

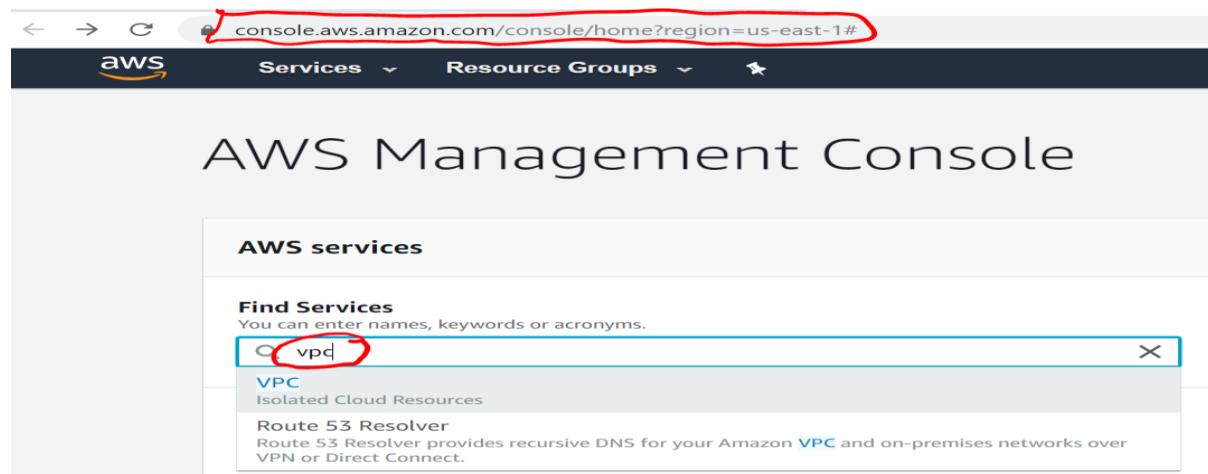
TUTORIAL FOR CREATION OF A JUMPBOX TO ACCESS ALL INSTANCES IN AWS

The step-by step procedure to create a jumpbox in AWS is detailed below:

1. CREATION OF A VPC, A PUBLIC SUBNET AND A PRIVATE SUBNET

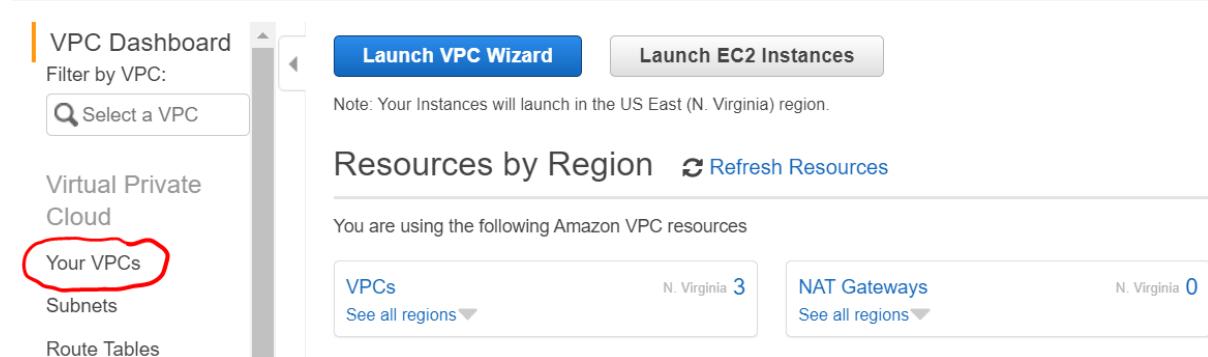
1.1 Creation of a VPC:

- Login to <https://www.console.aws.amazon.com> >> Find services - search for VPC and click on VPC



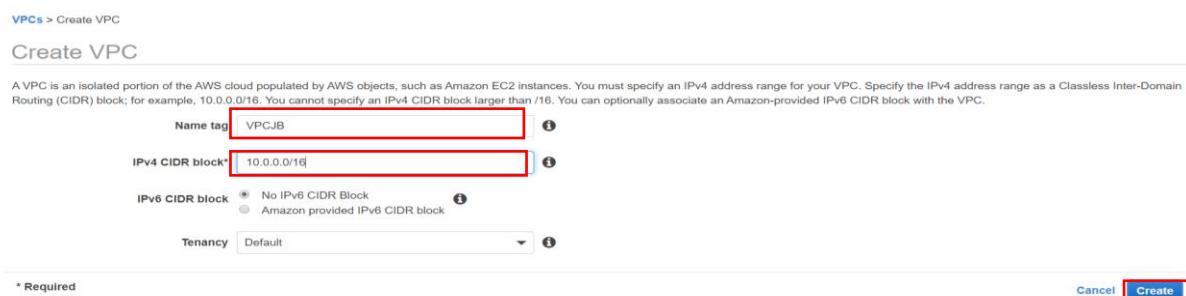
A screenshot of the AWS Management Console. The URL in the address bar is `console.aws.amazon.com/console/home?region=us-east-1#`. The search bar at the top has "vpc" typed into it. Below the search bar, the "AWS services" section shows a dropdown menu with "VPC" selected. The main content area displays the "AWS Management Console" header and some service links.

- Click on **Your VPCs** as shown below



A screenshot of the VPC Dashboard. On the left sidebar, there are links for "Virtual Private Cloud", "Your VPCs" (which is circled in red), "Subnets", and "Route Tables". In the center, there are buttons for "Launch VPC Wizard" and "Launch EC2 Instances". Below these buttons, a note says "Note: Your Instances will launch in the US East (N. Virginia) region." Under the heading "Resources by Region", there is a table showing "VPCs" (3 in N. Virginia) and "NAT Gateways" (0 in N. Virginia). A note at the bottom says "You are using the following Amazon VPC resources".

- Fill in the details in the **Name Tag** and **IPv4 CIDR Block** and click on **Create**



A screenshot of the "Create VPC" wizard. At the top, it says "VPCs > Create VPC" and "Create VPC". A note below says "A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You must specify an IPv4 address range for your VPC. Specify the IPv4 address range as a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16. You cannot specify an IPv4 CIDR block larger than /16. You can optionally associate an Amazon-provided IPv6 CIDR block with the VPC." The "Name tag" field contains "VPCJB" and the "IPv4 CIDR block" field contains "10.0.0.0/16". There are also fields for "IPv6 CIDR block" (radio buttons for "No IPv6 CIDR Block" and "Amazon provided IPv6 CIDR block"), "Tenancy" (dropdown menu with "Default"), and buttons for "Cancel" and "Create" (the "Create" button is highlighted).

- VPC is created as shown below. Click on **Close**

VPCs > Create VPC

Create VPC

- ✓ The following VPC was created:

VPC ID vpc-009ce8eab0d7d0d14

Close

1.2 Creation of a Public Subnet, Internet Gateway and Route table

- In the **VPC Dashboard** click on **Subnets**

Name	VPC ID	State	IPv4 CIDR	DHCP options set	Main Route table
padvpc1	vpc-056c3def	available	172.31.0.0/16	dopt-e40dff9e	rtb-f90ed287
PadVPC2	vpc-0c9c5f464f587667e	available	10.0.0.0/16	dopt-e40dff9e	rtb-0a1a8ce3c883bc0ec
Padtest	vpc-072155389e696a261	available	10.0.0.0/16	dopt-e40dff9e	rtb-08133fb7ff4a74a4b
VPCJB	vpc-009ce8eab0d7d0d14	available	10.0.0.0/16	dopt-e40dff9e	rtb-0fa2ad2fa0af06bd6

- In the subsequent screen click on **Create subnet**

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR
padsubnet1	subnet-08c3826d2d15ce4ac	available	vpc-072155389e696a261	10.0.1.0/24	251	-
Public subnet	subnet-0ebc265362a6a14c1	available	vpc-0c9c5f464f587667e	10.0.0.0/24	250	-
	subnet-1d581023	available	vpc-956c3def padvpc1	172.31.48.0/20	4091	-
	subnet-33a0747e	available	vpc-956c3def padvpc1	172.31.16.0/20	4091	-

- **Name Tag:** Provide an appropriate name; **VPC:** Select the name from the dropdown menu
IP4 CIDR block: Type the appropriate address Eg. 10.0.0.0/24 >> Click on **Create**

Subnets > Create subnet

Create 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 PublicSubnetJB

VPC* vpc-009ce8eab0d7d0d14

Filter by attributes

VPC CIDRs	Status	Status Reason
vpc-0c9c5f464f587667e	PadVPC2	
vpc-956c3def	padvpc1	
vpc-072155389e696a261	Padtest	
vpc-009ce8eab0d7d0d14	VPCJB	

Availability Zone No preference

IPv4 CIDR block* 10.0.0.0/24

* Required

Create

- A public subnet is created >> Click on **Close**

Subnets > Create subnet

Create subnet

The following Subnet was created:

Subnet ID: subnet-0a6519810dd276836

Close

- In the VPC Dashboard select the newly created Public Subnet. Click on Internet Gateways

VPC Dashboard

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR
padsubnet1	subnet-08c3826d2d15ce4ac	available	vpc-072155389e696a261 ...	10.0.1.0/24	251	-
PublicSubnetJB	subnet-0a6519810dd276836	available	vpc-009cce8eab0d7d0d14 ...	10.0.0.0/24	251	-
Public subnet	subnet-0ebc265362a6a14c1	available	vpc-09c5f464f587667e ...	10.0.0.0/24	250	-
subnet-1d581023	subnet-1d581023	available	vpc-956c3def padvpc1	172.31.48.0/20	4091	-
subnet-33a0747e	subnet-33a0747e	available	vpc-956c3def padvpc1	172.31.16.0/20	4091	-
subnet-68565734	subnet-68565734	available	vpc-956c3def padvpc1	172.31.32.0/20	4090	-
subnet-9448b79a	subnet-9448b79a	available	vpc-956c3def padvpc1	172.31.64.0/20	4091	-
subnet-d3cccf0	subnet-d3cccf0	available	vpc-956c3def padvpc1	172.31.80.0/20	4091	-
subnet-f0e1e497	subnet-f0e1e497	available	vpc-956c3def padvpc1	172.31.0.0/20	4091	-

- Name tag: Provide a suitable name >> Click on **Create**

Internet gateways > Create internet gateway

Create internet gateway

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Name tag: **PublicSubnetJB**

* Required

Create

- An Internet gateway is created for the Public subnet >> Click on **Close**

Internet gateways > Create internet gateway

Create internet gateway

The following internet gateway was created:

Internet gateway ID: igw-056ad980e6eb601d3

Close

- VPC Dashboard >> select the newly created Internet Gateway >> Actions >> Attach VPC

VPC Dashboard

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Name	State	VPC	Owner
igw-0111be1236739cbe3	attached	vpc-0c9c5f464f587667e PadVPC2	295613640041
PublicSubnetJBGW	detached	-	295613640041
Padgw1	attached	vpc-072155389e696a261 Padtest	295613640041
igw-80ff7bf0	attached	vpc-956c3def padvpc1	295613640041

- VPC >> Click on the **dropdown menu** >> select the required **VPC ID** >> **Attach**

Internet gateways > Attach to VPC

Attach to VPC

Attach an internet gateway to a VPC to enable communication with the internet. Specify the VPC you would like to attach below.

VPC*	vpc-009ce8eab0d7d0d14	<input type="button" value="Cancel"/>	<input type="button" value="Attach"/>
Filter by attributes			
VPC ID	Name		
* Required	vpc-009ce8eab0d7d0d14	VPCJB	

- The newly created **internet gateway** is attached to the **VPC**

VPC Dashboard

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Create Internet gateway

Name	ID	State	VPC	Owner
igw-0111bef256739cfef	igw-056ad980e6eb601d3	attached	vpc-0c9c5f464f587667e PadVPC2	295613640041
PublicSubnetJBGW	igw-056ad980e6eb601d3	attached	vpc-009ce8eab0d7d0d14 VPCJB	295613640041
Padgw1	igw-0cf084ea2aa4be0f2	attached	vpc-072155389e696a261 Padtest	295613640041
	igw-80ff7bf	attached	vpc-956c3def padvpc1	295613640041

- In the **VPC Dashboard** click on **Route Tables** >> **Create route table**

VPC Dashboard

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Create route table

Name	Route Table ID	Explicit subnet association	Main	VPC ID	Owner
rtb-0014a67d44ae4c6fa	subnet-0ebc265362a6a14c1	No		vpc-0c9c5f464f587667e ...	295613640041
rtb-08f3fb7ff4a74a4b	-	Yes		vpc-072155389e696a261 ...	295613640041
rtb-0a1a8ce3c883bc0ec	-	Yes		vpc-0c9c5f464f587667e ...	295613640041
rtb-0fa2ad2fa0af0bd6	-	Yes		vpc-009ce8eab0d7d0d14 ...	295613640041
rtb-f90ed287	-	Yes		vpc-956c3def padvpc1	295613640041

- **Name tag:** Provide a suitable name **VPC:** Select the relevant VPC from the dropdown menu

Click on **Create**

Route Tables > Create route table

Create route table

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Name tag	PSJBRT	<input type="button" value="Create"/>
VPC*	vpc-009ce8eab0d7d0d14	<input type="button" value="Cancel"/>
Filter by attributes		
* Required	vpc-0c9c5f464f587667e	PadVPC2
	vpc-956c3def	padvpc1
	vpc-072155389e696a261	Padtest
	vpc-009ce8eab0d7d0d14	VPCJB

- A Route table is created. Click on **Close**

[Route Tables](#) > Create route table

Create route table

The following Route Table was created:

Route Table ID rtb-05c4acb253a26173c

Close

- VPC Dashboard >> Route Tables >> Select the newly created route table

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

Name	Route Table ID	Explicit subnet association	Main	VPC ID	Owner
rtb-00f4a67d44ae4c6fa	subnet-0ebc265362a6a14c1	No	vpc-0c9c5f464f587667e ...	295613640041	
PSJBRT	rtb-05c4acb253a26173c	-	No	vpc-009ce8eab0d7d0d14 ...	295613640041
rtb-08f33fb7ff4a74a4b	-	Yes	vpc-072155389e696a261 ...	295613640041	
rtb-0a1a8ce3c83bc0ec	-	Yes	vpc-0c9c5f464f587667e ...	295613640041	
rtb-0fa2ad2fa0af06bd6	-	Yes	vpc-009ce8eab0d7d0d14 ...	295613640041	
rtb-f90ed287	-	Yes	vpc-956c3def padvpc1	295613640041	

Route Table: rtb-05c4acb253a26173c

Summary Routes Subnet Associations Route Propagation Tags

Route Table ID: rtb-05c4acb253a26173c
 Explicitly Associated with: -
 Owner: 295613640041

Main: No
 VPC: vpc-009ce8eab0d7d0d14 | VPCJB

- Click on **Routes** >> Edit 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

Name	Route Table ID	Explicit subnet association	Main	VPC ID	Owner
rtb-00f4a67d44ae4c6fa	subnet-0ebc265362a6a14c1	No	vpc-0c9c5f464f587667e ...	295613640041	
PSJBRT	rtb-05c4acb253a26173c	-	No	vpc-009ce8eab0d7d0d14 ...	295613640041
rtb-08f33fb7ff4a74a4b	-	Yes	vpc-072155389e696a261 ...	295613640041	
rtb-0a1a8ce3c83bc0ec	-	Yes	vpc-0c9c5f464f587667e ...	295613640041	
rtb-0fa2ad2fa0af06bd6	-	Yes	vpc-009ce8eab0d7d0d14 ...	295613640041	
rtb-f90ed287	-	Yes	vpc-956c3def padvpc1	295613640041	

Route Table: rtb-05c4acb253a26173c

Summary **Routes** Subnet Associations Route Propagation Tags

Edit routes

- Click on **Add route**

Route Tables > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No

Add route

* Required

Cancel **Save routes**

- **Destination:** Select **0.0.0.0/0** from the dropdown menu >> **Target:** New internet gateway from the dropdown menu >> Click on **Save routes**

Route Tables > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	igw-		No

Add route

* Required

Cancel **Save routes**

Route Tables > Edit routes

Edit routes

Routes successfully edited

Close

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	igw-056ad980e6eb601d3	active	No

- **Select the new Route table >> Subnet Associations >> Edit subnet associations**

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

Create route table Actions

Filter by tags and attributes or search by keyword

Name	Route Table ID	Explicit subnet association	Main	VPC ID	Owner
PSJBRT	rtb-05c4acb253a26173c	-	No	vpc-009ce8eb0d7d0d14...	295613640041
	rtb-08f33fb7ff4a74a4b	-	Yes	vpc-072155389e696a261...	295613640041
	rtb-0a1a8ce3c883bc0ec	-	Yes	vpc-0c9c5f464f587667e...	295613640041
	rtb-0fa2ad2fa0af06bd6	-	Yes	vpc-009ce8eb0d7d0d14...	295613640041
	rtb-f90ed287	-	Yes	vpc-956c3def padvpc1	295613640041

View All routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	igw-056ad980e6eb601d3	active	No

Route Table: rtb-05c4acb253a26173c

Summary Routes **Subnet Associations** Route Propagation Tags

Edit subnet associations

- Select the suitable **Public subnet** >> Click on **Save**. Subnet gets associated with the route table.

Route Tables > Edit subnet associations

Edit subnet associations

Subnet ID	IPv4 CIDR	Current Route Table
subnet-0a6519810dd276836 PublicSub...	10.0.0.0/24	Main

* Required

Cancel **Save**

DHCP Options Sets
Elastic IPs
Endpoints
Endpoint Services
NAT Gateways
Peering Connections
Security

Create route table Actions

Name	Route Table ID	Explicit subnet association	Main	VPC ID	Owner
rtb-00f4a67d4ae4c6fa	subnet-0ebc265362a6a14c1	No	vpc-0cb5f464f587667e ...	295613640041	
PSJBRT	rtb-05c4acb253a26173c	subnet-0a6519810dd276836	No	vpc-009ce8eab0d7d0d14 ...	295613640041
rtb-08f33fb7ff4a74a4b	-	Yes	vpc-072155389e696a261 ...	295613640041	
rtb-0a1a8ce3c883bc0ec	-	Yes	vpc-0cb5f464f587667e ...	295613640041	

1.3 Creation of a Private Subnet

- In the VPC Dashboard click on **Subnets**

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set	Main Route table
padvpc1	vpc-956c3def	available	172.31.0.0/16	-	dopt-e40dff9e	rtb-f90ed287
PadVPC2	vpc-0cb5f464f587667e	available	10.0.0.0/16	-	dopt-e40dff9e	rtb-0a1a8ce3c883bc0ec
Padtest	vpc-072155389e696a261	available	10.0.0.0/16	-	dopt-e40dff9e	rtb-08f33fb7ff4a74a4b
VPCJB	vpc-009ce8eab0d7d0d14	available	10.0.0.0/16	-	dopt-e40dff9e	rtb-0fa2ad2fa0fa06bd6

- In the subsequent screen click on **Create subnet**

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR
padsubnet1	subnet-08c3828d2d15ce4ac	available	vpc-072155389e696a261 ...	10.0.1.0/24	251	-
Public subnet	subnet-0ebc265362a6a14c1	available	vpc-0cb5f464f587667e ...	10.0.0.0/24	250	-
	subnet-1d581023	available	vpc-956c3def padvpc1	172.31.48.0/20	4091	-
	subnet-33a0747e	available	vpc-956c3def padvpc1	172.31.16.0/20	4091	-
	subnet-02ee724	available	vpc-0cb5f464f587667e ...	172.31.22.0/20	4091	-

Name tag: Provide a name suggesting that it is a Private subnet >> **VPC:** Select the VPC from the dropdown menu >> **IPv4 CIDR block:** Provide an address different from the Public IP Eg.10.0.1.0/24 >> **Create.** A private subnet is created. Click on **Close**

Subnets > Create subnet

Create 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	PrivateSubnetJB		
VPC*	vpc-009ce8eb0d7d0d14		
VPC CIDRs	CIDR	Status	Status Reason
	10.0.0.0/16	associated	
Availability Zone	No preference		
IPv4 CIDR block*	10.0.1.0/24		

* Required

Create

Subnets > Create subnet

Create subnet

The following Subnet was created:

Subnet ID: subnet-04705381b1870b5f0

Close

2. CREATION OF A NAT INSTANCE, JUMPBOX INSTANCE AND A FINAL INSTANCE

2.1 Creation of a NAT instance in the Public Subnet

➤ ‘console.aws.com’ >> Services >> EC2

console.aws.amazon.com/vpc/home?region=us-east-1#subnets:sort=SubnetId

aws Services Resource Groups

History Find a service by name or feature (for example, EC2, S3 or VM, storage)

Group A-Z

Compute Customer Enablement Analytics Business Applications

EC2 AWS IQ Support Athena Alexa for Business Amazon Chime

Lightsail

➤ Click on Launch Instance

New EC2 Experience Learn more

Launch Instance Connect Actions

EC2 Dashboard New Events Tags Reports

Name Instance ID Instance Type Availability Zone Instance State Status Checks Alarm Status Public DNS (IPv4) IPv4 Public IP IPv6 IPs

i-08d794b1b91616c7b0 t2.micro us-east-1c stopped None

- In the search window enter **amzn-ami-vpc-nat**

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review [Cancel and Exit](#)

Step 1: Choose an Amazon Machine Image (AMI)
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.

X

- **Community AMIs >> Select the first item in the listing (this is the latest)**

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group [Cancel and Exit](#)

Step 1: Choose an Amazon Machine Image (AMI)
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.

X

Quick Start (0)
My AMIs (0)
AWS Marketplace (4)
Community AMIs (46)
▼ Operating system

amzn-ami-vpc-nat-hvm-
2018.03.0.20181116-x86_64-ebs - ami-
00a9d4a05375b2763 Select
64-bit (x86)
Amazon Linux AMI 2018.03.0.20181116 x86_64
VPC HVM ebs
Root device type: ebs Virtualization type: hvm ENA
Enabled: Yes

- Select the second instance type **t.micro** >> **Configure Instance Details**

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review [Cancel and Exit](#)

Step 2: Choose an Instance Type
Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: All instance types Current generation ShowHide Columns

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.micro <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	t3a.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	General purpose	t3a.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes

Cancel Previous Review and Launch Next: Configure Instance Details

- **Network:** Select the correct VPC from the dropdown
- **Subnet:** Select the Public subnet from the dropdown
- **Auto-assign Public IP:** Enable >> Click on **Next: Add storage**

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

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 (i)
 Launch into Auto Scaling Group (i)

Purchasing option (i)
 Request Spot instances

Network (i)
vpc-009ce8ab0d7d0d14 | VPCJB (i) (i) Create new VPC

Subnet (i)
subnet-0a6519810dd276836 | PublicSubnetJB | us-1 (i) Create new subnet
 251 IP Addresses available

Auto-assign Public IP (i)
Enable

Placement group (i)
 Add instance to placement group

Capacity Reservation (i)
Open (i) (i) Create new Capacity Reservation

IAM role (i)
None (i) (i) Create new IAM role

Cancel Previous Review and Launch Next: Add Storage

- Click on **Next: Add Tags**

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 (i)	Device (i)	Snapshot (i)	Size (GiB) (i)	Volume Type (i)	IOPS (i)	Throughput (MB/s) (i)	Delete on Termination (i)	Encryption (i)
Root	/dev/xvda	snap-067424abc11f77a61	8	Magnetic (standard)	N/A	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Add New Volume

General Purpose (SSD) volumes provide the ability to burst to 3000 IOPS per volume, independent of volume size, to meet the performance needs of most applications and also deliver a consistent baseline of 3 IOPS/GiB. Set my root volume to General Purpose (SSD).

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

➤ Click on Add Tag

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

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
This resource currently has no tags					
Choose the Add tag button or click to add a Name tag . Make sure your IAM policy includes permissions to create tags.					
<input type="button" value="Add Tag"/> (Up to 50 tags maximum)					

➤ Key : Name >> Value: Eg. NAT INSTANCE >> Click on Next: Configure Security Group

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

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		NAT INSTANCE		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="button" value="Add another tag"/> (Up to 50 tags maximum)					

Cancel Previous Next: Configure Security Group

- Select Create new security group >> Security group name: Eg. NAT_SG >>
- Description: Eg. NAT_SG >> Click on Review and Launch

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

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:
 Description:

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	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.

Cancel Previous

➤ Click on **Launch**

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.

AMI Details

amzn2-ami-hvm-2.0.20191116.0-x86_64-gp2 - ami-00068cd7555f543d5
Amazon Linux 2 AMI 2.0.20191116.0 x86_64 HVM gp2
Root Device Type: ebs Virtualization type: hvm

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

Launch

- Choose an existing key pair (or Create a new key pair using Putty Gen)
- If available, Select an existing key pair from the dropdown menu >> **Launch Instances**

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair
Select a key pair
PadKeyValuePair

I acknowledge that I have access to the selected private key file (PadKeyValuePair.pem), and that without this file, I won't be able to log into my instance.

Launch Instances

- A NAT instance has been created. Click on **View Instances**

Launch Status

Your instances are now launching
The following instance launches have been initiated: i-09db6a64a76e3fb5b [View launch log](#)

Get notified of estimated charges
Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instances
Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances. Click [View Instances](#) to monitor your instances' status. Once your instances are in the **running** state, you can [connect](#) to them from the Instances screen. [Find out](#) how to connect to your instances.

Here are some helpful resources to get you started

- How to connect to your Linux instance
- Amazon EC2 User Guide
- Learn about AWS Free Usage Tier
- Amazon EC2 Discussion Forum

While your instances are launching you can also

- Create status check alarms to be notified when these instances fail status checks. (Additional charges may apply)
- Create and attach additional EBS volumes (Additional charges may apply)
- Manage security groups

View Instances

2.2 Creation of a Jumpbox instance in the Public Subnet

➤ ‘console.aws.com’ >> Services >> EC2

The screenshot shows the AWS Management Console with the URL <https://console.aws.amazon.com/ec2/home?region=us-east-1#subnets:sort=SubnetId>. The 'Services' tab is selected in the top navigation bar. On the left sidebar, 'Compute' and 'EC2' are listed under 'Compute'. The 'EC2' link is highlighted with a red box. In the main content area, there are several service links: Customer Enablement, AWS IQ, Support, Analytics (Athena, EMR), Business Applications (Alexa for Business, Amazon Chime), and Lightsail.

➤ Click on Launch Instance

The screenshot shows the 'Launch Instance' page. The 'Launch Instance' button is highlighted with a red box. Below it, a table lists an instance: i-06d794bb6f5fb7b0, t2.micro, us-east-1c, stopped, None. The table has columns for Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, Alarm Status, Public DNS (IPv4), IPv4 Public IP, and IPv6 IPs.

➤ Select the first Amazon Linux 2 AMI instance

The screenshot shows the 'Step 1: Choose an Amazon Machine Image (AMI)' page. The '1. Choose AMI' tab is selected. A search bar at the top contains the placeholder 'Search for an AMI by entering a search term e.g. "Windows"'. Below it, a 'Quick Start' sidebar includes 'My AMIs', 'AWS Marketplace', 'Community AMIs', and a 'Free tier only' checkbox. The main list shows two entries: 'Amazon Linux 2 AMI (HVM, SSD Volume Type - ami-00068cd7555f543d5 (64-bit x86) / ami-035240afa0793cddb (64-bit Arm))' and 'Amazon Linux AMI 2018.03.0 (HVM, SSD Volume Type - ami-00eb20669e0990cb4)'. The first entry is highlighted with a red box. A 'Select' button is located to the right of each entry. A note indicates that the first entry is 'Free tier eligible'.

➤ Select the second instance type t.micro >> Configure Instance Details

The screenshot shows the 'Step 2: Choose an Instance Type' page. The '2. Choose Instance Type' tab is selected. A note states: 'Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications.' Below this, a table lists various instance types. The 't2.micro' row is highlighted with a red box. The table includes columns for Family, Type, vCPUs, Memory (GiB), Instance Storage (GB), EBS-Optimized Available, Network Performance, and IPv6 Support. At the bottom, there are 'Cancel', 'Previous', 'Review and Launch' (highlighted with a red box), and 'Next: Configure Instance Details' buttons.

- **Network:** Select the correct VPC from the dropdown
- **Subnet:** Select the Public subnet from the dropdown
- **Auto-assign Public IP:** Enable >> Click on **Next: Add storage**

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

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 i
1 Launch into Auto Scaling Group i

Purchasing option i
 Request Spot instances

Network i
vpc-009ce8ab0d7d0d14 | VPCJB C Create new VPC

Subnet i
subnet-0a6519810dd276836 | PublicSubnetJB | us-▼ Create new subnet
251 IP Addresses available

Auto-assign Public IP i
 Enable ▼

Placement group i
 Add instance to placement group

Capacity Reservation i
Open C Create new Capacity Reservation

IAM role i
None C Create new IAM role

Cancel Previous Review and Launch Next: Add Storage

- Click on **Next: Add Tags**

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 (MiB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-067424abc11f77a61	8	Magnetic (standard)	N/A	N/A	<input checked="" type="checkbox"/>	Not Encrypted

[Add New Volume](#)

General Purpose (SSD) volumes provide the ability to burst to 3000 IOPS per volume, independent of volume size, to meet the performance needs of most applications and also deliver a consistent baseline of 3 IOPS/GiB. Set my root volume to General Purpose (SSD).

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

➤ Click on Add Tag

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

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
This resource currently has no tags					
Choose the Add tag button or click to add a Name tag . Make sure your IAM policy includes permissions to create tags.					
<input style="border: 2px solid red; padding: 2px; margin-right: 10px;" type="button" value="Add Tag"/> (Up to 50 tags maximum)					

➤ Key : Name >> Value: Eg. JUMPBOX >> Click on Next: Configure Security Group

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

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
<input type="text" value="Name"/>	<input type="text" value="JUMPBOX"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="X"/>	
<input type="button" value="Add another tag"/> (Up to 50 tags maximum)					
<input type="button" value="Cancel"/> <input type="button" value="Previous"/> <input style="background-color: blue; color: white; border: 2px solid red; border-radius: 5px; padding: 2px 10px;" type="button" value="Review and Launch"/> <input type="button" value="Next: Configure Security Group"/>					

- Select Create new security group >> Security group name: Eg. JB_SG >>
- Description: Eg. JB_SG >> Click on Review and Launch

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:	<input checked="" type="radio"/> Create a new security group	<input type="radio"/> Select an existing security group		
Security group name:	<input type="text" value="JB SG"/>			
Description:	<input type="text" value="JB SG"/>			
Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom	0.0.0.0/0
<input type="button" value="Add Rule"/> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> 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. </div>				
<input type="button" value="Cancel"/> <input type="button" value="Previous"/> <input style="background-color: blue; color: white; border: 2px solid red; border-radius: 5px; padding: 2px 10px;" type="button" value="Review and Launch"/>				

➤ Click on **Launch**

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.

⚠ Improve your instances' security. Your security group, JB_SG, 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](#)



Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-00068cd7555f543d5

Free tier eligible

Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras.

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

[Cancel](#)

[Previous](#)

Launch

- Select **Create a new key pair** from the dropdown menu
➤ **Key pair name:** Eg. JB_KEYPAIR >> **Download Key Pair**

Select an existing key pair or create a new key pair

X

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Create a new key pair

Key pair name

JB_KEYPAIR

Download Key Pair



You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

[Cancel](#)

Launch Instances

- Jumpbox instance has been created. Click on **View Instances**

Your instances are now launching
The following instance launches have been initiated: i-0719d1dd45ee40ea View launch log

Get notified of estimated charges
Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier)

How to connect to your instances
Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances. Click **View Instances** to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances screen. Find out how to connect to your instances.

Here are some helpful resources to get you started

- How to connect to your Linux instance
- Amazon EC2 User Guide
- Learn about AWS Free Usage Tier
- Amazon EC2 Discussion Forum

While your instances are launching you can also

- Create status check alarms to be notified when these instances fail status checks. (Additional charges may apply)
- Create and attach additional EBS volumes (Additional charges may apply)
- Manage security groups

View Instances

2.3 Creation of an EC2 instance (say F1) in the Private Subnet

- ‘console.aws.com’ >> Services >> EC2

console.aws.amazon.com/psc/home?region=us-east-1#subnets:sort=SubnetId

AWS Services Resource Groups

History VPC EC2 Console Home

Find a service by name or feature (example, EC2, S3 or VM, storage)

Compute Customer Enablement Analytics Business Applications

EC2 AWS IoT Athena Alexa for Business

Lightsail Support EMR Amazon Chime

Group A-Z

- Click on **Launch Instance**

New EC2 Experience Learn more

Launch Instance Connect Actions

EC2 Dashboard Events Tags Reports

Filter by tags and attributes or search by keyword

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs
i-06d794bb0f5f6c7b0	t2.micro	us-east-1c	running	None					

- Select the first **Amazon Linux 2 AMI** instance

Step 1: Choose an Amazon Machine Image (AMI)

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.

Cancel and Exit

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

Search for an AMI by entering a search term e.g. "Windows"

Quick Start

My AMIs	Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-00068cd7555f543d5 (64-bit x86) / ami-035240afa793cdedb (64-bit Arm)	Select
AWS Marketplace	Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras.	<input checked="" type="radio"/> 64-bit (x86) <input type="radio"/> 64-bit (Arm)
Community AMIs		
<input type="checkbox"/> Free tier only	Amazon Linux AMI 2018.03.0 (HVM), SSD Volume Type - ami-00eb20669e0990cb4	Select
	The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.	64-bit (x86)

➤ Select the second instance type t.micro >> **Configure Instance Details**

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: All instance types Current generation Show/Hide Columns

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
General purpose	t2.micro <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate	Yes
General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
General purpose	t3a.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
General purpose	t3a.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes

Cancel Previous Review and Launch Next: Configure Instance Details

- **Network:** Select the correct VPC from the dropdown
- **Subnet:** Select the **Private subnet** from the dropdown
- Click on **Next: Add storage**

Step 3: Configure Instance Details

No default VPC found. Select another VPC, or [create a new default VPC](#).

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-009ce8eab0d7d0d14 | VPCJB [Create new VPC](#)

Subnet subnet-082f4d04fb9cf3eeb | Private Subnet JB | us-east-1 [Create new subnet](#)

Auto-assign Public IP Use subnet setting (Disable)

Placement group [Add instance to placement group](#)

Cancel Previous Review and Launch Next: Add Storage

- Click on **Next: Add Tags**

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/xvda	snap-020ec4f43b42c0023	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

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

- Click on Add Tag >> Key: Name >> Value: Eg. Fl >> Next: Configure Security Group

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
This resource currently has no tags					
Choose the Add tag button or click to add a Name tag . Make sure your IAM policy includes permissions to create tags.					
Add Tag (Up to 50 tags maximum)					

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	Fl	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<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**

- Select Create a new security group >> Security group name: Eg. Fl_SG >>
➤ Description: Eg.Fl_SG >> Review and Launch

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.

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom	0.0.0.0/0
e.g. SSH for Admin Desktop				
Add Rule				

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.

Cancel **Previous** **Review and Launch**

- Click on Launch

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.

⚠ Improve your instances' security. Your security group, Fl_SG, 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

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-00068cd7555f543d5
Free tier eligible
Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras.
Root Device Type: ebs Virtualization type: hvm

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
Standard	1	1	2	10	No	Standard

Edit AMI **Cancel** **Previous** **Launch**

- Select **Choose and existing key pair** >> **JB_KEYPAIR** (your jumpbox key pair) >> **Launch Instances** and a new instance is created in the Private subnet

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair
Select a key pair
JB_KEYPAIR

I acknowledge that I have access to the selected private key file (JB_KEYPAIR.pem), and that without this file, I won't be able to log into my instance.

Cancel Launch Instances

- **VPC Dashboard >> Route Tables >> Create route table**

VPC Dashboard

Create route table

Name	Route Table ID	Explicit subnet associations	Edge associations	Main	VP
PUBJBRT	rtb-05c4acb253a26173c	subnet-0a6519810dd276836	-	No	vpc
main RT	rtb-0fa2ad2fa0af06bd6	-	-	Yes	vpc

Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways

- **Name tag: Eg.PVTJBRT >> VPC: Select the required VPC from the dropdown menu >> Create**

Route Tables > Create route table

Create route table

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Name tag PVTJBRT

VPC* vpc-009ce8eab0d7d0d14

* Required Cancel Create

- **The route table for the Private subnet is created >> Close**

Route Tables > Create route table

Create route table

✓ The following Route Table was created:

Route Table ID rtb-0f9e4623709414c2b

Close

Route tables >> Select the newly created Private route table >> Routes >> Edit 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

Name	Route Table ID	Explicit subnet associations	Edge associations	Main	VP
PUBJBRT	rtb-05c4acb253a26173c	subnet-0a6519810dd276836	-	No	vpc
PVTJBRT	rtb-0f9e4623709414c2b	-	-	No	vpc
main RT	rtb-0fa2ad2fa0af06bd6	-	-	Yes	vpc

Route Table: rtb-0f9e4623709414c2b
Summary Routes Subnet Associations Edge Associations Route Propagation Tags

Edit routes

- Add Route >> Destination: 0.0.0.0/0 >> Target: Select Instance from the dropdown and select the NAT instance >> Save routes. Route is edited >> Close

Route Tables > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	i-0caec06ccbf621745		No

* Required **Add route** **Save routes**

Route Tables > Edit routes

Edit routes

✓ Routes successfully edited

Close

- Subnets >> Select Private Subnet >> Route Table >> Edit route table association

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

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR
PublicSubnetJB	subnet-0a6519810dd276836	available	vpc-009ce8ab0d7d0d14 VPCJB	10.0.0.0/24	249	-
Private Subnet JB	subnet-082f4d04fb9cf3eeb	available	vpc-009ce8ab0d7d0d14 VPCJB	10.0.2.0/24	250	-

Subnet: subnet-082f4d04fb9cf3eeb
Description Flow Logs **Route Table** Network ACL Tags Sharing

Edit route table association

Route Table: rtb-0fa2ad2fa0af06bd6 | main RT

- **Subnet ID:** Select the Private Subnet ID >> **Route Table ID** >> Select the Private Route table ID from the dropdown menu >> **Save** >> Route table association for the private subnet is edited >> **Close**

Subnets > Edit route table association

Edit route table association

Subnet ID	subnet-082f4d04fb9cf3eeb
Route Table ID*	rtb-0fa2ad2fa0af06bd6
<input type="button" value="Cancel"/> <input type="button" value="Save"/>	

Route table ID **Route table name** **VPC ID**

Route table ID	Route table name	VPC ID
rtb-0f9e4623709414c2b	PVTJBRT	vpc-009ce8eab0d7d0d14
rtb-0fa2ad2fa0af06bd6	main RT	vpc-009ce8eab0d7d0d14
rtb-05c4acb253a26173c	PUBJBR	vpc-009ce8eab0d7d0d14

Subnets > Edit route table association

Edit route table association

Successfully edited route table association

3. CREATING/EDITING SECURITY GROUPS

Instances >> Select the **instance connected to the Private Subnet**, say FI, >> Click on the **Security group**, say, FI_SG

The screenshot shows the AWS EC2 Instances page. On the left sidebar, under the 'INSTANCES' section, the 'Instances' link is highlighted with a red box. In the main content area, a table lists four instances: FI, JUMPCBOX, NAT, and another FI instance. The second FI instance is selected, indicated by a blue outline. The 'Security groups' column for this instance shows 'FI_SG'. A red box highlights the 'FI_SG' entry. Below the table, detailed information for the selected instance is shown, including its private IP (10.0.2.213), secondary private IPs, VPC ID (vpc-009ce8eab0d7d0d14), and AMI ID (amzn2-ami-hvm-2.0.20191116-x86_64-gp2). The 'Scheduled events' section indicates 'No scheduled events'.

➤ Click on Inbound rules >> Edit

New EC2 Experience [Learn more](#)

Create Security Group Actions ▾

Group ID : sg-054a1693597a7b608 Add filter

Name	Group ID	Group Name	VPC ID	Owner	Description
FI_SG	sg-054a1693597a7b608	FI_SG	vpc-009ce8eab0d7d0d14	295613640041	FI_SG

Security Group: sg-054a1693597a7b608

Description **Inbound** Outbound Tags

Edit

INSTANCES Instances Instance Types Launch Templates New Spot Requests Savings Plans Reserved Instances Dedicated Hosts Scheduled Instances Capacity Reservations IMAGES AMIs Bundle Tasks

➤ Source: Type Sg and select the security group of the jumpbox from the dropdown menu >> Save

Edit inbound rules

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom	SG

Add Rule

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

sg-04ad135e1aeb690e9 - NAT SG
sg-054a1693597a7b608 - FI_SG
sg-0afa2057b2f2a1084 - JB_SG

Cancel **Save**

➤ Instances >> NAT instance >> NAT SG

New EC2 Experience [Learn more](#)

Launch Instance Connect Actions ▾

Filter by tags and attributes or search by keyword

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)
JUMPBOX	i-0719d1dd445ee40ea	t2.micro	us-east-1e	stopped	None	None	ec2-54-158-212-24
NAT	i-0cae06ccbf621745	t2.micro	us-east-1e	running	Initializing	None	ec2-54-158-212-24
FI	i-0cc211a65e2207fb	t2.micro	us-east-1e	stopped	None	None	ec2-54-158-212-24

Private DNS: ip-10-0-0-179.ec2.internal Private IPs: 10.0.0.179 Availability zone: us-east-1e Security groups: **NAT SG**, view inbound rules, view outbound rules

Secondary private IPs: VPC ID: vpc-009ce8eab0d7d0d14 (VPCJB) Scheduled events: No scheduled events

AMI ID: amzn-ami-vpc-nat-hvm-2018.03.0.20181116-x86_64-eks (ami-00a9d4a05375b2763)

INSTANCES Instances Instance Types Launch Templates New Spot Requests Savings Plans Reserved Instances Dedicated Hosts Scheduled Instances Capacity Reservations IMAGES AMIs Bundle Tasks

➤ Click on Inbound rules >> Edit

The screenshot shows the AWS EC2 interface under the 'Security Groups' section. A security group named 'NAT SG' is selected. The 'Inbound' tab is active, and the 'Edit' button is highlighted with a red box.

➤ Type: All traffic >> Source: Type Sg and select the security group of the Final Instance (FI) from the dropdown menu >> Save

The screenshot shows the 'Edit inbound rules' dialog box. The 'Source' field is populated with 'sg-054a1693597a7b608'. The 'Save' button is highlighted with a red box.

➤ NAT Instance >> Networking >> Change Source/Dest. Check >> Yes, Disable

The screenshot shows the AWS EC2 interface under the 'Instances' section. A context menu is open over the 'NAT' instance, with the 'Change Source/Dest. Check' option highlighted with a red box. Below, the 'Enable Source/Destination Check' dialog box is displayed, showing the instance details and a 'Yes, Disable' button highlighted with a red box.

4. COPYING THE PRIVATE KEY TO THE JUMPBOX INSTANCE AND CONNECTING TO JUMPBOX IN THE PUBLIC SUBNET AND FINAL INSTANCE IN THE PRIVATE SUBNET

- Copy the Private key pair, say, 'JB_JB_KEYPAIR.pem' to the Jumpbox instance by typing the command in the windows command prompt as shown in the example below:

```
scp -i JB_KEYPAIR.pem JB_KEYPAIR.pem ec2-user@ec2-3-83-18-78.compute-1.amazonaws.com:JB_KEYPAIR.pem (Use your filepath, key pair file name and the public ip address of your jumpbox instance)
```

- Connect to the jumpbox instance by typing the command in the windows command prompt as shown in the example below:

```
ssh -i "JB_KEYPAIR.pem" ec2-user@ec2-3-83-18-78.compute-1.amazonaws.com (Use your key pair file name and the public ip address of your jumpbox instance)
```

- Change the permission of the key pair file by typing the command in the windows command prompt as shown in the example below:

```
chmod 400 JB_KEYPAIR.pem (Use your key pair file name)
```

- Connect to the Final instance (say, F1) by typing the command in the windows command prompt as shown in the example below:

```
ssh -i "JB_KEYPAIR.pem" ec2-user@10.0.2.213
```

The screenshot shows a Windows Command Prompt window titled 'ec2-user@ip-10-0-2-213:~'. The window displays the following terminal session:

```
C:\>scp -i JB_KEYPAIR.pem JB_KEYPAIR.pem ec2-user@ec2-3-83-18-78.compute-1.amazonaws.com:JB_KEYPAIR.pem
JB_KEYPAIR.pem
100% 1692 15.3KB/s 00:00

C:\>ssh -i "JB_KEYPAIR.pem" ec2-user@ec2-3-83-18-78.compute-1.amazonaws.com
Last login: Sun Dec 8 20:15:46 2019 from ip-10-0-0-204.ec2.internal

[ec2-user@ip-10-0-0-204 ~]$ chmod 400 JB_KEYPAIR.pem
[ec2-user@ip-10-0-0-204 ~]$ ssh -i "JB_KEYPAIR.pem" ec2-user@10.0.2.213
Last login: Sun Dec 8 20:14:07 2019 from ip-10-0-0-204.ec2.internal

[ec2-user@ip-10-0-2-213 ~]$ ping google.com
PING google.com (172.217.15.78) 56(84) bytes of data.
64 bytes from iad23s63-in-f14.1e100.net (172.217.15.78): icmp_seq=1 ttl=47 time=1.99 ms
64 bytes from iad23s63-in-f14.1e100.net (172.217.15.78): icmp_seq=2 ttl=47 time=3.34 ms
64 bytes from iad23s63-in-f14.1e100.net (172.217.15.78): icmp_seq=3 ttl=47 time=1.76 ms
64 bytes from iad23s63-in-f14.1e100.net (172.217.15.78): icmp_seq=4 ttl=47 time=1.66 ms
64 bytes from iad23s63-in-f14.1e100.net (172.217.15.78): icmp_seq=5 ttl=47 time=1.75 ms
```