Clustering the Barracuda Load Balancer ADC Instances in the Same Availability Zone

https://campus.barracuda.com/doc/62652463/This article walks you through the steps to configure the Barracuda Load Balancer ADC instances for high availability in the same availability zone in Amazon Web Services.

Before you continue with the steps mentioned below, ensure that you have completed the configuration settings mentioned in the Clustering the Barracuda Load Balancer ADC Instances in Amazon Web Services article.

Step 1. Deploy Two Barracuda Load Balancer ADC Instances on Amazon Web Services

Follow the instructions mentioned in **Step 5. Deploy the Barracuda Load Balancer ADC on Amazon Web Services** in the Barracuda Load Balancer ADC Deployment and Quick Start Guide for Amazon Web Services article and deploy two Barracuda Load Balancer ADC instances in the same availability zone.

Ensure you select the IAM role created in **Create an IAM Role** when deploying the Barracuda Load Balancer ADC instances.

Step 2. Allocate and Assign an Elastic IP Address to Your Instance

Follow the instructions mentioned in **Step 6. Allocate and Assign an Elastic IP Address to your Instance** in the Barracuda Load Balancer ADC Deployment and Quick Start Guide for Amazon Web Services article to allocate the elastic IP address to the deployed Barracuda Load Balancer ADC instances

It is not required to assign the elastic IP address to the primary address of ge-1-1 and other subsequent interfaces, however, secondary private IP addresses of ge-1-1 and other subsequent interfaces must be assigned with an elastic IP address, so that the services can be accessed from the external network.

Step 3. License the Barracuda Load Balancer ADC

Follow the instructions mentioned in **Step 7. (BYOL Only) License the Barracuda Load Balancer ADC** in the Barracuda Load Balancer ADC Deployment and Quick Start Guide for Amazon Web Services to provision the deployed Barracuda Load Balancer ADC instances.

> This step is required only if you have deployed the BYOL model of the Barracuda Load Balancer ADC.

Step 4. Verify Your Configuration and Change the Password

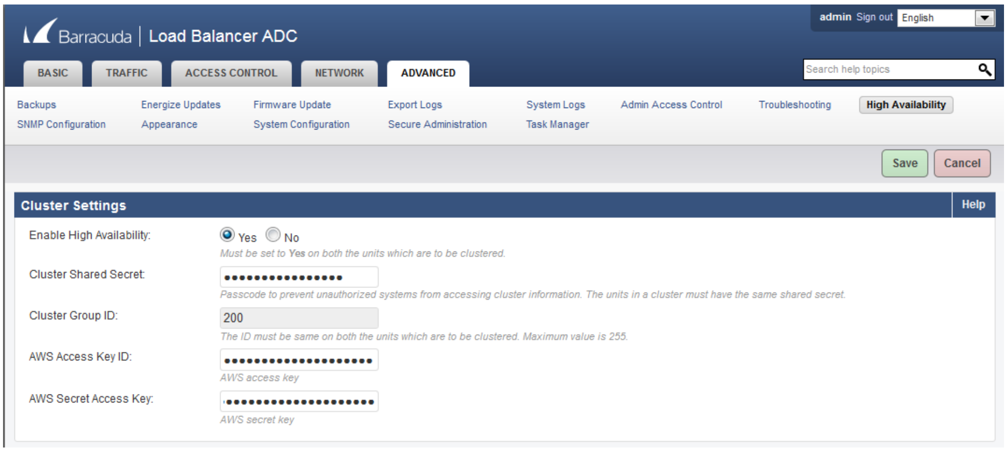
Follow the instructions mentioned in **Step 8. Verify your Configuration and Change the Password** in the Barracuda Load Balancer ADC Deployment and Quick Start Guide for Amazon Web Services article to verify your configuration and change the password on both of the deployed Barracuda Load Balancer ADC instances.

Step 5. Cluster the Deployed Barracuda Load Balancer ADC Instances

Follow the steps below to cluster your Barracuda Load Balancer ADC virtual machines in Amazon Web Services:

1. Log into the first Barracuda Load Balancer ADC web interface that will act as your Primary/Active unit. In the instructions below, consider this virtual machine as *Barracuda-LB-ADC1*.
2. In the *Barracuda-LB-ADC1* web interface, go to the **ADVANCED > High Availability** page and do the following configuration in the **Cluster Settings** section:
   1. Set **Enable High Availability** to *Yes*.
   2. Enter a **Cluster Shared Secret** password. This is the shared passcode that the clustered units use when communicating with one another. Both systems in the cluster must have the same shared secret.
   3. Enter the **Cluster Group ID**. The ID should be the same on both Barracuda Load Balancer ADC instances that are to be clustered. If, on the local network, other network components, such as firewalls, are clustered using VRRP, they should use a different **Cluster Group ID** than this one. Maximum value is 255.
   4. **AWS Access Key ID**: (Optional) Enter the access key ID created in Step 2: (Optional) Get the Access Keys for Your AWS Account.

   5. **AWS Secret Access Key**: (Optional) Enter the secret access key created in Step 2: (Optional) Get the Access Keys for Your AWS Account.
3. Click **Save**.



Cluster Settings

Enable High Availability: ● Yes ○ No
Must be set to Yes on both the units which are to be clustered.

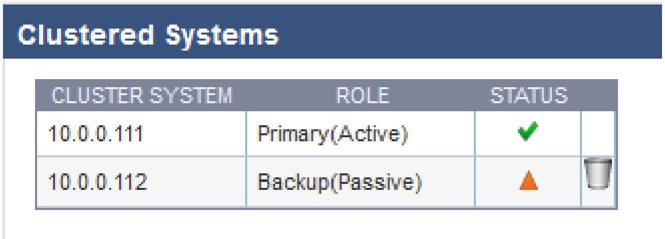
Cluster Shared Secret: ••••••••••••••••
Passcode to prevent unauthorized systems from accessing cluster information. The units in a cluster must have the same shared secret.

Cluster Group ID: 200
The ID must be same on both the units which are to be clustered. Maximum value is 255.

AWS Access Key ID: ••••••••••••••••••••
AWS access key

AWS Secret Access Key: ••••••••••••••••••••
AWS secret key

4. Log into the second Barracuda Load Balancer ADC web interface that will act as your Secondary/Backup unit. In the instructions below, consider this virtual machine as *Barracuda-LB-ADC2*.
5. In the *Barracuda-LB-ADC2* web interface, go to the **ADVANCED > High Availability** page and do the following configuration:
   1. Repeat step **2.a** to step **2.e** in the **Cluster Settings** section as mentioned in Step 7: Cluster the Deployed Barracuda Load Balancer ADC Instances.
   2. In the **Clustered Systems** section, enter the management IP address of the active Barracuda Load Balancer ADC and click **Join Cluster**.
   3. The clustering will run as a background task and take a few minutes to complete. Do not do any other configuration changes while the clustering task is running.
6. After a few minutes, refresh the **ADVANCED > High Availability** page on both systems and verify the following:
   1. Each system's management IP address appears in the **Clustered Systems** table.
   2. The status of the Primary (active) system should be .
   3. The status of the Backup (passive) system should be .



Clustered Systems

CLUSTER SYSTEM	ROLE	STATUS	
10.0.0.111	Primary(Active)	✓	
10.0.0.112	Backup(Passive)	▲	🗑

Continue with **Configuring Services on the Barracuda Load Balancer ADC in High Availability Environment**.

Step 6. Configure the Service(s) on the Barracuda Load Balancer ADC

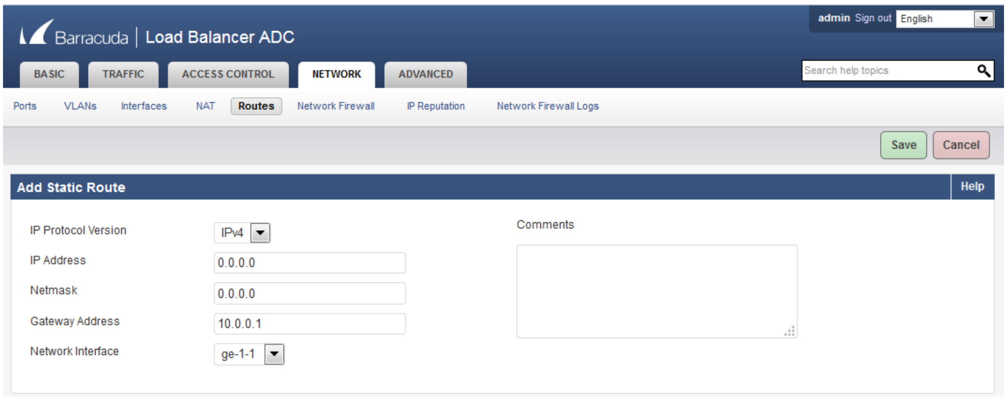
This section includes:

- Configuring the Service(s) on the Barracuda Load Balancer ADC Instance with Interfaces of the Same Subnet
- Configuring the Service(s) on the Barracuda Load Balancer ADC Instance with Interfaces from the Multiple Network

Configuring Services on the Barracuda Load Balancer ADC Instance with Interfaces of the Same Subnet.

If you have deployed the Barracuda Load Balancer ADC instance with two interfaces (i.e., mgmt (eth0) and ge-1-1 (eth1)) from the same network, create the service by following the steps mentioned below to reach the instance from the external network:

1. Log into the *Barracuda-LB-ADC1* (Primary/Active unit) web interface.
2. Go to the **BASIC > Services** page. Use the secondary private IP addresses assigned to the instance as your VIP to create services. See **Step.4 (Optional) Assign Multiple Private IP Address(es) to the Network Interface of Instance** in the Barracuda Load Balancer ADC Deployment and Quick Start Guide for Amazon Web Services article. For more information on how to add a service, click the **Help** button in the web interface.
3. Go to the **NETWORK > Routes** page.
4. In the **Add Static Route** section:
   1. **IP Protocol Version** - Select *IPv4*
   2. **IP Address** - Enter *0.0.0.0*.
   3. **Netmask** - Enter *0.0.0.0*.
   4. **Gateway Address** - Enter *10.0.0.1*.
   5. **Network Interface** - Select *ge-1-1*.
5. Click **Save**.



Add Static Route

IP Protocol Version	IPv4
IP Address	0.0.0.0
Netmask	0.0.0.0
Gateway Address	10.0.0.1
Network Interface	ge-1-1

Comments

All configuration should be done on the Primary/Active unit only, the configuration will be replicated to the Secondary/Backup unit automatically. As per the example above, the Primary unit is *Barracuda-LB-ADC1*, and the Secondary unit is *Barracuda-LB-ADC2*.

Configuring Services on the Barracuda Load Balancer ADC with Interfaces from Multiple Networks

> Skip this section if you have deployed the Barracuda Load Balancer ADC instance with two interfaces from the same network.

If you have deployed the Barracuda Load Balancer ADC instance with three interfaces, where two interfaces (i.e., mgmt (eth0) and ge-1-1 (eth1) are from the same network and the other interface (ge-1-2 (eth2)) is from a different network, you must assign secondary private IP address to each interface and then associate each secondary IP address with an elastic IP address, so that the instance can be accessed from the external network.

Perform the steps below to assign secondary private IP addresses and associate elastic IP address:

1. Follow step **1** and **2** mentioned in the Configuring Services on the Barracuda Load Balancer ADC Instance with Interfaces of the Same Subnet section.

   > If the service is configured using the primary private IP address, it will not failover in case of primary unit outage.
2. Go to the **NETWORK > Routes** page, and add a static route for ge-1-1 interface as mentioned below:
   1. **IP Protocol Version**: Select IPv4
   2. **IP Address**: Enter 0.0.0.0.
   3. **Netmask**: Enter 0.0.0.0.
   4. **Gateway Address**: Enter 10.0.0.1.
   5. **Network Interface**: Select ge-1-1.
3. Click **Save**.
4. Add a static route for ge-1-2 interface as mentioned below:
   1. **IP Protocol Version**: Select *IPv4*
   2. **IP Address**: Enter *0.0.0.0*.
   3. **Netmask**: Enter *0.0.0.0*.
   4. **Gateway Address**: Enter *10.0.1.1*.
   5. **Network Interface**: Select *ge-1-2*.
5. Click **Save**.

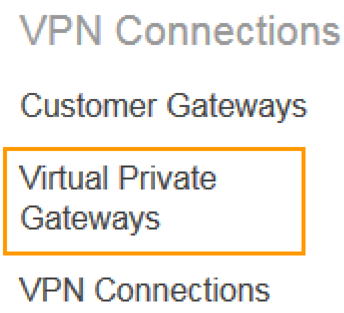
> All configuration should be done on the Primary/Active unit only; the configuration will be replicated to the Secondary/Backup unit automatically. As per the example above, the Primary unit is *Barracuda-LB-ADC1*, and the Secondary unit is *Barracuda-LB-ADC2*.

After creating services and adding routes to the Barracuda Load Balancer ADC instance that is deployed with interfaces from multiple networks, you must map the internet gateway in the routing table. See Map the Internet Gateway in the Routing Table.

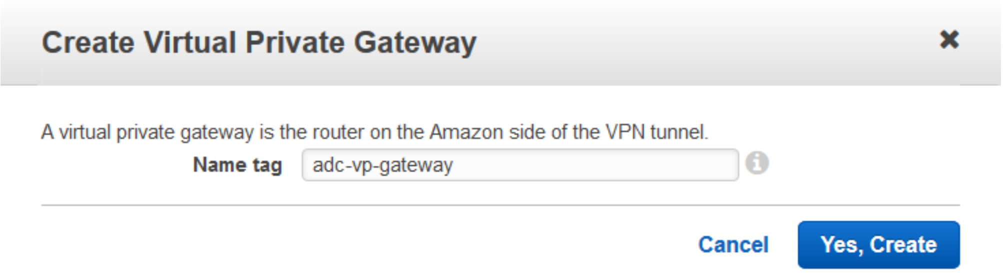
Map the Internet Gateway in the Routing Table

To transmit traffic through the ge-1-2 interface that is in a different subnet than that of the default public subnet, you should map the subnet to the internet gateway in the routing table, so that the subnet is reachable from the external network. Perform the following steps:

1. From the **VPC Dashboard**, select **Virtual Private Gateways** under **VPN Connections** in the left panel.



2. Click **Create Virtual Private Gateway**.
3. In the **Create Virtual Private Gateway** window, enter a name for the virtual private gateway in the **Name tag** field and click **Yes, Create**.

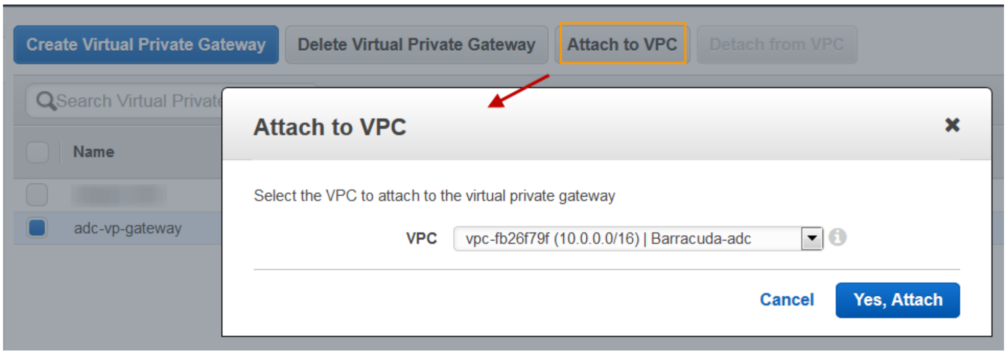


Create Virtual Private Gateway

A virtual private gateway is the router on the Amazon side of the VPN tunnel.

Name tag: adc-vp-gateway

4. Select the created virtual private gateway from the list, and click **Attach to VPC**.
5. In the **Attach to VPC** window, select the VPC to which you want to attach the virtual private gateway from the **VPC** list, and click **Yes, Attach**.



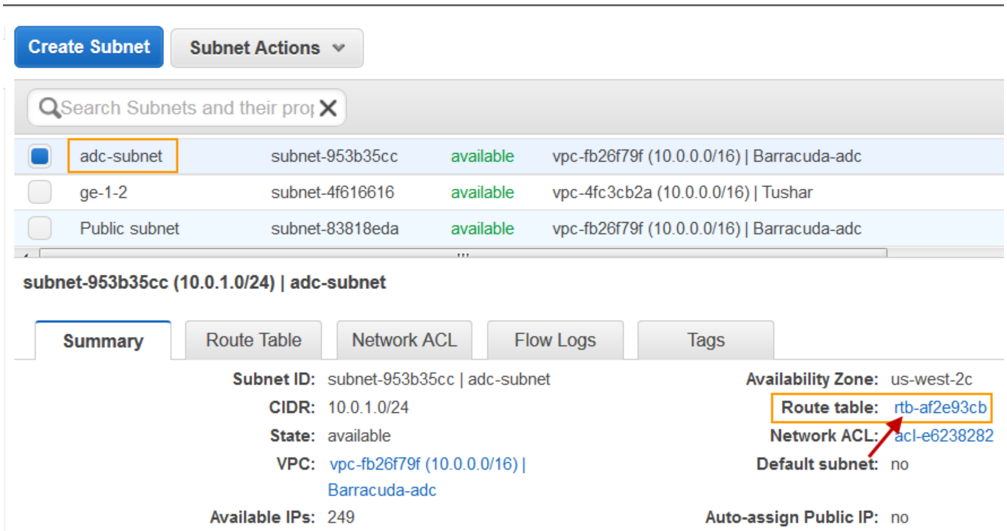
Attach to VPC

Select the VPC to attach to the virtual private gateway

VPC: vpc-fb26f79f (10.0.0.0/16) | Barracuda-adc

6. Select **Subnets** under **Virtual Private** in the left panel.

7. Select the subnet that is used for creating the ge-1-2 interface from the subnets list. Note the **Route table** entry under **Summary**.

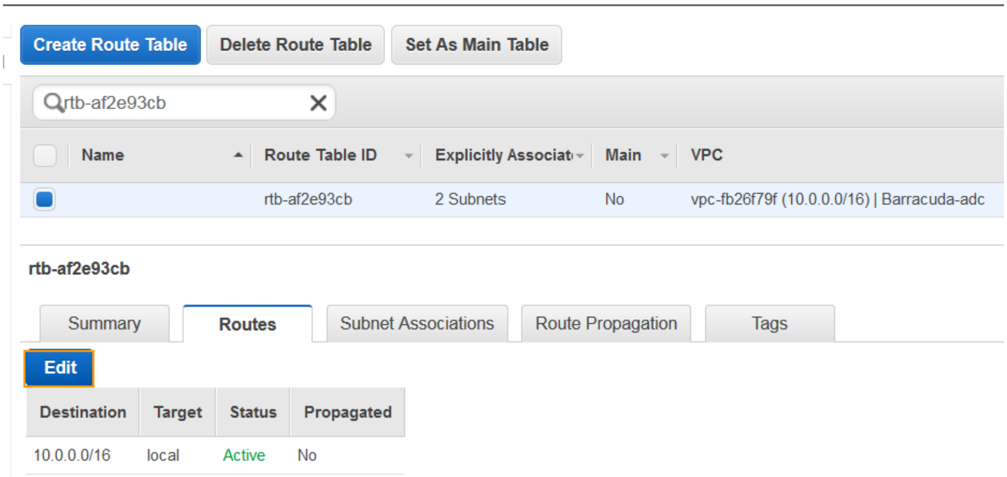


☑	adc-subnet	subnet-953b35cc	available	vpc-fb26f79f (10.0.0.0/16) | Barracuda-adc
☐	ge-1-2	subnet-4f616616	available	vpc-4fc3cb2a (10.0.0.0/16) | Tushar
☐	Public subnet	subnet-83818eda	available	vpc-fb26f79f (10.0.0.0/16) | Barracuda-adc

subnet-953b35cc (10.0.1.0/24) | adc-subnet

Subnet ID:	subnet-953b35cc | adc-subnet	Availability Zone:	us-west-2c
CIDR:	10.0.1.0/24	Route table:	rtb-af2e93cb
State:	available	Network ACL:	acl-e6238282
VPC:	vpc-fb26f79f (10.0.0.0/16) | Barracuda-adc	Default subnet:	no
Available IPs:	249	Auto-assign Public IP:	no

8. Select **Route Tables** under **Virtual Private Cloud** in the left panel.
9. Select the route you noted in step **7,** click on the **Routes** tab and click **Edit**.

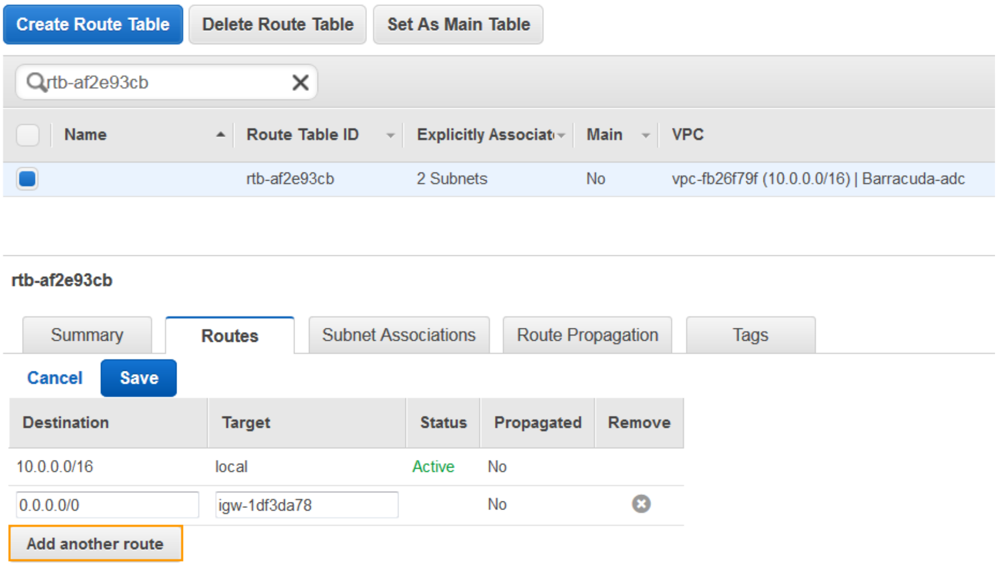


☐	Name	Route Table ID	Explicitly Associat	Main	VPC
☑		rtb-af2e93cb	2 Subnets	No	vpc-fb26f79f (10.0.0.0/16) | Barracuda-adc

rtb-af2e93cb

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

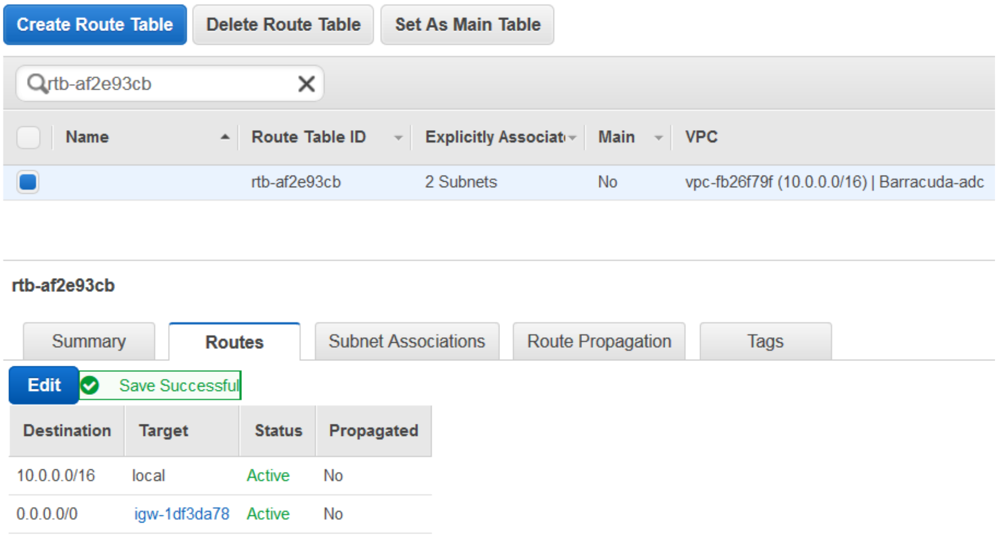
10. Click **Add another route** with Destination as **0.0.0.0** and Target as “**igw-1df3da78**”, which is the internet gateway. Click **Save**.



☐	Name	Route Table ID	Explicitly Associat	Main	VPC
■		rtb-af2e93cb	2 Subnets	No	vpc-fb26f79f (10.0.0.0/16) | Barracuda-adc

rtb-af2e93cb

Destination	Target	Status	Propagated	Remove
10.0.0.0/16	local	Active	No	
0.0.0.0/0	igw-1df3da78		No	⊗

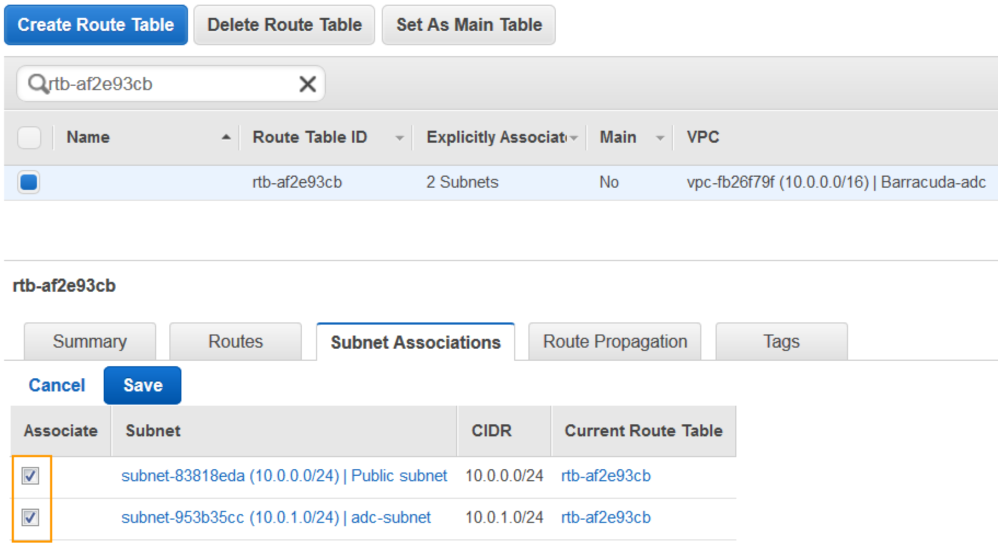


☐	Name	Route Table ID	Explicitly Associat	Main	VPC
■		rtb-af2e93cb	2 Subnets	No	vpc-fb26f79f (10.0.0.0/16) | Barracuda-adc

rtb-af2e93cb

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-1df3da78	Active	No

11. Select the **Subnet Associations** tab, and click **Edit**.
12. Ensure the **Associate** check box is selected for both the subnets, and click **Save**.

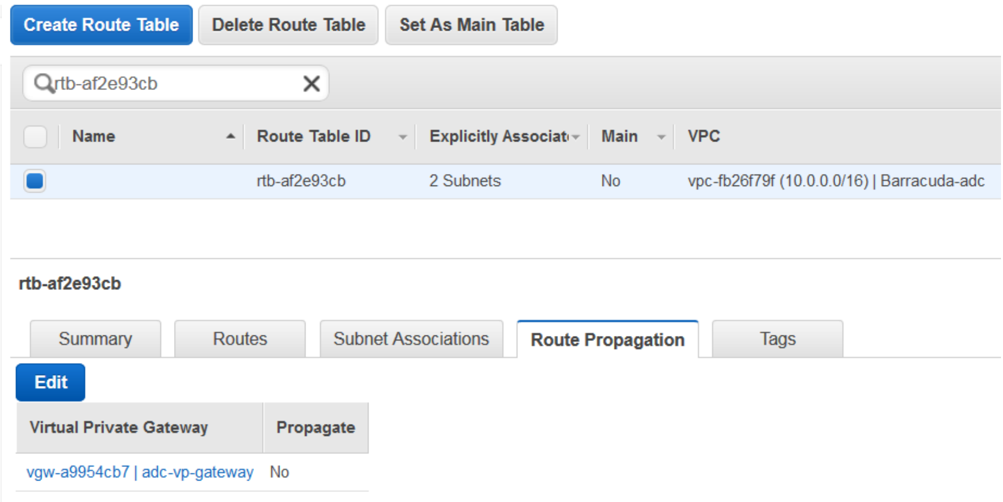


☐	Name	Route Table ID	Explicitly Associat	Main	VPC
■		rtb-af2e93cb	2 Subnets	No	vpc-fb26f79f (10.0.0.0/16) | Barracuda-adc

rtb-af2e93cb

Associate	Subnet	CIDR	Current Route Table
☑	subnet-83818eda (10.0.0.0/24) | Public subnet	10.0.0.0/24	rtb-af2e93cb
☑	subnet-953b35cc (10.0.1.0/24) | adc-subnet	10.0.1.0/24	rtb-af2e93cb

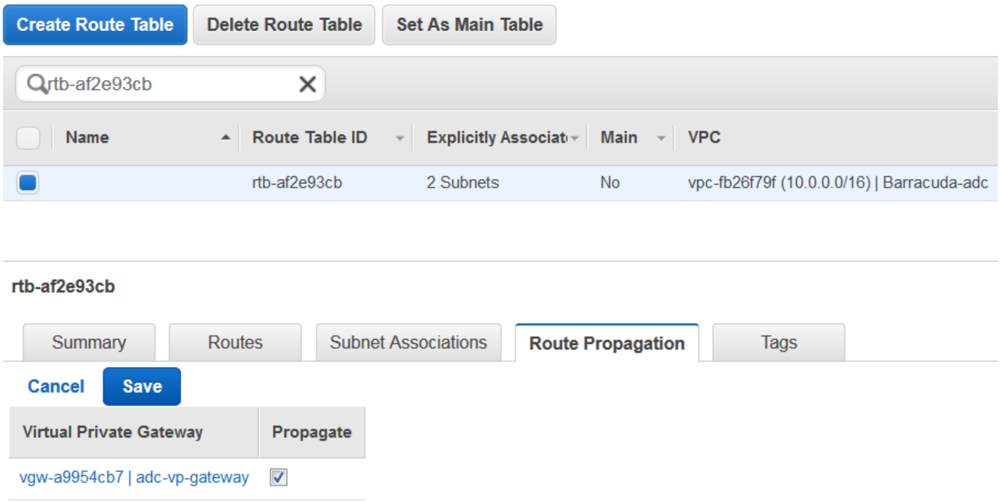
13. Select the **Route Propagation** tab, click **Edit,** and select the **Propagate** check box next to virtual private gateway. Click **Save**.



☐	Name	Route Table ID	Explicitly Associat	Main	VPC
■		rtb-af2e93cb	2 Subnets	No	vpc-fb26f79f (10.0.0.0/16) | Barracuda-adc

rtb-af2e93cb

Virtual Private Gateway	Propagate
vgw-a9954cb7 | adc-vp-gateway	No



☐	Name	Route Table ID	Explicitly Associat	Main	VPC
■		rtb-af2e93cb	2 Subnets	No	vpc-fb26f79f (10.0.0.0/16) | Barracuda-adc

rtb-af2e93cb

Virtual Private Gateway	Propagate
vgw-a9954cb7 | adc-vp-gateway	☑

Now, you can access the service from the external network using the elastic IP address assigned to the service virtual IP addresses.

Figures