

A10

Installing vThunder on Amazon Web Services (AWS)

September, 2023

© 2023 A10 Networks, Inc. All rights reserved.

Information in this document is subject to change without notice.

PATENT PROTECTION

A10 Networks, Inc. products are protected by patents in the U.S. and elsewhere. The following website is provided to satisfy the virtual patent marking provisions of various jurisdictions including the virtual patent marking provisions of the America Invents Act. A10 Networks, Inc. products, including all Thunder Series products, are protected by one or more of U.S. patents and patents pending listed at:

[a10-virtual-patent-marking](#).

TRADEMARKS

A10 Networks, Inc. trademarks are listed at: [a10-trademarks](#)

CONFIDENTIALITY

This document contains confidential materials proprietary to A10 Networks, Inc. This document and information and ideas herein may not be disclosed, copied, reproduced or distributed to anyone outside A10 Networks, Inc. without prior written consent of A10 Networks, Inc.

DISCLAIMER

This document does not create any express or implied warranty about A10 Networks, Inc. or about its products or services, including but not limited to fitness for a particular use and non-infringement. A10 Networks, Inc. has made reasonable efforts to verify that the information contained herein is accurate, but A10 Networks, Inc. assumes no responsibility for its use. All information is provided "as-is." The product specifications and features described in this publication are based on the latest information available; however, specifications are subject to change without notice, and certain features may not be available upon initial product release. Contact A10 Networks, Inc. for current information regarding its products or services. A10 Networks, Inc. products and services are subject to A10 Networks, Inc. standard terms and conditions.

ENVIRONMENTAL CONSIDERATIONS

Some electronic components may possibly contain dangerous substances. For information on specific component types, please contact the manufacturer of that component. Always consult local authorities for regulations regarding proper disposal of electronic components in your area.

FURTHER INFORMATION

For additional information about A10 products, terms and conditions of delivery, and pricing, contact your nearest A10 Networks, Inc. location, which can be found by visiting www.a10networks.com.

Table of Contents

Getting Started	6
Overview of AWS	7
Supported Instance Types	7
AWS Architecture and Terminology	10
Feature Support	11
Interfaces	11
Important Guidelines for AWS Data and Management Ports	11
Limitations	12
Launching vThunder on AWS	14
Creating an AWS Account	14
Creating and Configuring a VPC	15
Assigning a Subnet to the VPC	19
Creating a Security Group	22
Launching a vThunder Instance on AWS	26
Step 1. Choose AMI	27
Step 2. Choose Instance Type	30
Step 3. Configure the Instance	30
Step 4. Add Storage	33
Expanding Virtual Hard Disk Size	34
Step 5. Add Tags	35
Step 6. Configure Security Group	36
Step 7. Review the Configuration Changes	37
Manage Subscriptions	40
Post-Installation Tasks	47
Monitoring and Configuring the vThunder Instance	48
Accessing vThunder	49
Elastic IP Address	49
Associating an Elastic IP Address	49

Login to vThunder Instances	51
Login through CLI	51
Login through GUI	53
Configuring DHCP and the VIP in vThunder	55
Changing Source or Destination Checks	56
Disabling Change Source or Destination Checks	56
AWS High Availability	59
AWS Access Key ID and Secret Access Key	60
Importing AWS Access Key and Secret Access Key	60
AWS HA Architecture	61
Configuring HA	63
Sample ACOS Configuration for Active vThunder	64
Sample ACOS Configuration for Standby vThunder	65
Initial vThunder Configuration	67
About Licensing the vThunder Instance	68
Changing the Admin Password	68
Saving the Configuration Changes—Write Memory	68
Configuring vThunder on AWS as an SLB	69
Creating the vThunder Instance	69
Configuring the Interfaces	69
Configuring the vThunder ACOS	70
vThunder for AWS GovCloud	72
Overview	73
Features	73
Running vThunder in GovCloud	73
Step 1. Launch the vThunder AMI	74
Step 2. Apply for the vThunder BYOL license	74
Step 3. Configure the vThunder instance.	74

Advanced vThunder Configuration	75
About Shared Polling Mode	76
Enabling Shared Polling Mode	77
Disabling Shared Polling Mode	78
About Jumbo Frames	79
Enabling Jumbo Frames for vThunder	80
Dynamic Interface Attachment and Detachment	80
Platforms Supported	81
Known Issues or Limitations	81
Configuration	81
Attaching or Detaching Network Interface	81
Memory Support	82
Configuring vThunder on SLB or CGN	82
Configure Thunder Observability	86
Internal Thunder Observability Agent (iTOA)	86
External Thunder Observability Agent (TOA)	87

Getting Started

vThunder for AWS is a software version of the ACOS Series Application Delivery Controller (ADC), IPsec, Convergent Firewall (CFW), and an SSL Insight (SSLi) solution that runs on the Amazon Web Services (AWS) Cloud. vThunder is a virtual appliance, similar in functionality to the hardware-based ACOS appliances. vThunder is configurable by ACOS CLI, GUI, AXAPI, and Harmony Controller. For more information, see [Virtual Instances in Harmony Controller](#).

The following topics are covered:

Overview of AWS	7
Supported Instance Types	7
AWS Architecture and Terminology	10
Feature Support	11
Interfaces	11
Limitations	12

Overview of AWS

AWS is a cloud computing platform that enables businesses to move their network infrastructure to the cloud. Enterprises can set up virtual servers (or “instances”), and other computing resources, in the AWS cloud platform. You can set up vThunder as a virtual instance in the AWS cloud and configure it to provide a robust load balancing solution.

The maximum throughput of vThunder for AWS is variable and depends on the vThunder software license and an instance type used. For more information, see <http://docs.aws.amazon.com>.

Supported Instance Types

List of supported instance types are as follows:

Table 1 : List of Supported Instance Type

Instance Type	vCPU	Architecture	Memory (MiB)	Storage (GB)	Storage Type
With ixgbevf support					
c4.xlarge	4	x86_64	7680	-	-
c4.4xlarge	16	x86_64	30720	-	-
c4.8xlarge	36	x86_64	61440	-	-
d2.xlarge	4	x86_64	31232	6144	hdd
d2.2xlarge	8	x86_64	62464	12288	hdd
d2.4xlarge	16	x86_64	124928	24576	hdd
d2.8xlarge	36	x86_64	249856	49152	hdd
m4.xlarge	4	x86_64	16384	-	-
m4.2xlarge	8	x86_64	32768	-	-
m4.4xlarge	16	x86_64	65536	-	-
m4.10xlarge	40	x86_64	163840	-	-

Table 1 : List of Supported Instance Type

Instance Type	vCPU	Architecture	Memory (MiB)	Storage (GB)	Storage Type
i2.xlarge	4	x86_64	31232	800	ssd
i2.2xlarge	8	x86_64	62464	1600	ssd
i2.4xlarge	16	x86_64	124928	3200	ssd
i2.8xlarge	32	x86_64	249856	6400	ssd
With ENA support					
c5d.large	2	x86_64	4096	50	ssd
c5d.9xlarge	36	x86_64	73728	900	ssd
c5d.2xlarge	8	x86_64	32768	200	ssd
c5d.4xlarge	16	x86_64	73728	400	ssd
C5d.9xlarge	36	x86_64	73728	900	ssd
c5.xlarge	4	x86_64	8192	-	-
c5.2xlarge	8	x86_64	16384	-	-
c5.4xlarge	16	x86_64	32768	-	-
c5.9xlarge	36	x86_64	73728	-	-
g3.4xlarge	16	x86_64	124928	-	-
g3.8xlarge	32	x86_64	249856	-	-
i3.large	2	x86_64	15616	475	ssd
i3.xlarge	4	x86_64	31232	950	ssd
i3.2xlarge	8	x86_64	62464	1900	ssd
i3.4xlarge	16	x86_64	124928	3800	ssd
i3.8xlarge	32	x86_64	249856	7600	ssd
m5d.large	2	x86_64	8192	75	ssd
m5d.xlarge	4	x86_64	16384	150	ssd
m5d.2xlarge	8	x86_64	32768	300	ssd
m5d.4xlarge	16	x86_64	65536	600	ssd
m5.large	2	x86_64	8192	-	-

Table 1 : List of Supported Instance Type

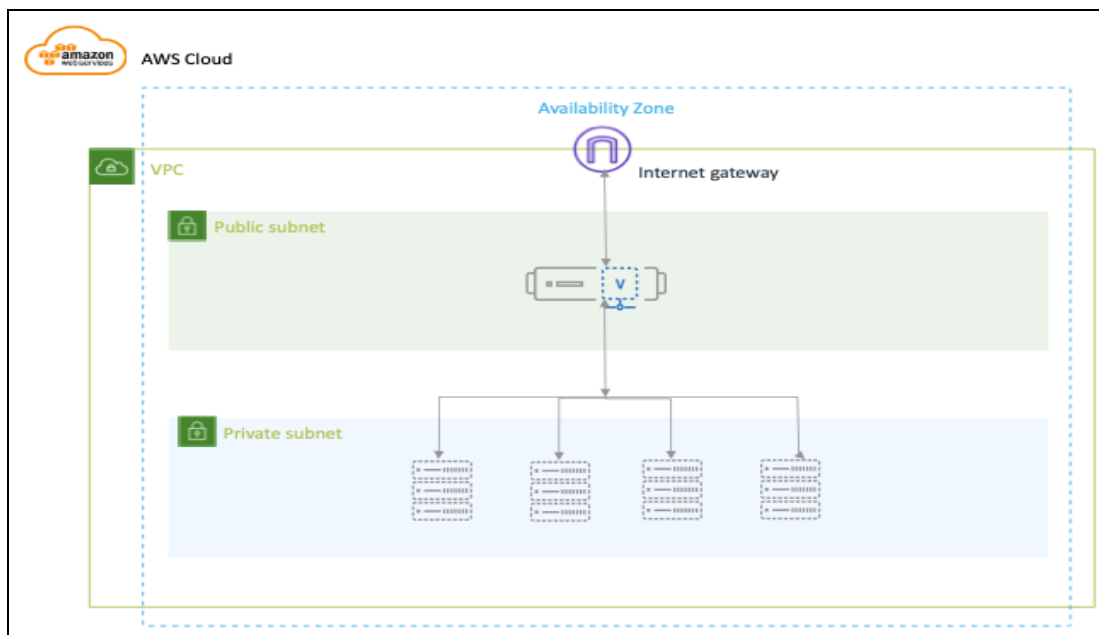
Instance Type	vCPU	Architecture	Memory (MiB)	Storage (GB)	Storage Type
m5.xlarge	4	x86_64	16384	-	-
m5.2xlarge	8	x86_64	32768	-	-
m5.4xlarge	16	x86_64	65536	-	-
r5d.large	2	x86_64	16384	75	ssd
r5d.xlarge	4	x86_64	32768	150	ssd
r5d.2xlarge	8	x86_64	65536	300	ssd
r5d.4xlarge	16	x86_64	131072	600	ssd
r5.large	2	x86_64	16384	-	-
r5.xlarge	4	x86_64	32768	-	-
r5.2xlarge	8	x86_64	65536	-	-
r5.4xlarge	16	x86_64	131072	-	-
r4.large	2	x86_64	15616	-	-
r4.xlarge	4	x86_64	31232	-	-
r4.2xlarge	8	x86_64	62464	-	-
r4.4xlarge	16	x86_64	124928	-	-
r4.8xlarge	32	x86_64	249856	-	-
t3.medium	2	x86_64	4096	-	-
t3.large	2	x86_64	8192	-	-
t3.xlarge	4	x86_64	16384	-	-
t3.2xlarge	8	x86_64	32768	-	-
z1d.large	2	x86_64	16384	75	ssd
z1d.xlarge	4	x86_64	32768	150	ssd
z1d.2xlarge	8	x86_64	65536	300	ssd
z1d.3xlarge	12	x86_64	98304	450	ssd
z1d.6xlarge	24	x86_64	196608	900	ssd

AWS Architecture and Terminology

The following are some common terms used in AWS deployments.

- **Amazon Elastic Compute Cloud (Amazon EC2)** — An Amazon technology that helps to launch virtual servers in the AWS cloud. Amazon EC2 is scalable to suit the requirements of the network.
- **Amazon Machine Image (AMI)** — An AMI contains a pre-defined configuration including the operating system, applications, and so on and is a type of image template for AWS. The vThunder instance created in AWS uses an AMI. In the AWS marketplace, vThunder is available as an AMI image.
- **Virtual Private Cloud (VPC)** — A virtual network is built on AWS and inherits its scalability. To access the vThunder instance by using SSH configure a VPC and specify a subnet. The subnets are used for grouping of the vThunder instances based on the requirements of the network.
- **Elastic IP address** — An IP address that is associated with your AWS account. These IP addresses are elastic as they can be attached and detach the IP address from the vThunder instances. Unlike traditional static IP addresses, Elastic IP addresses can get remapped to another instance at run time.

Figure 1 : vThunder for AWS



Feature Support

vThunder for AWS supports many of the same features as the Thunder Series hardware-based models, but the exact set of supported features varies based on whether vThunder is running as an ADC, CFW, or as an SSLi solution.

Refer to the [vThunder Software for Virtual and Cloud Infrastructure Data Sheet](#) for a complete summary of supported features.

Interfaces

A vThunder for AWS can be deployed with two or more interfaces. The following are the interfaces:

- **Ethernet 0**—Dedicated management interface
- **Ethernet (1-n)**—Data interface

Important Guidelines for AWS Data and Management Ports

The following is a list of important guidelines for data and management ports:

- For SLB configuration using a single data port, source NAT must be configured.
- If AWS is configured with two data interfaces with DHCP, the AWS instance has two default routes. Configure static IP addressing on the incoming data interface to maintain the traffic.
- The auto-assigning of public IP addresses feature is disabled if there are multiple interfaces in an AMI instance.
- For one management port and 3 data ports, the total number of CPUs required is either four or eight.
- For one management port and seven data ports, the total number of CPUs required is more than eight.

Limitations

The following is a list of limitations for running vThunder in AWS:

- vThunder for AWS requires that the management port be configured on a separate interface (eth0). Configure the management interface to access the ACOS GUI and CLI.
- After an IP is assigned to the vThunder management port, subsequent changes to this IP are not supported.
- LACP and Static trunk groups are not supported in vThunder.
- Port Mirror is not supported.
- RIP (v1 and v2), OSPF, and ISIS routing protocols are not supported.
- VLAN, Tagged VLAN, and Virtual Ethernet (VE) interfaces are not supported.
- Layer 2 Switching (VLAN) is not supported.
- Maximum interface (32) is not supported.
- Layer 2 deployment is not supported.
- Bridge Protocol Data Unit (BPDU) Forward Group is not supported.
- AWS cannot be configured as a CGN device or a TPS device.
- Interfaces cannot be set in promiscuous mode in AWS. For more information on *Installing vThunder on Amazon Web Services (AWS)*, see the “[system promiscuous mode](#)” command of CLI Guide.
- The maximum binding limitations are as follows:
 - For vTPS 3.2.x and 5.0.x, maximum vCPU is 48.
 - For ACOS 5.2.1-Px, maximum vCPU is 96.
- vThunder launched using 5.1.0 release AMI cannot be downgraded with releases before 5.1.0. The following error message is displayed:

```
# vThunder(config) (NOLICENSE)#upgarde hd pri local <ACOS Upgrade Image (.upg)>
Password []?
Do you want to reboot the system after the upgrade?[yes/no]:yes
```



```
Getting upgrade package ...
.....
Done (0 minutes 47 seconds)
Decrypt upgrade package ...
.....
Done (0 minutes 18 seconds)
Checking integrity of upgrade package ...
.. Upgrade file integrity checking passed (0 minutes 3 seconds)
Expand the upgrade package now ...
.....Failed to downgrade, due to unsupported previous version of image
found, pls contact support team for more information.
```

NOTE: To launch the AWS instance successfully, launch an instance using any older release build (lesser than 5.1.0 version) and then upgrade to the required build version.

Launching vThunder on AWS

This section provides the step-by-step procedures to launch vThunder on AWS.

NOTE: After buying software, customers launch Amazon Machine Images (AMIs) by using the [Manage Subscriptions](#) option in AWS Marketplace. Or launch it by setting up an account by using the AWS management tools, including the AWS Management Console, the Amazon EC2 console, Amazon EC2 APIs, or the AWS Cloud Formation console.

The following topics are covered:

Creating an AWS Account	14
Creating and Configuring a VPC	15
Assigning a Subnet to the VPC	19
Creating a Security Group	22
Launching a vThunder Instance on AWS	26
Manage Subscriptions	40

Creating an AWS Account

Before installing vThunder, the user first set up an account with AWS. Creating this account enrolls the user into standard AWS services, such as EC2 and VPC. The user creates an AWS account with Amazon by navigating to the following URL and following the on-screen instructions: <http://aws.amazon.com>.

NOTE: Details, including billing, availability of resources, and so on, is dependent on the selected region.

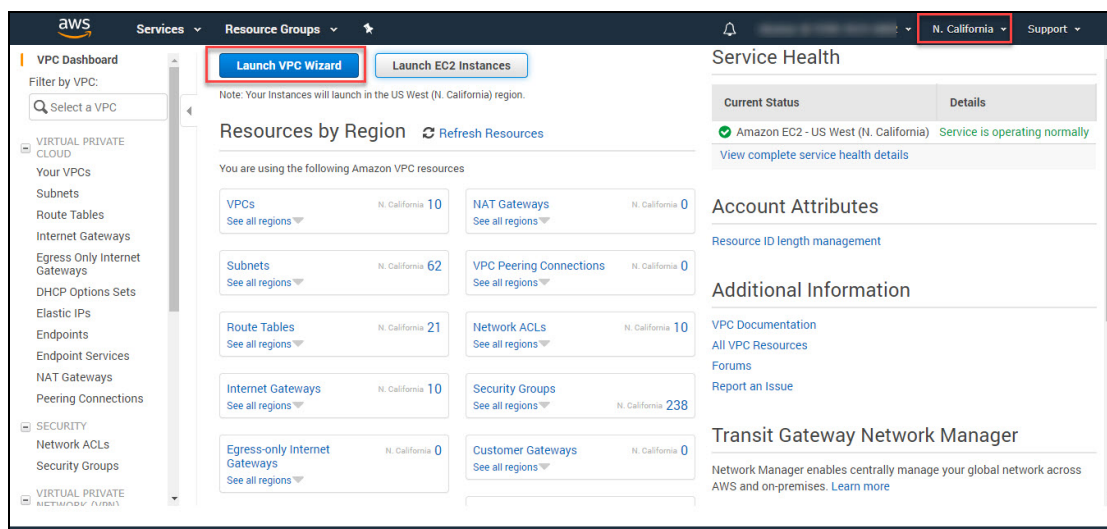
Creating and Configuring a VPC

Configure a VPC for the vThunder instance enables the user to use the Amazon VPC wizard to create a VPC, subnets, gateways, and routing tables. Alternatively, for manually creating a VPC and subnets users have to manually add gateways and routing tables.

To create an empty VPC using the Amazon VPC console and assign an IPv4 CIDR block (a range of private IPv4 addresses) perform the following:

1. Log in to AWS console at <https://console.aws.amazon.com/vpc>.
2. In the navigation pane, select the **VPC Dashboard** menu option. From the dashboard, click on the **Launch VPC Wizard** tab.

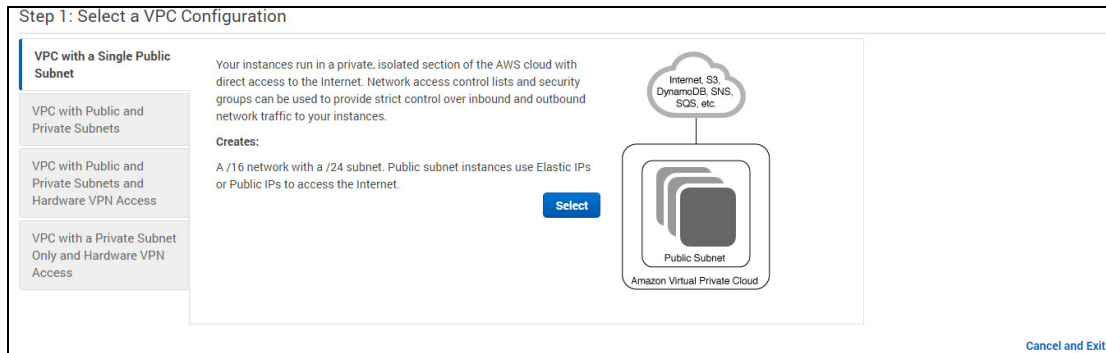
Figure 2 : VPC Dashboard window



NOTE: Do not select **Your VPCs** in the navigation pane; a user cannot access the VPC wizard using the Create VPC button on that page.

3. Select the option for the configuration to implement, for example, VPC with a Single Public Subnet, and then click on the **Select** button on the Select a VPC Configuration window.

Figure 3 : Step 1: Select a VPC Configuration window



4. On the configuration page, enter a name for the VPC in the **VPC name** field; for example, A10-Bangalore, and enter a name for the subnet in the **Subnet name** field. This helps you to identify the VPC and subnet in the Amazon VPC console after it is created.

Figure 4 : Step2: VPC with a Single Public Subnet window



5. (Optional) If you prefer, modify the configuration settings as follows:

Table 2 : Fields and description

Fields	Description
IPv4 CIDR block	Displays the IPv4 address range that is used for your VPC. Default value is 10.0.0.0/16).
Public subnet's IPv4	Displays the IPv4 address range that is used for the

Table 2 : Fields and description

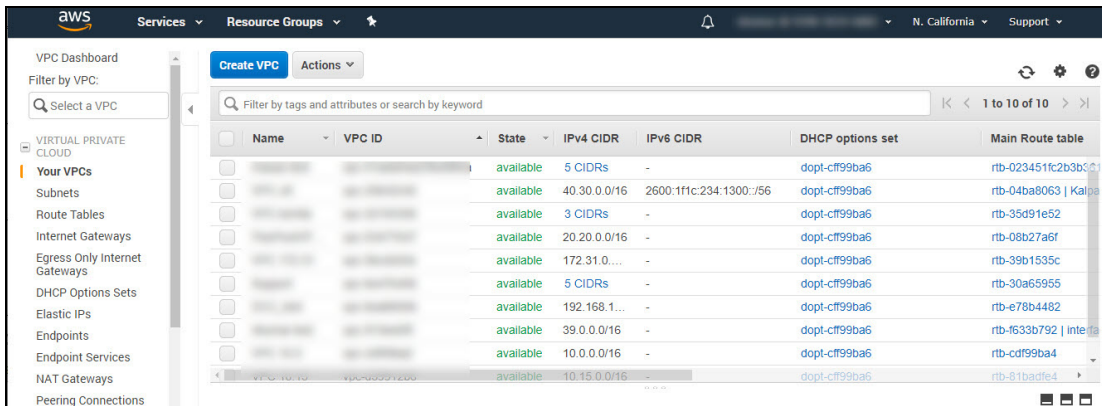
Fields	Description
CIDR	subnet. Default value is 10.0.0.0/24.
Availability Zone	Enables to select the Availability Zone in which to create the subnet. If it left as No Preference to, then AWS chooses an Availability Zone.
Service endpoints	Enables to select a subnet in which to create a VPC endpoint to Amazon S3 in the same region.
Enable DNS hostnames	Enables to set the DNS hostname. When set to Yes, it ensures that instances that are launched into your VPC receive a DNS hostname.
Hardware tenancy	Enables to select whether instances launched into your VPC are run on shared or dedicated hardware. NOTE: Selecting a dedicated tenancy incurs additional costs.
Enable ClassicLink	Displays the default VPC and the new VPC that is created. The VPC that is created is a non-default VPC, therefore the default VPC column displays No option.

6. Click on the **Create VPC** button.

To create a VPC using the console manually, perform the following steps:

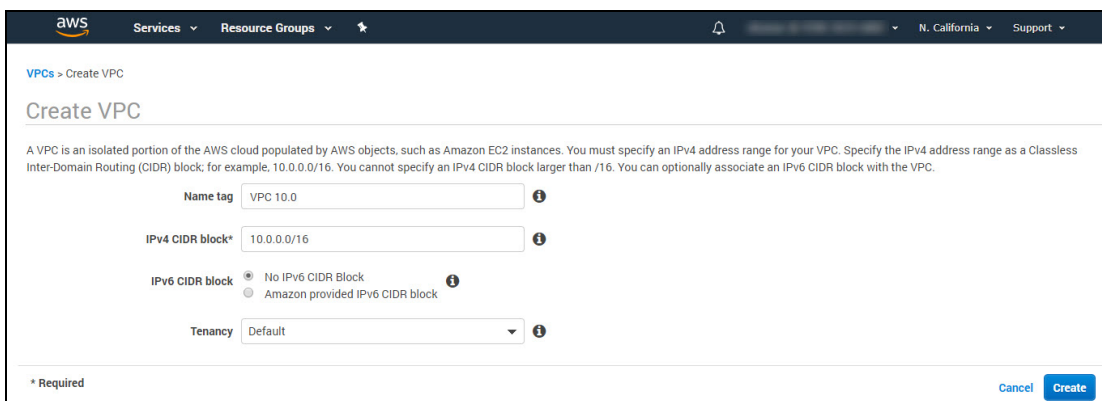
1. Launch the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. In the navigation pane, Select **Your VPCs**. Take note of the name and the ID of the VPC that you created (look in the Name and VPC ID columns). This information helps to identify the components that are associated with your VPC.

Figure 5 : Your VPCs window



3. Click on the **Create VPC** tab. The Create VPC window is displayed.

Figure 6 : Create VPC window



4. Specify the following VPC details as necessary as:

Table 3 : Fields and Descriptions

Fields	Description
Name tag	Optionally specify a name for the VPC. It creates a tag with a key of <code>Name</code> and the value
IPv4 CIDR block	Specify an IPv4 CIDR block for the VPC. It is recommended to specify a CIDR block from the private (non-publicly routable) IP address ranges. For example, 10.0.0.0/16 or 192.168.0.0/16.
IPv6 CIDR block	Optionally associate an IPv6 CIDR block with your VPC by

Table 3 : Fields and Descriptions

Fields	Description
	<p>choosing one of the following options:</p> <ul style="list-style-type: none"> • Amazon-provided IPv6 CIDR block: It requests an IPv6 CIDR block from Amazon's pool of IPv6 addresses. • IPv6 CIDR owned by me: The (BYOIP) Allocates an IPv6 CIDR block from your IPv6 address pool. For Pool, select the IPv6 address pool from which to allocate the IPv6 CIDR block.
Tenancy	Select a tenancy option. Dedicated tenancy ensures that your instances run on single-tenant hardware.

5. Click **Create** button to save the changes.

To add a CIDR Block to your VPC, perform the following steps:

1. In the navigation pane, choose Your VPCs.
2. Select the VPC, and select **Actions > Edit CIDRs** option.
3. Select **Add IPv4 CIDR**, and enter the CIDR block to add; for example, 10.2.0.0/16. select the tick icon.
4. Click the **Close** tab.

Assigning a Subnet to the VPC

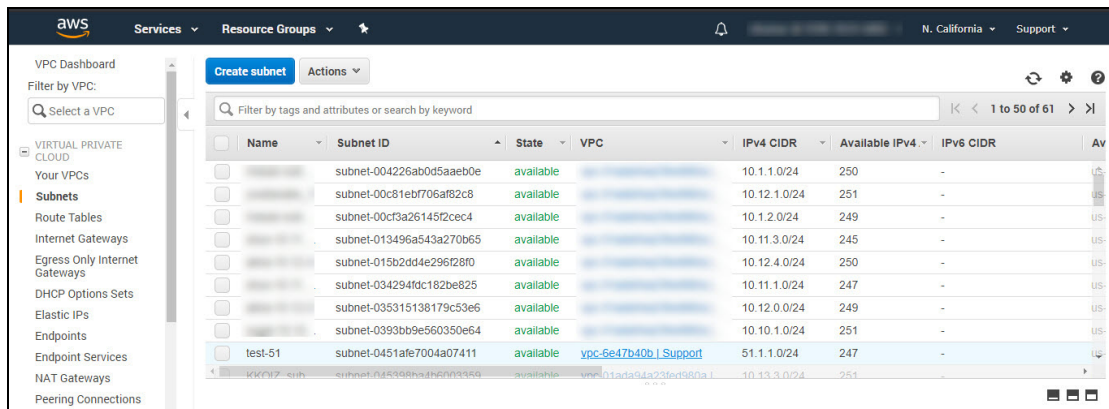
To add a new subnet to the VPC, specify an IPv4 CIDR block for the subnet from the range of the VPC. It is recommended to specify the Availability Zone in which a user wants the subnet to reside. Users can have multiple subnets in the same Availability Zone.

Optionally specify an IPv6 CIDR block for your subnet if an IPv6 CIDR block is associated with the VPC.

To add a subnet to your VPC using the console, perform the following:

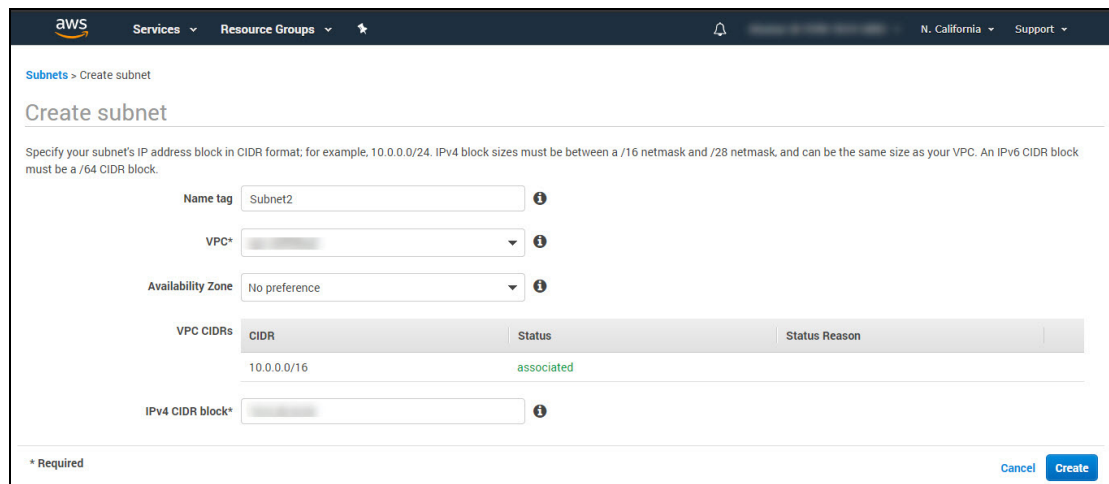
1. Navigate to **VPC Dashboard > Virtual Private Cloud > Subnet** menu option.

Figure 7 : Subnets window



2. Click **Create subnet** tab. The Create subnet window is displayed.

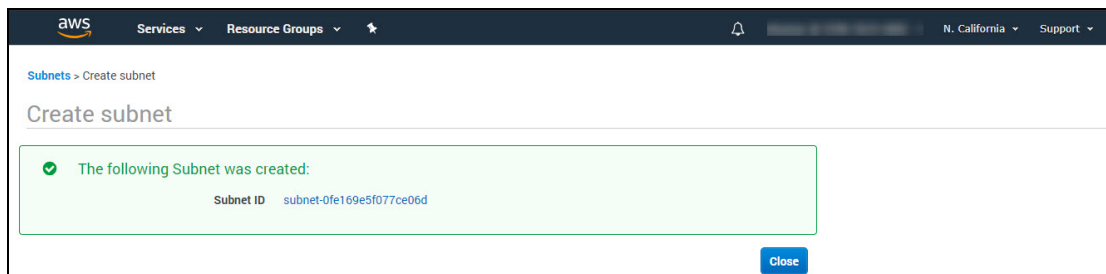
Figure 8 : Create subnet window



3. On the configuration page, enter a **Name tag** for the subnet, choose your **VPC** and **Availability Zone**, and **IPv4 CIDR block** details.
 - The **IPv4 CIDR block** displays the IPv4 address range that is used for the VPC (10.0.0.0/16), and the Public subnet's IPv4 CIDR field displays the IPv4 address range that is used for the subnet (10.0.0.0/24).

- The **Availability Zone** list enables users to select the Availability Zone in which to create the subnet.
 - (Optional) If an IPv6 CIDR block is associated with your VPC, then select **Specify a custom IPv6 CIDR**. It is recommended to specify the hexadecimal pair value for the subnet or leave the default value.
4. Click **Create** button to save. The confirmation message window with Subnet ID is displayed.

Figure 9 : Create subnet- Confirmation message window



NOTE: A public subnet is a subnet that has access to the Internet through an Internet gateway.

The subnets enable group vThunder instances based on the requirements of the network. This configuration of a VPC for vThunder instance is also accessed by using SSH.

NOTE: A single subnet is sufficient to launch a vThunder instance. (Optional) If required, repeat the steps above to create more subnets in your VPC.

To associate an IPv6 CIDR block with a subnet using the console:

The subnet must not have an existing IPv6 CIDR block associated with it.

1. In the navigation pane, choose **Subnets**.
2. Select your **Subnet**, and select **Actions > Edit IPv6 CIDRs**.
3. Select **Add IPv6 CIDR**. Specify the hexadecimal pair for the subnet (for example, 00) and confirm the entry by selecting the tick icon.
4. Click on the **Close** tab to save.

Creating a Security Group

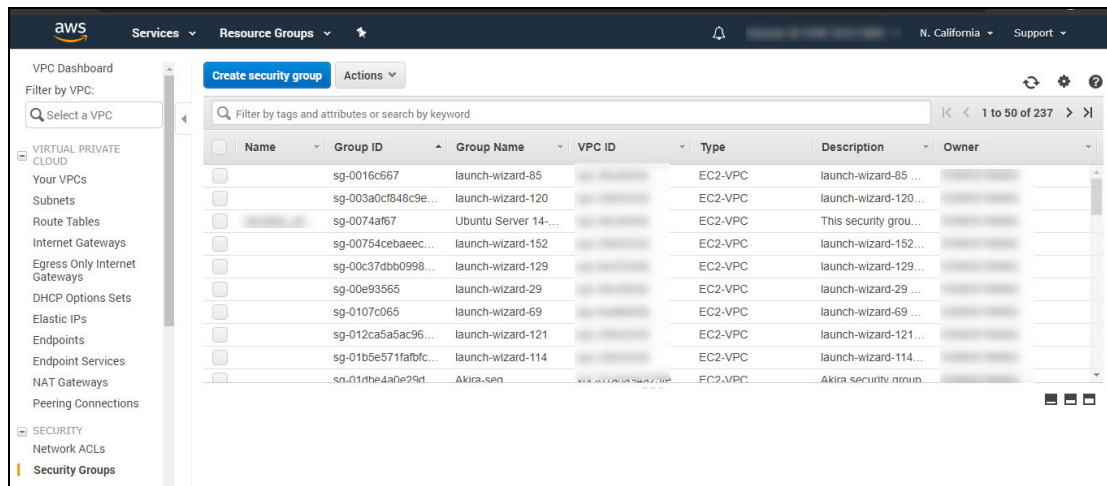
The VPC is also configured with a default security group, which acts as a firewall for all instances associated with the security group. To use a security group, the inbound rules are added to control incoming traffic to the instance, and outbound rules to control the outgoing traffic from the user's instance. To associate a security group with an instance, it recommended specifying the security group when the instance is launched.

NOTE: The VPC comes with a default security group. Any instance, not associated with another security group during the launch is associated with the default security group. specify this security group when you launch an instance into your VPC.

To create a new security group and associate with the vThunder image, perform the following:

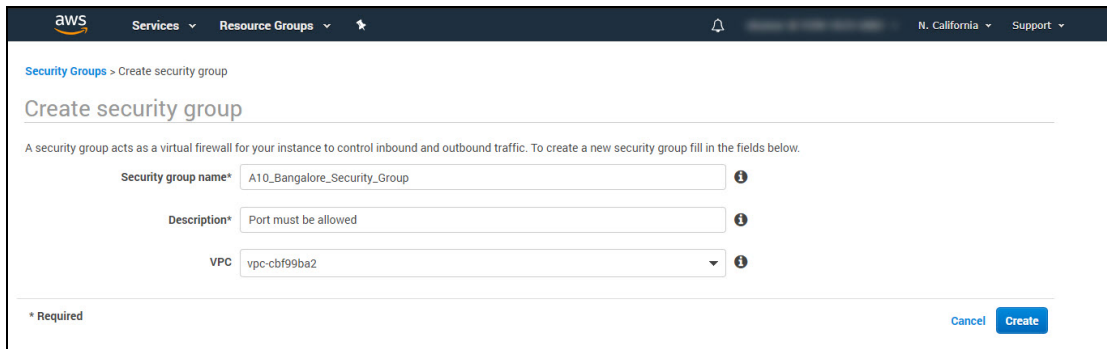
1. Navigate to **VPC Dashboard > Security > Security Groups** menu option.

Figure 10 : Security Groups window



2. Click on the **Create security group** tab. The Create security group window is displayed.

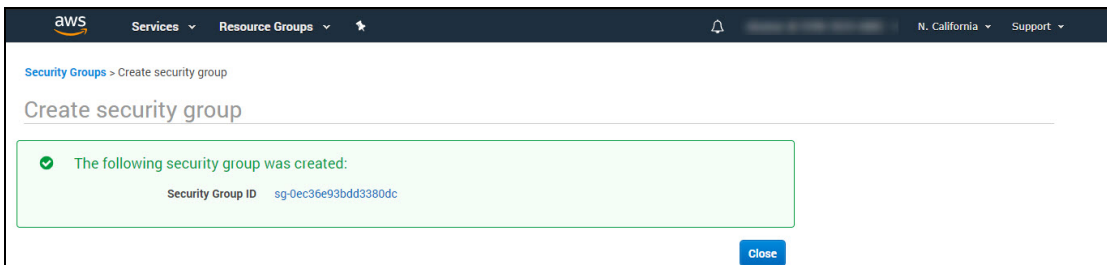
Figure 11 : Create security group window



The screenshot shows the AWS console interface for creating a security group. The breadcrumb navigation is 'Security Groups > Create security group'. The main heading is 'Create security group'. Below this, a note states: 'A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group fill in the fields below.' The form contains three required fields: 'Security group name*' with the value 'A10_Bangalore_Security_Group', 'Description*' with the value 'Port must be allowed', and 'VPC' with a dropdown menu showing 'vpc-cbf99ba2'. At the bottom right, there are 'Cancel' and 'Create' buttons. A legend at the bottom left indicates '* Required'.

3. In the Security group name field, enter the name of the security group, and provide a description.
4. Select the ID of the above created VPC from the VPC drop-down list.
5. Click **Create** button to save the changes. The confirmation message window with Security Group ID is displayed.

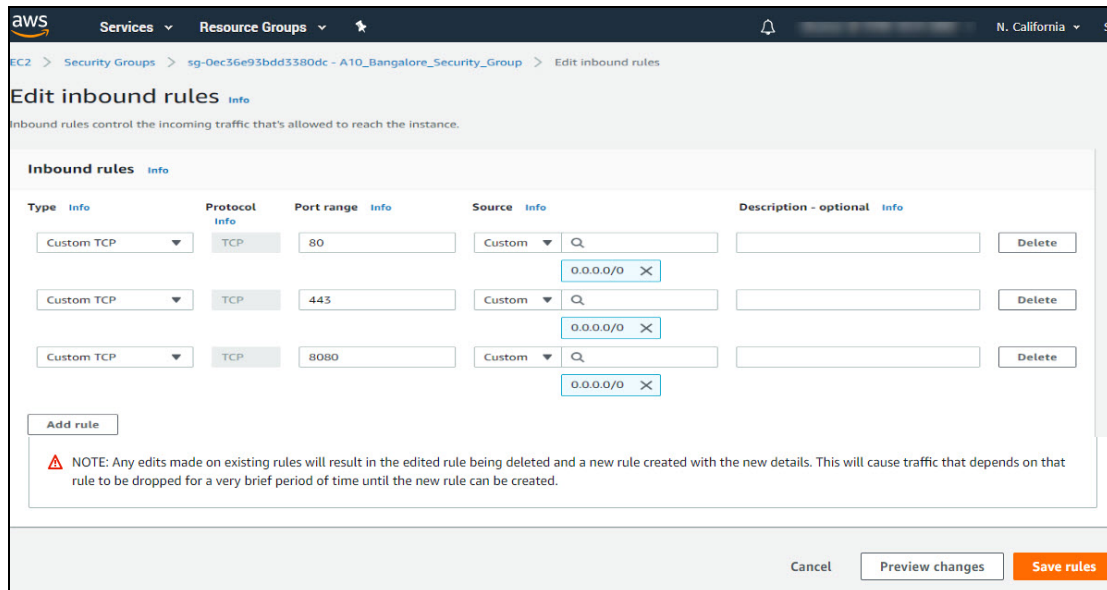
Figure 12 : Confirmation message window



The screenshot shows the confirmation message window in the AWS console. The breadcrumb navigation is 'Security Groups > Create security group'. The main heading is 'Create security group'. A green message box contains a checkmark icon and the text: 'The following security group was created: Security Group ID sg-0ec36e93bdd3380dc'. A 'Close' button is located at the bottom right of the message box.

6. Filter the security group ID, and navigate to **Actions > Edit Inbound rules** option. The Edit inbound rules info window is displayed.

Figure 13 : Edit Inbound rules window



Edit inbound rules

Inbound rules control the incoming traffic that's allowed to reach the instance.

Type	Protocol	Port range	Source	Description - optional
Custom TCP	TCP	80	0.0.0.0/0	
Custom TCP	TCP	443	0.0.0.0/0	
Custom TCP	TCP	8080	0.0.0.0/0	

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

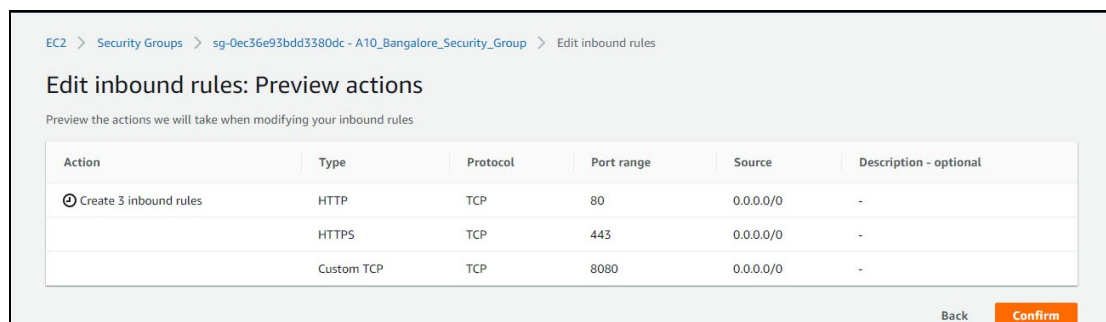
Buttons: Cancel, Preview changes, Save rules

7. Select and enter the **Type**, **Protocol**, **Port Range**, **Source**, and **Description** for the inbound rule.
8. Click the **Add Rule** button to add more or new Inbound rules for the Security Group ID.

NOTE: Add a rule that allows SSH access from any IPv6 address. Specify all IP addresses or range of addresses that users want to access for the instance.

9. Click **Save rules** or **Preview Changes** button to preview the edited inbound rules.

Figure 14 : Preview actions window



Edit inbound rules: Preview actions

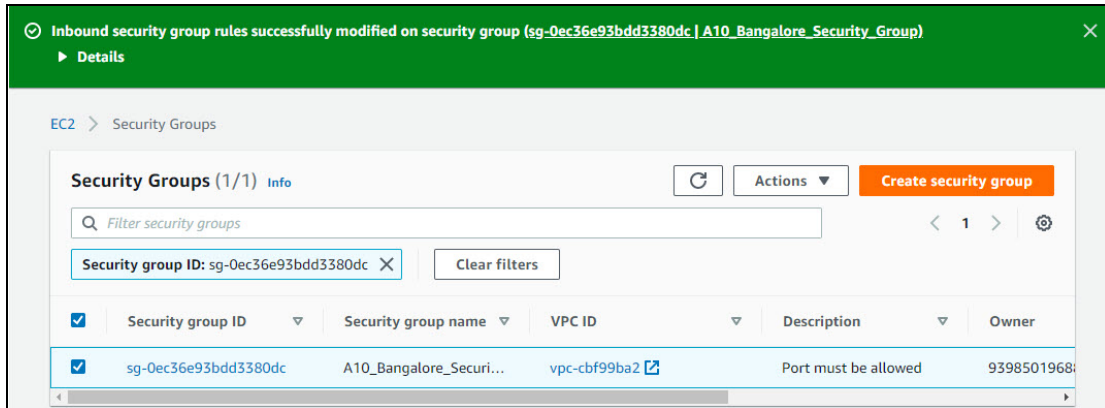
Preview the actions we will take when modifying your inbound rules

Action	Type	Protocol	Port range	Source	Description - optional
⊕ Create 3 inbound rules	HTTP	TCP	80	0.0.0.0/0	-
	HTTPS	TCP	443	0.0.0.0/0	-
	Custom TCP	TCP	8080	0.0.0.0/0	-

Buttons: Back, Confirm

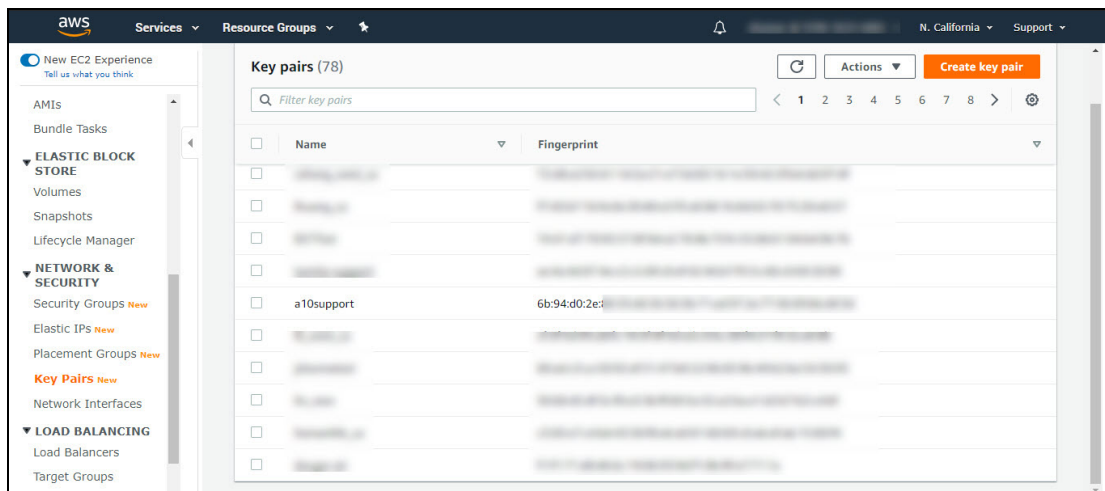
- Click the **Confirm** button to save and confirm the changes. The confirmation message is displayed.

Figure 15 : Confirmation Message window



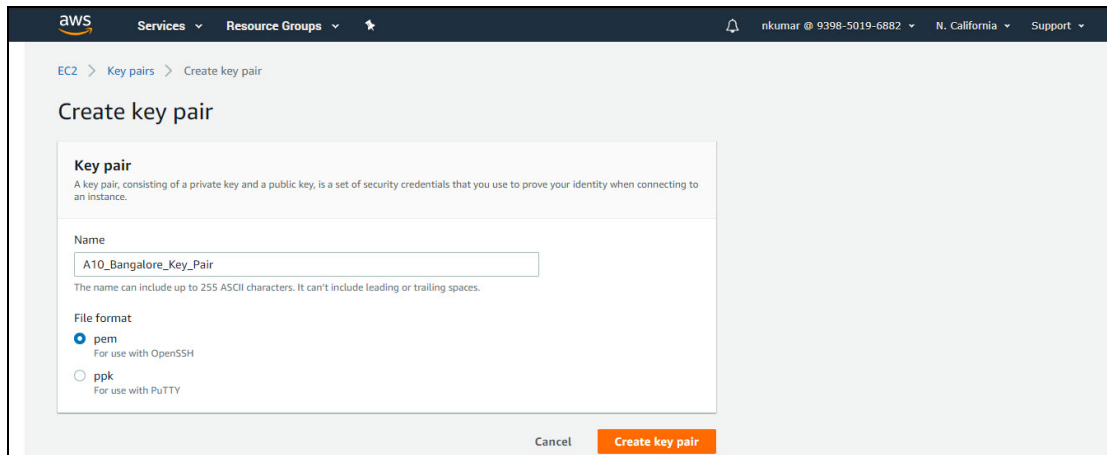
- Navigate to **Services > Compute > EC2 Dashboard > Network & Security > Key Pairs** menu option.

Figure 16 : Key pairs window



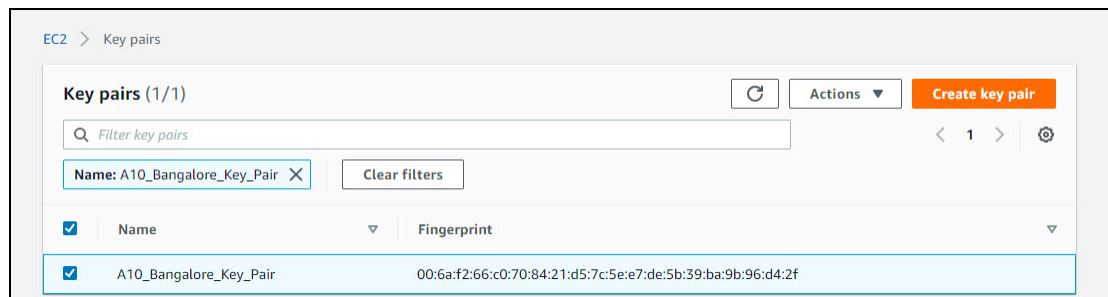
- Click **Create key pair** tab. The Create key pair window is displayed.

Figure 17 : Create key pair window



13. Enter the **Name** of the Key pair.
14. Select the **File format** radio button.
15. Click **Create key pair** button to save the changes. The Key pairs window is displayed with generated <Name>.pem file, save the file.

Figure 18 : Key pairs-<Name>.pem file window



Name	Fingerprint
A10_Bangalore_Key_Pair	00:6af2:66:c0:70:84:21:d5:7c:5e:e7:de:5b:39:ba:9b:96:d4:2f

If a user already has a VPC, and intend to start the vThunder AMI in that VPC, refer to the next sections.

Launching a vThunder Instance on AWS

The launching of a vThunder Instance on AWS workflow consists of the following steps:

The following topics are covered:

Step 1. Choose AMI	27
Step 2. Choose Instance Type	30
Step 3. Configure the Instance	30
Step 4. Add Storage	33
Expanding Virtual Hard Disk Size	34
Step 5. Add Tags	35
Step 6. Configure Security Group	36
Step 7. Review the Configuration Changes	37

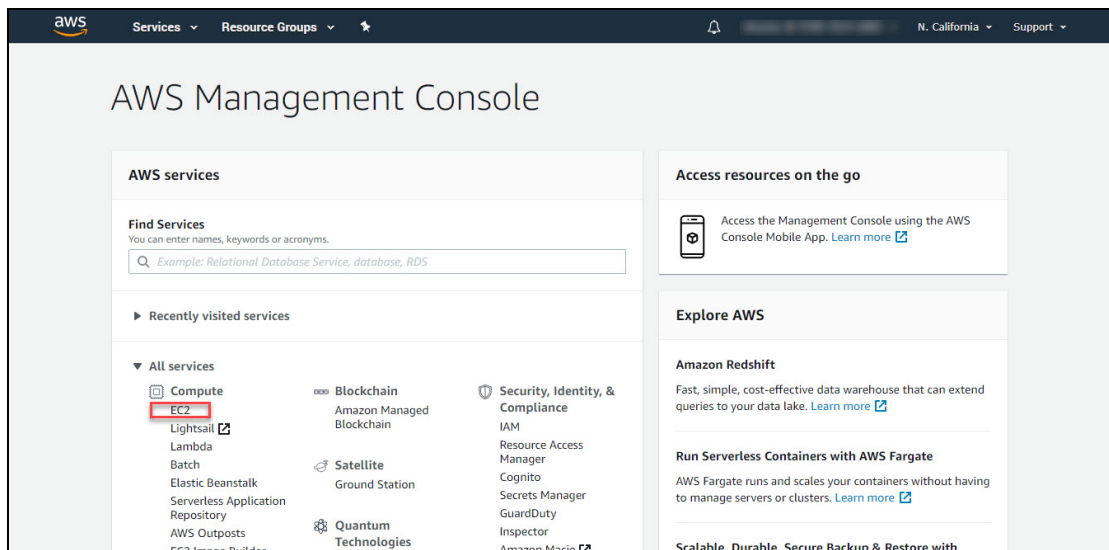
NOTE: If you prefer a 1-click AWS deployment, see [Manage Subscriptions](#) section.

Step 1. Choose AMI

To create a vThunder AMI instance, perform the following:

1. Access AWS and log in using your standard credentials.
The AWS Management Console - AWS services window is displayed.

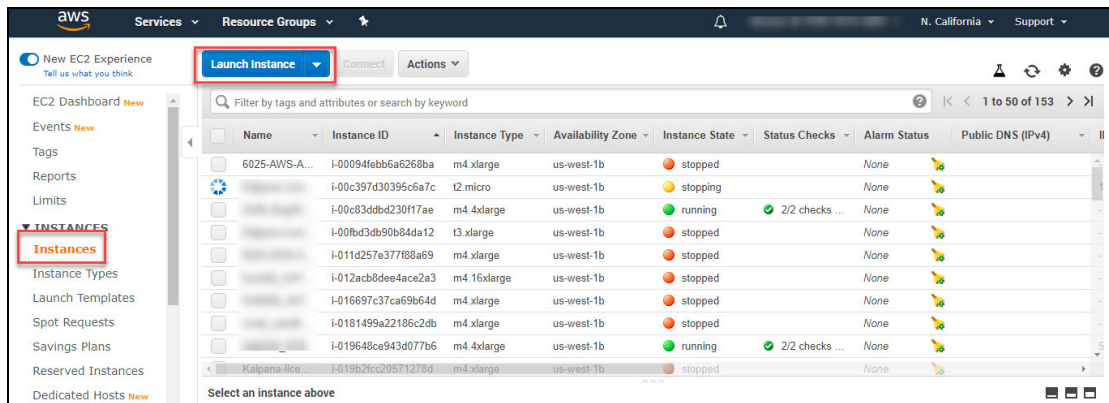
Figure 19 : AWS Management Console window



2. Select the **EC2** menu option (under Compute) as shown in [Figure 19](#).

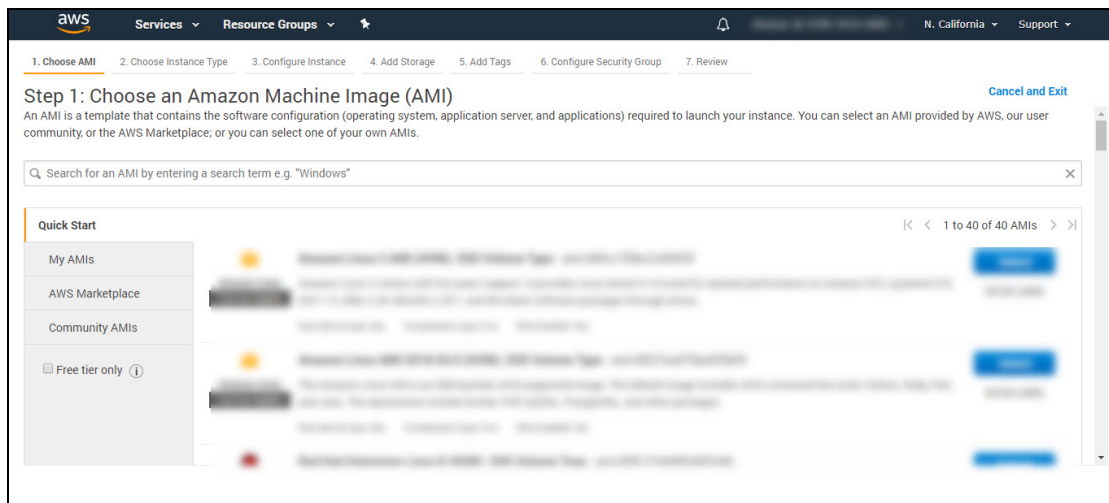
The EC2 dashboard window is displayed, with a list of your resources.

Figure 20 : EC2 Dashboard



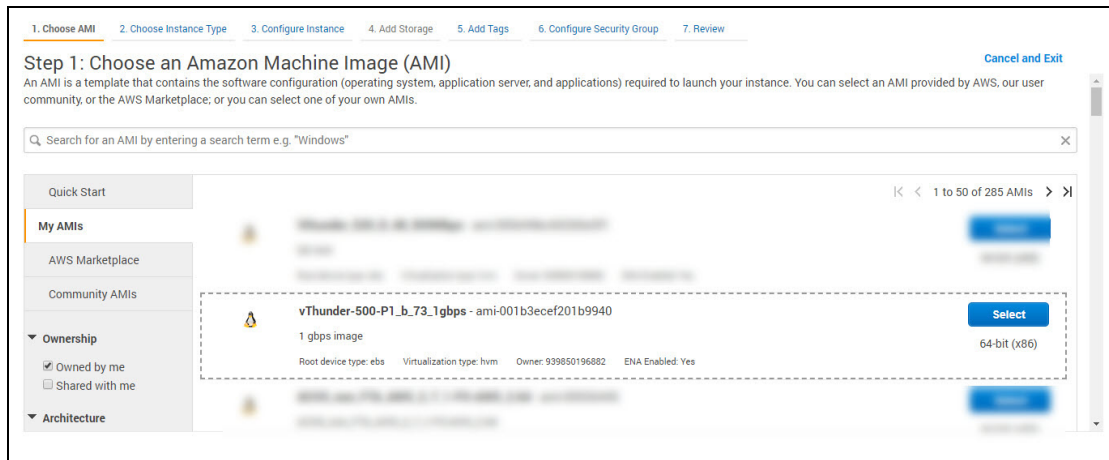
3. In the EC2 Dashboard, click on the **Instance > Launch Instance** as shown above.
Step 1: Choose an Amazon Machine Image (AMI) window is displayed.

Figure 21 : Choose an Amazon Machine Image (AMI) window



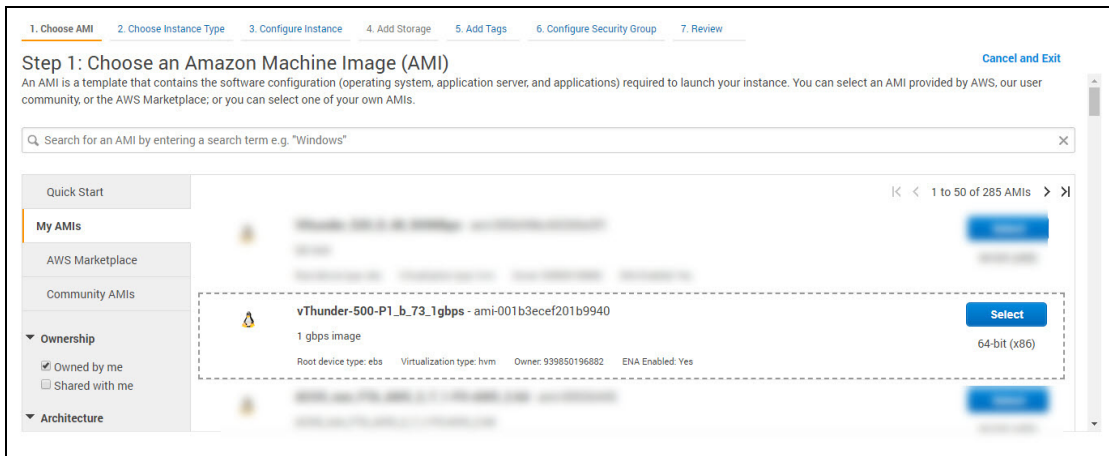
4. From the left-most column, under **Quick Start**, click the select **My AMIs** tab as shown in [Figure 22](#)

Figure 22 : Quick Start - My AMIs window



5. Select a vThunder AMI based on your requirements.

Figure 23 : Step1- Choose an Amazon Machine Image (AMI) window



6. Optionally, select **AWS Marketplace** from the Quick Start menu option. In the **Search AWS Marketplace Products** field, enter `A10 Networks` and press **Enter**.

NOTE: BYOL is a permanent license. This option is recommended if you prefer to own the license rather than being charged licensing fees on an hourly basis. Contact sales@a10networks.com for more information about the different pricing structures, or if you wish to purchase a permanent license.

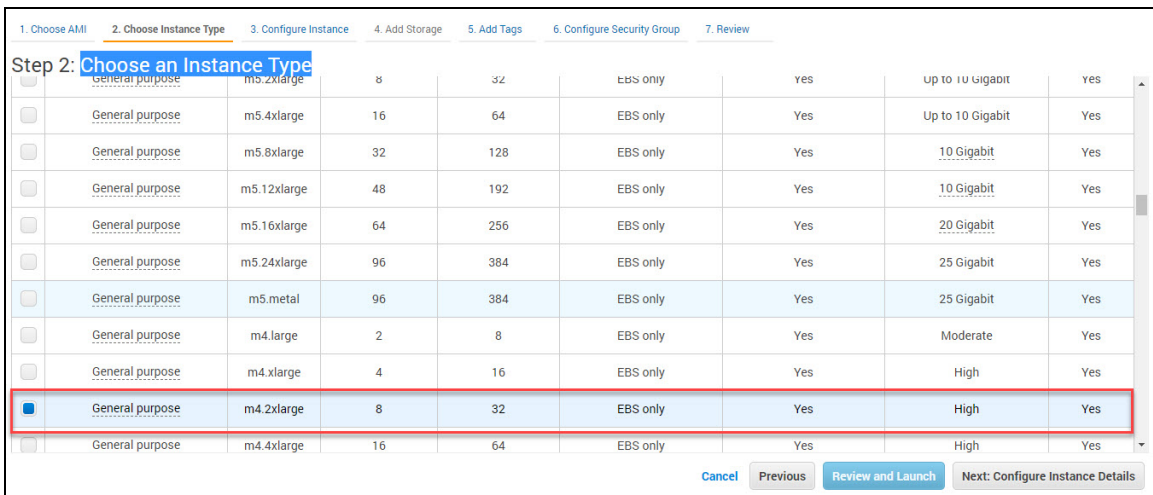
Step 2. Choose Instance Type

After you select a vThunder AMI, determine the instance type. The instance type defines the CPU, memory, storage, networking capacity, and performance. Each vThunder AMI has a recommended instance type highlighted.

After the vThunder AMI is selected, the Choose an Instance Type window is displayed.

NOTE: In general, A10 Networks recommends that you select an instance type with a minimum of 4 vCPUs, such as **m4.xlarge**.

Figure 24 : Step 2: Choose an Instance Type window:



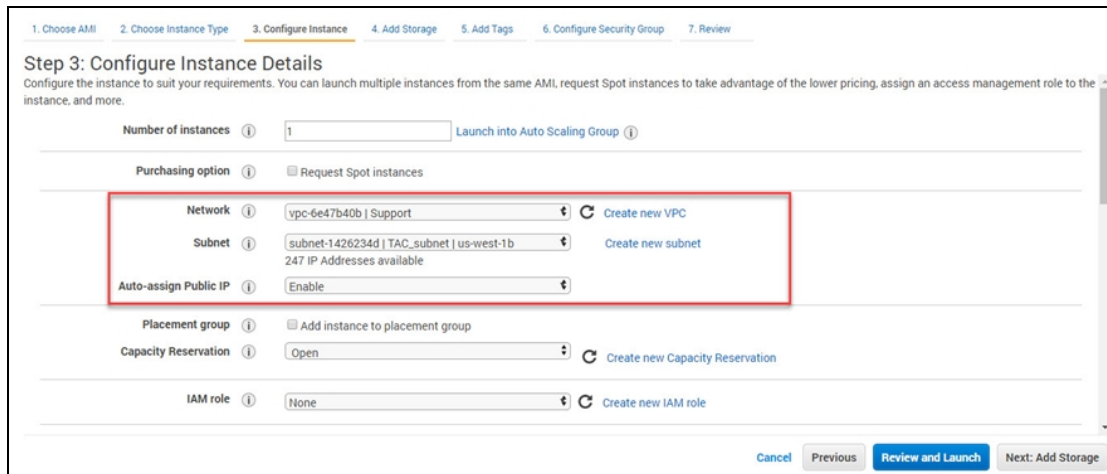
Instance Type	vCPUs	Memory (MiB)	Storage	EBS only	Network Bandwidth	On-demand Capacity
m3.xlarge	8	32	EBS only	Yes	Up to 10 Gigabit	Yes
m5.xlarge	16	64	EBS only	Yes	Up to 10 Gigabit	Yes
m5.8xlarge	32	128	EBS only	Yes	10 Gigabit	Yes
m5.12xlarge	48	192	EBS only	Yes	10 Gigabit	Yes
m5.16xlarge	64	256	EBS only	Yes	20 Gigabit	Yes
m5.24xlarge	96	384	EBS only	Yes	25 Gigabit	Yes
m5.metal	96	384	EBS only	Yes	25 Gigabit	Yes
m4.large	2	8	EBS only	Yes	Moderate	Yes
m4.xlarge	4	16	EBS only	Yes	High	Yes
m4.2xlarge	8	32	EBS only	Yes	High	Yes
m4.4xlarge	16	64	EBS only	Yes	High	Yes

Step 3. Configure the Instance

You can configure the new vThunder instance details as follows:

1. After the instance type is selected, click **Next: Configure Instance Details** button. The Configure Instance Details window is displayed.

Figure 25 : Step 3: Configure Instance Details window



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

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

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

Purchasing option Request Spot instances

Network [Create new VPC](#)

Subnet [Create new subnet](#)
247 IP Addresses available

Auto-assign Public IP

Placement group Add instance to placement group

Capacity Reservation [Create new Capacity Reservation](#)

IAM role [Create new IAM role](#)

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

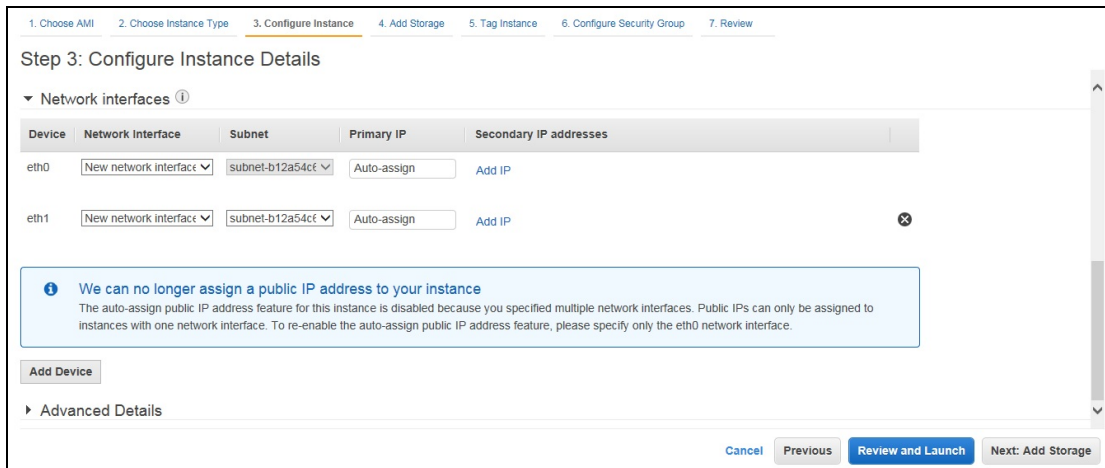
2. Retain the default values that appear in the window, except for the **Network**, **Subnet**, and setting **Auto-assign Public IP** to “*enable*.” It is recommended to select the correct VPC.

The VPC and subnet must already be set up when the instance was created. For more information, see [Creating and Configuring a VPC](#).

When you select a value for the Network and Subnet, a separate set of fields are displayed, which allow you to configure eth0 (the management interface), as shown in [Figure 26](#).

NOTE: Make sure all the interfaces are in different subnets. Make sure the primary interface (eth0) is in the public Internet-facing subnet for management.

Figure 26 : Configure the Instance Details - Network interface window



Step 3: Configure Instance Details

Network interfaces ⓘ

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses
eth0	New network interface	subnet-b12a54cf	Auto-assign	Add IP
eth1	New network interface	subnet-b12a54cf	Auto-assign	Add IP

i We can no longer assign a public IP address to your instance
The auto-assign public IP address feature for this instance is disabled because you specified multiple network interfaces. Public IPs can only be assigned to instances with one network interface. To re-enable the auto-assign public IP address feature, please specify only the eth0 network interface.

Add Device

Advanced Details

Cancel Previous **Review and Launch** Next: Add Storage

3. Click the **Add Device** button. The options for configuring “eth1” are displayed.
 - a. Select the network interface and subnet in the associated VPC.
 - b. The eth0 should use a different subnet than eth1.
 - c. In the **Primary IP** field, enter the IP, which should be in your designated subnet.

Although DHCP is used to assign an IP address to the network interfaces, by entering a specific IP address in this field, you can ensure that the DHCP server assigns the same IP address every time the vThunder instance is rebooted. Doing this helps avoid having to rewrite the aXAPI scripts, which contain IP addresses that could keep changing.
4. Click **Advanced Details** to provision the vThunder instance.

Figure 27 : Configure the Instance Details - Advanced Details window



- a. Accept the defaults for **Kernel ID** and **RAM disk ID**.
- b. Edit the following cloud-init configuration as appropriate:

```
a10_blob: |
!TEST
ip dns pri 8.8.8.8
glm use-mgmt-port
glm token vThxxxxxxxxxxx
glm enable-requests
glm send license-request
wr mem
```

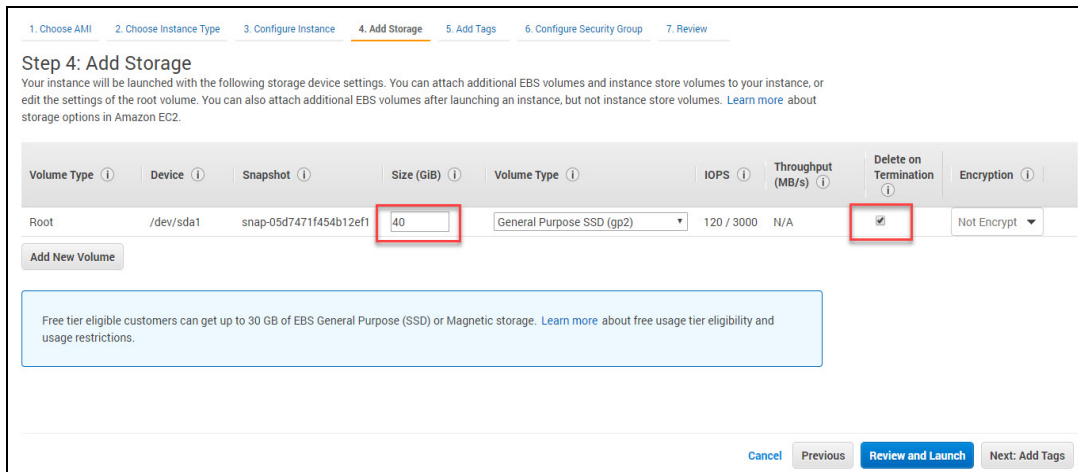
- c. Copy and paste the configuration as text in the blank field.
5. Click **Next: Add Storage** button.
The **Add Storage** window is displayed.

Step 4. Add Storage

1. In the **Add Storage** window, accept the default values.

NOTE: By default, the Add Storage value is 40GB. Enter the value in GB if more storage is required.

Figure 28 : Step 4- Add Storage” window



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

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/sda1	snap-05d7471f454b12ef1	40	General Purpose SSD (gp2)	120 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypt

[Add New Volume](#)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

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

2. Check the **Delete on Termination** box.
3. Click **Next: Add Tags** button.
The **Tag Instance** window is displayed.

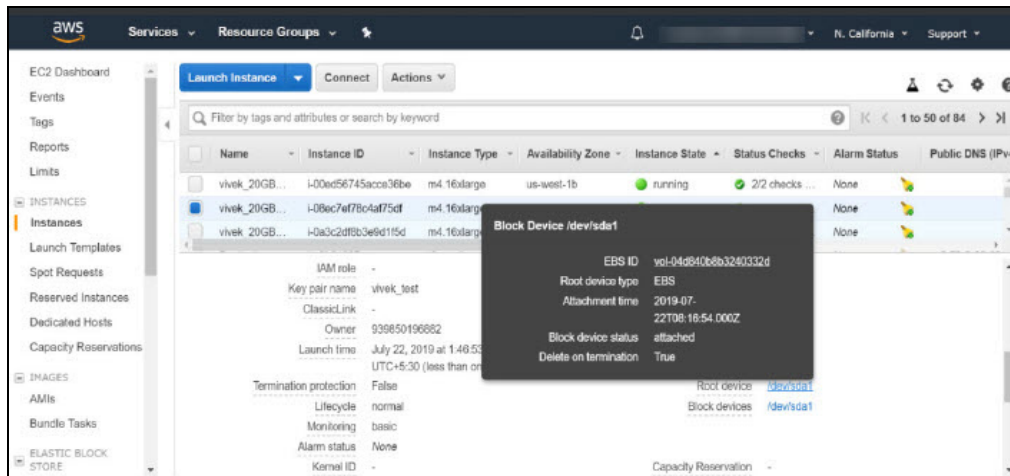
Expanding Virtual Hard Disk Size

The virtual Hard disk size in a vThunder can be expanded, even after the creation of the VM.

To expand the virtual hard disk size follow the following steps:

1. Navigate to **AWS > Services > Instances** option from the list of a menu option. The Launch instance window is displayed.
2. Select VM from instance window and power **OFF** the selected VM.

Figure 29 : Block Device window



3. Navigate to the bottom of the Instance window, and select **Root Device > EBS ID > Actions**.
4. On **Action** window choose the **Modify Volume** option and then provide the size.
5. Click the **Modify** tab to save the changes.
6. Power **ON** the VM. The virtual hard disk size in a vThunder is expanded and it gets reflected in "[show hardware](#)" command of vThunder CLI.

CAUTION: The size of the virtual disk can only be expanded but cannot be decreased.

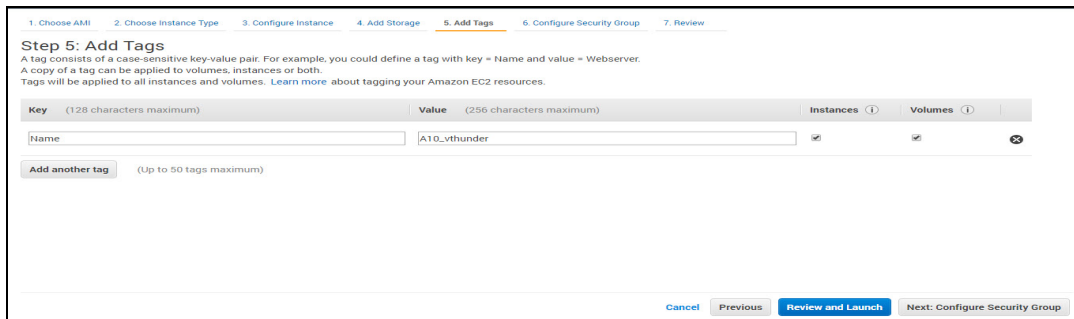
Step 5. Add Tags

1. In the **Tag Instance** window, you can assign a name to the instance or other aspects of the vThunder instance.

For example, enter a name for this instance in the Value field to make this instance easier to find from many instances.

NOTE: This is an optional setting and is intended for better user experience.

Figure 30 : Tag the Instance window



Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes
Name	A10_vthunder	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[Add another tag](#) (Up to 50 tags maximum)

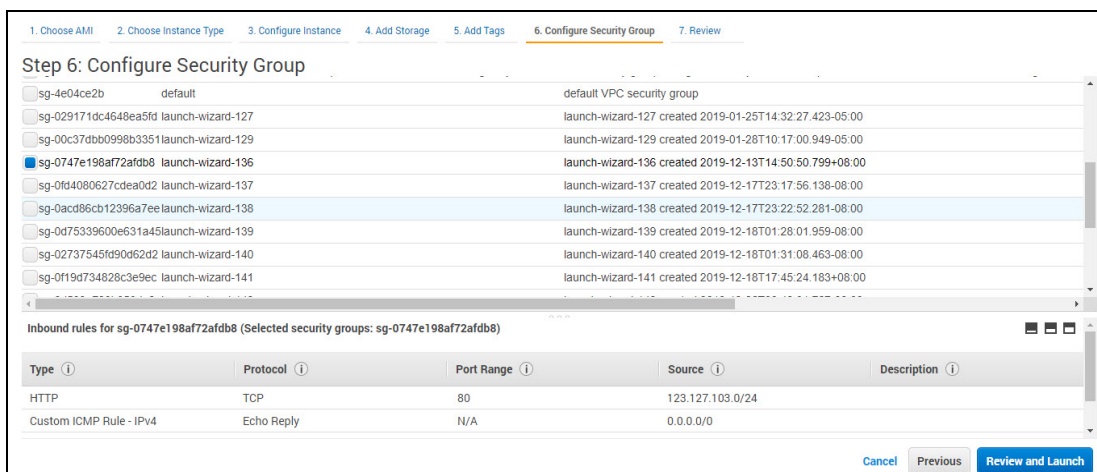
[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Security Group](#)

2. Click **Next: Configure Security Group** button.
The Configure Security Group window is displayed.

Step 6. Configure Security Group

1. User can configure the security group settings in one of the following ways:
 - Choose a pre-configured (default) security group.
 - Create a security group.

Figure 31 : Configure Security Group



Step 6: Configure Security Group

<input type="checkbox"/>	sg-4e04ce2b	default	default VPC security group
<input type="checkbox"/>	sg-029171dc4648ea5fd	launch-wizard-127	launch-wizard-127 created 2019-01-25T14:32:27.423-05:00
<input type="checkbox"/>	sg-00c37dbb0998b3351	launch-wizard-129	launch-wizard-129 created 2019-01-28T10:17:00.949-05:00
<input checked="" type="checkbox"/>	sg-0747e198af72afdb8	launch-wizard-136	launch-wizard-136 created 2019-12-13T14:50:50.799+08:00
<input type="checkbox"/>	sg-0fd4080627cdea0d2	launch-wizard-137	launch-wizard-137 created 2019-12-17T23:17:56.138-08:00
<input type="checkbox"/>	sg-0acd86cb12396a7ee	launch-wizard-138	launch-wizard-138 created 2019-12-17T23:22:52.281-08:00
<input type="checkbox"/>	sg-0d75339600e631a45	launch-wizard-139	launch-wizard-139 created 2019-12-18T01:28:01.959-08:00
<input type="checkbox"/>	sg-02737545fd90d62d2	launch-wizard-140	launch-wizard-140 created 2019-12-18T01:31:08.463-08:00
<input type="checkbox"/>	sg-0f19d734828c3e9ec	launch-wizard-141	launch-wizard-141 created 2019-12-18T17:45:24.183+08:00

Inbound rules for sg-0747e198af72afdb8 (Selected security groups: sg-0747e198af72afdb8)

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	123.127.103.0/24	
Custom ICMP Rule - IPv4	Echo Reply	N/A	0.0.0.0/0	

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

2. If creating a new security group, it is recommended that you use the following settings:

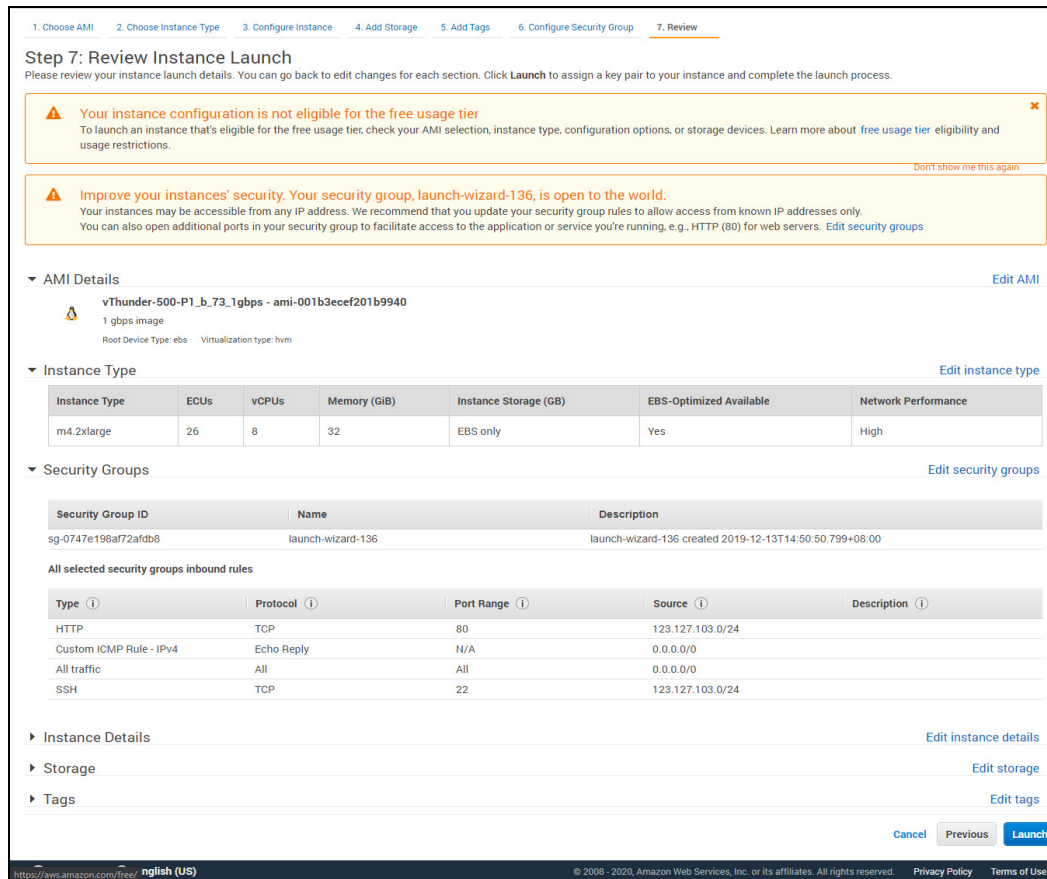
Type ⁱ	Protocol ⁱ	Port Range ⁱ	Source ⁱ	
SSH <input type="button" value="v"/>	TCP	22	Anywhere <input type="button" value="v"/> 0.0.0.0/0	<input type="button" value="x"/>
HTTP <input type="button" value="v"/>	TCP	80	Anywhere <input type="button" value="v"/> 0.0.0.0/0	<input type="button" value="x"/>
HTTPS <input type="button" value="v"/>	TCP	443	Anywhere <input type="button" value="v"/> 0.0.0.0/0	<input type="button" value="x"/>
Custom TCP Rule <input type="button" value="v"/>	TCP	8080	Anywhere <input type="button" value="v"/> 0.0.0.0/0	<input type="button" value="x"/>
Custom TCP Rule <input type="button" value="v"/>	TCP	8443	Anywhere <input type="button" value="v"/> 0.0.0.0/0	<input type="button" value="x"/>
Custom TCP Rule <input type="button" value="v"/>	TCP	4149	Anywhere <input type="button" value="v"/> 0.0.0.0/0	<input type="button" value="x"/>
Custom UDP Rule <input type="button" value="v"/>	UDP	161	Anywhere <input type="button" value="v"/> 0.0.0.0/0	<input type="button" value="x"/>

3. Click **Review and Launch** to proceed.
The **Review Instance Launch** window is displayed.

Step 7. Review the Configuration Changes

1. In the **Review Instance Launch** window as shown in [Figure 32](#), verify the settings, and if everything appears in order, click the **Launch** button to launch the vThunder instance.

Figure 32 : Review Instance Launch - Settings for this vThunder Instance



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

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

⚠ Your instance configuration is not eligible for the free usage tier

To launch an instance that's eligible for the free usage tier, check your AMI selection, instance type, configuration options, or storage devices. Learn more about [free usage tier](#) eligibility and usage restrictions.

[Don't show me this again](#)

⚠ Improve your instances' security. Your security group, launch-wizard-136, is open to the world.

Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only. You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. [Edit security groups](#)

AMI Details [Edit AMI](#)

vThunder-500-P1_b_73_1gbps - ami-001b3ecef201b9940
1 gbps image
Root Device Type: ebs Virtualization type: hvm

Instance Type [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
m4.2xlarge	26	8	32	EBS only	Yes	High

Security Groups [Edit security groups](#)

Security Group ID	Name	Description
sg-0747e198af72afdb8	launch-wizard-136	launch-wizard-136 created 2019-12-13T14:50:50.799+08:00

All selected security groups inbound rules

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	123.127.103.0/24	
Custom ICMP Rule - IPv4	Echo Reply	N/A	0.0.0.0/0	
All traffic	All	All	0.0.0.0/0	
SSH	TCP	22	123.127.103.0/24	

Instance Details [Edit instance details](#)

Storage [Edit storage](#)

Tags [Edit tags](#)

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

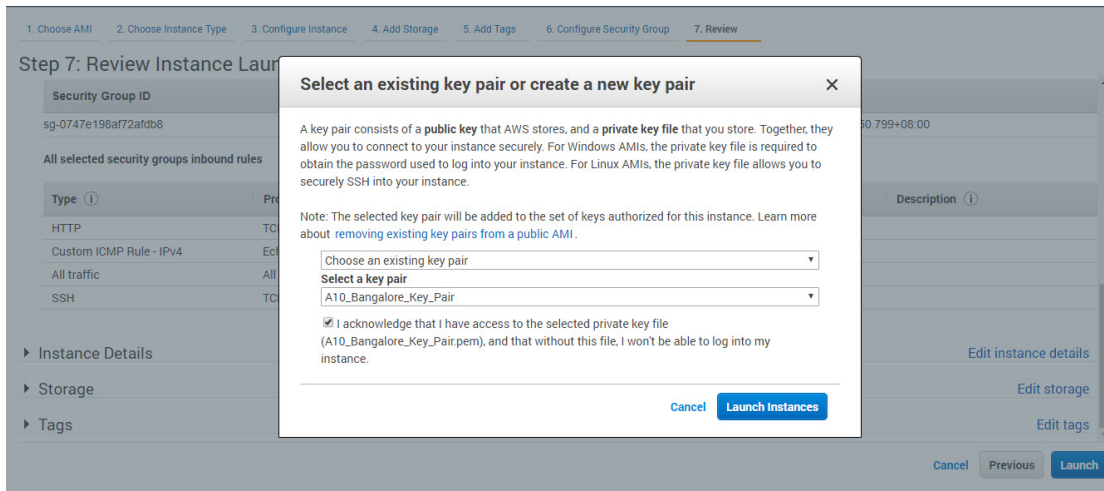
https://aws.amazon.com/Free/ english (US) © 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

2. In the **Select an existing key pair or create a new key pair** window as shown in [Figure 33](#). Click the drop-down menu and select one of the following options from the drop-down menu:

- Choose an existing key pair
- Create a new key pair
 - Enter a name in the **Key pair name** field.
 - Click **Download Key Pair**.
- Proceed without a Key Pair.

If you have questions about setting up the key pairs, or if you have trouble using the SSH key to log in, review the EC2 documentation about key pairs at <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html>.

Figure 33 : Select an existing Key Pair or create a new Key pair window

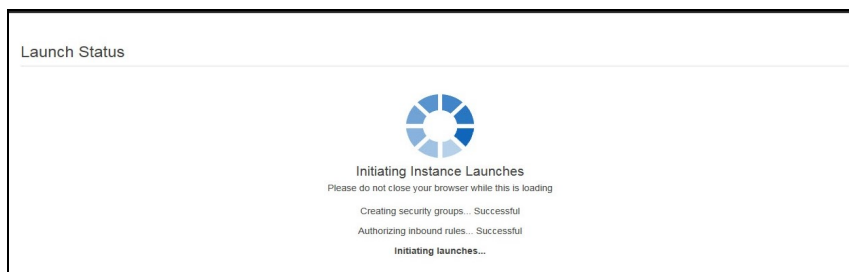


3. Check the Acknowledgment statement box.

4. Click **Launch Instance**.

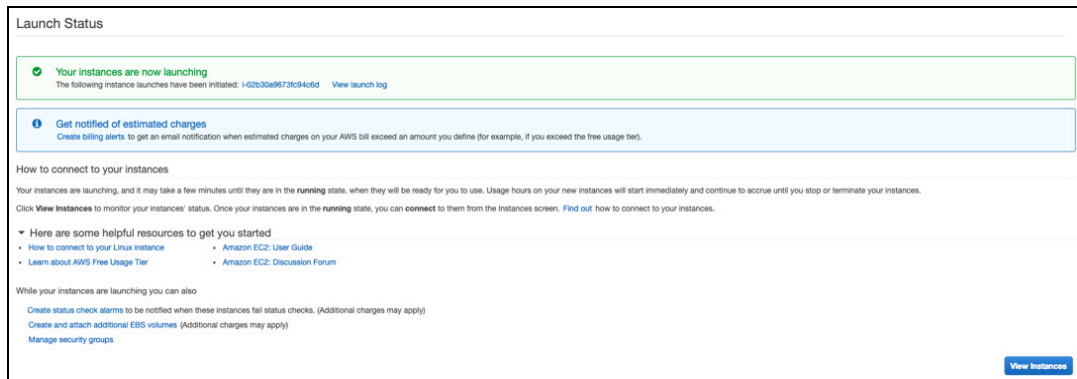
The **Launch Status** - Initiating Instance Launches window is displayed.

Figure 34 : Launch Status window



When finished launching, the **Launch Status** window offers a confirmation message similar to that shown in [Figure 35](#).

Figure 35 : Launch Status – Confirmation Message window



5. Click **View Instance** button to view the launched instance in the Instance page.

NOTE: Select the instance, and view its details in the **Description** tab. The Private IPs field displays the private IP address that is assigned to the created instance from the range of IP addresses in the subnet.

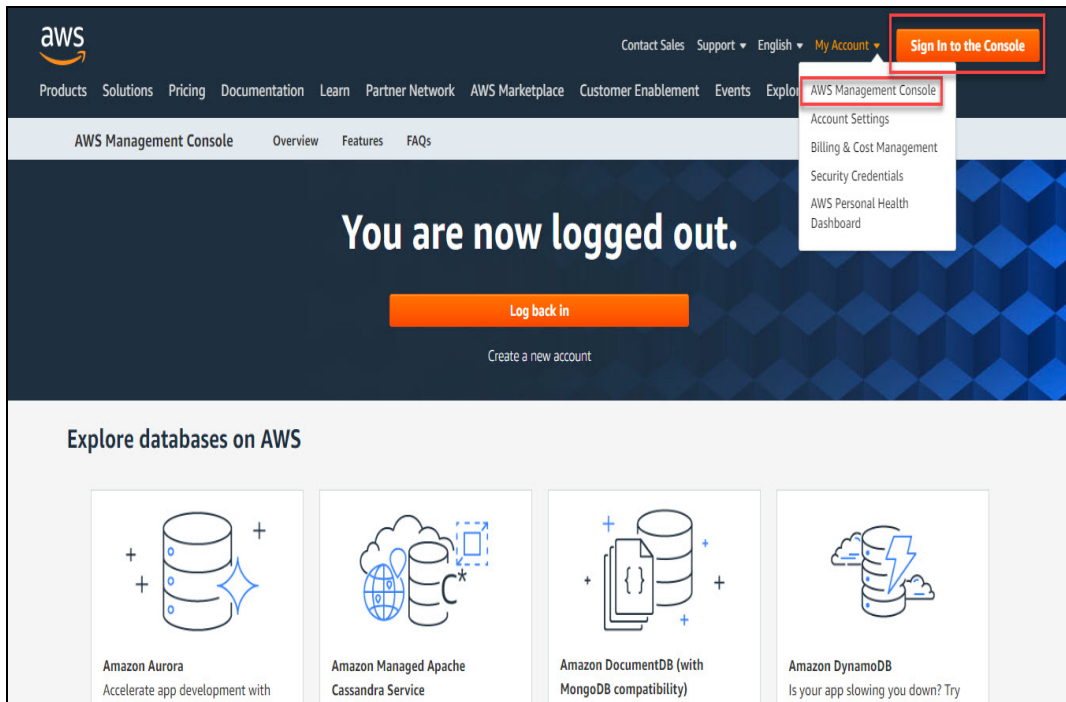
Manage Subscriptions

The launching AWS image with manage subscriptions option allows users to quickly review, modify, and then launch a single instance of the software with settings recommended by the software seller.

For the launching AWS image, perform the following:

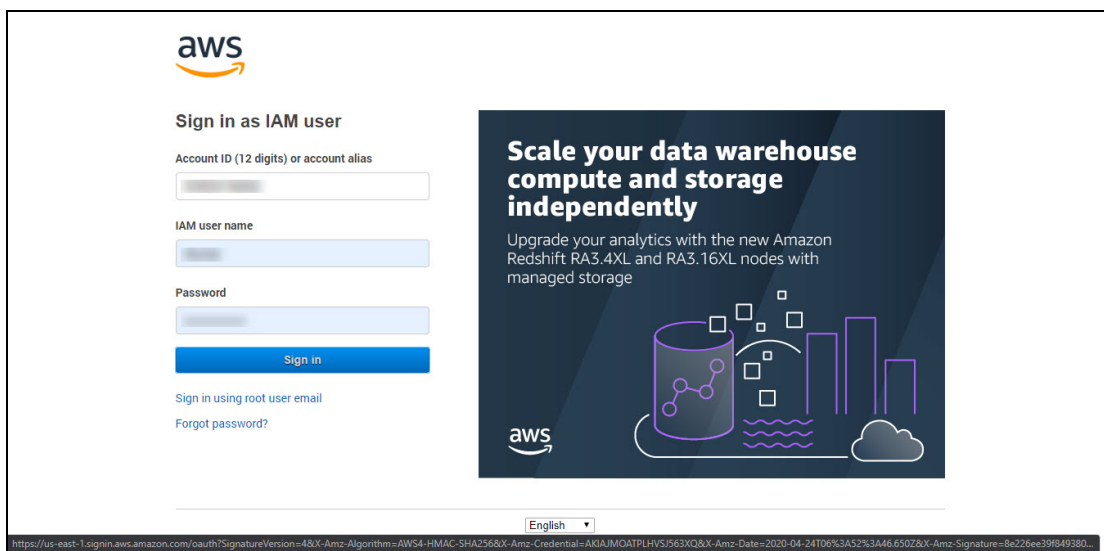
1. Access the AWS website at <https://aws.amazon.com/console/>.
2. Click the **Sign In to Console** button on the upper-left corner or navigate to **My Account > AWS Management Console** option from the list of available options.

Figure 36 : AWS Management Console window



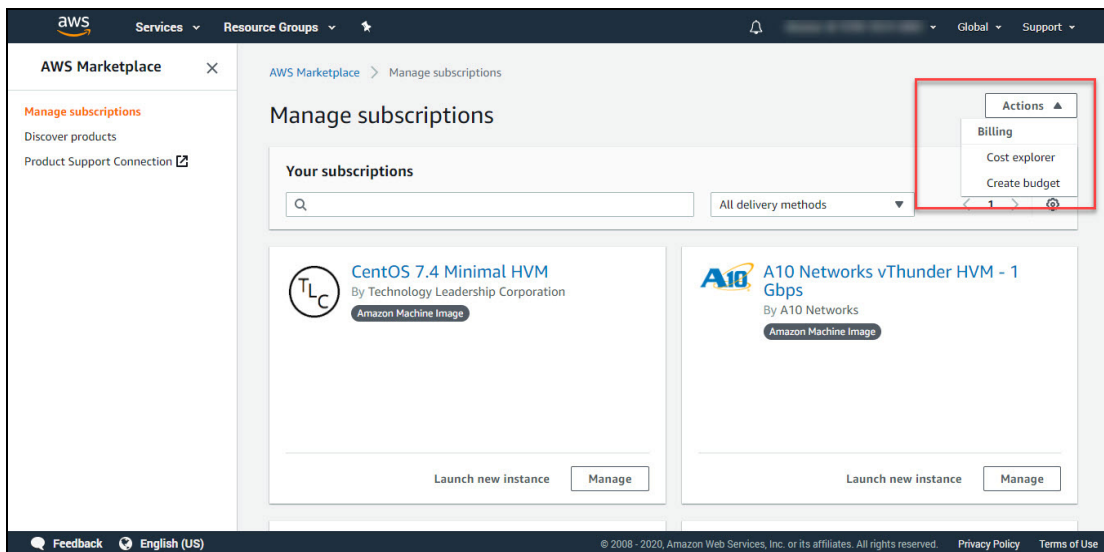
3. Sign in to the Amazon console with valid **Account Id (12 digits)** or **account alias**, **IAM user name** and **Password**. For more information, see [Creating an AWS Account](#)

Figure 37 : Sign in window



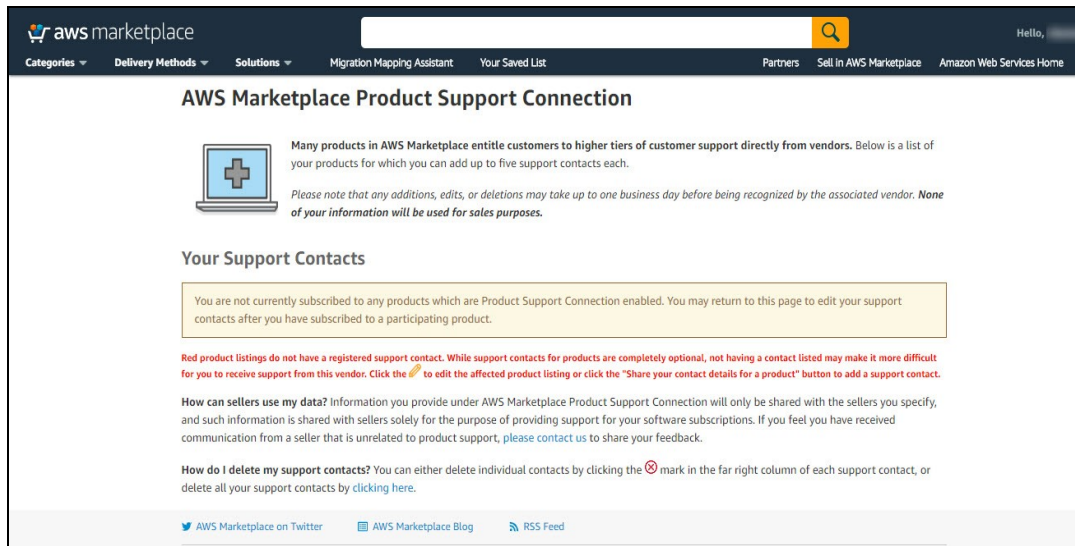
4. On the AWS Management Console page, navigate to **All services > AWS Cost Management > AWS Market Subscriptions** option. The AWS Marketplace > Manage subscriptions window is displayed. Do one of the following:
 - From the right pane, click the **Discover products** link under the **AWS Marketplace** to Search AWS marketplace products.
 - From the right pane, click the **Product Support Connection** link under the **AWS Marketplace** to learn more about the AWS Marketplace product support connection. The AWS Marketplace Product Support Connection window is displayed.

Figure 38 : Manage subscription window

**NOTE:**

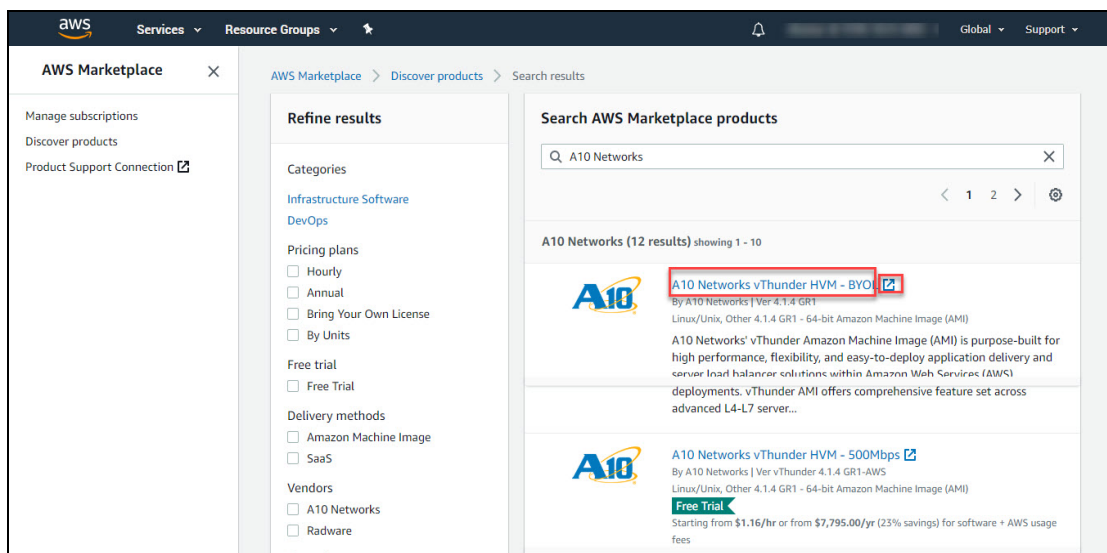
The manage subscription option launches pre-configured software with just a few clicks, and choose software solutions in AMI, SaaS, and other formats. Users can also browse and subscribe to data products. Flexible pricing options include free trial, hourly, monthly, annual, multi-year, and BYOL, and get billed from one source. AWS handles billing and payments, and charges appear on customers' AWS bill.

Figure 39 : AWS Marketplace Product Support Connection window



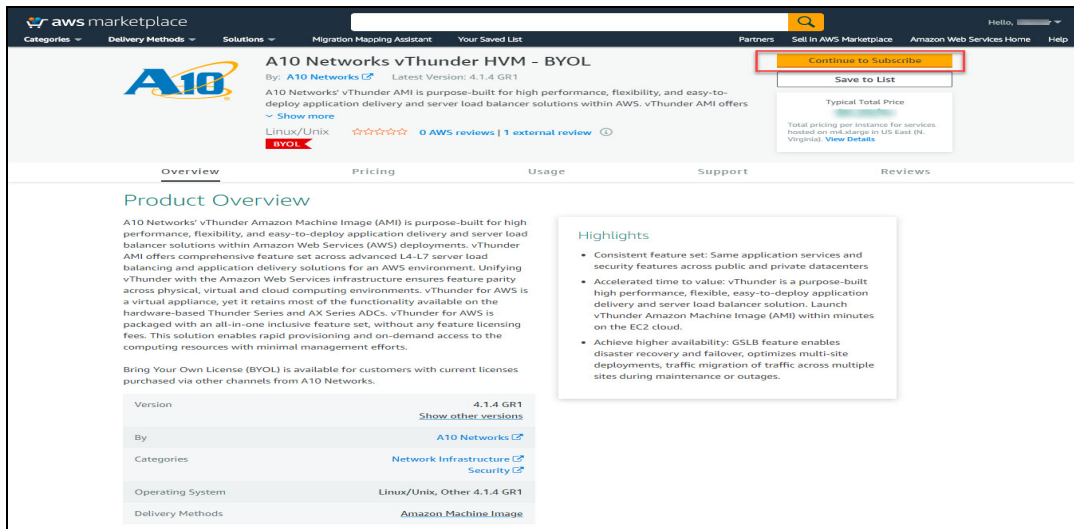
5. (Optional) From the right pane, click the **Discover products** link under the AWS Marketplace to Search AWS marketplace products.
6. In the search box, enter `A10 Networks`.
A list of Search results - AWS images published by A10 Networks is displayed.

Figure 40 : Search results window



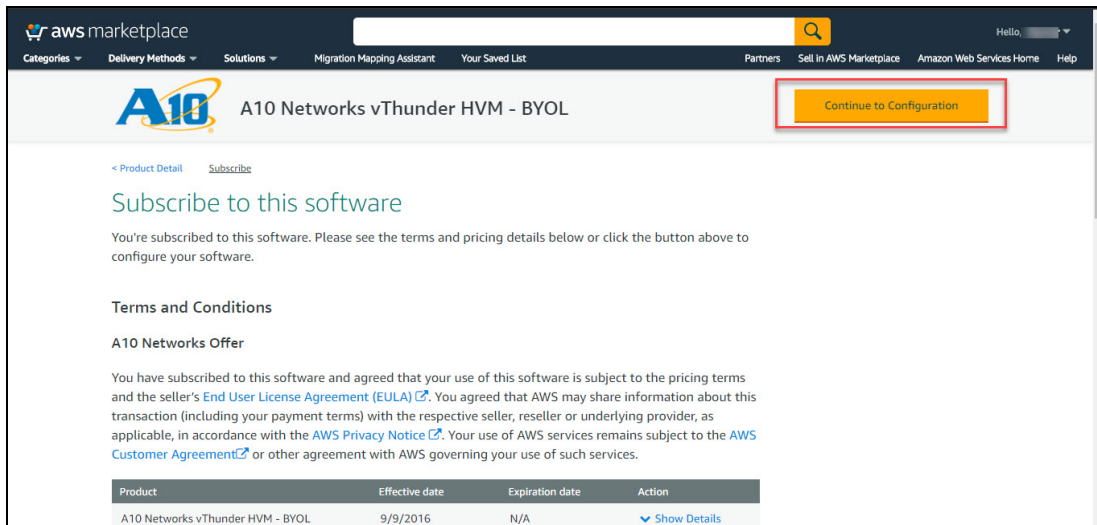
7. Click the required AWS Image link.
The product details window is displayed.

Figure 41 : Product Details window



8. Click **Continue to Subscribe** tab. The Subscribe to this software window is displayed.

Figure 42 : Subscribe to this software-1 window



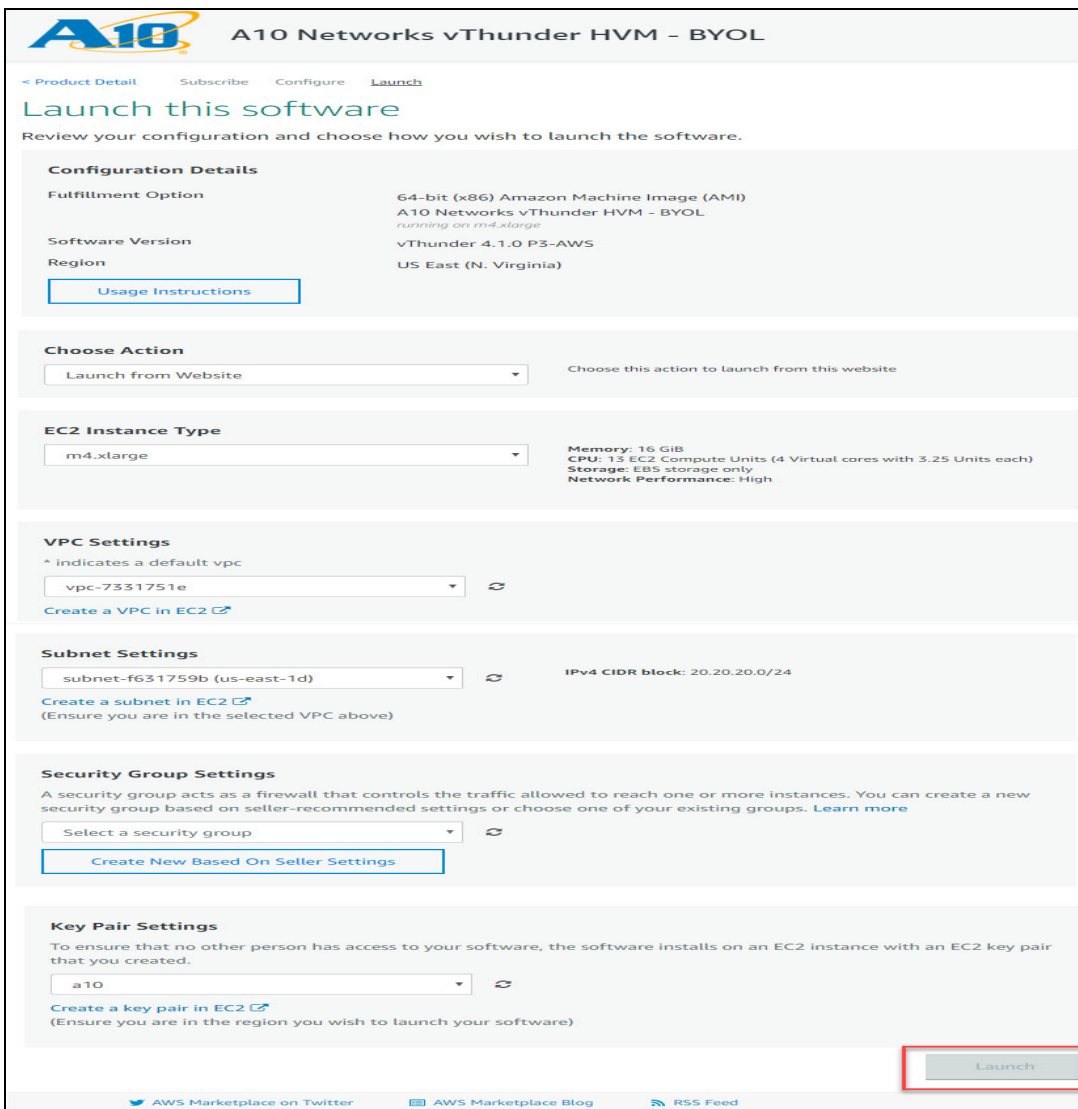
9. Click the **Continue to Configuration** tab. The Configure this software window is displayed.

Figure 43 : Configure this software - 2 window

|

10. Confirm that the settings under the following fields are correct.
 - Fulfillment Option
 - Software Version
 - Region
11. Click **Continue Launch** to create the AWS instance.
If the field is grayed out, review your settings; there might be an invalid value assigned to one of the fields. The Launch this software window is displayed.

Figure 44 : Launch this software window



A10 Networks vThunder HVM - BYOL

< Product Detail Subscribe Configure **Launch**

Launch this software

Review your configuration and choose how you wish to launch the software.

Configuration Details

Fulfillment Option	64-bit (x86) Amazon Machine Image (AMI) A10 Networks vThunder HVM - BYOL <small>running on m4.xlarge</small>
Software Version	vThunder 4.1.0 P3-AWS
Region	US East (N. Virginia)

[Usage Instructions](#)

Choose Action

Launch from Website Choose this action to launch from this website

EC2 Instance Type

m4.xlarge Memory: 16 GiB
CPU: 13 EC2 Compute Units (4 Virtual cores with 3.25 Units each)
Storage: EBS storage only
Network Performance: High

VPC Settings

* indicates a default vpc

vpc-7331751e [Create a VPC in EC2](#)

Subnet Settings

subnet-f631759b (us-east-1d) IPv4 CIDR block: 20.20.20.0/24

[Create a subnet in EC2](#)
(Ensure you are in the selected VPC above)

Security Group Settings

A security group acts as a firewall that controls the traffic allowed to reach one or more instances. You can create a new security group based on seller-recommended settings or choose one of your existing groups. [Learn more](#)

Select a security group [Create New Based On Seller Settings](#)

Key Pair Settings

To ensure that no other person has access to your software, the software installs on an EC2 instance with an EC2 key pair that you created.

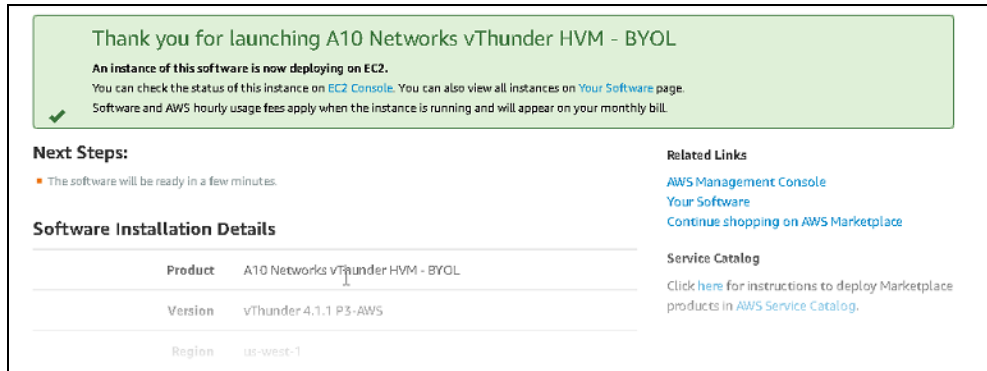
a10 [Create a key pair in EC2](#)
(Ensure you are in the region you wish to launch your software)

Launch

[AWS Marketplace on Twitter](#) [AWS Marketplace Blog](#) [RSS Feed](#)

- Click on the **Launch** button to launch the selected software with the set configuration.
The AWS instance is created and a Thank you message window is displayed.

Figure 45 : Thank you message window



Thank you for launching A10 Networks vThunder HVM - BYOL

An instance of this software is now deploying on EC2.
You can check the status of this instance on [EC2 Console](#). You can also view all instances on [Your Software](#) page.
Software and AWS hourly usage fees apply when the instance is running and will appear on your monthly bill.

Next Steps:

- The software will be ready in a few minutes.

Software Installation Details

Product	A10 Networks vThunder HVM - BYOL
Version	vThunder 4.1.1 P3-AWS
Region	us-west-1

Related Links

- [AWS Management Console](#)
- [Your Software](#)
- [Continue shopping on AWS Marketplace](#)

Service Catalog

Click [here](#) for instructions to deploy Marketplace products in [AWS Service Catalog](#).

Post-Installation Tasks

This section provides information about the post-installation tasks required for monitoring and configuring the vThunder instance.

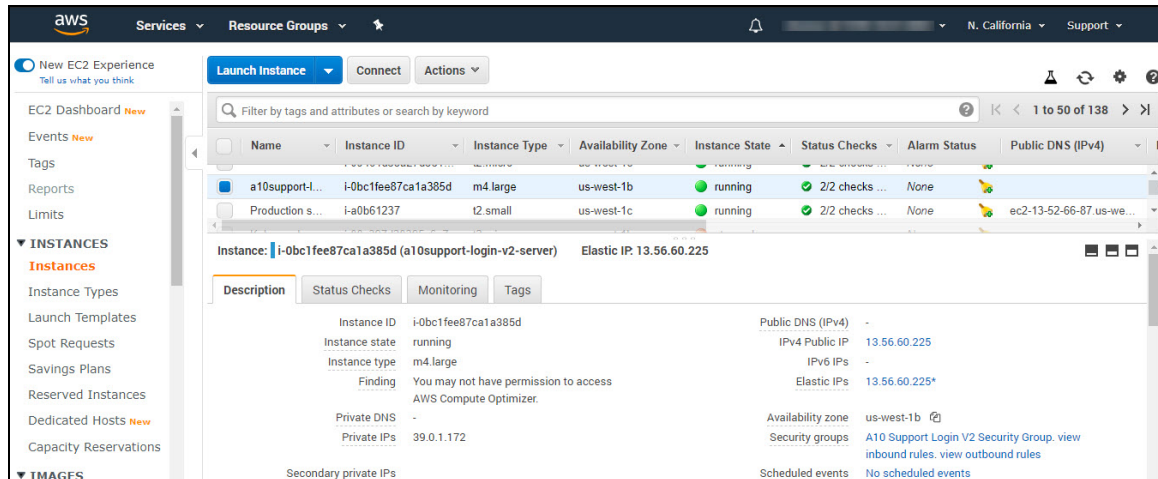
The following topics are covered:

Monitoring and Configuring the vThunder Instance	48
Accessing vThunder	49
Elastic IP Address	49
Associating an Elastic IP Address	49
Login to vThunder Instances	51
Login through CLI	51
Login through GUI	53
Configuring DHCP and the VIP in vThunder	55
Changing Source or Destination Checks	56
Disabling Change Source or Destination Checks	56

Monitoring and Configuring the vThunder Instance

To monitor the vThunder instance you just created, scroll to the bottom right and click the **View Instances** button. [Figure 46](#) shows the new vThunder instance just created.

Figure 46 : Monitor the New vThunder Instance



From the above-mentioned window, view the information about all instances or establish a connection to the instance. Select a vThunder instance and click on any of the tabs near the bottom of the window for information about the instance. The tabs are described as follows:

- **Description** — View details about an instance.
- **Status Checks** — Create a status check.
- **Monitoring** — Set up an alarm that is based on CPU utilization rates, disk usage, or other parameters.
- **Tags** — Edit the tags for an instance.

Now that the vThunder instance is launched, you can access the instance by using either the GUI or CLI.

Accessing vThunder

The following are the prerequisite to access vThunder by using either the CLI or the GUI:

- The default management IP address is the Elastic IP associated with the IP of the first interface (eth0). To assign the elastic IP, refer to [Elastic IP Address](#).
- SSH access is enabled by default on the management interface only and disabled by default on all data interfaces. SSH access uses the key-pair defined in [Step 7. Review the Configuration Changes](#) . Configure your SSH client accordingly for CLI access.

NOTE: For accessing GUI, the instance ID is the default password.

Elastic IP Address

Once the VPC instance is launched into a public subnet — a subnet that has a route to an Internet gateway. However, the instance in the subnet also needs a public IPv4 address to be able to communicate with the Internet.

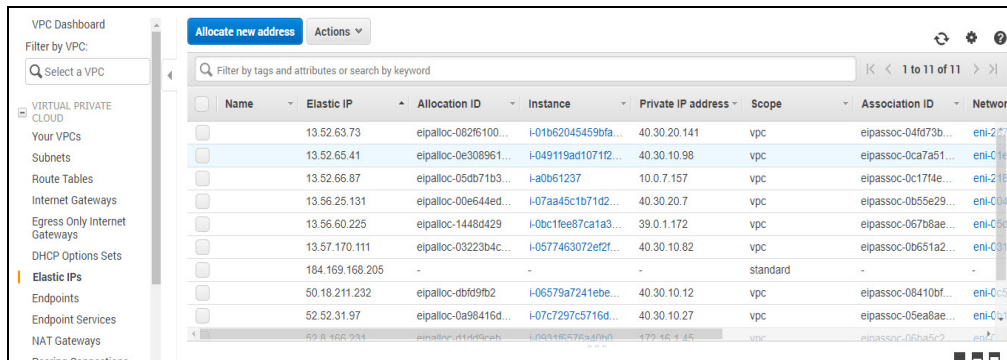
NOTE: By default, an instance in a non-default VPC is not allocated to a public IPv4 address.

Associating an Elastic IP Address

To allocate an Elastic IP address to the account, and then associate it with the above created instance, perform the following:

1. In the Services navigation pane, navigate to **Networking & Content Delivery** > **VPC** > **Elastic IPs** menu open.

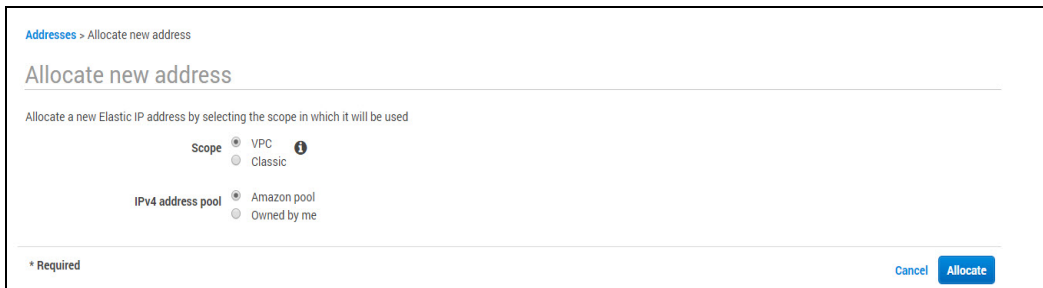
Figure 47 : Elastic IPs window



Name	Elastic IP	Allocation ID	Instance	Private IP address	Scope	Association ID	Network
	13.52.63.73	eipalloc-082f6100...	I-01b62045459bfa...	40.30.20.141	vpc	eipassoc-04fd73b...	eni-227...
	13.52.65.41	eipalloc-0e308961...	I-049119ad1071f2...	40.30.10.98	vpc	eipassoc-0ca7a51...	eni-01e...
	13.52.66.87	eipalloc-05db71b3...	I-a0b61237	10.0.7.157	vpc	eipassoc-0c17f4e...	eni-218...
	13.56.25.131	eipalloc-00e644ed...	I-07aa45c1b71d2...	40.30.20.7	vpc	eipassoc-0b55e29...	eni-004...
	13.56.60.225	eipalloc-1448d429	I-0bc1fee87ca1a3...	39.0.1.172	vpc	eipassoc-067b8ae...	eni-050...
	13.57.170.111	eipalloc-03223b4c...	I-0577463072ef2f...	40.30.10.82	vpc	eipassoc-0b651a2...	eni-081...
	184.169.168.205	-	-	-	standard	-	-
	50.18.211.232	eipalloc-dbfd9fb2	I-06579a7241ebe...	40.30.10.12	vpc	eipassoc-08410bf...	eni-0c5...
	52.52.31.97	eipalloc-0a98416d...	I-07c7297c5716d...	40.30.10.27	vpc	eipassoc-05ea8ae...	eni-0c1...
	52.8.168.231	eipalloc-d1fd95ab...	I-09316575a4f9d...	172.16.4.45	vpc	eipassoc-06ba5c2...	eni-...

2. Select the **Allocate new address** tab, then **Allocate**.

Figure 48 : Allocate new address window



Addresses > Allocate new address

Allocate new address

Allocate a new Elastic IP address by selecting the scope in which it will be used

Scope VPC Classic

IPv4 address pool Amazon pool Owned by me

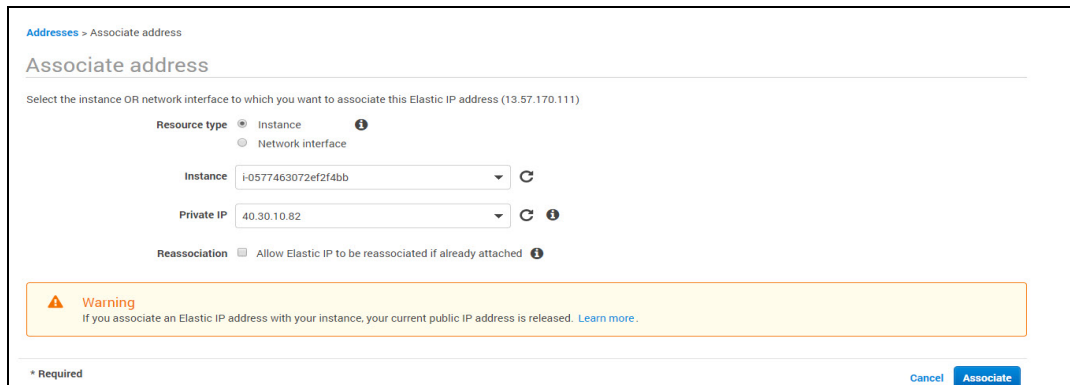
* Required

Cancel Allocate

NOTE: If the user account supports EC2-Classic, first choose VPC.

3. Select the **Elastic IP address** from the Elastic IP list page, select the **Actions** tab, and then select the **Associate Address**. The Associate Address window is displayed.

Figure 49 : Associate address window



4. For the Resource type, ensure that **Instance** is selected. Select the **Instance** from the Instance list.
5. Select the corresponding private IP address.
6. Click the **Associate** tab to save and to associate the elastic IP address.

NOTE: An Elastic IP address is a public IPv4 address that the user allocates to their account. It is associated with and from instances as required, and it's allocated to the user's account until the user chooses to release it.

Login to vThunder Instances

ACOS devices provide advance features for securing management access to the vThunder instances through:

- [Login through CLI](#)
- [Login through GUI](#)

NOTE: A10 Networks recommends that the basic security settings are done before assessing vThunder devices.

Login through CLI

To log into the CLI by using SSH, perform the following steps:

On a PC connected to a network that can access the vThunder management interface, open an SSH client.

1. On a PC connected to a network that can access the vThunder management interface, open an SSH client.
2. Locate the private key that you created in [Step 7. Review the Configuration Changes](#).

The wizard automatically detects the key you used to launch the instance.

3. Use the following command to change the permissions on the file so that only the root user can read the key:

```
chmod 400 vThunderkp.pem
```

4. Connect to the AWS instance by using the elastic IP you associated in [Associating an Elastic IP Address](#).

For example, if the elastic IP address is **10x.xx.xx.xxx**, run the following command:

```
ssh -i "vthunderkp.pem" admin@10x.xx.xx.xxx
```

5. Generally, if this is the first time the SSH client has accessed the vThunder instance, the SSH client displays a security warning. Read the warning carefully, then acknowledge the warning to complete the connection. Press **Enter**.

The command prompt for the User EXEC level of the CLI is displayed:

```
vThunder (NOLICENSE) >
```

The User EXEC level allows you to enter a few basic commands, including some **show** commands as well as **ping** and **traceroute**.

NOTE: The vThunder prompt indicates that the vThunder instance is not licensed.

6. To access the Privileged EXEC level of the CLI and allow access to all configuration levels, enter the **enable** command.

At the `Password:` prompt, press enter.

The command prompt for the Privileged EXEC level of the CLI is displayed as follows:

```
vThunder (NOLICENSE) #
```


- To access the global configuration level, enter the `configure` command. The following command prompt is displayed:

```
vThunder (config) (NOLICENSE) #
```

Login through GUI

Web access to the vThunder instance is supported on the Web browsers listed in [GUI Browser Support](#).

Table 4 : GUI Browser Support

Browser	Windows	Linux	MAC
IE 10.0 and higher	Supported	N/A	N/A
Firefox 40.0.3 and higher	Supported	Supported	N/A
Chrome 45.0.2454.93 and higher	Supported	Supported	Supported

A screen resolution of at least 1024x768 is recommended.

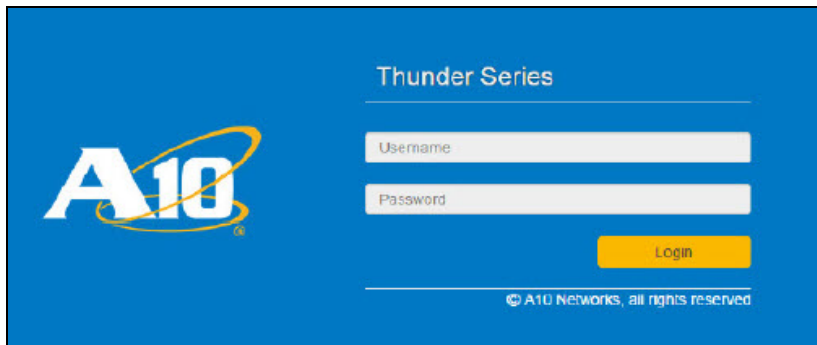
To access the vThunder instance by using the GUI, perform the following steps:

- Open a supported web browser.
- In the URL field, enter the IP address of the management interface of the vThunder instance.
- If the browser displays a certificate warning, select the option to continue.

NOTE: To prevent the certificate warning from appearing in the future, you can install a certificate signed by a Certificate Authority.

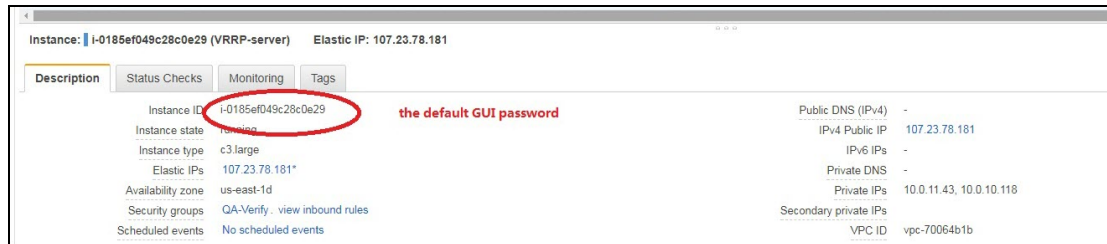
A login page is displayed as shown in [Figure 50](#). The name and appearance of the dialog depend on the browser you are using and the specific device which you are trying to access.

Figure 50 : Example GUI Login Dialog



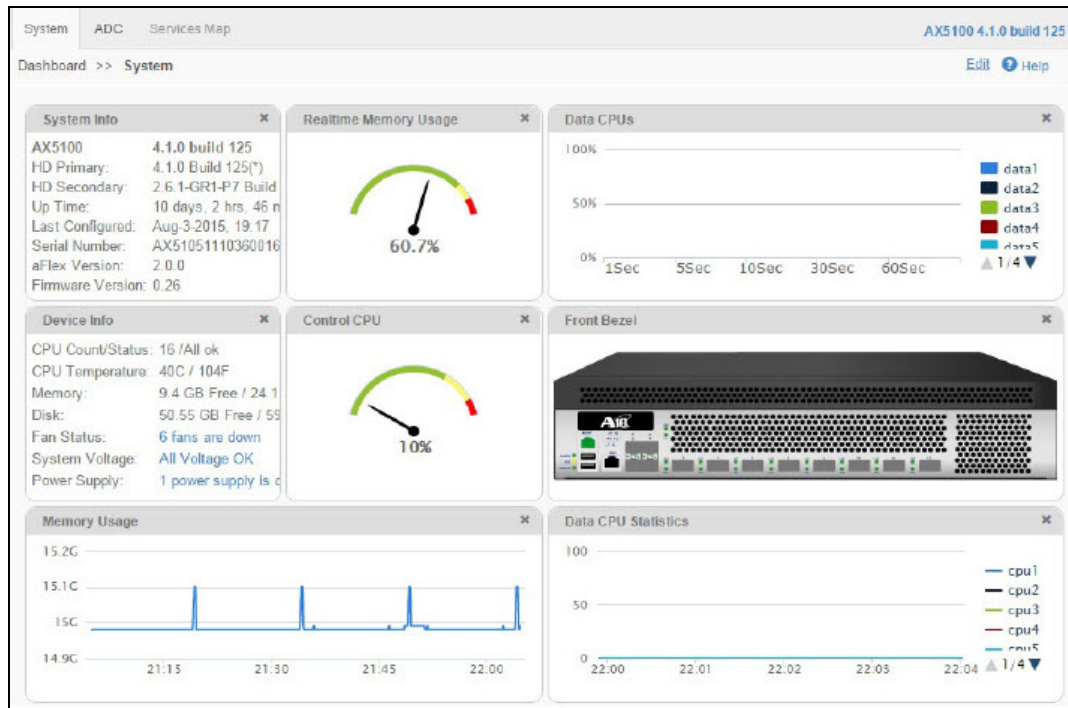
4. Enter your default username `admin` and default password and click **Login**. The default password is the instance-id as shown in [Figure 51](#) below.

Figure 51 : Default GUI Password



The Dashboard is displayed as shown in [Figure 52](#), showing at-a-glance information for your vThunder instance. You can access this page again at any time while using the GUI by selecting the **Dashboard**. Refer to the GUI online help for detailed information about this and all other GUI screens.

Figure 52 : Dashboard



NOTE: GUI management sessions are not automatically terminated when user closes the browser window. The session remains in effect until it times out. To immediately terminate a GUI session, click the Sign Out icon in the menu bar.

Configuring DHCP and the VIP in vThunder

To configure DHCP and the VIP for the vThunder Instance, perform the following:

1. SSH to the Elastic IP of the vThunder instance.
2. Use the following CLI commands to force the interfaces to use the private IP that was assigned by DHCP:

```
interface ethernet 1
  ip address dhcp
interface ethernet 2
  ip address dhcp
```

3. Use the following commands to configure the vThunder to use the private IP (assigned to the interface by DHCP) as the VIP:

```
slb virtual-server v1 <IP>
  port 80 tcp
  service-group http-sg1
```

In this case, the IP address that is configured here needs to be added as the “secondary IP address” from the AWS GUI.

4. To configure additional private IPs, (which are necessary for adding VIPs to your vThunder instance), do the following:
 - a. In the AWS management console, add additional private IPs on the client-side interface. Right-click the instance, and then select Manage Private IP addresses from the drop-down menu.
 - b. Associate the Elastic IPs with the recently-added private IPs.
 - c. From within vThunder, directly configure the private IP as a VIP by using the following CLI commands:

```
slb virtual-server v2 10.0.1.11
  port 80 tcp
  service-group http-sg2
```

Changing Source or Destination Checks

By default, each EC2 instance performs source or destination checks for all instances. For any instance has the source or destination of any traffic that it sends or receives. However, a NAT instance enables one to send and receive traffic when the source or destination is not itself. Therefore, disable the source/destination checks on the NAT instance.

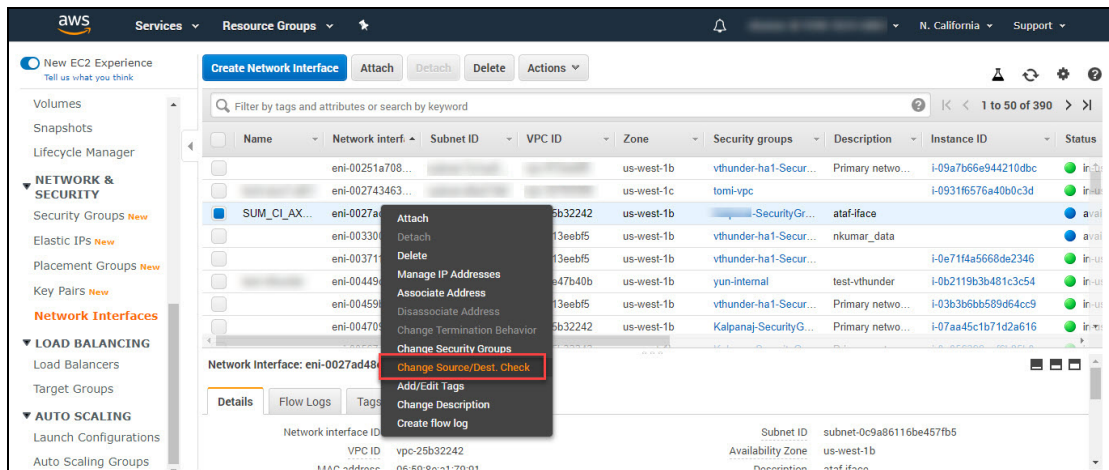
Disabling Change Source or Destination Checks

Disabling source and destination checking are required to make EC2 ignore the checks while operating as NAT type of interface.

To disable source or destination checking using the console, perform the following:

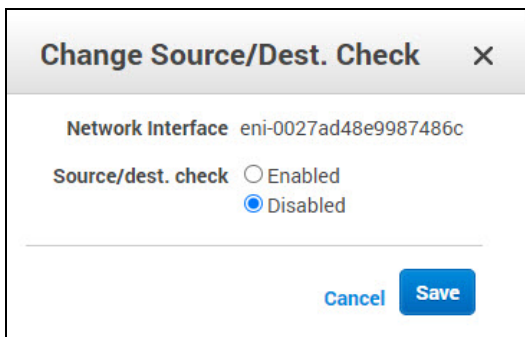
1. Navigate to the EC2 dashboard (at left) and then scroll down and click the **Network Interfaces** link.
2. Select the required Elastic Network Interface (ENI) and then click the **Actions** drop-down button and select **Change Source/Dest Check**, as shown below.

Figure 53 : Select the ENI



The selected Elastic Network Interfaces are displayed in a dialog box, as shown below.

Figure 54 : Change Source/Dest Checking (Disabled)



3. For the selected ENI, select the **Disabled** radio button for **Source/Destination Check**.

NOTE:

There are two elastic interfaces associated with this instance. A10 Networks recommends disabling the **Source/Destination Check** for both of them.

4. Click **Save** to save the changes.



AWS High Availability

Starting from ACOS 4.1.4-P2, configuring vThunder in High Availability (HA) mode is supported for AWS. HA is supported within the availability zone.

High availability refers to systems that are durable and likely to operate continuously without failure for a long time. vThunder already supports VRRP to make it highly available. It requires a minimum of two network nodes as VRRP creates one master (active) instance and at least one backup/ standby instance. VRRP-A determines the Active or Standby status based on received weight priority information. When an active vThunder instance has fail-over, then VRRP-A determines the Active or Standby status based on received weight information. The AWS cloud's elastic IP address (EIP) is mapped to the secondary IP address (VIP) of the data interface. During fail-over, the EIP and the VIP move from the active vThunder instance to the standby vThunder instance, making it the new active instance.

Configuring vThunder for HA in an AWS environment requires access to the [AWS Access Key ID and Secret Access Key](#).

The following topics are covered:

AWS Access Key ID and Secret Access Key	60
Importing AWS Access Key and Secret Access Key	60
AWS HA Architecture	61
Configuring HA	63

AWS Access Key ID and Secret Access Key

The AWS Access Key ID and AWS Secret Access Key are special tokens that enable AWS to connect to a customer account by using a secure REST or Query protocol API.

Perform the following steps to locate the keys:

1. Log in to your AWS Management Console.
2. Click on the user name at the top right of the page and then click the **Security Credentials** link from the drop-down menu.
3. In the **Access Credentials** section, copy the latest Access Key ID.
4. Click on the **Show** link and copy the Secret Access Key.
5. Save both of the keys in the following format in a file:

```
[default]
aws_access_key_id = <Access Key ID>
aws_secret_access_key = <access key>
```

Importing AWS Access Key and Secret Access Key

Each vThunder instance requires a copy of the AWS Access Key and AWS Secret Access Key. User with administrative privilege can perform the following steps:

1. Log into the vThunder instance.
2. Go to the config mode.

```
vThunder> enable
Password:
vThunder#config
```

3. Go to the admin mode.

```
vThunder(config)#admin ?
  admin
  NAME<length:1-31> System admin user name
vThunder(config)#admin admin
```


4. Import the AWS Access key by using any of the recommended file transfer methods.

```
vThunder (config-admin:admin) #aws-accesskey import ?
  use-mgmt-port  Use management port as source port
  tftp:          Remote file path of tftp: file system(Format:
tftp://host/file)
  ftp:          Remote file path of ftp: file system(Format: ftp://
[user@]host[:port]/file)
  scp:          Remote file path of scp: file system(Format: scp://
[user@]host/file)
  sftp:         Remote file path of sftp: file system(Format: sftp://
[user@]host/file)
```

For example

```
vThunder (config-admin:admin) #aws-accesskey import
scp://john@40.30.20.166:/home/john/credentials_latest
```

NOTE: To delete the AWS Access key, use the `aws-accesskey delete` command. This feature is available from ACOS 4.1.4-P3 release onwards.

AWS HA Architecture

High Availability for vThunder instances in AWS is supported only for the same availability zone. In a sample HA architecture, launch two vThunder instances in the same availability zone. Both the vThunder instances require at least one management interface and one data interface.

To achieve HA the following configurations are required:

- Ensure to select the re-assignment option while creating the secondary IP address so that the IP address can be directly assigned to a standby VM during fail-over without explicitly un-assigning it from the active vThunder.

NOTE: Inactive vThunder, a secondary IP address is for the client-facing data interface.

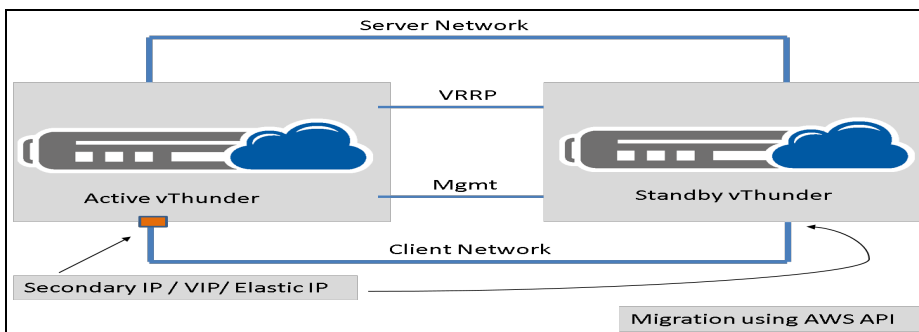
- Assign the elastic IP address to the management interface and to the secondary IP address assigned to the data interface (VIP). Also, assign the elastic IP address to the management IP address of the standby vThunder.
- Select the “Re-association” option, while associating an elastic IP address to the secondary interface to allow the association of the IP address even when it is already associated to some other VM.
- Additionally, each vThunder instance requires a copy of the AWS Access Key and AWS Secret Access Key. For more information, see [Importing AWS Access Key and Secret Access Key](#).

NOTE: In ACOS 5.2.1-P7 and later releases, the `ip control-apps-use-mgmt-port` command controls the outgoing interface for vThunder device API calls. If this command is enabled, API uses the management interface. Otherwise, it uses the data interface. In the previous releases, the outgoing interface used the route settings for API calls.

The following is an architectural representation of the HA architecture and how the migration happens from an active HA instance to a standby HA instance.

In [Figure 55](#), for the red box which is the data port of the active vThunder, there is also a secondary IP address assigned, and the EIP is mapped to the secondary IP address. The VIP is a logical name for these IP addresses.

Figure 55 : AWS HA Architecture



Configuring HA

The example discussed in this section uses two vThunders for HA. Each vThunder instance is configured to run a simple SLB configuration. Make appropriate changes in the steps if the vThunders are running a different configuration.

Perform the following steps:

1. Create two vThunders in a VPC.
Each vThunder must have one management interface and one or more data interfaces.
For more information, refer to [Launching vThunder on AWS](#).
2. Create a secondary IP address and assign it to the client-facing data interface on the active vThunder. Ensure that you select the **re-assignment** option.
To assign a secondary private IPv4 address to a network interface:
 - a. Open the Amazon console.
 - b. Select **Network Interfaces**, and then select the network interface attached to the instance and configured as the data interface.
 - c. Select **Actions > Manage IP Addresses**.
 - d. Under **IPv4 Addresses**, select **Assign new IP**.
 - e. Enter a specific IPv4 address which is within the subnet range for the instance.
 - f. Select **Allow reassignment**.
 - g. Select **Yes, Update**.
3. Assign an elastic IP (EIP) to the secondary network interface. Select the **Re-association** option.
To associate an elastic IP address with a secondary private IPv4 address:
 - a. Open the Amazon EC2 console.
 - b. In the navigation pane, select **Elastic IPs**.
 - c. Select **Actions > Associate address**.
 - d. Select the network interface, and then select the secondary IP address from

- the Private IP list.
- e. Select **Associate**.
4. Associate the Elastic IP address with both the management interfaces of the active and standby vThunders. To associate an elastic IP address with a secondary private IPv4 address:
 - a. Open the Amazon EC2 console.
 - b. In the navigation pane, select **Elastic IPs**.
 - c. Select **Actions > Associate address**.
 - d. Select the network interface, and then select the management IP address from the private IP list.
 - e. Select **Associate**.
 5. Complete the SLB configuration on both the vThunder instances. This configuration includes:
 - Creating a real server with L4 port and protocol defined.
 - Creating a service group with the already created virtual server as a member.
 - Create a virtual server referencing the service group with a VIP IP address defined. The VIP IP address is the secondary IP address created on the data interface.
 - Completing the VRRP configuration on both the vThunder instances to use unicast-based VRRP.

NOTE: For more information on the ACOS configuration of the vThunder instances, see [Sample ACOS Configuration for Active vThunder](#) and [Sample ACOS Configuration for Standby vThunder](#).

- Under admin user (admin XYZ), use the `aws-accesskey import <file path>` command to import the keys to each vThunder instance.

Sample ACOS Configuration for Active vThunder

The following is the consolidated ACOS configuration for the active vThunder with VRRP and SLB configured.

```
vrrp-a common
```

```
device-id 1
set-id 1
enable
!
interface ethernet 1
enable
ip address dhcp
!
vrrp-a vrid 0
floating-ip 10.0.2.229
!
vrrp-a peer-group
peer 10.0.2.41
peer 10.0.2.22
!
ip route 0.0.0.0 /0 10.0.1.1
!
slb server s1 10.0.2.230
health-check-disable
port 80 tcp
health-check-disable
!
slb service-group sg1 tcp
health-check-disable
member s1 80
!
slb virtual-server vip 10.0.2.228
port 80 http
source-nat auto
service-group sg1
```

Sample ACOS Configuration for Standby vThunder

The following is the consolidated ACOS configuration for the standby vThunder with VRRP and SLB configured.

```
vrrp-a common
device-id 2
set-id 1
enable
```

```
!  
interface ethernet 1  
  enable  
  ip address dhcp  
!  
vrrp-a vrid 0  
  floating-ip 10.0.2.229  
!  
vrrp-a peer-group  
  peer 10.0.2.41  
  peer 10.0.2.22  
!  
ip route 0.0.0.0 /0 10.0.1.1  
!  
slb server s1 10.0.2.230  
  health-check-disable  
  port 80 tcp  
  health-check-disable  
!  
slb service-group sg1 tcp  
  health-check-disable  
  member s1 80  
!  
slb virtual-server vip 10.0.2.228  
  port 80 http  
  source-nat auto  
  service-group sg
```

Initial vThunder Configuration

This section provides information about the initial vThunder configuration.

The following topics are covered:

About Licensing the vThunder Instance	68
Changing the Admin Password	68
Saving the Configuration Changes—Write Memory	68
Configuring vThunder on AWS as an SLB	69

About Licensing the vThunder Instance

A10 Networks offers different types of licenses for your vThunder instance. If you opted for a BYOL license, contact A10 Sales for more information.

The GLM is the master licensing system for A10 Networks. The GLM is managed by A10 Networks and is the primary portal to view licensing information, device status, and data usage for the ACOS devices. The GLM collects information from ACOS devices and issues licenses upon request. The GLM provides a GUI view and manages advanced licensing functions. Creating a GLM account is optional. Users can use the CLI to license the ACOS devices. However, a GLM account enables us to perform advanced licensing functions. The GLM GUI is available at <https://glm.a10networks.com>.

Changing the Admin Password

A10 Networks recommends changing the admin password immediately for security.

```
vThunder(config)# admin admin password newpassword  
vThunder(config)#
```

NOTE: The vThunder is now network accessible for configuration under the new IP address and admin password.

Saving the Configuration Changes—Write Memory

Configuration changes must be saved to system memory to take effect the next time the vThunder is powered on. Otherwise, the changes are lost if the vThunder virtual machine or its host machine is powered down.

To write the current configuration to system memory, run the following command:

```
vThunder(config)# write memory  
Building configuration...  
[OK]
```


Configuring vThunder on AWS as an SLB

The following image is a simple topological example of configuring vThunder on AWS as an SLB. In this example, the vThunder device is inserted directly between the gateway router and the real servers. Requests from clients for virtual server 10.0.10.100 are routed by the Layer 3 router to the vThunder device, which then selects a real server and sends the request to that server. The server reply passes back through the vThunder device to the client.

To configure the vThunder instance on AWS as an SLB, perform the following:

- [Creating the vThunder Instance](#)
- [Configuring the Interfaces](#)
- [Configuring the vThunder ACOS](#)

Creating the vThunder Instance

Follow the procedure in [Launching a vThunder Instance on AWS](#) to create the vThunder instance. While creating the instance, create three interfaces. Follow the procedure in [Step 3. Configure the Instance](#) to create the following three interfaces required for this SLB solution:

- eth0 is the management interface.
- eth1 and eth2 are the data interfaces connected to the real servers.

Configuring the Interfaces

Make sure all the interfaces are in different subnets. Make sure the primary interface (eth0) is in the public Internet-facing subnet for management.

To create each extra interface, click **Add Device**. For each interface, you can specify the primary IP address and a secondary IP address.

After the vThunder instance is created, you can now associate an elastic IP address to the vThunder instance. This is the IP address that is presented to the Internet by the SLB solution. Additionally, there is also the private IP address for the vThunder instance. In this example, this is 10.0.10.100. After assigning the elastic IP address,

you can associate the private IP address and the elastic IP address. For more information, see [Elastic IP Address](#).

Configuring the vThunder ACOS

Perform the following steps on the vThunder device by using the CLI.

1. Enable the interfaces that connect the real servers to the vThunder by performing the following commands:

```
ACOS(config)# interface ethernet 1
ACOS(config-if:ethernet:1)# enable
ACOS(config-if:ethernet:1)# ip address dhcp
ACOS(config-if:ethernet:1)# exit
ACOS(config)#
ACOS(config)# interface ethernet 2
ACOS(config-if:ethernet:2)# enable
ACOS(config-if:ethernet:2)# ip address dhcp
ACOS(config-if:ethernet:1)# exit
```

2. Configure the real servers and ports by performing the following commands:

```
ACOS(config)# slb server s1 10.0.20.2
ACOS(config-real server)# port 22 tcp
ACOS(config-real server-node port)# port 80 tcp
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
ACOS(config)#
ACOS(config)# slb server s2 10.0.20.3
ACOS(config-real server)# port 22 tcp
ACOS(config-real server-node port)# port 80 tcp
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
ACOS(config)#
```

3. Configure the service group and add the real servers by performing the following commands:

```
ACOS(config)# slb service-group sg-http tcp
ACOS(config-slb svc group)# health-check Check.txt
ACOS(config-slb svc group)# member s1 80
```

```
ACOS(config-slb svc group-member:80)# member s2 80
ACOS(config-slb svc group-member:80)# exit
ACOS(config-slb svc group)# exit
```

4. Configure the virtual server by performing the following commands:

```
ACOS(config)# slb virtual-server VIP-1 10.0.10.100
ACOS(config-slb vserver)# port 80 http
ACOS(config-slb vserver-vport)# source-nat auto
ACOS(config-slb vserver-vport)# service-group sg-http
ACOS(config-slb vserver-vport)# exit
ACOS(config-slb vserver)# exit
```

vThunder for AWS GovCloud

This section provides an overview of installing and configuring AWS GovCloud.

The following topics are covered:

Overview	73
Features	73
Running vThunder in GovCloud	73

Overview

According to the AWS website: “AWS GovCloud (US) is an AWS region designed to allow US government agencies at the federal, state and local level, along with contractors, educational institutions and other US customers to run sensitive workloads in the cloud by addressing their specific regulatory and compliance requirements. Beyond the assurance programs applicable to all AWS regions, the AWS GovCloud (US) region allows customers to adhere to U.S. International Traffic in Arms Regulations (ITAR) regulations, the Federal Risk and Authorization Management Program (FedRAMP) requirements and Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG) Levels 2 and 4.”

For more information about AWS GovCloud (US), see <https://aws.amazon.com/govcloud-us/faqs/>

vThunder for AWS GovCloud is an AMI that is available through AWS. Customers can use this AMI for load balancing traffic in the AWS GovCloud region. The vThunder for AWS GovCloud instance helps facilitate the collaboration of GovCloud (US) stakeholders at the federal, state, and local levels by increasing the speed and reliability of sensitive workloads in the cloud.

Features

The following are the features for AWS GovCloud:

- **Licensing** — vThunder for AWS GovCloud supports a BYOL licensing model. Unlike the AWS marketplace, GovCloud does not support an hourly rental model.
- **Supported ACOS Releases** — vThunder for AWS GovCloud is supported from ACOS 4.1.0-P3 onwards.
- **Supported Regions** — AWS GovCloud is only available for US government agencies.

Running vThunder in GovCloud

There are several steps involved in the process of running vThunder in the AWS GovCloud, listed as follows:

[Step 1. Launch the vThunder AMI](#)

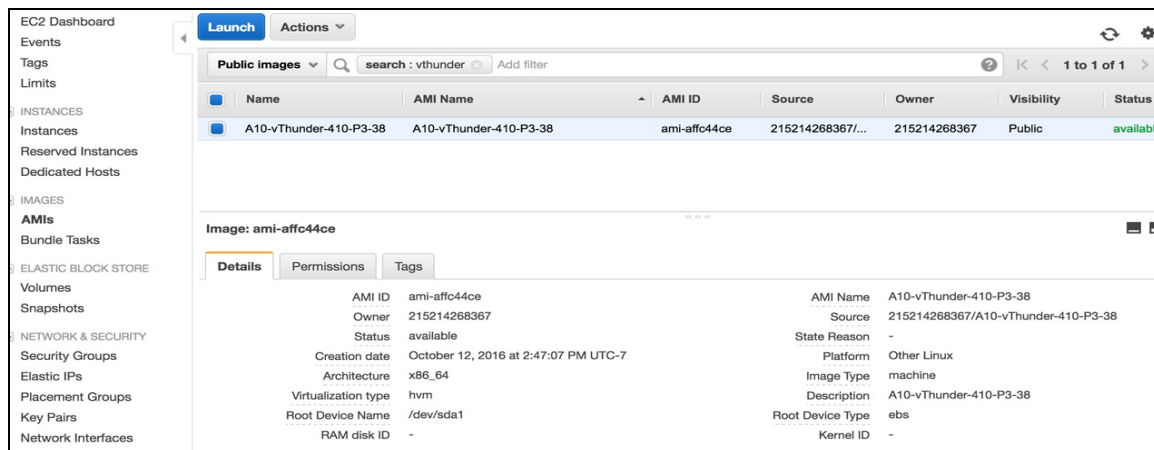
[Step 2. Apply for the vThunder BYOL license](#)

[Step 3. Configure the vThunder instance.](#)

Step 1. Launch the vThunder AMI

Launch the vThunder Amazon Machine Image (AMI), which is available as a public image from the EC2 dashboard, as shown in [Figure 56](#).

Figure 56 : Search EC2 Dashboard for keywords: “vThunder AMI image”



Step 2. Apply for the vThunder BYOL license

Procure a vThunder BYOL license from the A10 Networks sales channel.

Step 3. Configure the vThunder instance.

The basic configuration for a vThunder instance is the same for AWS GovCloud as a regular vThunder instance. For more information about basic configurations, see [Monitoring and Configuring the vThunder Instance](#) and [Initial vThunder Configuration](#).

Advanced vThunder Configuration

This section describes advanced vThunder configuration for AWS.

The following topics are covered:

About Shared Polling Mode	76
About Jumbo Frames	79
Dynamic Interface Attachment and Detachment	80
Memory Support	82

About Shared Polling Mode

ACOS release 4.1.4-GR1-P1 and later only supports shared polling mode¹ for deployments having a total number of CPUs less than four. From ACOS release 5.2.0 onwards, this support is also provided for deployments having a total number of CPUs greater than four.

When shared polling mode is enabled, both I/O and data processing both are performed by all the vCPUs except the control CPU. If there is no I/O and data processing task in the queue, then the system automatically switches the CPU to idle mode to conserve CPU cycles.

NOTE: This mode is only preferred when performance or latency is not the key criterion for the success and the user wants to maximize host CPU utilization due to multiple VMs running on it.

Table 5 : ACOS Modes and Selection Criteria

Mode	Behavior	Criteria	Additional Requirements	Performance
Polling Mode	In polling mode, both I/O and Data threads continuously poll for the packet and process it. This mode always consumes 100% of the allotted CPU cycles.	High performance + low latency required, combined with SR-IOV.	Configure CPU pinning with NUMA.	High Performance

¹This support is available on BareMetal and vThunder on KVM, ESXi, Hyper V, AWS, Azure, and OpenStack.

Table 5 : ACOS Modes and Selection Criteria

Mode	Behavior	Criteria	Additional Requirements	Performance
	Note: System poll mode is default for more than 4 vCPUs.			
Shared Polling Mode	When the shared poll mode is enabled, I/O and data processing are both performed on all cores except the control CPU.	Maximum utilization of CPU resources with some compromise on latency and performance.	The host needs to share physical CPUs with multiple VMs.	Lower CPU cycles consumed by the host.

NOTE: The shared polling mode feature is supported for ACOS 5.2.0 and later versions.

Enabling Shared Polling Mode

By default, shared polling mode is disabled. The following procedure has to be followed to enable Shared Polling mode:

1. Use the following CLI command from global config mode:

```
vThunder(config)#system shared-poll-mode enable
```

2. Exit global config mode and reload the vThunder instance using the following command:

```
vThunder(config)#exit
vThunder#reload
```

After vThunder finishes reloading, Shared Polling Mode will be enabled.

- To verify Shared Polling Mode is enabled on the vThunder instance, check the output from the “show system shared-poll-mode” command.

```
vThunder(config)# show system shared-poll-mode
```

For example,

```
A2# show system shared-poll-mode
Shared poll mode is enabled
A2#
```

- CPU distribution can be viewed, with the “show cpu” command as shown below. From the output, it can be observed that no CPU does IO processing exclusively.

For example,

```
vThunder#show cpu
Time: Mar-2-2019, 01:39
          1Sec          5Sec          10Sec          30Sec
60Sec
-----
-----
Controll1      15%          15%          14%          18%
 18%
Data1          0%           0%           0%           0%
 0%
Data2          0%           0%           0%           0%
 0%
Data3          0%           0%           0%           0%
 0%
```

Disabling Shared Polling Mode

The following procedure is followed to disable Shared Polling mode:

- Use the following command from global config mode to **disable** shared polling mode:

For example:

```
vThunder(config)#system shared-poll-mode disable
```

2. Exit global config mode and reload the vThunder instance using the following command:

```
vThunder(config)#exit
vThunder#reload
```

After vThunder finishes reloading, Shared Polling Mode will be disabled.

3. CPU distribution can be viewed, when shared poll mode is disabled with the “show cpu” command as shown below. From the output, it can be observed that some CPUs are designated for IO processing.

For example:

```
vThunder(config)#show cpu
Time: Mar-2-2019, 01:37
          1Sec          5Sec          10Sec          30Sec
60Sec
-----
-----
Controll1      20%          21%          21%          21%
 21%
Data1          0%           0%           0%           0%
 0%
Data2          0%           0%           0%           0%
 0%
I/O1          0%           0%           0%           0%
```

NOTE: For one vCPU, the control and data usage are shown separately, but both share the same vCPU. The actual usage of the CPU is cumulative of control and data usage.

About Jumbo Frames

A jumbo frame is an Ethernet frame with a payload greater than the standard maximum transmission unit (MTU) of 1,500 bytes. This modification improves

vThunder throughput and performance. Additional advantages of enabling jumbo frames include reduced interrupts and lower RAM utilization. For vThunder, jumbo frames are supported on ACOS 2.7.x, 2.8.x, 4.x, 5.x versions, and non-FTA platforms.

The following is a list of limitations and requirements for running jumbo frames for the vThunder-Intel and ENA devices:

- The vThunder instance must be running on top of an Intel 10Gb Ethernet Controller.
- Jumbo frames are not supported on 1Gb NICs.
- Supported jumbo frame packet types include: ICMP, UDP, and TCP.
- vThunder can support jumbo frame packets up to a maximum size of 9216 bytes.

Enabling Jumbo Frames for vThunder

By default, jumbo frame support is disabled. Use the following appropriate CLI command to enable jumbo frame support on a vThunder data interface:

- For ACOS version 2.7.x: `enable-jumbo`
- For ACOS version 4.1.x: `system-jumbo-global enable-jumbo`

Set the MTU size on the vThunder data interface to a value ranging from 1500 to 9216 bytes. The configured value must be larger than any jumbo packet expected to arrive on that data interface. To disable Jumbo Frames, run the command `no system-jumbo-global enable-jumbo`.

Dynamic Interface Attachment and Detachment

In virtualization and cloud platforms, dynamic interface detection is required to make the vThunder deployment easier. ACOS supports interface attachment and detachment when the VM is running and does not require a reboot.

The following are supported:

- Attaching or detaching one or more interfaces at the same time.
- Dynamic interface attachment and detachment is only for data interfaces.

- No impact on the existing interface functionality.

Platforms Supported

Dynamic interface attachment is supported only on Openstack, AWS, and OCI platforms.

Known Issues or Limitations

- Hypervisor must support interface detachment.
- Management interface detachment is not supported.
- Users must clean the existing configuration of the detached interface.
- Detachment impacts ongoing data traffic on the network interface.
- Interface detachment must be followed by vThunder reload.
- There is a mapping between interface and pci-address. As the pci-addresses are sequential, if there are any gaps or holes, when the interfaces are added the pci-address gaps or holes are filled first.

Configuration

ACOS configuration supports the following:

- Remove and clean-up the information of the detached interface on vThunder.
- A reload of vThunder is required to make ACOS ready after the interface removal.

Attaching or Detaching Network Interface

To attach or detach a network interface, perform the following:

1. Select a VM that is in Running State.
2. Attach or detach a network interface from running vThunder using the hypervisor tool.
3. Run the following command to detect the attached or detached interface:

```
system probe-network-devices
```

4. Run the following command to reload vThunder:

```
reload
```

5. Run the following command to verify the newly added interface:

```
show interface brief
```

Memory Support

vThunder devices support 128 GB memory and provision the resources to satisfy the high number of users and their throughput in a virtualized environment.

Both NUMAs inside the compute host are used for provisioning the resources. Memory allocation is 64 GB from NUMA0 and 64 GB from NUMA1. This feature supports all platforms with 2 NUMA, 128 GB memory, and 35 virtual CPUs.

NOTE: The memory allocation limits change according to available memory.

Configuring vThunder on SLB or CGN

To configure vThunder and validate 128 GB memory support, perform the following:

1. Configure the vThunder on SLB or CGN.

For example

Configure vThunder with SLB as:

```
slb server s1 <Server-IP>
  port 80 tcp

slb server s2 <Server-IP>
  port 80 tcp

slb service-group sg1 tcp
  member s1 80
  member s2 80
```

```
slb virtual-server Platform-vip <VIP>
  port 80 tcp
  source-nat auto
  service-group sgl
```

Configure vThunder with CGN as:

```
interface ethernet {cli}
  enable
  ip address <Data1-IP> <net mask>
  ip nat inside

interface ethernet {srv}
  enable
  ip address <Data2-IP> 2xx.xxx.xxx.0
  ip nat outside

class-list cgn_test
  <cli_subnet> lsn-lid 1

cgnv6 lsn inside source class-list cgn_test

cgnv6 nat pool lsn-pool {pool} netmask /<net-mask>

cgnv6 lsn-lid 1
  source-nat-pool lsn-pool
```

2. Verify 128 GB memory support for each vThunder instance in terms of vCPUs and increased application resources such as fixed-NAT public IP addresses, private users count, etc, perform the following:
 - a. Launch the vThunder system with 128GB memory and 35 vCPUs ACOS image.
 - b. Verify the limits using `show system resource-usage` and `show cgnv6 resource-usage` command.

```
vThunder(NOLICENSE)#sh system resource-usage
Resource                                Current    Default    Minimum
Maximum
-----
```

Advanced vThunder Configuration

l4-session-count 201326592	12582912	12582912	3145728
nat-pool-addr-count 15000	10	10	10
class-list-ipv6-addr-count 1048576	524288	524288	524288
class-list-ac-entry-count 9216000	65536	65536	65536
auth-portal-html-file-size 120	20	20	4
auth-portal-image-file-size 80	6	6	1
max-aflex-file-size 256	32	32	16
aflex-table-entry-count 15728640	102400	102400	102400
max-aflex-authz-collection-number 4096	512	512	256
radius-table-size 12000000	12000000	12000000	2000000
monitored-entity-count 800288	32960	32960	32816
authz-policy-number 2000	128	128	32
ram-cache-memory-limit 27648	27648	27648	6912
ipsec-sa-number 30000	30000	30000	120

cg n resource-usage

```
vThunder#show cg n resource-usage
Resource                               Current   Default   Minimum
Maximum
-----
-----
lsn-nat-addr-count                     2048     2048     2048
20000
```



```

fixed-nat-ip-addr-count      20480      20480      20480
512000
fixed-nat-inside-user-count  256000    256000    256000
8000000
radius-table-size           8000000    8000000    2000000
8000000
vThunder#

```

- c. Configure the maximum fixed-NAT IPs and inside users per the default limits and verify that they can be achieved. The default value is 30720k.
- d. Change the system resource for L4 sessions and reach the count.

NOTE: The accumulative L4 session count should be lesser than the current value. Every value don't exceed the current configured value.

- e. Verify that the configured limits take effect only after reboot.

NOTE: For some of the parameter update, reboot is not required. For example

- auth-portal-html-file-size
- auth-portal-image-file-size
- max-aflex-file-size

- f. On reboot configure the Minimum - maximum number of fixed-NAT IPs and inside "User/RADIUS/IP-List" value between pre-defined range (Min-Max).
- g. Reboot or reload the system to view the updated value.

Configure Thunder Observability

The A10 Thunder Observability Agent is introduced to monitor A10 Thunder® Application Delivery Agent (ADC) performance metrics and syslogs.

There are two types of A10 Thunder Observability Agent available:

- [Internal Thunder Observability Agent \(iTOA\)](#)
- [External Thunder Observability Agent \(TOA\)](#)

NOTE: It is recommended to configure any one TOA at a time.

Internal Thunder Observability Agent (iTOA)

This is an in-built Python plugin within ACOS which is configured using ACOS Command Line Interface (CLI) or aXAPI.

You can use iTOA for the following:

- For ACOS v6.0.1 or later.
- For configuring vThunder using aXAPI or CLI to publish the 14 performance metrics on AWS CloudWatch directly from vThunder with outbound internet connectivity.
- For configuring vThunder using aXAPI or CLI to publish the syslogs on:
 - AWS CloudWatch directly from vThunder with outbound internet connectivity.
 - Azure Log Analytics Workspace directly from vThunder with outbound internet connectivity to access '*.microsoftonline.com' and '*.azure.com'.
 - VMware vRealize Log Insight (vRLI) which is accessible from vThunder.
- For managing the data collection, processing, aggregation, and publishing internally for configured L3V partitions.
- For supporting maximum 20 partitions per vThunder instance.
- For publishing metrics or logs every 1 minute.

To configure the Internal Thunder Observability Agent for a vThunder deployed on AWS, see [Internal Thunder Observability Agent](#).

External Thunder Observability Agent (TOA)

This external plugin can be installed on Linux, CentOS, and Ubuntu platforms as a Python Plugin installation package and Docker containerization.

You can use TOA:

- For any ACOS deployment platform.
- For any ACOS software version.
- For a Thunder with outbound internet connectivity restrictions.

In this case, TOA can have outbound internet connectivity. It can collect data from Thunder and then publish the metrics and syslogs on the cloud monitoring tool through internet.

To install the external Thunder Observability Agent on AWS, see [External Thunder Observability Agent](#).



©2023 A10 Networks, Inc. All rights reserved. A10 Networks, the A10 Networks logo, ACOS, A10 Thunder, Thunder TPS, A10 Harmony, SSLi and SSL Insight are trademarks or registered trademarks of A10 Networks, Inc. in the United States and other countries. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. For the full list of trademarks, visit: www.a10networks.com/company/legal/trademarks/.