

Barracuda Load Balancer ADC Deployment and Quick Start Guide for Amazon Web Services

<https://campus.barracuda.com/doc/41102122/>

Deprecation Notice: Barracuda Load Balancer ADC is no longer supported on AWS.

You can deploy the Barracuda Load Balancer ADC in a flat network (i.e., your management IP address and VIP address both reside in the same network) on Amazon Web Services (AWS). Complete the steps in this guide to configure, launch, and license your Barracuda Load Balancer ADC instance. Then log into the Barracuda Load Balancer ADC to verify your configuration and change your password before you start creating services.

Requirements

Before you deploy the Barracuda Load Balance ADC on Amazon Web Services, ensure that you have completed the following:

- [Set up an Amazon Virtual Private Cloud \(VPC\)](#) for the Barracuda Load Balancer ADC.
- If you want to use the Bring Your Own Licensing (BYOL) model, get the Barracuda Load Balancer ADC license. See [Bring Your Own License \(BYOL\)](#).

Step 1. Create a Security Group

Create a security group with rules that specify the protocols, ports, and source IP ranges permitted to reach the instance. Multiple security groups can be created with different rules and assigned to each instance. For more information on security groups, refer to the AWS article [Amazon EC2 Security Groups](#).

1. Log into the [Amazon EC2 Management Console](#).
2. From the EC2 dashboard, select **Security Groups** under **NETWORK & SECURITY**.
3. Click **Create Security Group**.
4. In the **Create Security Group** window, do the following:
 1. **Security group name:** Enter a name to identify the security group.
 2. **Description:** Specify the description for the security group.
 3. **VPC:** Select a **VPC ID** from the list.
5. Under **Security group rules**, specify the inbound and outbound traffic to be allowed for the instance.

1. Add ports 8000 and 443 in the inbound rule of the security group associated with the Barracuda Load Balancer ADC.

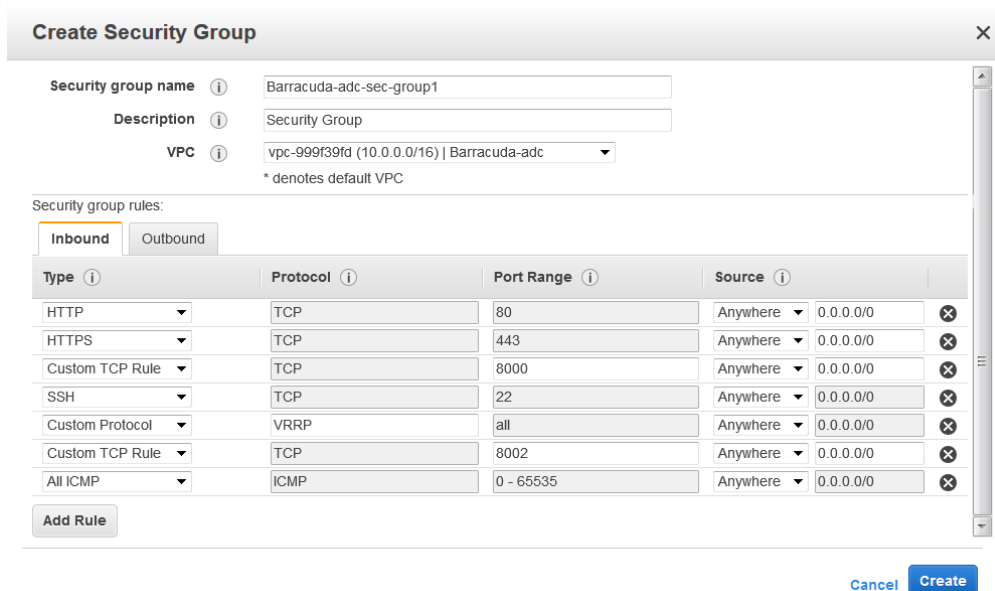
By default, the Barracuda Load Balancer ADC web interface listens on port 8000 for HTTP and port 443 for HTTPS.

If the instances are in cluster, add port 8002 (TCP) and port ALL for VRRP as inbound rule in the security group to synchronize the configuration between them.

2. Add inbound rules to open the ports through which you configure the services on this instance.

Layer 4 services on the Barracuda Load Balancer ADC require all ports to be open for Inbound rules, so you must open all ports if you are configuring any Layer 4 services on the Barracuda Load Balancer ADC.

3. Add an outbound rule to ensure that all ports are open irrespective of the service type:
 - TYPE: All Traffic
 - Protocol: All
 - Port Range: All
 - Destination: 0.0.0.0/0
4. If you are configuring Layer 4 services, add an inbound rule to ensure that all ports are open:
 - TYPE: All Traffic
 - Protocol: All
 - Port Range: All
 - Source: 0.0.0.0/0
5. After adding the inbound and outbound rules, click **Create**.



Create Security Group

Security group name: Barracuda-adc-sec-group1

Description: Security Group

VPC: vpc-999f39fd (10.0.0.0/16) | Barracuda-adc

* denotes default VPC

Security group rules:

Inbound | Outbound

Type	Protocol	Port Range	Source	
HTTP	TCP	80	Anywhere 0.0.0.0/0	✕
HTTPS	TCP	443	Anywhere 0.0.0.0/0	✕
Custom TCP Rule	TCP	8000	Anywhere 0.0.0.0/0	✕
SSH	TCP	22	Anywhere 0.0.0.0/0	✕
Custom Protocol	VRRP	all	Anywhere 0.0.0.0/0	✕
Custom TCP Rule	TCP	8002	Anywhere 0.0.0.0/0	✕
All ICMP	ICMP	0 - 65535	Anywhere 0.0.0.0/0	✕

Add Rule

Cancel Create

6. The created group appears in the security group table.

Step 2. Create a Network Interface

Create a minimum of two network interfaces (one for MGMT access and the other for creating services). Ensure that you create the network interfaces in the subnet where you want to deploy the Barracuda Load Balancer ADC. The number of interfaces that can be attached to the Barracuda Load Balancer ADC depends on the instance type that you selected on Amazon Web Services. For information about instance types, see [Licensing Options and Models](#).

1. Log into the [Amazon EC2 Management Console](#).
2. From the EC2 dashboard, select **Network Interfaces** under **NETWORK & SECURITY**.
3. Click **Create Network Interface**.
4. In the **Create Network Interface** window, provide the following information for the network interface:
 - **Description** – Enter a name for the interface.
 - **Subnet** – Select the subnet of the VPC where you want to create the instance.
 - **Private IP** – It is recommended that you enter a static primary private IP address.
 - **Security Groups** – Select the security group that you created.
5. Click **Yes, Create**.

Step 3. Disable Source/Dest. check

You must also disable the **Source/Dest. check** in the interfaces that you created for the Barracuda Load Balancer ADC instance and configured servers. When this check is enabled, it breaks the Layer 4 services.

1. Log into the [AWS EC2 Management Console](#).
2. From the EC2 dashboard, select **Network Interfaces** under **NETWORK & SECURITY**.
3. Right click the interface and select **Change Source/Dest. Check**.
4. In the **Change Source/Dest. Check** window, set **Source/dest. check** to **Disabled** and then click **Save**.

Step 4. (Optional) Assign Multiple Private IP Address(es) to the Network Interface of the Instance

Depending on the Barracuda Load Balancer ADC instance type, you can add multiple secondary IP addresses on the interfaces that are used to create services on the Barracuda Load Balancer ADC. Do not add secondary IP addresses on the interface that is used for management access of the Barracuda Load Balancer ADC. For more information on multiple IP addresses, refer to the Amazon EC2 article [Multiple IP Addresses](#).

To assign a secondary private IP address:

1. Log into the [Amazon EC2 Management Console](#).
2. From the EC2 dashboard, select **Network Interfaces** under **NETWORK & SECURITY**.
3. Identify the interface needing a secondary private IP address assignment, and right-click the network interface attached to the instance.
4. Select **Manage Private IP Addresses**.
5. In the **Manage Private IP Addresses** window:
 1. Click **Assign a secondary private address**.
 2. In the **Address** field, enter an IP address that is within the subnet range for the instance. It is recommended that you use the static IP address instead of auto-assign.
 3. (Optional) To allow the secondary private IP address to be reassigned if it is already assigned to another network interface, select **Allow reassignment**.
 4. Click **Yes, Update**.
6. Click **Close**.

Step 5. Deploy the Barracuda Load Balancer ADC on Amazon Web Services

In the Amazon VPC that you configured, launch an Amazon EC2 instance with the Barracuda Load Balancer ADC AMI image. The **Amazon Launch Instance** wizard guides you through the following steps:

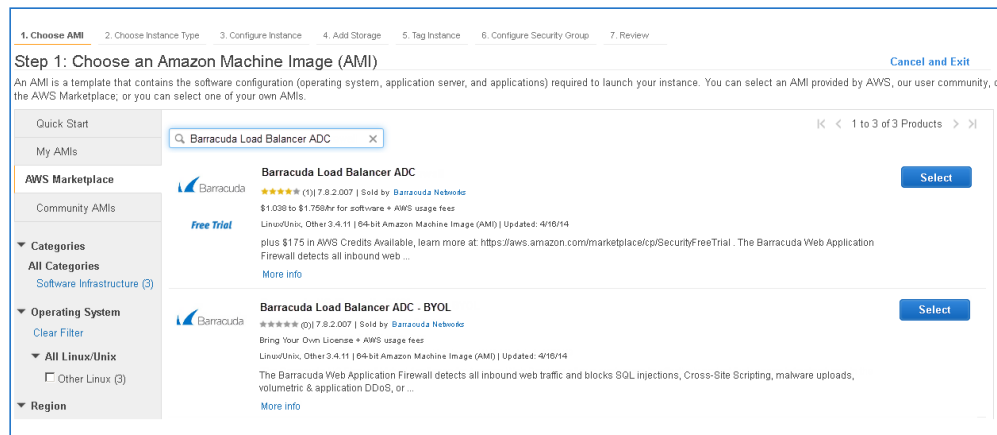
1. Log into the AWS Management Console and open the [EC2 Management Console](#).
2. In the top right corner of the page, select the region for the instance. This is important because some Amazon EC2 resources can be shared between regions.



3. Click **Launch Instance**.

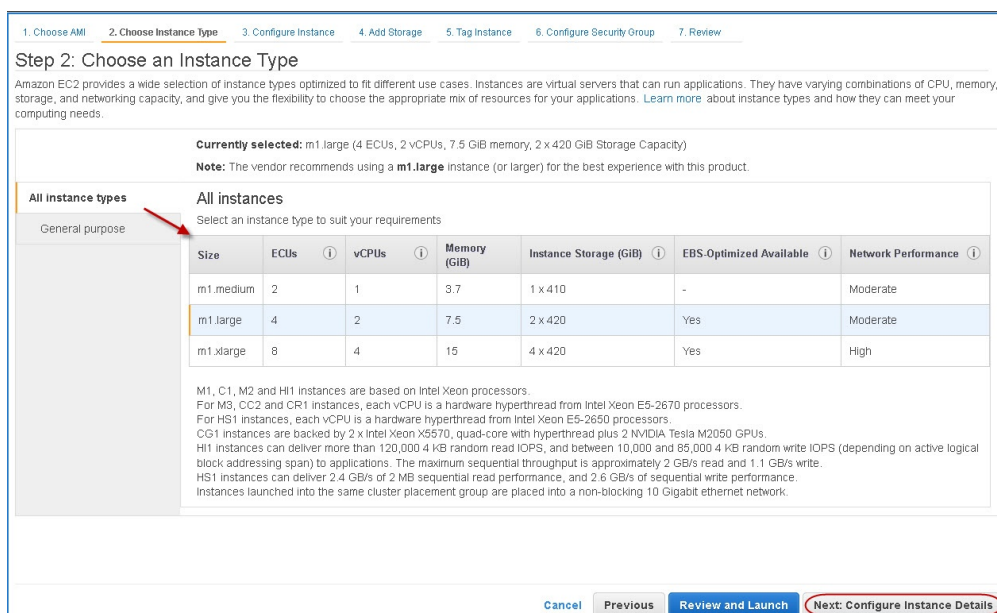


4. On the **Step 1: Choose an Amazon Machine Image (AMI)** page, select **AWS Marketplace** and then search for and select the **Barracuda Load Balancer ADC** AMI.



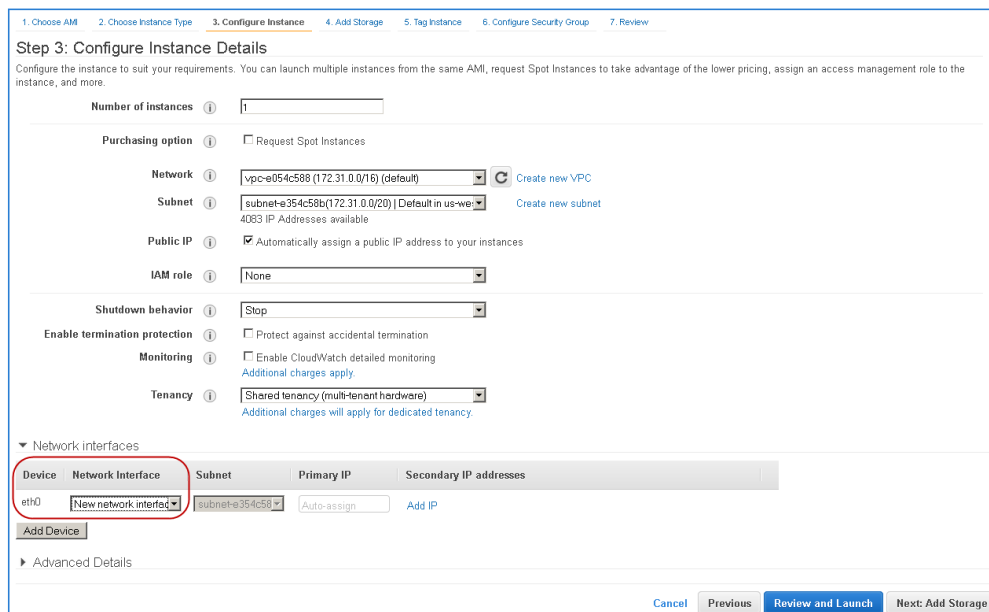
5. On the **Step 2: Choose an Instance Type** page, select an instance type from the **All Instance types** or **General purpose** table and then click **Next: Configure Instance Details** to continue.

See [Licensing Options](#) to verify the recommended instance type for your Barracuda Load Balancer ADC model. Select the recommended instance type.



6. On the **Step 3: Configure Instance Details** page:
1. Enter the **Number of instances** you want to launch.

2. Select the appropriate **Network** in which you want to deploy the instance.
3. Select the Subnet of the VPC where you want to create the instance.
4. In the **Network Interface** section:
 1. Select the network interface for Management access of the Barracuda Load Balancer ADC.
 2. Click **Add Device** and select the network interface for creating services on the Barracuda Load Balancer ADC.
5. In the **Advanced Details** pane, keep the default setting for all parameters and then click **Next: Add Storage**.



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 1

Purchasing option ☐ Request Spot Instances

Network vpc-e054c588 (172.31.0.0/16) (default) [Create new VPC](#)

Subnet subnet-e354c58b (172.31.0.0/20) (Default in us-we) [Create new subnet](#)
4093 IP Addresses available

Public IP ☒ Automatically assign a public IP address to your instances

IAM role None

Shutdown behavior Stop

Enable termination protection ☐ Protect against accidental termination

Monitoring ☐ Enable CloudWatch detailed monitoring
[Additional charges apply](#)

Tenancy Shared tenancy (multi-tenant hardware)
[Additional charges will apply for dedicated tenancy](#)

Network interfaces

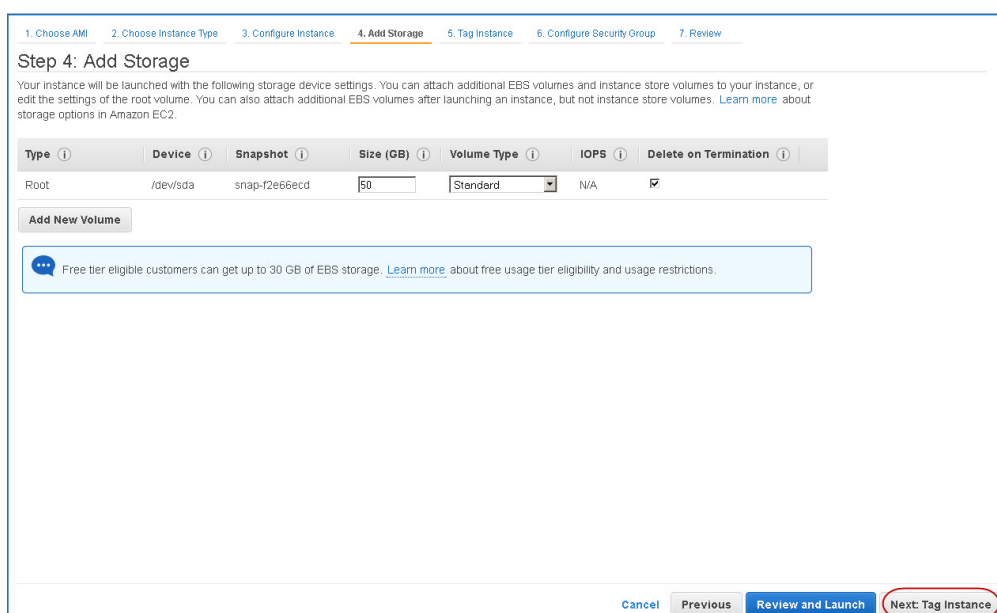
Device	Network Interface	Subnet	Primary IP	Secondary IP addresses
eth0	New network interface	subnet-e354c58b	Auto-assign	Add IP

[Add Device](#)

[Advanced Details](#)

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

7. On the **Step 4: Add Storage** page, review the storage device settings for the instance. Modify the values if required, and then click **Next: Tag Instance**.



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.

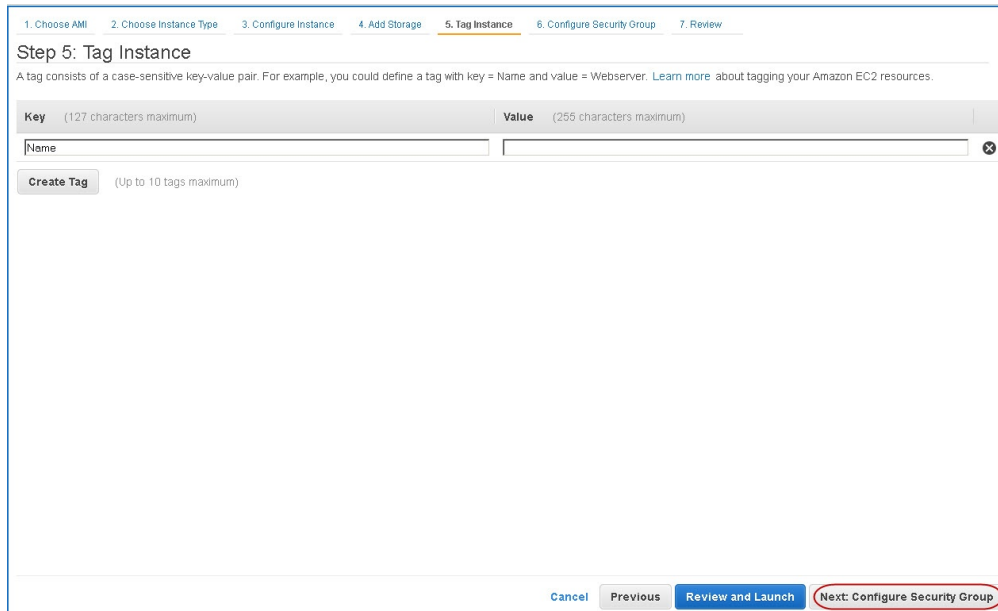
Type	Device	Snapshot	Size (GB)	Volume Type	IOPS	Delete on Termination
Root	/dev/sda	snap-f2e66ecd	50	Standard	N/A	<input checked="" type="checkbox"/>

[Add New Volume](#)

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

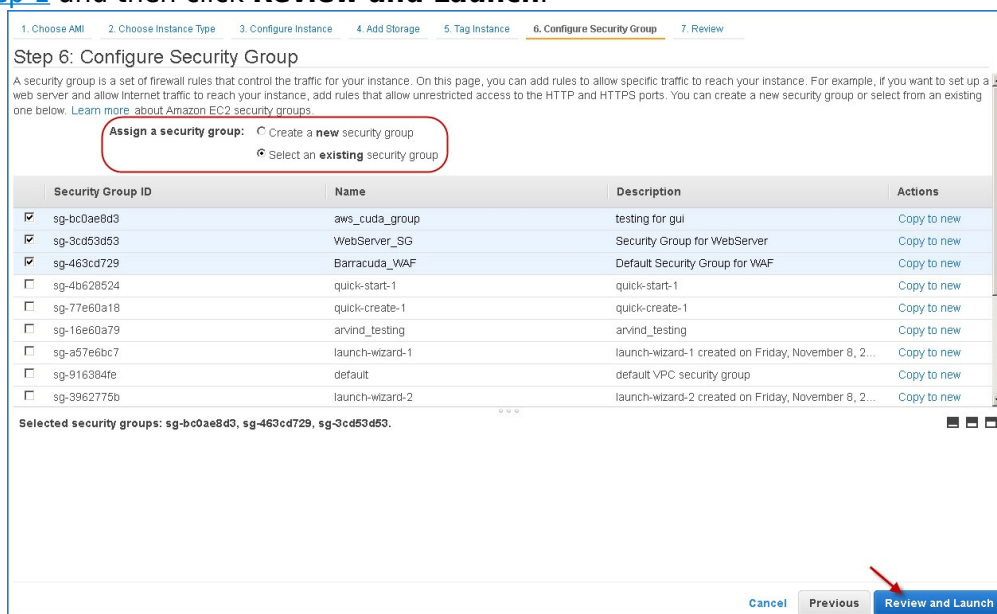
[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Tag Instance](#)

8. On the **Step 5: Tag Instance** page, add/remove the tags for the instance (if required) and then click **Next: Configure Security Group**.



The screenshot shows the 'Step 5: Tag Instance' page in the AWS Management Console. The page has a progress bar at the top with steps: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Tag Instance (active), 6. Configure Security Group, and 7. Review. Below the progress bar, there's a heading 'Step 5: Tag Instance' and a subheading 'A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. Learn more about tagging your Amazon EC2 resources.' There are two input fields: 'Key' (127 characters maximum) and 'Value' (255 characters maximum). Below these fields is a 'Create Tag' button and a note '(Up to 10 tags maximum)'. At the bottom right, there are four buttons: 'Cancel', 'Previous', 'Review and Launch', and 'Next: Configure Security Group' (highlighted with a red circle).

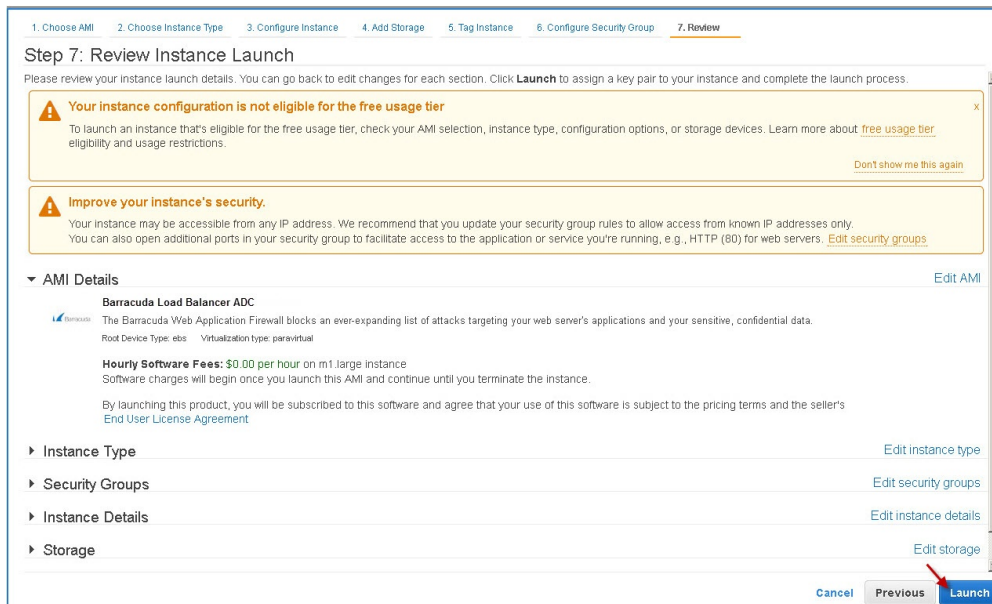
9. On the **Step 6: Configure Security Group** page, select the security groups that you created in [Step 1](#) and then click **Review and Launch**.



The screenshot shows the 'Step 6: Configure Security Group' page in the AWS Management Console. The page has a progress bar at the top with steps: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Tag Instance, 6. Configure Security Group (active), and 7. Review. Below the progress bar, there's a heading 'Step 6: Configure Security Group' and a subheading 'A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.' There are two radio buttons: 'Assign a security group: Create a new security group' and 'Select an existing security group' (selected). Below these radio buttons is a table with columns: 'Security Group ID', 'Name', 'Description', and 'Actions'. The table lists several security groups, with the first three selected (checked). At the bottom, there's a section 'Selected security groups: sg-bc0ae8d3, sg-463cd729, sg-3cd53d53.' and a 'Review and Launch' button (highlighted with a red arrow).

Security Group ID	Name	Description	Actions
<input checked="" type="checkbox"/> sg-bc0ae8d3	aws_cuda_group	testing for gui	Copy to new
<input checked="" type="checkbox"/> sg-3cd53d53	WebServer_SG	Security Group for WebServer	Copy to new
<input checked="" type="checkbox"/> sg-463cd729	Barracuda_WAF	Default Security Group for WAF	Copy to new
<input type="checkbox"/> sg-4b628524	quick-start-1	quick-start-1	Copy to new
<input type="checkbox"/> sg-77e60a18	quick-create-1	quick-create-1	Copy to new
<input type="checkbox"/> sg-16e60a79	arvind_testing	arvind_testing	Copy to new
<input type="checkbox"/> sg-a57e6bc7	launch-wizard-1	launch-wizard-1 created on Friday, November 8, 2...	Copy to new
<input type="checkbox"/> sg-916384fe	default	default VPC security group	Copy to new
<input type="checkbox"/> sg-3962775b	launch-wizard-2	launch-wizard-2 created on Friday, November 8, 2...	Copy to new

10. On the **Step 7: Review Instance Launch** page, review your settings and then click **Launch**.



After you click **Launch**, Amazon Web Services begins provisioning the Barracuda Load Balancer ADC. Allow a few minutes for the Amazon Web Services Agent and the Barracuda Load Balancer ADC image to boot up.

DO NOT restart the Barracuda Load Balancer ADC while it is launching.

Step 6. Allocate and Assign an Elastic IP Address to your Instance

As multiple interfaces are assigned to the instance, the Barracuda Load Balancer ADC will not be accessible to the outside world via the Internet because the unit does not yet have a public IP address. To resolve this issue, assign a persistent public IP address to the instance using Elastic IP addressing. For more information, refer to the AWS article [Elastic IP Addresses](#).

The elastic IP address associated to the first interface (eth0) will be the management IP address for the Barracuda Load Balancer ADC, and the elastic IP address associated to the second interface (eth1) will be used to access the services created on the **Primary IP Address** of the interface on the Barracuda Load Balancer ADC. Interface eth1 will be displayed as ge-1-1 on the Barracuda Load Balancer ADC.

1. Log into the [Amazon EC2 Management Console](#).
2. From the EC2 dashboard, select **Elastic IPs** under **NETWORK & SECURITY**.
3. Click **Allocate New Address**.
4. Click **Allocate** to confirm and allocate a new IP address. A random public IP address is

generated and displayed in the **Allocate New Address** table.

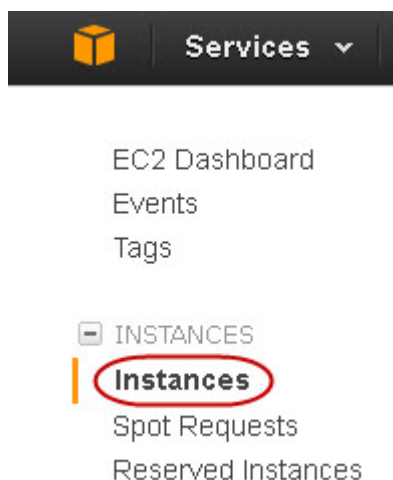
5. On the **Allocate New Address** page, right-click the new IP address and select **Associate**.
6. In the **Associate Address** window:
 1. Either select the **Instance** and the **Private IP Address** of the instance or select a **Network Interface** and the **Private IP Address**.
 2. Select the **Reassociation** check box.
7. Click **Associate**.
8. If you completed [Step 4. \(Optional\) Assign Multiple Private IP Address\(es\) to the Network Interface of the Instance](#) to assign multiple private IP address(es) to eth1 (which is displayed as ge-1-1 on the Barracuda Load Balancer ADC), repeat the steps above to assign the Elastic IP address to each internal IP address so that they can be reachable from the outside world via the Internet.

Step 7. (BYOL Only) License the Barracuda Load Balancer ADC

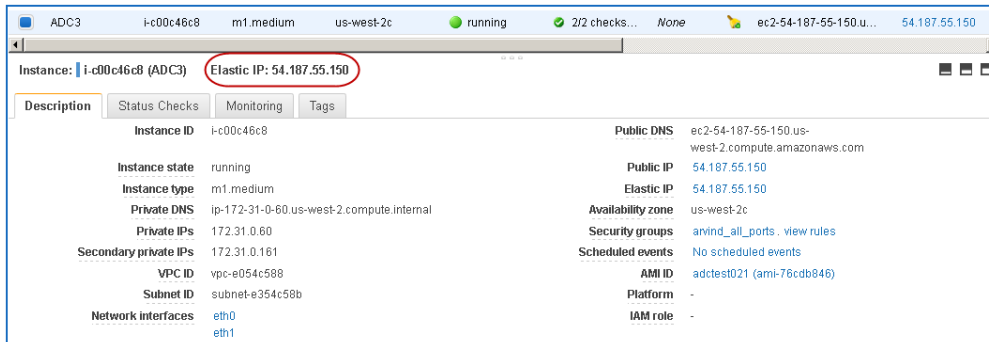
If you deployed the Barracuda Load Balancer ADC with the Hourly/Metered option, you do not need to license the system; skip ahead to [Step 8. Verify your Configuration and Change the Password](#).

If you deployed the Barracuda Load Balancer ADC with BYOL, complete the licensing and provisioning of your system.

1. Log into the [Amazon EC2 Management Console](#).
2. From the EC2 Dashboard, select **Instances** under **INSTANCES**.



3. In the **Instances** table, select the Barracuda Load Balancer ADC instance that you created and note the **Elastic IP** address associated with eth0.



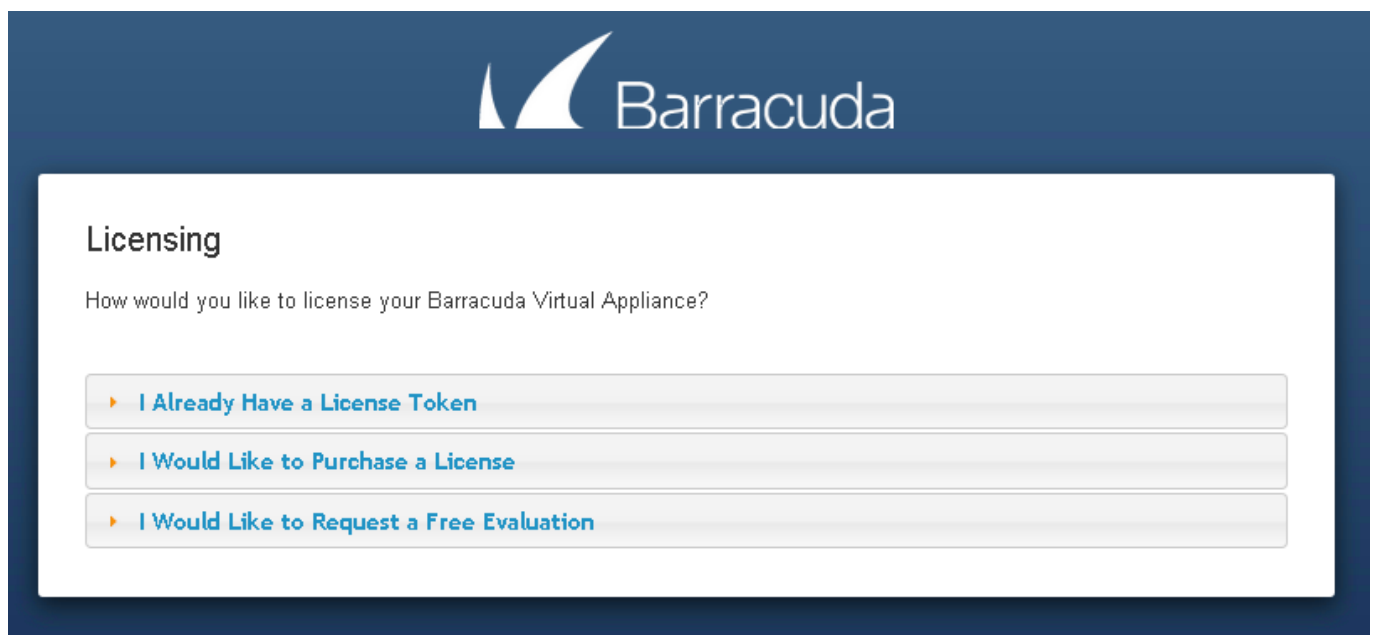
4. In a web browser, go to the Barracuda Load Balancer ADC web interface at the **Elastic IP** address that was assigned to eth0. Use port 8000 for HTTP. No port is required for HTTPS. For example:

- **For HTTP:** `http://<EIP>:8000`
- **For HTTPS:** `https://<EIP>`

The Barracuda Load Balancer ADC is not accessible via the HTTPS port while it is booting up. Use the HTTP port to access the unit while it is booting. This displays the status of the unit (i.e., System Booting). After the boot process completes, you are redirected to the login page.

5. On the **Licensing** page, enter your Barracuda Networks **Token** and **Default Domain** to complete licensing and then click **Provision**. The Barracuda Load Balancer ADC connects to the Barracuda Update Server to get the required information based on your license and then reboots automatically. Allow a few minutes for the reboot process.

After the boot process is complete, the **Licensing** page displays with the following options:



1. **I Already Have a License Token** – Use this option to provision your Barracuda Load

Balancer ADC with the license token you have already obtained from Barracuda Networks. Enter your Barracuda Networks **Token** and **Default Domain** to complete licensing, and then click **Provision**.

The Barracuda Load Balancer ADC connects to the Barracuda Update Server to get the required information based on your license, and then reboots automatically. Allow a few minutes for the reboot process. Once the instance is provisioned, you are redirected to the login page.

2. **I Would Like to Purchase a License** – Use this option to purchase the license token for the Barracuda Load Balancer ADC. Provide the required information in the form, accept the terms and conditions, and click **Purchase**.

The Barracuda Load Balancer ADC connects to the Barracuda Update Server to get the required information based on your license, and then reboots automatically. Allow a few minutes for the reboot process. Once the instance is provisioned, you are redirected to the login page.

3. **I Would Like to Request a Free Evaluation** – Use this option to get 30 days free evaluation of the Barracuda Load Balancer ADC. Provide the required information in the form, accept the terms and conditions, and click **Evaluate**.

The Barracuda Load Balancer ADC connects to the Barracuda Update Server to get the required information based on your license, and then reboots automatically. Allow a few minutes for the reboot process. Once the instance is provisioned, you are redirected to the login page.

Step 8. Verify your Configuration and Change the Password

1. In a web browser, go to the Barracuda Load Balancer ADC web interface at the Elastic IP address that was assigned to eth0. Use port 8000 for HTTP. No port is required for HTTPS. For example:
 - **For HTTP:** `http://<EIP>:8000`
 - **For HTTPS:** `https://<EIP>`
2. Log into as the administrator. Use the following credentials:
 - **Username:** `admin`
 - **Password:** The **Instance ID** of your Barracuda Load Balancer ADC in Amazon Web Services.
3. Go to the **BASIC > Administration** page and change your password.

Next Steps

Before you start configuring services on the Barracuda Load Balancer ADC, you can attach multiple interfaces to the Barracuda Load Balancer ADC, and bond those interfaces to increase the throughput of the Barracuda Load Balancer ADC. It is recommended that you create the link bond before you

configure your services because the Barracuda Load Balancer ADC cannot have any configurations when you create the link bond. For instructions, see [Creating a Link Bond on the Barracuda Load Balancer ADC for Amazon Web Services](#).

To start configuring your services in the Barracuda Load Balancer ADC, continue with [Configuring Services on the Barracuda Load Balancer ADC for Amazon Web Services](#).

If you need help troubleshooting any issues with your Barracuda Load Balancer ADC, see [Troubleshooting the Barracuda Load Balancer ADC on Amazon Web Services](#).

Figures

1. Security Group.png
2. region.jpg
3. launch_instance.jpg
4. Choose_ADC_AMI.png
5. instance_type.jpg
6. Config_instance_details.png
7. add_storage.jpg
8. tag_instance.jpg
9. security_group.jpg
10. review_instance_launch.jpg
11. step7_instances.jpg
12. Elastic_IP_Address.png
13. Licensing_ADC_Vx.PNG

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.