A CLOUD GURU

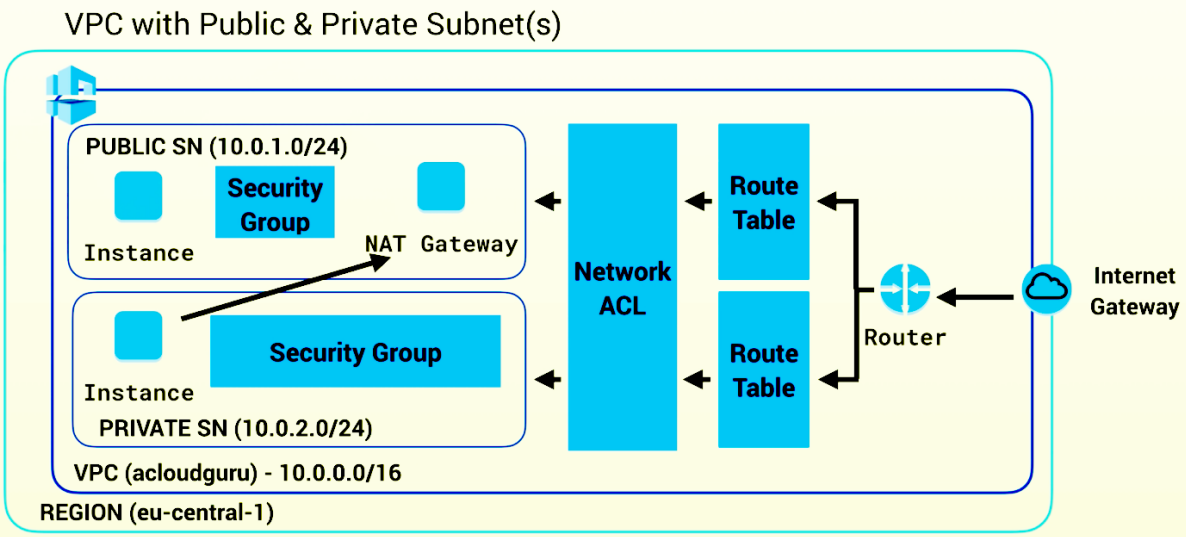
NAT Instances & NAT Gateways - LAB

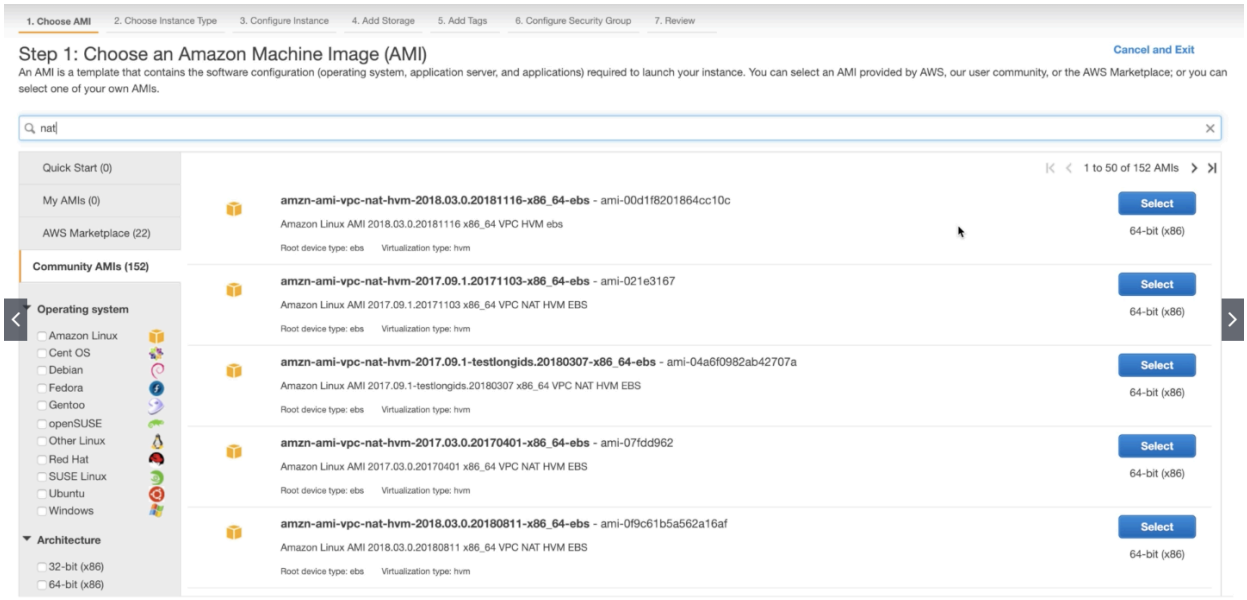
Ryan Kroonenburg
AWS COMMUNITY HERO & ALEXA CHAMPION
FOUNDER OF A CLOUD GURU

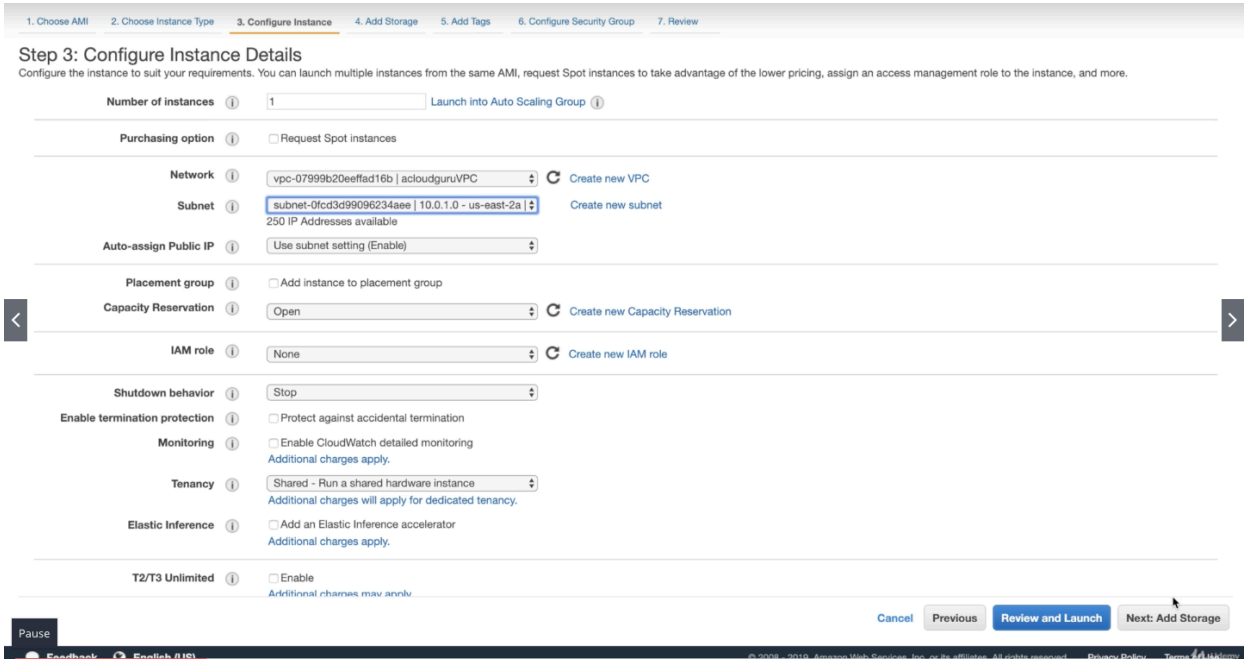
NAT INSTANCES & NAT GATEWAYS

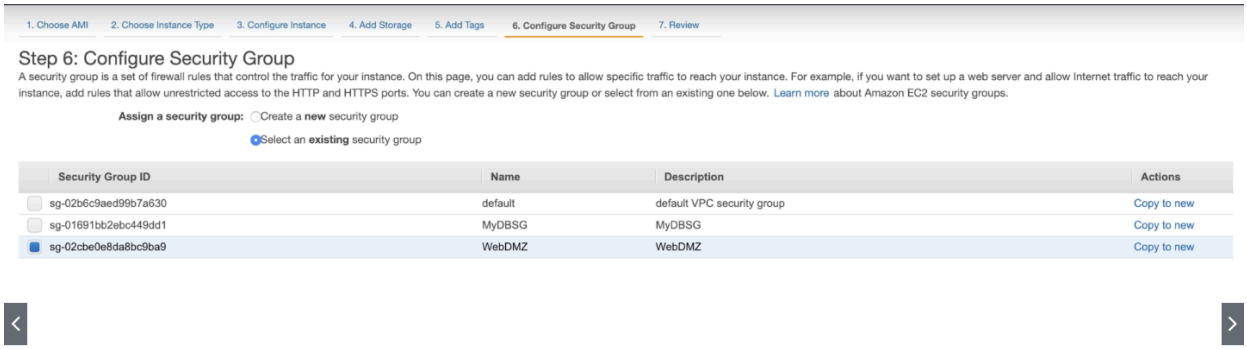
NAT Gateways Explained

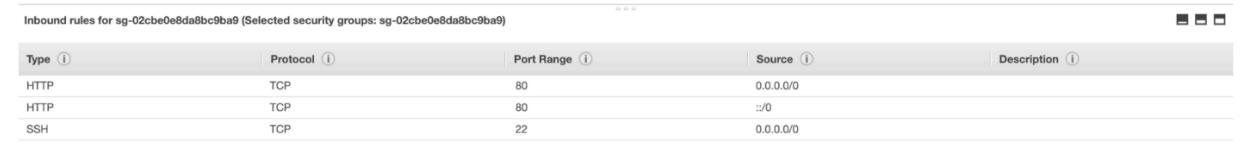
A CLOUD GURU

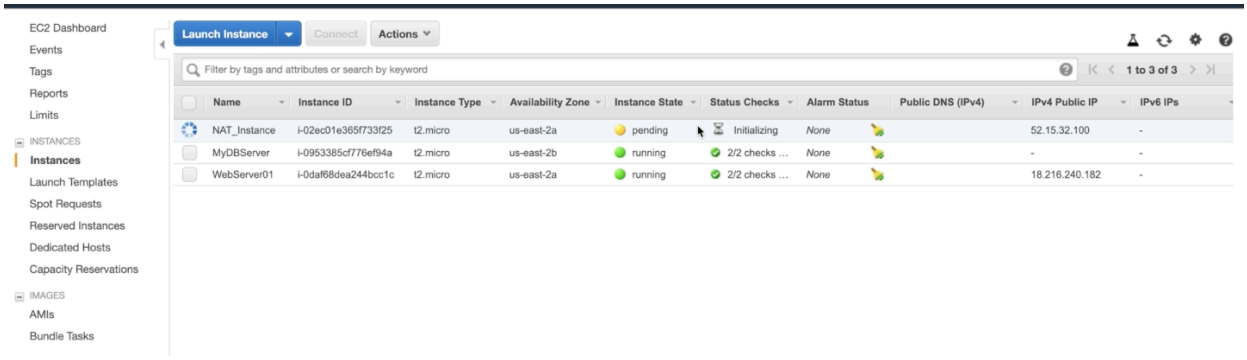



1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 1: Choose an Amazon Machine Image (AMI)
Cancel and Exit
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.
nat
Quick Start (0)
My AMIs (0)
AWS Marketplace (22)
Community AMIs (152)
Operating system
Amazon Linux
Cent OS
Debian
Fedora
Gentoo
openSUSE
Other Linux
Red Hat
SUSE Linux
Ubuntu
Windows
Architecture
32-bit (x86)
64-bit (x86)
1 to 50 of 152 AMIs
amzn-ami-vpc-nat-hvm-2018.03.0.20181116-x86_64-ebs - ami-00d1f8201864cc10c
Amazon Linux AMI 2018.03.0.20181116 x86_64 VPC HVM ebs
Root device type: ebs Virtualization type: hvm
Select
64-bit (x86)
amzn-ami-vpc-nat-hvm-2017.09.1.20171103-x86_64-ebs - ami-021e3167
Amazon Linux AMI 2017.09.1.20171103 x86_64 VPC NAT HVM EBS
Root device type: ebs Virtualization type: hvm
Select
64-bit (x86)
amzn-ami-vpc-nat-hvm-2017.09.1-testlongids.20180307-x86_64-ebs - ami-04a6f0982ab42707a
Amazon Linux AMI 2017.09.1-testlongids.20180307 x86_64 VPC NAT HVM EBS
Root device type: ebs Virtualization type: hvm
Select
64-bit (x86)
amzn-ami-vpc-nat-hvm-2017.03.0.20170401-x86_64-ebs - ami-07fdd962
Amazon Linux AMI 2017.03.0.20170401 x86_64 VPC NAT HVM EBS
Root device type: ebs Virtualization type: hvm
Select
64-bit (x86)
amzn-ami-vpc-nat-hvm-2018.03.0.20180811-x86_64-ebs - ami-0f9c61b5a562a16af
Amazon Linux AMI 2018.03.0.20180811 x86_64 VPC NAT HVM EBS
Root device type: ebs Virtualization type: hvm
Select
64-bit (x86)


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
1
Launch into Auto Scaling Group
Purchasing option
Request Spot instances
Network
vpc-07999b20eeffad16b | acloudguruVPC
Create new VPC
Subnet
subnet-0fcd3d99096234aee | 10.0.1.0 - us-east-2a
Create new subnet
250 IP Addresses available
Auto-assign Public IP
Use subnet setting (Enable)
Placement group
Add instance to placement group
Capacity Reservation
Open
Create new Capacity Reservation
IAM role
None
Create new IAM role
Shutdown behavior
Stop
Enable termination protection
Protect against accidental termination
Monitoring
Enable CloudWatch detailed monitoring
Additional charges apply.
Tenancy
Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy.
Elastic Inference
Add an Elastic Inference accelerator
Additional charges apply.
T2/T3 Unlimited
Enable
Cancel
Previous
Review and Launch
Next: Add Storage
Pause


1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
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 ID
Name
Description
Actions
sg-02b6c9aed99b7a630
default
default VPC security group
Copy to new
sg-01691bb2ebc449dd1
MyDBSG
MyDBSG
Copy to new
sg-02cbe0e8da8bc9ba9
WebDMZ
WebDMZ
Copy to new


Inbound rules for sg-02cbe0e8da8bc9ba9 (Selected security groups: sg-02cbe0e8da8bc9ba9)
Type
Protocol
Port Range
Source
Description
HTTP
TCP
80
0.0.0.0/0
HTTP
TCP
80
::/0
SSH
TCP
22
0.0.0.0/0


EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Launch Templates
Spot Requests
Reserved Instances
Dedicated Hosts
Capacity Reservations
IMAGES
AMIs
Bundle Tasks
Launch Instance
Connect
Actions
Filter by tags and attributes or search by keyword
1 to 3 of 3
Name
Instance ID
Instance Type
Availability Zone
Instance State
Status Checks
Alarm Status
Public DNS (IPv4)
IPv4 Public IP
IPv6 IPs
NAT_Instance
i-02ec01e365f733f25
t2.micro
us-east-2a
pending
Initializing
None
52.15.32.100
MyDBServer
i-0953385cf776ef94a
t2.micro
us-east-2b
running
2/2 checks ...
None
WebServer01
i-0daf68dea244bcc1c
t2.micro
us-east-2a
running
2/2 checks ...
None
18.216.240.182

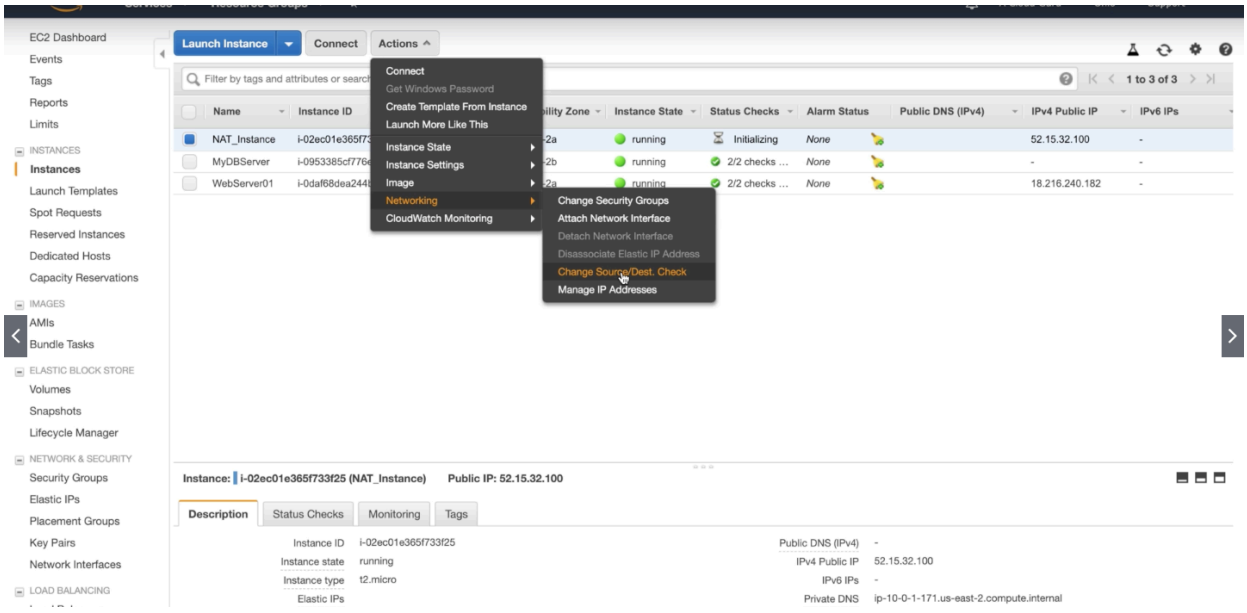
Disabling Source/Destination Checks

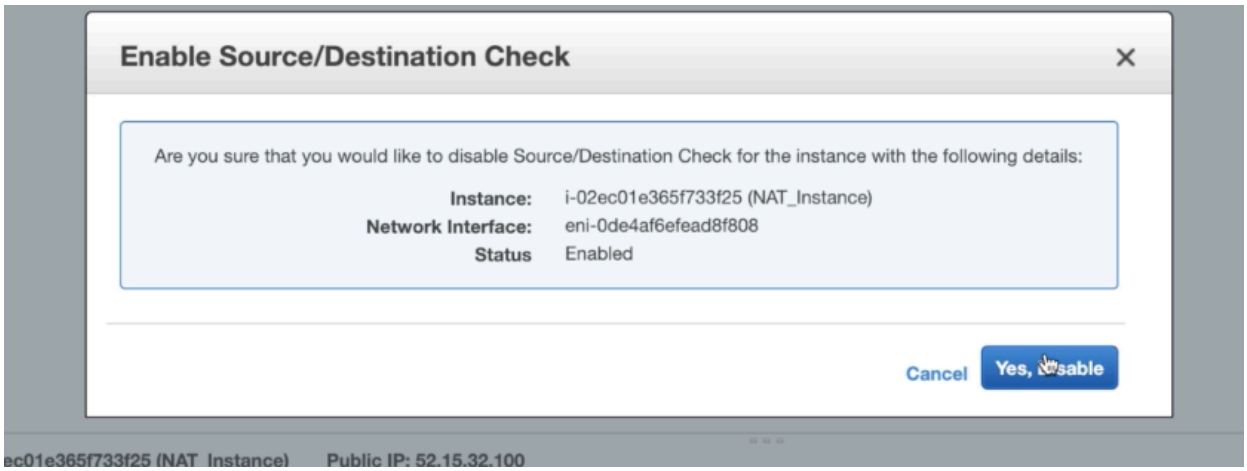
Each EC2 instance performs source/destination checks by default. This means that the instance must be the source or destination of any traffic it sends or receives. However, a NAT instance must be able to send and receive traffic when the source or destination is not itself. Therefore, you must disable source/destination checks on the NAT instance.

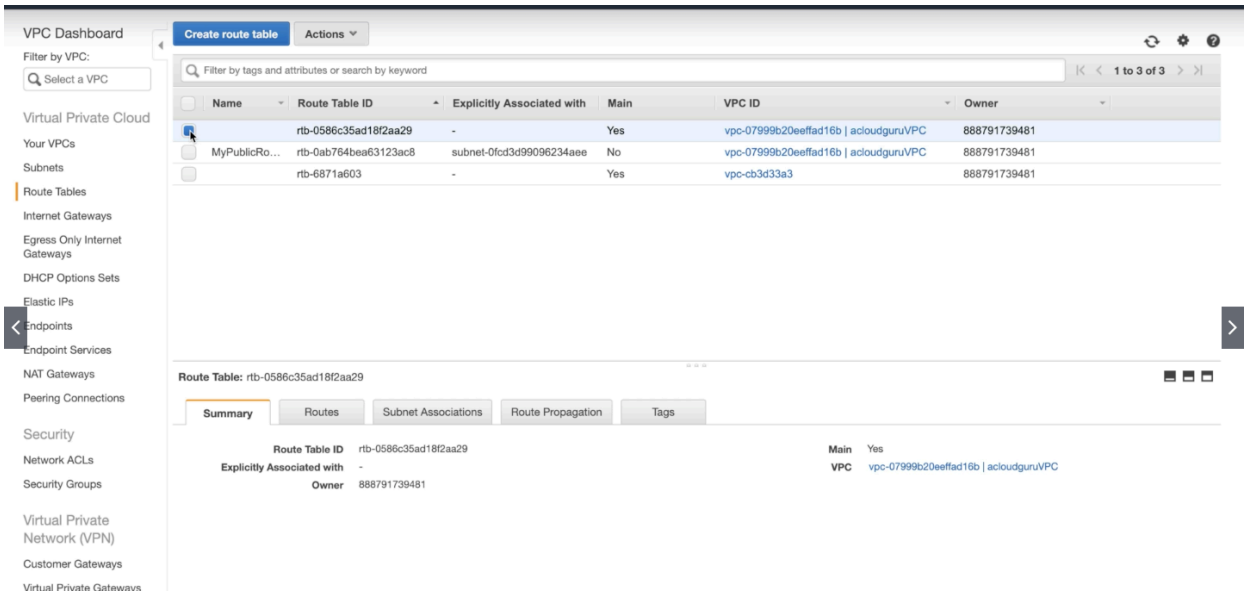
You can disable the `SrcDestCheck` attribute for a NAT instance that's either running or stopped using the console or the command line.

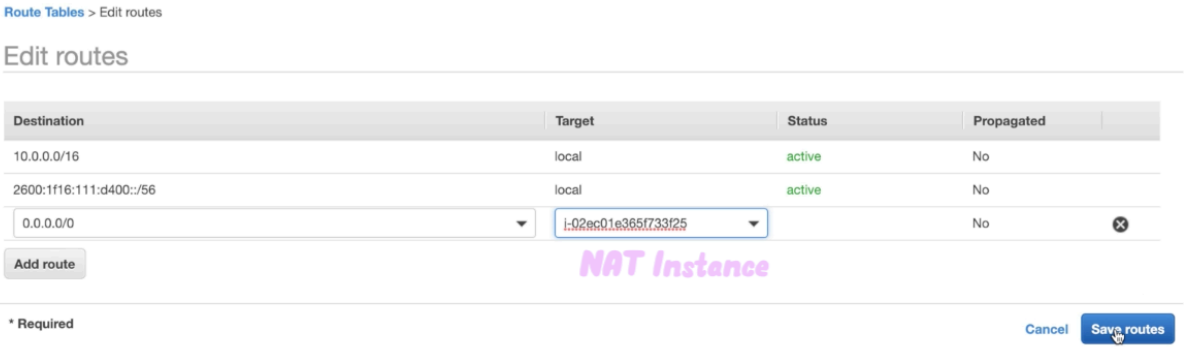
To disable source/destination checking using the console

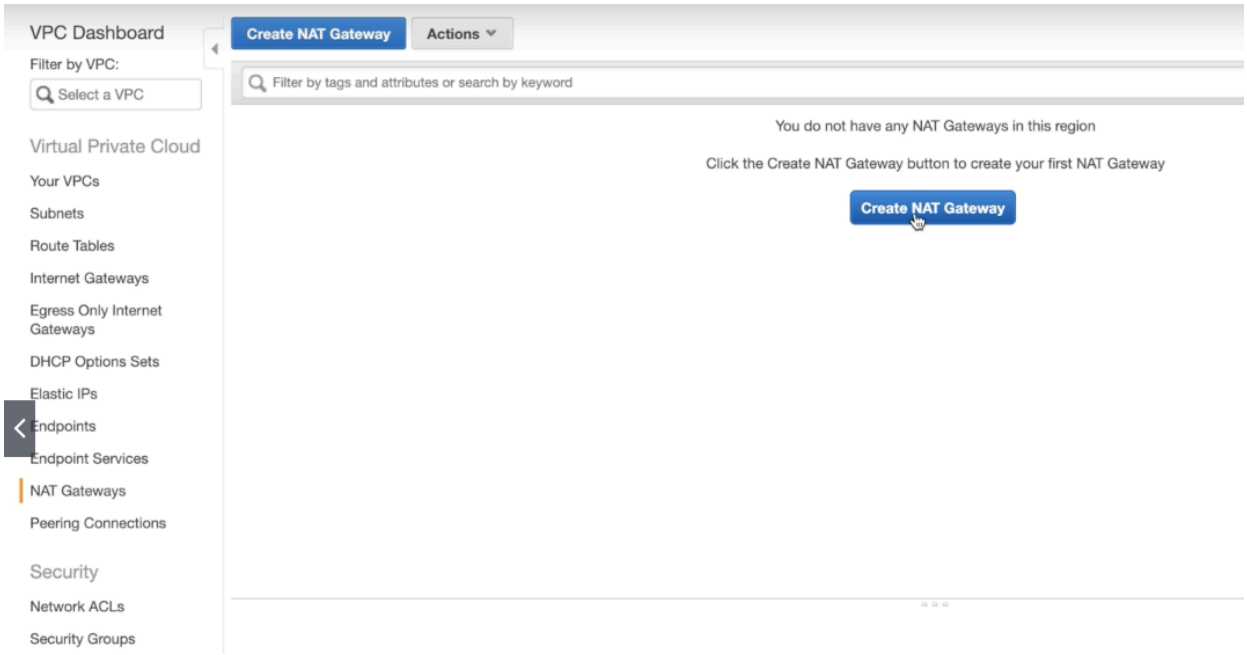
1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. In the navigation pane, choose **Instances**.
3. Select the NAT instance, choose **Actions**, **Networking**, **Change Source/Dest. Check**.
4. For the NAT instance, verify that this attribute is disabled. Otherwise, choose **Yes, Disable**.
5. If the NAT instance has a secondary network interface, choose it from **Network interfaces** on the **Description** tab and choose the interface ID to go to the network interfaces page. Choose **Actions**, **Change Source/Dest. Check**, disable the setting, and choose **Save**.

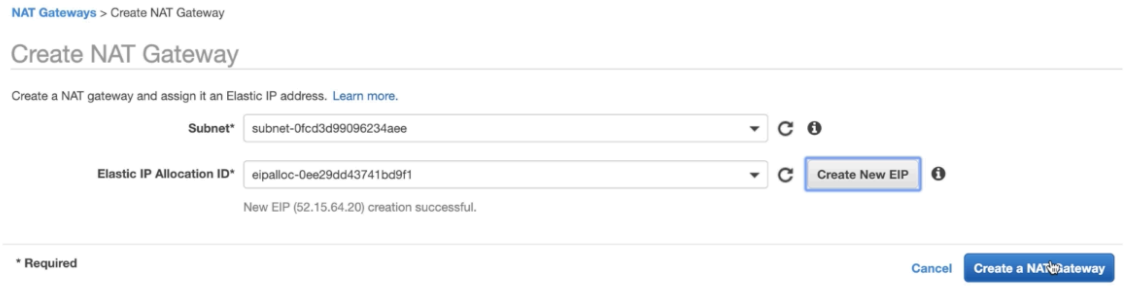


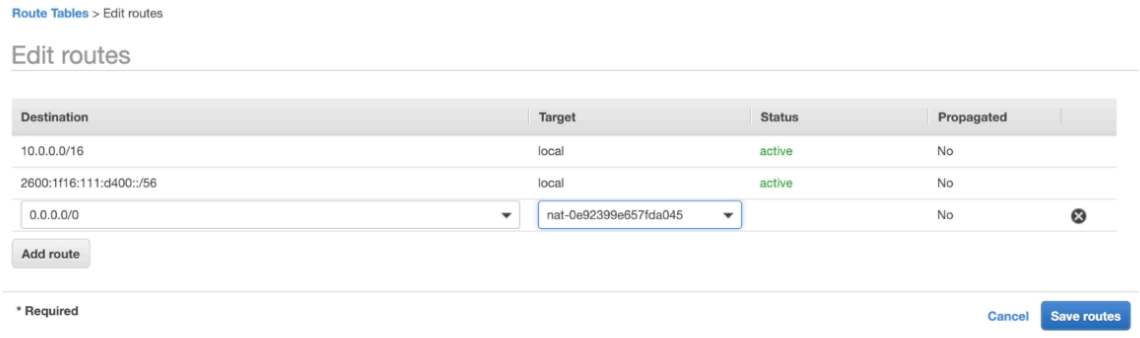

Enable Source/Destination Check
Are you sure that you would like to disable Source/Destination Check for the instance with the following details:
Instance: i-02ec01e365f733f25 (NAT_Instance)
Network Interface: eni-0de4af6efead8f808
Status Enabled
Cancel
Yes, Disable
ec01e365f733f25 (NAT_Instance) Public IP: 52.15.32.100


VPC Dashboard
Filter by VPC:
Select a VPC
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
Endpoint Services
NAT Gateways
Peering Connections
Security
Network ACLs
Security Groups
Virtual Private Network (VPN)
Customer Gateways
Virtual Private Gateways
Create route table
Actions
Filter by tags and attributes or search by keyword
1 to 3 of 3
Name
Route Table ID
Explicitly Associated with
Main
VPC ID
Owner
rtb-0586c35ad18f2aa29 - Yes vpc-07999b20eeffad16b | acloudguruVPC 888791739481
MyPublicRo... rtb-0ab764bea63123ac8 subnet-0fcd3d99096234aee No vpc-07999b20eeffad16b | acloudguruVPC 888791739481
rtb-6871a603 - Yes vpc-cb3d33a3 888791739481
Route Table: rtb-0586c35ad18f2aa29
Summary
Routes
Subnet Associations
Route Propagation
Tags
Route Table ID rtb-0586c35ad18f2aa29
Explicitly Associated with -
Owner 888791739481
Main Yes
VPC vpc-07999b20eeffad16b | acloudguruVPC


Route Tables > Edit routes
Edit routes
Destination
Target
Status
Propagated
10.0.0.0/16
local
active
No
2600:1f16:111:d400::/56
local
active
No
0.0.0.0/0
i-02ec01e365f733f25
No
Add route
NAT Instance
* Required
Cancel
Save routes


VPC Dashboard
Filter by VPC:
Select a VPC
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
Endpoint Services
NAT Gateways
Peering Connections
Security
Network ACLs
Security Groups
Create NAT Gateway
Actions
Filter by tags and attributes or search by keyword
You do not have any NAT Gateways in this region
Click the Create NAT Gateway button to create your first NAT Gateway
Create NAT Gateway


NAT Gateways > Create NAT Gateway
Create NAT Gateway
Create a NAT gateway and assign it an Elastic IP address. Learn more.
Subnet*
subnet-0fcd3d99096234aee
Elastic IP Allocation ID*
eipalloc-0ee29dd43741bd9f1
Create New EIP
New EIP (52.15.64.20) creation successful.
* Required
Cancel
Create a NAT Gateway


Route Tables > Edit routes
Edit routes
Destination
Target
Status
Propagated
10.0.0.0/16
local
active
No
2600:1f16:111:d400::/56
local
active
No
0.0.0.0/0
nat-0e92399e657fda045
No
Add route
* Required
Cancel
Save routes

Nat Instances Exam Tips

- When creating a NAT instance, Disable Source/Destination Check on the Instance.
- NAT instances must be in a public subnet.
- There must be a route out of the private subnet to the NAT instance, in order for this to work.
- The amount of traffic that NAT instances can support depends on the instance size. If you are bottlenecking, increase the instance size.
- You can create high availability using Autoscaling Groups, multiple subnets in different AZs, and a script to automate failover.
- Behind a Security Group.

Nat Gateways

- Redundant inside the Availability Zone
- Preferred by the enterprise
- Starts at 5Gbps and scales currently to 45Gbps
- No need to patch
- Not associated with security groups
- Automatically assigned a public ip address
- Remember to update your route tables.

Nat Gateways

- If you have resources in multiple Availability Zones and they share one NAT gateway, in the event that the NAT gateway's Availability Zone is down, resources in the other Availability Zones lose internet access. To create an Availability Zone-independent architecture, create a NAT gateway in each Availability Zone and configure your routing to ensure that resources use the NAT gateway in the same Availability Zone.