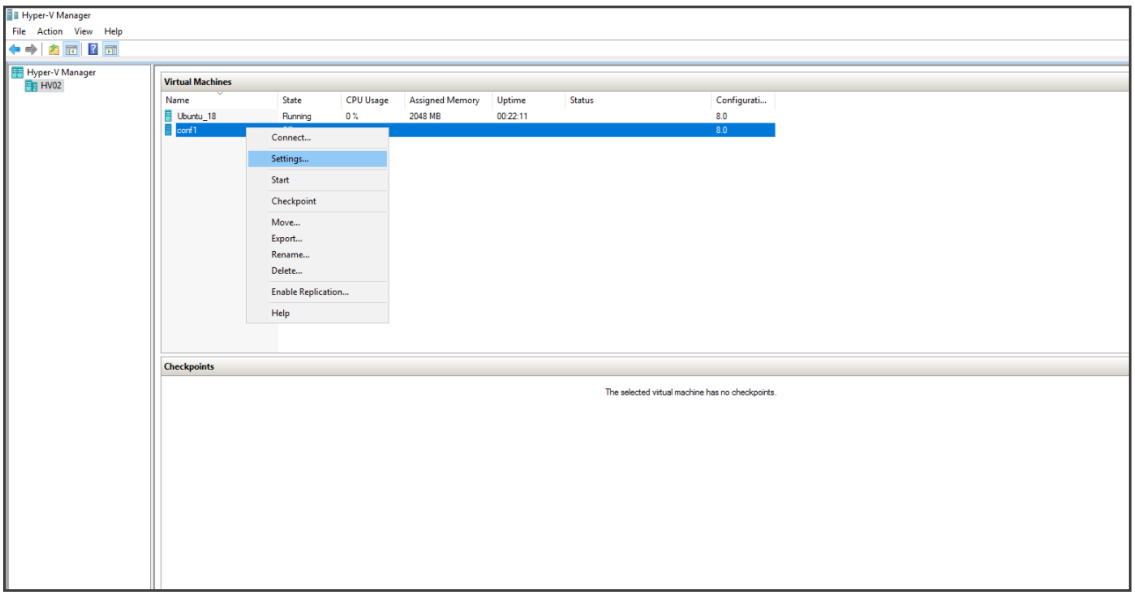


You now need to change the number of CPU cores to **2** in the ARM Router and **4** in the ARM Configurator, for each VM.

➢ To change the number of CPU cores for each VM:

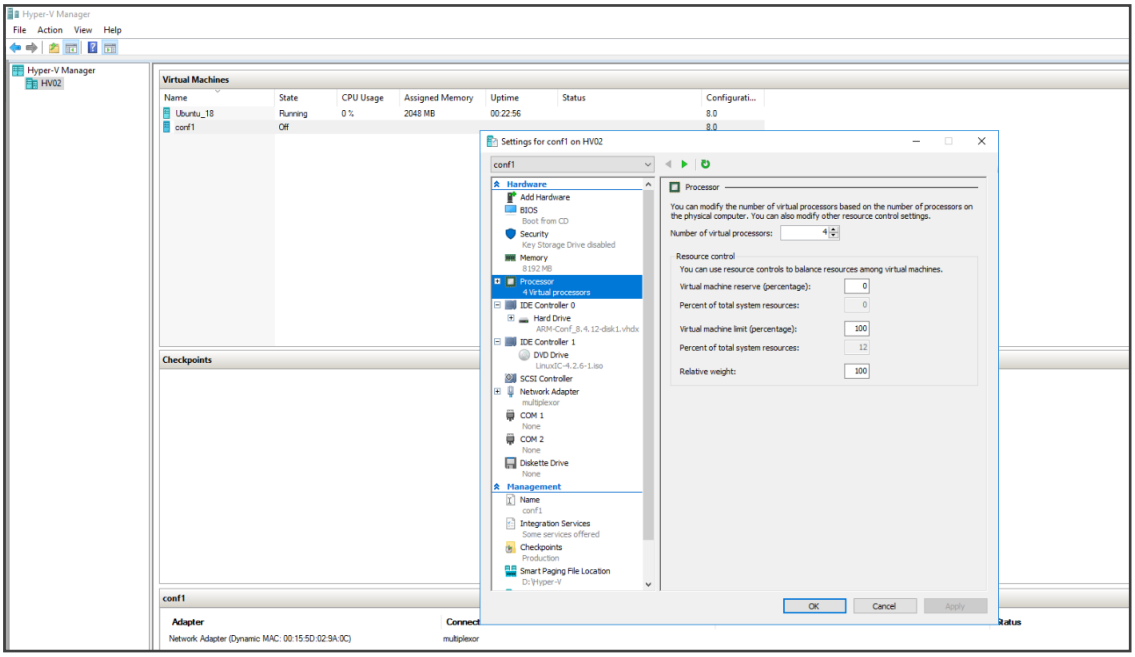
1. In Hyper-V Manager, right-click the VM and from the pop-up menu select **Settings**.

Figure 2-17: Settings



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

Figure 2-18: Processor



3. Click **OK**.

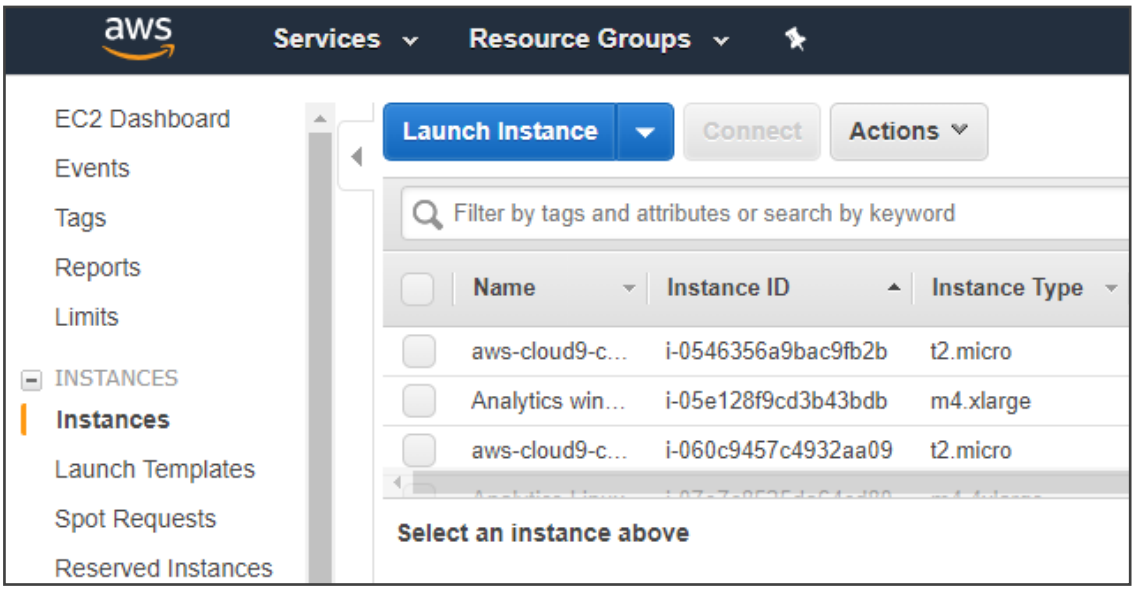
Deploying the ARM's AMIs on AWS

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

➢ To deploy the ARM's AMIs on AWS:

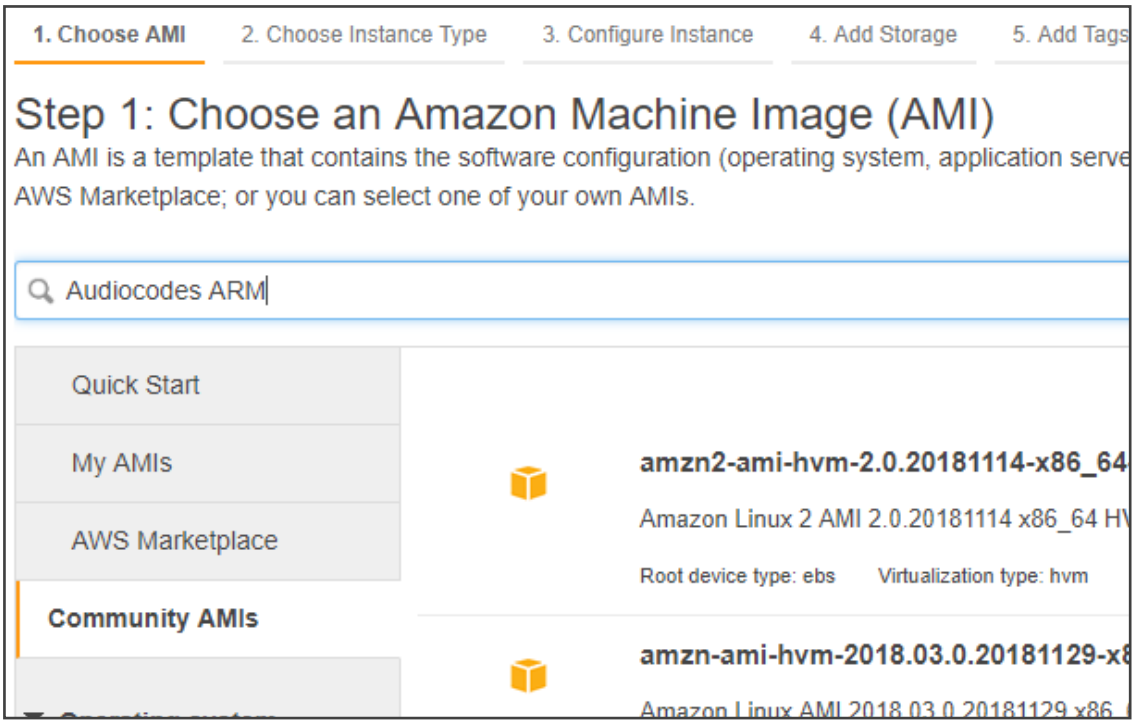
1. In the AWS console EC2, go to **Instances** and click **Launch Instance**.

Figure 2-19: Launch Instance



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

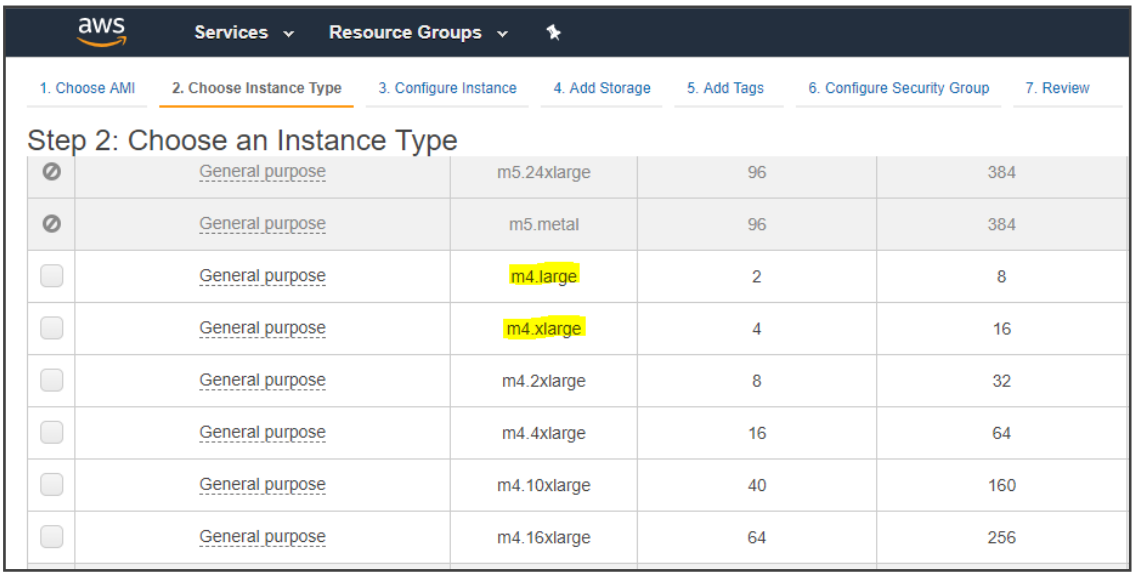
Figure 2-20: Community AMIs



3. Select the **ARM configurator** and then the **ARM router** of the correct version.

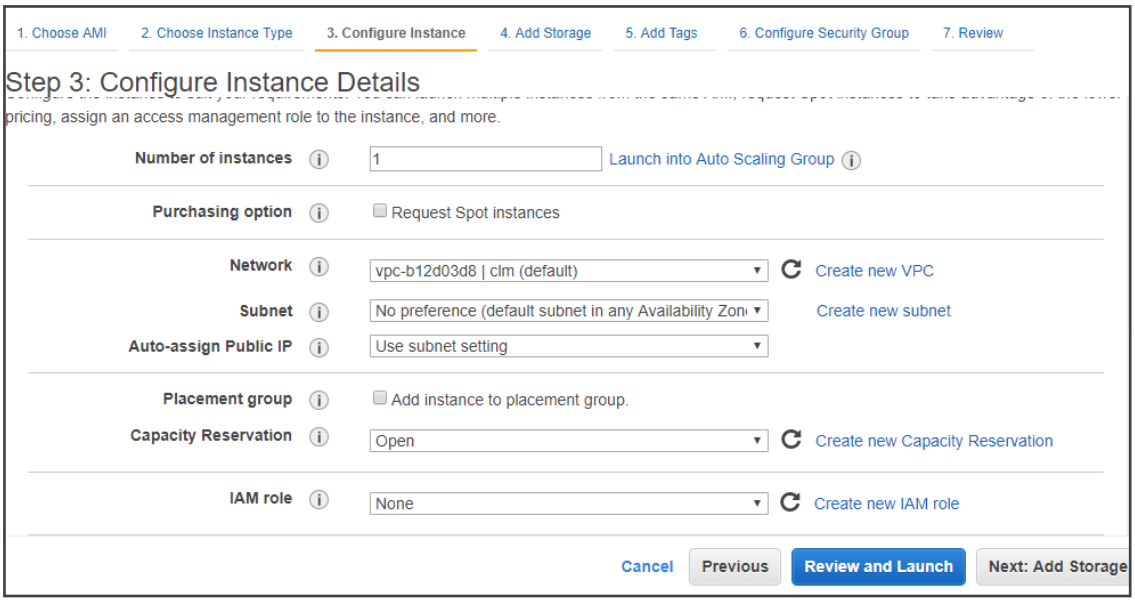
4. Select **Instance Type**: For Router, select **m4.large** and for configurator, select **m4.xlarge**.

Figure 2-21: Instance Type



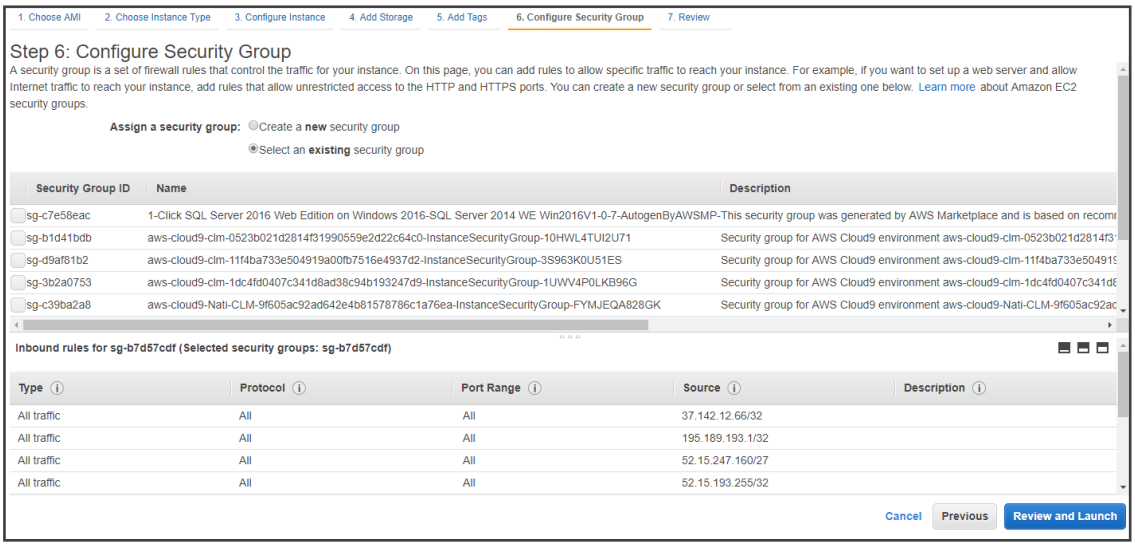
5. Select the correct IAM role, network and subnet to suit your network environment and AWS account environment (for more information, see the *AWS documentation*), and then click **Next** three times.

Figure 2-22: Configure Instance Details



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

Figure 2-23: Security Group



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

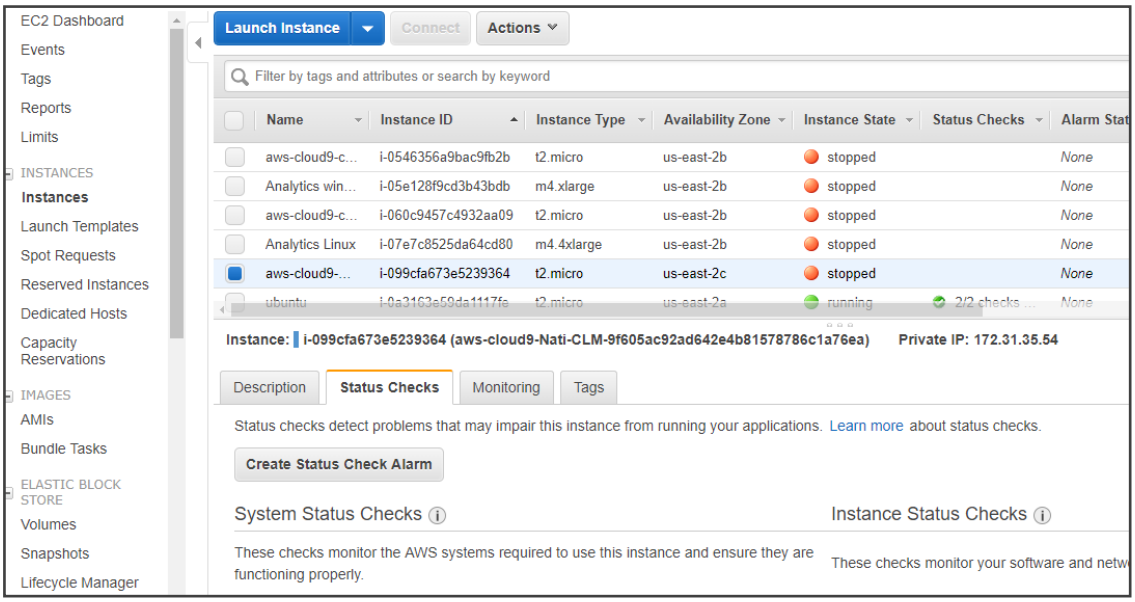
Online upgrade of the ARM on AWS is performed in the same way as on VMWare.

➢ To set up High Availability:

Configure auto-recovery in case hardware failure occurs:

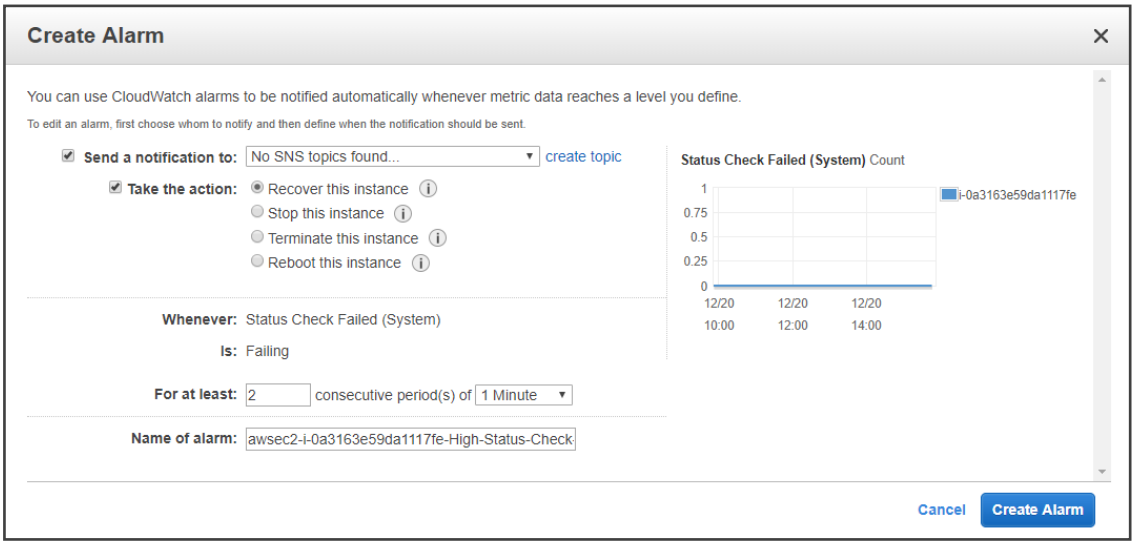
1. In the AWS console, go to **EC2** and then **Instances**.
2. Select your ARM VM Instance.
3. Go to the **Status Checks** tab.
4. Click **Create Status Check**.

Figure 2-24: Create Status Check



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

Figure 2-25: Take the action > Recover this instance



6. Click **Create Alarm**.

Configure auto-reboot in case VM failure occurs:

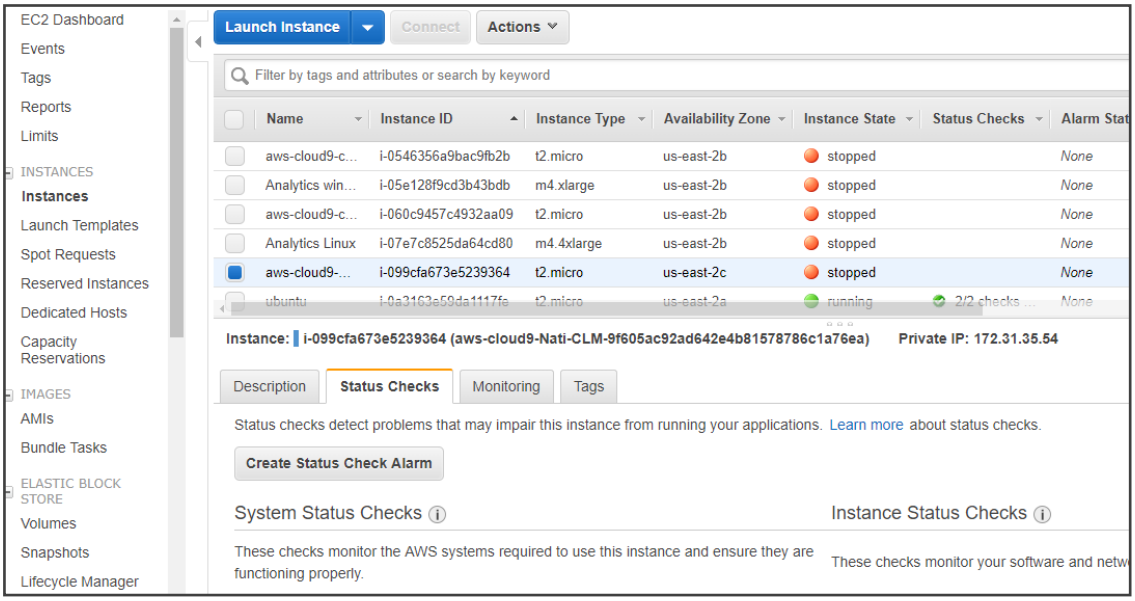
7. In the AWS console, go to **EC2** and then **Instances**.

8. Select your ARM VM Instance.

9. Go to the **Status Checks** tab.

10. Click Create Status Check.

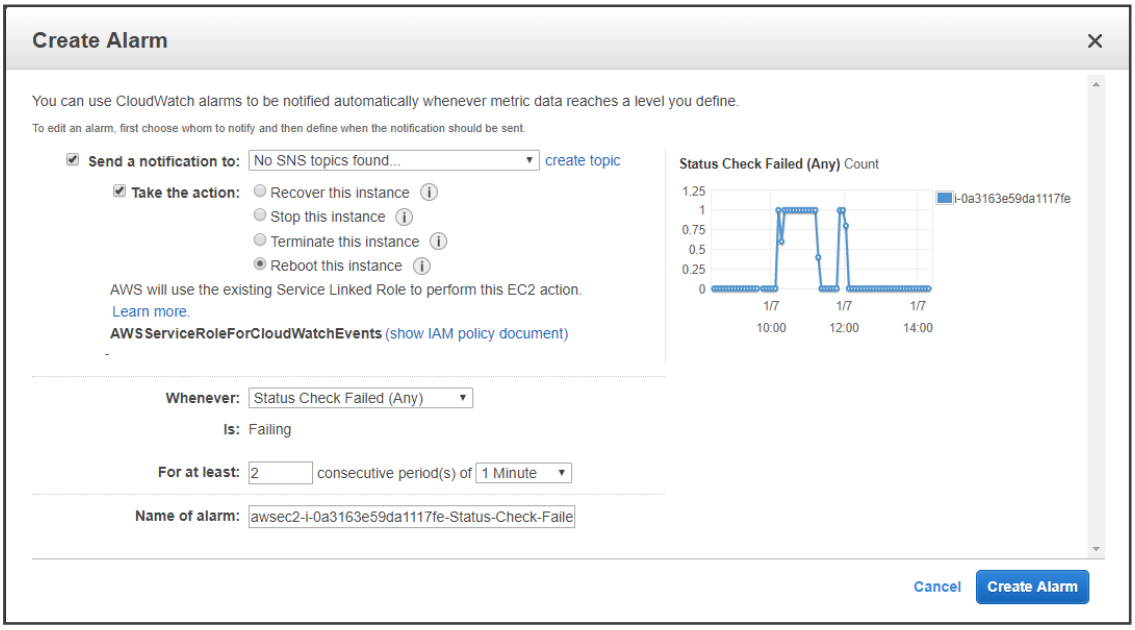
Figure 2-26: Create Status Check



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

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

Figure 2-27: Create Status Check



13. Click **Create Alarm**.

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

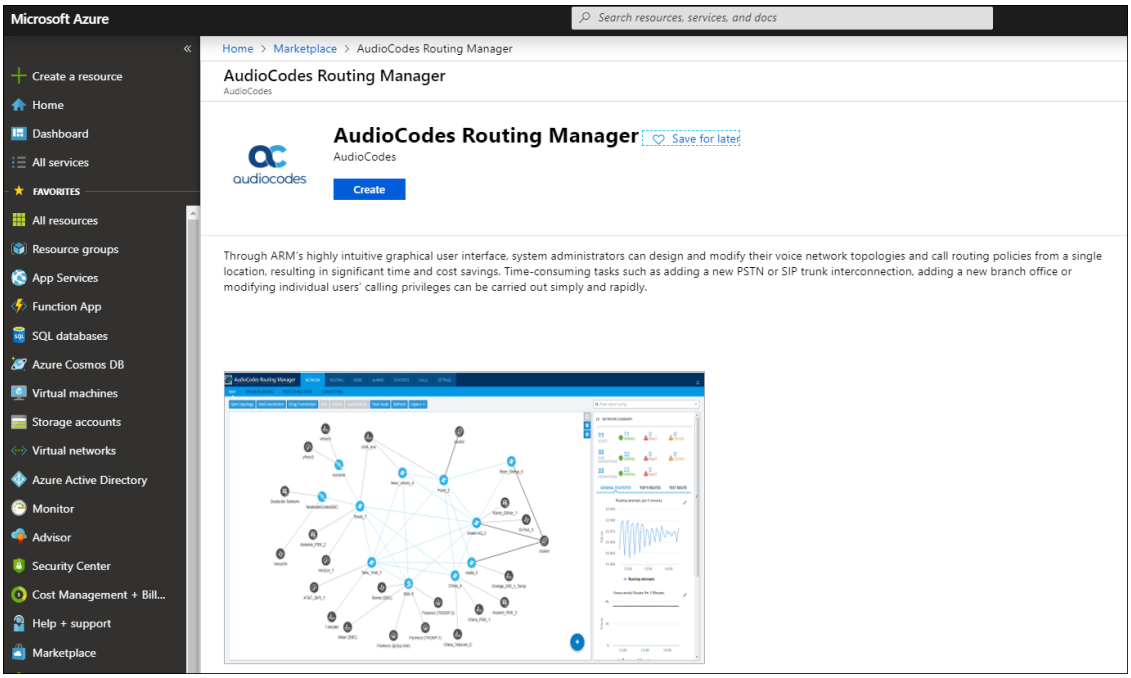
Deploying the ARM from Microsoft's Azure Marketplace

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 3.

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

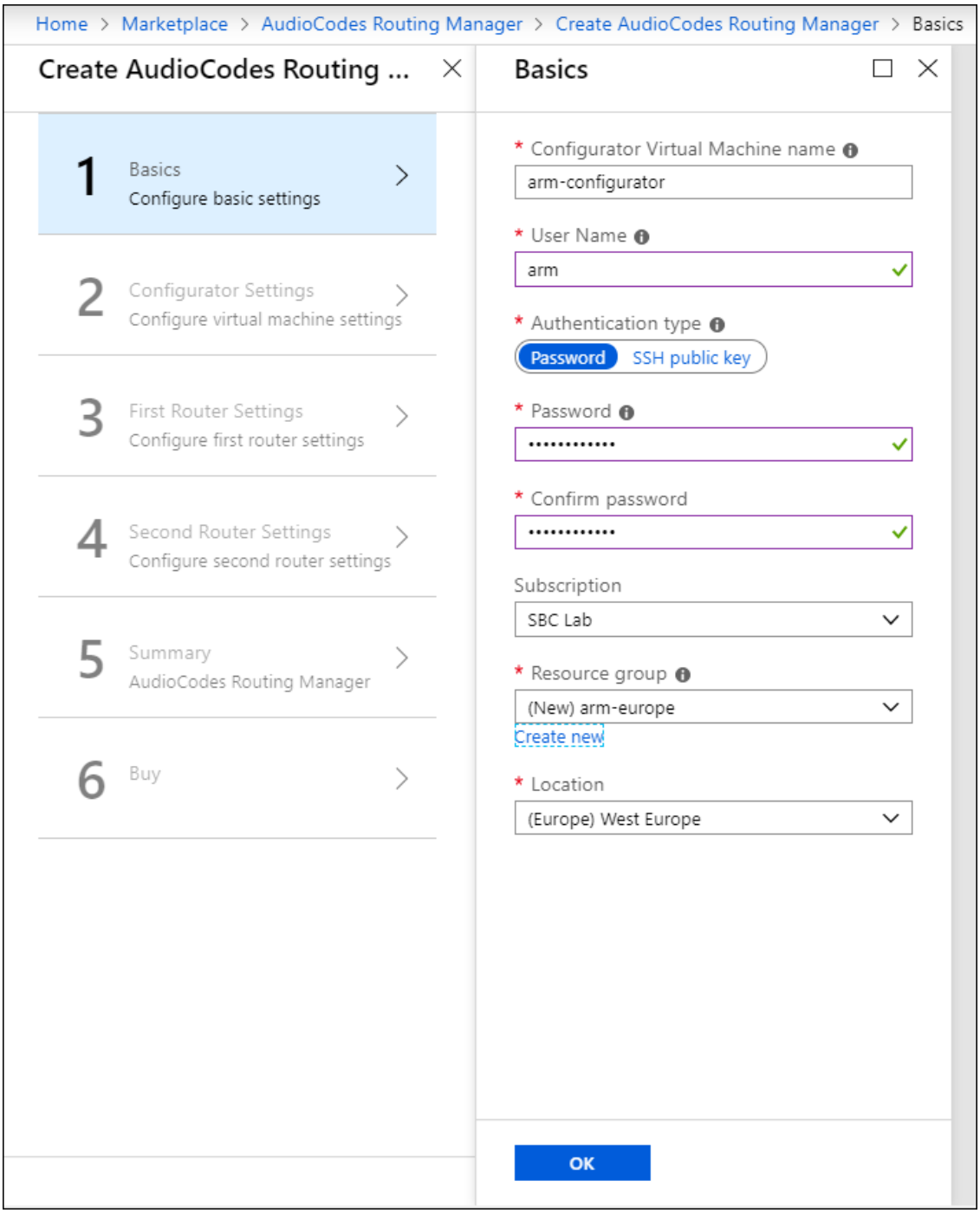
1. In your browser, navigate to Microsoft Azure Marketplace and then search for 'AudioCodes Routing Manager'.

Figure 2-28: Microsoft Azure Marketplace - AudioCodes Routing Manager



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

Figure 2-29: Create ARM (1) Basics



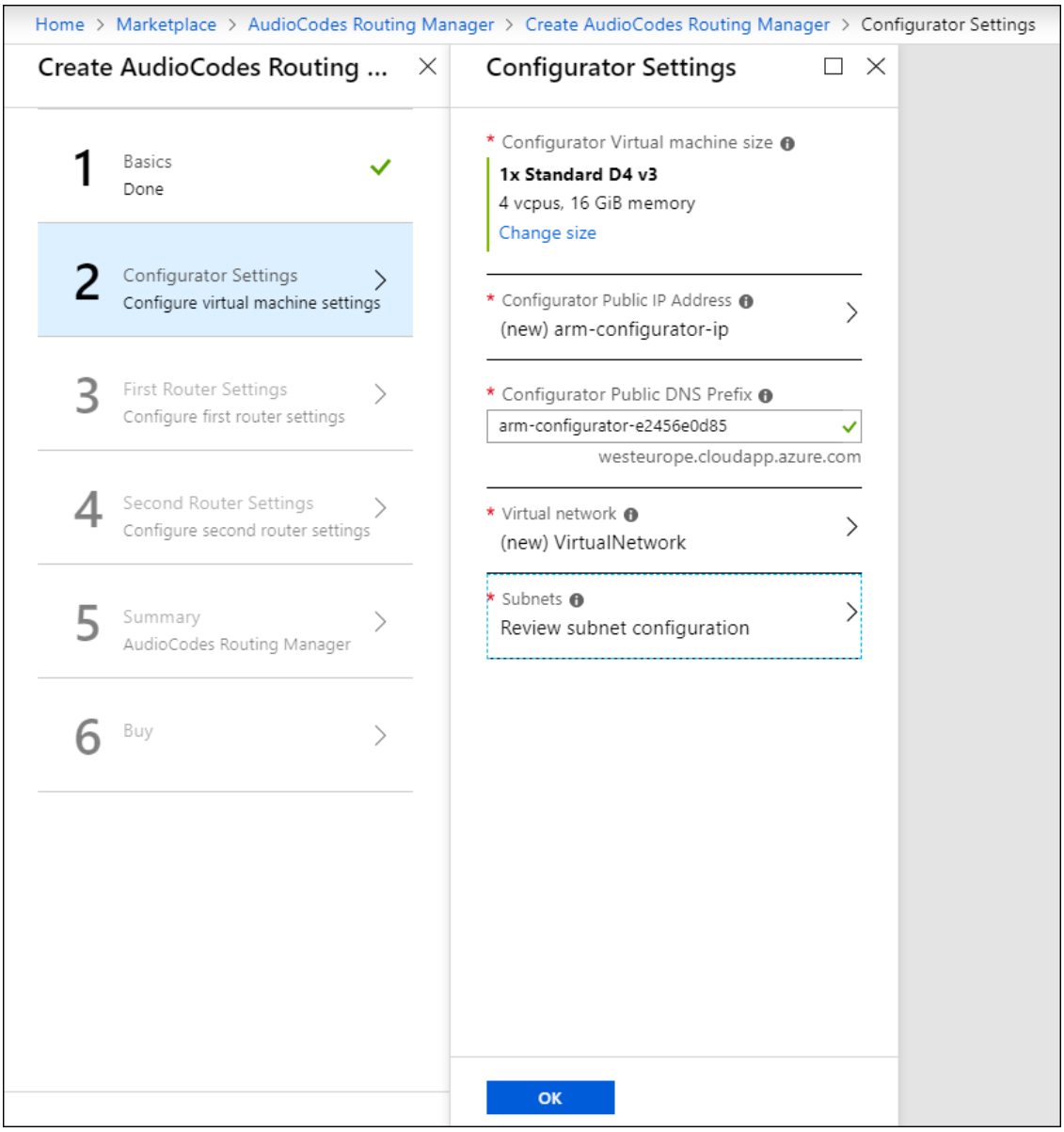
3. Configure Step 1, basic settings. Define the name of the Configurator VM **arm-configurator** as shown in the preceding figure. Use the **i** (information) icon for clarification. This VM is one of two routers that must be defined: ARM Configurator and ARM Router.

4. Define the name of the Configurator VM user, **arm**, as shown in the preceding figure. Use the **i** (information) icon for clarification.

5. For 'Authentication type', select the **SSH public key** option. Use the **i** (information) icon for clarification.

6. In the 'Password' and 'Confirm Password' fields, enter the generated RSA SSH key password. Use the **i** (information) icon for clarification.
7. From the 'Subscription' drop-down, select **SBC Lab**.
8. 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 2-30: Create ARM (2) Configure virtual machine settings

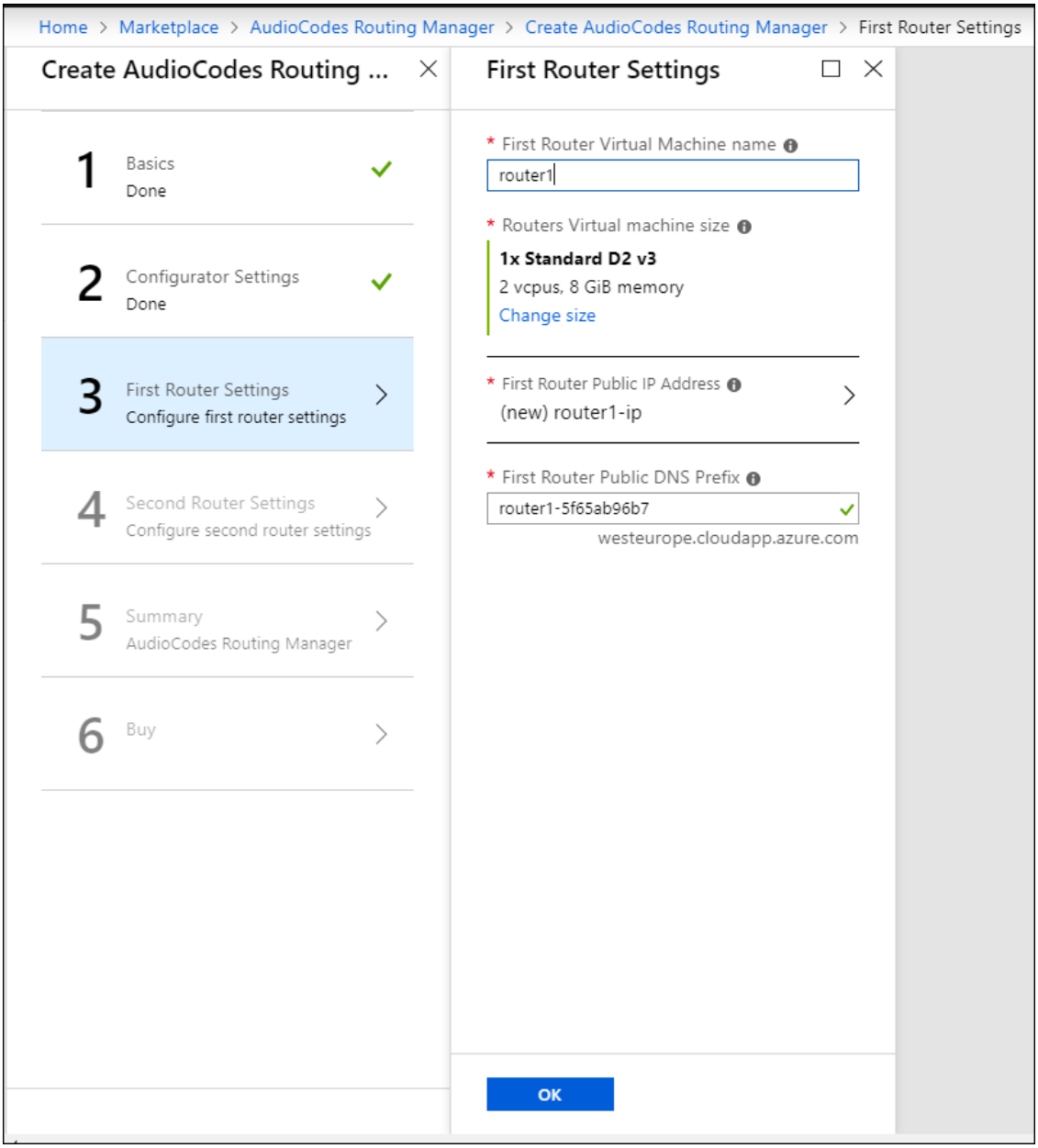


11. In Step **2** in the wizard, click **Change size** and select **D2s_v3** for Router VMs and **D4s_v3** for Configurator VMs. Use the **i** (information) icon for clarification.

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.

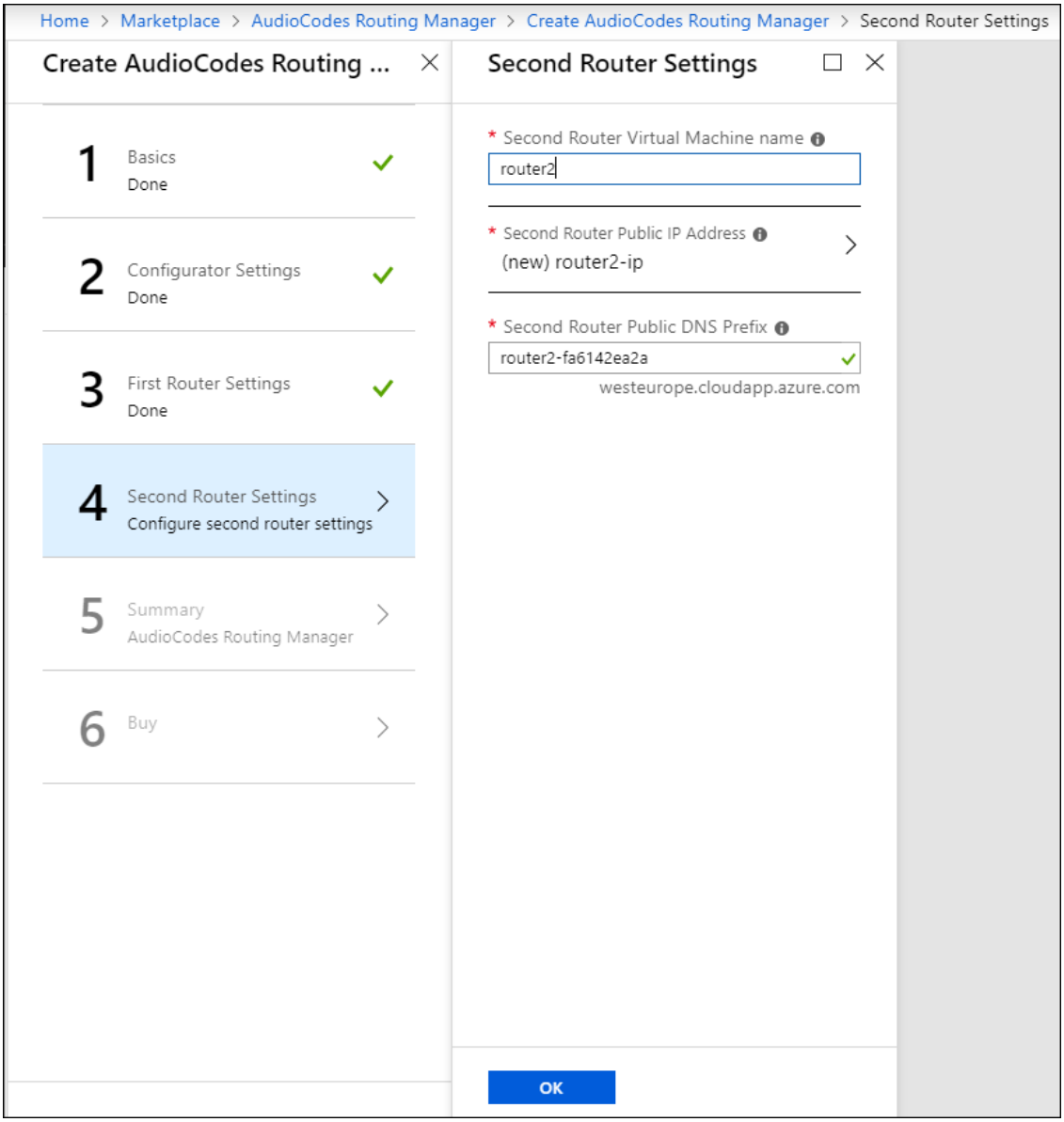
- By default, the ARM uses private IPs but network administrators can opt to change to public IPs. See Moving from Private IPs to Public IPs for more information.
- All VMs should be in the same virtual network and in the same subnet. All VMs should be in a security group that allows all
  - ✔ outgoing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

Figure 2-31: Create ARM (3) First Router Settings



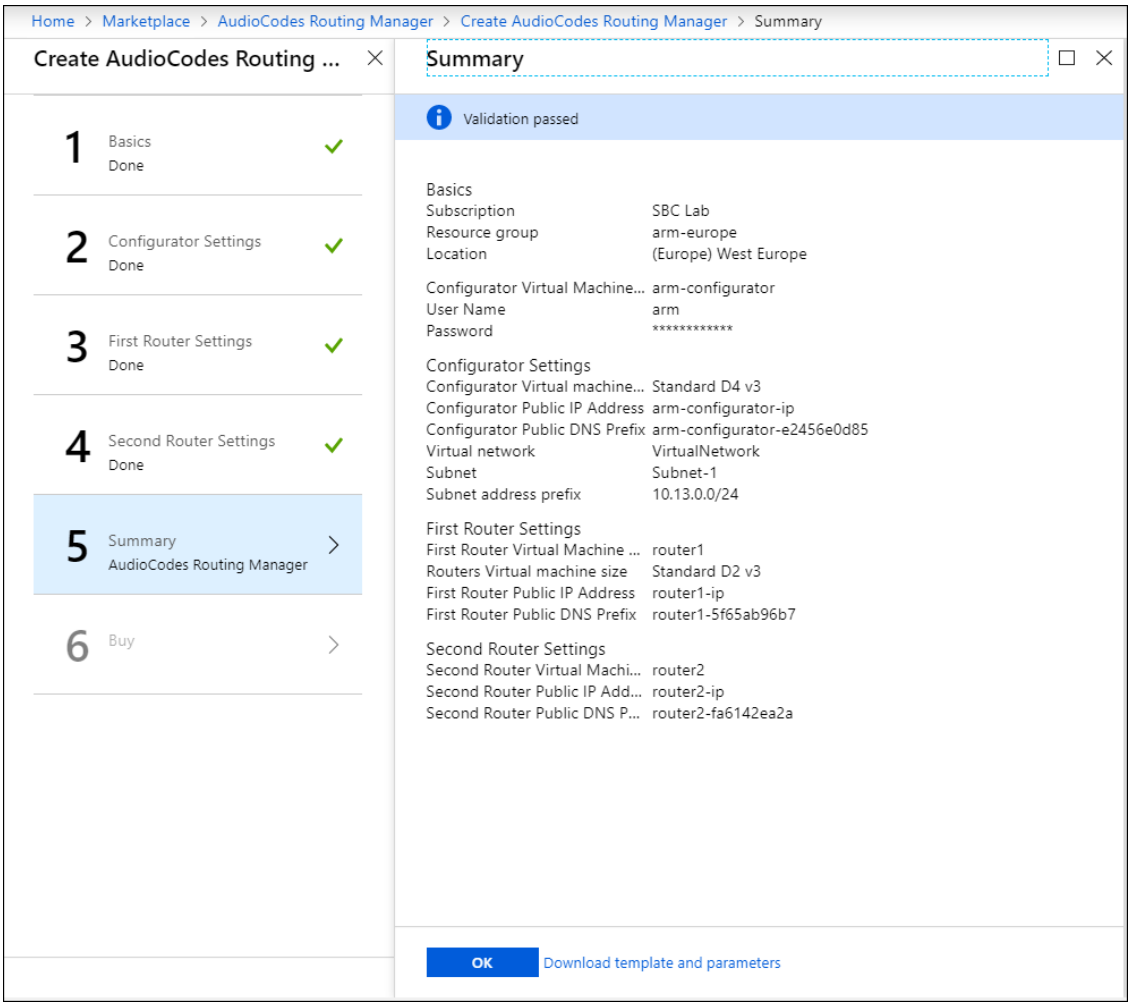
13. Define the settings of the first router. Use the **i** (information) icon for clarifications. Click **OK**.

Figure 2-32: Create ARM (4) Second Router Settings



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

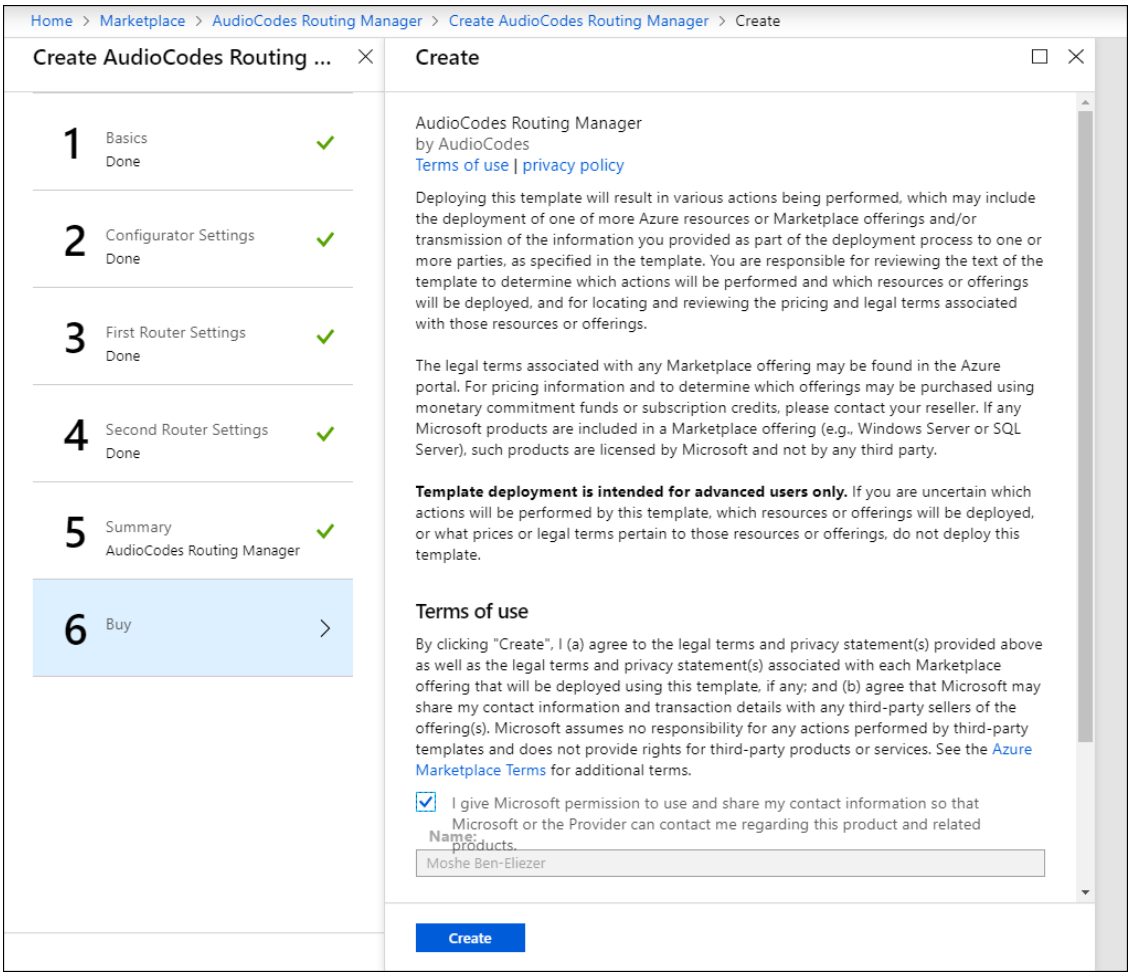
Figure 2-33: Create ARM (5) Summary



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 2-34: Create ARM (6) Buy



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 32)
3. Delete the ARM if necessary (see Deleting the ARM Deployed through the PowerShell CLI on page 35)

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 = "80"
$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 29, you can deploy the ARM environment, namely, the ARM Configurator as shown in Deploying the ARM Environment - ARM Configurator on page 29 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.

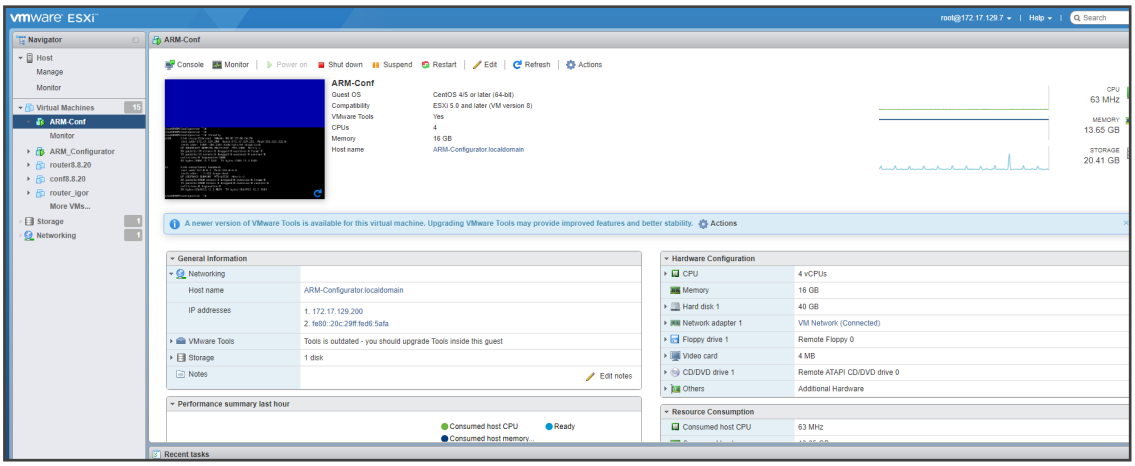
Initial configuration involves configuration of a static IP address and hostname for the VM.

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



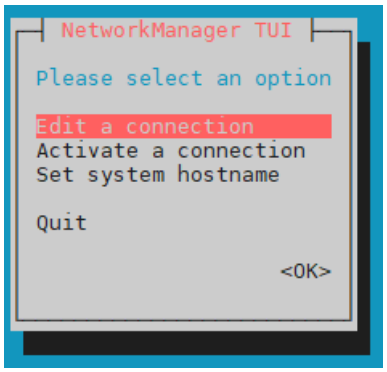
➢ To configure a static IP address and hostname for the VM:

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 **armAdmin** for username and **Arm!default1** for password.
3. Run the following commands:

```
su -
Password:password
nmtui
```

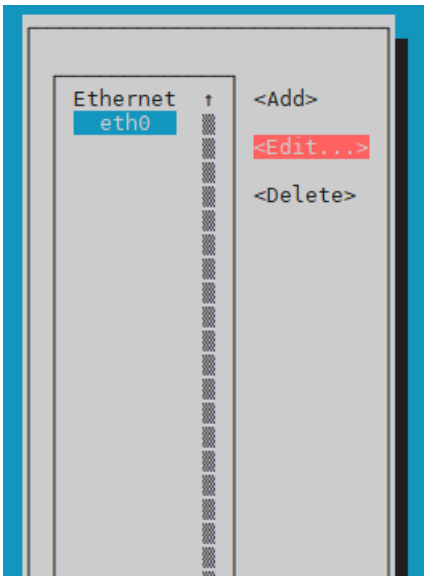
4. You're prompted for a Text User Interface.
5. Select **Edit a connection**.

Figure 3-2: NetworkManager TUI - Edit a connection



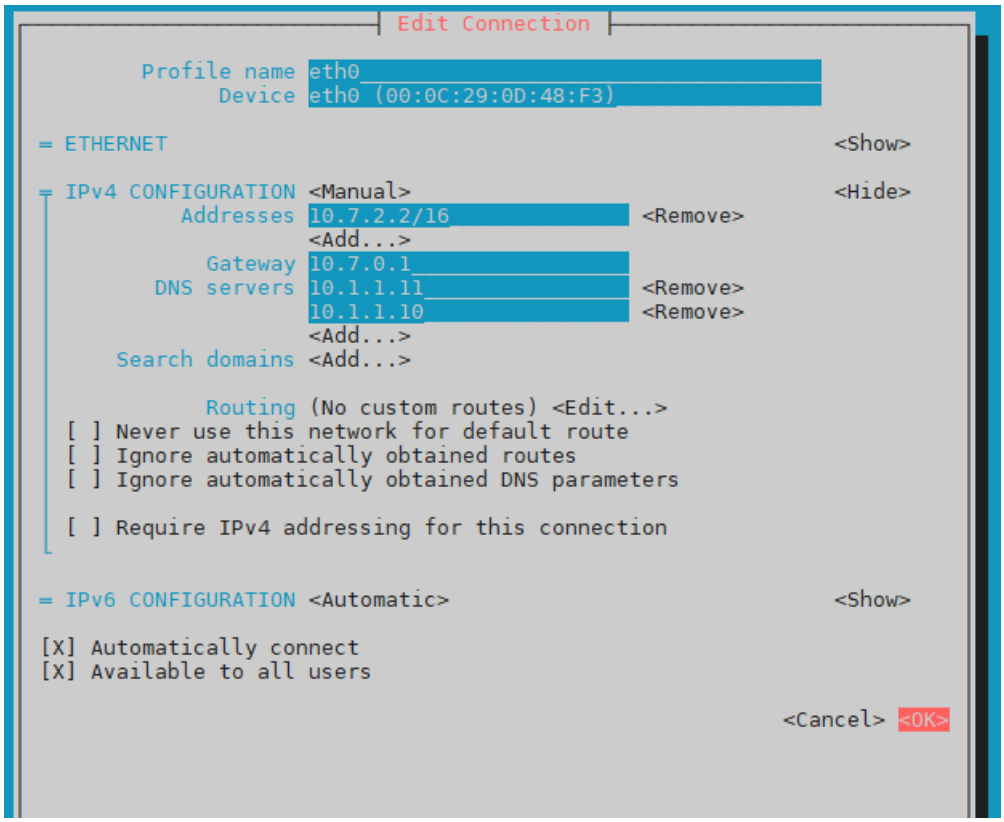
6. Select **eth0** and **Edit**.

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. Use the following figure as a configuration reference.

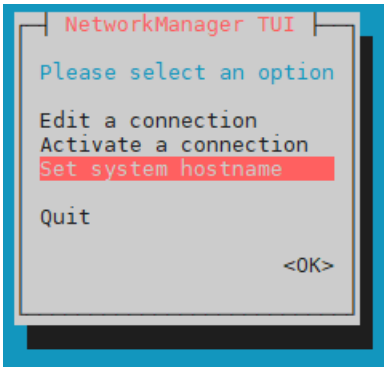
Figure 3-4: Edit Connection



Select **OK** and then in the next screen, select **Back**.

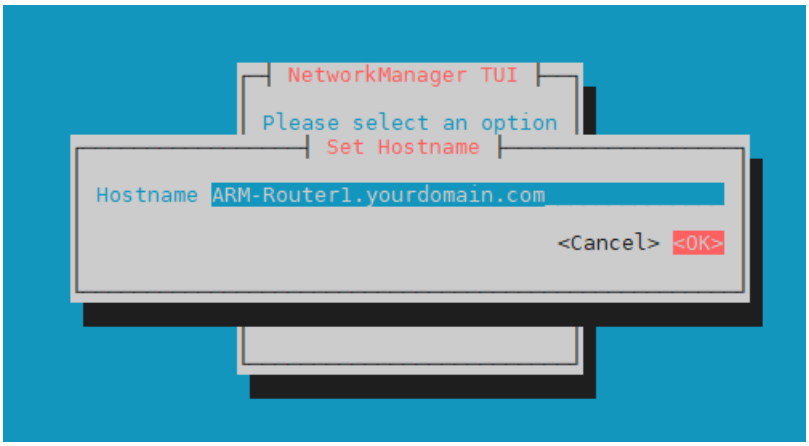
8. Select **Set system hostname**.

Table 3-1: Set system hostname



9. Enter a new hostname, for example, **ARM-Router1.yourdomain.com**

Figure 3-5: Set Hostname



10. Select **OK** and then in the next screen, select **OK** to exit the Text User Interface.

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

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

```
reboot
```

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

13. 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)

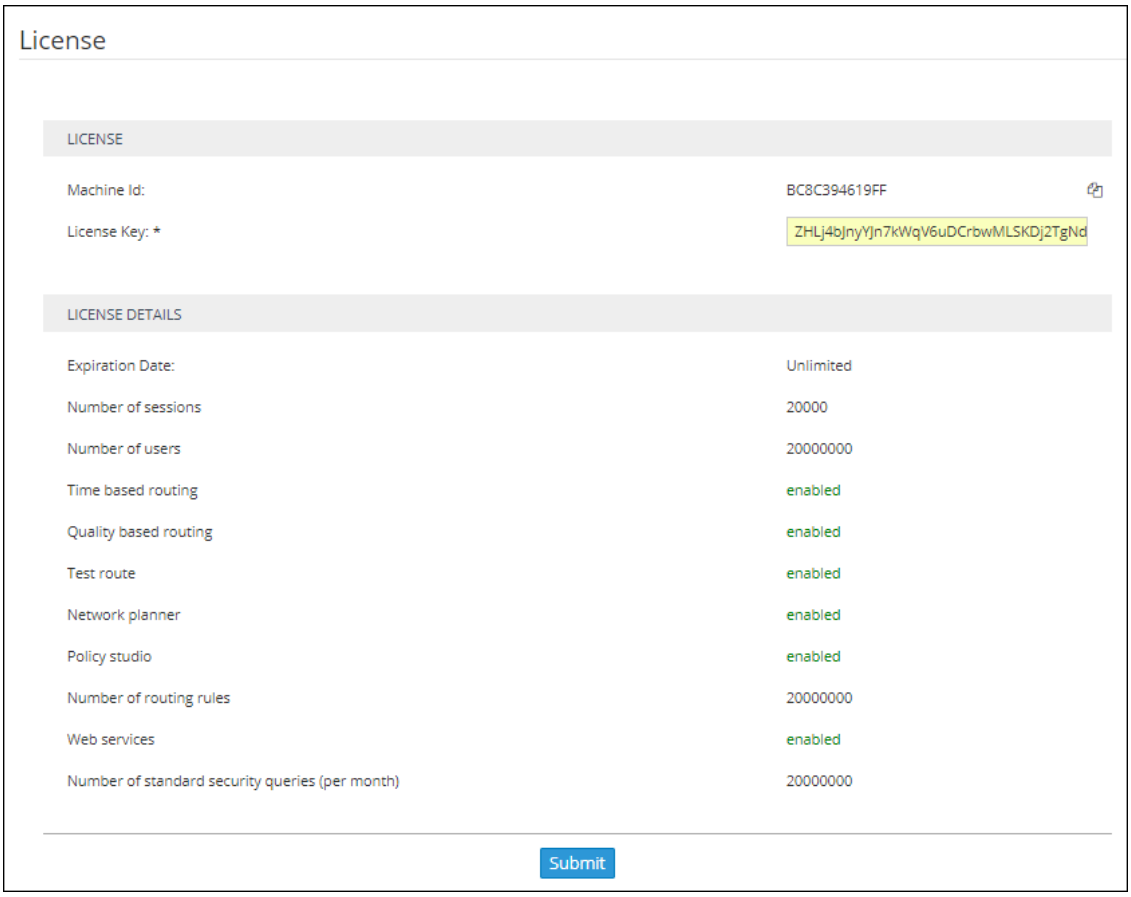
- Network Planner (can be either enabled or disabled)
- Policy Studio (can be either enabled or disabled)
- Number portability
- Number of standard security queries (per month)
- Analytics View
- Number of users route registrations

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 3-6: License



2. Select and copy the 'Machine ID' shown 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, shown 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.

> The ARM supports a license key for *security-based routing*. The License Details in the preceding figure display the 'Number of standard security queries (per month)' purchased by the customer. This number does not indicate the dynamic information of the remaining number of queries available on the security server but rather *the number of queries per month that were ordered*.

The ARM additionally features *enforcement based on this value*. If 'Number of standard security queries' = 0, the customer will not be able to define an external Web service for pre-routing call security score consultation with SecureLogix's Orchestra One CAS (Call Authentication Service).

> A customer upgrading to ARM 9.0 from a previous ARM load can use the ARM with an existing license key; it's unnecessary to regenerate a new license though if the customer wants to use security-based routing, the license for security queries should be purchased from AudioCodes and a new ARM license (with enabled security queries) will be provided.

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.

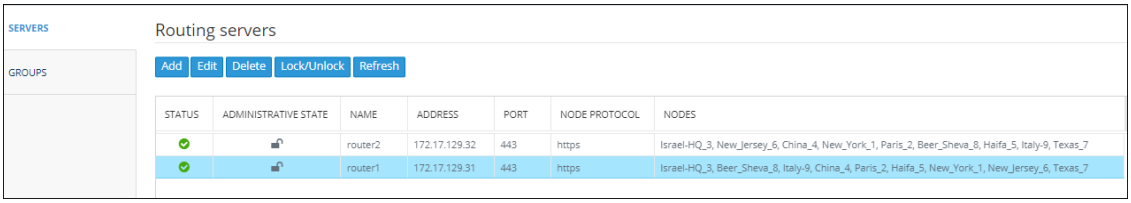
Defining Routing Servers

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:

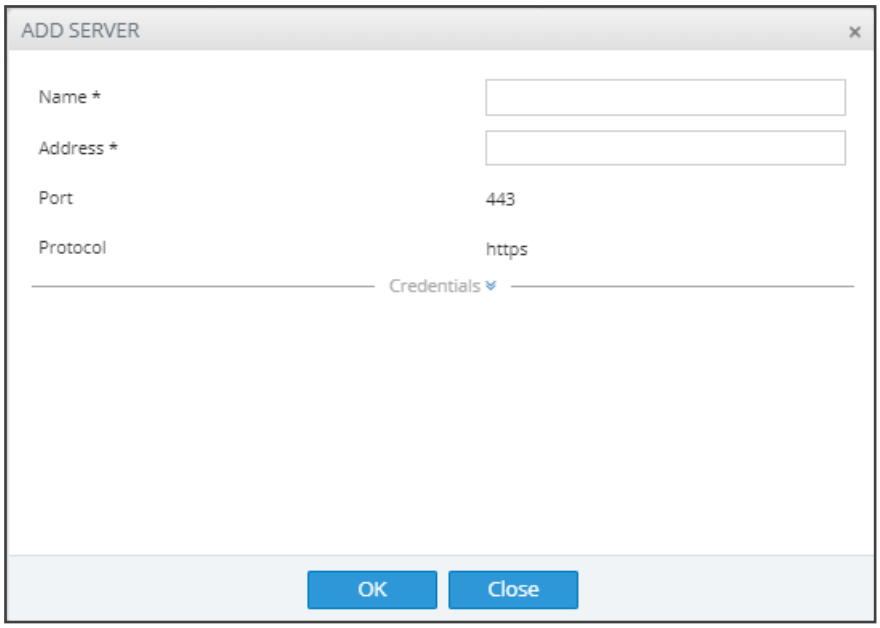
1. In the ARM GUI, open the Routing Servers page (**Settings** > **Routing Servers** > **Servers**).

Figure 3-7: Routing Servers



2. Click **Add**.

Figure 3-8: Add Server

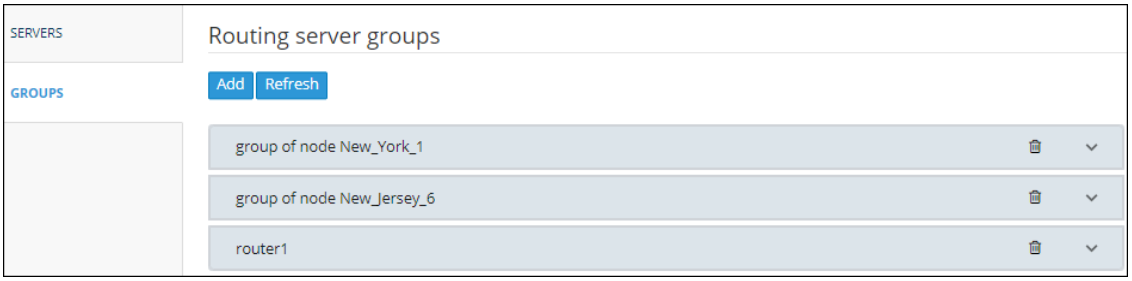


3. Configure the Routing Server VM to connect to the device.
4. Point the Routing Server to the VM's IP address or Host name.

➢ To define a Routing Server Group:

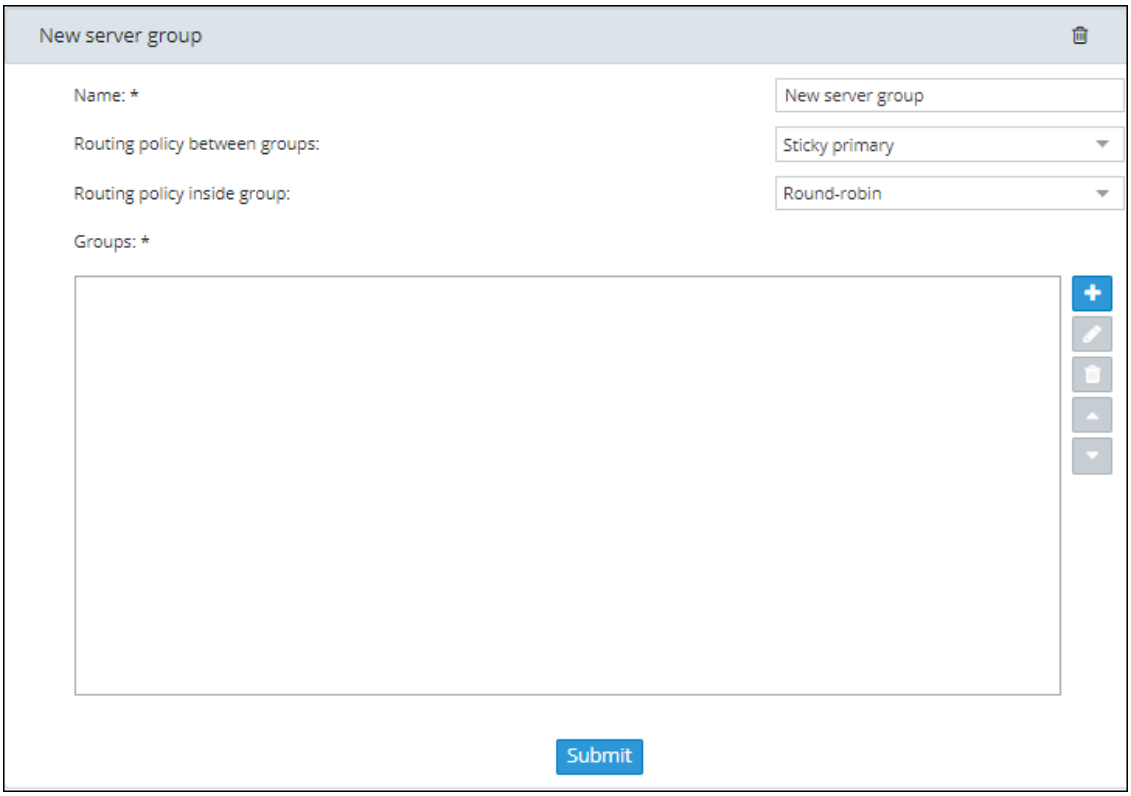
1. In the ARM GUI, open the Routing Servers page (**Settings** > **Routing Servers**) and then click **Groups**.

Figure 3-9: Routing Server Groups



2. Click **Add**.

Figure 3-10: New server group



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 47.

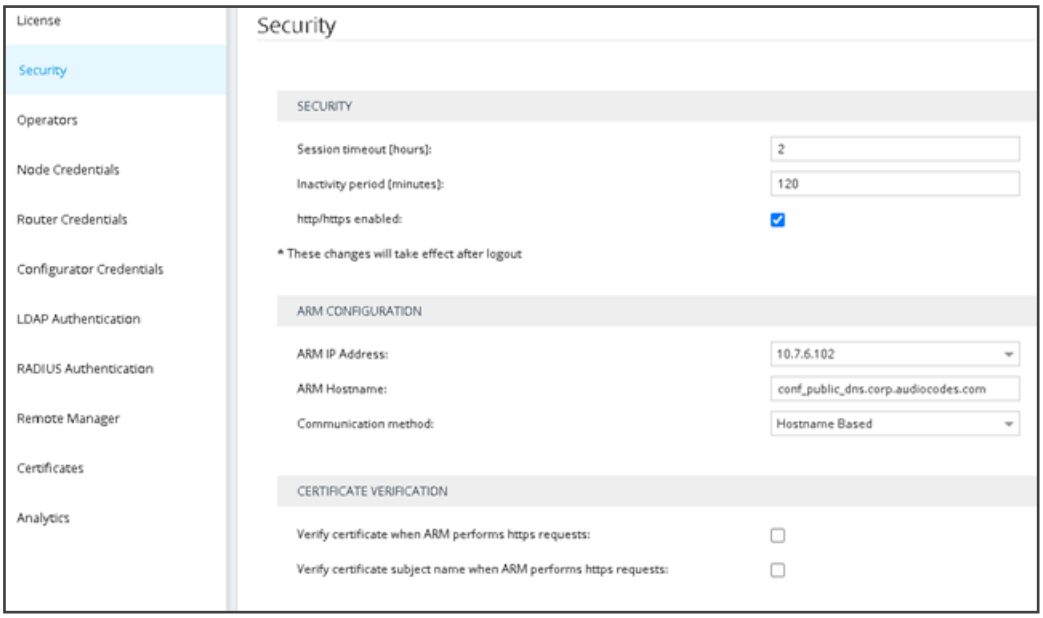
Public IP / DNS (Host Name)

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

➢ To configure the ARM Configurator:

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

Figure 4-1: Security

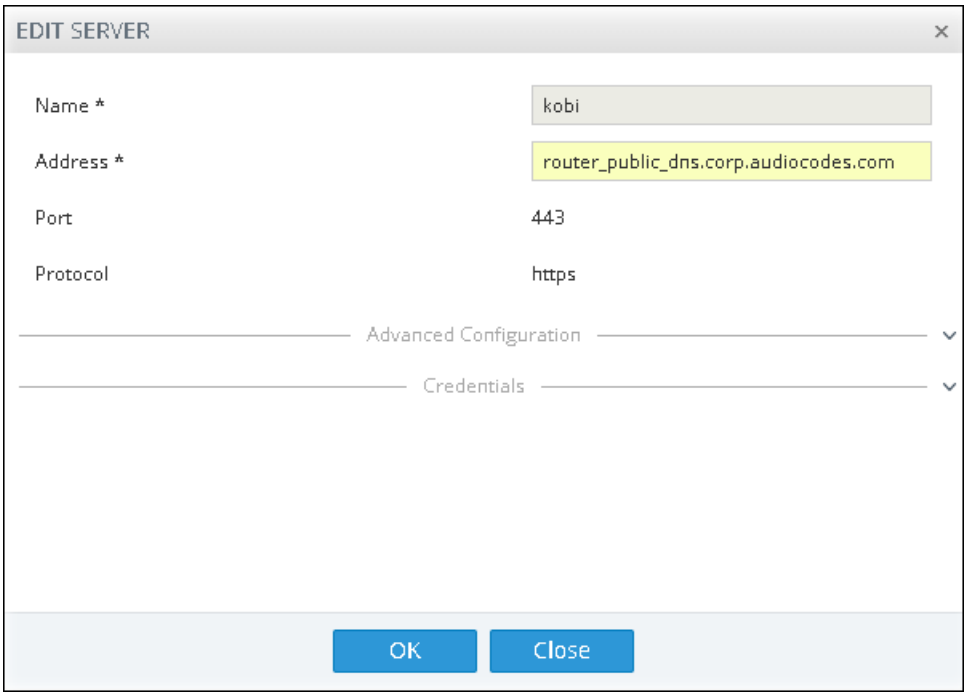


2. Paste the public DNS or the public IP of the ARM Configurator in the 'ARM Hostname' field under the ARM Configuration page section.
3. Set the 'Communication method' to **Hostname Based**.

➢ To configure the ARM Router:

1. In the ARM GUI, open the 'Routing servers' page (**Settings** > **Routing Servers** > **Servers**) and configure routers with a Public DNS (not the public IP).

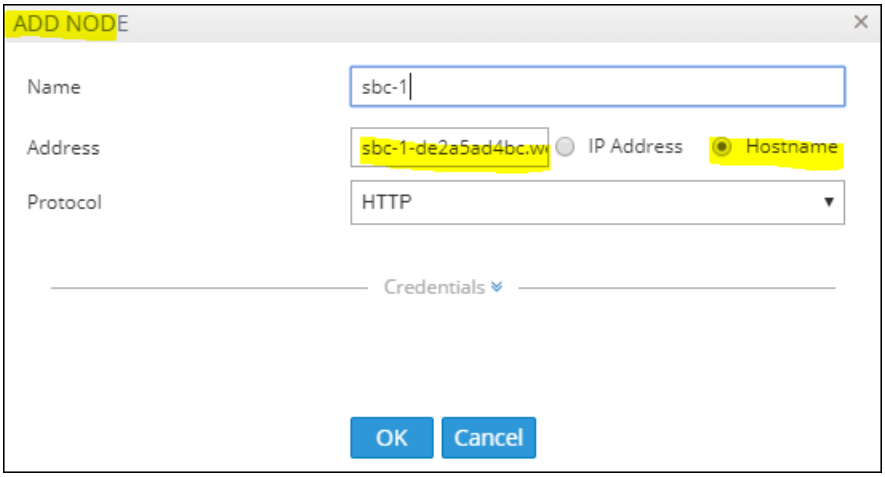
Figure 4-2: Routing servers page



➢ To configure a node:

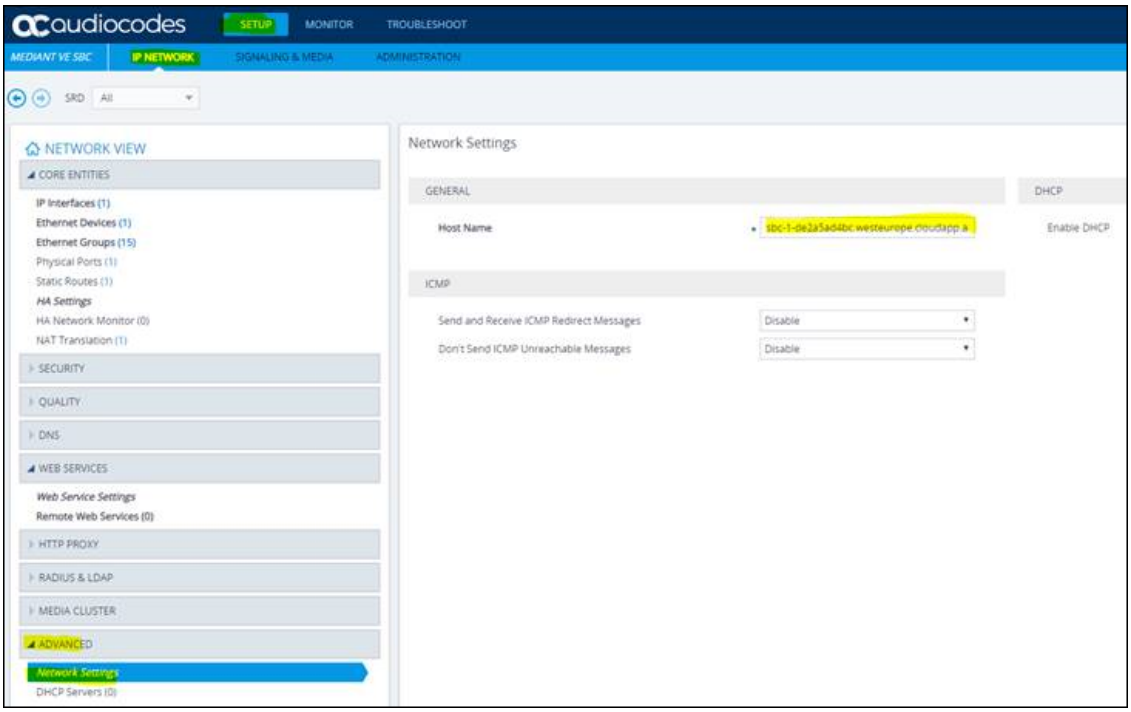
1. When adding a node, select **Hostname** in the Add Node screen in the ARM GUI.

Figure 4-3: Hostname in the Add Node screen



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

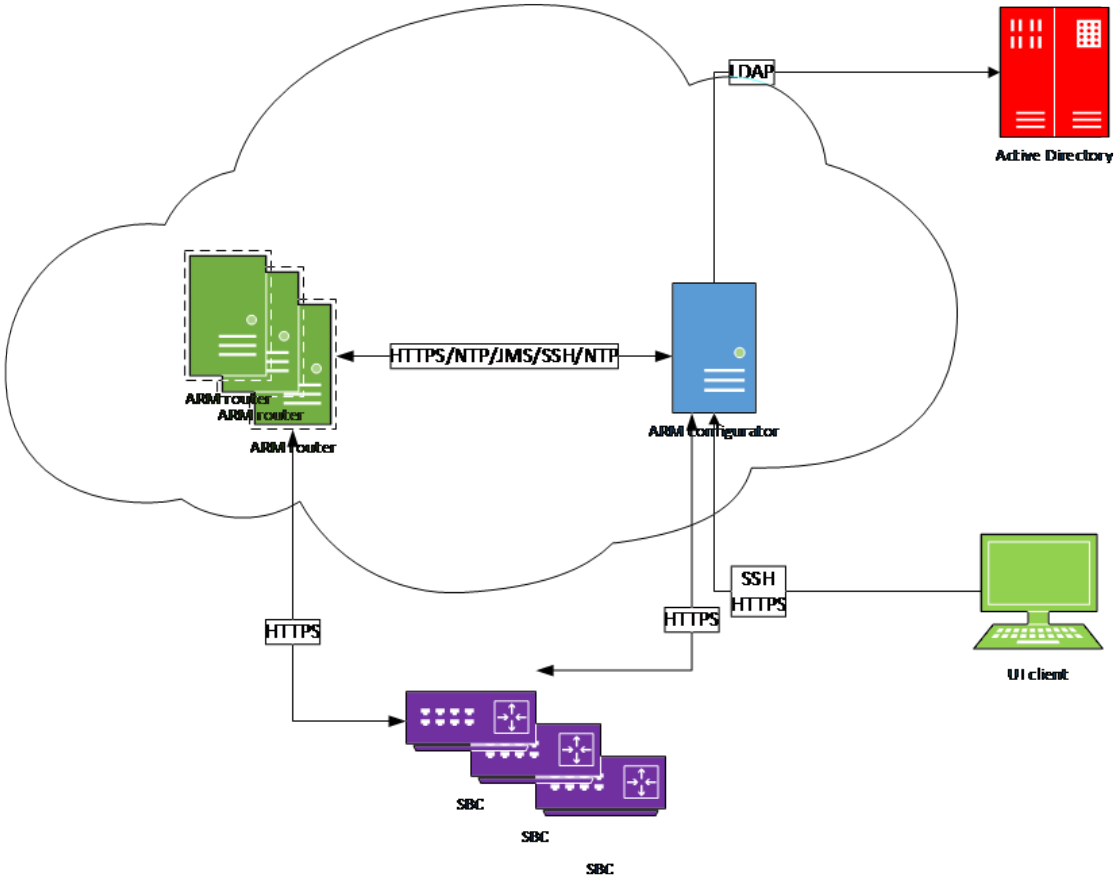
Figure 4-4: Web Interface Network Settings



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

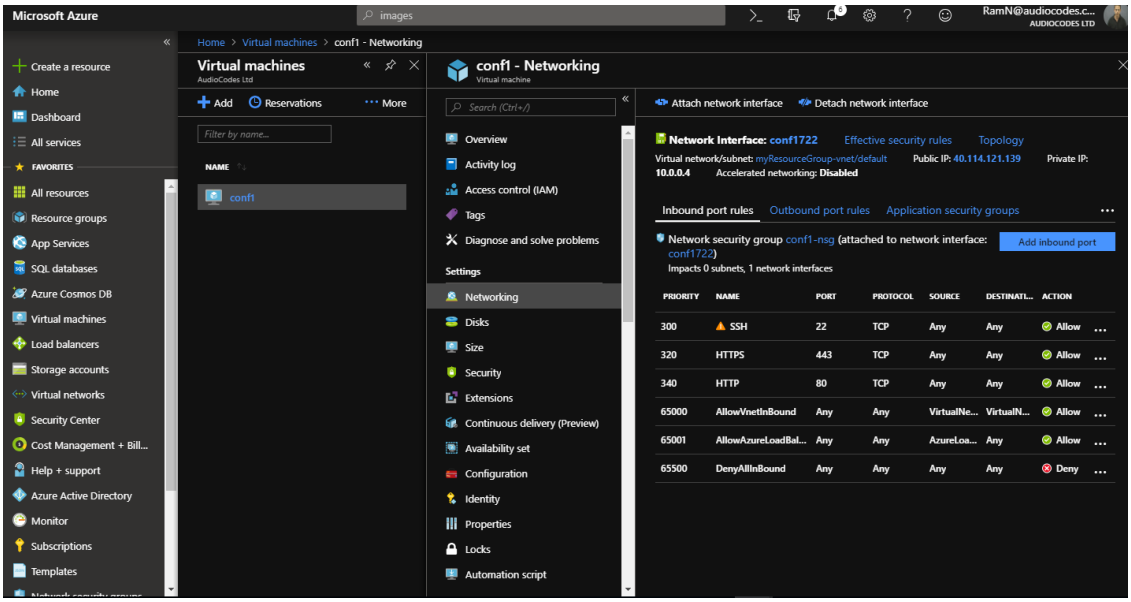
Go to **Virtual machines**, click the VM and then **Networking**.

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

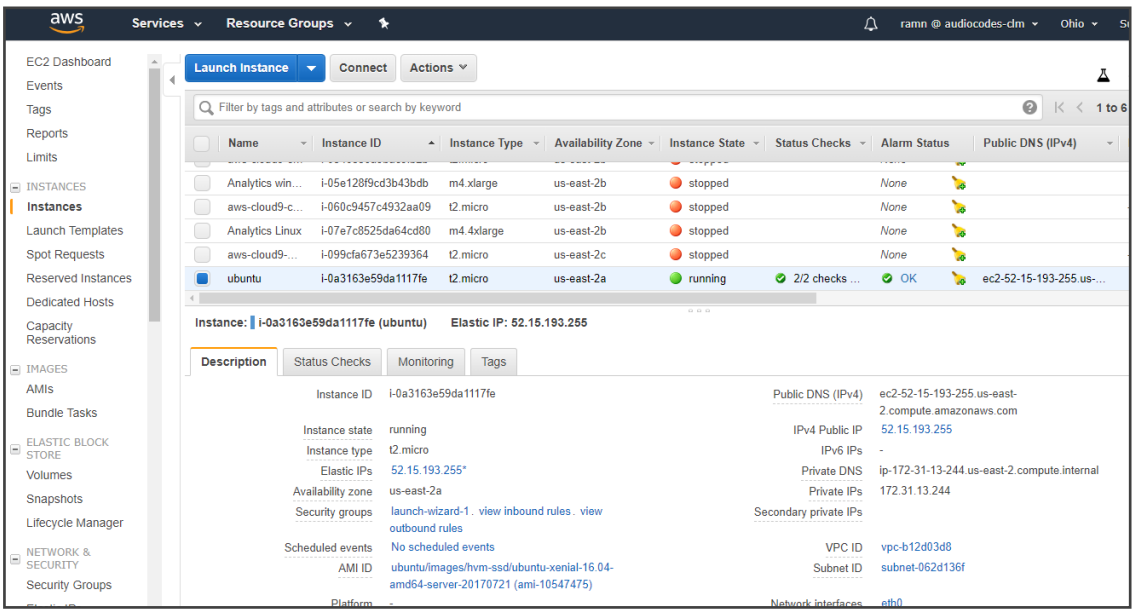


On AWS

➢ To configure:

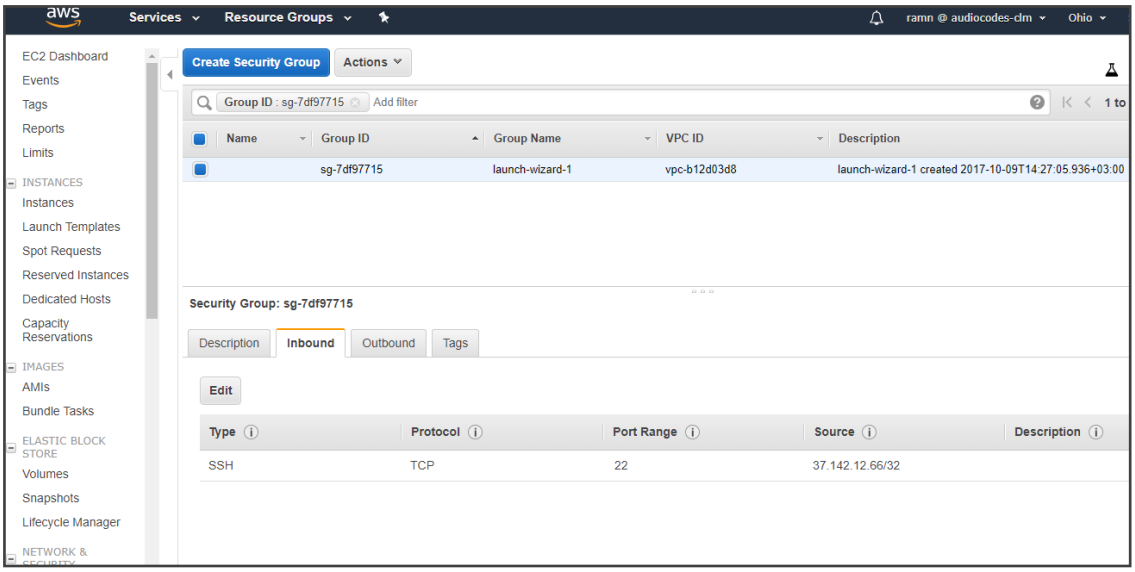
1. In the AWS console EC2, go to **Instances**, click the instance and then under the **Description** tab, click the security group.

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

ARM 9.4+ indicates *ARM version 9.4 or later*.

Operators 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 goes down at a time. Routers can operate temporarily without the Configurator so there's no downtime and the impact on the ARM is minimal. After the initial operator enters inputs (answers a few questions and enters their password), the upgrade continues and completes without operator interaction. Software upgrade to ARM 9.2 incorporates upgrade to the new OS. ARM 9.2 does not support the old version of CentOS (CentOS 6). The upgrade to ARM version 9.2 can be done only from ARM Version 8.8 or 9.0. To upgrade from earlier ARM versions (8.4 or 8.6), the operator must upgrade first to ARM 8.8 and then upgrade to 9.4+ **(see the APPENDIX)**.

Upgrading from ARM 9.2+ to ARM 9.4+

The following steps are for upgrades from ARM version 9.2 or later to ARM version 9.4 or later. 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 to ARM 9.4+

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 the Configurator Virtual Machine.
5. Obtain the upgrade tar.gz archive file for the version you want to upgrade to.
6. Obtain the **cent9Xupdate-repo.tar.gz** archive file for the version you want to upgrade to. The file contains Linux security updates. Note that this upgrade will take longer due to the Linux update.
7. Copy both files to the '/tmp' directory on the ARM Configurator using SFTP (SSH File Transfer Protocol).
8. Choose a time with low call traffic.

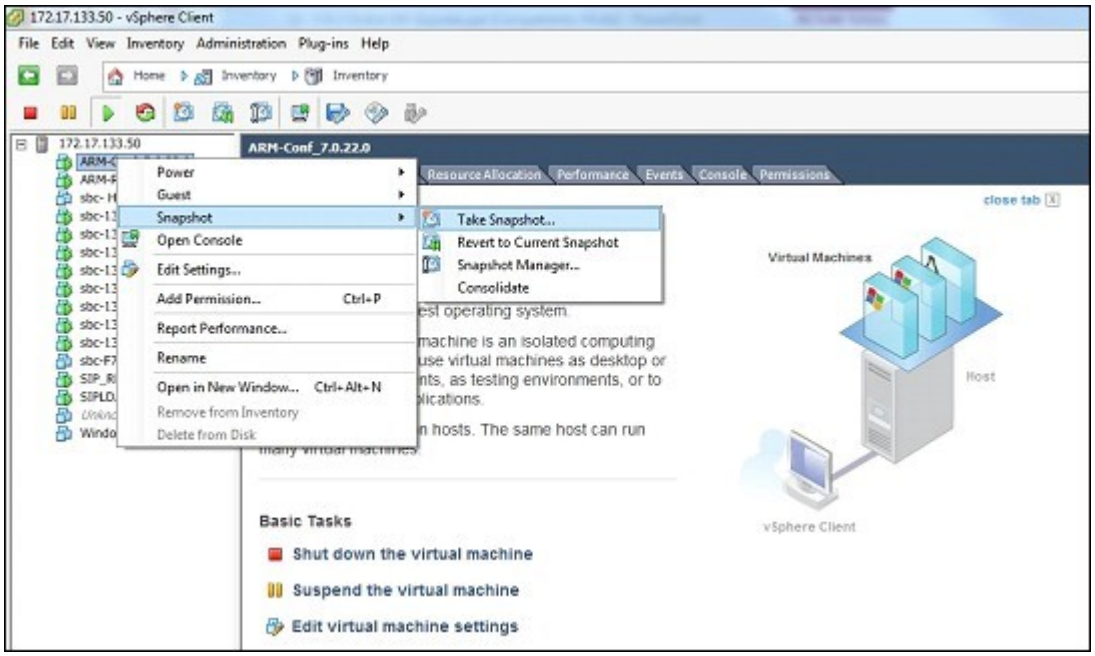
Performing the Upgrade to ARM 9.4+

You're now ready to perform the upgrade.

➢ To perform an upgrade:

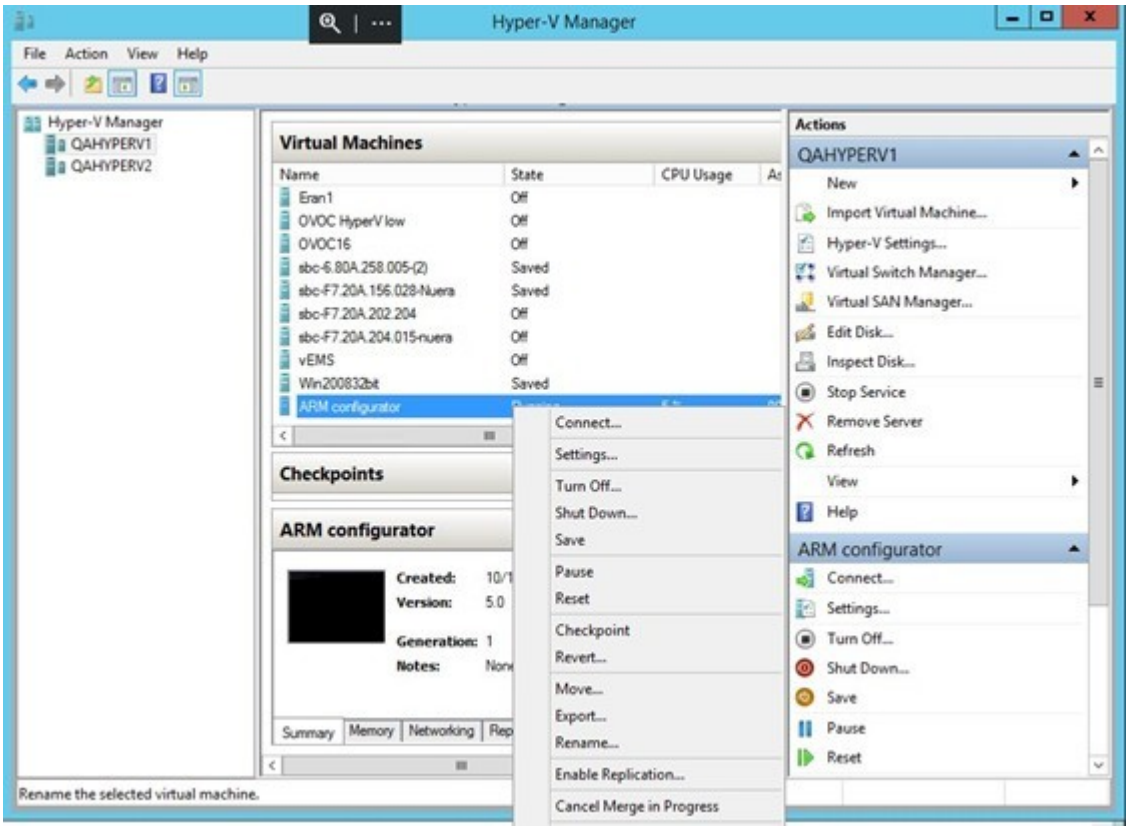
1. Perform a Virtual Machine snapshot of the Configurator and all of the Routers:
   - If you’re on VMWare: In the vSphere client, right-click the **Virtual Machine** and select **Snapshot** > **Take Snapshop**.

Figure 5-1: Take Snapshop



   - 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



- Log into the Configurator using SSH.
- Switch user to **root** by "su –"
- Enter the **root** password.
- Execute the following command:

```
cd /tmp
upgrade_arm < upgrade tar.gz  filename>
```

- Answer **y** to the following question:

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

```
============================
Starting ARM Upgrade
Validating configuration
Exporting certificate
Preparing Routers
About to perform upgrade from 9.2.16 to 9.4.14. Are you sure ? (y - upgrade, other key - quit)
```

- Wait for the notification **ARM has been successfully upgraded…**

Figure 5-4: ARM has been successfully upgraded…

```
============================
Starting ARM Upgrade
Validating configuration
Exporting certificate
Preparing Routers
About to perform upgrade from 9.2.16 to 9.4.14. Are you sure ? (y - upgrade, other key - quit)
y
Starting Configurator Upgrade
Running the backup script
Stopping tomcat service
Synchronizing all files
Upgrading database
Upgrading java from 11.0.7 to 11.0.9.1
Importing certificates
Installing OS patches - it might take a while...
Restarting services
successfully upgraded Configurator
Starting Routers upgrade
Router: r1 (10.7.2.10)
 Starting Router Upgrade
 Stopping tomcat service
 Synchronizing all files
 Upgrading java from 11.0.7 to 11.0.9.1
 Installing OS patches - it might take a while...
 Restarting services
 successfully upgraded Router from 9.2.16 to 9.4.14
Waiting for Router status (up to 300 sec)
Router r1 is available
Waiting for nodes status (up to 300 sec)
All nodes were connected to r1
Router: r2 (10.7.2.22)
 Starting Router Upgrade
 Stopping tomcat service
 Synchronizing all files
 Upgrading java from 11.0.7 to 11.0.9.1
 Installing OS patches - it might take a while...
 Restarting services
 successfully upgraded Router from 9.2.16 to 9.4.14
Waiting for Router status (up to 300 sec)
Router r2 is available
Waiting for nodes status (up to 300 sec)
All nodes were connected to r2
All routers are available and have upgraded successfully
ARM has been successfully upgraded from 9.2.16 to 9.4.14
==========================================================
```

- Execute the following command:

```
exec bash
```

If you're upgrading from ARM 9.4+, an option is available to prepare the Routers by copying all files from the Configurator to the Routers. This action can be performed before the upgrade to reduce the duration of the upgrade.

➢ **To copy all upgrade files to the Routers, execute the following command:**

```
upgrade_arm < upgrade tar.gz filename> --sync
```

```
[root@configurator tmp]# upgrade_arm upgrade_9.4.14.tar.gz --sync
Running: VMFiles/Shared/usr/local/bin/upgrade.py upgrade_9.4.14.tar.gz --sync
============================
Starting ARM Upgrade
Sync option is on - copy all files to router without any upgrading
Validating configuration
Preparing Routers
Upgrade Configurator (only sync) - End
=====================================
```

Troubleshooting the Upgrade to ARM 9.4+

➢ **To troubleshoot:**

1. If the upgrade fails during a Router upgrade, press **Y** 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 steps 3-4.
2. If upgrade fails and there is no option to retry, or the failure is consistent, or you decided to revert to the previous version, follow steps 3-4.
3. Log into the ARM Configurator Virtual Machine via SSH and type the following commands:

```
su -
Password:password
logCollect
```

4. Copy the created tar.gz file to your computer and then revert to the pre-upgrade snapshot in the VMware vSphere client.
5. 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.

Upgrading to ARM 9.4+ with the New CentOS

The following steps apply to upgrades from ARM 8.8 or 9.0 to ARM 9.4+. ARM 9.2 is provided with the latest CentOS Operating System (CentOS 8).

Software upgrade to ARM 9.4+ incorporates upgrade to the new OS. ARM 9.4+ does not support the old version of CentOS (CentOS 6). Upgrading to ARM 9.4+ can be done only from ARM 8.8 or 9.0. To upgrade from earlier ARM versions (8.4 or 8.6), the operator must upgrade first to ARM 8.8 and then to 9.4+. The customer's first upgrade to ARM 9.4+ (including CentOS 6 > CentOS 8 upgrade) is more complex than previous software upgrades (which didn't upgrade the major OS version). However, future ARM software upgrades from ARM 9.4+ with CentOS 8 will be simple again. It should nevertheless be noted that upgrading to ARM 9.4+ (with CentOS 8) preserves the customer's configuration and is performed without impacting service. Upgrade of CentOS within the same Virtual Machine is impossible so for each ARM server (Configurator and Routers) the operator should prepare and install a new ARM version Virtual Machine (with CentOS 8). The IP addresses of the previous servers will be preserved. In this way, the new VM (server) is turned on during the upgrade only after the old Configurator or Routers are shut down. This means that for each ARM server during the upgrade there will temporarily be two VMs (one old and one new, loaded with ARM 9.4+). This requires an additional temporary IP address, additional temporary resources for VM (cores, memory, disk) and a new Feature Key (for migrating the Configurator with all its features).

The next table describes the upgrade process as it should be performed step by step. The table is relevant to VMware / HyperV / Public IPs of AWS and Azure. It does not include Private IPs of AWS and Azure.

Table 5-1: Upgrade process

		Centos 6			Centos 8		
Steps	Action	Configurator	Router 1	Router 2	New Configurator	New Router 1	New Router 2
Starting		Active	Active	Active	Doesn't exist	Doesn't exist	Doesn't exist
Preparing for the upgrade	Prepare Centos 8 Configurator	Active IP-1	Active IP-2	Active IP-3	Available IP-4 With New Feature Key UI works	Doesn't exist	Doesn't exist
	Centos 8 Configurator - stop Tomcat Service	Active IP-1	Active IP-2	Active IP-3	ssh/ping Available IP-4 UI not available	Doesn't exist	Doesn't exist
	Prepare Centos 8 Router 1	Active IP-1	Active IP-2	Active IP-3	ssh/ping Available IP-4 UI not available	ssh/ping Available IP-5	Doesn't exist
	Centos 8 Router 1 - stop Tomcat Service	Active IP-1	Active IP-2	Active IP-3	ssh/ping Available IP-4 UI not available	ssh/ping Available IP-5 Tomcat is Down	Doesn't exist
	Prepare Centos 8 Router 2	Active IP-1	Active IP-2	Active IP-3	ssh/ping Available IP-4 UI not available	ssh/ping Available IP-5 Tomcat is Down	ssh/ping Available IP-6
	Centos 8 Router 2 - stop Tomcat Service	Active IP-1	Active IP-2	Active IP-3	ssh/ping Available IP-4 UI not available	ssh/ping Available IP-5 Tomcat is Down	ssh/ping Available IP-6 Tomcat is Down
Backup	Operator	Active IP-1	Active IP-2	Active IP-3	ssh/ping	ssh/ping	ssh/ping

		Centos 6			Centos 8		
Centos 6 configuration	copy to Configurator on Centos 6 script and got 2 files of Centos 6 configuration				Available IP-4 UI not available	Available IP-5 Tomcat is Down	Available IP-6 Tomcat is Down
Performing Upgrade - Configurator of Centos 8	Copy 3 files to "New Configurator"	Active IP-1	Active IP-2	Active IP-3	ssh/ping Available IP-4 UI not available	ssh/ping Available IP-5 Tomcat is Down	ssh/ping Available IP-6 Tomcat is Down
	Power off Configurator of Centos 6	Not available IP-1	Active IP-2 Not Connected to Configurator of CentOS 6	Active IP-3 Not Connected to Configurator of CentOS 6	ssh/ping Available IP-4 UI not available	ssh/ping Available IP-5 Tomcat is Down	ssh/ping Available IP-6 Tomcat is Down
	Change "New Configurator" IP using Configurator Centos 6 IP	Not available IP-1	Active IP-2 Not Connected to Configurator of CentOS 6	Active IP-3 Not Connected to Configurator of CentOS 6	ssh/ping available IP-1 UI not available	ssh/ping Available IP-5 Tomcat is Down	ssh/ping Available IP-6 Tomcat is Down
	Performing Restore DB and Upgrade DB	Not available IP-1	Active IP-2 Not Connected to Configurator of CentOS 6 and not to Centos 8	Active IP-3 Not Connected to Configurator of CentOS 6 and not to Centos 8	ssh/ping available IP-1 UI available	ssh/ping Available IP-5 Tomcat is Down	ssh/ping Available IP-6 Tomcat is Down
Performing Upgrade - Router 1 of Centos 8	Power off Router 1 of Centos 6	Not available IP-1	Not available IP-2	Active IP-3 Not Connected to Configurator of CentOS 6 and not to	ssh/ping available IP-1 UI available	ssh/ping Available IP-5 Tomcat is Down	ssh/ping Available IP-6 Tomcat is Down

		Centos 6			Centos 8		
				Centos 8			
	Change Router 1 of Centos 8 IP using Router 1 of Centos 6 IP	Not available IP-1	Not available IP-2	Active IP-3 Not Connected to Configurator of CentOS 6 and not to Centos 8	ssh/ping available IP-1 UI available	ssh/ping available IP-2 Tomcat is Down	ssh/ping Available IP-6 Tomcat is Down
	Starting tomcat on Router 1 of Centos 8	Not available IP-1	Not available IP-2	Active IP-3 Not Connected to Configurator of CentOS 6 and not to Centos 8	ssh/ping available IP-1 UI available	ssh/ping available IP-2 Tomcat is UP Connected to Configurator of Centos 8	ssh/ping Available IP-6 Tomcat is Down
Performing Upgrade - Router 2 of Centos 8	Power off Router 2 of Centos 6	Not available IP-1	Not available IP-2	Not available IP-3	ssh/ping available IP-1 UI available	ssh/ping available IP-2 Tomcat is UP Connected to Configurator of Centos 8	ssh/ping Available IP-6 Tomcat is Down
	Change Router 2 of Centos 8 IP using Router 2 of Centos 6 IP	Not available IP-1	Not available IP-2	Not available IP-3	ssh/ping available IP-1 UI available	ssh/ping available IP-2 Tomcat is UP Connected to Configurator of Centos 8	ssh/ping available IP-3 Tomcat is Down
	Starting tomcat on Router 2 of Centos 8	Not available IP-1	Not available IP-2	Not available IP-3	ssh/ping available IP-1 UI available	ssh/ping available IP-2 Tomcat is UP Connected to	ssh/ping available IP-3 Tomcat is UP Connected to

		Centos 6			Centos 8		
						Configurator of Centos 8	Configurator of Centos 8

Preparing for this 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. To upgrade from version 8.8:
   - Obtain the **root** user password for all Virtual Machines.
5. To upgrade from version 9.0:
   - Obtain the **root** user password for the Configurator Virtual Machine.
   - Obtain the **armAdmin** user password for all Virtual Machines.
6. Obtain the OVA files (Configurator and Router) for the version you want to upgrade to.
7. Obtain the backupAndRestore.zip file for the version you want to upgrade to.
8. Choose a maintenance time with low call traffic.
9. Prepare temporary IP and VM resources required for each server upgrade.
10. Prepare extended storage for the ARM Configurator (ARM Configurator allocates 80 GB in ARM 9.4+, Router 40 GB – no change for the older versions).

➢ To prepare the Configurator:

1. Install ARM 9.4+ on a new Virtual Machine (see Installing the ARM on page 5)
2. Request from AudioCodes a Feature Key with all the ordered features and ordered number of sessions for the new VM in ARM 9.4+.
3. Submit the license via the ARM GUI (**Settings** > **Administration** > **License**).
4. Shut down the tomcat service with the command "systemctl stop tomcat"
5. If you have only one spare IP in your network or no resources (memory/cores/disk) in your host (VmWare/HyperV), shut down this VM.

➢ To prepare the Routers

1. Install ARM 9.4+ on a new Virtual Machine (see Installing the ARM on page 5).

2. Shut down the tomcat service with the command "systemctl stop tomcat".
3. If you have only one spare IP in your network or no resources (memory/cores/disk) in your host (VmWare/HyperV), shut down this VM.
4. Repeat steps 1-2 for each Router.

Backing up the CentOS 6 Configurator

➢ **To back up the CentOS 6 Configurator:**

1. Extract the backupAndRestore.zip file on your PC.
2. Copy backupCentos6.tar.gz to /tmp directory on Centos 6 Configurator. You'll need to SFTP using **root** user for ARM 8.8 and **armAdmin** user for ARM 9.0.
3. Log in to Centos 6 Configurator as **root**. For ARM 9.0, log in as **armAdmin** and switch **root** user using command "su –" and enter the **root** password.
4. Run the following commands:

```
cd /tmp
tar xf backupCentos6.tar.gz backupCentos6.py
python backupCentos6.py
```

   The output of the backup process will create two files:

   - A backup file - /home/backup/backup_*.tar.gz
   - A checksum file - /home/backup/backup_*.sfv

5. Copy both files to your PC.

Performing this Upgrade

You're now ready to perform the upgrade to ARM 9.4+.

When the upgrade is finished, make sure all old ARM servers (Configurator and Routers) are shut down to avoid duplicate IP addresses or services in the network.

Performing it on VMware

➢ **To perform the upgrade on VMware:**

1. If your new 9.4+ Configurator VM is down, bring the VM up and shut down the tomcat service with the command **systemctl stop tomcat**.
2. Copy the restoreFromCentos6to8.tar.gz file to the /tmp directory on the Centos 8 Configurator. You'll need to SFTP using the **armAdmin** user.
3. Copy the backup (backup_*.tar.gz) file to the /tmp directory on the Centos 8 Configurator (the backup from Centos 6).

4. Copy the checksum file (backup_*.sfv) to the /tmp directory on the Centos 8 Configurator (the backup from Centos 6).

5. Show the network configuration by running "ip route show" and making a note of the IP address, the subnet mask and the default gateway. For example:

   10.7.0.0/16 dev eth0 proto kernel scope link src 10.7.20.200

   169.254.0.0/16 dev eth0 scope link metric 1002

   default via 10.7.0.1 dev eth0

   Run "cat /etc/resolv.conf" and remember the DNSs servers and the search domain.

   For example:

   search corp.audiocodes.com

   nameserver 10.1.1.11

   nameserver 10.1.1.10

6. Power off the Centos 6 Configurator. Note: Routers of Centos 6 are running, and call traffic will not be affected.

7. Connect to the Centos 8 Configurator by console – not SSH but the console API of VMWare because the next step changes the VM IP and the SSH connection to it is lost. Note: AudioCodes will provide more information related to Azure / AWS / HyperV.

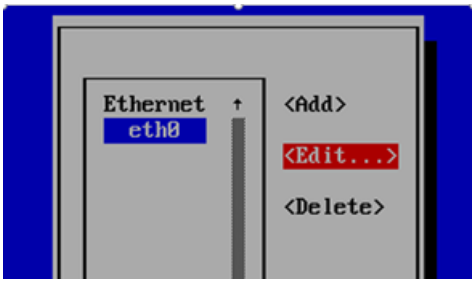
8. Change the IP address to the same IP Address of the Centos 6 Configurator using the command **nmtui**

9. Select **Edit a connection** shown in the next figure and press **Enter**.

Figure 5-5: NetworkManager TUI - Edit a connection

10. Select **Edit** and press **Enter**.

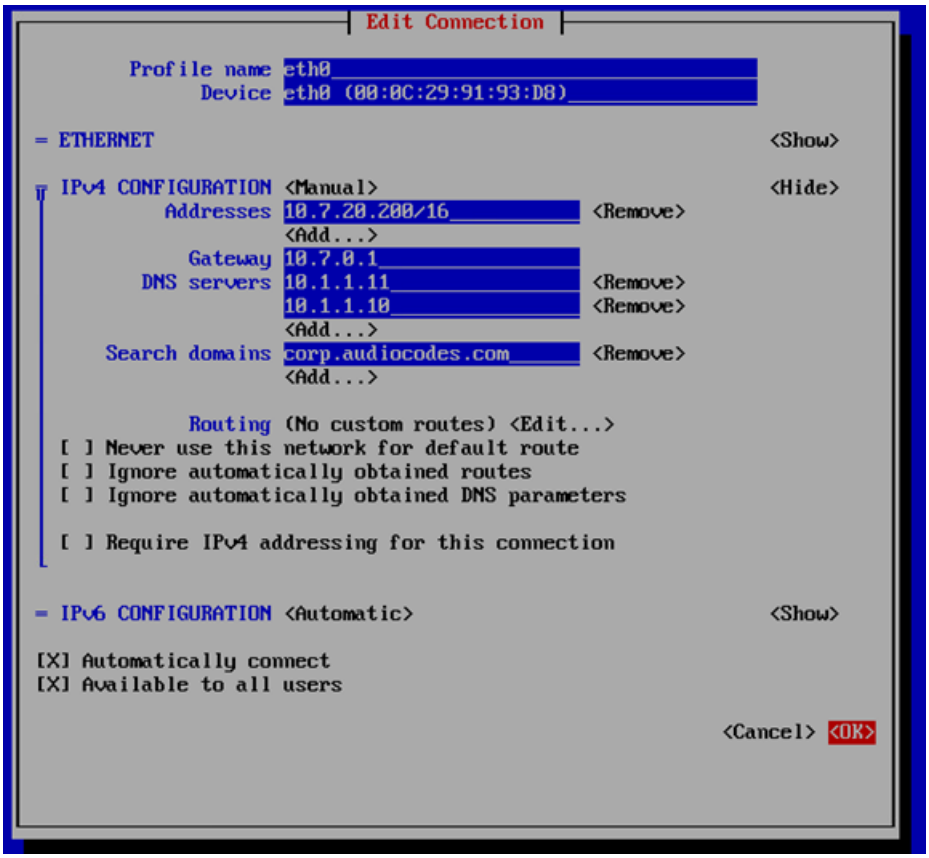
Figure 5-6: Eth0 - Edit



11. Change **IP4 CONFIGURATION** to **Manual**.
12. Press **Show**.
13. Add the IP address and the subnet mask.
14. Add the gateway.
15. Add the DNS servers.
16. Add the Search domains.
17. Press **OK**.

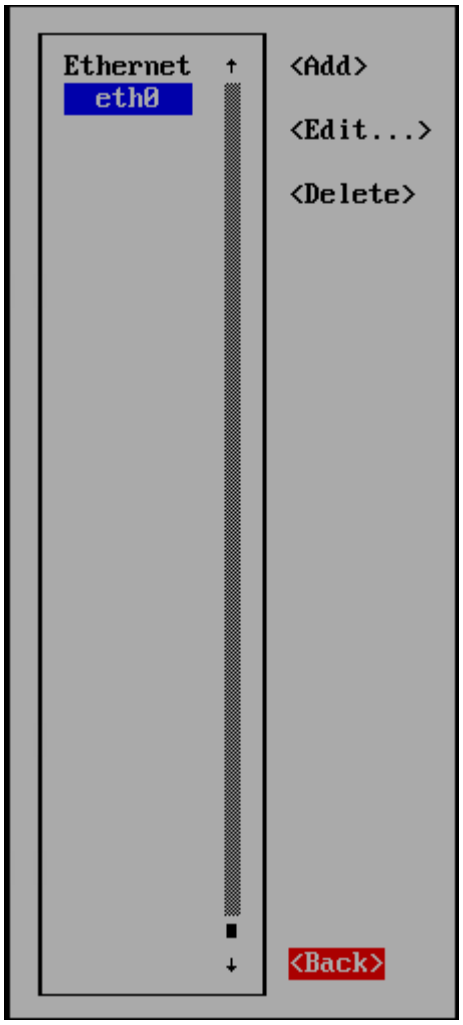
Warning: Profile name should be “eth0”. Don’t change it.

Figure 5-7: Edit Connection



18. Select **Back** in the next screen and press **Enter**.

Figure 5-8: Edit

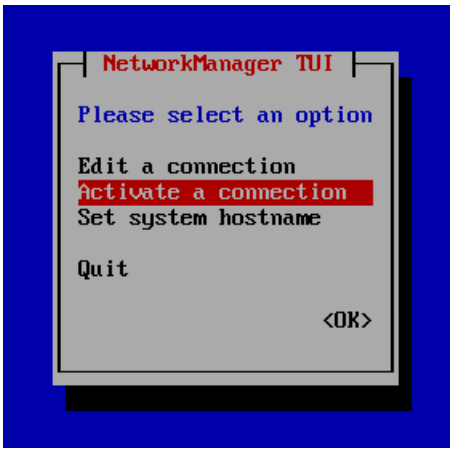


19. Select **Set system hostname** and then **OK**.

20. Enter the **hostname**.

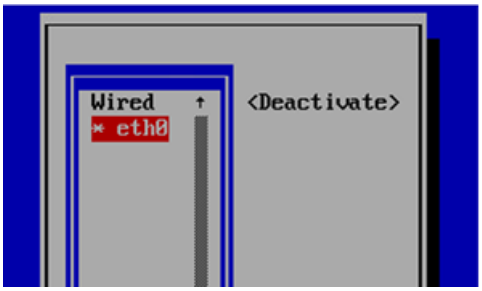
21. Select **Activate a connection** and then **OK**.

Figure 5-9: Activate a connection



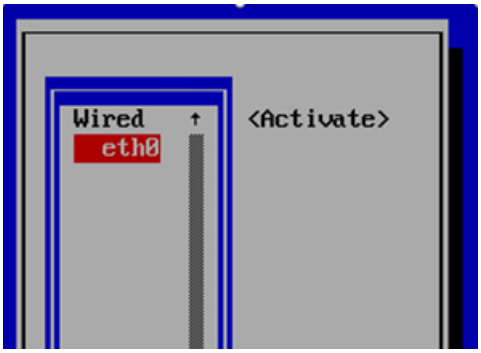
22. Select **Deactivate** and press **Enter**.

Figure 5-10: Eth0 Deactivate



23. Select **Activate** and press **Enter**.

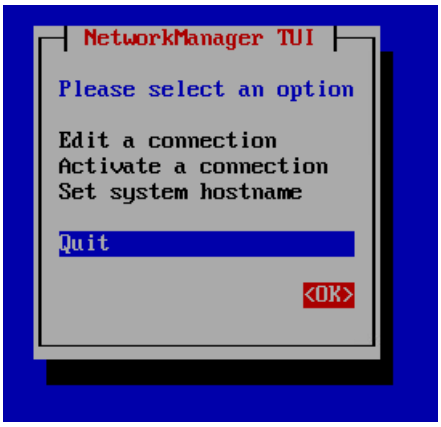
Figure 5-11: Eth0 Activate



24. Select **Back** and press **Enter**.

25. Select **OK** and press **Enter**.

Figure 5-12: Quit



26. Check that new Configurator is available with the IP by SSH.

27. On the Configurator version 9.4+, perform a restore of the DB from Centos 6 and upgrade it to 9.4+:

    Run the following commands:

    cd /tmp
    tar xf restoreFromCentos6to8.tar.gz restoreCentos8.py
    ./restoreCentos8.py *backup.tar.gz* (change the *backup.tar.gz* to your backup file name from step 3)

28. The Configurator is updated with your old Centos 6 configuration. Check in the GUI that the new Configurator is available.

29. For each Router:

    a. If your new ARM 9.4+ Router VM is down, bring the VM up and shut down the tomcat service with the command **systemctl stop tomcat**.

    b. Show the network configuration by running “ip route show” and make a note of the IP address, the subnet mask and the default gateway.

       For example: 10.7.0.0/16 dev eth0 proto kernel scope link src 10.7.20.201
       169.254.0.0/16 dev eth0 scope link metric 1002
       default via 10.7.0.1 dev eth0
       Run “cat /etc/resolv.conf” and remember the DNSs servers and the search domain.
       For example:
       search corp.audiocodes.com
       nameserver 10.1.1.11
       nameserver 10.1.1.10 3

    c. Power off the Centos 6 Router

    d. Connect to the Centos 8 Router by console - not SSH as you did for the Configurator.

e. Change the IP address to the same IP address of the Centos 6 Router by **nmtui** as you did for the Configurator.

f. Start the tomcat service using the command **systemctl start tomcat**

g. Check in the GUI that the Router has become available, and sync.

Performing it on Cloud AWS, Azure

There are two kinds of setups in the Cloud:

- using public IP addresses
- using private IP addresses

When upgrading from versions earlier than version 9.2 which use CentOS 6, to version 9.4+ which uses CentOS 8, there is no OS upgrade and operators should prepare new VMs for the procedure.

When using public IP addresses, the operator will move the public IP addresses between VMs while the private IP addresses cannot be moved due to a restriction of Cloud.

This documentation covers both setup *and* upgrade on the Cloud:

- Public
- Private

Performing it on AWS

- Public
- Private

Public IP Addresses

➢ **To perform the upgrade using public IP addresses:**

1. If your new Configurator 9.4+ instance is stopped, start the instance and shut down the tomcat service with the command **systemctl stop tomcat**.
2. Copy the restoreFromCentos6to8.tar.gz file to the /tmp directory on the Centos 8 Configurator. You'll need to SFTP using the **armAdmin** user.
3. Copy the backup.tar.gz file to the /tmp directory on the Centos 8 Configurator (the backup from Centos 6).
4. Copy the checksum file (.sfv) to the /tmp directory on the Centos 8 Configurator (the backup from Centos 6).
5. Stop the Centos 6 Configurator instance. Note: Routers of Centos 6 are running and call traffic will not be affected.
6. Associate the Elastic IP address of the Centos 6 Configurator instance with the new Configurator 9.4+ instance:

a. Open the Amazon EC2 console and choose **Elastic IPs**.

b. Select the Elastic IP address of the Centos 6 Configurator instance to associate and choose **Actions**, **Associate Elastic IP address**.

c. For 'Resource type', choose **Instance**.

d. For 'instance', choose the new Configurator 9.2 instance.

e. Choose **Associate**.

7. Check that new Configurator is available with the associated IP address by SSH.

8. On the Configurator 9.4+, perform a restore of the DB from Centos 6 and upgrade it to 9.4+: Run the following commands (change the backup.tar.gz to your backup file name):

```
cd /tmp
tar xf restoreFromCentos6to8.tar.gz restoreCentos8.py
./restoreCentos8.py backup.tar.gz
```

9. The Configurator is updated with your old Centos 6 configuration. Check in the ARM GUI that the new Configurator is available.

10. For each Router:

a. If your new ARM 9.4+ Router VM is down, start the instance, and shut down the tomcat service with the command "systemctl stop tomcat".

b. Stop the Centos 6 Router instance.

c. Associate the Elastic IP address of the Centos 6 Router instance with the new Router 9.2 instance as you did for the Configurator.

d. Start the tomcat service using the command **systemctl start tomcat**.

e. Check in the GUI that the Router has become available and sync.

Private IP Addresses

➢ **To perform the upgrade using private IP addresses:**

When upgrading to ARM 9.4+ on the AWS while using private IP addresses, operators must change the IP addresses of the ARM Configurator and ARM Routers because private IP addresses were given by the AWS and cannot be moved between instances.

To avoid moving to new IP addresses, you can configure the network by using public IP addresses (see Public IP / DNS (Host name)) and then perform the upgrade without changing ARM servers' IP addresses (see Public IP Addresses on the previous page), or perform the following:

1. If your new Configurator 9.4+ instance is stopped, start the instance and shut down the tomcat service with the command **systemctl stop tomcat**.

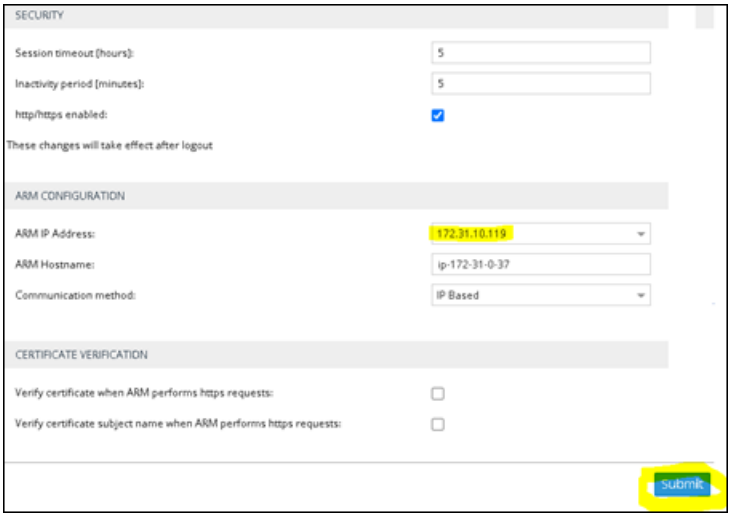
2. Copy the restoreFromCentos6to8.tar.gz file to the /tmp directory on the Centos 8 Configurator. You'll need to SFTP using the **armAdmin** user.
3. Copy the backup.tar.gz file to the /tmp directory on the Centos 8 Configurator (the backup from Centos 6).
4. Copy the checksum file (.sfv) to the /tmp directory on the Centos 8 Configurator (the backup from Centos 6).
5. Stop the Centos 6 Configurator instance. Note: Routers of Centos 6 are running and call traffic will not be affected.
6. On the Configurator 9.4+, perform a restore of the DB from Centos 6 and upgrade it to 9.4+:

   Run the following commands (change the backup.tar.gz to your backup file name):

```
cd /tmp
tar xf restoreFromCentos6to8.tar.gz restoreCentos8.py
./restoreCentos8.py backup.tar.gz
```

7. The Configurator is updated with your old Centos 6 configuration. Check in the ARM GUI that the new Configurator is available.
8. Open the Security page (**Settings** > **Administration** > **Security**).

Figure 5-13: Security



9. Under ARM Configuration, select from the 'Communication method' drop-down **IP Based** or **Hostname Based**.
   - If 'Communication method' is **IP based**, select the IP address from the 'ARM IP Address' drop-down.
   - If 'Communication method' is **Hostname based**, enter the DNS in the 'ARM Hostname' field.
10. Click the **Submit** button *even if you didn't change anything.*
11. Open the Network map (**Network** > **Map**).

12. Click the **Sync topology** button. Wait until nodes have become available (it can take a few minutes).

13. For each Router:

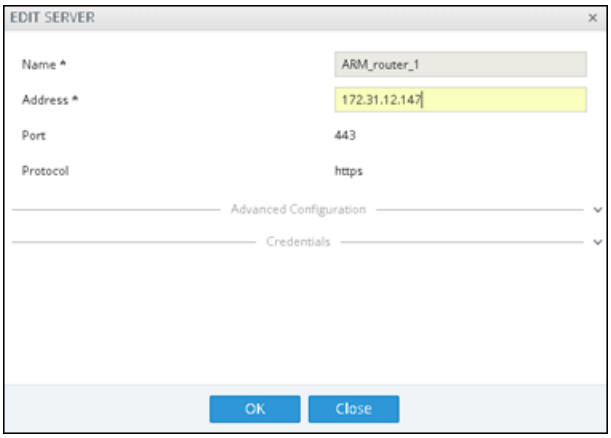
    a. If your new ARM 9.4+ Router VM is down, start the instance.

    b. Otherwise, start the tomcat service with the command **systemctl start tomcat**.

    c. Open the Routing Servers page (**Settings** > **Routing Servers** > **Servers**).

    d. Select the Centos 6 Router and press **Edit**.

Figure 5-14: Edit Server



    e. Replace the 'Address' with the new ARM 9.4+ Router Address and click **OK**.

    f. Click the **Refresh** button until the Router becomes available and sync.

    g. Stop the Centos 6 Router instance.

    h. Wait two minutes before upgrading the next router.

Performing it on Azure

➢ To perform the upgrade in Microsoft's Azure:

- Public
- Private

Private IP Addresses

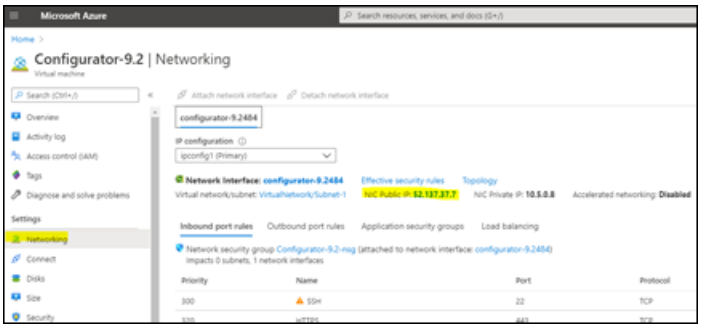
Using Public IP Addresses

Covered here is how to move public IP addresses between two VMs on Azure Cloud. You need to *dissociate* the public IP address from VM-**A** and *associate* it with VM-**B**. But firstly, you need to *dissociate* the public IP address from VM-**B** (Centos8). When that's done, VM-**B** (Centos8) won't have a public IP address.

➢ To move a Public IP Address between two VMs in Azure:

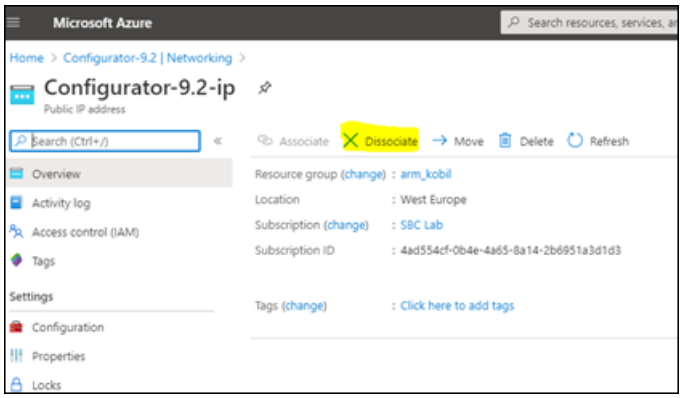
1. On the Centos8 VM > **Networking** > click **NIC Public IP**.

Figure 5-15: NIC Public IP



2. On the Centos8 VM > click **Dissociate**.

Figure 5-16: Dissociate

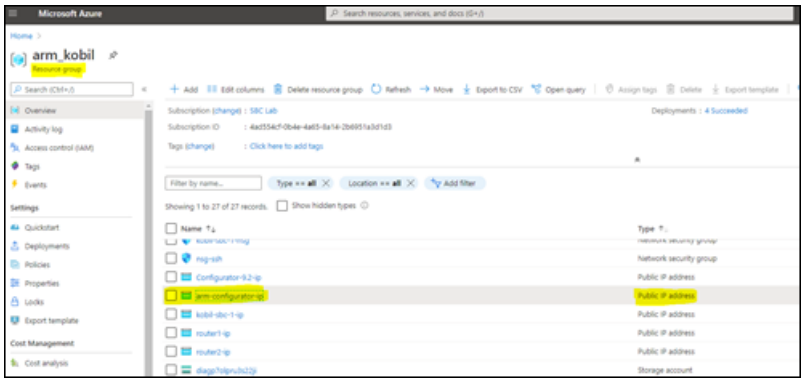


Secondly, dissociate the public IP address from VM-**A** (Centos6); it'll be moved to Centos8. The motivation is to preserve the original IP address. Perform the same two steps you performed for "Firstly, *dissociate* the public IP address from VM-**B**". When that's done, VM-**A** (Centos6) won't have a public IP address.

Thirdly, associate the IP address of VM-**A** (Centos6) with VM-**B** (Centos8). When that's done, VM-**B** (Centos8) will have the public IP address of VM-**A** (Centos6) and VM-**A** (Centos6) won't have any public IP address at all.

3. Go to the Resource group which contains your VM-**A** (Centos6) IP address and click it.

Figure 5-17: Resource group

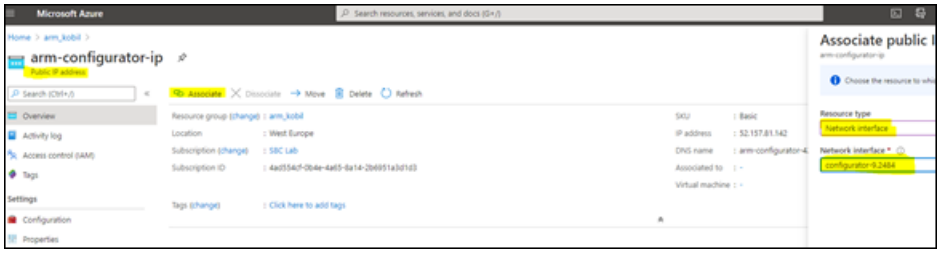


4. Perform the association. Two possible scenarios:

- **VM-A and VM-B are in the *same* resource group**

- Click **Associate** and choose Resource type **Network Interface** and then choose the Network Interface of VM-**B** (Centos8).

Figure 5-18: VM-A and VM-B are in the *same* resource group



- **VM-A and VM-B are *not in the same* resource group**

  i. Move the Public IP Address from the resource group of VM-**A** to the new resource group of VM-**B**

  ii. Click **Move** and choose **Move to another resource group**.

Figure 5-19: VM-A and VM-B are *not in the same* resource group

  iii. Choose the new resource group of VM-**B**.

Figure 5-20: Choose new resource group of VM-B

  iv. Click **Associate** and choose Resource type **Network Interface** and then choose the Network Interface of VM-**B** (Centos8).

Figure 5-21: Associate

The ARM by default creates a default Network Security Group (NSG) when installing via Market Place. If all new version 9.4+ installations are in a new resource group, you need to make sure the NSG is the same as the older version.

➢ To perform the upgrade using public IP addresses:

1. If your new Configurator 9.4+ VM is stopped, start the VM and shut down the tomcat service with the command **systemctl stop tomcat**.
2. Copy the restoreFromCentos6to8.tar.gz file to the /tmp directory on the Centos 8 Configurator. You'll need to SFTP using the **armAdmin** user.
3. Copy the backup.tar.gz file to the /tmp directory on the Centos 8 Configurator (the backup from Centos 6).
4. Copy the checksum file (.sfv) to the /tmp directory on the Centos 8 Configurator (the backup from Centos 6).
5. Stop the Centos 6 Configurator instance. Note: Routers of Centos 6 are running and call traffic will not be affected.
6. Dissociate the Public IP address of the Centos 6 Configurator and Centos 8 Configurator. Associate the Public IP address of the Centos 6 Configurator with the Centos 8 Configurator as described in the introductory paragraph above.
7. Check that new Centos 8 Configurator is available with the associated IP address by SSH.
8. On the Configurator 9.4+, perform a restore of the DB from Centos 6 and upgrade it to 9.4+: Run the following commands (change the backup.tar.gz to your backup file name):

```
cd /tmp
tar xf restoreFromCentos6to8.tar.gz restoreCentos8.py
./restoreCentos8.py backup.tar.gz
```

9. The Configurator is updated with your old Centos 6 configuration. Check in the ARM GUI that the new Configurator is available.
10. For each Router:
    a. If your new ARM 9.4+ Router VM is down, start the instance and shut down the tomcat service with the command **systemctl stop tomcat**.
    b. Stop the Centos 6 Router VM.

c. Associate the Public IP address of the Centos 6 Router with the new Router 9.4+ VM as you did for the Configurator.

d. Start the tomcat service using the command **systemctl start tomcat**.

e. Check in the GUI that the Router has become available, and sync.

f. Wait two minutes before upgrading the next router.

Using Private IP Addresses

Perform the same procedure that you performed for AWS.

Troubleshooting this Upgrade

If the upgrade process fails, the operator must shut down all the new servers and must turn on all the old servers.

If there were public IP addresses, the operator must move them back to the correct VM.

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 ‘armAdmin’.
2. Switch user to root user by "su -"
3. Execute the command:

```
backup_arm
```

The backup utility prompts:

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

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

The backup utility prompts:

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

5. 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 ‘armAdmin’.
2. Switch user to root user by "su -"
3. 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 Collecting Log Files

The ARM's reports feature collects log files which network administrators can use to analyze and troubleshoot issues that may occur. Log files can be collected on the Configurator or on the Router.

➢ **To create a report file:**

1. Log in to the VM (Topology Manager or Routing Manager) using ssh with user **armAdmin**.
2. Switch user to root user with "su -"
3. Execute the command:

```
logCollect
```

4. The report utility prompts:

```
Collect only log files that are less than specified number of days old ([y]/n):
```

5. Answer **yes** to include part of the log files or **no** to include all log files; the report utility prompts (if the previous answer was **yes**):

```
Number of days old to keep (5):
```

6. Specify the number of days old for the log; the report utility prompts:

```
Include heap dump? (y/[n]):
```

7. Answer **yes** to include the heap dump file; the report utility prompts:

```
Include atop logs? (y/n)
```

8. Answer **yes** to include atop logs; if the report utility is done on the Configurator, the prompt will be:

```
Collect logs from the routers? ([y]/[n]):
```

9. Answer **yes** to include log files from all Routers or **no** to include log files only from the Configurator; the collecting feature creates a report file and prompts:

```
>>> collecting arm DB ...
>>> Collect some summary data (please wait patiently)...
>>> Creating tar archive...
```

```
.....
>>> Compress tar file...
Completed building report file
```

Locate the file **ConfiguratorLogs_10.7.20.150_2001160747_9.0.12.tar.gz** in its current directory and send it to your technical support staff for analysis.

8 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.

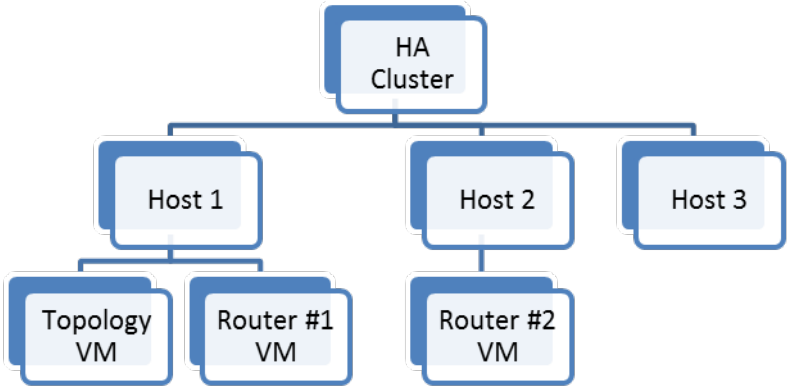
- For VM Monitoring to function, VMware tools must be installed. The provided ARM VM includes VMware tools software.
- vSphere HA supports both IPv4 and IPv6. A cluster that mixes the use of both of these protocol versions, however, is more likely to result in a network partition.

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 8-1: 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 armAdmin user, and type the following command:

```
sudo 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 commands:

```
su -
Password:password
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 commands in the LINUX shell:

```
su -
Password:password
cd /usr/local/bin
perl 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:

```
sudo service tomcat restart
```

8 Upgrading to ARM 9.0

ARM 9.2+ indicates ARM version 9.2 or later.

The following steps are for upgrades to ARM 9.0. If you're upgrading from ARM 8.8 or ARM 9.0 to ARM 9.2+, you can skip this documentation. 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. To upgrade from version 8.8 or earlier:
   - Obtain the **root** user password for all virtual machines.
5. To upgrade from version 9.0:
   - Obtain the **root** user password for the Configurator Virtual Machine.
   - Obtain the **armAdmin** user password for all Virtual Machines.
6. Obtain the upgrade tar.gz archive file for the version you want to upgrade to.
7. Copy the tar.gz files to the Configurator using SFTP (SSH File Transfer Protocol).
8. Choose a time with low call traffic.

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

9. Copy the file **cent90update-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.

10. Perform the following actions for the Configurator VM only (this step is necessary because as of ARM 8.4, the ARM Configurator requires four CPU cores while ARM 8.2 only required two, and as of ARM 8.6 the ARM Configurator requires 16 GB of RAM while ARM 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 7.8 or earlier. If you're upgrading from ARM 8.0 or later, you can skip it.

11. This step is necessary because as of ARM 8.0, the ARM Router requires a RAM memory allocation of 8 GB, while ARM 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.

When performing an upgrade in Microsoft's Azure Marketplace from ARM 8.6 / 8.8 to ARM 9.0 and later, you need to enable the ssh **root** user as follows:

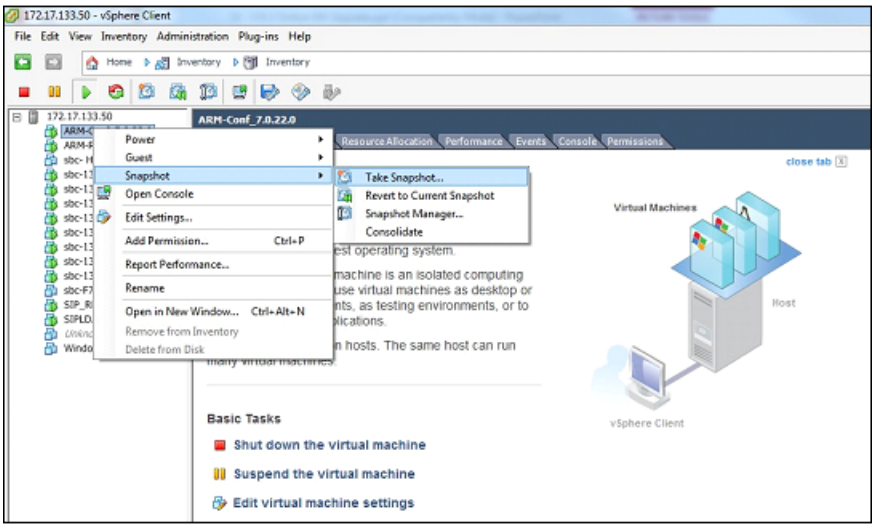
- Change to **root** user: Run the command "sudo -i".
- Edit the file "/etc/ssh/sshd_config". Change the line containing PermitRootLogin to "PermitRootLogin yes".
- Run the command "service sshd restart".

➢ To perform an upgrade:

1. Perform a Virtual Machine snapshot of the Configurator and all of the Routers:

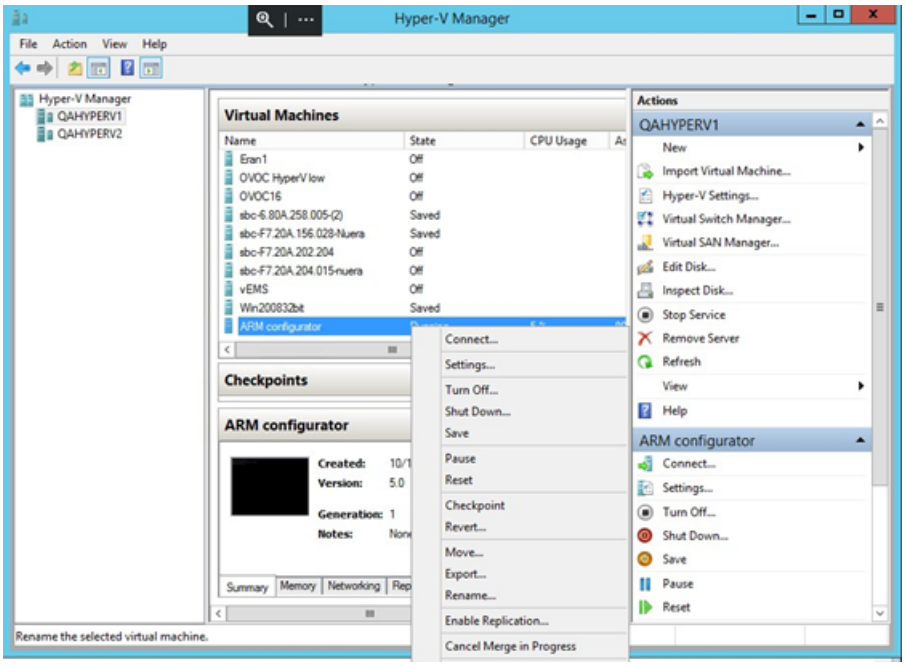
   a. If you're on VMWare: In the vSphere client, right-click the Virtual Machine and select **Snapshot** > **Take Snapshop**.

Figure 8-2: Take Snapshop



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

Figure 8-3: Hyper-V Manager: Select 'Checkpoint' from VM's Right-Click Menu



c. Log into the configurator using SSH.

d. Switch user to **root** by "su –"

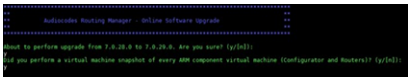
e. Enter the **root** password.

f. Execute the following command:

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

g. Answer **y** to the following questions:

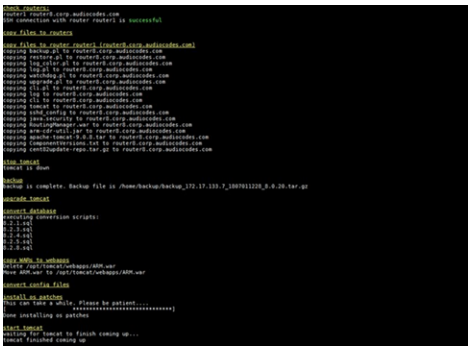
Figure 8-4: Answer 'y' to the Questions



h. On the first upgrade, you may be prompted to enter each of the Router's **root** or **armAdmin** user password (the Configurator **root/armAdmin** user fingerprint is stored in the Router so Router password entry is not needed on future upgrades).

i. Wait for the notification **ARM has been successfully upgraded to…**

Figure 8-5: ARM has been successfully upgraded to…

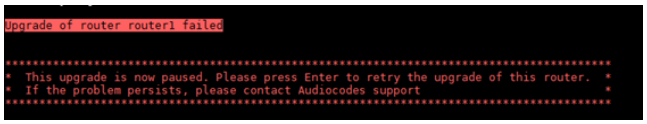


For the OS upgrade to take effect, the Configurator must be restarted at the end of the upgrade. Press **Enter** to reboot the Configurator.

Troubleshooting the Upgrade

If the upgrade fails:

1. You'll view the following message if the failure occurs during a router upgrade:



2. 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.

3. 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:

4. Log into the ARM Configurator Virtual Machine via SSH and type the following commands:

```
su -
Password:password
logCollec
```

5. Copy the created tar.gz file to your computer and then revert to the pre-upgrade snapshot in the VMware vSphere client.

6. 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.

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/

Documentation Feedback: https://online.audiocodes.com/documentation-feedback

Document #: LTRT-42163