Amazon Web Services VPC

Amazon AWS Installation Overview

This section describes how to set up an Amazon AWS Virtual Private Cloud (VPC) which will support either a single instance or a high availability (HA) pairing of SoftNAS Cloud instances using **SoftNAS SNAP HA™**. SoftNAS SNAP HA™ for EC2 now supports the use of Virtual IPs, and is our best practice recommendation. Configuration with Elastic IPs is still fully supported.

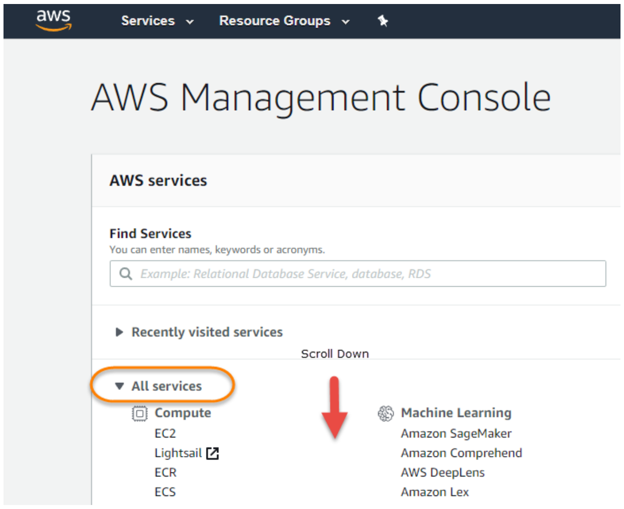
The following is required:

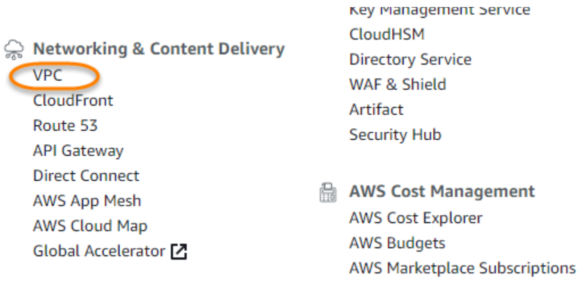
- Create the VPC in AWS.
- Specify the IAM User for SoftNAS Cloud®
- Create required subnets
- Configure the routing tables.
- Launch an Instance of **SoftNAS Cloud®** into the VPC.
- Create and Associate the Required Elastic or Virtual IPs.
- Set up **SoftNAS Cloud®** for HA.

Note: The HA IAM Role is caps sensitive, and must be named **SoftNAS_HA_IAM**.

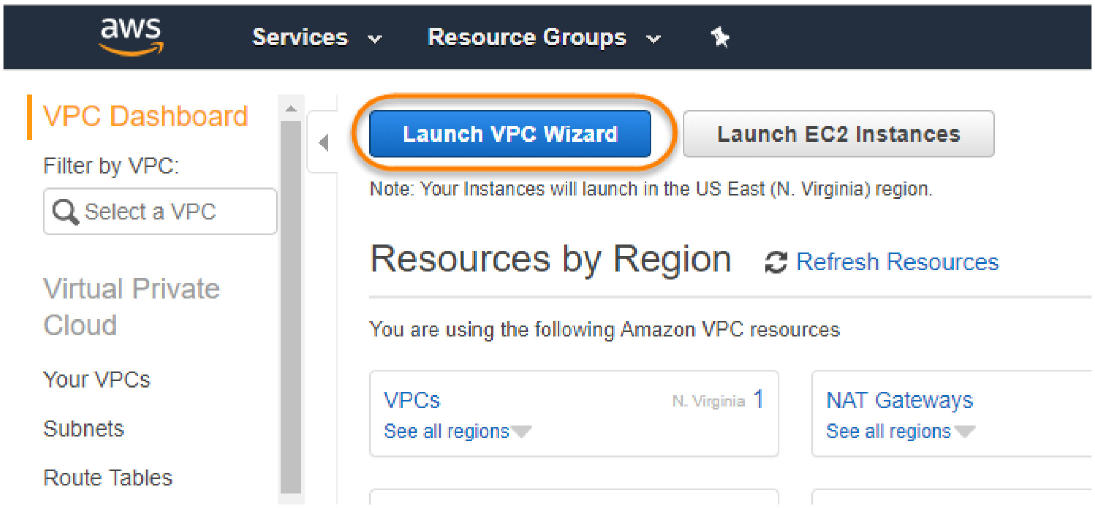
Creating the VPC

A VPC is a private, isolated section of the AWS cloud that can be set up in a variety of configurations. To create your VPC, log into the AWS console with your AWS credentials, and expand **All Services** (if not already open). Scroll down to **Networking and Content Delivery,** and select **VPC**.





From the VPC Dashboard, click on **Launch VPC Wizard.**

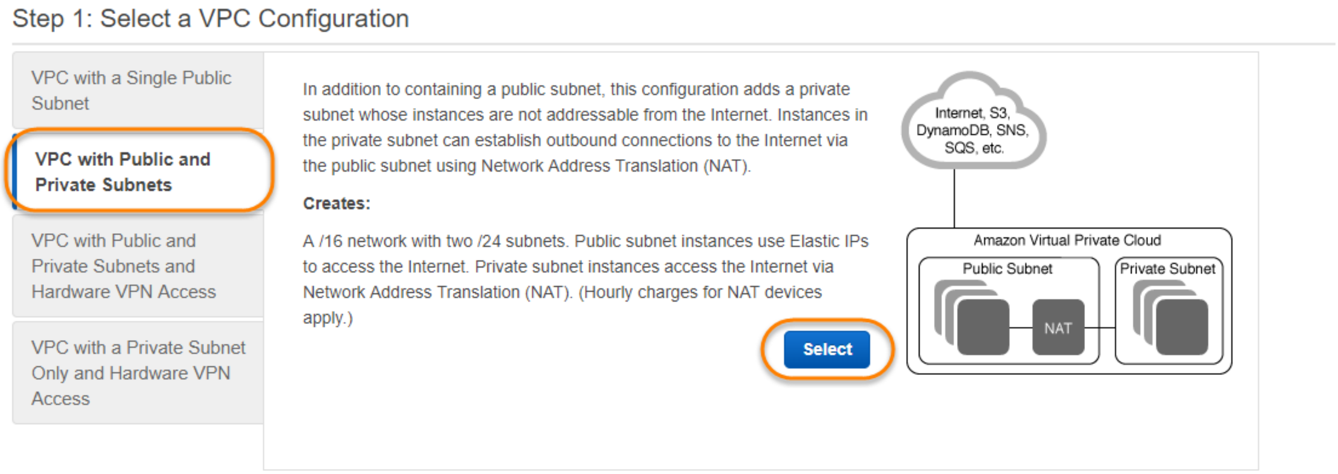


Note: Your Instances will launch in the US East (N. Virginia) region.

You are using the following Amazon VPC resources

Select **VPC with Public and Private Subnets** as the configuration scenario.

Click on **Select.** The **Create an Amazon Virtual Private Cloud** screen is displayed.


Step 1: Select a VPC Configuration
VPC with a Single Public Subnet
VPC with Public and Private Subnets
VPC with Public and Private Subnets and Hardware VPN Access
VPC with a Private Subnet Only and Hardware VPN Access
Select
Internet, S3, DynamoDB, SNS, SQS, etc.
Amazon Virtual Private Cloud
Public Subnet
Private Subnet
NAT

In addition to containing a public subnet, this configuration adds a private subnet whose instances are not addressable from the Internet. Instances in the private subnet can establish outbound connections to the Internet via the public subnet using Network Address Translation (NAT).

Creates:

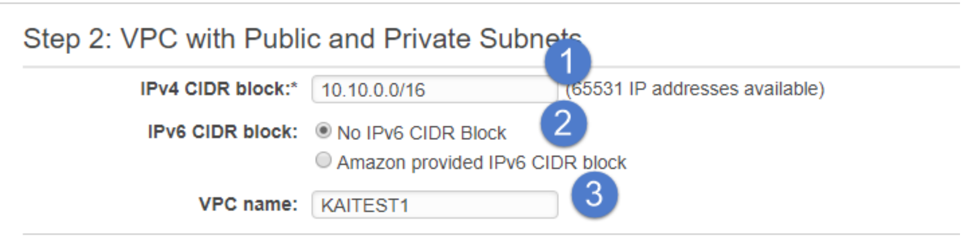
A /16 network with two /24 subnets. Public subnet instances use Elastic IPs to access the Internet. Private subnet instances access the Internet via Network Address Translation (NAT). (Hourly charges for NAT devices apply.)

Note: Private subnet instances access the Internet via a Network Address Translation (NAT) instance in the public subnet. (Hourly charges for NAT instances apply.)

Note: You may not require NAT setup if setting up a Private instance using Virtual IPs. While not required for Private instances, there are some organization specific instances where set up of NAT is relevant.

Configure the IP CIDR block, Public and Private Subnets, and all other settings as appropriate.

1. Provide a CIDR block for your VPC. The default can be kept, provided it does not conflict with other CIDR blocks within your organization. For this example, we will use 10.10.0.0/16.
2. **IPv6 CIDR block** can be kept at the default of '**No IPv6 CIDR block**' unless your use case necessitates an Amazon provided IPv6 CIDR block.
3. Provide an easily recognized VPC name.



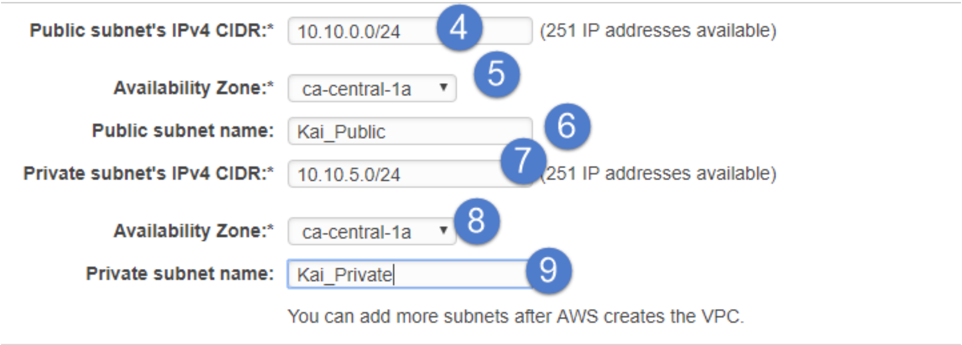
Step 2: VPC with Public and Private Subnets

IPv4 CIDR block:* 10.10.0.0/16 (65531 IP addresses available)

IPv6 CIDR block: ● No IPv6 CIDR Block
○ Amazon provided IPv6 CIDR block

VPC name: KAITEST1

4. Select an IPV4 CIDR block for your public subnet within the VPC range. In this example, we use 10.10.0.0/24.
5. Select a specific availability zone for your VPC public subnet. Note the availability zone selected for future reference.
6. Provide a name for your public subnet name.
7. Select an IPV4 CIDR block for your private subnet within the VPC range. In this example, we use 10.10.5.0/24.
8. Select the same availability zone as the public subnet, for simplicity's sake.
9. Provide a name for the private subnet.



Public subnet's IPv4 CIDR:* 10.10.0.0/24 (251 IP addresses available)

Availability Zone:* ca-central-1a

Public subnet name: Kai_Public

Private subnet's IPv4 CIDR:* 10.10.5.0/24 (251 IP addresses available)

Availability Zone:* ca-central-1a

Private subnet name: Kai_Private

You can add more subnets after AWS creates the VPC.

10. Provide the elastic IP address for a NAT gateway.

Configuration Best Practices to Consider Now:

- Select different availability zones when configuring the subnets for the greatest level of VPC redundancy.
- Select the proper instance type for intended usage, including anticipated networking and storage needs.
- Select a valid Key Pair that is secured and available for use.

Click on Create VPC. AWS will create a VPC with Public and Private subnets.

Note: If a NAT instance is not required for the local **SoftNAS Cloud®** deployment, delete the NAT instance and release any assigned Elastic IPs. Amazon hourly charges apply to NAT instances.

Specify the IAM User for SoftNAS Cloud®

About Amazon IAM Users

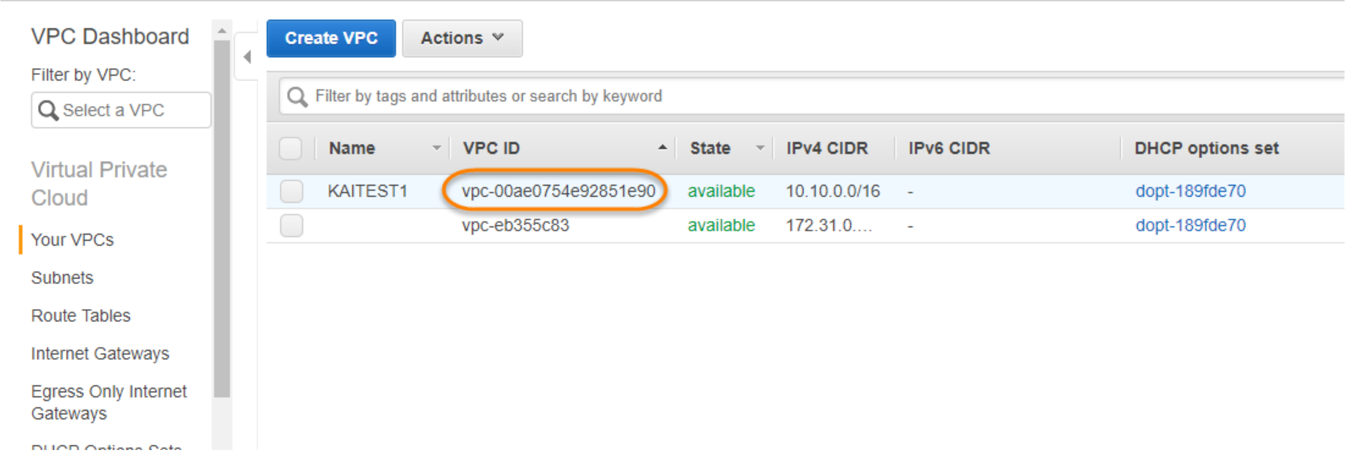
AWS Identity and Access Management is a web service that enables Amazon Web Services (AWS) customers to manage users and user permissions in AWS. The service is targeted at organizations with multiple users or systems that use AWS products such as Amazon EC2, Amazon RDS, and the AWS Management Console. With IAM, centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users can access.

Create an AWS IAM User for **SoftNAS Cloud®** . This will allow **SoftNAS Cloud®** instances to use the credentials of the AWS IAM User when accessing the VPC. For a step-by-step guide to setting up your IAM user, see **Creating the SoftNAS Cloud® IAM Role for AWS**.

Creating a Subnet

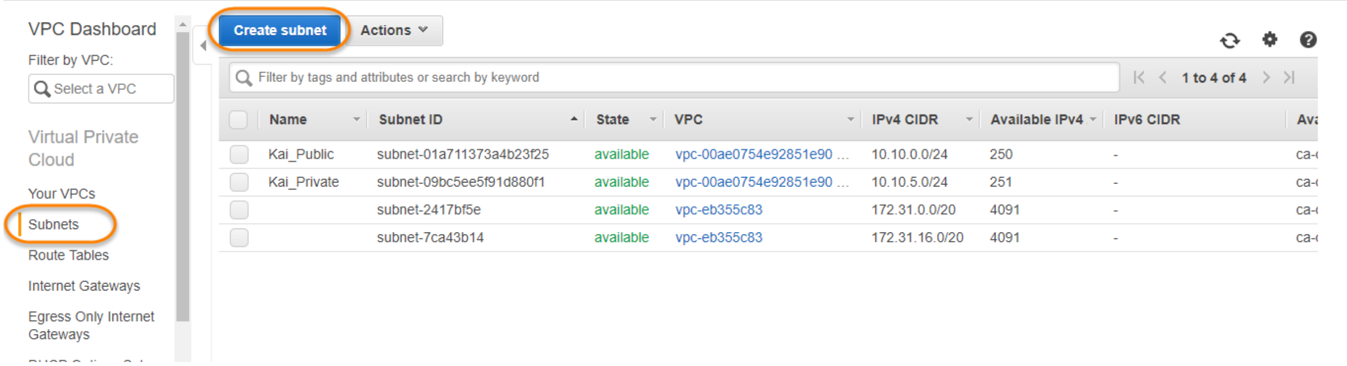
SoftNAS' **No Downtime Guarantee** requires that each instance in an HA pairing must belong to a separate Availability zone or region for redundancy. For this reason, at least two subnets are required for your VPC, each in a different Availability Zone. The first can be the default public or private subnet created when setting up the VPC. The second can be created now.

If you are going to assign additional subnets to your newly created VPC, it is important to log the VPC ID. The VPC ID can be found in **Your VPCs** from the **VPC Dashboard.**



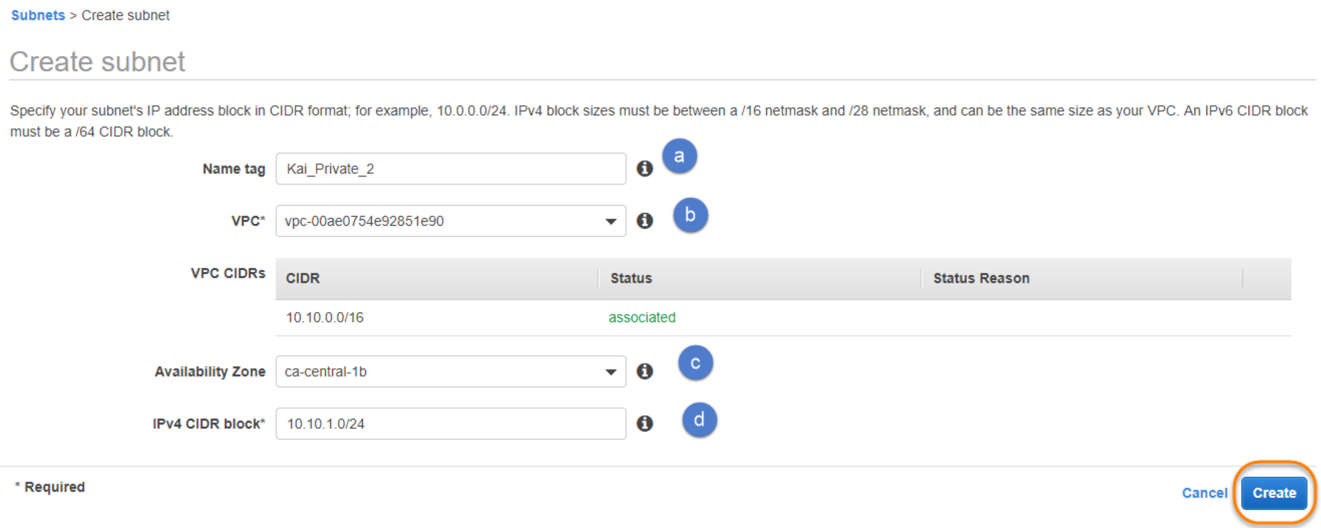
Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set
KAITEST1	vpc-00ae0754e92851e90	available	10.10.0.0/16	-	dopt-189fde70
	vpc-eb355c83	available	172.31.0....	-	dopt-189fde70

Select **Subnets** from the **VPC Dashboard**, and click **Create Subnet**.



Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Ava
Kai_Public	subnet-01a711373a4b23f25	available	vpc-00ae0754e92851e90 ...	10.10.0.0/24	250	-	ca-
Kai_Private	subnet-09bc5ee5f91d880f1	available	vpc-00ae0754e92851e90 ...	10.10.5.0/24	251	-	ca-
	subnet-2417bf5e	available	vpc-eb355c83	172.31.0.0/20	4091	-	ca-
	subnet-7ca43b14	available	vpc-eb355c83	172.31.16.0/20	4091	-	ca-

In **Create Subnet**, you will provide the following information to create each subnet:



Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag: Kai_Private_2

VPC*: vpc-00ae0754e92851e90

VPC CIDRs:

CIDR	Status	Status Reason
10.10.0.0/16	associated	

Availability Zone: ca-central-1b

IPv4 CIDR block*: 10.10.1.0/24

* Required

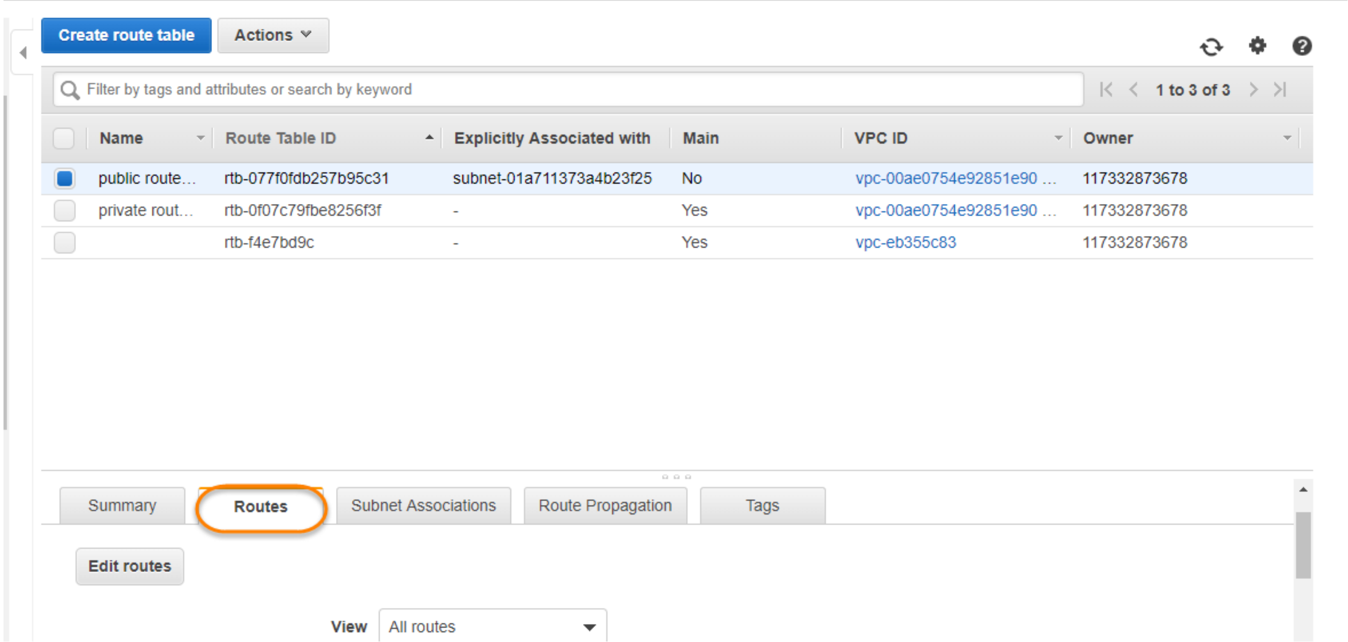
a. **Name Tag:** Provide a name for the subnet, ideally one that identifies it as a secondary public or private subnet, dependent on which you will be deploying into (this creates a key and value for the subnet).
b. **VPC:** Here you will specify the **VPC ID** of the VPC you wish this subnet associated with. (This will be the VPC ID you logged earlier)
c. **Availability Zone:** Next you will specify an Availability Zone. This should be a separate availability zone from the default VPC public /private subnets.
d. **IPv4 CIDR block:** The IPv4 CIDR block specifies an IP range for your instance. As we are creating two subnets, the CIDR block provided should be smaller than the CIDR block specified for the VPC.

Click **Yes, Create** when the information has been provided.

Associating Subnets to a Route Table

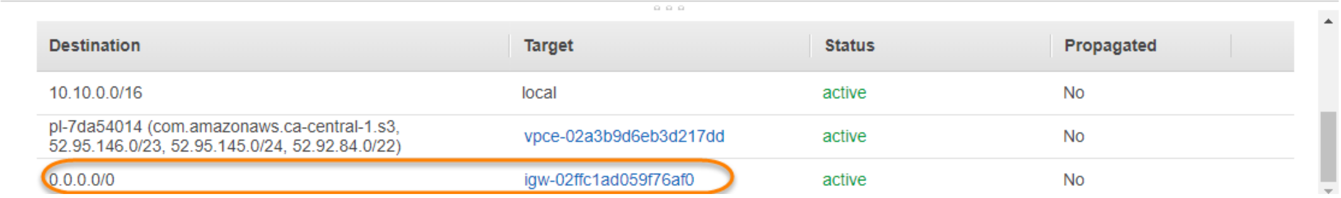
Once your subnets have been created, they need to be associated with the correct route table. If creating a private VPC HA deployment, the two private subnets just created will need to be associated with the NAT Gateway or private Route Table. If public, you will need to associate a second public subnet to the route table. In the below example, we will be associating private subnets to a private route table. However, the process is the same in either case. Simply be sure to select the correct route table, and associate the appropriate subnet.

To determine or verify the correct route table to assign the private subnets to, select one of the two route tables associated with your VPC (Remember, this can be determined by checking the VPC ID). Click on the **Route** tab.



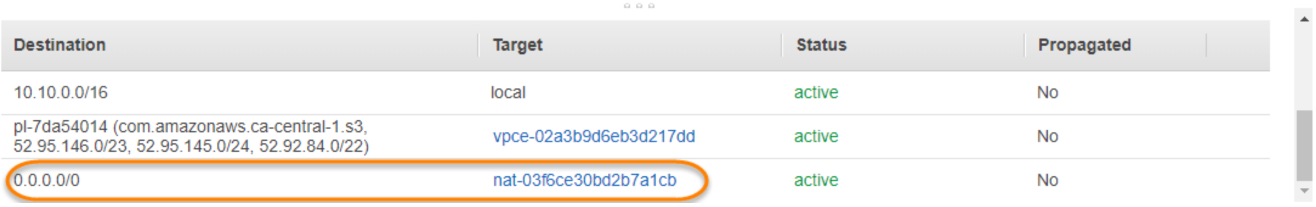
	Name	Route Table ID	Explicitly Associated with	Main	VPC ID	Owner
☑	public route…	rtb-077f0fdb257b95c31	subnet-01a711373a4b23f25	No	vpc-00ae0754e92851e90 …	117332873678
□	private rout…	rtb-0f07c79fbe8256f3f	-	Yes	vpc-00ae0754e92851e90 …	117332873678
□		rtb-f4e7bd9c	-	Yes	vpc-eb355c83	117332873678

Scroll down to see the default route (identified by the 0.0.0.0 IP address). If this route is associated with an internet gateway, this is the public route table. Labelling the route table can help identify it at a glance.



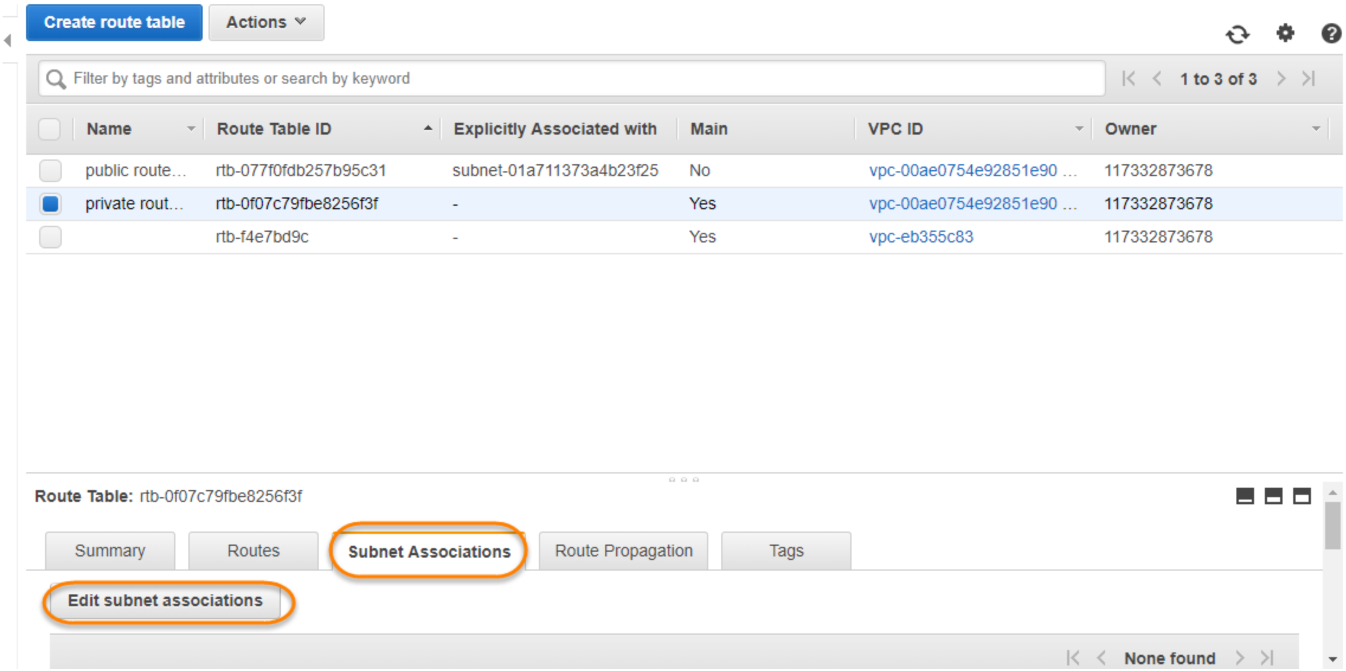
Destination	Target	Status	Propagated
10.10.0.0/16	local	active	No
pl-7da54014 (com.amazonaws.ca-central-1.s3, 52.95.146.0/23, 52.95.145.0/24, 52.92.84.0/22)	vpce-02a3b9d6eb3d217dd	active	No
0.0.0.0/0	igw-02ffc1ad059f76af0	active	No

Move to the second route table associated with the VPC if the first is associated with an internet gateway. The private route table to which we will associate the private subnets can be identified because the default route will be associated with the NAT Gateway.



Destination	Target	Status	Propagated
10.10.0.0/16	local	active	No
pl-7da54014 (com.amazonaws.ca-central-1.s3, 52.95.146.0/23, 52.95.145.0/24, 52.92.84.0/22)	vpce-02a3b9d6eb3d217dd	active	No
0.0.0.0/0	nat-03f6ce30bd2b7a1cb	active	No

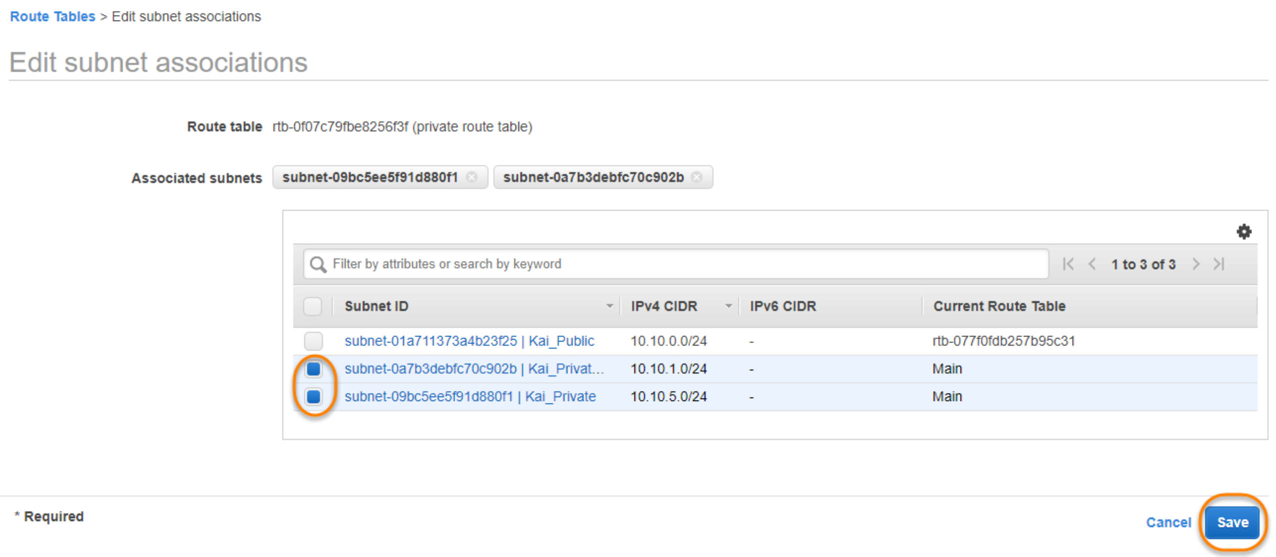
After verifying the private route table (associated with the NAT Gateway), select this route table, and select the **Subnet Associations**tab. Click **Edit subnet associations**.



	Name	Route Table ID	Explicitly Associated with	Main	VPC ID	Owner
□	public route...	rtb-077f0fdb257b95c31	subnet-01a711373a4b23f25	No	vpc-00ae0754e92851e90 ...	117332873678
☑	private rout...	rtb-0f07c79fbe8256f3f	-	Yes	vpc-00ae0754e92851e90 ...	117332873678
□		rtb-f4e7bd9c	-	Yes	vpc-eb355c83	117332873678

Route Table: rtb-0f07c79fbe8256f3f

Select the two private subnets created earlier, and click **Save**.



Route Tables > Edit subnet associations

Edit subnet associations

Route table rtb-0f07c79fbe8256f3f (private route table)

Associated subnets subnet-09bc5ee5f91d880f1 subnet-0a7b3debfc70c902b

	Subnet ID	IPv4 CIDR	IPv6 CIDR	Current Route Table
□	subnet-01a711373a4b23f25 | Kai_Public	10.10.0.0/24	-	rtb-077f0fdb257b95c31
☑	subnet-0a7b3debfc70c902b | Kai_Privat...	10.10.1.0/24	-	Main
☑	subnet-09bc5ee5f91d880f1 | Kai_Private	10.10.5.0/24	-	Main

* Required

If deploying into a public subnet, you would simply associate a second public subnet instead (This public subnet should have been created as described earlier in the **Creating a Subnet** section of this guide).

Launch An Instance of SoftNAS Cloud® into the VPC

To launch an instance of **SoftNAS Cloud®** into the already-set-up VPC, the following is required:

1. Select the appropriate **SoftNAS Cloud® AMI** from the Marketplace AMI section of EC2 services.
2. Select at least the small instance.
3. Configure the instance details.
4. Launch instance into the subnet.
5. Add an additional ethernet interface.
6. Add storage as required.
7. Tag the instance.
8. Set up security groups.
9. Select a key pair for SSH.

The above procedure is repeated to create a second **SoftNAS Cloud®** instance for HA.

Selecting the SoftNAS Cloud® AMI

1. For **SoftNAS Cloud®**, navigate to AWS Marketplace AMIs.
2. Select the **SoftNAS AMI** from the **Community AMI** section of **EC2** services.
3. From EC2 services, click on **Launch Instance>Marketplace AMIs** and enter **SoftNAS** in the search text box**.**
4. Select the appropriate **SoftNAS Cloud®** version for expected need (Platinum, Enterprise, or Essentials).

Choosing an Instance Type

SoftNAS recommends an instance size of r5.2xlarge for any production deployment or any deployment testing production workload capacity. For SoftNAS Instance sizing guidance, see **SoftNAS' Sizing Tool**.

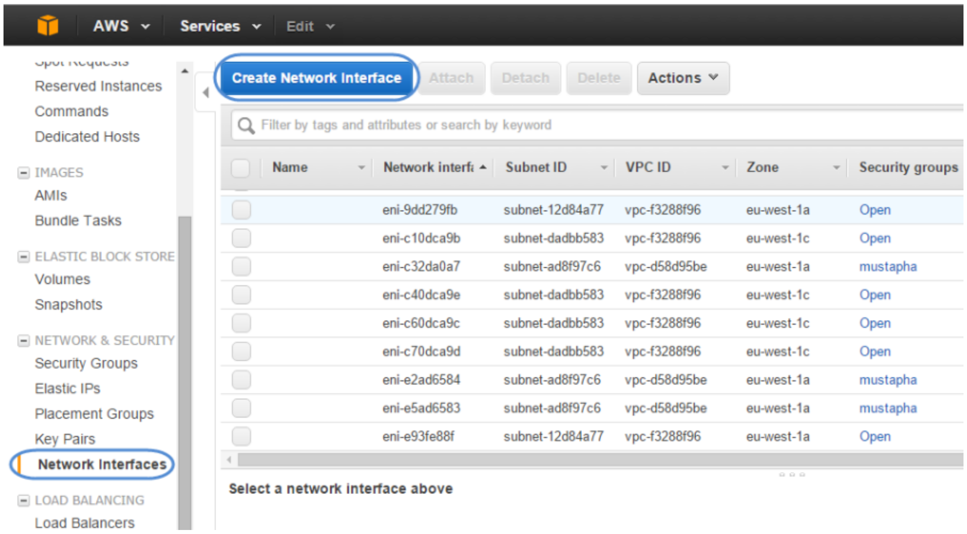
1. From **Step 2. Choose an Instance Type**.
2. Select the appropriate machine type for expected usage from the matrix given. For more information on Amazon Instance types, click **here**.
3. Click on **Next: Configure Instance Details.**

Instance Details

1. For **Network**, select the previously configured VPC.
2. Select one of the available public or private subnets to associate with this instance.
3. Scroll to **Network Interfaces**, expand, and click **Add Device**. If using Elastic IPs for your HA instance, it is very important to add an additional **NIC** here as well as your storage.

   To add an additional NIC after instance creation:

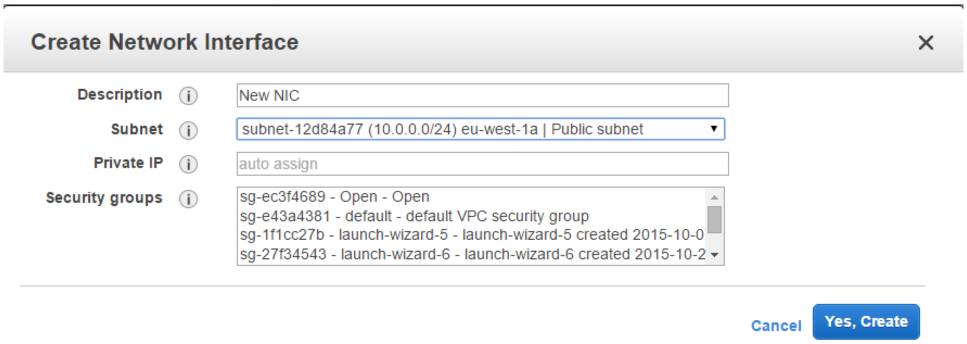
   a. Select Network Interfaces from within the EC2 console, then **Create Network Interface**.



Name	Network interfa	Subnet ID	VPC ID	Zone	Security groups
	eni-9dd279fb	subnet-12d84a77	vpc-f3288f96	eu-west-1a	Open
	eni-c10dca9b	subnet-dadbb583	vpc-f3288f96	eu-west-1c	Open
	eni-c32da0a7	subnet-ad8f97c6	vpc-d58d95be	eu-west-1a	mustapha
	eni-c40dca9e	subnet-dadbb583	vpc-f3288f96	eu-west-1c	Open
	eni-c60dca9c	subnet-dadbb583	vpc-f3288f96	eu-west-1c	Open
	eni-c70dca9d	subnet-dadbb583	vpc-f3288f96	eu-west-1c	Open
	eni-e2ad6584	subnet-ad8f97c6	vpc-d58d95be	eu-west-1a	mustapha
	eni-e5ad6583	subnet-ad8f97c6	vpc-d58d95be	eu-west-1a	mustapha
	eni-e93fe88f	subnet-12d84a77	vpc-f3288f96	eu-west-1a	Open

Select a network interface above

b. Provide a name, select your subnet and a security group. Click **Create**.



Create Network Interface

Description	New NIC
Subnet	subnet-12d84a77 (10.0.0.0/24) eu-west-1a | Public subnet
Private IP	auto assign
Security groups	sg-ec3f4689 - Open - Open sg-e43a4381 - default - default VPC security group sg-1f1cc27b - launch-wizard-5 - launch-wizard-5 created 2015-10-0 sg-27f34543 - launch-wizard-6 - launch-wizard-6 created 2015-10-2

4. Click on **Next: Add Storage.**

Adding Storage and Tagging

1. From the storage screen, add storage volumes as necessary. Remember that storage can be added after instance creation from within the SoftNAS Cloud UI making this step entirely optional. Ensure that **Delete on Termination** is selected.

2. Click **Next**: **Tag Instance** and add an instance name to the **Value** field.

3. Click **Next: Configure Security Group**

Note: Disk names for EBS volumes must follow **SoftNAS Cloud®** storage naming conventions. For more information, see the document SoftNAS Installation Guide.

Security Groups

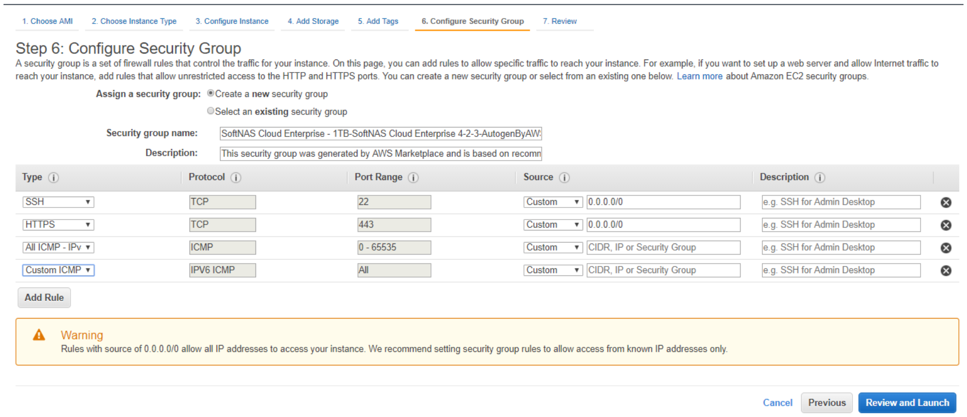
Security groups for SoftNAS Cloud® must include TCP 443, TCP 22, and ICMP Echo Reply and Echo Response. Source can be locked down per security requirements.

Note: When assigning the Security Group for a **SoftNAS Cloud®** instance, either create a new Security Group or select a preexisting security Group. Regardless of the decision, ensure it includes the above-mentioned rules.

Create the required rules for the security group

1. From the available selection, choose **Create**.

2. Select **Custom ICMP Rule**. **Source** can be set to "Anywhere, My IP, or Custom IP," based on local security requirements. Assign **Type** and **Port** as appropriate.



Step 6: Configure Security Group

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

Assign a security group: ● Create a **new** security group
○ Select an **existing** security group

Security group name: SoftNAS Cloud Enterprise - 1TB-SoftNAS Cloud Enterprise 4-2-3-AutogenByAW:
Description: This security group was generated by AWS Marketplace and is based on recomn

Type	Protocol	Port Range	Source		Description
SSH	TCP	22	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop
HTTPS	TCP	443	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop
All ICMP - IPv	ICMP	0 - 65535	Custom	CIDR, IP or Security Group	e.g. SSH for Admin Desktop
Custom ICMP	IPV6 ICMP	All	Custom	CIDR, IP or Security Group	e.g. SSH for Admin Desktop

Warning
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

3. Repeat the above procedure to add the Custom TCP Rule for ports 443 and 22.
   Enable ALL ICMP for both IPv4 and IPv6 as shown above.

   Note: It is recommended to restrict the Source IP address to an address or range of valid addresses for best security.
   Note: Port 3389 can also be enabled for RDP access to Clients in the environment.

4. Click on **Review and Launch.**
5. Provide the appropriate key pair when prompted.

Keep in mind that two instances are required for **HA.** Create a second instance at this time.

In order to complete the set up high availability for Amazon Web Services VPCs in either a Virtual IP or Elastic IP setup, select the appropriate link below:

- Amazon Web Services VPC: Virtual IP Setup
- Amazon Web Services VPC: Elastic IP