

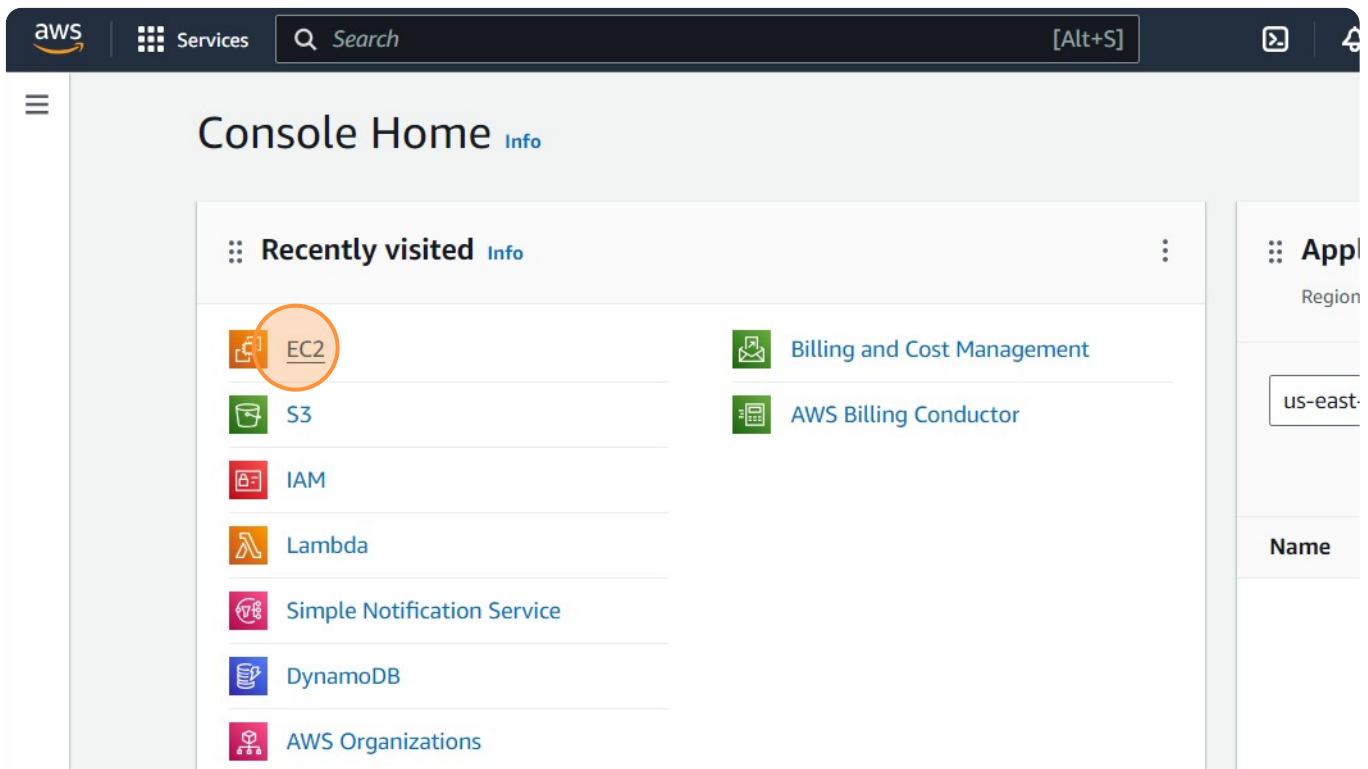
# Basic Labs

## EC2 Basic Lab

### Launching a new EC2 instance

- 1 Navigate to AWS Management Console.

- 2 Navigate to EC2 Service.



### 3 Click "Launch instance"

The screenshot shows the AWS EC2 Dashboard. On the left, there's a sidebar with navigation links like Events, Console-to-Code, Instances, Images, and Elastic Block Store. The main area displays a summary of resources: 0 Instances (running), 0 Auto Scaling Groups, 0 Dedicated Hosts, 1 Elastic IP, 1 Instance, 1 Key pair, 1 Load balancer, 0 Placement groups, 3 Security groups, 1 Snapshot, and 0 Volumes. Below this, there's a section titled "Launch instance" with a large orange circle highlighting the "Launch instance" button. To the right, there's a "Service health" section with a link to the AWS Health Dashboard and a note about the region being US East (N. Virginia). A vertical sidebar on the far right lists various AWS services with their names partially visible.

### 4 Enter name of instance to be created.

#### Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

##### Name and tags Info

Name

e.g. My Web Server

Add additional tags

##### ▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

5

Select an Amazon Machine Image (AMI) based on the requirements.

Search our full catalog including 1000s of application and OS images

My AMIs    Quick Start

Amazon Linux    macOS    Ubuntu    Windows    Red Hat    SUSE Li

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

**Amazon Linux 2023 AMI**

Free tier eligible

ami-0277155c3f0ab2930 (64-bit (x86), uefi-preferred) / ami-07ce5684ee3b5482c (64-bit (Arm), uefi)  
Virtualization: hvm   ENA enabled: true   Root device type: ebs

Description

Amazon Linux 2023 AMI 2023.3.20240131.0 x86\_64 HVM kernel-6.1

Architecture    Boot mode    AMI ID

6

Select an instance type that meets the needs of your application. I selected t2.micro.

Amazon Linux 2023 AMI 2023.3.20240131.0 x86\_64 HVM kernel-6.1

Architecture    Boot mode    AMI ID

64-bit (x86)    uefi-preferred    ami-0277155c3f0ab2930    Verified provider

**Instance type** [Info](#) | [Get advice](#)

Instance type

t2.micro    Free tier eligible

Family: t2    1 vCPU    1 GiB Memory    Current generation: true  
On-Demand Windows base pricing: 0.0162 USD per Hour  
On-Demand SUSE base pricing: 0.0116 USD per Hour  
On-Demand RHEL base pricing: 0.0716 USD per Hour  
On-Demand Linux base pricing: 0.0116 USD per Hour

All generations

Additional costs apply for AMIs with pre-installed software

Compare instance types

Number of instances [Info](#)

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.3.20240131.0 x86\_64 HVM kernel-6.1

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

**Free tier:** In your first 12 months, AWS Lambda includes 750 hours of free usage per month. After that, t2.micro is unavailable.

**Key pair (login)** [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Cancel

7

Select an existing key pair or create a new key pair. I selected an existing key pair "test" that I already created.

*Key pair is used to securely connect to the instance.*

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

Select

Q |

Proceed without a key pair (Not recommended) Default value

vockey  
Type: rsa

test  
Type: rsa  
vpc-U289T69e56Z6447a7

Subnet [Info](#)  
No preference (Default subnet in any availability zone)

Auto-assign public IP [Info](#)  
Enable

Firewall (security groups) [Info](#)  
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group

Select existing security group

We'll create a new security group called `Launch wizard` with the following rules.

▼ Summary

Number of instances [Info](#)  
1

Software Image (AMI)  
Amazon Linux 2023 AMI 2023.3.2...[read more](#)  
ami-0277155c3f0ab2930

Virtual server type (instance type)  
t2.micro

Firewall (security group)  
New security group

Storage (volumes)  
1 volume(s) - 8 GiB

**Free tier:** In your first month, includes 750 hours of t3.micro in the Region. t2.micro is unavailable.

Cancel

8

Click "Edit" on the right of Network settings to configure security group.

[Alt+S]

▼

C Create new key pair

Edit

▼ Summary

Number of instances [Info](#)  
1

Software Image (AMI)  
Amazon Linux 2023 AMI 2023.3.2...[read more](#)  
ami-0277155c3f0ab2930

Virtual server type (instance type)  
t2.micro

Control the traffic for your instance. Add rules to allow specific traffic to reach your

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

9

A VPC must be selected. I selected default VPC.

Key pair name - required

test

Create new key pair

▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-0289f69e3626447a7  
172.31.0.0/16

(default) [▼](#)

Subnet [Info](#)

No preference

Create new subnet [▼](#)

Auto-assign public IP [Info](#)

Enable

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

10

Now, we must create security group or select an existing security group. For creating security group, we must give it a name and description.

Auto-assign public IP [Info](#)

Enable

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group

Select existing security group

Security group name - required

launch-wizard-1

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and \_-:/()#@[]+=&;!\$\*

Description - required | Info

launch-wizard-1 created 2024-02-05T02:34:24.784Z

### Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0)

Remove

Type | Info

Protocol | Info

Port range | Info

11

Now, we must specify inbound security group rules to allow necessary traffic. Here, SSH is selected so that we can connect to the instance later.

255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and \_-:/()#@[]+=&;!\$\*

Description - required | Info

launch-wizard-1 created 2024-02-05T02:34:24.784Z

### Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0)

Remove

Type | Info

Protocol | Info

Port range | Info

ssh

TCP

22

Source type | Info

Source | Info

Description - optional | Info

Anywhere

Add CIDR, prefix list or security

e.g. SSH for admin desktop

0.0.0.0/0 X



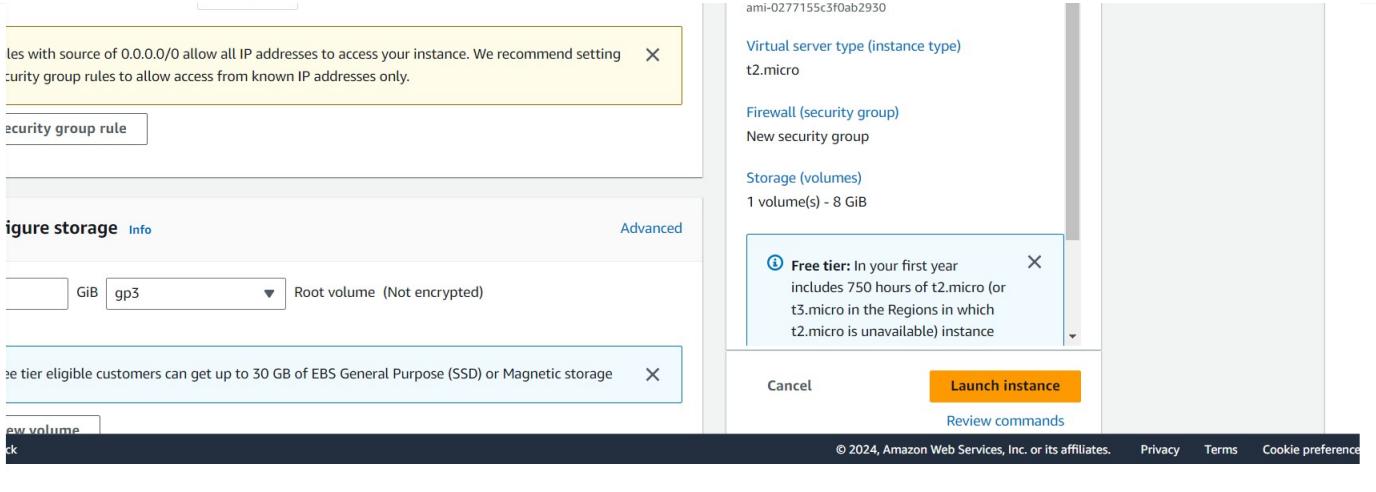
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only. X

12

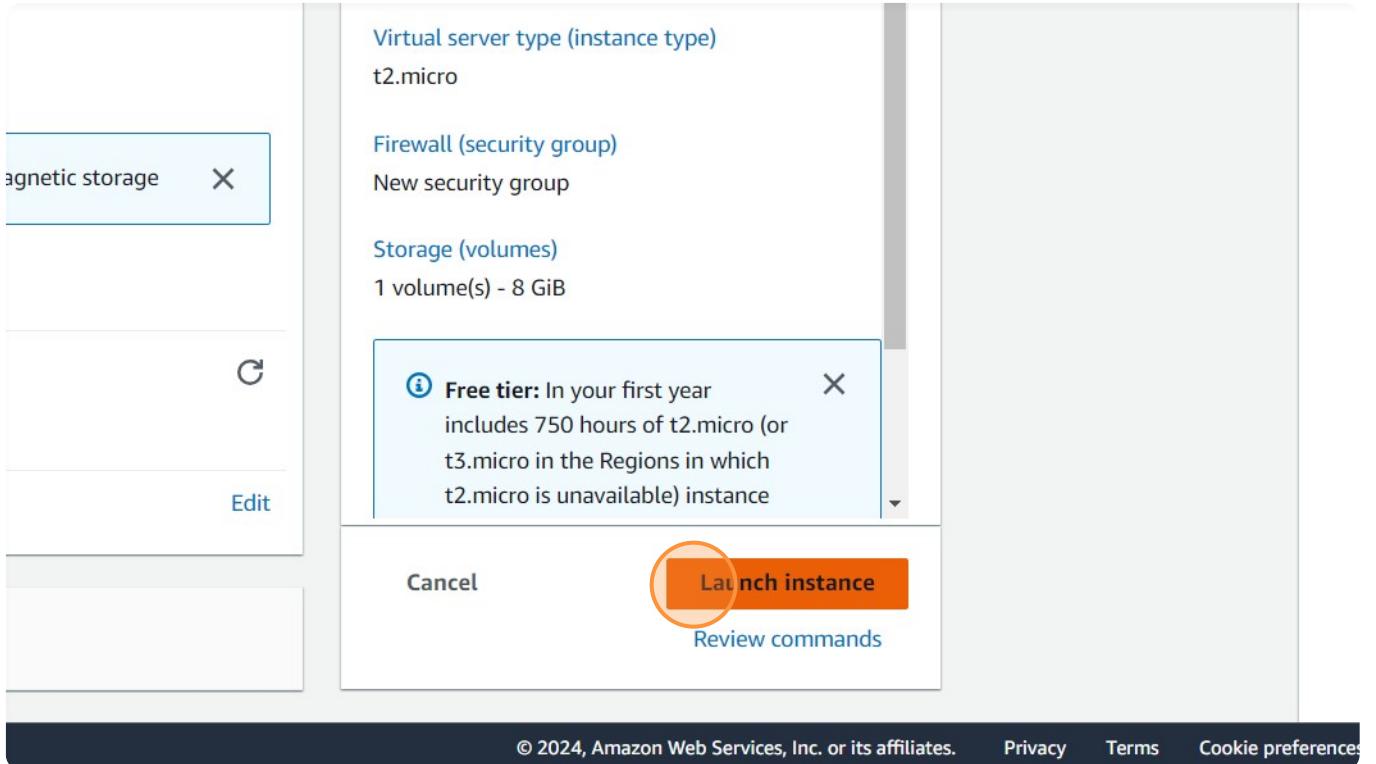
Provide the number of instances you want to launch.

In summary tab, you can view the summarized details of EC2 instance.

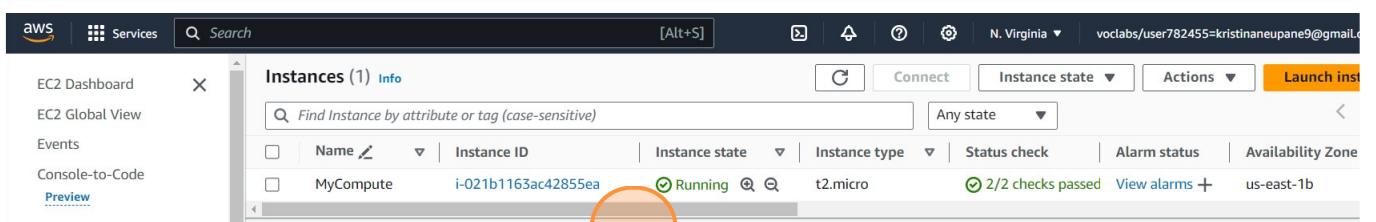
The screenshot shows the AWS EC2 instance creation process. On the left, the 'Inbound Security Group Rules' section is visible, containing one rule: 'Security group rule 1 (TCP, 22, 0.0.0.0/0)'. This rule has its 'Type' set to 'ssh', 'Protocol' set to 'TCP', and 'Port range' set to '22'. Its 'Source type' is 'Anywhere', and its 'Source' is '0.0.0.0/0'. An orange circle highlights the 'Anywhere' dropdown. Below this, a warning message states: '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.' On the right, the 'Summary' tab is active, showing the 'Number of instances' set to '1'. An orange circle highlights the '1' in the dropdown. Other details shown include the 'Software Image (AMI)' as 'Amazon Linux 2023 AMI 2023.3.2...' and a 'read more' link.



## 13 Click "Launch instance".



**14** Finally, an instance is launched and it is in "Running" state.



The screenshot shows the AWS CloudShell interface. On the left, there is a sidebar with navigation links: Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, New, Images (AMIs, AMI Catalog), and Elastic Block Store (with a circular icon). At the bottom of the sidebar are CloudShell and Feedback buttons. The main area has a header "Select an instance" and a footer with copyright information: © 2024, Amazon Web Services, Inc. or its affiliates., Privacy, and Terms.

## Allocate an Elastic IP address to the instance

15 Click Instance ID to view it's details.

The screenshot shows the AWS Instances page. The search bar at the top contains "Search" and "[Alt+S]". Below the search bar is a toolbar with icons for Filter, Connect, and a gear. The main area displays a table titled "Instances (1) Info". The table has columns: Name, Instance ID, Instance state, Instance type, and Status. A search bar below the table says "Find Instance by attribute or tag (case-sensitive)" and "Any state". The table shows one instance: "MyCompute" with Instance ID "i-021b1163ac42855ea". The Instance state is "Running" (green checkmark). The Instance type is "t2.micro". The Status column shows "2/". The "Instance ID" column is highlighted with an orange circle. Below the table, a message says "Select an instance".

16

Here, you can see there is no Elastic IP address associated with instance.

EC2 > Instances > i-021b1163ac42855ea

**Instance summary for i-021b1163ac42855ea (MyCompute) [Info](#)**

Updated less than a minute ago

Instance ID i-021b1163ac42855ea (MyCompute)	Public IPv4 address 34.228.32.79 <a href="#">[open address]</a>	Private IPv4 addresses 172.31.23.246
IPv6 address -	Instance state <span style="color: green;">Running</span>	Public IPv4 DNS ec2-34-228-32-79.compute-1.amazonaws.com <a href="#">[open address]</a>
Hostname type IP name: ip-172-31-23-246.ec2.internal	Private IP DNS name (IPv4 only) ip-172-31-23-246.ec2.internal	Elastic IP addresses -
Answer private resource DNS name IPv4 (A)	Instance type t2.micro	AWS Compute Optimizer finding <a href="#">Opt-in to AWS Compute Optimizer for recommendations.</a> <a href="#">[Learn more]</a>
Auto-assigned IP address 34.228.32.79 [Public IP]	VPC ID vpc-0289f69e3626447a7 <a href="#">[copy]</a>	Auto Scaling Group name -
IAM Role -	Subnet ID subnet-01104b0fef4a971d9 <a href="#">[copy]</a>	
IMDSv2 Required		

**Details** | Status and alarms [New](#) | Monitoring | Security | Networking | Storage | Tags

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

17

On the left sidebar, click Elastic IPs.

AMI Catalog

**Elastic Block Store**

- Volumes
- Snapshots
- Lifecycle Manager

**Network & Security**

- Security Groups
- Elastic IPs** (highlighted)
- Placement Groups
- Key Pairs
- Network Interfaces

**Load Balancing**

- Load Balancers
- Target Groups
- Trust Stores [New](#)

**Instance: i-021b1163ac42855ea (MyCompute)**

**Details** | Status and alarms [New](#) | Monitoring | Security | Networking

**Instance summary [Info](#)**

Instance ID i-021b1163ac42855ea (MyCompute)	Public IPv4 address 18.234.46.152 <a href="#">[open ad]</a>
IPv6 address -	Instance state <span style="color: green;">Running</span>

18

On top there is "Allocate Elastic IP address" button. Click it.

The screenshot shows the AWS Elastic IP Addresses page. On the left, there's a navigation sidebar with sections like Images, Elastic Block Store, Network & Security (with 'Elastic IPs' selected), Load Balancing, Auto Scaling, and CloudShell. The main area displays a table titled 'Elastic IP addresses (1/1)'. A single row is listed with the following details: Name (empty), Allocated IPv4 address (23.21.229.25), Type (Public IP), Allocation ID (eipalloc-0ea2f466091f38017), and Reverse DNS record (empty). At the top right of the table, there's a 'Actions' dropdown menu with an 'Allocate Elastic IP address' option. This option is highlighted with a large orange circle. Below the table, a modal window for the IP address 23.21.229.25 is open, showing tabs for 'Summary' and 'Tags', with 'Summary' selected.

19

The settings can be configured based on requirements. I kept it as default. Then, click "Allocate".

The screenshot shows the 'Allocate Elastic IP address' configuration dialog. It has several sections: 'Public IPv4 address pool' (Amazon's pool of IPv4 addresses, Public IPv4 address from BYOIP, Customer-owned pool from on-premises), 'Global static IP addresses' (AWS Global Accelerator), 'Tags - optional' (a note about tags and a 'Create accelerator' button), and 'Tags' (a section for adding new tags with a 'Add new tag' button and a note about the limit of 50 tags). At the bottom right, there are 'Cancel' and 'Allocate' buttons, with 'Allocate' being highlighted with a large orange circle.

20

Click "Associate this Elastic IP address" button to associate it with the required instance.

Elastic IP address allocated successfully.  
Elastic IP address 52.73.11.134

**Elastic IP addresses (1/1)**

Public IPv4 address: 52.73.11.134

Name	Allocated IPv4 addr...	Type	Allocation ID	Reverse DNS record
–	52.73.11.134	Public IP	eipalloc-0a29987b31c7999d5	–

View IP address usage and recommendations to release unused IPs with [Public IP insights](#).

**52.73.11.134**

[Summary](#) [Tags](#)

21

Choose an instance.

Elastic IP address: 52.73.11.134

Resource type  
Choose the type of resource with which to associate the Elastic IP address.

Instance

Network interface

**⚠️** If you associate an Elastic IP address with an instance that already has an Elastic IP address associated, the previously associated Elastic IP address will be disassociated, but the address will still be allocated to your account. [Learn more](#)

If no private IP address is specified, the Elastic IP address will be associated with the primary private IP address.

**Instance**

i-021b1163ac4285ea (MyCompute) - running

The private IP address with which to associate the Elastic IP address.

**Reassociation**  
Specify whether the Elastic IP address can be reassigned with a different resource if it is already associated with a resource.

Allow this Elastic IP address to be reassigned



CloudShell Feedback

Cancel

Associate

© 2024, Amazon Web Services, Inc. or its affiliates.

Privacy Terms

22

Click "Associate"

Elastic IP address: 52.73.11.134

Resource type  
Choose the type of resource with which to associate the Elastic IP address.

Instance

Network interface

**Important** If you associate an Elastic IP address with an instance that already has an Elastic IP address associated, the previously associated Elastic IP address will be disassociated, but the address will still be allocated to your account. [Learn more](#)

If no private IP address is specified, the Elastic IP address will be associated with the primary private IP address.

Instance

Private IP address  
The private IP address with which to associate the Elastic IP address.

Reassociation  
Specify whether the Elastic IP address can be reassigned to a different resource if it already associated with a resource.  
 Allow this Elastic IP address to be reassociated

Cancel Associate

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms

23

Now, you can see an elastic IP address is associated with the given instance.

Instances (1/1) Info

Find Instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
MyCompute	i-021b1163ac42855ea	Running	t2.micro	2/2 checks passed	<a href="#">View alarms</a>	us-east-1b	ec2-52-73-11-134. compute-1.amazonaws.com

Instance: i-021b1163ac42855ea (MyCompute)

Instance ID	Public IPv4 address	Private IPv4 addresses
i-021b1163ac42855ea (MyCompute)	52.73.11.134 <a href="#">open address</a>	172.31.23.246
IPv6 address	Instance state	Public IPv4 DNS
-	Running	ec2-52-73-11-134.compute-1.amazonaws.com <a href="#">open address</a>
Hostname type	Private IP DNS name (IPv4 only)	Elastic IP addresses
IP name: ip-172-31-23-246.ec2.internal	ip-172-31-23-246.ec2.internal	-
Answer private resource DNS name	Instance type	-
-	-	-

IPv4 (A)

Auto-assigned IP address

-

t2.micro

VPC ID

[vpc-0289f69e3626447a7](#)

52.73.11.134 [Public IP]

AWS Compute Optimizer finding

[Opt-in to AWS Compute Optimizer for recommendation](#)

s.

| Learn more

© 2024, Amazon Web Services, Inc. or its affiliates.

[Privacy](#)

[Terms](#)

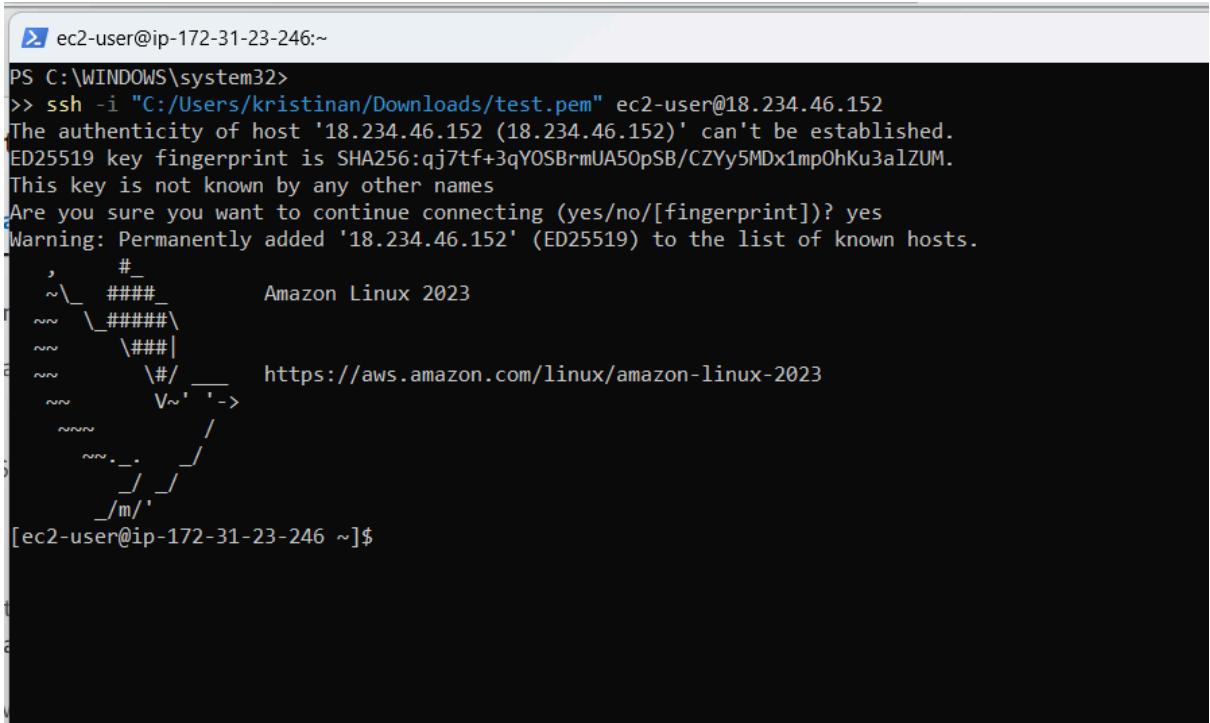
[Cookie preferences](#)

## Step to connect to instance via SSH

24 Open Powershell and type the SSH command with this structure:

```
ssh -i file.pem username@ip-address
```

Now, you are connected to an EC2 instance.



The screenshot shows a Windows Command Prompt window with the following text output:

```
PS C:\WINDOWS\system32>
>> ssh -i "C:/Users/kristinan/Downloads/test.pem" ec2-user@18.234.46.152
The authenticity of host '18.234.46.152 (18.234.46.152)' can't be established.
ED25519 key fingerprint is SHA256:qj7tf+3qYOSBrmUA50pSB/CZYy5MDx1mpOhKu3alZUM.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '18.234.46.152' (ED25519) to the list of known hosts.

,      #
~\_ #####
~~ \####\ Amazon Linux 2023
~~  \###|
~~   \##| https://aws.amazon.com/linux/amazon-linux-2023
~~    \#/  V~' '-'>
~~~   / 
~~~_. / 
~~~/_/ 
~~~/_m/ 
[ec2-user@ip-172-31-23-246 ~]$
```

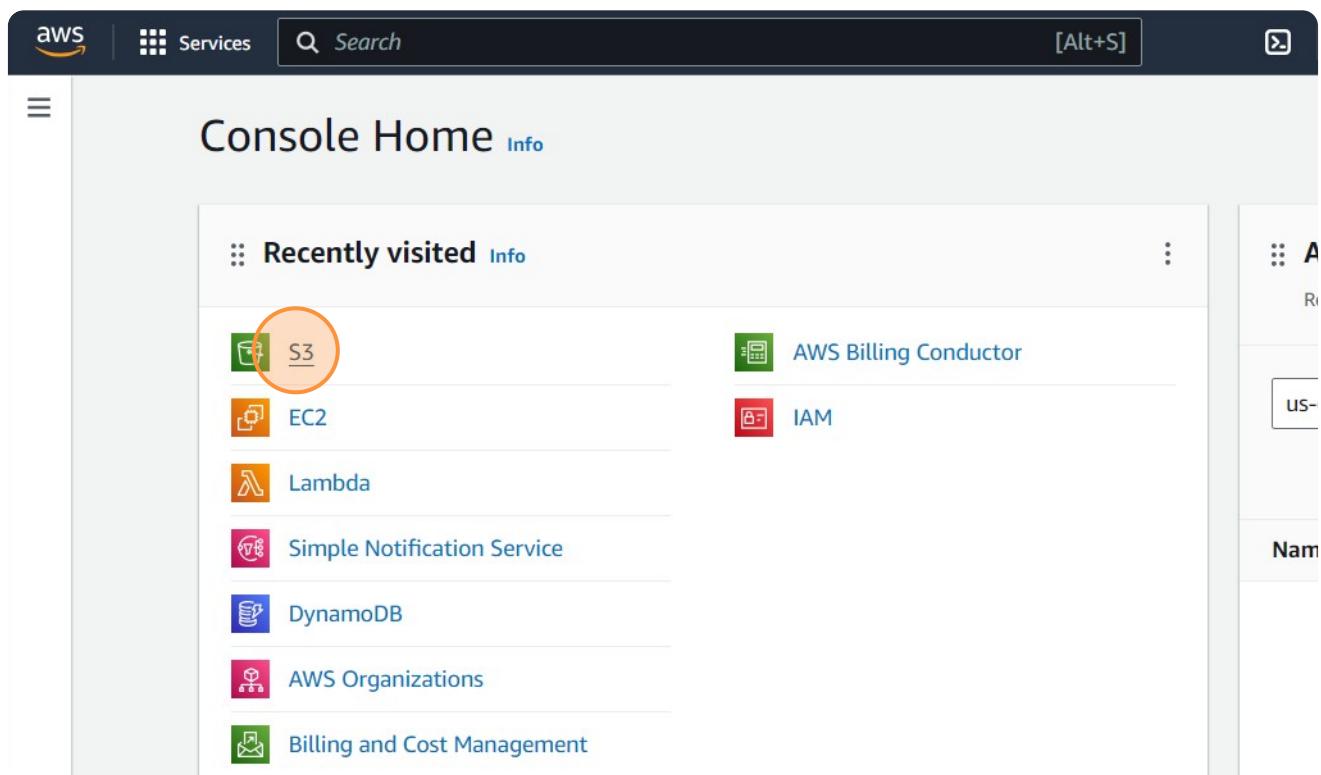
# S3 Storage Fundamentals Lab

Understanding how to use S3 for storing and managing data, learn about S3 security and permissions, and become familiar with S3's user interface.

## Steps to create bucket and upload file

- 1 Navigate to AWS Management Console

- 2 Navigate to "S3" service



3

Click "Create bucket"

The screenshot shows the Amazon S3 landing page. At the top right, there is a call-to-action box titled "Create a bucket" with the sub-instruction: "Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored." Below this, the "Create bucket" button is circled in red. The main content area features the heading "Amazon S3" and the sub-headline "Store and retrieve any amount of data from anywhere". A brief description of the service follows: "Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance." On the left, there's a section titled "How it works" with a video thumbnail titled "Introduction to Amazon S3". On the right, there are sections for "Pricing" and "Resources". The bottom of the page includes standard footer links like "Privacy", "Terms", and "Cookie preferences".

4

Choose the region for your bucket. I choosed "US East (N. Virginia) us-east-1".

The screenshot shows the "General configuration" page for creating a new AWS bucket. The "AWS Region" dropdown is set to "US East (N. Virginia) us-east-1", which is highlighted with a red circle. Below the dropdown, the "Bucket type" section offers two options: "General purpose" (selected) and "Directory - New". The "Bucket name" field contains "myawsbucket". A note at the bottom states: "Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming." There is also a section for "Copy settings from existing bucket - optional". The top navigation bar includes the AWS logo, "Services", a search bar, and other standard navigation links.

- 5 Enter a globally unique name for your bucket in the "Bucket name" field. I entered "kristina-bucket".

US East (N. Virginia) us-east-1

Bucket type | Info

General purpose  
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

Directory - New  
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name | Info

kristina-bucket

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

Copy settings from existing bucket - optional  
Only the bucket settings in the following configuration are copied.

Choose bucket

Format: s3://bucket/prefix

### Object Ownership [Info](#)

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object owner

- 6 Configure other features if needed. Click "Create bucket"

Default encryption [Info](#)  
Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type [Info](#)  
 Server-side encryption with Amazon S3 managed keys (SSE-S3)  
 Server-side encryption with AWS Key Management Service keys (SSE-KMS)  
 Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)  
Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the Storage tab of the [Amazon S3 pricing page](#).

Bucket Key  
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)  
 Disable  
 Enable

Advanced settings

After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Create bucket

- 7 Bucket "kristina-bucket" is successfully created. Click on name to view or edit bucket features.

The screenshot shows the AWS S3 console. At the top, a green banner indicates that the bucket "kristina-bucket" has been successfully created. Below the banner, the "Account snapshot" section is visible, featuring a storage lens for visibility into usage and activity trends. The "General purpose buckets" tab is selected, showing one bucket named "kristina-bucket". This bucket is located in the "US East (N. Virginia) us-east-1" region and was created on February 4, 2024, at 14:06:4. A search bar and filter options for Name, AWS Region, Access, and Creation date are present. The bucket name "kristina-bucket" is highlighted with an orange circle.

- 8 Click "Upload" to upload files or folders in bucket.

The screenshot shows the AWS S3 console on the "kristina-bucket" details page. The "Objects" tab is selected, displaying a table with no objects. The table headers are Name, Type, Last modified, Size, and Storage class. A large orange circle highlights the "Upload" button, which is located at the bottom center of the table area. The page also includes tabs for Properties, Permissions, Metrics, Management, and Access Points, along with standard AWS navigation and search tools.

9

Click "Add files"

The screenshot shows the AWS S3 'Upload' interface. At the top, there's a navigation bar with 'Services' and a search bar. Below it, the path 'Amazon S3 > Buckets > kristina-bucket > Upload' is visible. The main area is titled 'Upload' with a 'Info' link. A large dashed box contains the instruction 'Drag and drop files and folders you want to upload here, or choose Add files or Add folder.' Below this is a table titled 'Files and folders (0)' with a count of '(0)'. It has columns for 'Name', 'Folder', and 'Type'. A search bar 'Find by name' is at the top of the table. The message 'All files and folders in this table will be uploaded.' is displayed above the table. The 'Add files' button is highlighted with an orange circle. Below the table, a message says 'No files or folders' and 'You have not chosen any files or folders to upload.' At the bottom, there's a 'Destination' section with 'Info' and a table showing '1 Total, 40.3 KB'. The 'Upload' button is also highlighted with an orange circle.

10

Select file from your local machine and click "Upload".

This screenshot shows the 'Upload' interface after a file has been selected. The 'Files and folders' table now lists '1 Total, 40.3 KB' with one item: 'programmer.jpg' (image/jpeg). The 'Upload' button is highlighted with an orange circle. The 'Destination' section shows 's3://kristina-bucket'. There are sections for 'Permissions' and 'Properties'. The 'CloudShell' and 'Feedback' buttons are at the bottom.

11

Click name of file to view its details.

The information below will no longer be available after you navigate away from this page.

### Summary

Destination s3://kristina-bucket	Succeeded 1 file, 40.3 KB (100.00%)	Failed 0 fi
-------------------------------------	--	----------------

**Files and folders** (1 Total, 40.3 KB)

Name	Folder	Type	Size	Status	Error
programmer...	-	image/jpeg	40.3 KB	Succeeded	-

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates.

12

Here, you can see object details.

Search [Alt+S] X Global v vocabs/user782455=kristinaneupane9@gmail.com @ 6958-9852-66

Amazon S3 > Buckets > kristina-bucket > programmer.jpg

**programmer.jpg** [Info](#)

[Copy S3 URI](#) [Download](#) [Open](#) [Object actions](#)

[Properties](#) [Permissions](#) [Versions](#)

### Object overview

Owner	s3://kristina-bucket/programmer.jpg
AWS Region	arn:aws:s3:::kristina-bucket/programmer.jpg
Last modified	Entity tag (Etag)
February 17, 2024, 13:11:39 (UTC+05:45)	49db3f93e66f5c13df8705ffa7375bf
Size	Object URL
40.3 KB	<a href="https://kristina-bucket.s3.amazonaws.com/programmer.jpg">https://kristina-bucket.s3.amazonaws.com/programmer.jpg</a>
Type	
jpg	
Key	
programmer.jpg	

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

# Setting up bucket policies for access control

- 13 Click name of the bucket.

The screenshot shows the AWS S3 console interface. On the left, there's a sidebar with various links like Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, and Storage Lens. Below that is a Feature spotlight section. At the bottom of the sidebar is a CloudShell icon. The main area is titled "General purpose buckets (1) Info". It contains a search bar with "Find buckets by name" and a table with one row. The table has columns for "Name" and "AWS Region". The row for "kristina-bucket" is highlighted with an orange circle around the bucket name. The "AWS Region" column shows "US East (N. Virginia) us-east".

- 14 Click "Permissions"

The screenshot shows the "kristina-bucket" details page in the AWS S3 console. The top navigation bar includes a search bar, a CloudShell icon, and other navigation icons. The breadcrumb navigation shows "Amazon S3 > Buckets > kristina-bucket". The main title is "kristina-bucket Info". Below the title is a navigation bar with tabs: Objects (highlighted), Properties, Permissions (circled in orange), Metrics, Management, and Access Points. The "Permissions" tab is active. Under the "Permissions" tab, there's a sub-section titled "Objects (1) Info". It contains a table with one row and several buttons: Copy S3 URI, Copy URL, Download, Open, and Delete. A note below says "Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects and their permissions." There's also a search bar at the bottom with "Find objects by prefix".

15 Click "Edit" on the right of Block public access.

The screenshot shows the AWS S3 Permissions overview page. In the 'Block public access (bucket settings)' section, there is a note: 'Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases.' Below this note, there is a checkbox labeled 'Block all public access' with the value 'On'. To the right of this section, there is an 'Edit' button, which is circled in orange. Below this section, there is a 'Bucket policy' section with an 'Edit' and 'Delete' button.

16 Click this checkbox to allow public access.

- Buckets
- Access Grants
- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3
  
- Block Public Access settings for this account
  
- ▼ Storage Lens
  - Dashboards
  - Storage Lens groups
  - AWS Organizations settings

## Edit Block public access (bucket settings)

### Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases.

#### Block all public access

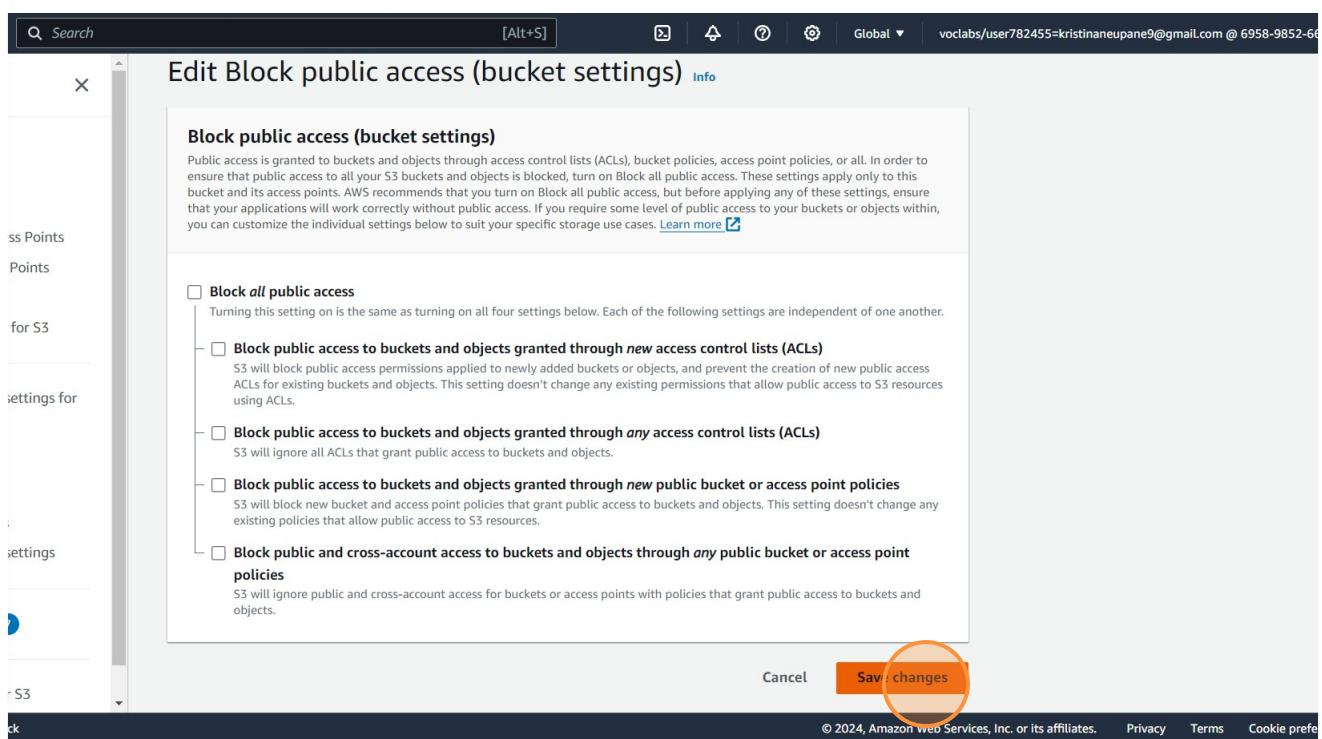
Turning this setting on is the same as turning on all four settings below. Each of the following settings applies to this bucket and its access points.

- Block public access to buckets and objects granted through new access control lists (ACLs)**  
S3 will block public access permissions applied to newly added buckets or objects. This setting doesn't change any existing public access permissions using ACLs.
- Block public access to buckets and objects granted through any access control list (ACL)**  
S3 will ignore all ACLs that grant public access to buckets and objects.
- Block public access to buckets and objects granted through new policies**

S3 will block new bucket and access point policies that grant public access to buckets or objects within the bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

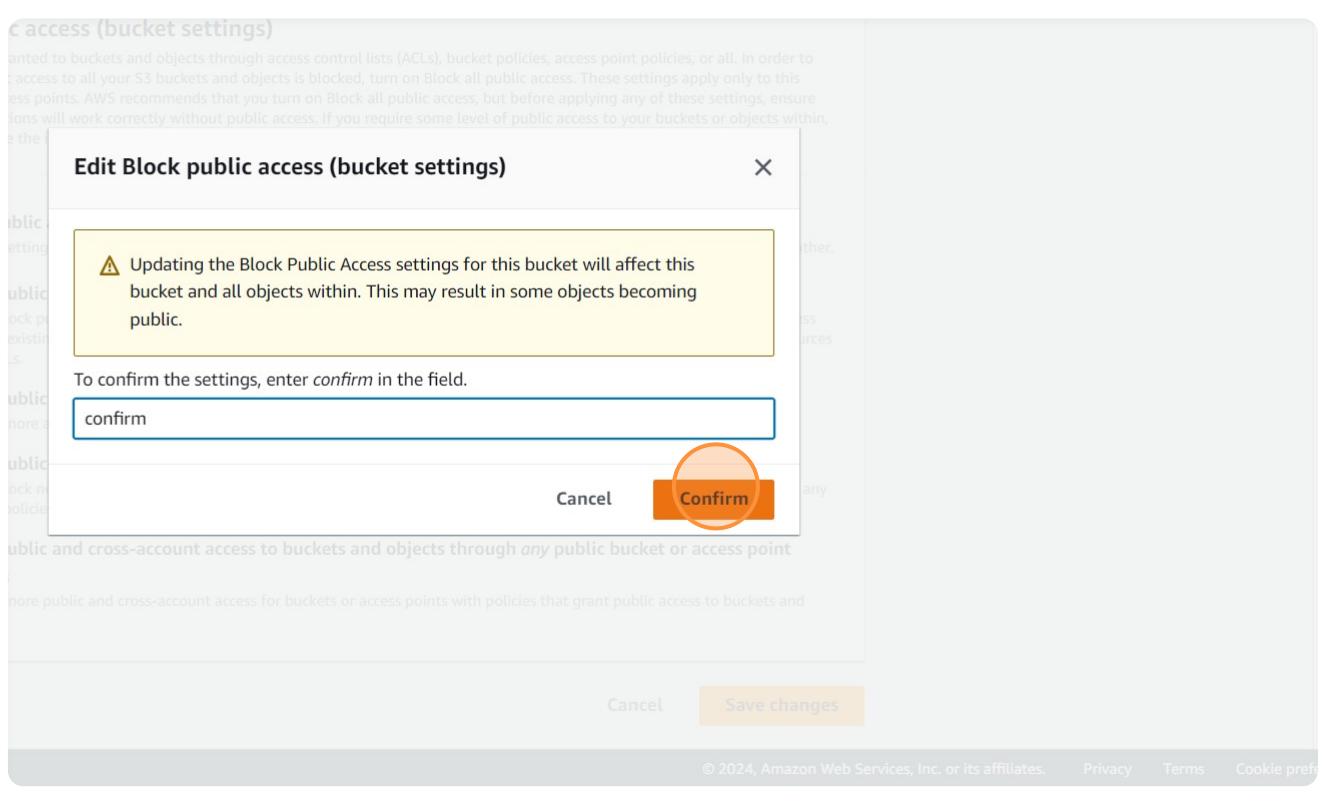
17

Click "Save changes"



18

To confirm the settings, enter "confirm" in the field and click "Confirm"



19

Click "Edit" on the right of Bucket Policy.

The screenshot shows the AWS S3 console. On the left, there's a sidebar with links like Buckets, Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Block Public Access settings for this account, Storage Lens, Dashboards, Storage Lens groups, AWS Organizations settings, Feature spotlight, Marketplace for S3, CloudShell, and Feedback. The main area has a green banner at the top stating 'Successfully edited Block Public Access settings for this bucket.' Below it, there's a section for 'Block all public access' which is currently 'Off'. Under 'Bucket policy', it says 'No policy to display.' There are 'Edit' and 'Delete' buttons. A large orange circle highlights the 'Edit' button. At the bottom, there's a footer with links for Privacy, Terms, and Cookie preferences.

20

Click "Add new statement"

The screenshot shows the 'Edit statement' section of the AWS S3 Bucket Policy. It displays a JSON policy with one statement. To the right, there's a panel titled 'Select a statement' with the sub-instruction 'Select an existing statement in the policy or add a new statement.' Below this is a button labeled '+ Add new statement' with a large orange circle around it. The footer of the page includes links for Privacy, Terms, and Cookie preferences.

- 21** Add a bucket policy to control access. I added policy to make recently uploaded file public.

The screenshot shows the AWS CloudShell interface with a "Bucket policy" editor. At the top, it says "Bucket ARN" followed by "arn:aws:s3:::kristina-bucket". Below that is a "Policy" section containing a JSON code block:

```
1▼ {
2  "Version": "2012-10-17",
3 ▼  "Statement": []
4 ▼    {
5      "Effect": "Allow",
6      "Principal": "*",
7      "Action": "s3:GetObject",
8      "Resource": "arn:aws:s3:::kristina-bucket/programmer.jpg"
9    }
10   ]
11 }
12 }
```

A large orange circle highlights the closing brace of the JSON object at line 11. At the bottom of the editor, there are buttons for "CloudShell" and "Feedback", and a copyright notice "© 2024, Amazon Web Services, Inc. or its affiliates.".

- 22** Click "Save changes"

The screenshot shows the AWS Lambda function configuration page. At the top, there is a search bar and a toolbar with various icons. The main area contains a JSON editor with the following code:

```
"Resource": "arn:aws:s3:::kristina-bucket/programmer.jpg"
}
```

To the right of the editor, there is a message: "Select an existing statement in the policy or add a new statement." Below this is a button labeled "+ Add new statement". Further down, there is a "dd new statement" button and a status bar indicating "Ln 11, Col 1" with "0 Errors: 0 Warnings: 0 Suggestions: 0". At the bottom right, there is a "Save changes" button, which is highlighted with a large orange circle. Other buttons at the bottom include "Cancel", "Preview external access", and links for "Privacy", "Terms", and "Cookie preferences".

## Accessing file through it's URL

23 Copy object URL which is under object properties.

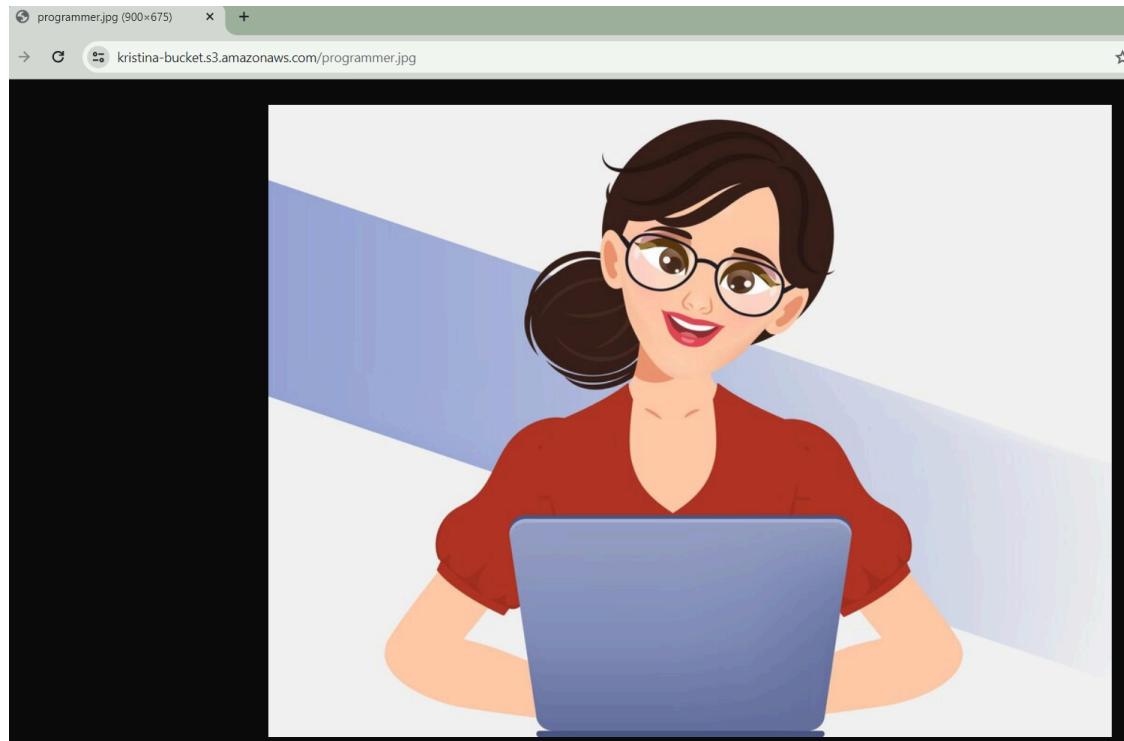
programmer.jpg [Info](#)

[Properties](#) [Permissions](#) [Versions](#)

**Object overview**

Owner	S3 URI
awslabsc0w6979644t1703210996	<a href="s3://kristina-bucket/programmer.jpg">s3://kristina-bucket/programmer.jpg</a>
AWS Region	Amazon Resource Name (ARN)
US East (N. Virginia) us-east-1	<a href="arn:aws:s3:::kristina-bucket/programmer.jpg">arn:aws:s3:::kristina-bucket/programmer.jpg</a>
Last modified	Entity tag (Etag)
February 17, 2024, 13:11:39 (UTC+05:45)	<a href="#">49db3f93e66f5c13df8705fffa7375bf</a>
Size	Object URL
40.3 KB	<a href="https://kristina-bucket.s3.amazonaws.com/programmer.jpg">https://kristina-bucket.s3.amazonaws.com/programmer.jpg</a>
Type	
jpg	
Key	
<a href="#">programmer.jpg</a>	

24 Now, paste that URL in a new tab. As a result, image inside bucket can be accessed publicly.

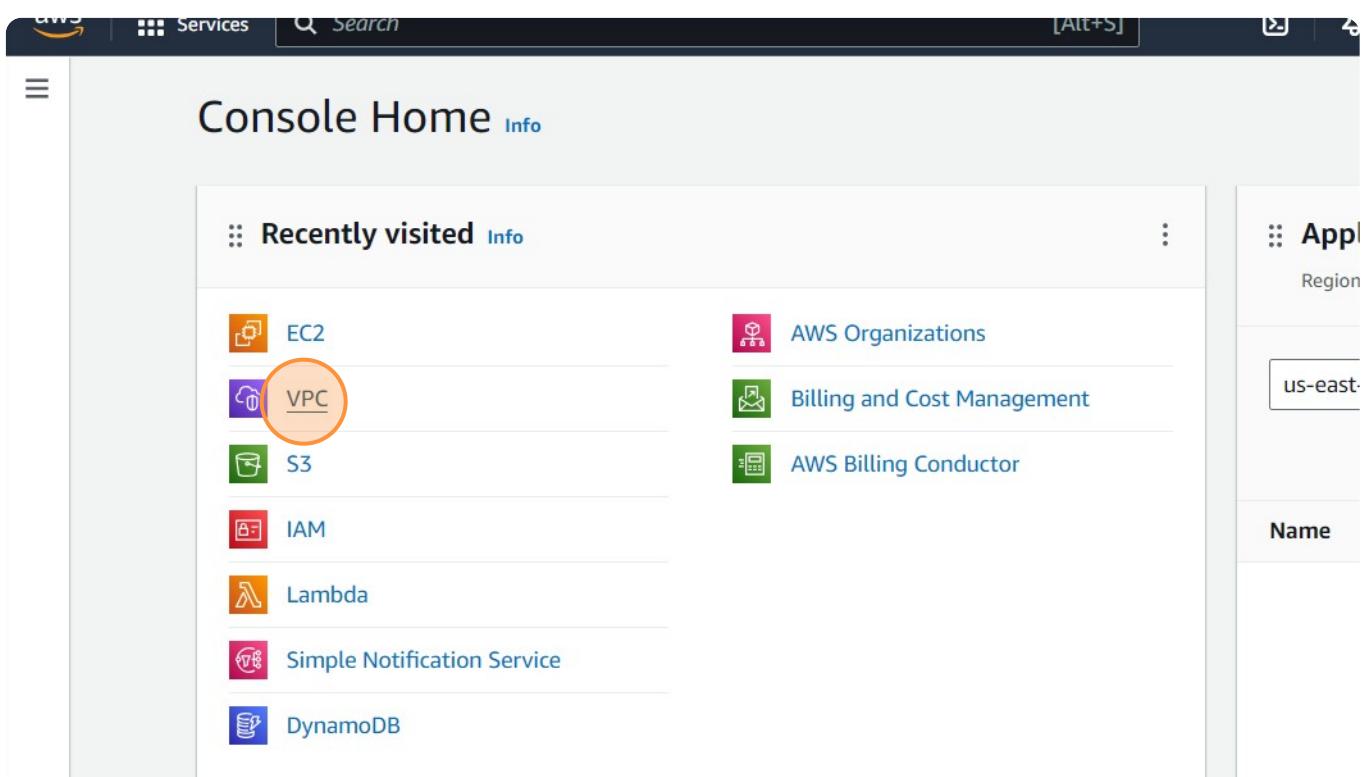


# VPC Configuration Lab

## Steps to Create VPC

- 1 Navigate to AWS Management Console.

- 2 Click "VPC"



- 3 Click "Create VPC"



The screenshot shows the AWS VPC dashboard. At the top, there are two buttons: "Create VPC" (highlighted with a red circle) and "Launch EC2 Instances". A note below says, "Note: Your instances will launch in the US East region." On the left, a sidebar titled "Filter by VPC:" has a dropdown menu "Select a VPC". Under "Virtual private cloud", there are several options: "Your VPCs", "Subnets", "Route tables", "Internet gateways", "Egress-only internet gateways", "Carrier gateways", and "DHCP option sets". The main area is titled "Resources by Region" and shows the following counts for the US East region: VPCs (1), Subnets (6), Route Tables (1), Internet Gateways (1), NAT Gateways (0), VPC Peering Connections (0), Network ACLs (0), and Security Groups (0). A "Refresh Resources" button is also present.

- 4 You can create only the VPC resource or the VPC and other networking resources. I created VPC only.

[VPC](#) > [Your VPCs](#) > [Create VPC](#)

## Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances. Mouse over a resource to

The screenshot shows the "Create VPC" configuration page. On the left, under "VPC settings", there is a section for "Resources to create" with two options: "VPC only" (selected, highlighted with a red circle) and "VPC and more". Below this, there is a "Name tag auto-generation" section with a checkbox "Auto-generate" checked and a text input field containing "project". At the bottom, there is an "IPv4 CIDR block" section with a note about determining starting IP and size using CIDR notation. On the right, under "Preview", there is a summary: "VPC [Show details](#)" followed by "Your AWS virtual network" and a text input field containing "project-vpc".

## 5 Provide name for your VPC.

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

### VPC settings

Resources to create [Info](#)

Create only the VPC resource or the VPC and other networking resources.

VPC only

VPC and more

Name tag - *optional*

Creates a tag with a key of 'Name' and a value that you specify.

my-vpc-01

IPv4 CIDR block [Info](#)

- IPv4 CIDR manual input
- IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.0.0.0/24

CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)

## 6 Specify IPv4 CIDR block.

Name tag - *optional*

Creates a tag with a key of 'Name' and a value that you specify.

my-vpc-1

IPv4 CIDR block [Info](#)

- IPv4 CIDR manual input
- IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.0.0.0/24

CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)

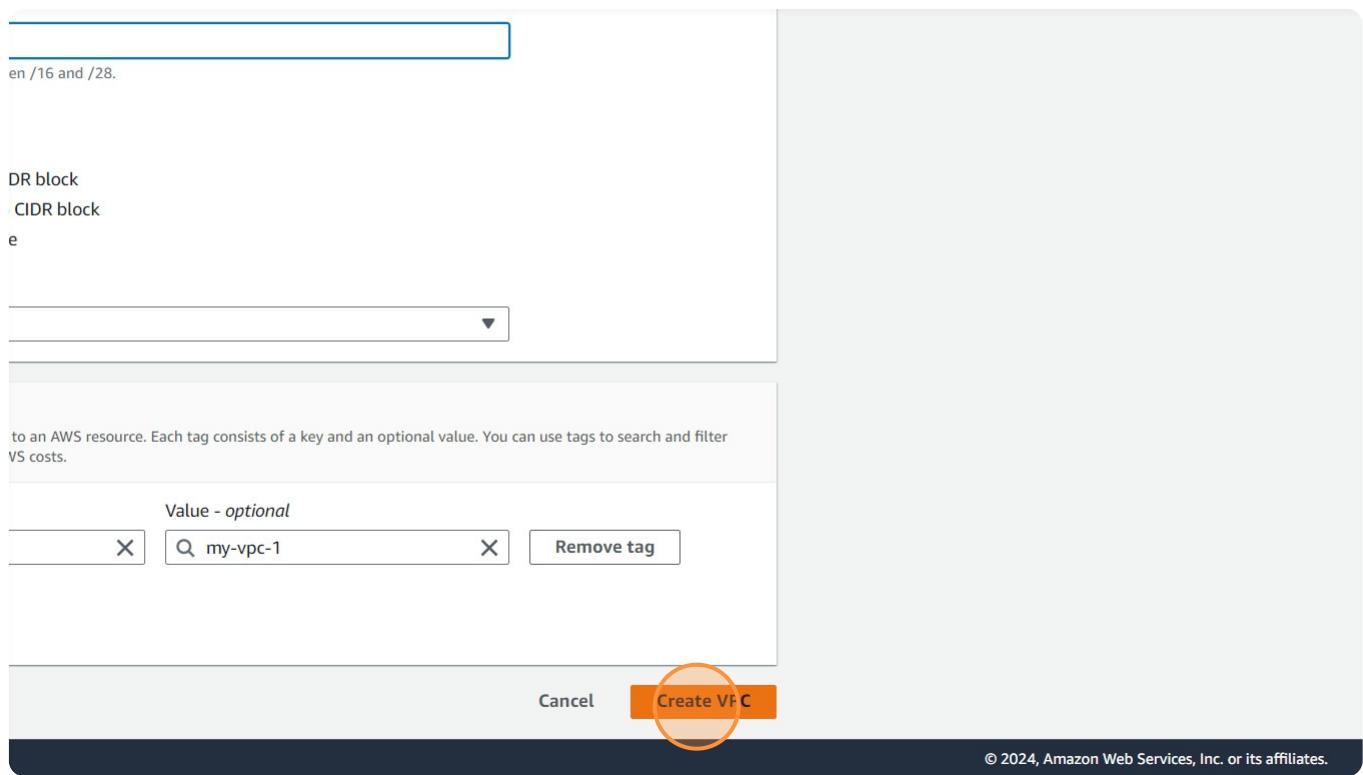
- No IPv6 CIDR block
- IPAM-allocated IPv6 CIDR block
- Amazon-provided IPv6 CIDR block
- IPv6 CIDR owned by me

Tenancy [Info](#)

Default

7

Click "Create VPC"



8

VPC is created successfully.

## Steps to add subnet to VPC

9

Click "Subnets" on left sidebar.

The screenshot shows the AWS VPC dashboard. On the left, there's a sidebar with 'VPC dashboard' and 'EC2 Global View'. Under 'Filter by VPC', there's a dropdown set to 'Select a VPC'. At the bottom, it says 'Virtual private cloud'. The main area shows a green success message: 'You successfully created vpc-085856ede292c0583 / my-vpc-1'. Below this, the breadcrumb navigation shows 'VPC > Your VPCs > vpc-085856ede292c0583'. The VPC ID 'vpc-085856ede292c0583 / my-vpc-1' is displayed prominently. At the bottom, there are 'Details' and 'Info' buttons.

Your VPCs	VPC ID	State
Subnets	vpc-085856ede292c0583	Available
Route tables	Tenancy	DHCP option set
Internet gateways	Default	dopt-08e0fe01f4143cdda
Egress-only internet gateways	Default VPC	IPv4 CIDR
Carrier gateways	No	10.0.0.0/24
DHCP option sets	Network Address Usage metrics	Route 53 Resolver DNS Firewall rule groups
Elastic IPs	Disabled	Failed to load rule groups
Managed prefix lists		

10 Click "Create subnet"

	State	VPC	IPv4 CIDR
8e167e8141311cb	Available	vpc-0289f69e3626447a7	172.31.32.0/20
c91a5590a075821	Available	vpc-0289f69e3626447a7	172.31.48.0/20
5c41e7dd3d91069	Available	vpc-0289f69e3626447a7	172.31.0.0/20
2f57e25edc2d99c	Available	vpc-0289f69e3626447a7	172.31.80.0/20
104b0fef4a971d9	Available	vpc-0289f69e3626447a7	172.31.16.0/20
d38762e2f0fb208	Available	vpc-0289f69e3626447a7	172.31.64.0/20

11 Select a VPC to which you want to add subnet.

### VPC

#### VPC ID

Create subnets in this VPC.

Select a VPC

Select a VPC first to create new subnets.

Add new subnet

Cancel Create subnet

12 Provide a name for subnet.

aws Services Search [Alt+S]

### Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

#### Subnet 1 of 1

**Subnet name**  
Create a tag with a key of 'Name' and a value that you specify.  
my-subnet-01

The name can be up to 256 characters long.

**Availability Zone** Info  
Choose the zone in which your subnet will reside, or let Amazon choose one for you.  
No preference

**IPv4 VPC CIDR block** Info  
Choose the IPv4 VPC CIDR block to create a subnet in.  
10.0.0.0/24

IPv4 subnet CIDR block

13 Specify IPv4 subnet CIDR block.

The name can be up to 256 characters long.

**Availability Zone** Info

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

No preference

#### IPv4 VPC CIDR block [Info](#)

Choose the IPv4 VPC CIDR block to create a subnet in.

10.0.0.0/24

#### IPv4 subnet CIDR block

10.0.0.0/28

< > ^ v

#### ▼ Tags - optional

Key

Name

Value - optional

my-subnet-1

X

Remove

Add new tag

You can add 49 more tags.

Remove

14

Click "Create subnet"

Value - optional

my-subnet-1

Remove

Cancel

Create subnet

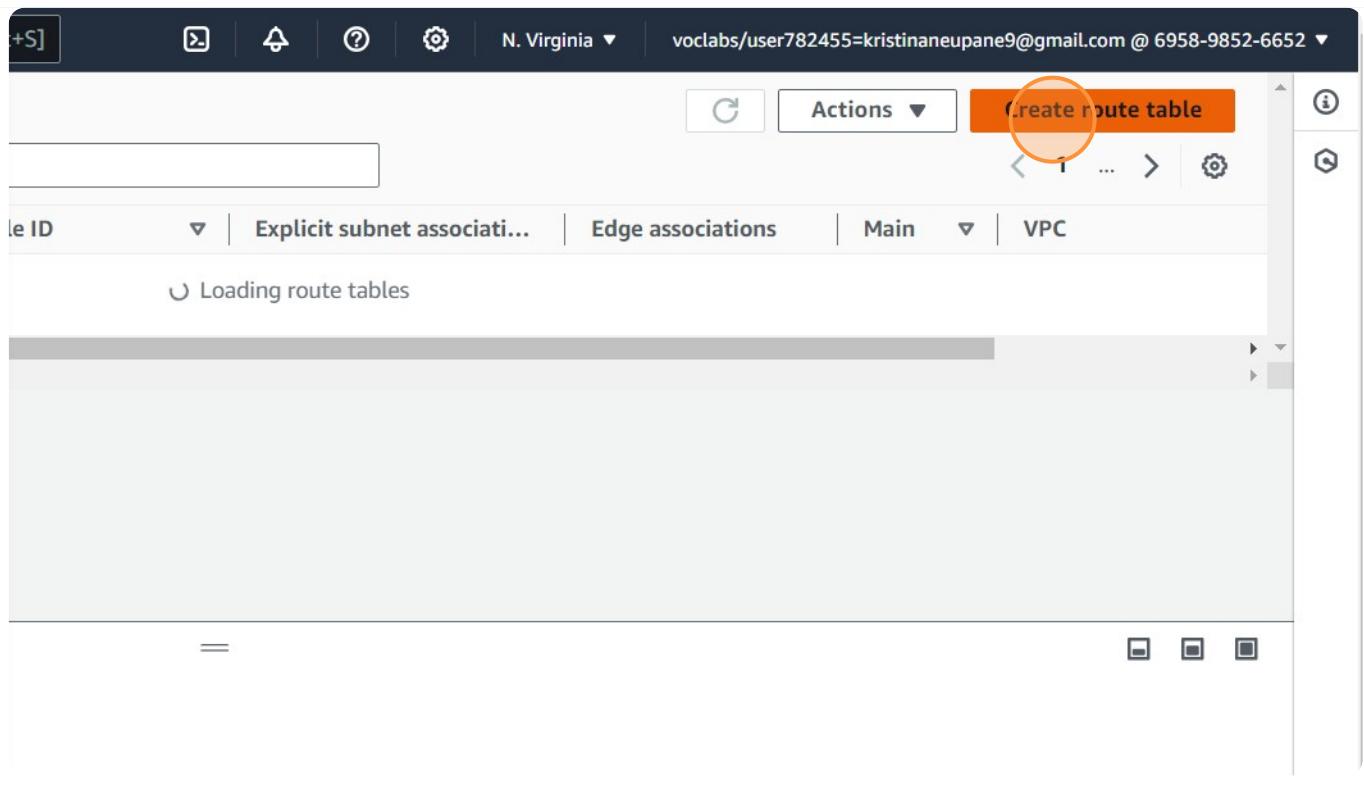
© 2024, Amazon Web Services

Steps to configure  
route tables

15 Click "Route tables" on left sidebar.

The screenshot shows the AWS VPC dashboard. On the left sidebar, under 'Virtual private cloud', the 'Route tables' link is highlighted with an orange circle. The main content area displays the 'Subnets (1)' section. A search bar at the top has 'Subnet ID : subnet-0d2a298dea91dd008' entered. Below it is a table with two columns: 'Name' and 'Subnet ID'. A single row is shown, labeled 'my-subnet-1' with the ID 'subnet-0d2a298dea91dd008'. At the bottom of the table, there is a button labeled 'Select a subnet'.

16 Click "Create route table"



17 Provide name for route table.

VPC > [Route tables](#) > Create route table

## Create route table Info

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

### Route table settings

#### Name - optional

Create a tag with a key of 'Name' and a value that you specify.

A text input field containing the value "my-route-table-01". This input field is circled in orange.

#### VPC

The VPC to use for this route table.

A dropdown menu button labeled "Select a VPC".

### Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

**18** Select a VPC to use for route table.

Name - *optional*  
Create a tag with a key of 'Name' and a value that you specify.

my-route-table-1

VPC  
The VPC to use for this route table.

Select a VPC

Q |

vpc-0289f69e3626447a7 (default)  
vpc-019a041aa289e56d9 (my-vpc-1)

can use tags to search and filter

Key Value - *optional*

Q Name X Q my-route-table-1 X Remove

Add new tag

You can add 49 more tags.

Cancel Create route table

**19** Click "Create route table"

that you specify.

Value - optional

X Q my-route-table-1 X Remove

Cancel Create route table

## Steps to set up Internet Gateway

- 20 Click "Internet gateways"

The screenshot shows the AWS VPC Route Tables page. On the left, there is a sidebar with a dropdown for 'Select a VPC'. Below it, a list of options includes 'Virtual private cloud', 'Your VPCs', 'Subnets', 'Route tables' (which is selected and highlighted in blue), 'Internet gateways' (which is circled in orange), 'Egress-only internet gateways', 'Carrier gateways', 'DHCP option sets', 'Elastic IPs', 'Managed prefix lists', 'Endpoints', and 'Endpoint services'. The main content area displays a route table named 'rtb-08cebd4cf5f45bc2 / my-route-table-1'. The 'Details' tab is selected, showing information such as Route table ID (rtb-08cebd4cf5f45bc2), Main status (No), VPC (vpc-085856ede292c0583 | my-vpc-1), and Owner ID (695898526652). Below this, the 'Routes' tab is selected, showing one route with Destination 10.0.0.0/24 and Target local. There are also tabs for 'Subnet associations', 'Edge associations', and 'Route propagation'.

- 21 Click "Create internet gateway"

The screenshot shows the AWS VPC Internet Gateways page. At the top, there is a header with a search bar, filter icons, and account information (N. Virginia, user782455=kristinaneupane9@gmail.com @ 6958-9852-6652). Below the header, there is a toolbar with a refresh icon, an 'Actions' dropdown, and a prominent orange 'Create internet gateway' button. The main content area is a table with columns: Internet Gateway ID, State, VPC ID, and Owner. One row is visible, showing 'a8a2a4588270' as the Internet Gateway ID, 'Attached' as the State, 'vpc-0289f69e3626447a7' as the VPC ID, and '695898526652' as the Owner. There are navigation arrows and a settings icon at the bottom right of the table.

- 22** Provide a name for Internet Gateway.

Create internet gateway Info

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.

**Internet gateway settings**

**Name tag**  
Creates a tag with a key of 'Name' and a value that you specify.

my-internet-gateway

**Tags - optional**  
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

Add new tag

You can add 50 more tags.

- 23** Click "Create internet gateway"

' and a value that you specify.

an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter costs.

Value - optional

X  X Remove

Cancel

Create internet gateway

© 2024, Amazon

24

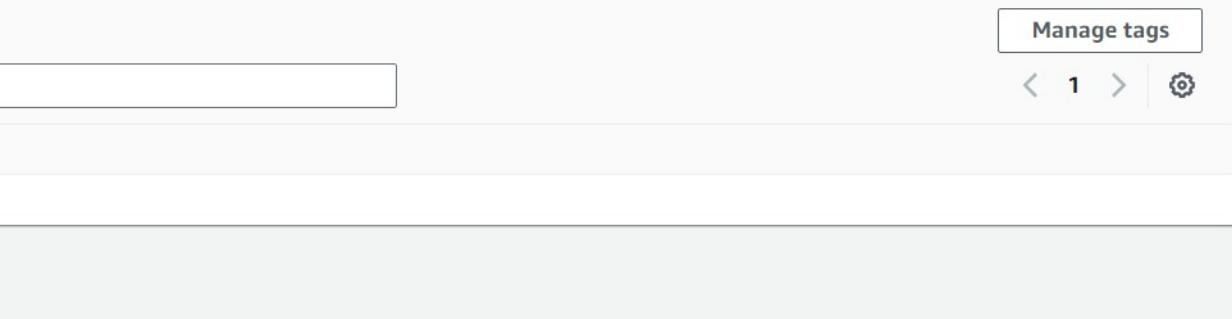
Click "Actions"

This screenshot shows the AWS Lambda console interface. At the top, there are navigation icons and a header bar with the text 'N. Virginia' and a user profile. Below the header, the title 'internet-gateway' is displayed. On the right side of the main content area, there is an 'Actions' dropdown menu with several options: 'Manage tags', '< 1 >', and a gear icon. A large orange circle highlights the 'Actions' button. The main content area contains two sections: 'VPC ID' with a value of '-' and 'Owner' with a value of '695898526652'. There is also a large, empty rectangular input field.

25

Click "Attach to VPC"

This screenshot shows the AWS Lambda console interface, similar to the previous one but with a different view. The title 'internet-gateway' is visible. On the right, the 'Actions' dropdown menu is open, showing options: 'Attach to VPC' (which is highlighted with an orange circle), 'Detach from VPC', 'Manage tags', and 'Delete'. The main content area displays the same information as the previous screenshot: 'VPC ID' (value '-'), 'Owner' (value '695898526652'), and an empty input field.



**26** Select VPC to which you want to attach Internet Gateway

VPC > Internet gateways > Attach to VPC (igw-05d838cb39f113e1e)

## Attach to VPC (igw-05d838cb39f113e1e) Info

### VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

#### Available VPCs

Attach the internet gateway to this VPC.

Select a VPC

vpc-019a041aa289e56d9 - my-vpc-1

AWS Command Line Interface command

Cancel

Attach internet gateway

**27** Click "Attach internet gateway"

the VPC to communicate with the internet. Specify the VPC to attach below.

X

emand

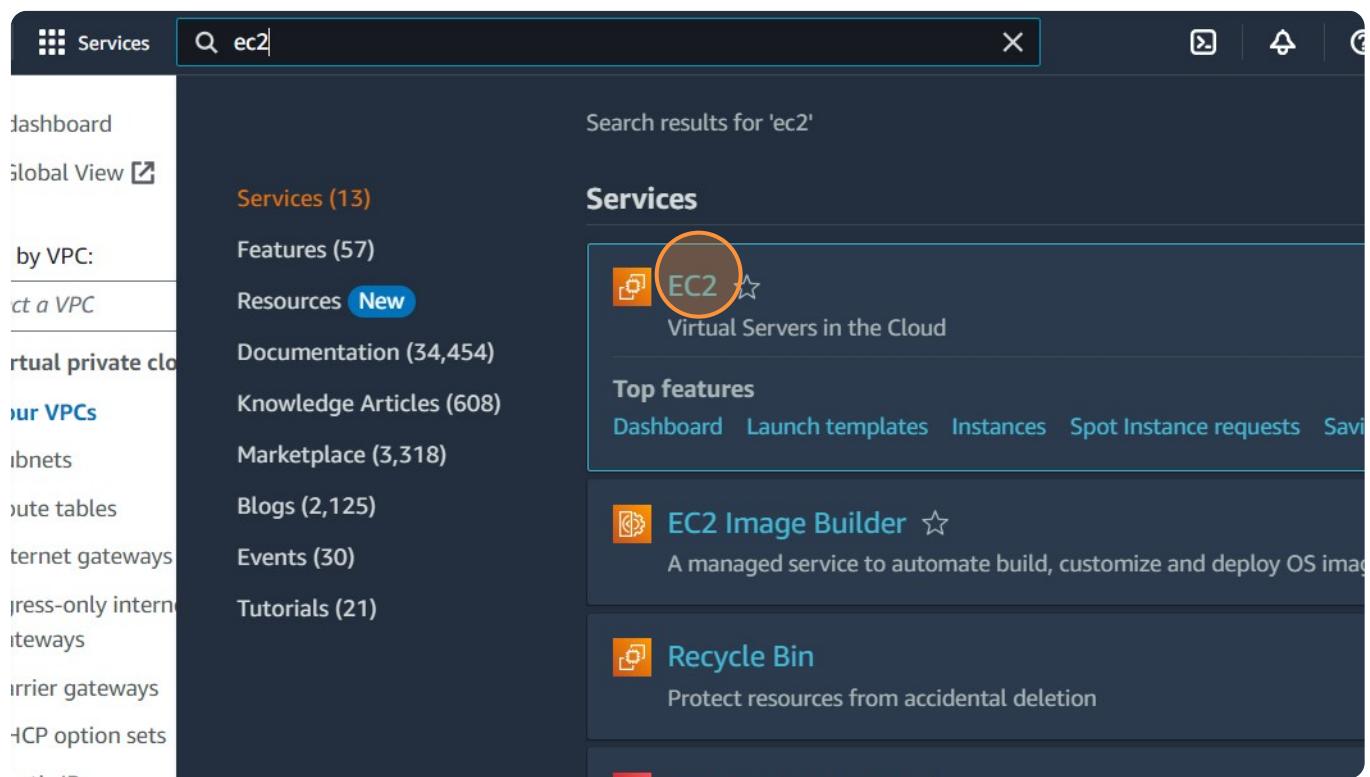
Cancel

Attach internet gateway

## Steps to setup EC2 instance within VPC

28

Click "EC2"



29

Click "Launch instance"

Instances

The screenshot shows the AWS EC2 Instances page. On the left sidebar, there are several navigation items: Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, and a New section. Below these are Images (AMIs, AMI Catalog) and Elastic Block Store (EBS, Snapshots). At the bottom of the sidebar is a Feedback button. The main content area has tabs for Load balancers, Placement groups, and Security. Under the Load balancers tab, there are links for Snapshots (1) and Volumes (1). A large orange circle highlights the "Launch instance" button, which is part of a dropdown menu. The menu also includes "Migrate a server". Below the dropdown, a note states: "Note: Your instances will launch in the US East (N. Virginia) Region". To the right, there's a "Service health" section with an "AWS Health Dashboard" link, and a "Zones" section showing the Region as "US East (N. Virginia)" and Zone name as "us-east-1a".

30 Provide name for EC2.

The screenshot shows the "Name and tags" step of the AWS EC2 Launch Instance wizard. At the top, there's a navigation bar with the AWS logo, Services, a search bar, and keyboard shortcuts [Alt+S]. Below the navigation is a message: "Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below." The main form has a "Name" field containing "e.g. My Web Server", which is highlighted with an orange circle. To the right of the name field is a "Add additional tags" link. Below the name field is a section titled "Application and OS Images (Amazon Machine Image)" with a "Search our full catalog including 1000s of application and OS images" input field.

31

### Select a key pair name.

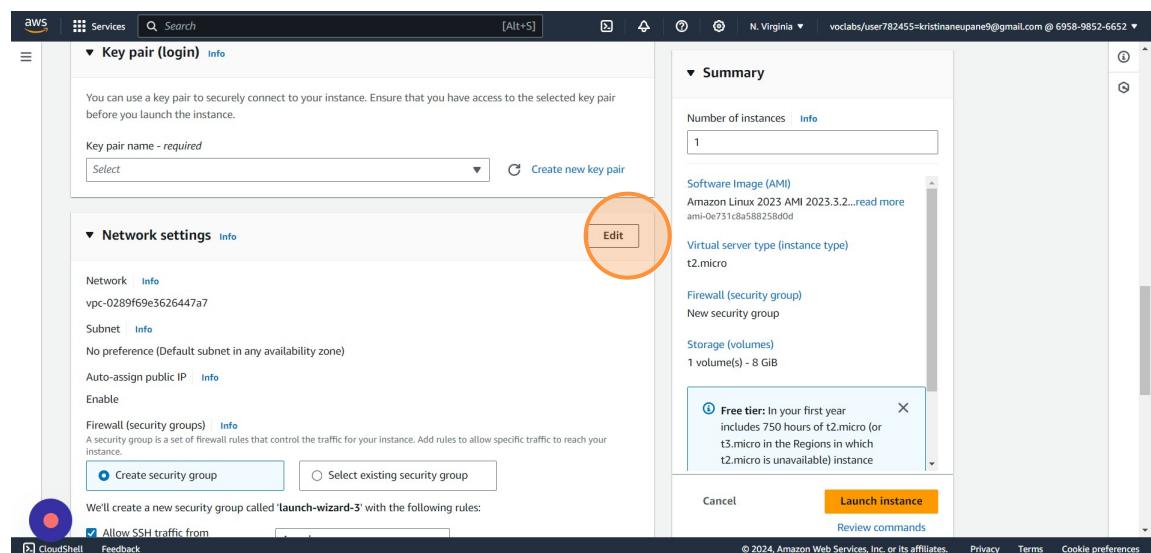
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

**Key pair name - required**

Select		<a href="#">Create new key pair</a>
<input type="text"/>		
Proceed without a key pair (Not recommended)		Default value
vockey	Type: rsa	
test	Type: rsa	
vpc-019a041aa289e56d9 (my-vpc-1)		▼
10.0.0.0/24		
<a href="#">Subnet</a> <a href="#">Info</a> <b>subnet-0e9f903290e83d0f2</b> my-subnet-1		▼
VPC: vpc-019a041aa289e56d9 Owner: 695898526652 Availability Zone: us-east-1d IP addresses available: 11 CIDR: 10.0.0.0/28		
<a href="#">Auto-assign public IP</a> <a href="#">Info</a>		

32

### Click "Edit" on right side of Network settings.



The screenshot shows the AWS Launch Wizard interface. The user is at the 'Network settings' step. On the left, there's a sidebar with 'Key pair (login)' and 'Network settings'. The 'Network settings' section is expanded, showing network details like 'vpc-0289f69e3626447a7' and 'Subnet: Info'. Below this, there's a 'Firewall (security groups)' section with options to 'Create security group' or 'Select existing security group'. A note says 'We'll create a new security group called 'launch-wizard-3' with the following rules: Allow SSH traffic from...'. On the right, there's a 'Summary' panel with information about the instance: 'Number of instances: 1', 'Software Image (AMI): Amazon Linux 2023 AMI 2023.5.2...', 'Virtual server type (instance type): t2.micro', 'Firewall (security group): New security group', 'Storage (volumes): 1 volume(s) - 8 GiB', and a 'Free tier' info box. At the bottom right are 'Cancel', 'Launch instance' (which is highlighted in orange), and 'Review commands' buttons.

- 33 Select VPC you just created.

The screenshot shows the 'Network settings' section of the AWS CloudFormation console. It displays a list of VPCs under the 'VPC - required' section. The first two VPCs are listed as '(default)'. The third VPC, 'vpc-019a041aa289e56d9 (my-vpc-1)', is listed with a CIDR range of '10.0.0.0/24' and is highlighted with an orange circle. Below the list, there is a 'Firewall (security groups)' section with two options: 'Create security group' (selected) and 'Select existing security group'. At the bottom, there is a 'Security group name - required' field and a progress bar indicating the creation process.

- 34 Click "Launch instance"

The screenshot shows the 'Launch instance' dialog box. On the left, there is a 'Storage (volumes)' section indicating '1 volume(s) - 8 GiB'. A tooltip for the storage section explains the 'Free tier': 'Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.' At the bottom of the dialog, there are three buttons: 'Cancel', 'Launch instance' (which is circled in orange), and 'Review commands'.

**35**

Successfully launched a simple EC2 instance within VPC just created.