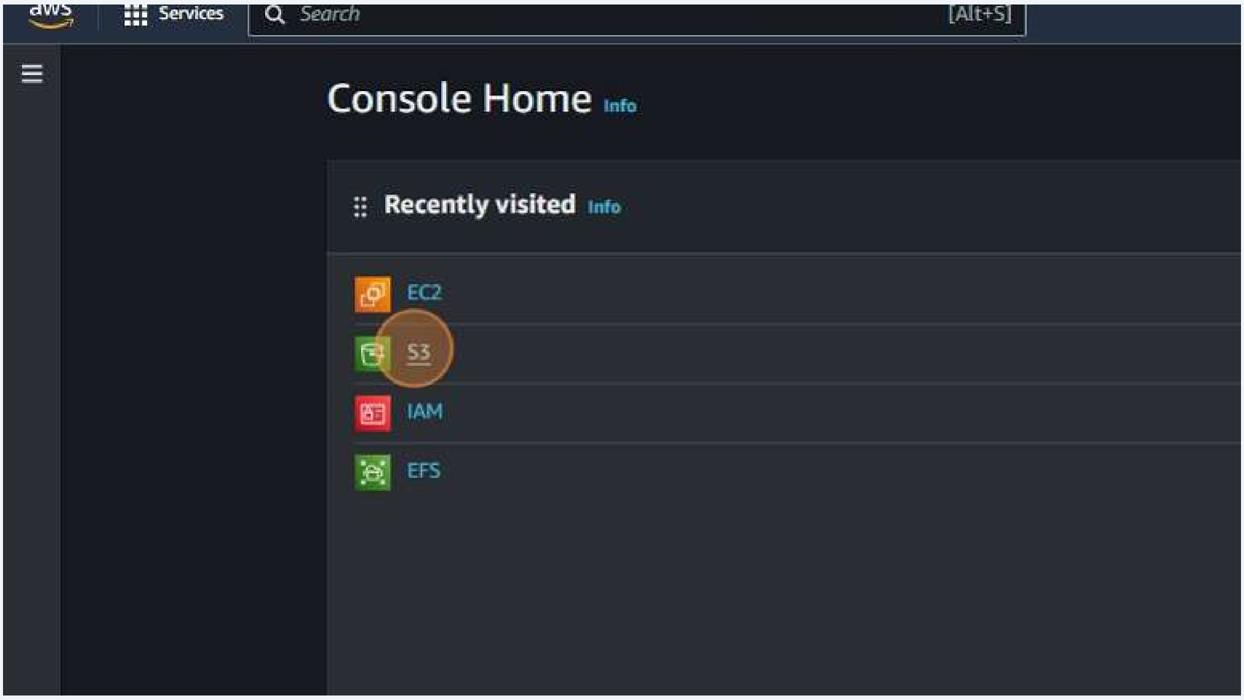
# Create a Bucket on AWS S3

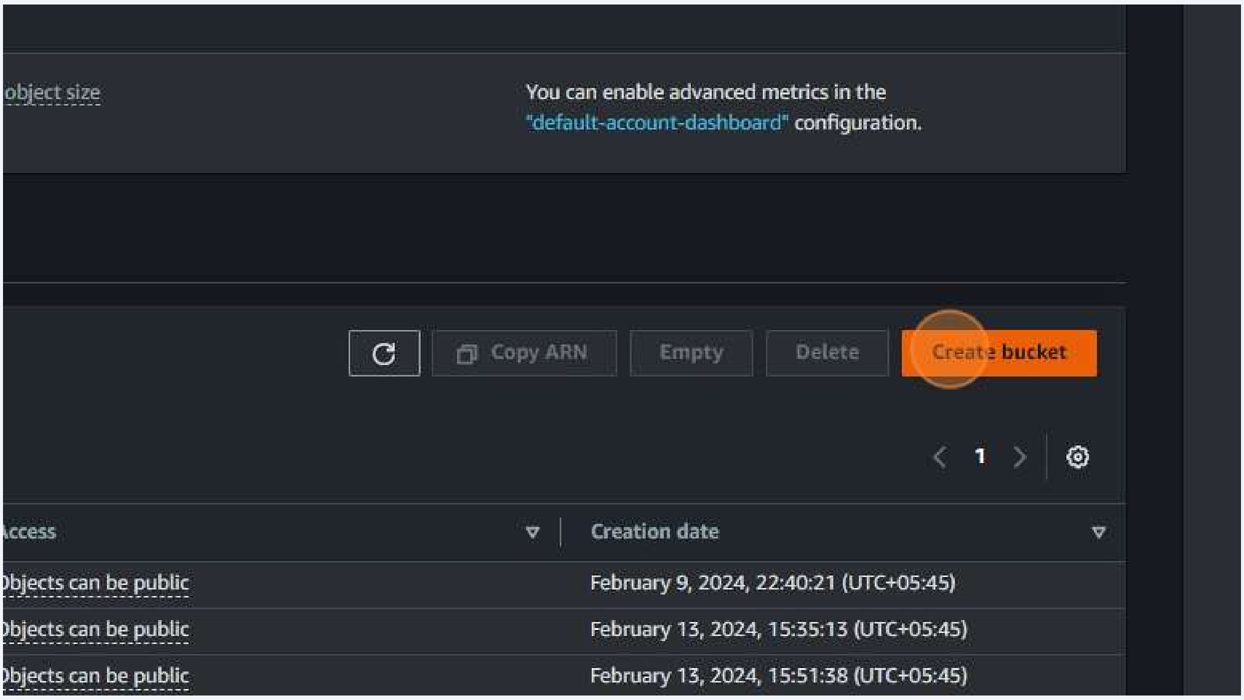
## S3 Bucket

1 Navigate to [https://us-east-1.console.aws.amazon.com/console/home?region=us-east-1](https://us-east-1.console.aws.amazon.com/console/home?region=us-east-1)

2 Click "S3"



3 Click "Create bucket"



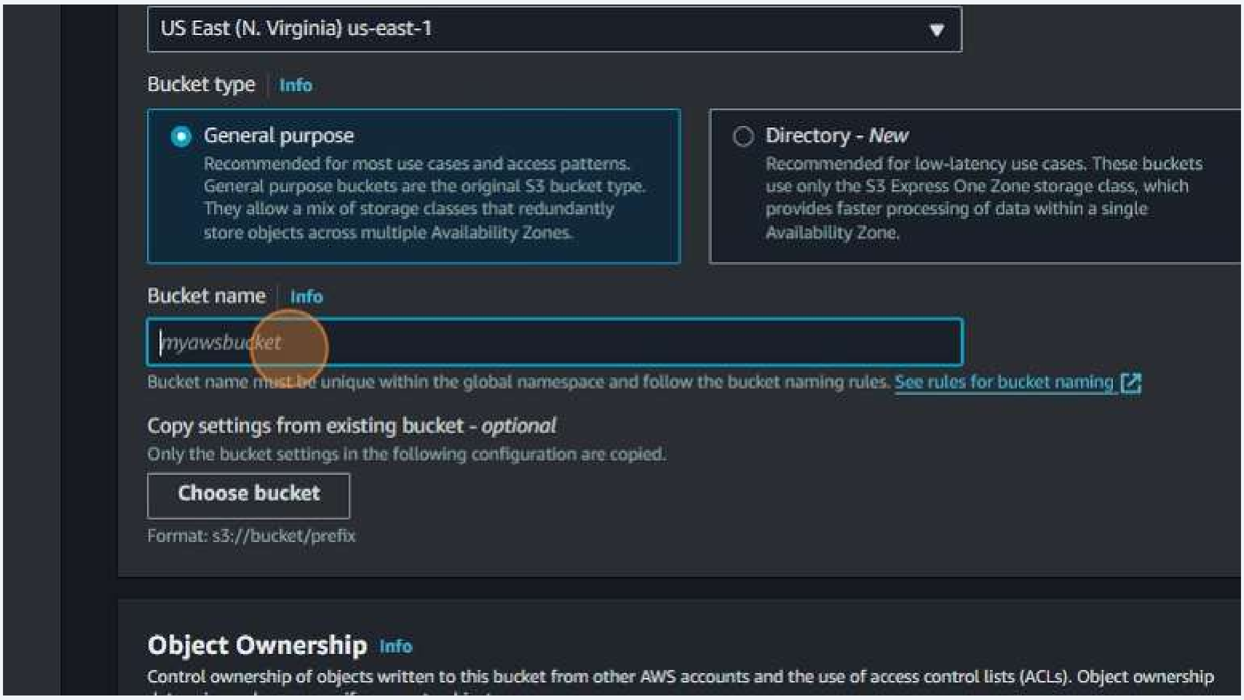
object size

You can enable advanced metrics in the "default-account-dashboard" configuration.

| Access | Creation date |
|---|---|
| Objects can be public | February 9, 2024, 22:40:21 (UTC+05:45) |
| Objects can be public | February 13, 2024, 15:35:13 (UTC+05:45) |
| Objects can be public | February 13, 2024, 15:51:38 (UTC+05:45) |

4 Navigate to https://s3.console.aws.amazon.com/s3/bucket/create?region=us-east-1

5 Click the "Bucket name" field.



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

*myawsbucket*

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

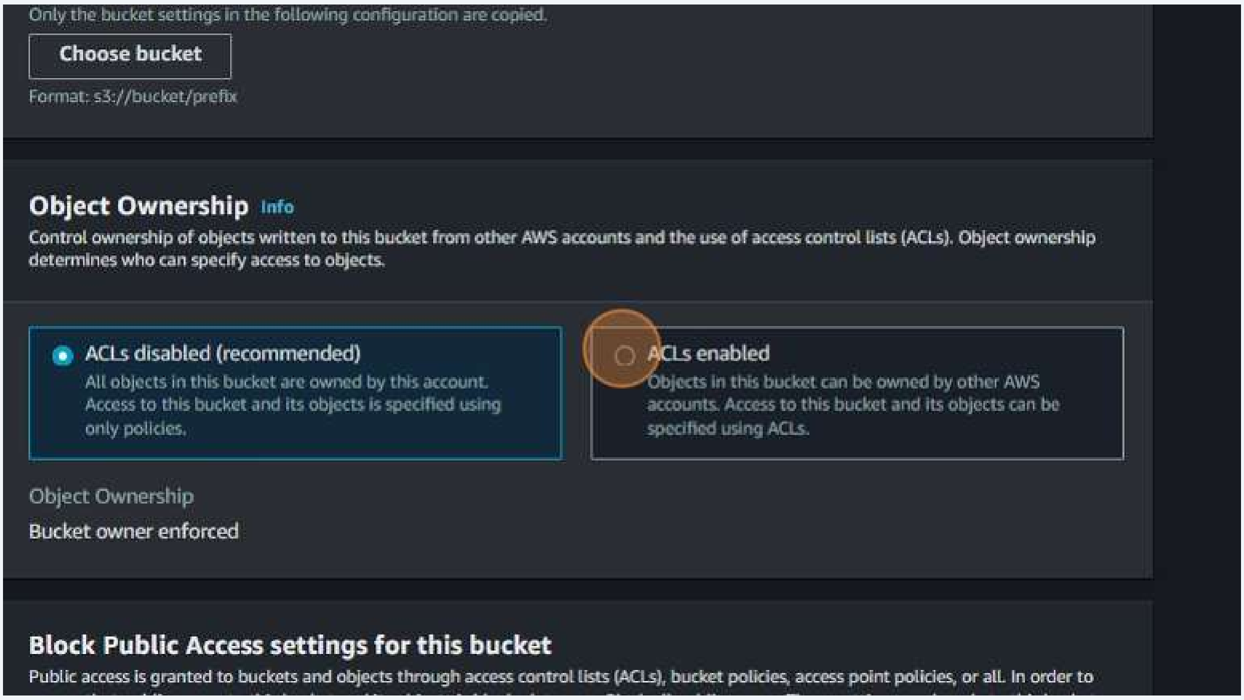
Format: s3://bucket/prefix

**Object Ownership** Info

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

6 Type " **Backspace** my-s3-bucket-files"

7 Click this radio button.



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 ownership determines who can specify access to objects.

● ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

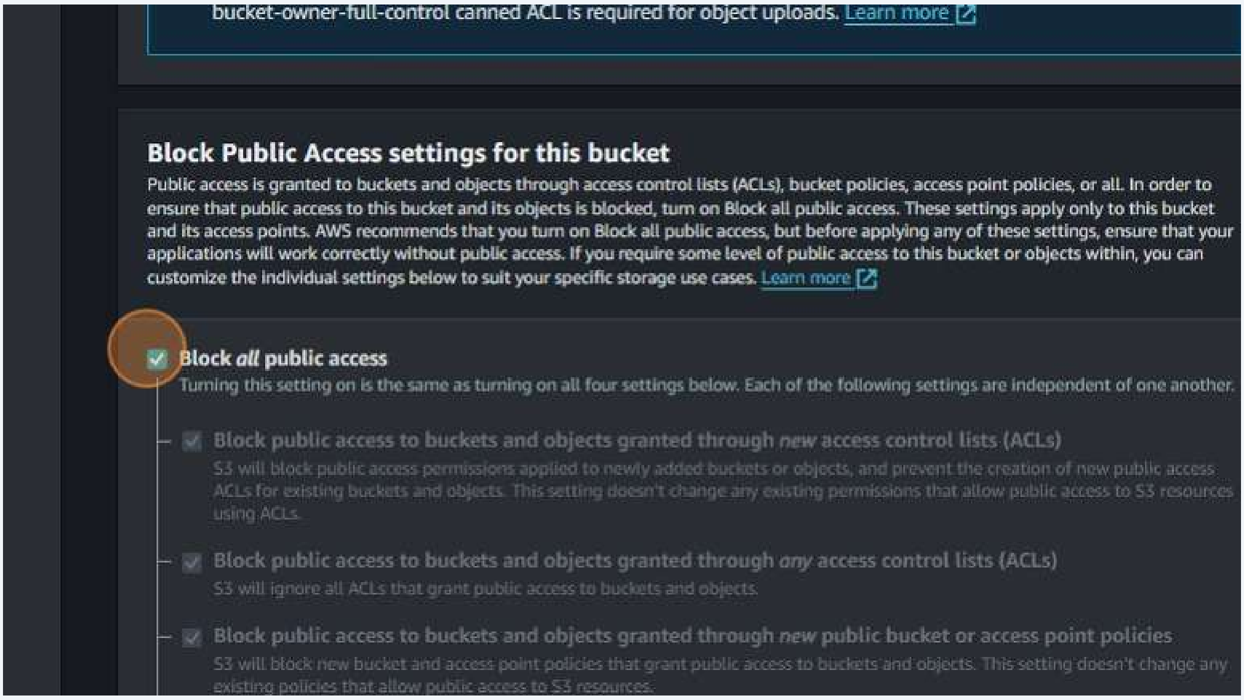
○ ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership
Bucket owner enforced

**Block Public Access settings for this bucket**

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to

8 Click this checkbox.



bucket-owner-full-control canned ACL is required for object uploads. Learn more

**Block Public Access settings for this bucket**

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 this bucket and its 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 this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

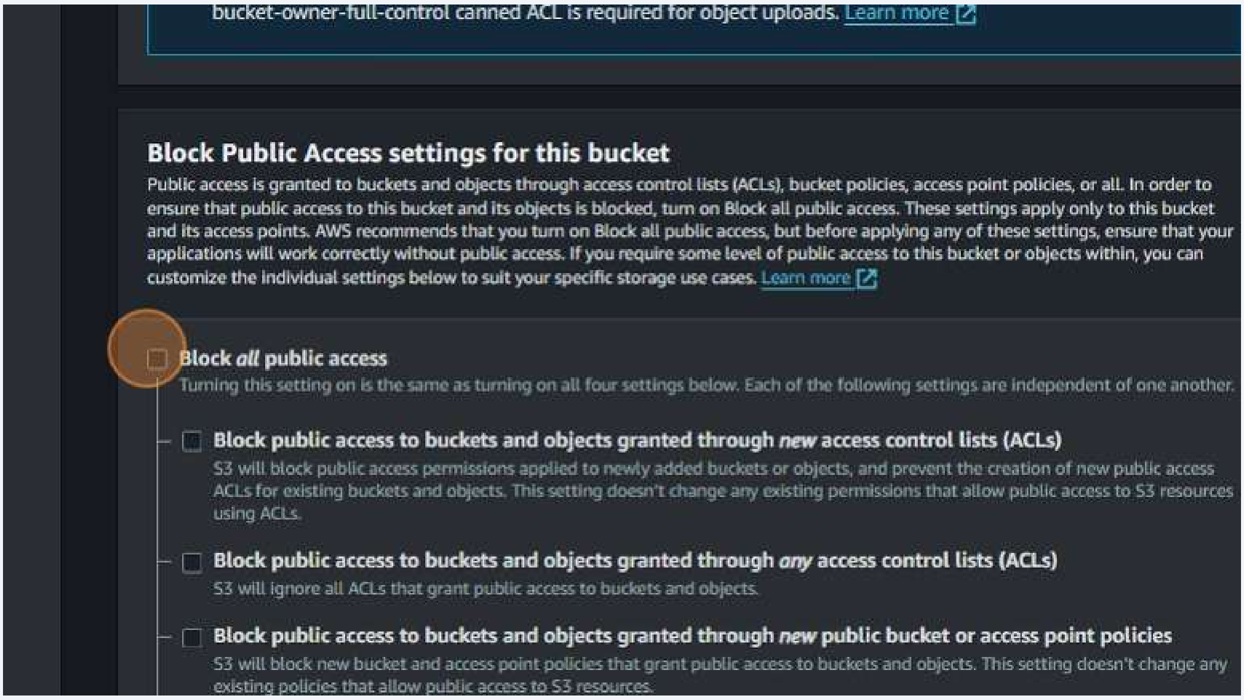
☑ Block *all* public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☑ 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, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

- ☑ Block public access to buckets and objects granted through *any* access control lists (ACLs)
S3 will ignore all ACLs that grant public access to buckets and objects.

- ☑ Block public access to buckets and objects granted through *new* public bucket or access point policies
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

**9** Click this checkbox.



bucket-owner-full-control canned ACL is required for object uploads. Learn more

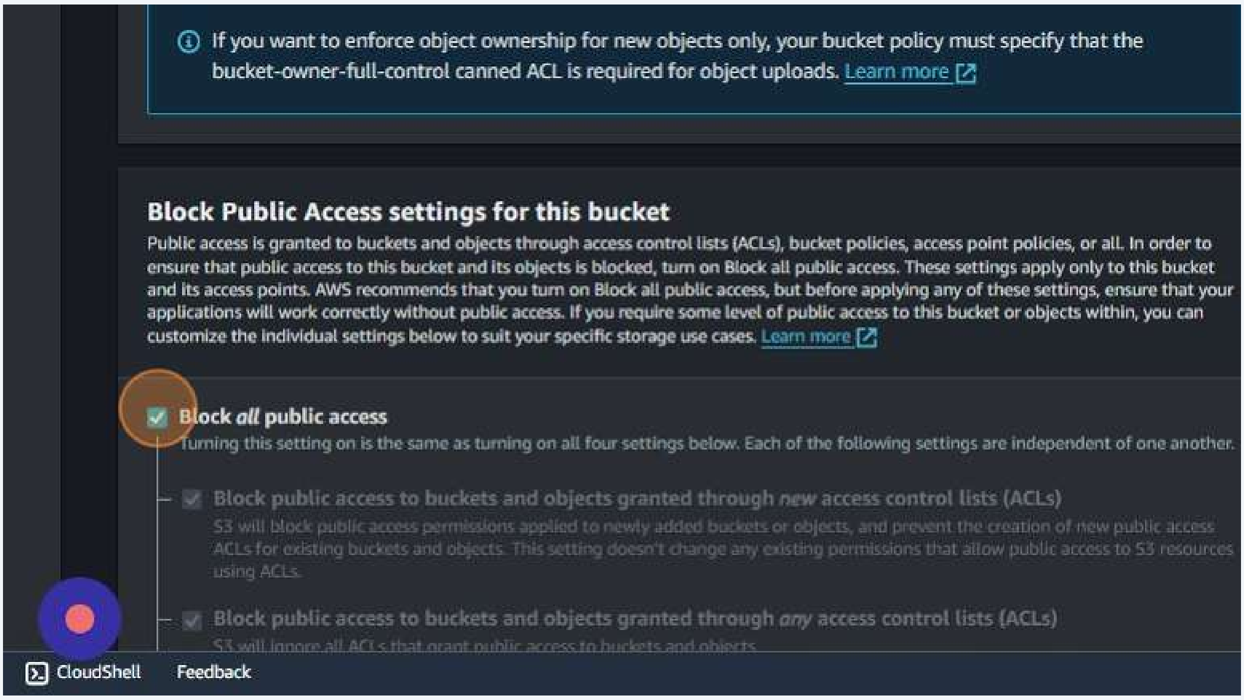
**Block Public Access settings for this bucket**

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 this bucket and its 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 this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

□ **Block *all* public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- □ **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, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- □ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
  S3 will ignore all ACLs that grant public access to buckets and objects.
- □ **Block public access to buckets and objects granted through *new* public bucket or access point policies**
  S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

**10** Click this checkbox.



If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. Learn more

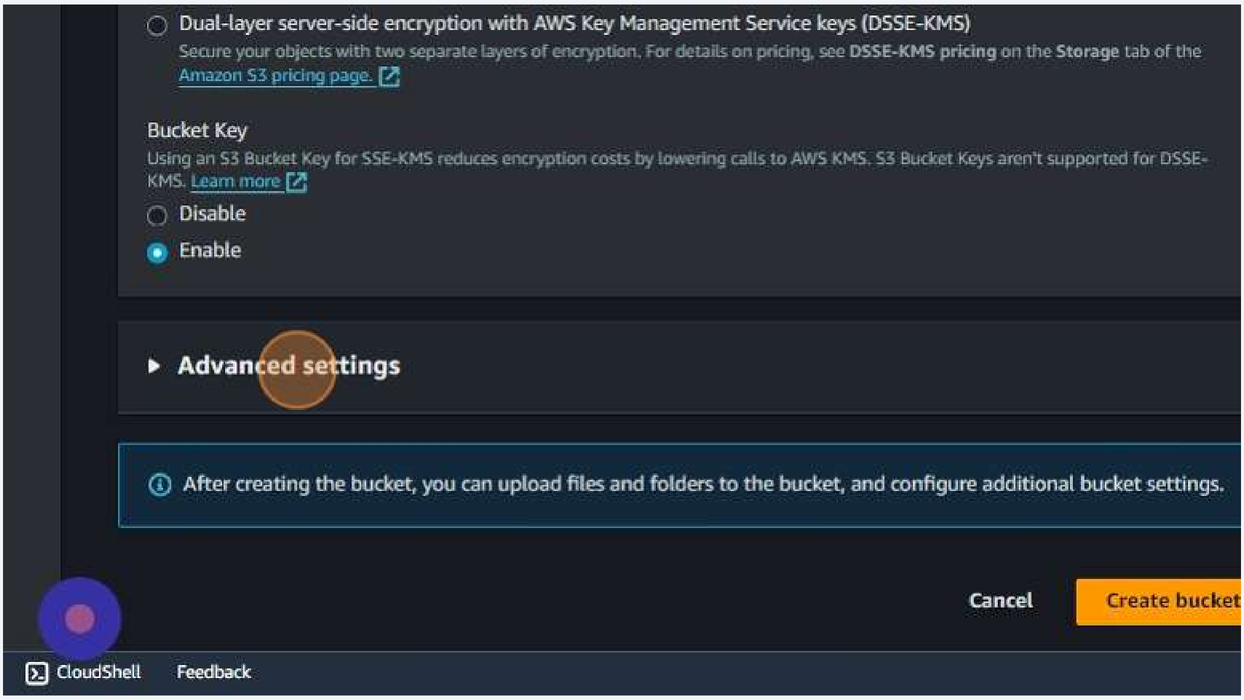
**Block Public Access settings for this bucket**

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 this bucket and its 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 this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

☑ **Block *all* public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☑ **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, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- ☑ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
  S3 will ignore all ACLs that grant public access to buckets and objects.

11 Click "Advanced settings"



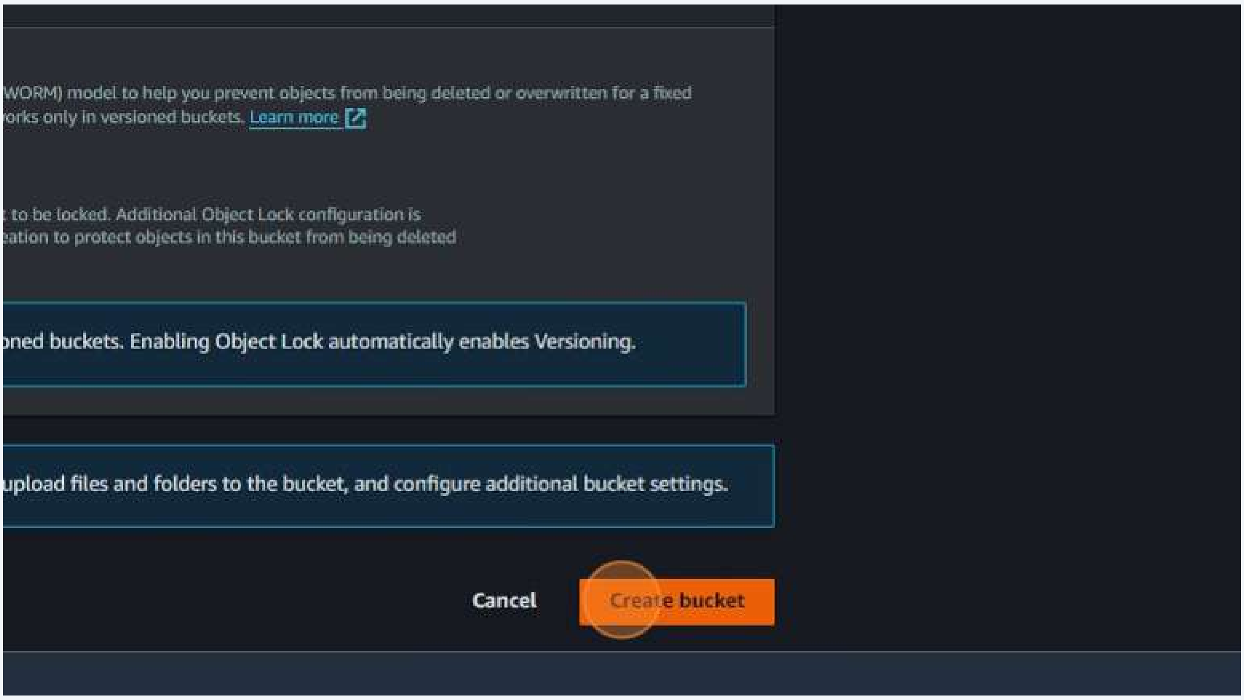
○ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see **DSSE-KMS pricing** on the **Storage** tab of the Amazon S3 pricing page.

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

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

12 Click "Create bucket"



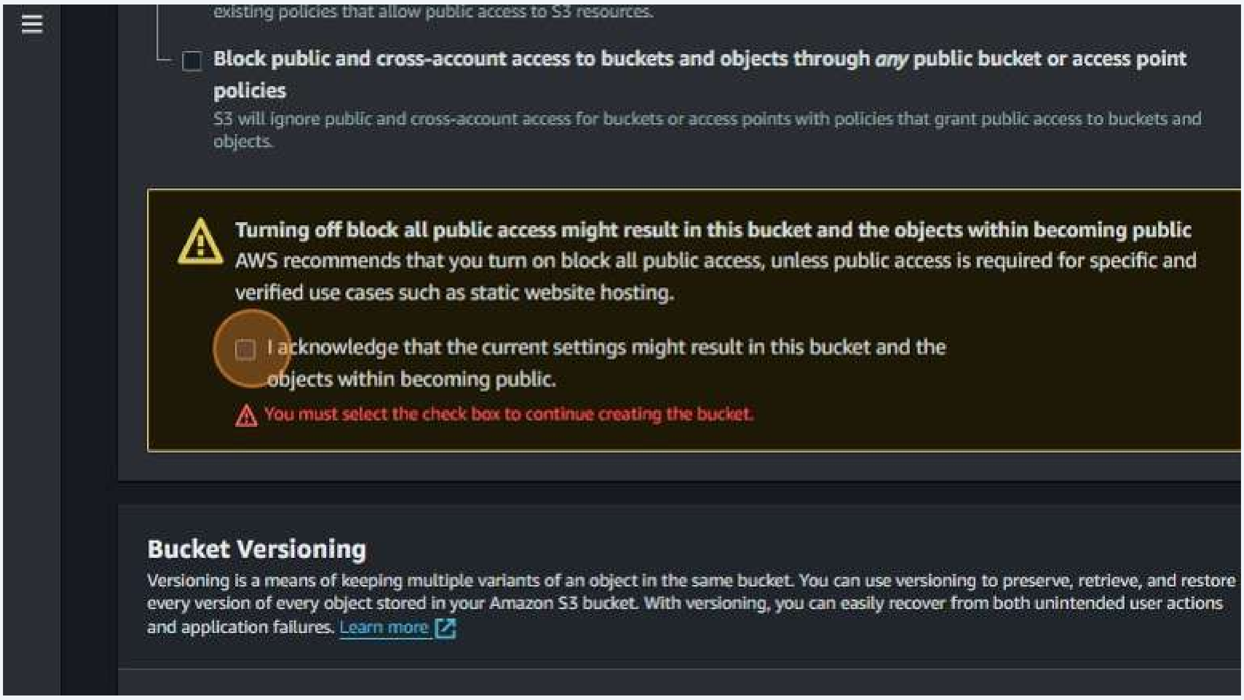
WORM) model to help you prevent objects from being deleted or overwritten for a fixed
orks only in versioned buckets. Learn more

to be locked. Additional Object Lock configuration is
eation to protect objects in this bucket from being deleted

oned buckets. Enabling Object Lock automatically enables Versioning.

upload files and folders to the bucket, and configure additional bucket settings.

13 Click this checkbox.



existing policies that allow public access to S3 resources.

□ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

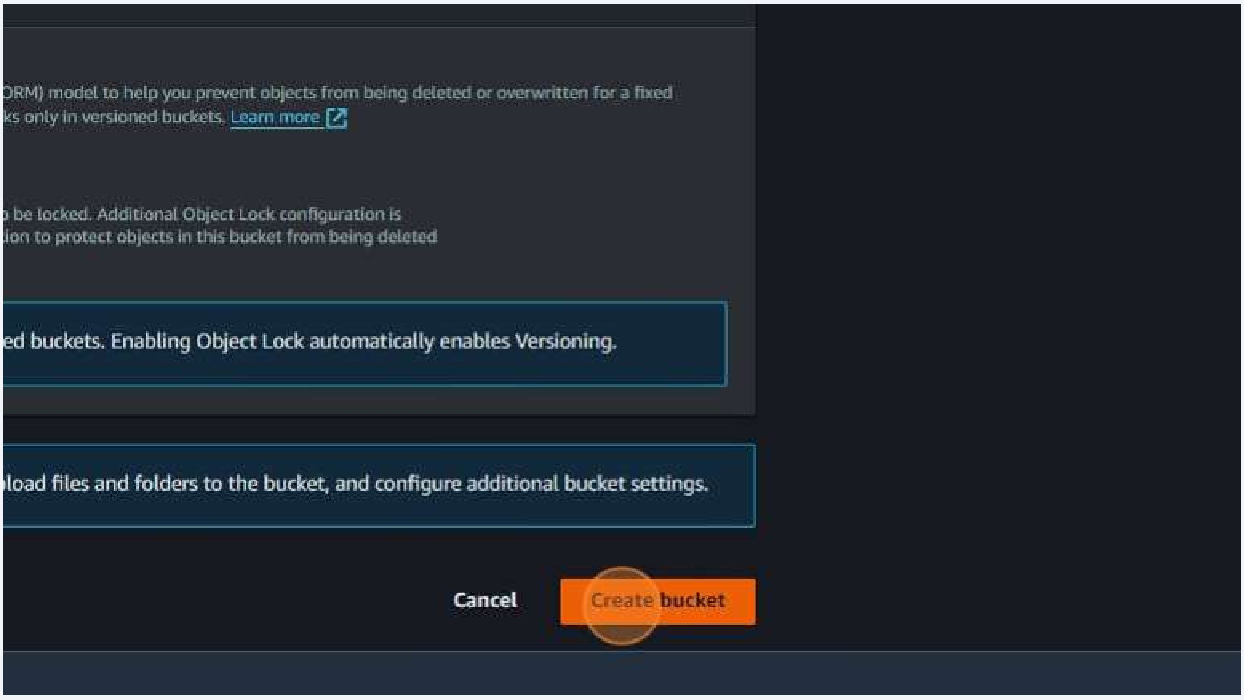
**Turning off block all public access might result in this bucket and the objects within becoming public**
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

□ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

You must select the check box to continue creating the bucket.

**Bucket Versioning**
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

14 Click "Create bucket"



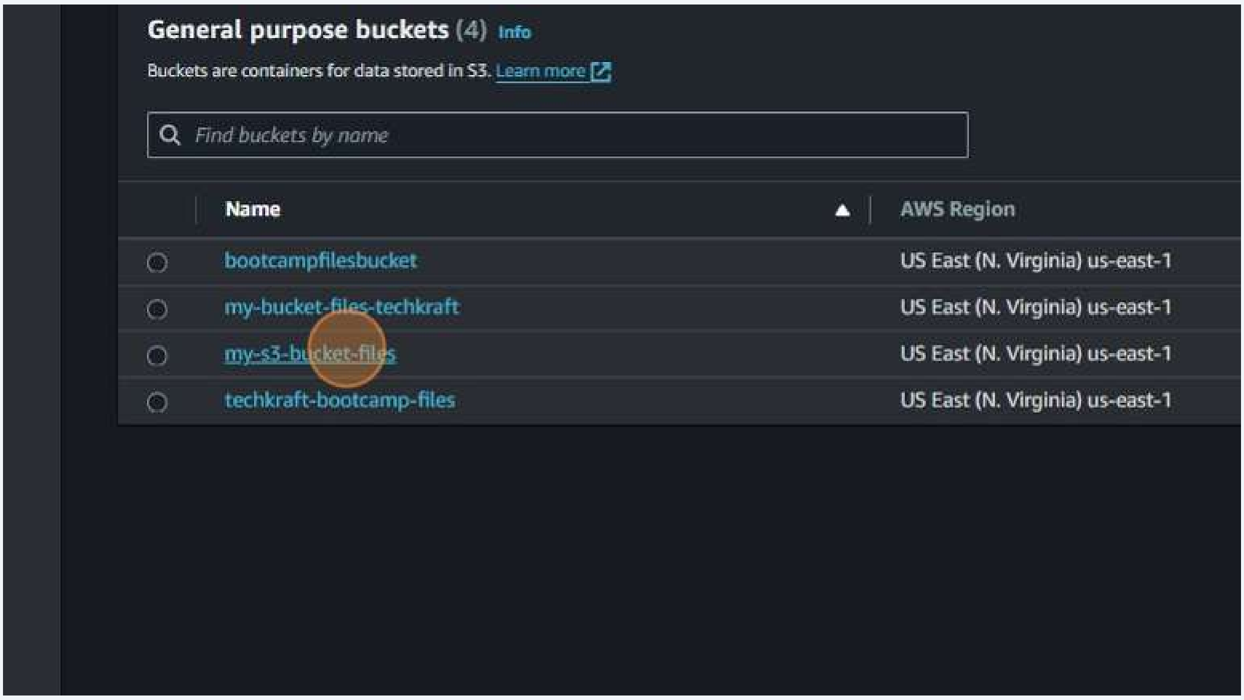
ORM) model to help you prevent objects from being deleted or overwritten for a fixed
ks only in versioned buckets. Learn more

be locked. Additional Object Lock configuration is
ion to protect objects in this bucket from being deleted

ed buckets. Enabling Object Lock automatically enables Versioning.

load files and folders to the bucket, and configure additional bucket settings.

15 Click "my-s3-bucket-files"



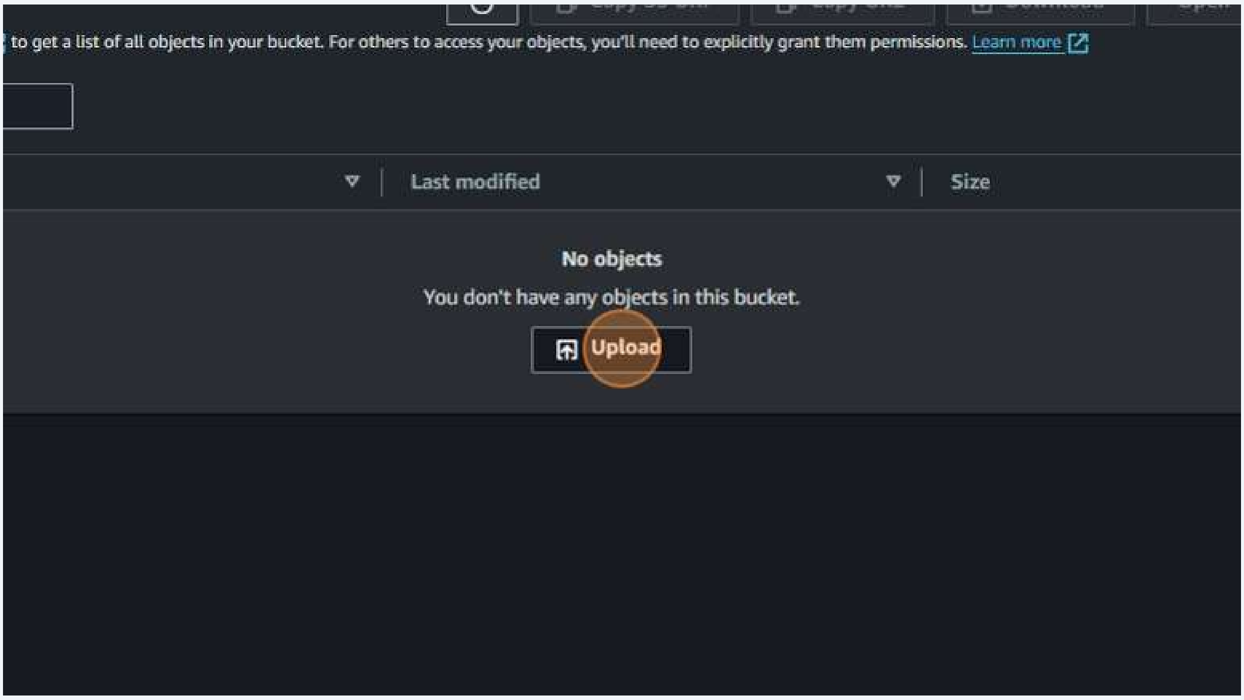
General purpose buckets (4) Info

Buckets are containers for data stored in S3. Learn more

Find buckets by name

| | Name | AWS Region |
|---|---|---|
| ○ | bootcampfilesbucket | US East (N. Virginia) us-east-1 |
| ○ | my-bucket-files-techkraft | US East (N. Virginia) us-east-1 |
| ○ | my-s3-bucket-files | US East (N. Virginia) us-east-1 |
| ○ | techkraft-bootcamp-files | US East (N. Virginia) us-east-1 |

16 Click "Upload"

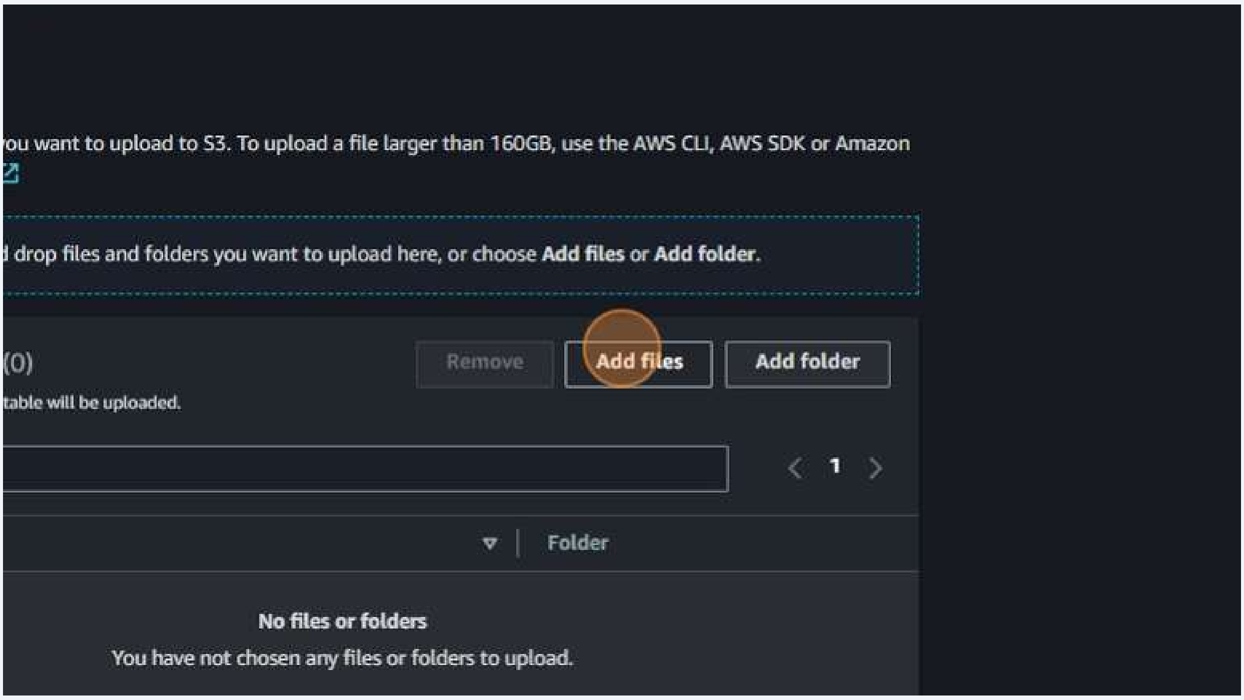


to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

No objects

You don't have any objects in this bucket.

17 Click "Add files"



ou want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon

l drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

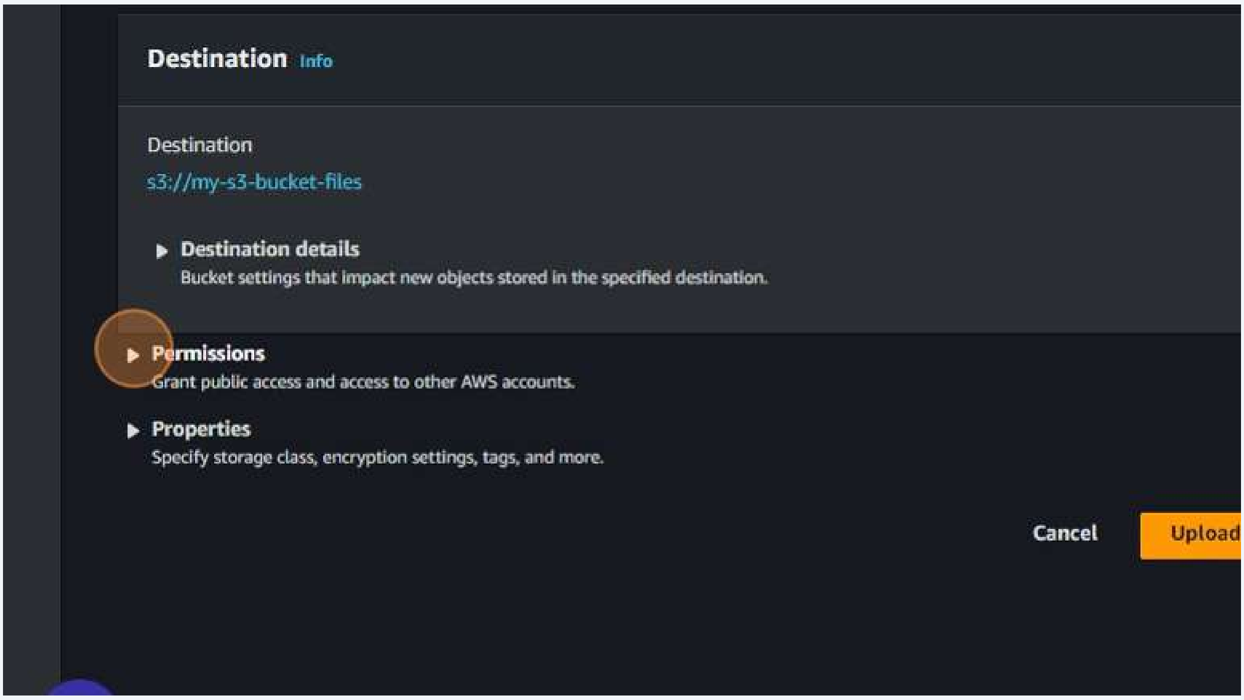
(0)

table will be uploaded.

No files or folders

You have not chosen any files or folders to upload.

18 Click here.



Destination

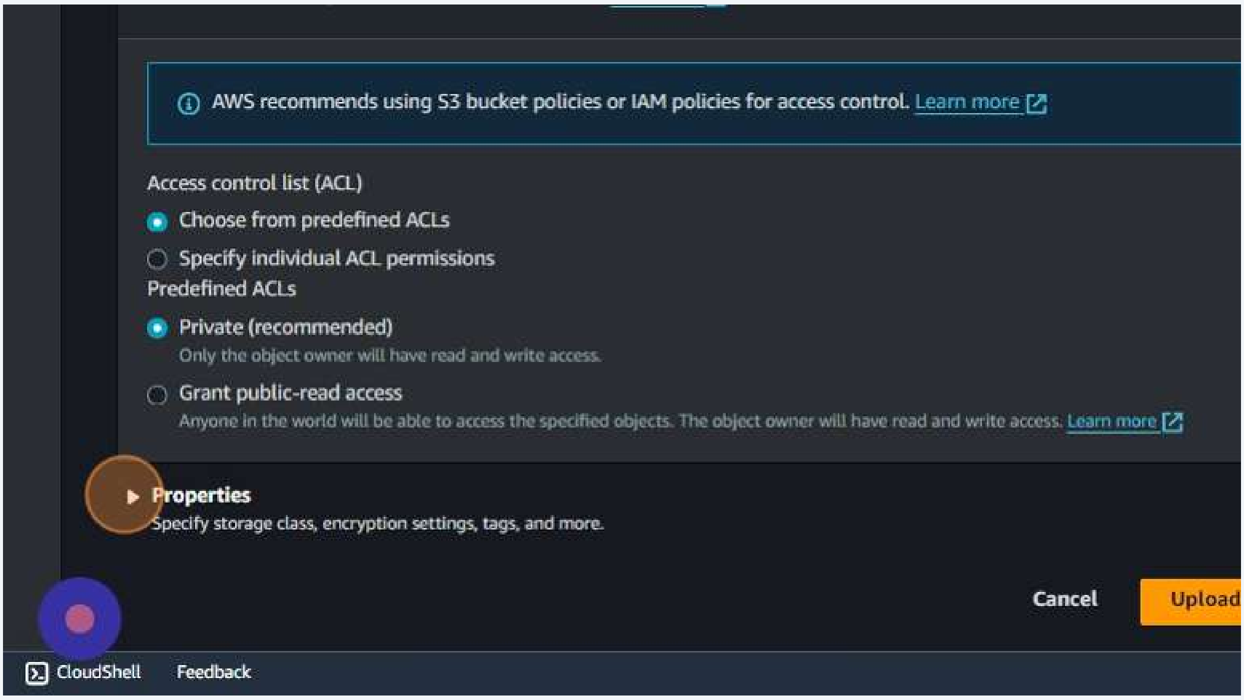
Destination
s3://my-s3-bucket-files

Destination details
Bucket settings that impact new objects stored in the specified destination.

Permissions
Grant public access and access to other AWS accounts.

Properties
Specify storage class, encryption settings, tags, and more.

**19** Click here.



AWS recommends using S3 bucket policies or IAM policies for access control. Learn more

Access control list (ACL)

● Choose from predefined ACLs

○ Specify individual ACL permissions

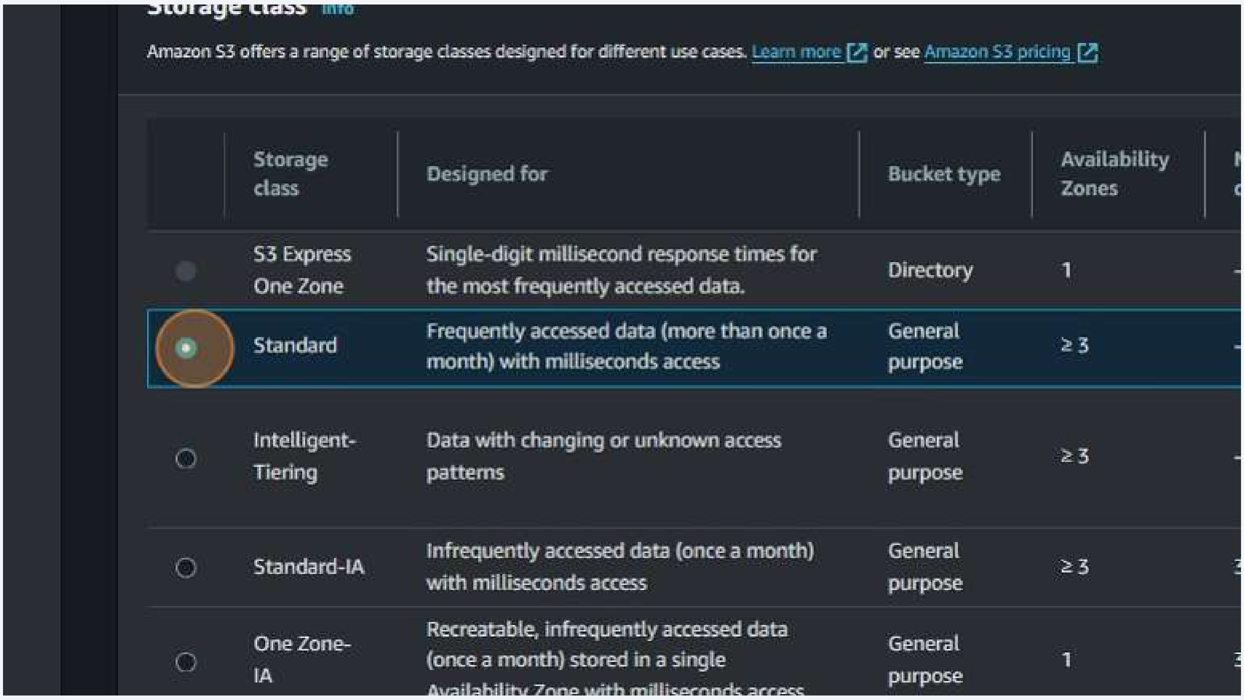
Predefined ACLs

● Private (recommended)
Only the object owner will have read and write access.

○ Grant public-read access
Anyone in the world will be able to access the specified objects. The object owner will have read and write access. Learn more

▸ Properties
Specify storage class, encryption settings, tags, and more.

**20** Click "Table Selection Select STANDARD"

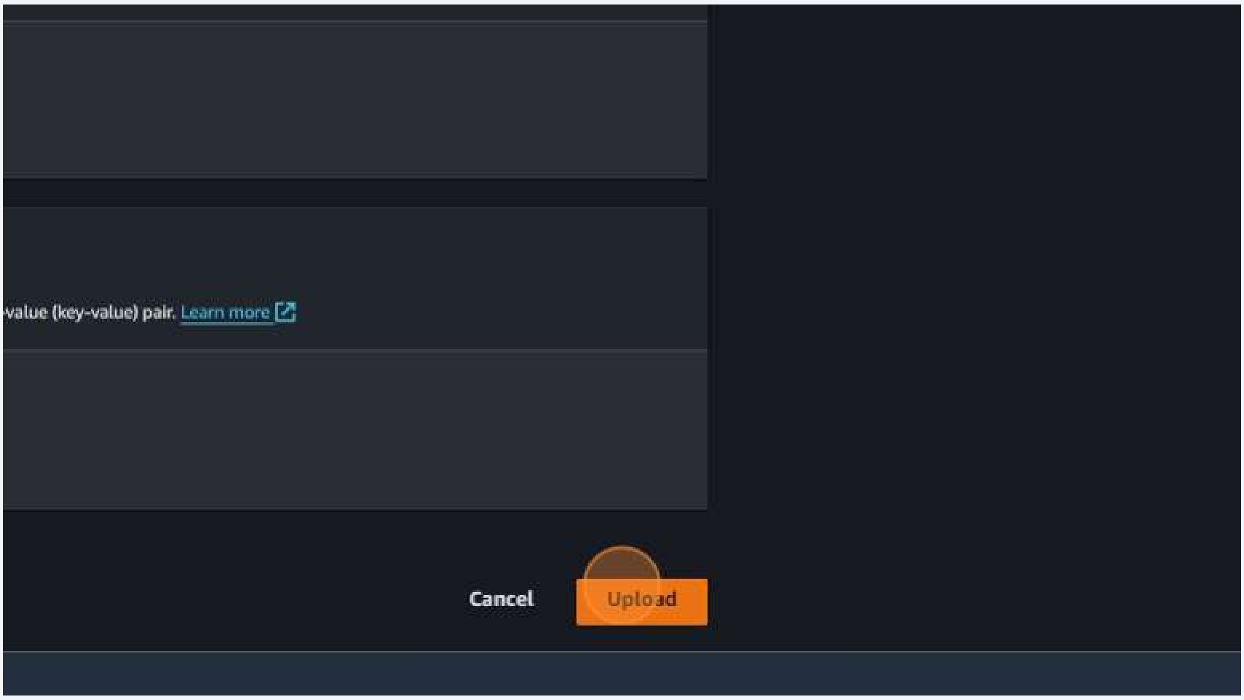


Storage class Info

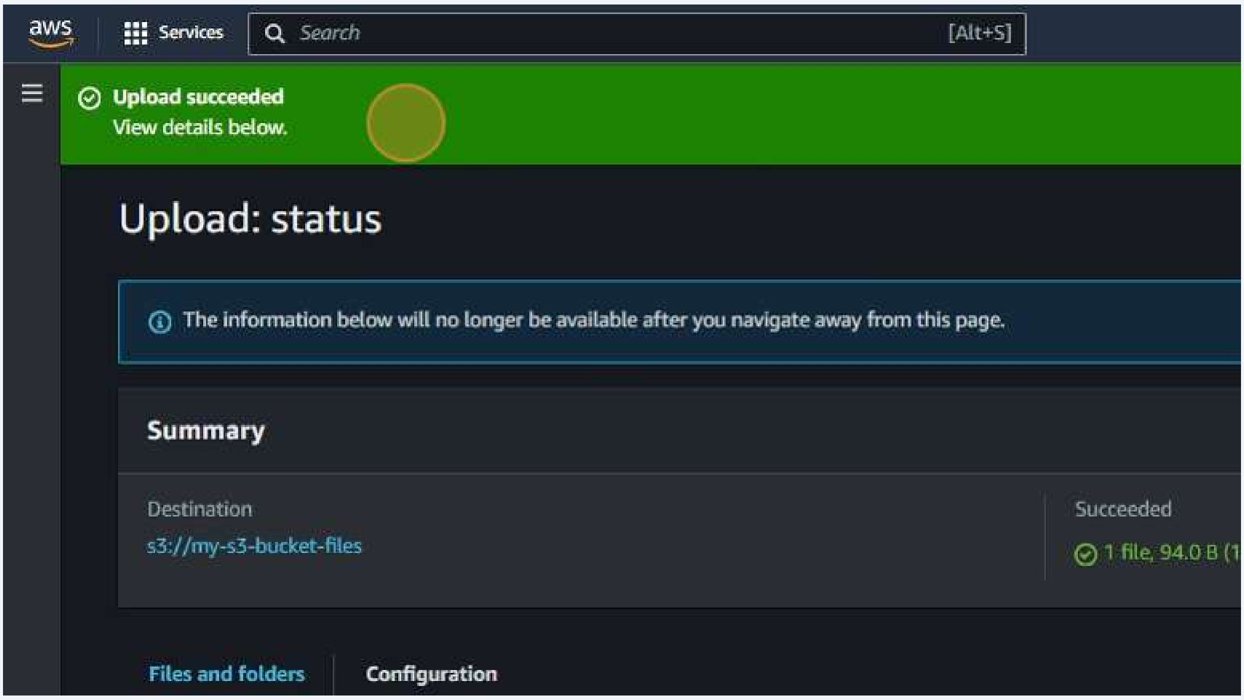
Amazon S3 offers a range of storage classes designed for different use cases. Learn more or see Amazon S3 pricing

| | Storage class | Designed for | Bucket type | Availability Zones |
|---|---|---|---|---|
| ○ | S3 Express One Zone | Single-digit millisecond response times for the most frequently accessed data. | Directory | 1 |
| ● | Standard | Frequently accessed data (more than once a month) with milliseconds access | General purpose | ≥ 3 |
| ○ | Intelligent-Tiering | Data with changing or unknown access patterns | General purpose | ≥ 3 |
| ○ | Standard-IA | Infrequently accessed data (once a month) with milliseconds access | General purpose | ≥ 3 |
| ○ | One Zone-IA | Recreatable, infrequently accessed data (once a month) stored in a single Availability Zone with milliseconds access | General purpose | 1 |

21 Click "Upload"



22 Click "View details below."



Upload succeeded
View details below.

Upload: status

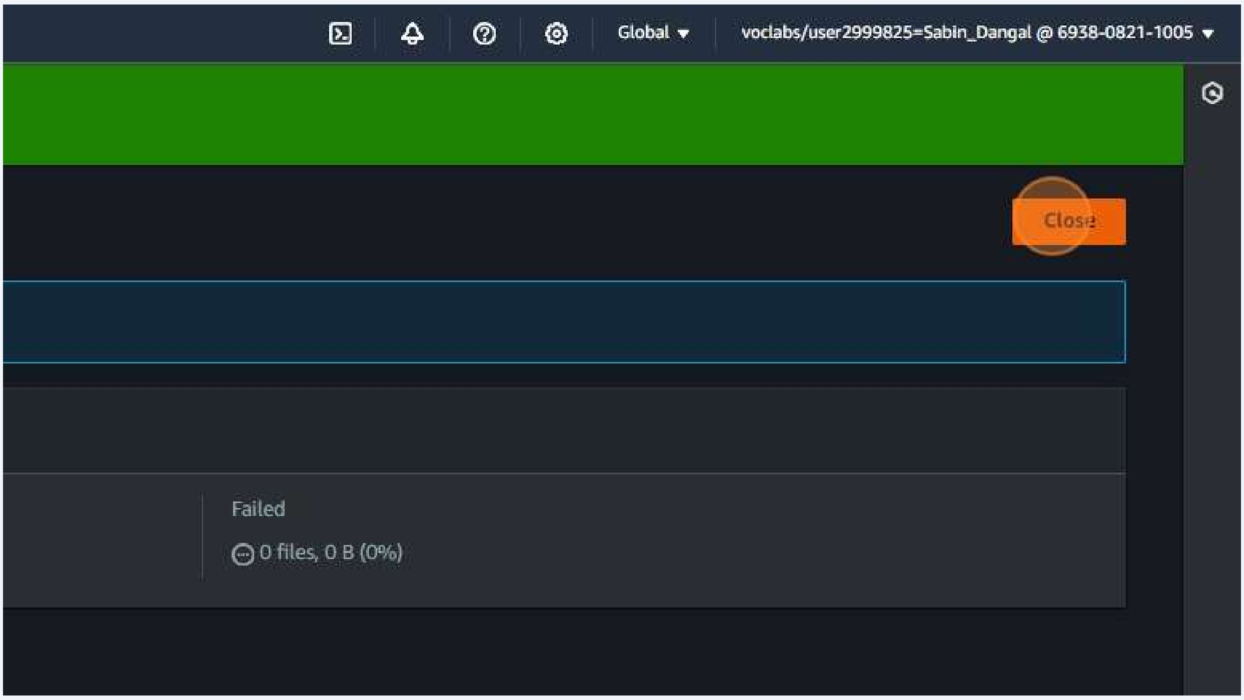
The information below will no longer be available after you navigate away from this page.

Summary

Destination
s3://my-s3-bucket-files

Succeeded
1 file, 94.0 B (1

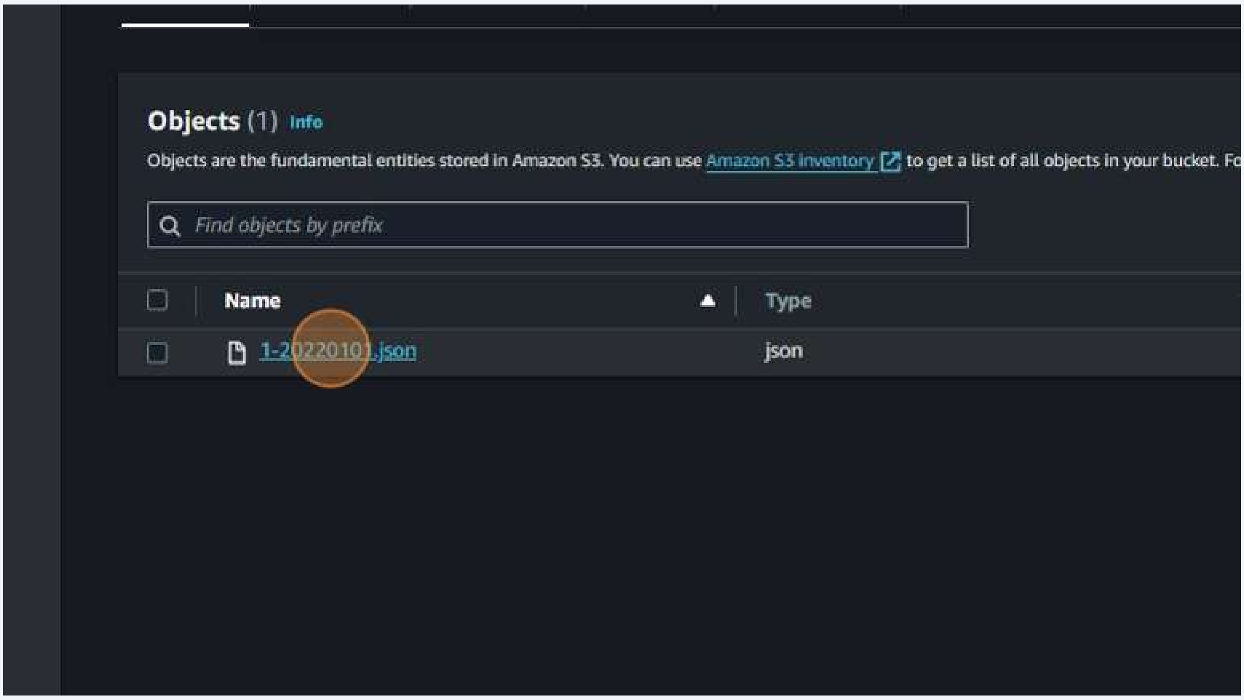
23 Click "Close"



Failed

0 files, 0 B (0%)

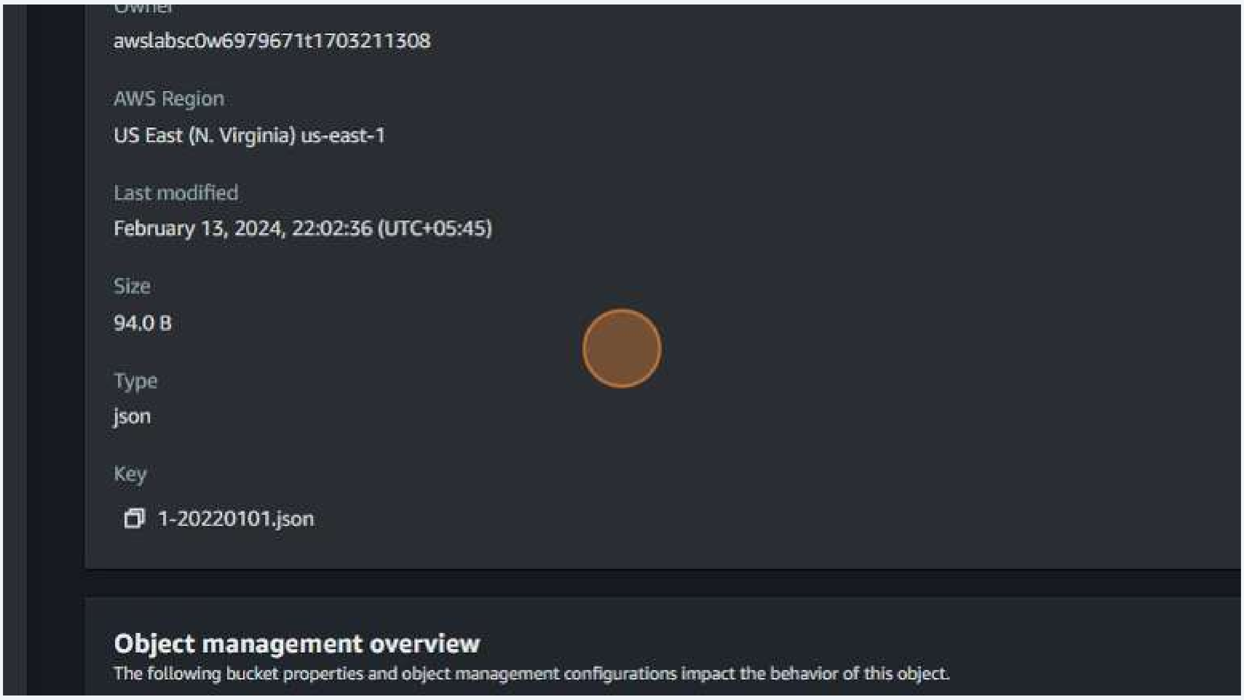
24 Click "1-20220101.json"


Objects (1) Info

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. Fo

| Name | Type |
|---|---|
| 1-20220101.json | json |

25 Click here.



Owner

awslabsc0w6979671t1703211308

AWS Region

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

Last modified

February 13, 2024, 22:02:36 (UTC+05:45)

Size

94.0 B

Type

json

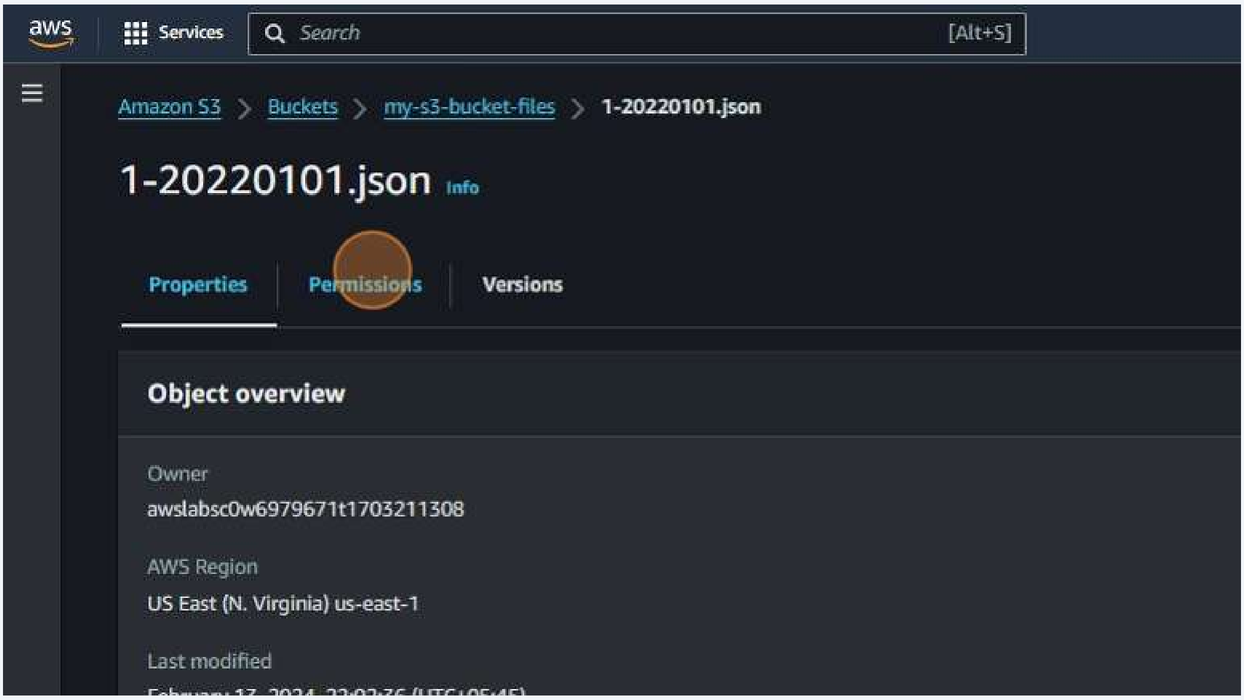
Key

1-20220101.json

Object management overview

The following bucket properties and object management configurations impact the behavior of this object.

26 Click "Permissions"



Amazon S3 > Buckets > my-s3-bucket-files > 1-20220101.json

1-20220101.json Info

Object overview

Owner

awslabsc0w6979671t1703211308

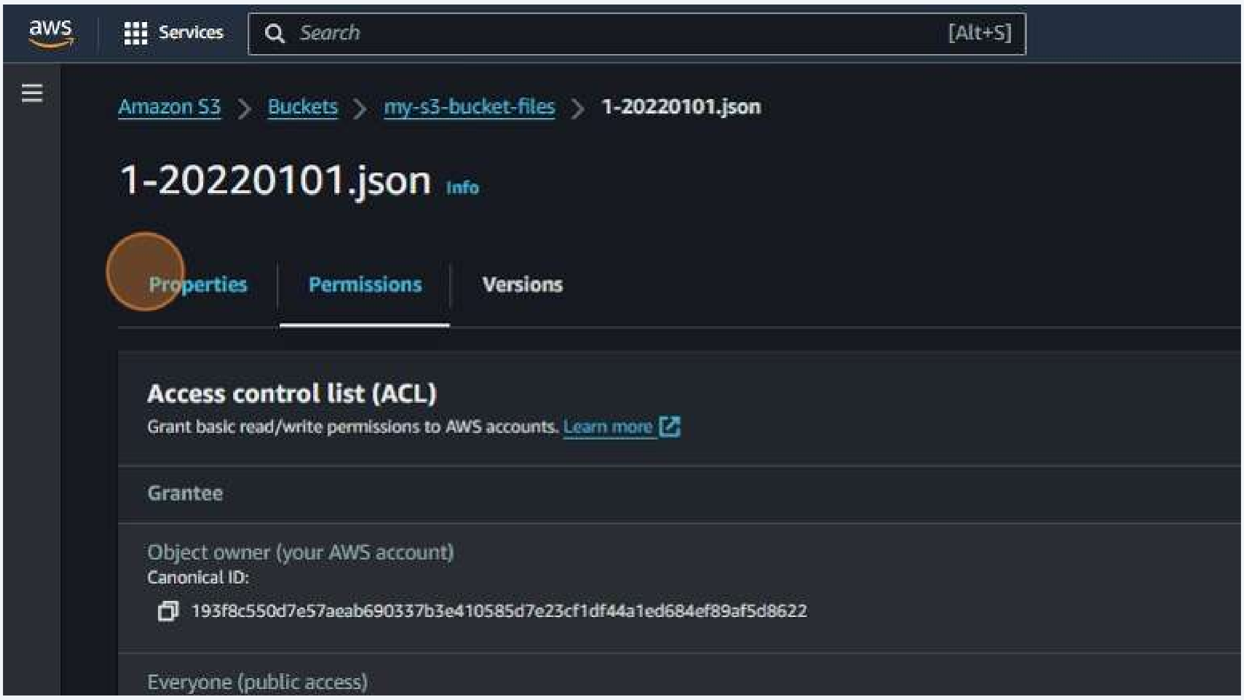
AWS Region

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

Last modified

February 13, 2024, 22:02:36 (UTC+05:45)

27 Click "Properties"



1-20220101.json

Access control list (ACL)

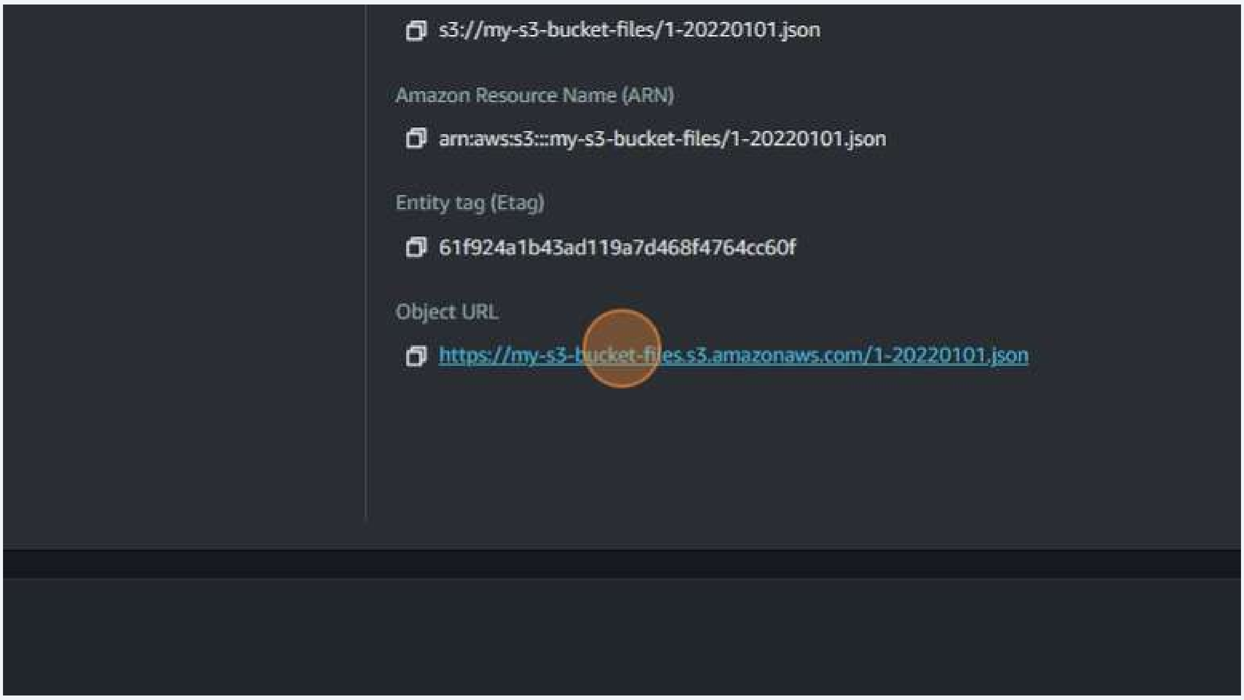
Grant basic read/write permissions to AWS accounts. Learn more

Grantee

Object owner (your AWS account)
Canonical ID:
193f8c550d7e57aeab690337b3e410585d7e23cf1df44a1ed684ef89af5d8622

Everyone (public access)

28 Click "[https://my-s3-bucket-files.s3.amazonaws.com/1-20220101.json](https://my-s3-bucket-files.s3.amazonaws.com/1-20220101.json)"



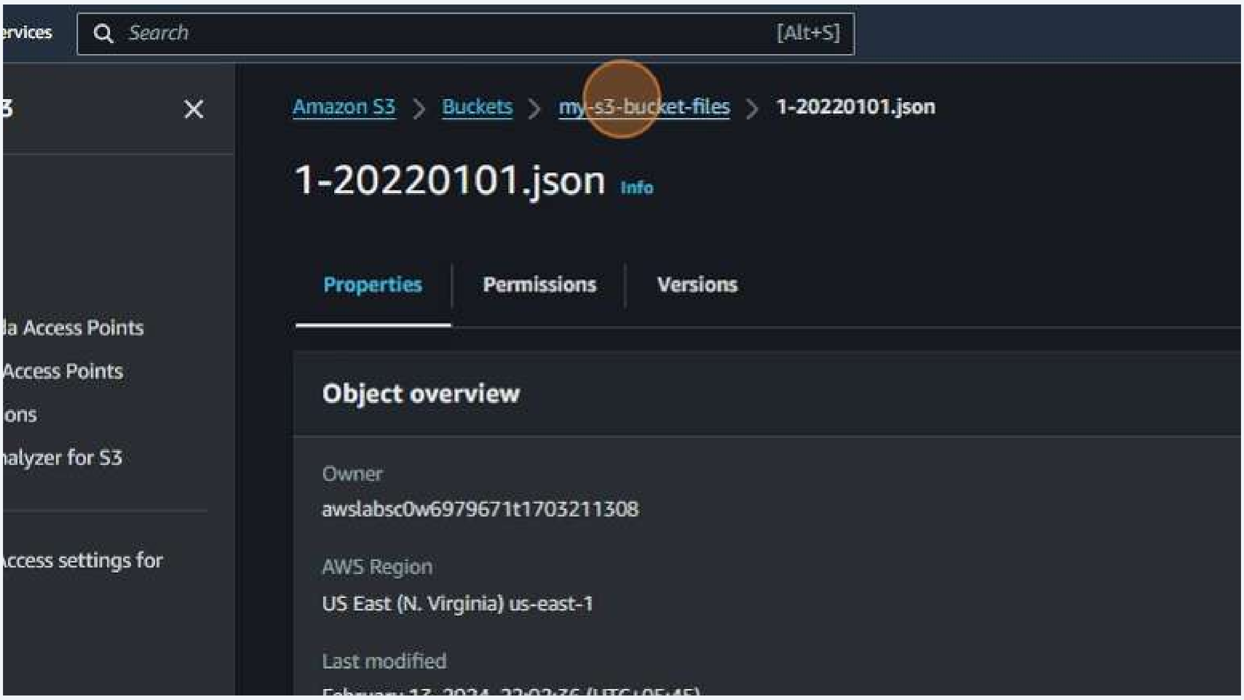
s3://my-s3-bucket-files/1-20220101.json

Amazon Resource Name (ARN)
arn:aws:s3:::my-s3-bucket-files/1-20220101.json

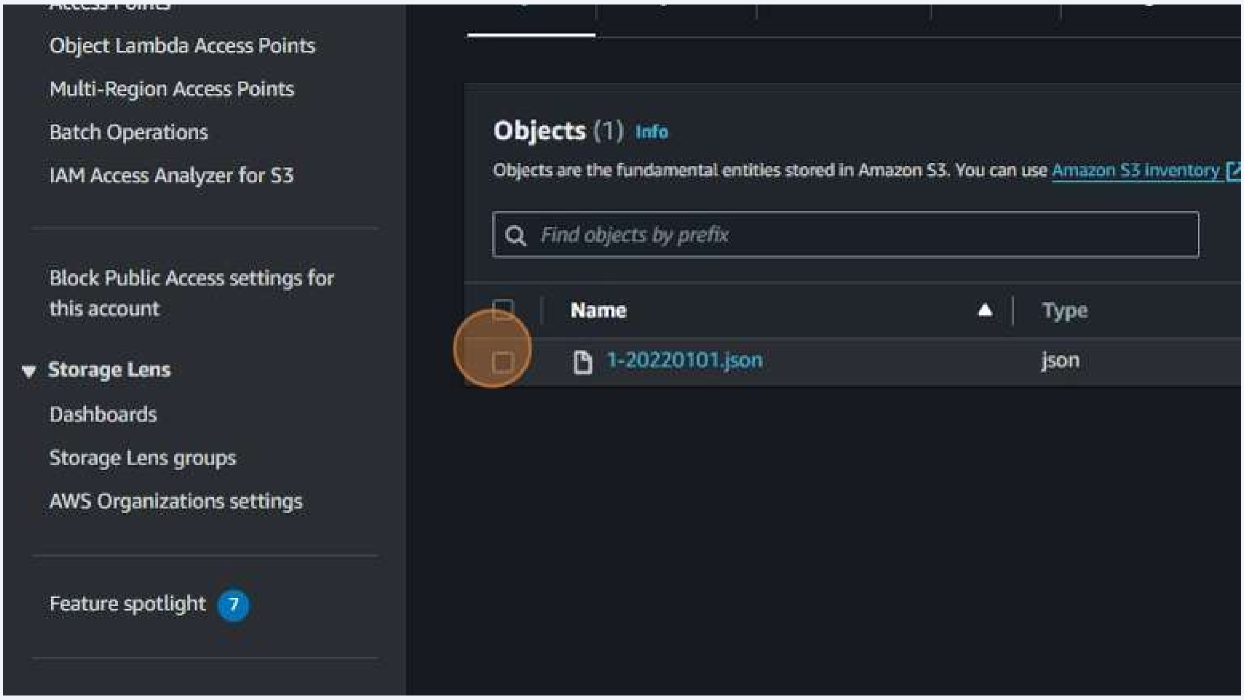
Entity tag (Etag)
61f924a1b43ad119a7d468f4764cc60f

Object URL
https://my-s3-bucket-files.s3.amazonaws.com/1-20220101.json

29 Click "my-s3-bucket-files"

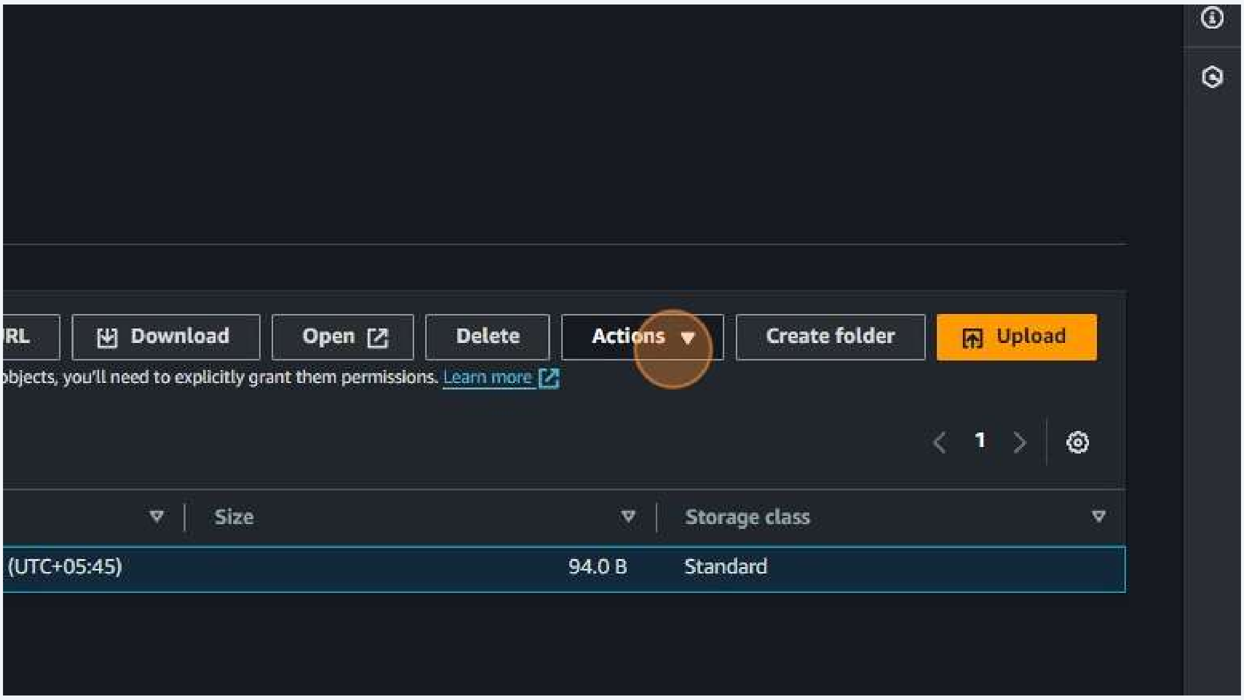


30 Click this checkbox.

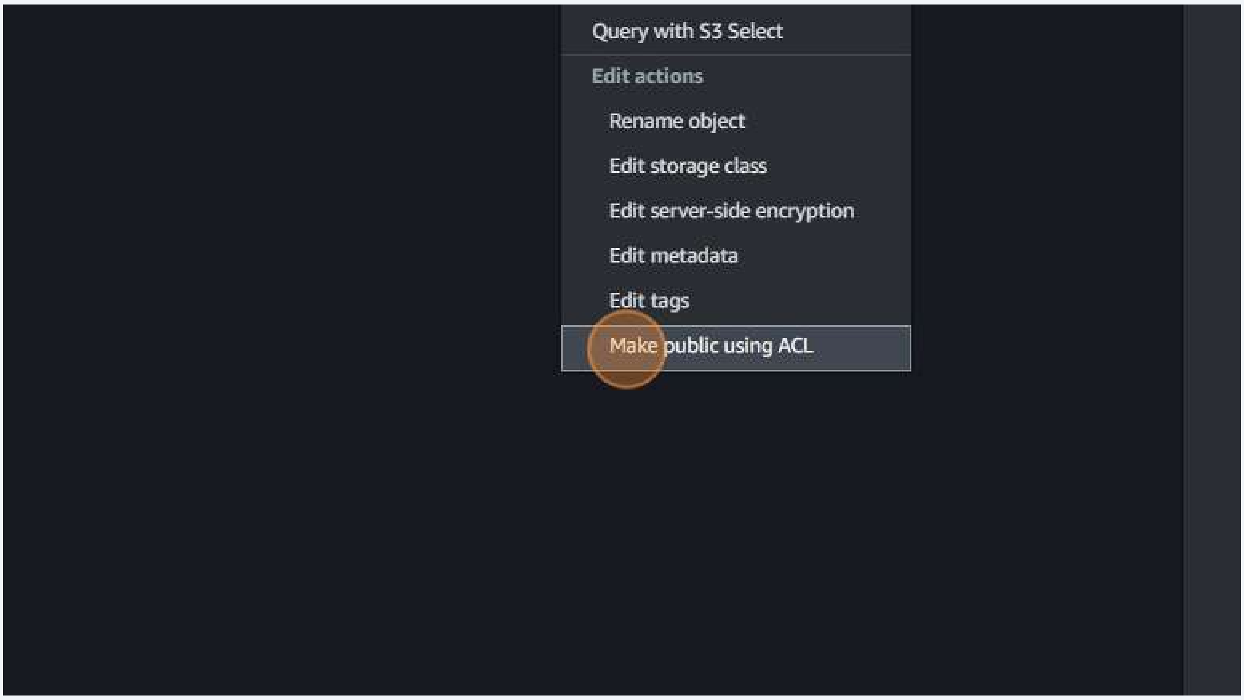


Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
▼ Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight 7
Objects (1) Info
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory
Find objects by prefix
Name
Type
1-20220101.json
json

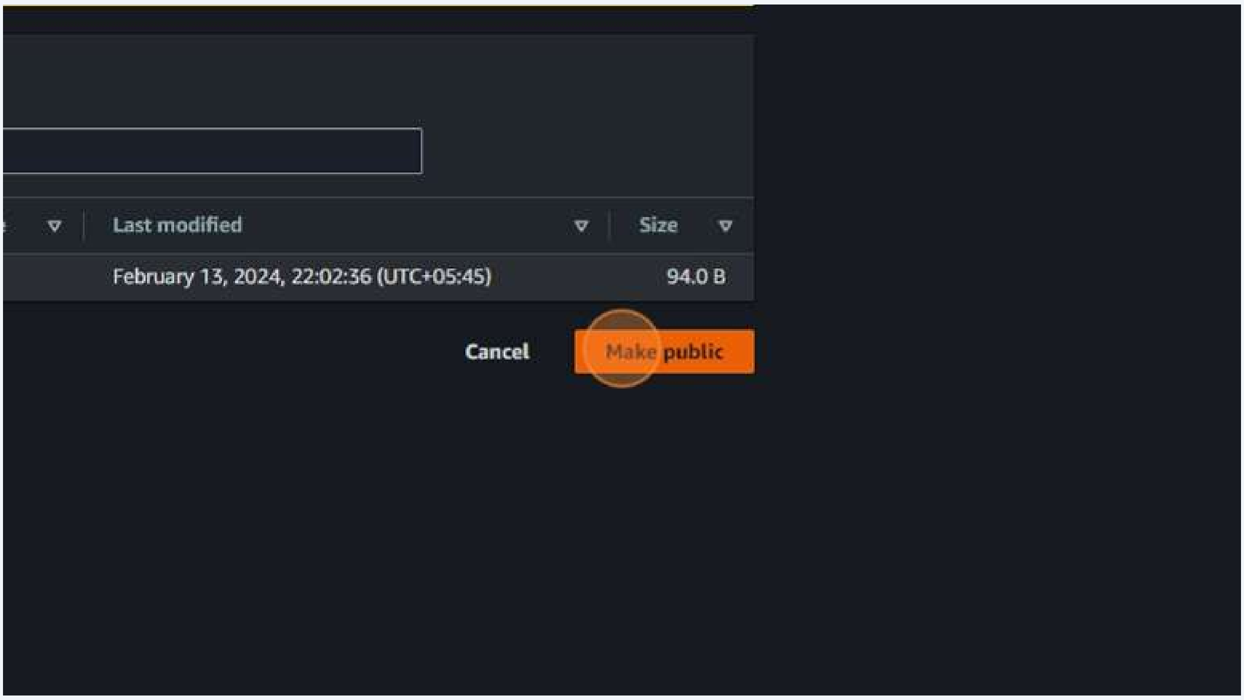
31 Click "Actions"



32 Click "Make public using ACL"

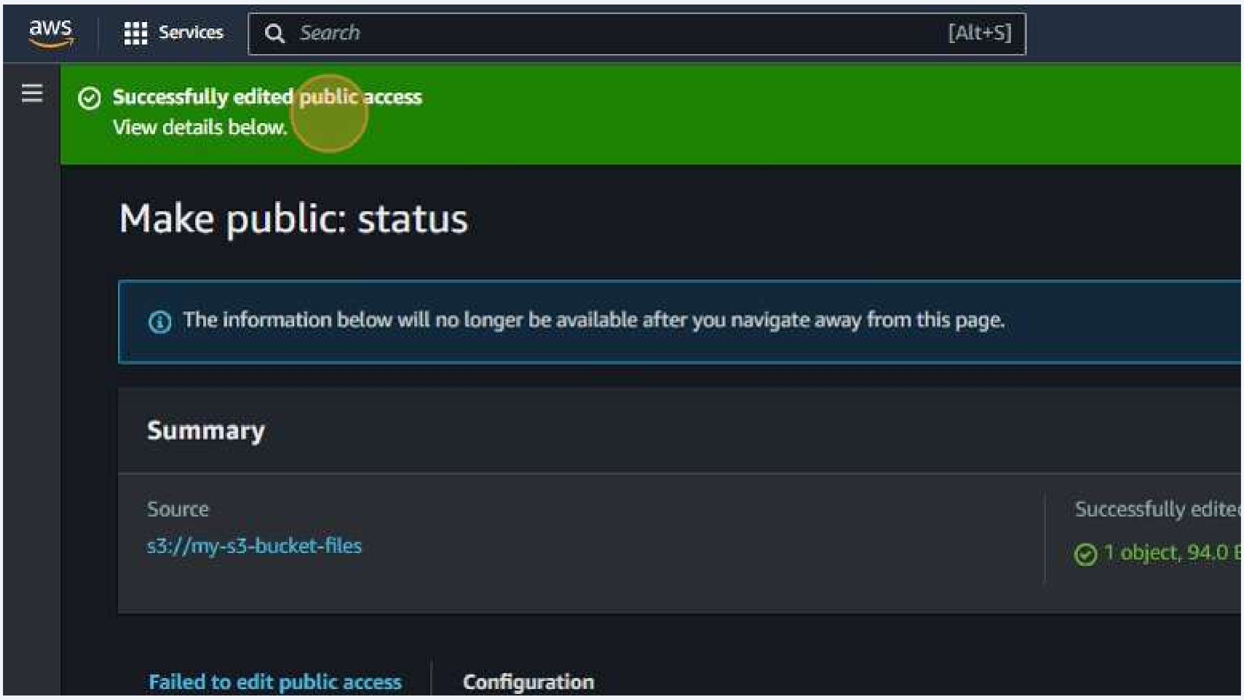


33 Click "Make public"



February 13, 2024, 22:02:36 (UTC+05:45) 94.0 B

34 Click "View details below."



Successfully edited public access
View details below.

Make public: status

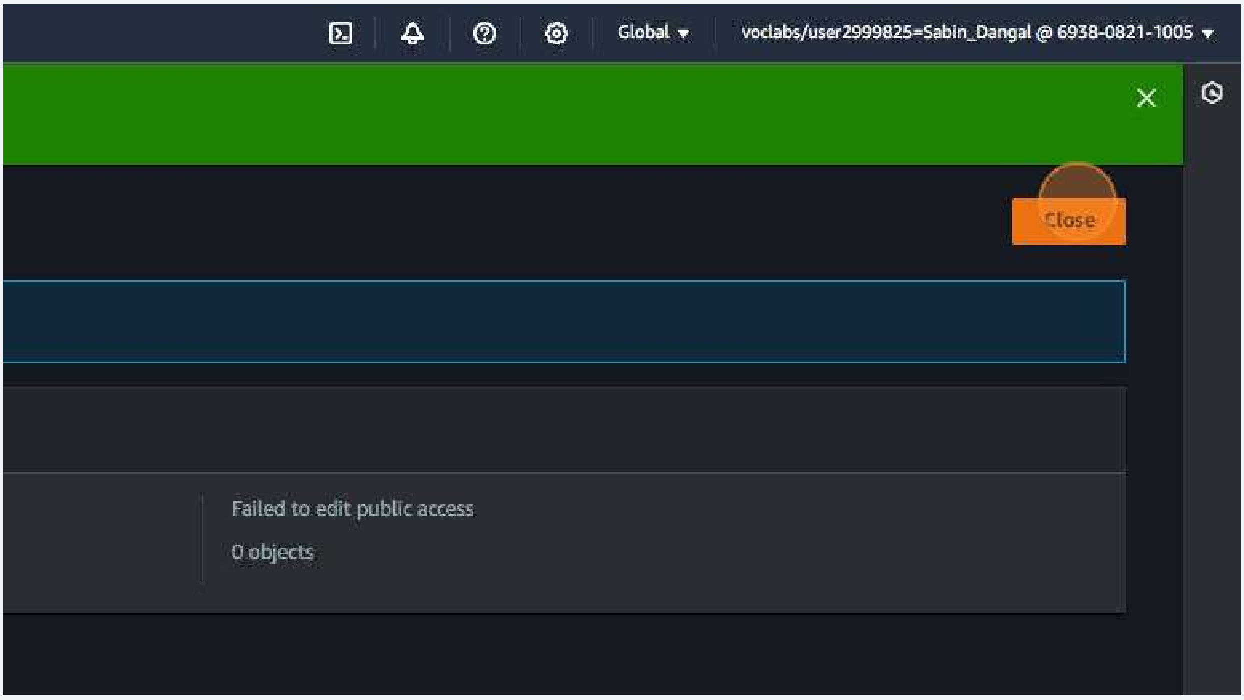
The information below will no longer be available after you navigate away from this page.

Summary

Source
s3://my-s3-bucket-files

Successfully edite
1 object, 94.0 B

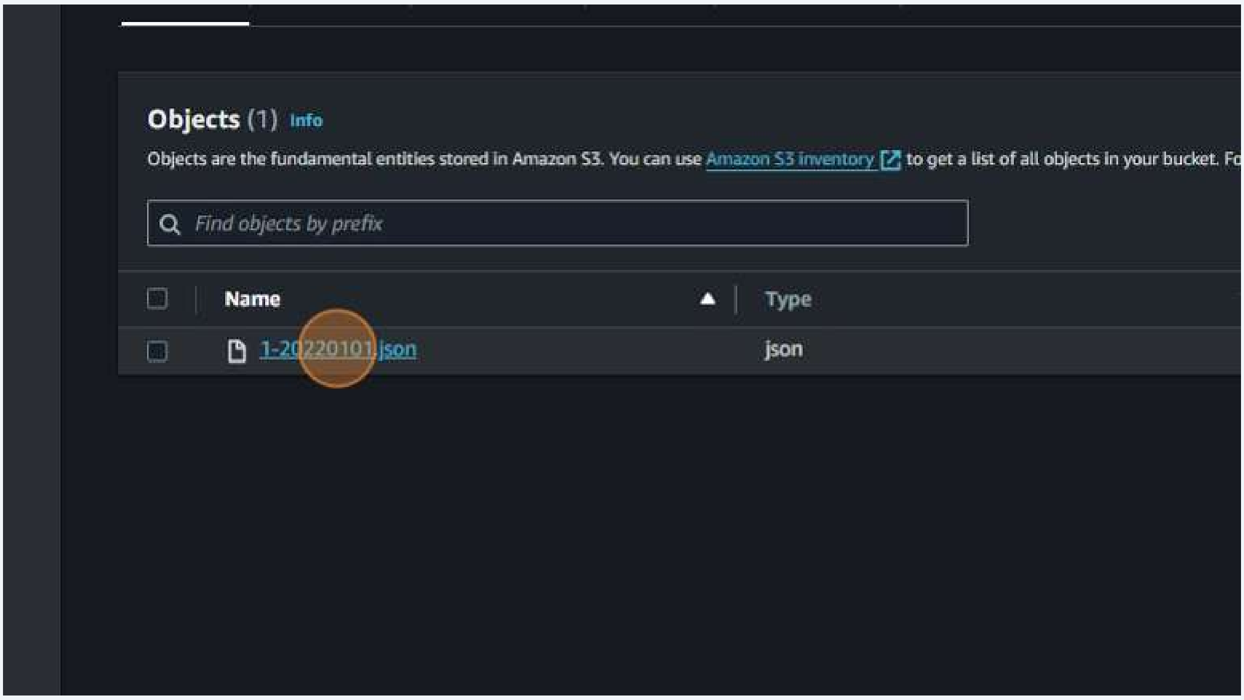
**35** Click "Close"



Failed to edit public access

0 objects

**36** Click "1-20220101.json"

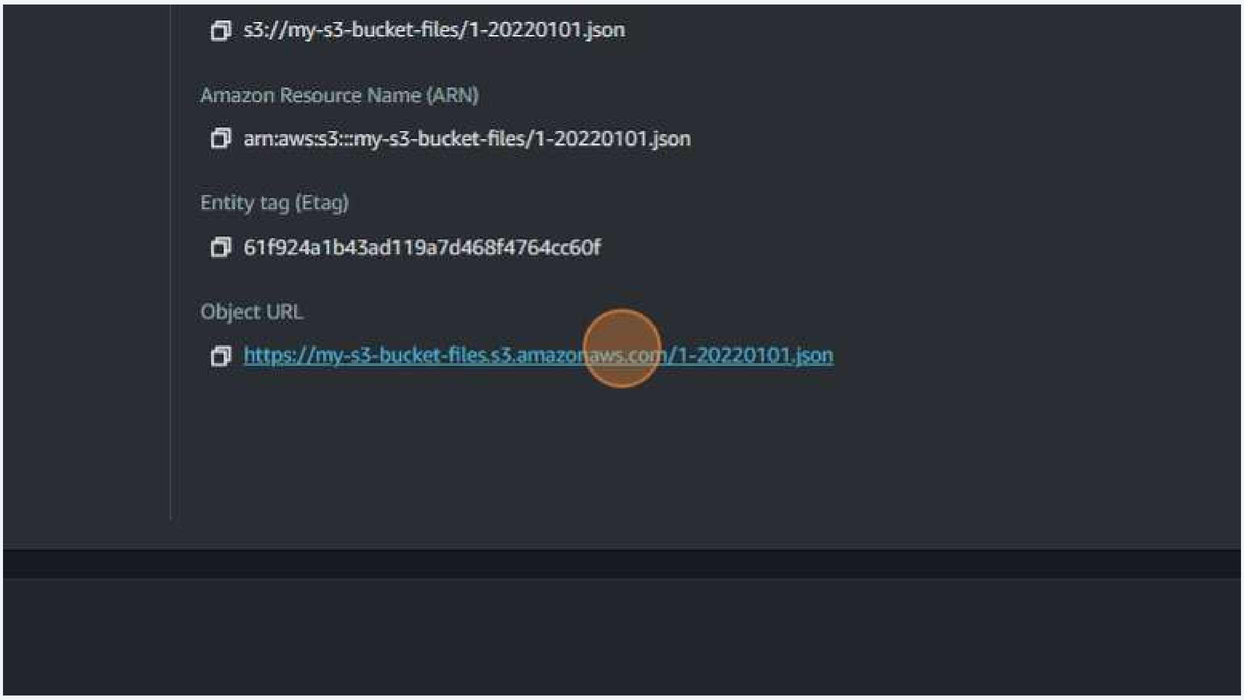


Objects (1) Info

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. Fo

| Name | Type |
|---|---|
| 1-20220101.json | json |

37 Click "[https://my-s3-bucket-files.s3.amazonaws.com/1-20220101.json](https://my-s3-bucket-files.s3.amazonaws.com/1-20220101.json)"



s3://my-s3-bucket-files/1-20220101.json

Amazon Resource Name (ARN)

arn:aws:s3:::my-s3-bucket-files/1-20220101.json

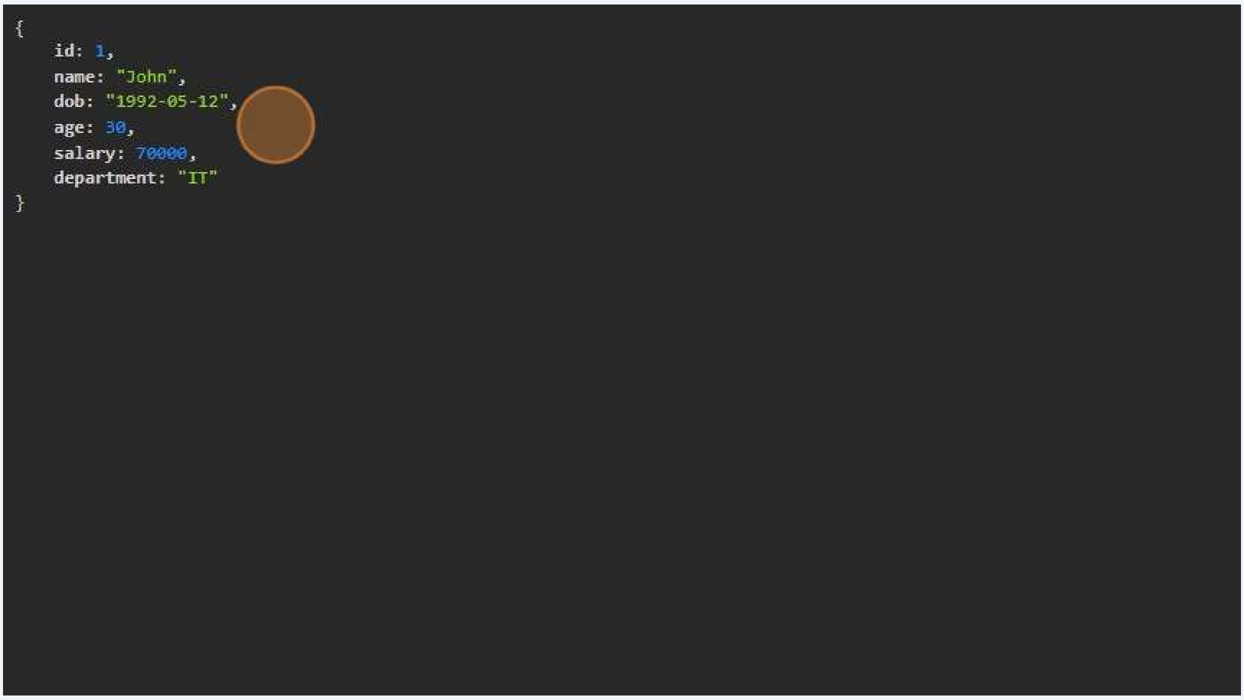
Entity tag (Etag)

61f924a1b43ad119a7d468f4764cc60f

Object URL

https://my-s3-bucket-files.s3.amazonaws.com/1-20220101.json

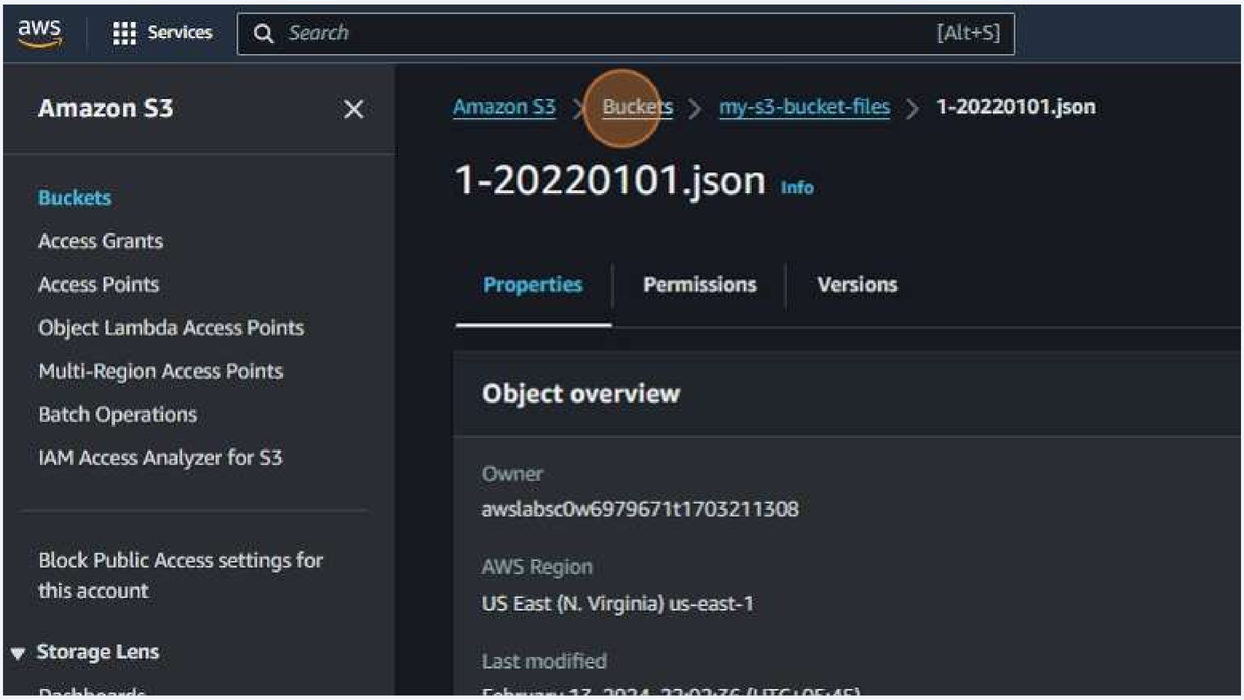
38 Click "age: 30,"



```
{
    id: 1,
    name: "John",
    dob: "1992-05-12",
    age: 30,
    salary: 70000,
    department: "IT"
}
```

39 Navigate to https://s3.console.aws.amazon.com/s3/object/my-s3-bucket-files?region=us-east-1&bucketType=general&prefix=1-20220101.json

40 Click "Buckets"

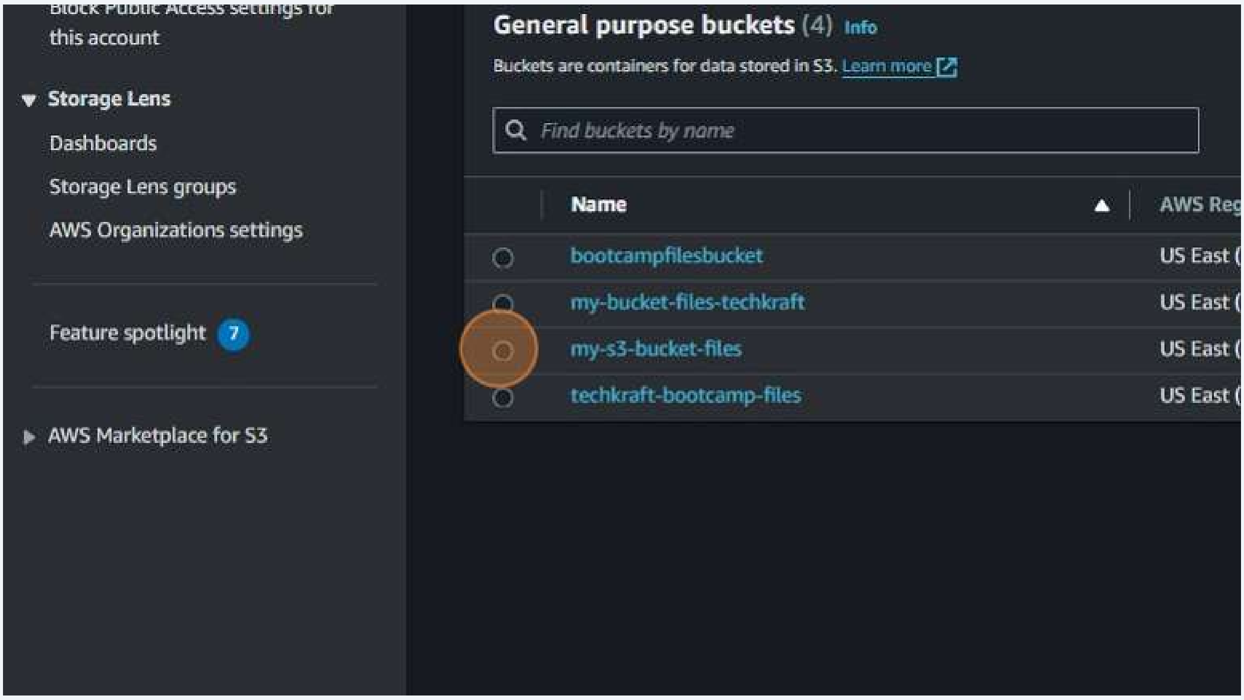

aws
Services
Search
[Alt+S]
Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Amazon S3 > Buckets > my-s3-bucket-files > 1-20220101.json
1-20220101.json Info
Properties
Permissions
Versions
Object overview

Owner
awslabsc0w6979671t1703211308

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

Last modified

41 Lists of buckets

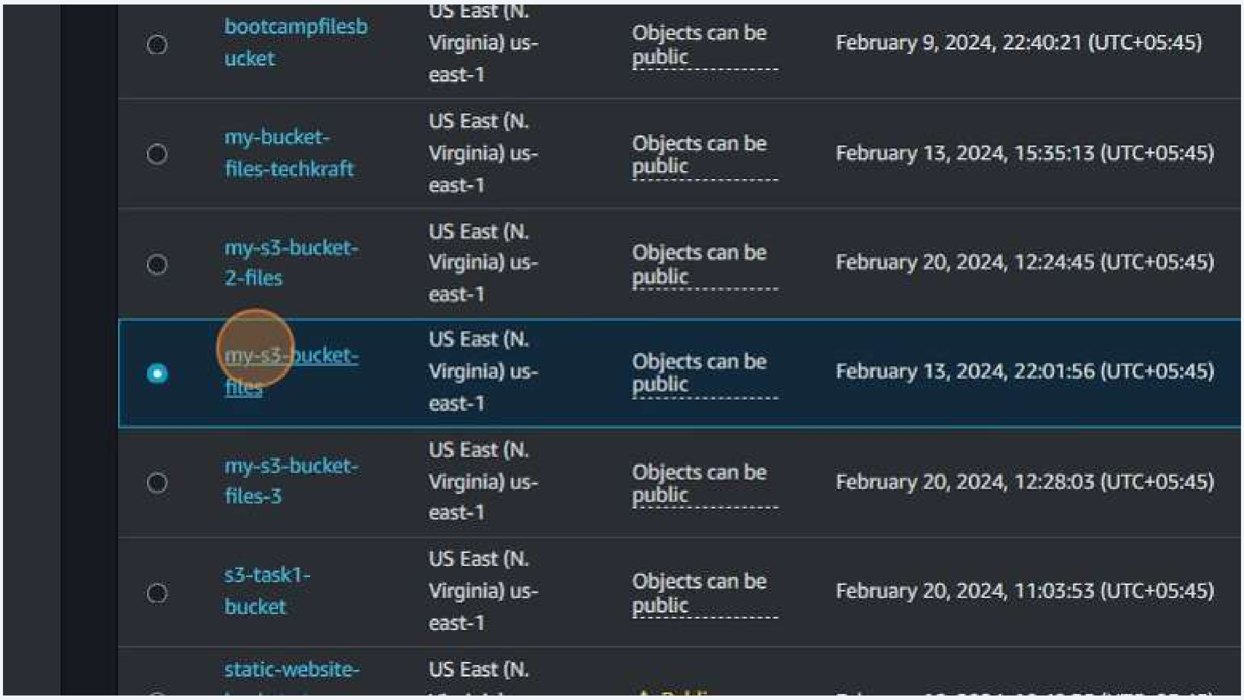


Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight 7
AWS Marketplace for S3
General purpose buckets (4) Info
Buckets are containers for data stored in S3. Learn more
Find buckets by name

| | Name | AWS Reg |
|---|---|---|
| ○ | bootcampfilesbucket | US East ( |
| ○ | my-bucket-files-techkraft | US East ( |
| ○ | my-s3-bucket-files | US East ( |
| ○ | techkraft-bootcamp-files | US East ( |

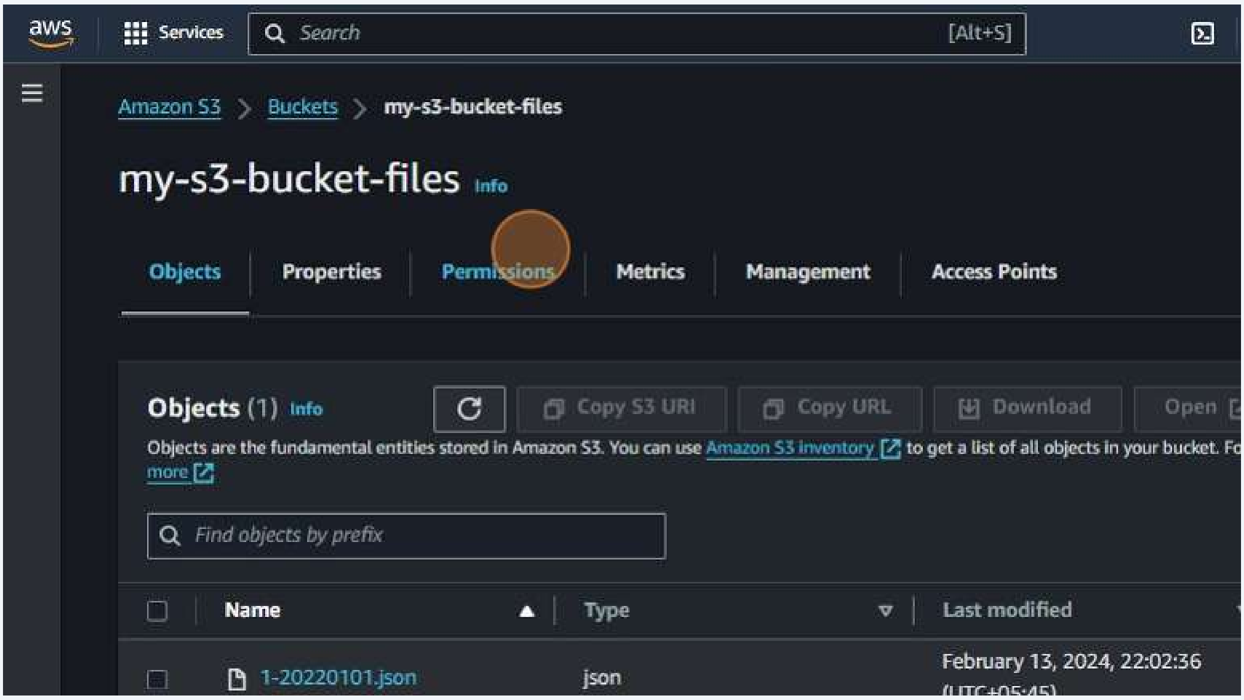
42 Navigate to https://s3.console.aws.amazon.com/s3/buckets?region=us-east-1&bucketType=general&region=us-east-1

**43** Click "my-s3-bucket-files"



| | | | | |
|---|---|---|---|---|
| ○ | bootcampfilesbucket | US East (N. Virginia) us-east-1 | Objects can be public | February 9, 2024, 22:40:21 (UTC+05:45) |
| ○ | my-bucket-files-techkraft | US East (N. Virginia) us-east-1 | Objects can be public | February 13, 2024, 15:35:13 (UTC+05:45) |
| ○ | my-s3-bucket-2-files | US East (N. Virginia) us-east-1 | Objects can be public | February 20, 2024, 12:24:45 (UTC+05:45) |
| ● | my-s3-bucket-files | US East (N. Virginia) us-east-1 | Objects can be public | February 13, 2024, 22:01:56 (UTC+05:45) |
| ○ | my-s3-bucket-files-3 | US East (N. Virginia) us-east-1 | Objects can be public | February 20, 2024, 12:28:03 (UTC+05:45) |
| ○ | s3-task1-bucket | US East (N. Virginia) us-east-1 | Objects can be public | February 20, 2024, 11:03:53 (UTC+05:45) |
| | static-website- | US East (N. | | |

**44** Click "Permissions"



Amazon S3 > Buckets > my-s3-bucket-files

my-s3-bucket-files Info

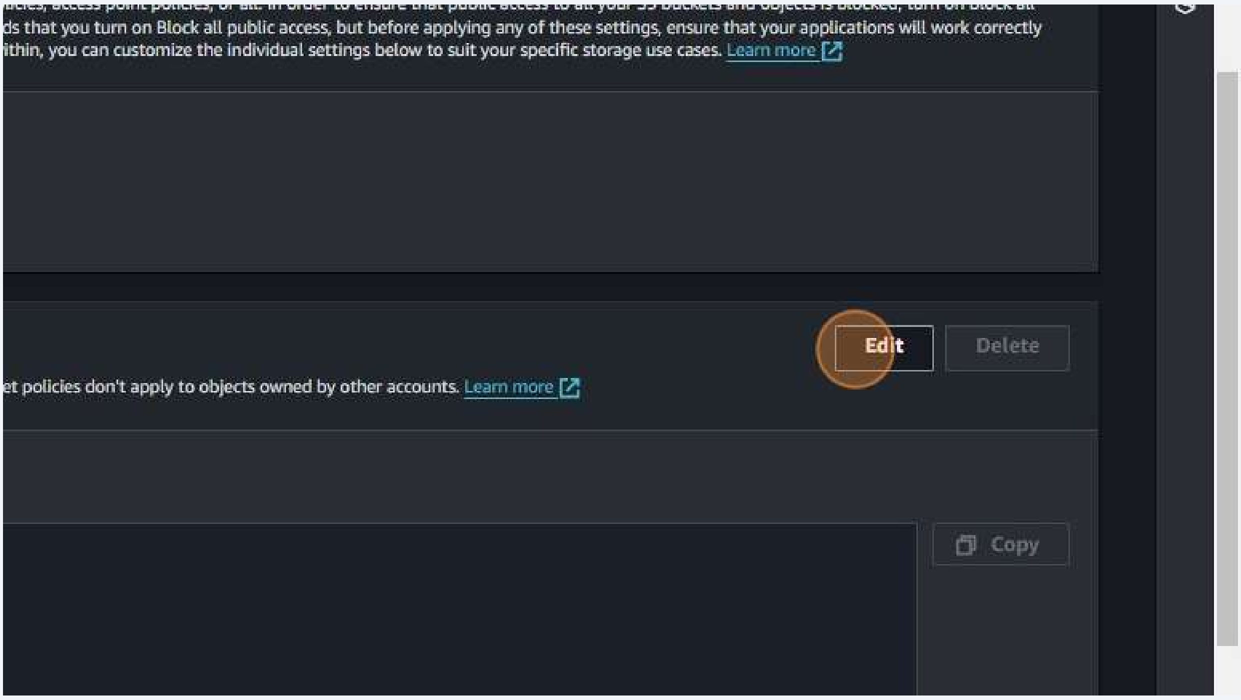
Objects (1) Info

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. Fo more

Find objects by prefix

| □ | Name ▲ | Type ▽ | Last modified |
|---|---|---|---|
| □ | 1-20220101.json | json | February 13, 2024, 22:02:36 (UTC+05:45) |

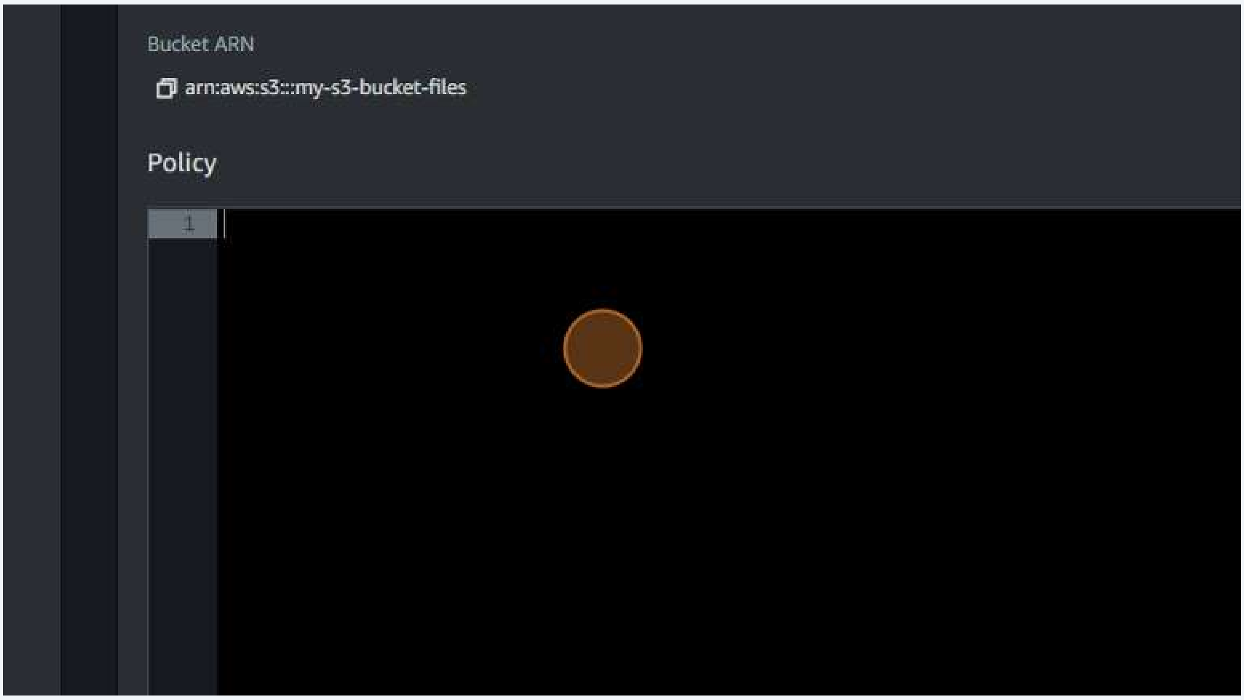
45 Click "Edit"



ds that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly
ithin, you can customize the individual settings below to suit your specific storage use cases. Learn more

et policies don't apply to objects owned by other accounts. Learn more

46 Click here.

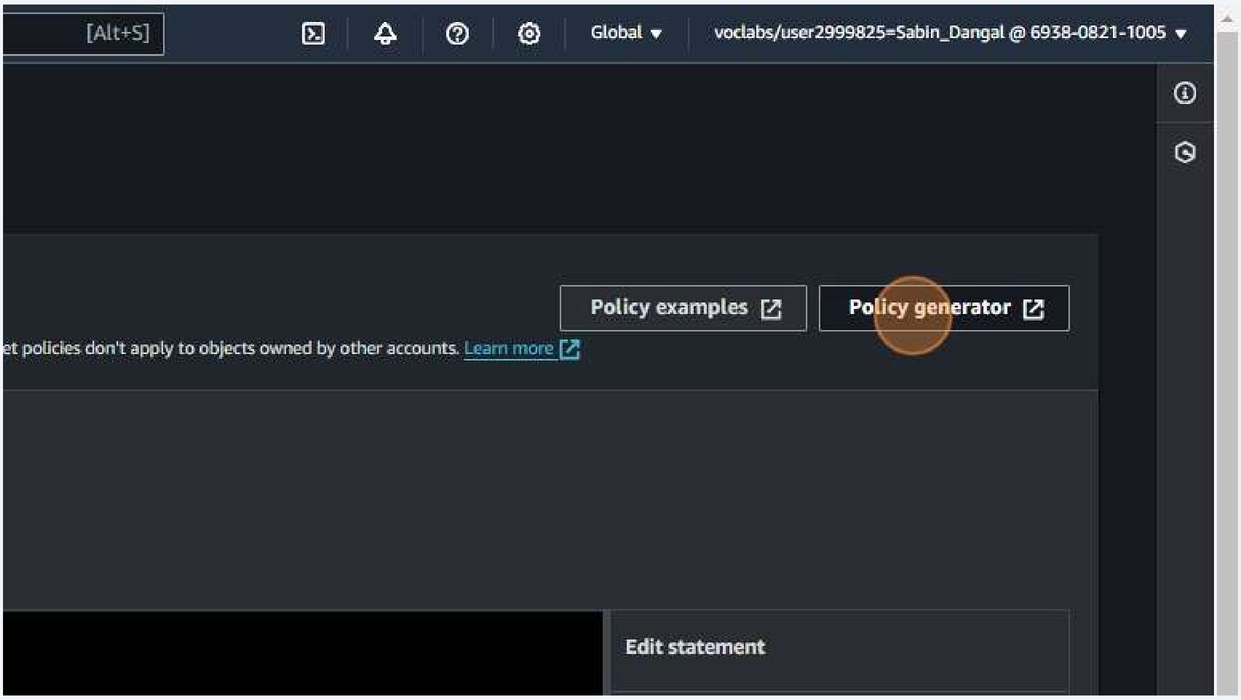


Bucket ARN

arn:aws:s3:::my-s3-bucket-files

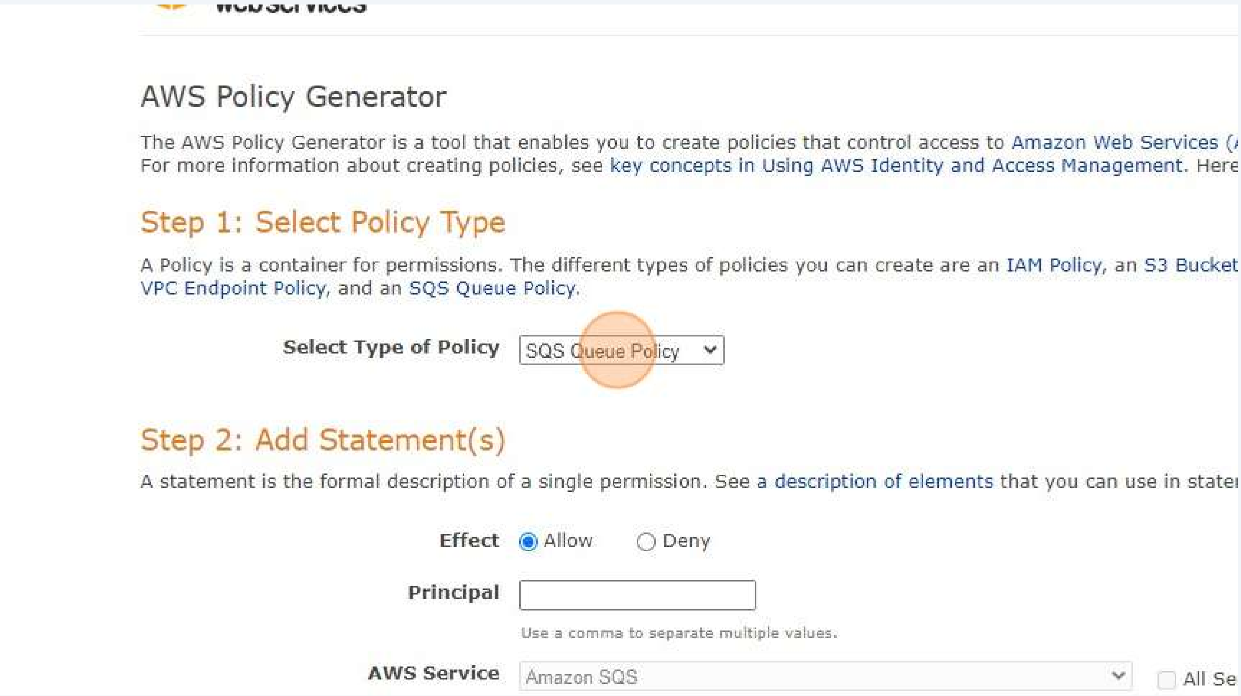
Policy

47 Click "Policy generator"



[Alt+S]
Global
voclabs/user2999825=Sabin_Dangal @ 6938-0821-1005
Policy examples
Policy generator
et policies don't apply to objects owned by other accounts. Learn more
Edit statement

48 Click this dropdown.



AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (
For more information about creating policies, see key concepts in Using AWS Identity and Access Management. Here

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket
VPC Endpoint Policy, and an SQS Queue Policy.

Select Type of Policy: SQS Queue Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a description of elements that you can use in state

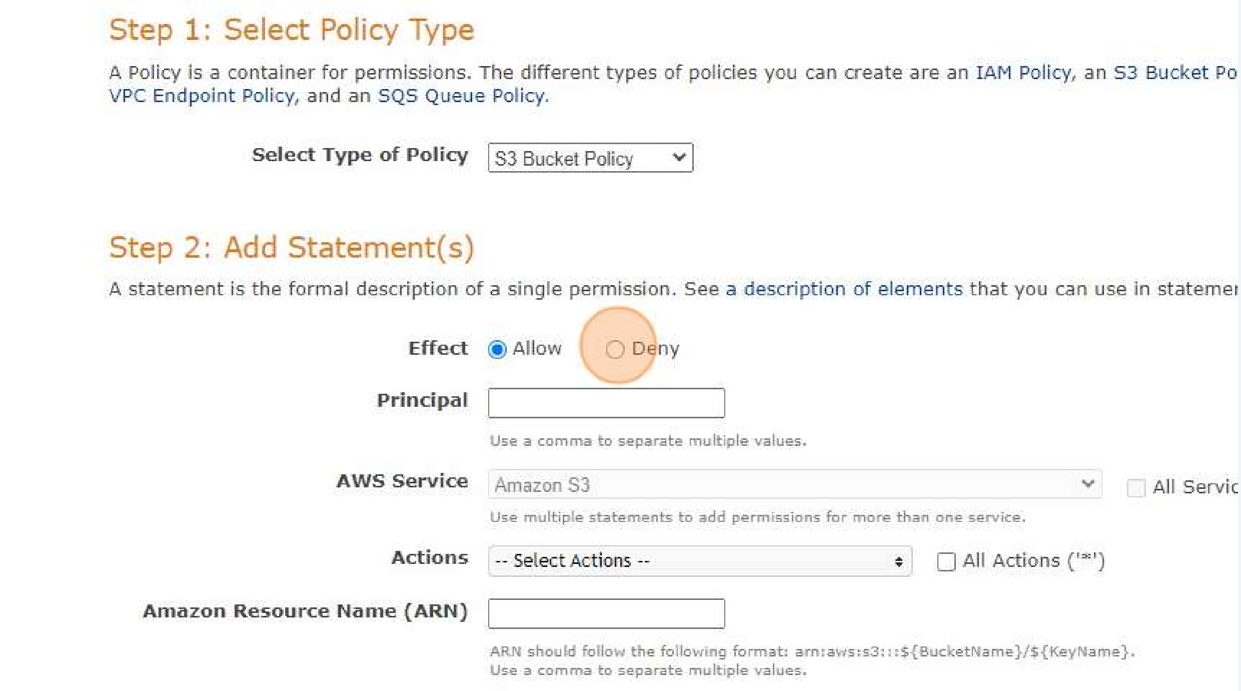
Effect: ● Allow ○ Deny

Principal:

Use a comma to separate multiple values.

AWS Service: Amazon SQS □ All Se

49 Click this radio button.



Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Po VPC Endpoint Policy, and an SQS Queue Policy.

Select Type of Policy: S3 Bucket Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a description of elements that you can use in statemer

Effect: ● Allow ○ Deny

Principal:

Use a comma to separate multiple values.

AWS Service: Amazon S3 □ All Servic

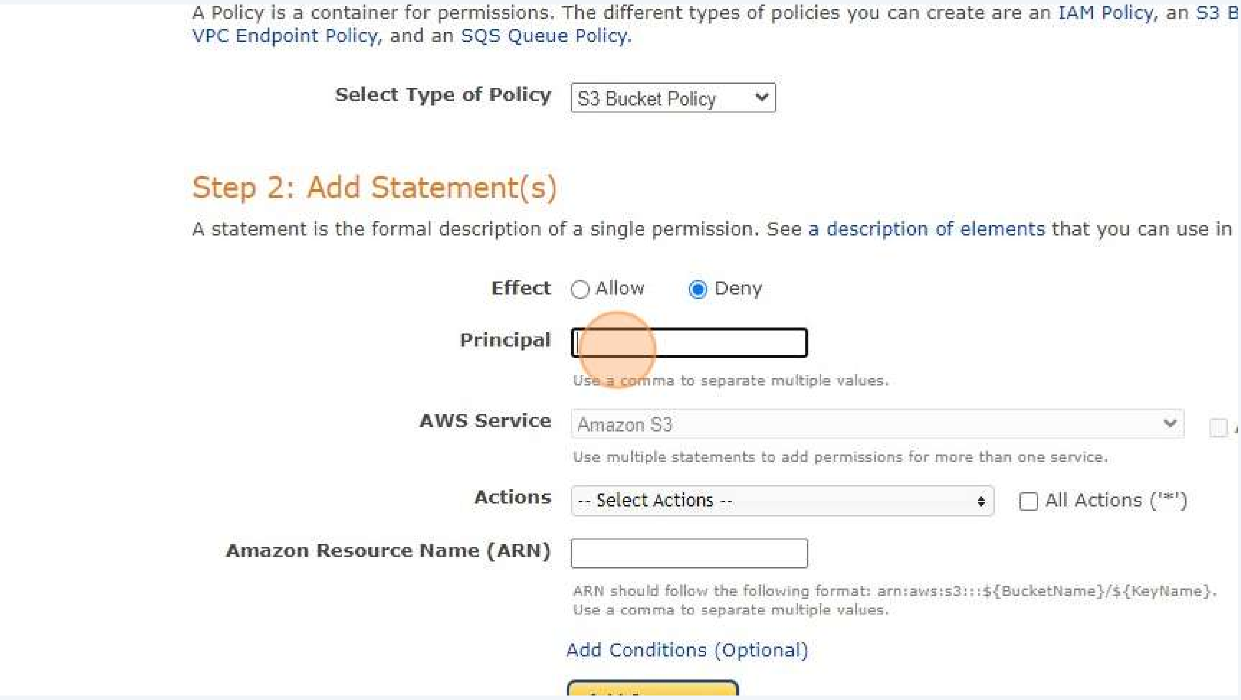
Use multiple statements to add permissions for more than one service.

Actions: -- Select Actions -- □ All Actions ('*')

Amazon Resource Name (ARN):

ARN should follow the following format: arn:aws:s3:::${BucketName}/${KeyName}.
Use a comma to separate multiple values.

50 Click the "Principal" field.



A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 B VPC Endpoint Policy, and an SQS Queue Policy.

Select Type of Policy: S3 Bucket Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a description of elements that you can use in

Effect: ○ Allow ● Deny

Principal:

Use a comma to separate multiple values.

AWS Service: Amazon S3 □

Use multiple statements to add permissions for more than one service.

Actions: -- Select Actions -- □ All Actions ('*')

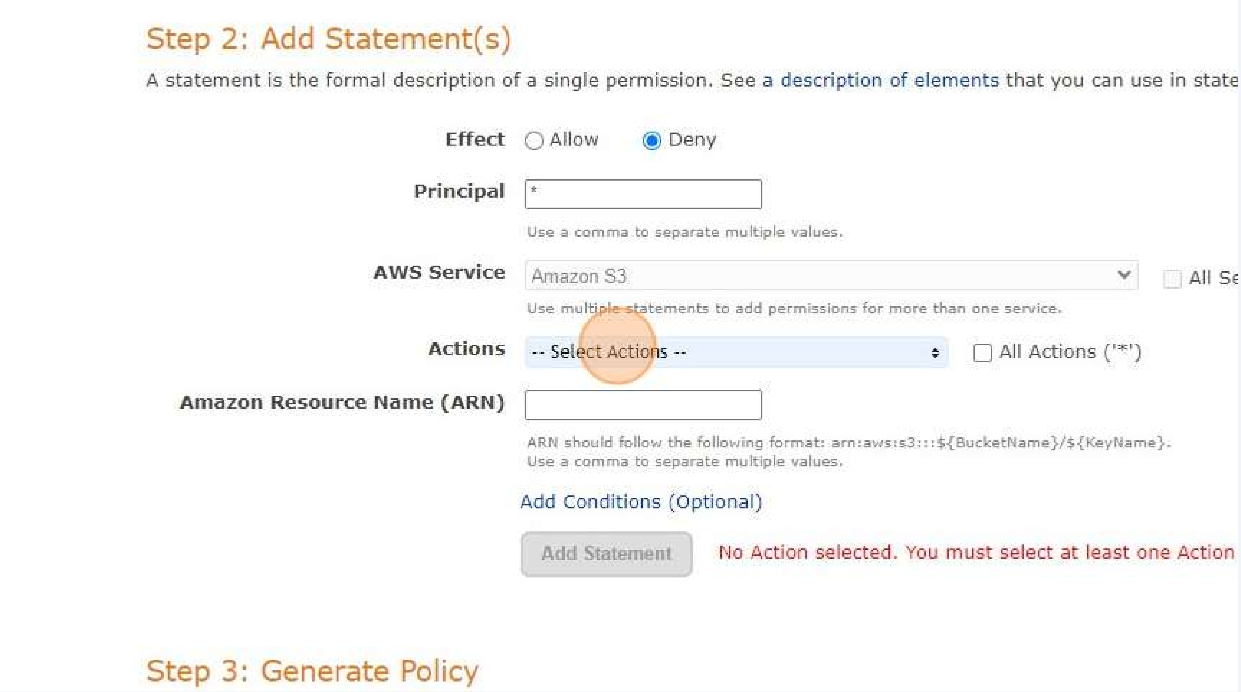
Amazon Resource Name (ARN):

ARN should follow the following format: arn:aws:s3:::${BucketName}/${KeyName}.
Use a comma to separate multiple values.

Add Conditions (Optional)

**51** Type "*"

**52** Click "-- Select Actions --"



Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a description of elements that you can use in state

Effect ○ Allow ● Deny

Principal *

Use a comma to separate multiple values.

AWS Service Amazon S3 □ All Se

Use multiple statements to add permissions for more than one service.

Actions -- Select Actions -- □ All Actions ('*')

Amazon Resource Name (ARN)

ARN should follow the following format: arn:aws:s3:::${BucketName}/${KeyName}.
Use a comma to separate multiple values.

Add Conditions (Optional)

Add Statement No Action selected. You must select at least one Action

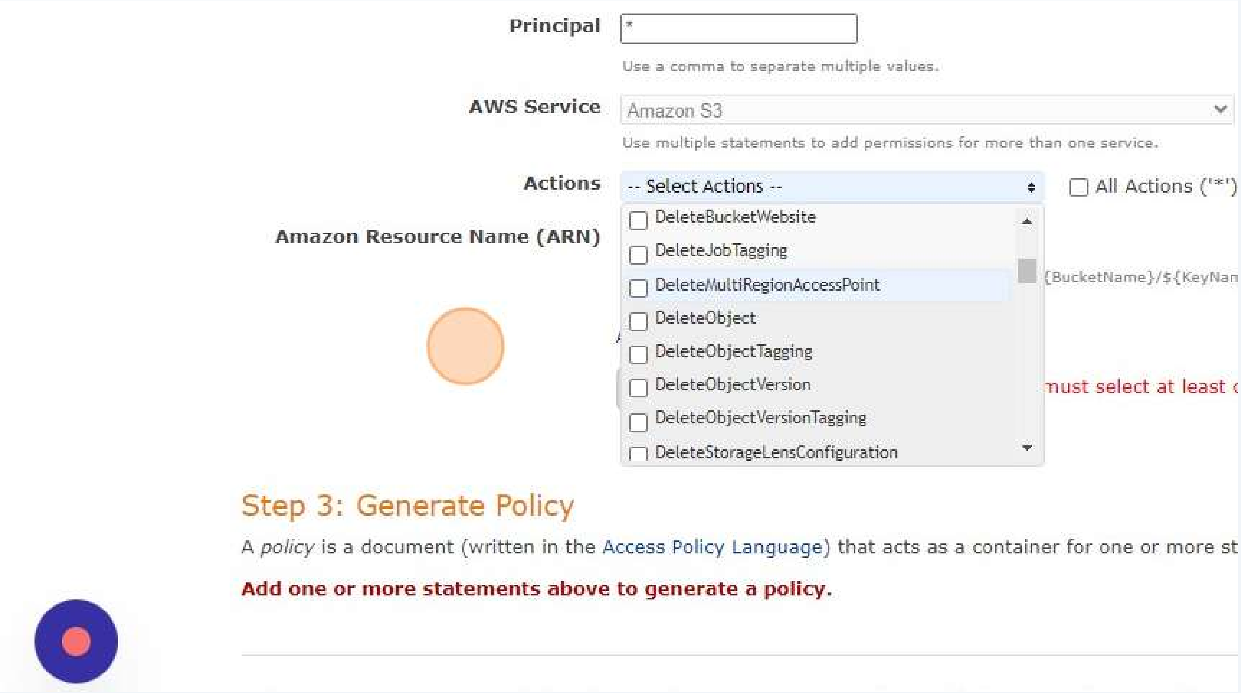
Step 3: Generate Policy

53

Click "Effect
Allow Deny
Principal

Use a comma to separate multiple values.

AWS Service
AWS Account Management
AWS Activate
AWS Amplify
AWS Amplify..."



Principal *

Use a comma to separate multiple values.

AWS Service Amazon S3

Use multiple statements to add permissions for more than one service.

Actions -- Select Actions -- □ All Actions ('*')

□ DeleteBucketWebsite
□ DeleteJobTagging
□ DeleteMultiRegionAccessPoint
□ DeleteObject
□ DeleteObjectTagging
□ DeleteObjectVersion
□ DeleteObjectVersionTagging
□ DeleteStorageLensConfiguration

Amazon Resource Name (ARN) {BucketName}/${KeyNam

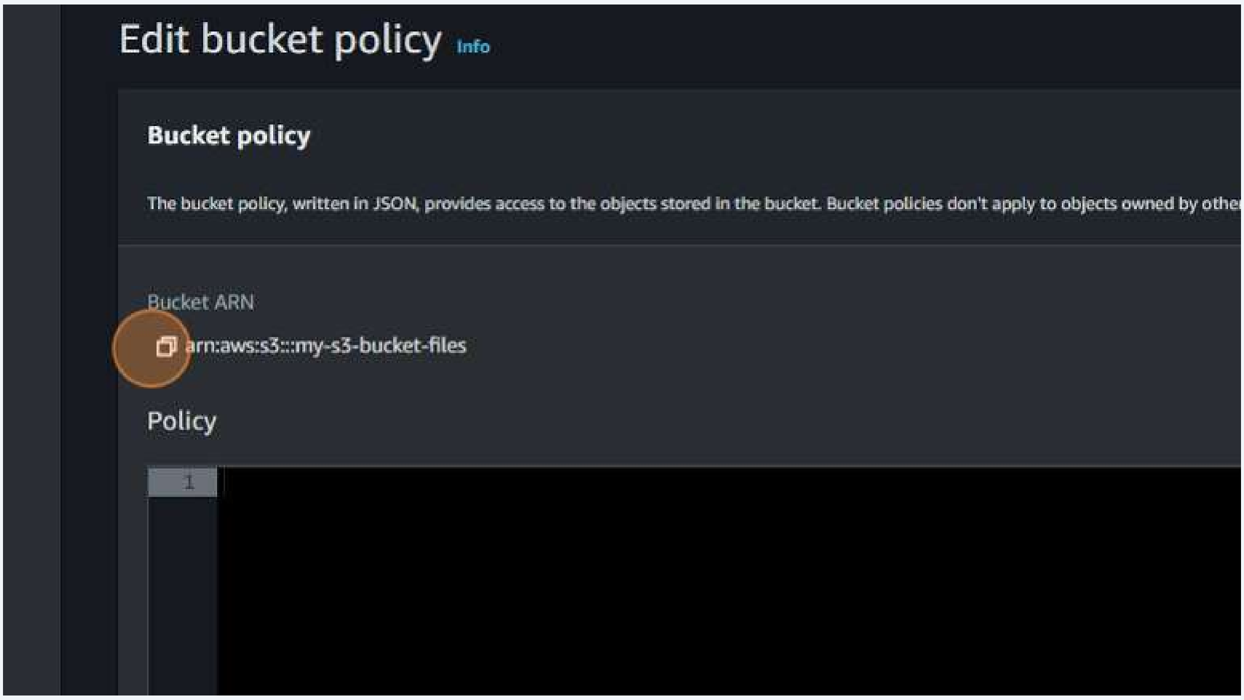
must select at least o

Step 3: Generate Policy

A *policy* is a document (written in the Access Policy Language) that acts as a container for one or more st

**Add one or more statements above to generate a policy.**

54 Click here.



Edit bucket policy Info

**Bucket policy**

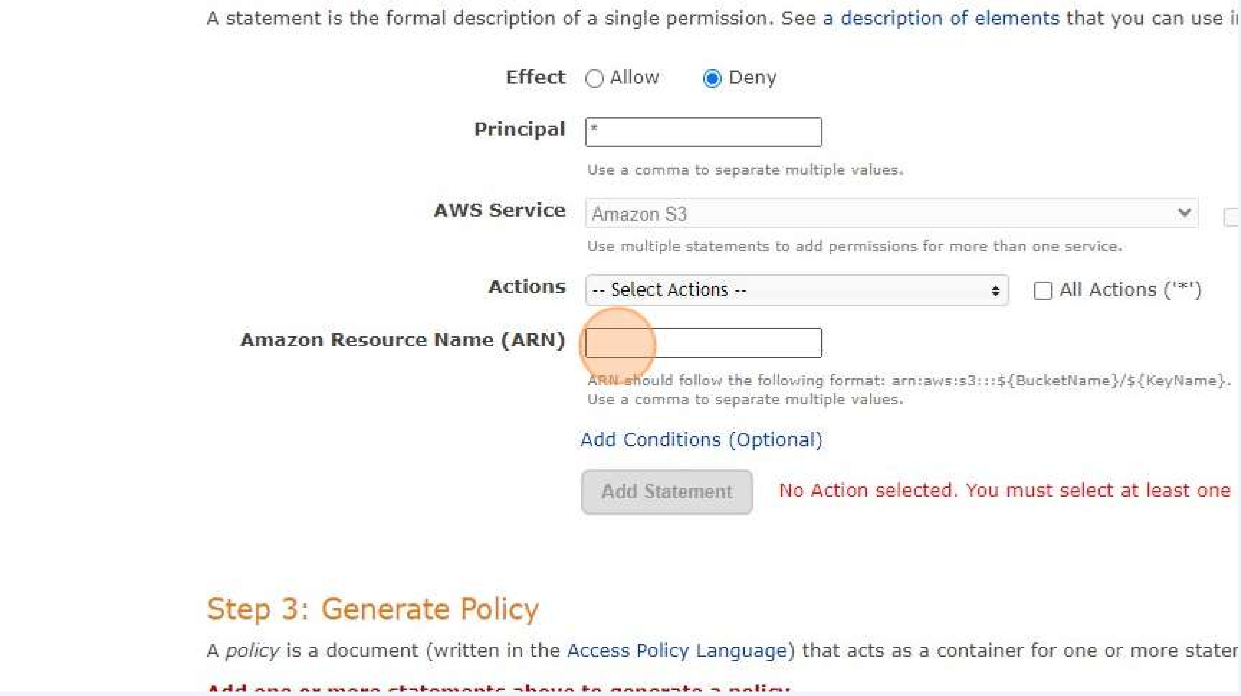
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by othe

Bucket ARN

arn:aws:s3:::my-s3-bucket-files

Policy

55 Click the "Amazon Resource Name (ARN)" field.



A statement is the formal description of a single permission. See a description of elements that you can use i

Effect ○ Allow ● Deny

Principal *

Use a comma to separate multiple values.

AWS Service Amazon S3

Use multiple statements to add permissions for more than one service.

Actions -- Select Actions -- □ All Actions ('*')

Amazon Resource Name (ARN)

ARN should follow the following format: arn:aws:s3:::${BucketName}/${KeyName}.
Use a comma to separate multiple values.

Add Conditions (Optional)

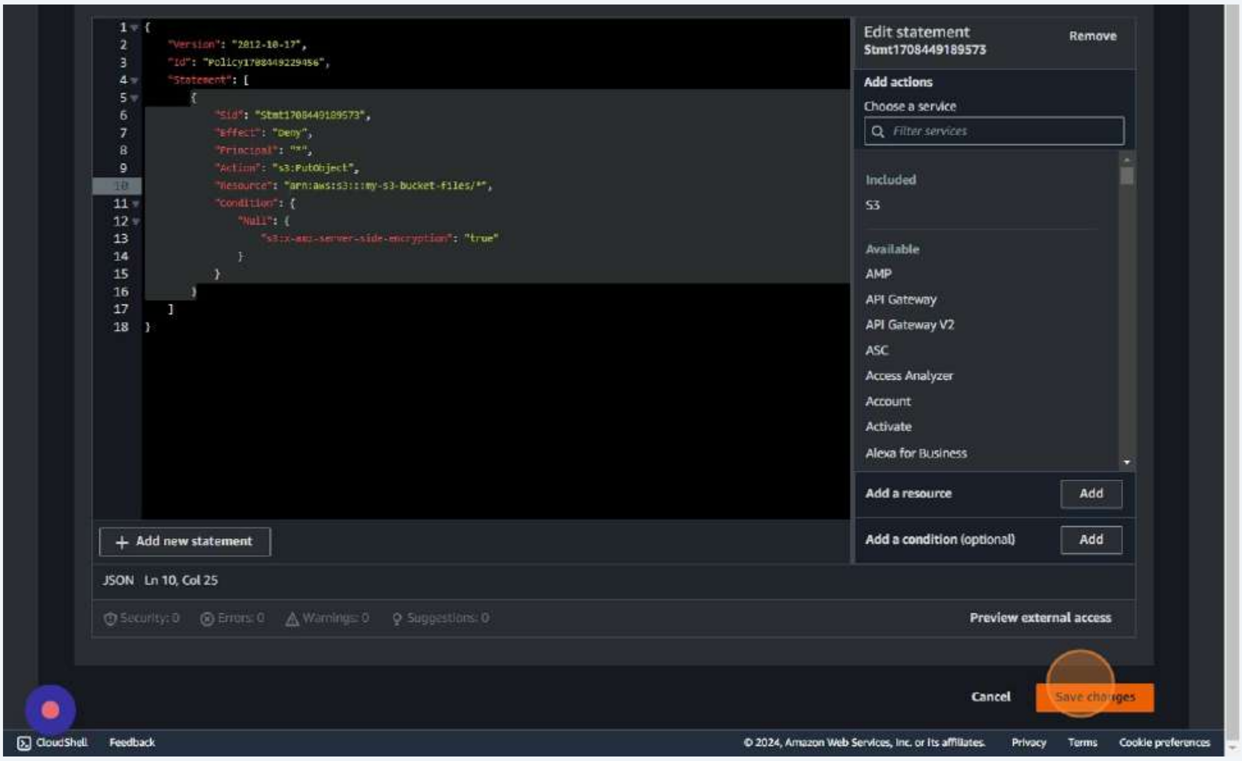
Add Statement   No Action selected. You must select at least one

Step 3: Generate Policy

A *policy* is a document (written in the Access Policy Language) that acts as a container for one or more stater

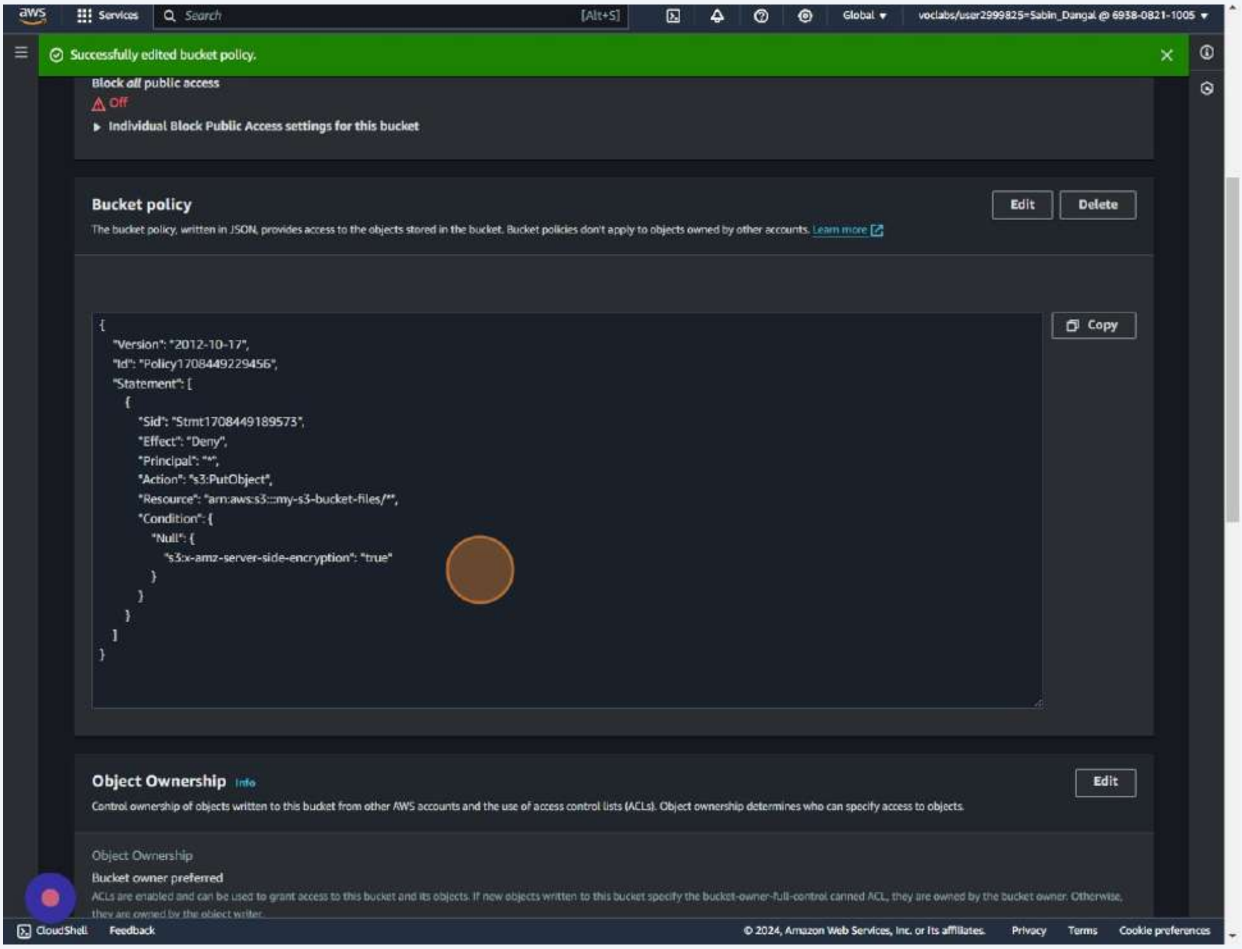
Add one or more statements above to generate a policy

## 56 Click "Save changes"



```
{
    "Version": "2012-10-17",
    "Id": "Policy1708449229456",
    "Statement": [
        {
            "Sid": "Stmt1708449189573",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::my-s3-bucket-files/*",
            "Condition": {
                "Null": {
                    "s3:x-amz-server-side-encryption": "true"
                }
            }
        }
    ]
}
```

57 Click this field.



Successfully edited bucket policy.

Block *all* public access

⚠ Off

▸ Individual Block Public Access settings for this bucket

**Bucket policy**

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

```
{
  "Version": "2012-10-17",
  "Id": "Policy1708449229456",
  "Statement": [
    {
      "Sid": "Stmt1708449189573",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::my-s3-bucket-files/*",
      "Condition": {
        "Null": {
          "s3:x-amz-server-side-encryption": "true"
        }
      }
    }
  ]
}
```

**Object Ownership** Info

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

Object Ownership

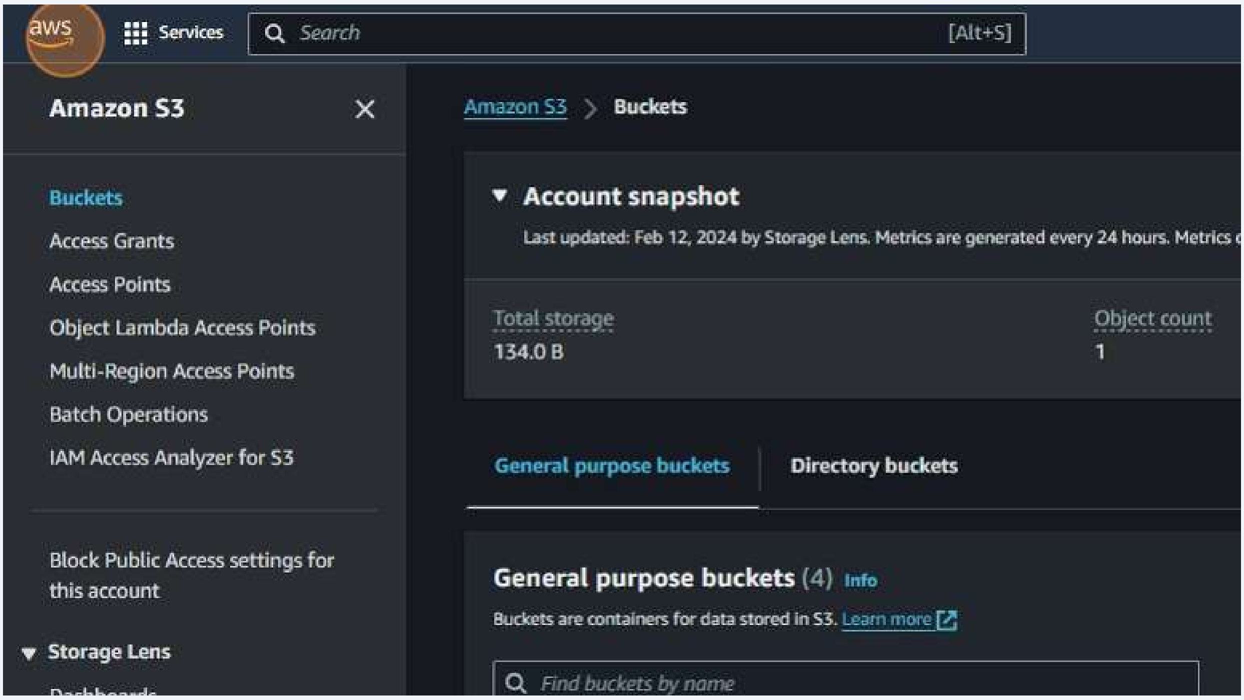
Bucket owner preferred

ACLs are enabled and can be used to grant access to this bucket and its objects. If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

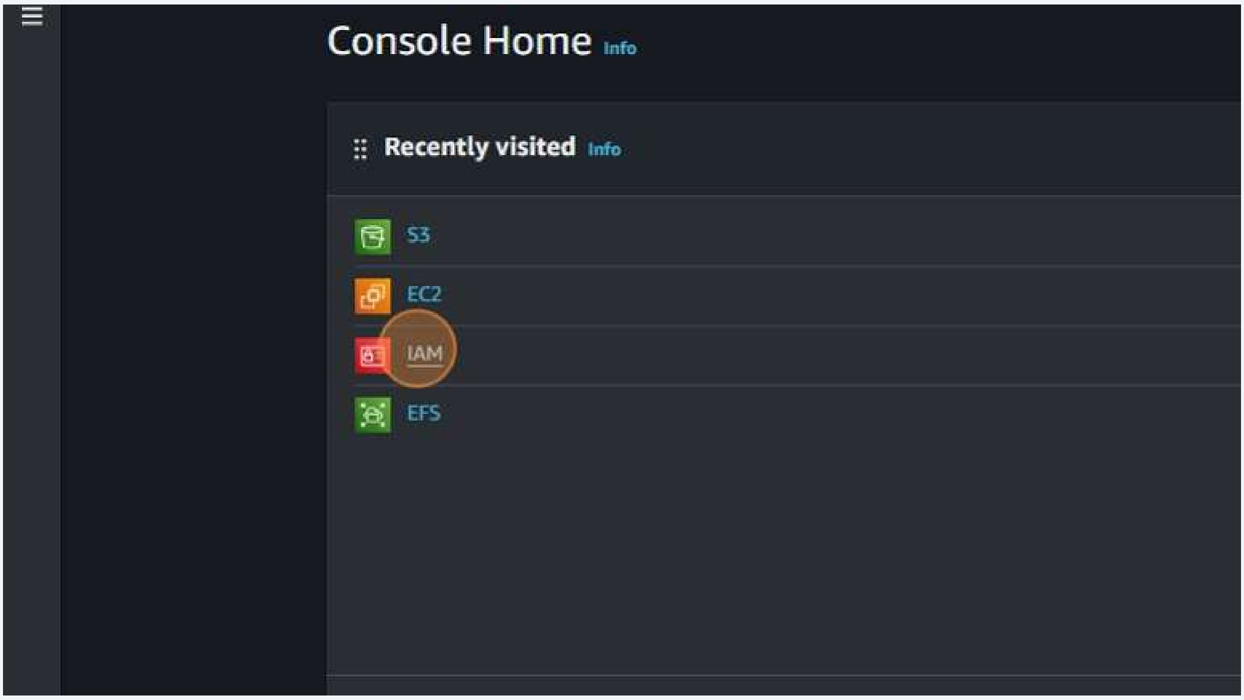
# IAM Users and Roles Lab

58 Navigate to [https://s3.console.aws.amazon.com/s3/buckets?region=us-east-1&bucketType=general&region=us-east-1](https://s3.console.aws.amazon.com/s3/buckets?region=us-east-1&bucketType=general&region=us-east-1)

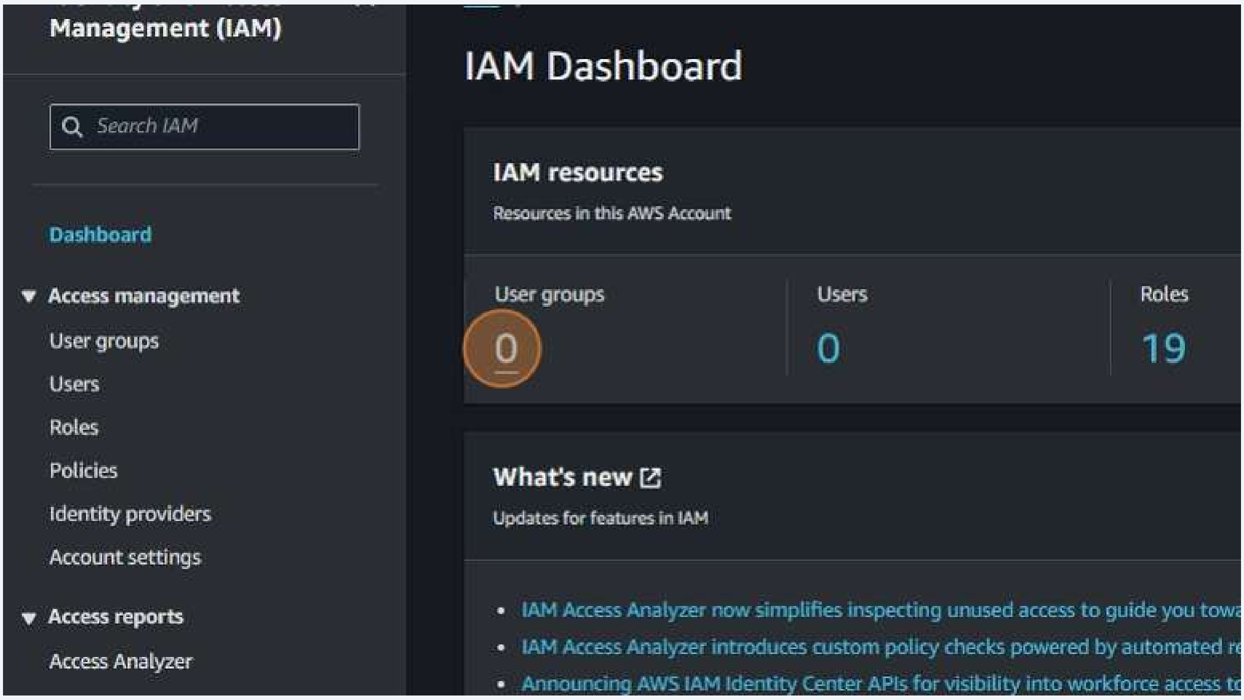
**59** Click this link.


aws
Services
Search
[Alt+S]
Amazon S3
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
Amazon S3 > Buckets
Account snapshot
Last updated: Feb 12, 2024 by Storage Lens. Metrics are generated every 24 hours. Metrics
Total storage
134.0 B
Object count
1
General purpose buckets
Directory buckets
General purpose buckets (4) Info
Buckets are containers for data stored in S3. Learn more
Find buckets by name

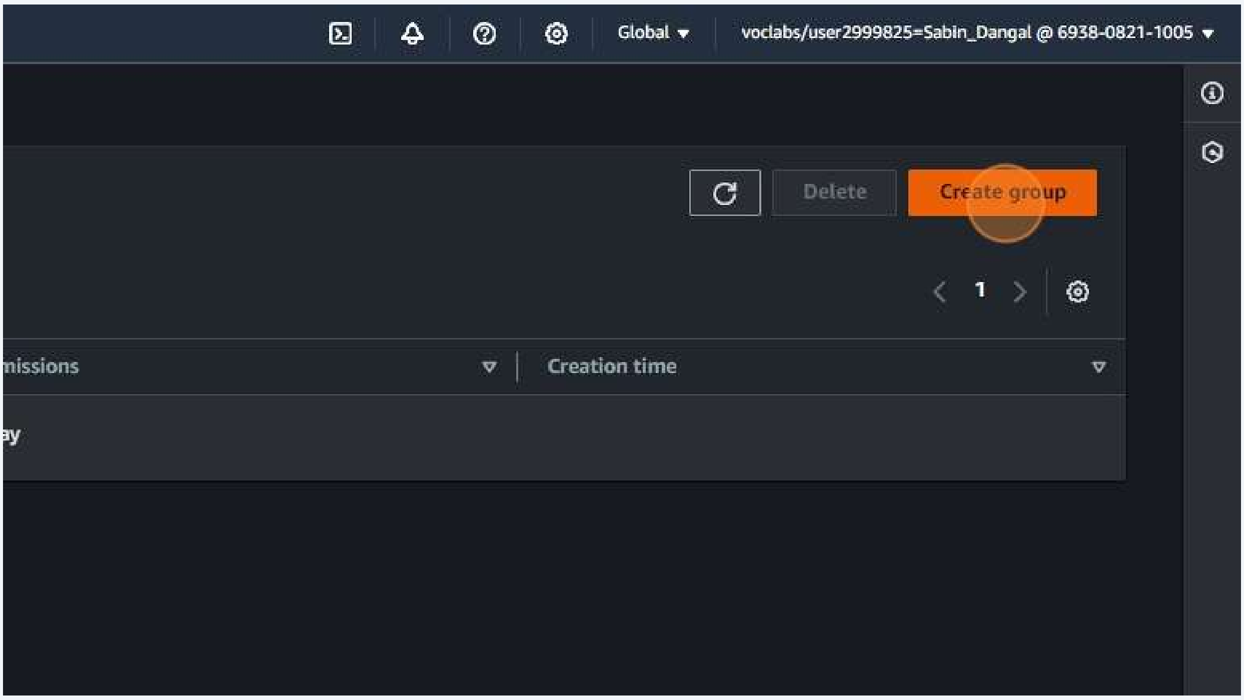
**60** Click "IAM"



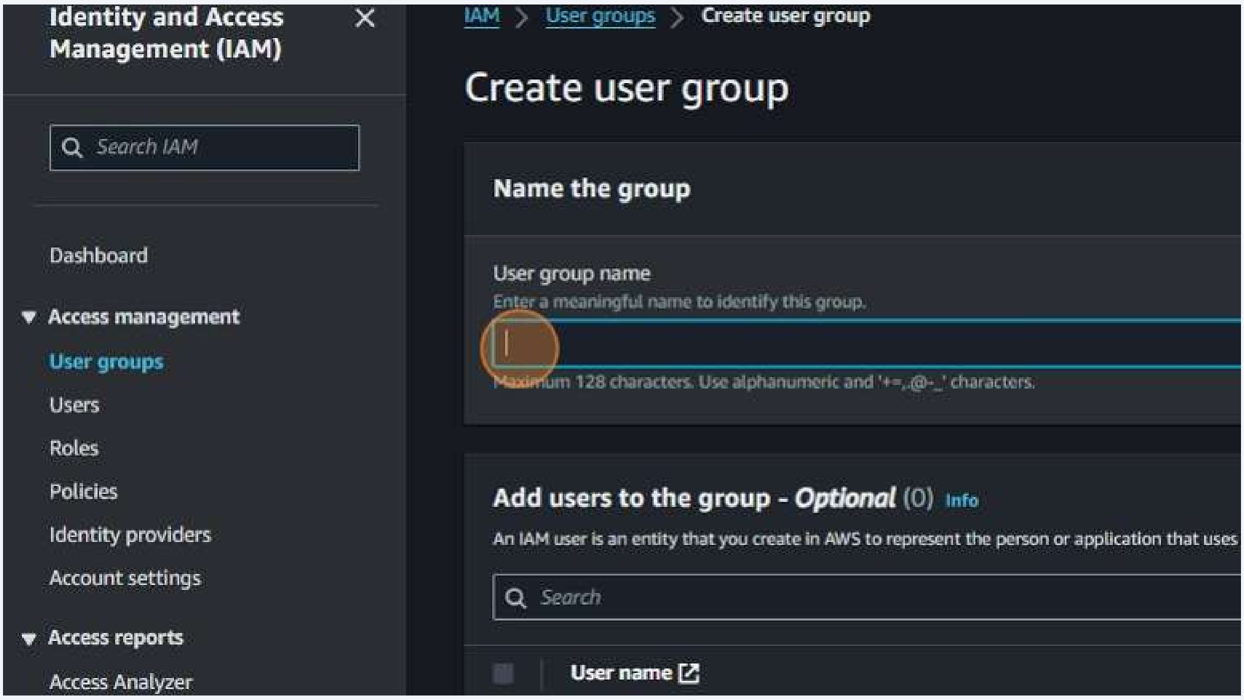
61 Click "0"


Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
IAM Dashboard
IAM resources
Resources in this AWS Account
User groups
0
Users
0
Roles
19
What's new
Updates for features in IAM
IAM Access Analyzer now simplifies inspecting unused access to guide you towa
IAM Access Analyzer introduces custom policy checks powered by automated re
Announcing AWS IAM Identity Center APIs for visibility into workforce access to

62 Click "Create group"



63 Click the "User group name" field.



Identity and Access Management (IAM)

IAM > User groups > Create user group

Create user group

Name the group

User group name

Enter a meaningful name to identify this group.

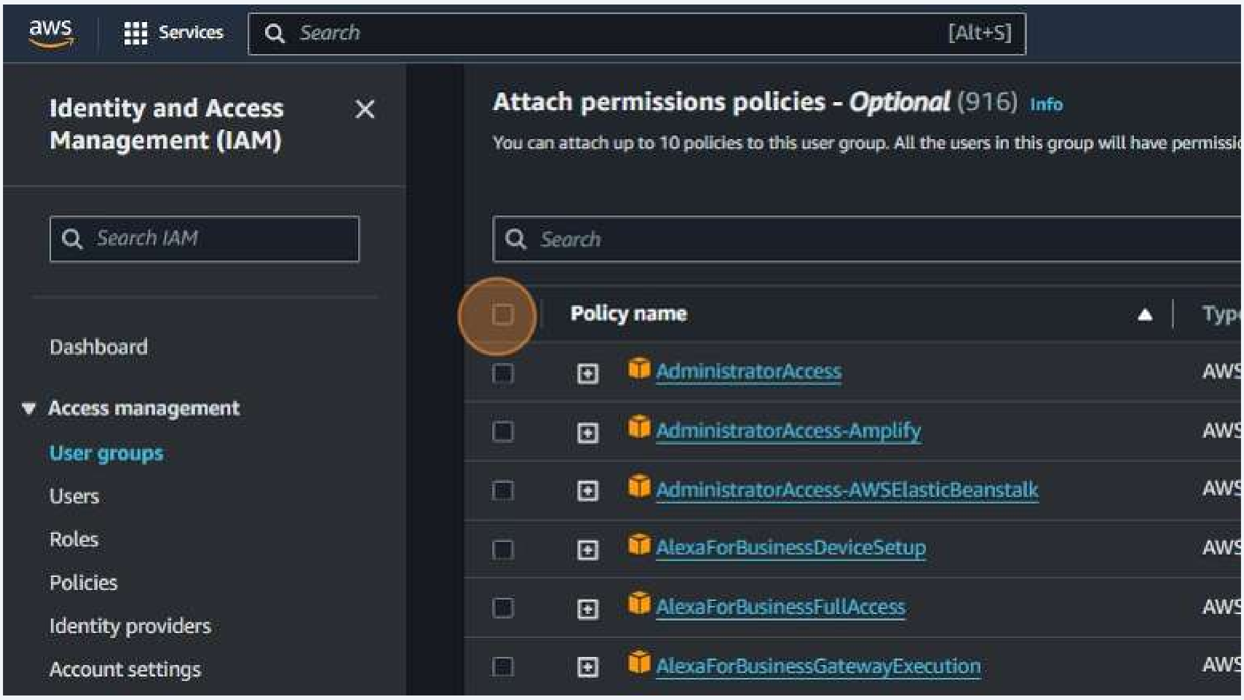
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Add users to the group - *Optional* (0) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses

64 Type "my-user-group"

65 Click this checkbox.



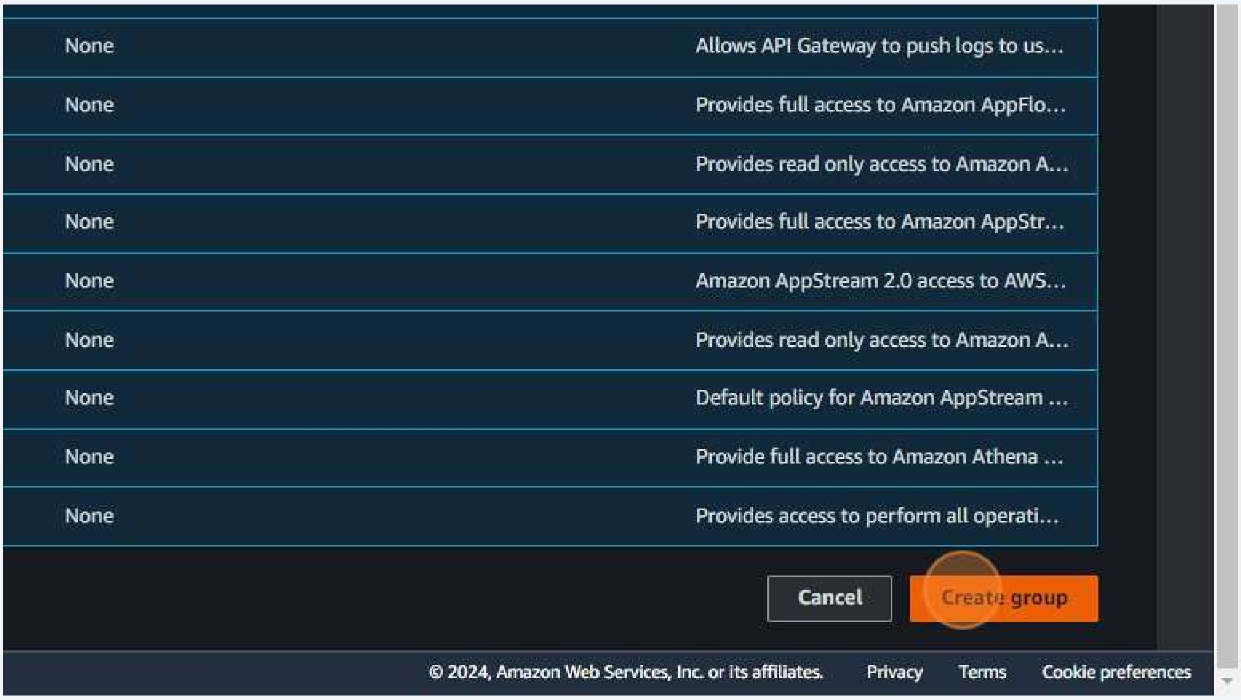
Identity and Access Management (IAM)

Attach permissions policies - *Optional* (916) Info

You can attach up to 10 policies to this user group. All the users in this group will have permissi

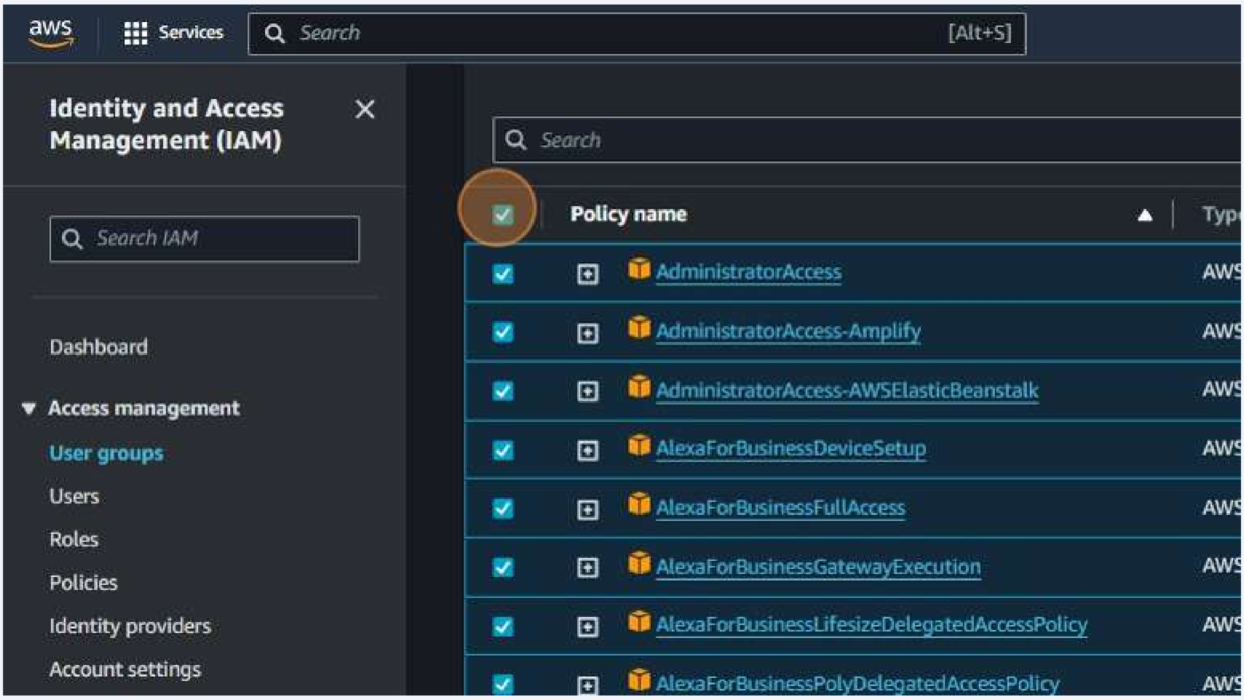
| □ | Policy name | Typ |
|---|---|---|
| □ | ⊞ AdministratorAccess | AWS |
| □ | ⊞ AdministratorAccess-Amplify | AWS |
| □ | ⊞ AdministratorAccess-AWSElasticBeanstalk | AWS |
| □ | ⊞ AlexaForBusinessDeviceSetup | AWS |
| □ | ⊞ AlexaForBusinessFullAccess | AWS |
| □ | ⊞ AlexaForBusinessGatewayExecution | AWS |

66 Click "Create group"

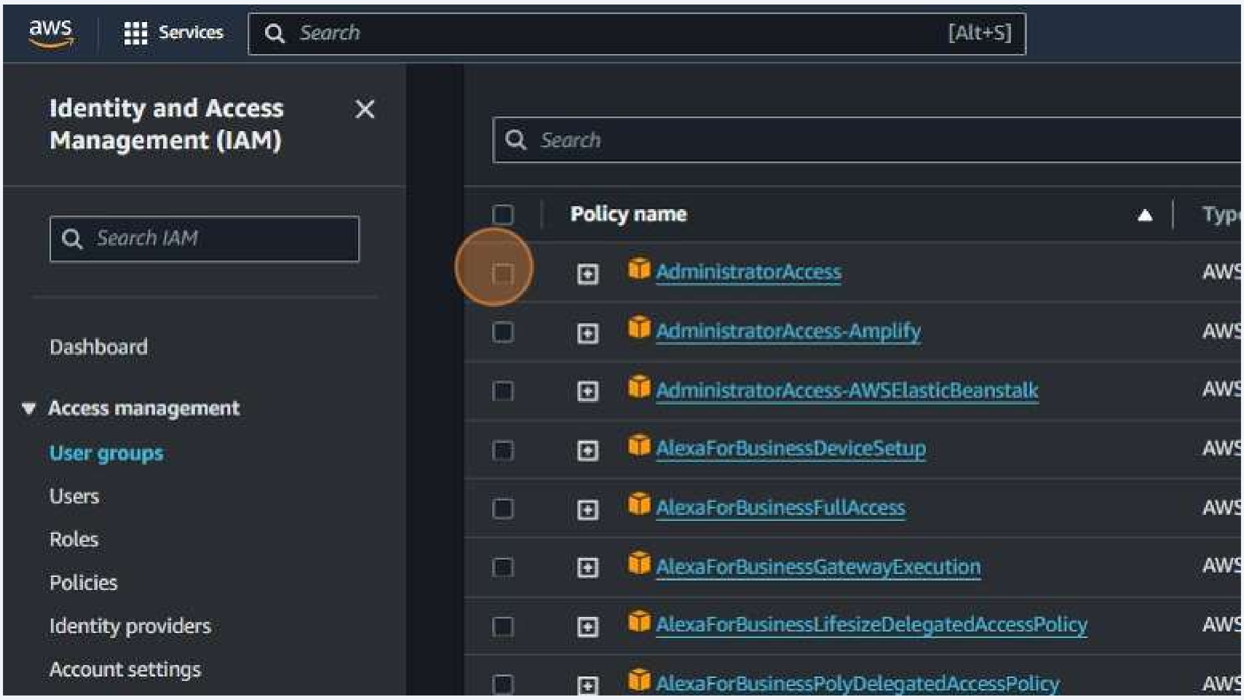


| | |
|---|---|
| None | Allows API Gateway to push logs to us... |
| None | Provides full access to Amazon AppFlo... |
| None | Provides read only access to Amazon A... |
| None | Provides full access to Amazon AppStr... |
| None | Amazon AppStream 2.0 access to AWS... |
| None | Provides read only access to Amazon A... |
| None | Default policy for Amazon AppStream ... |
| None | Provide full access to Amazon Athena ... |
| None | Provides access to perform all operati... |

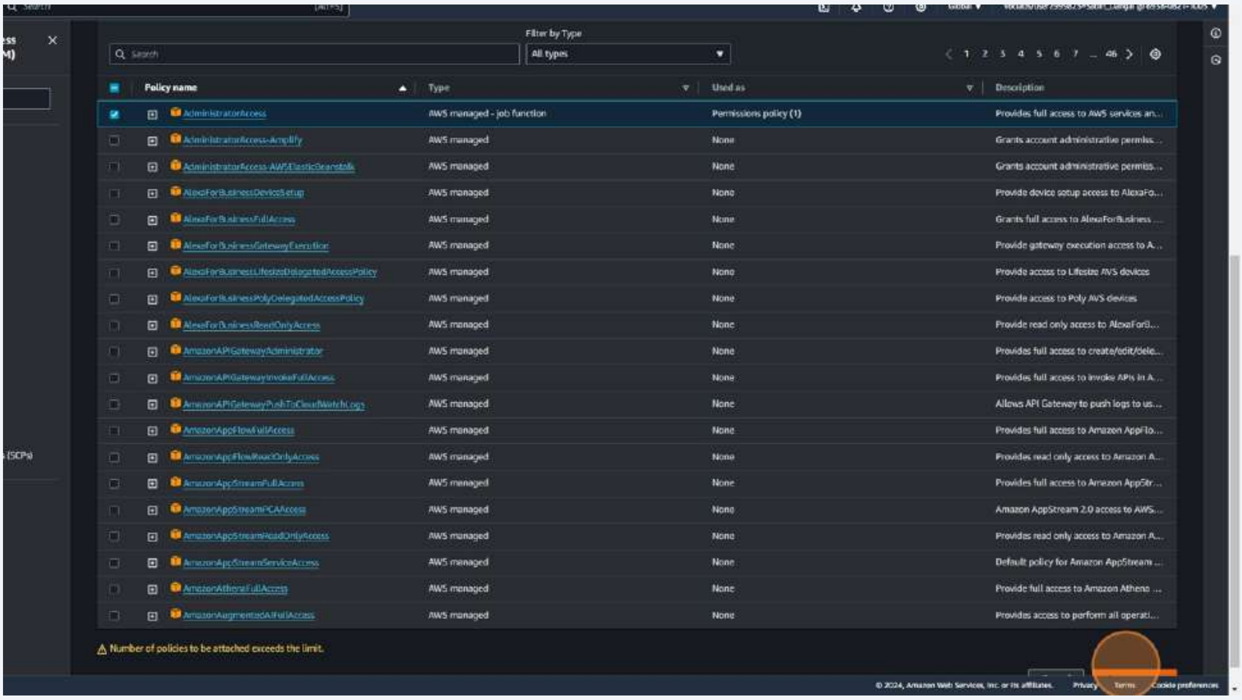
67 Click this checkbox.


aws
Services
Search
[Alt+S]
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Search
Policy name
Typ
AdministratorAccess
AdministratorAccess-Amplify
AdministratorAccess-AWSElasticBeanstalk
AlexaForBusinessDeviceSetup
AlexaForBusinessFullAccess
AlexaForBusinessGatewayExecution
AlexaForBusinessLifesizeDelegatedAccessPolicy
AlexaForBusinessPolyDelegatedAccessPolicy
AWS

68 Click this checkbox.


aws
Services
Search
[Alt+S]
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Search
Policy name
Typ
AdministratorAccess
AdministratorAccess-Amplify
AdministratorAccess-AWSElasticBeanstalk
AlexaForBusinessDeviceSetup
AlexaForBusinessFullAccess
AlexaForBusinessGatewayExecution
AlexaForBusinessLifesizeDelegatedAccessPolicy
AlexaForBusinessPolyDelegatedAccessPolicy
AWS

69 Click "Create group"



Filter by Type: All types

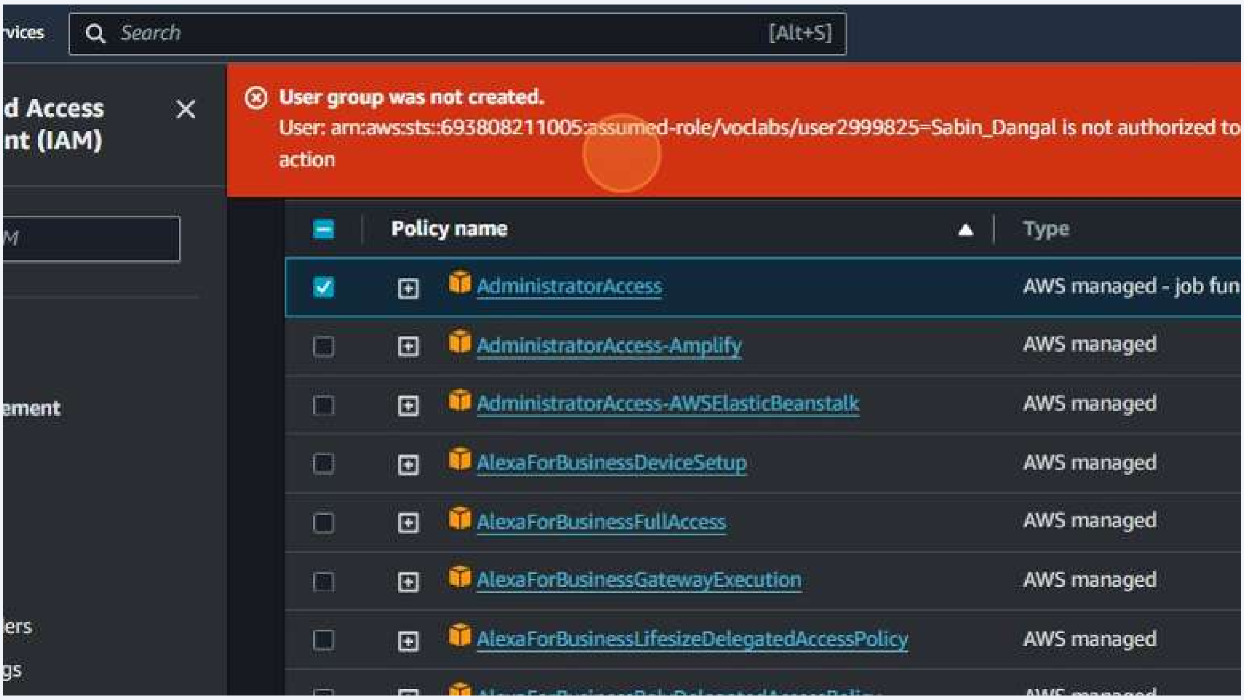
‹ 1 2 3 4 5 6 7 … 46 ›

| | | Policy name | Type | Used as | Description |
|---|---|---|---|---|---|
| ☑ | ⊞ | AdministratorAccess | AWS managed - job function | Permissions policy (1) | Provides full access to AWS services an... |
| □ | ⊞ | AdministratorAccess-Amplify | AWS managed | None | Grants account administrative permiss... |
| □ | ⊞ | AdministratorAccess-AWSElasticBeanstalk | AWS managed | None | Grants account administrative permiss... |
| □ | ⊞ | AlexaForBusinessDeviceSetup | AWS managed | None | Provide device setup access to AlexaFo... |
| □ | ⊞ | AlexaForBusinessFullAccess | AWS managed | None | Grants full access to AlexaForBusiness ... |
| □ | ⊞ | AlexaForBusinessGatewayExecution | AWS managed | None | Provide gateway execution access to A... |
| □ | ⊞ | AlexaForBusinessLifesizeDelegatedAccessPolicy | AWS managed | None | Provide access to Lifesize AVS devices |
| □ | ⊞ | AlexaForBusinessPolyDelegatedAccessPolicy | AWS managed | None | Provide access to Poly AVS devices |
| □ | ⊞ | AlexaForBusinessReadOnlyAccess | AWS managed | None | Provide read only access to AlexaForB... |
| □ | ⊞ | AmazonAPIGatewayAdministrator | AWS managed | None | Provides full access to create/edit/dele... |
| □ | ⊞ | AmazonAPIGatewayInvokeFullAccess | AWS managed | None | Provides full access to invoke APIs in A... |
| □ | ⊞ | AmazonAPIGatewayPushToCloudWatchLogs | AWS managed | None | Allows API Gateway to push logs to us... |
| □ | ⊞ | AmazonAppFlowFullAccess | AWS managed | None | Provides full access to Amazon AppFlo... |
| □ | ⊞ | AmazonAppFlowReadOnlyAccess | AWS managed | None | Provides read only access to Amazon A... |
| □ | ⊞ | AmazonAppStreamFullAccess | AWS managed | None | Provides full access to Amazon AppStr... |
| □ | ⊞ | AmazonAppStreamPCAAccess | AWS managed | None | Amazon AppStream 2.0 access to AWS... |
| □ | ⊞ | AmazonAppStreamReadOnlyAccess | AWS managed | None | Provides read only access to Amazon A... |
| □ | ⊞ | AmazonAppStreamServiceAccess | AWS managed | None | Default policy for Amazon AppStream ... |
| □ | ⊞ | AmazonAthenaFullAccess | AWS managed | None | Provide full access to Amazon Athena ... |
| □ | ⊞ | AmazonAugmentedAIFullAccess | AWS managed | None | Provides access to perform all operati... |

⚠ Number of policies to be attached exceeds the limit.

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

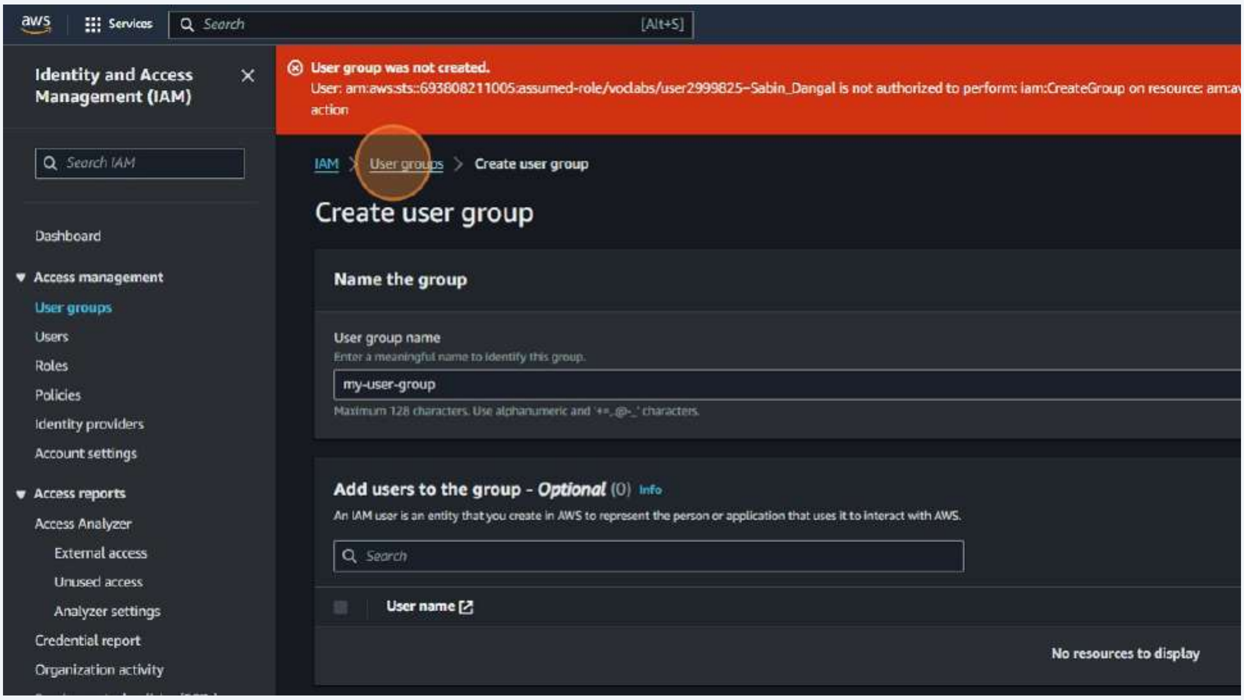
70 Click "User: arn:aws:sts::693808211005:assumed-role/voclabs/user2999825=Sabin_Dangal is not authorized to perform: iam:CreateGroup on resource: arn:aws..."



User group was not created.
User: arn:aws:sts::693808211005:assumed-role/voclabs/user2999825=Sabin_Dangal is not authorized to
action

| | | Policy name | Type |
|---|---|---|---|
| ☑ | ⊞ | AdministratorAccess | AWS managed - job fun |
| □ | ⊞ | AdministratorAccess-Amplify | AWS managed |
| □ | ⊞ | AdministratorAccess-AWSElasticBeanstalk | AWS managed |
| □ | ⊞ | AlexaForBusinessDeviceSetup | AWS managed |
| □ | ⊞ | AlexaForBusinessFullAccess | AWS managed |
| □ | ⊞ | AlexaForBusinessGatewayExecution | AWS managed |
| □ | ⊞ | AlexaForBusinessLifesizeDelegatedAccessPolicy | AWS managed |

71 Click "User groups"



**User group was not created.**
User: arn:aws:sts::693808211005:assumed-role/voclabs/user2999825–Sabin_Dangal is not authorized to perform: iam:CreateGroup on resource: arn:av
action

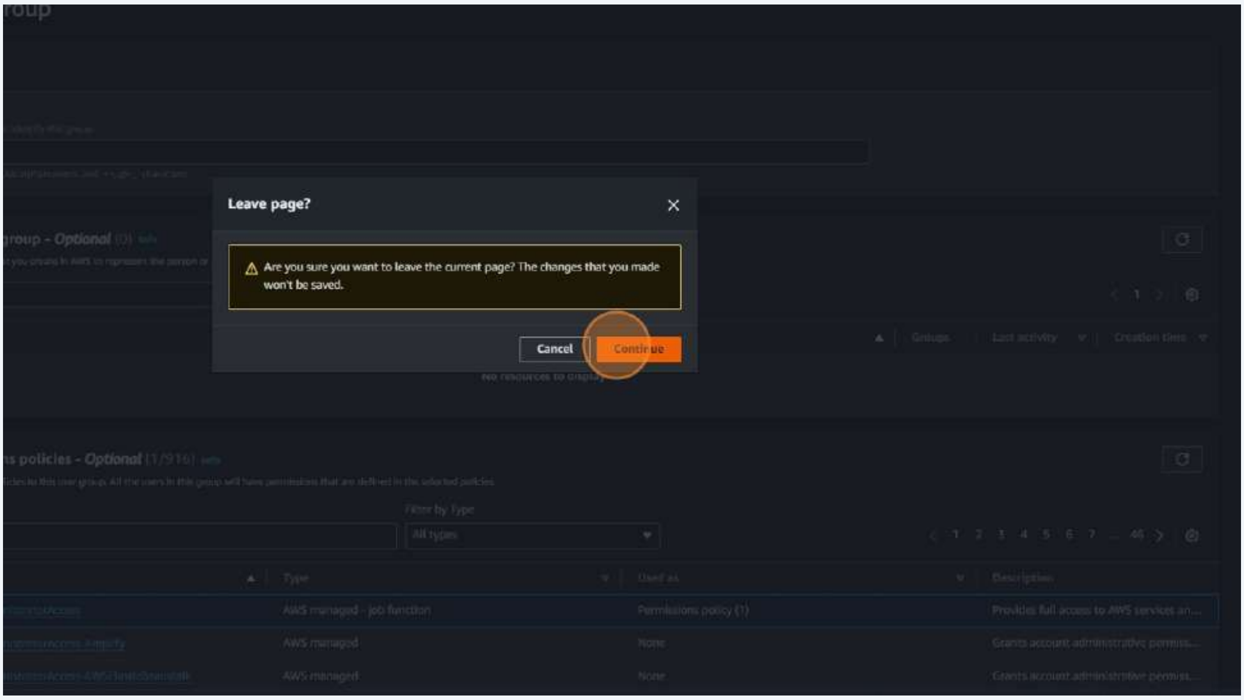
Create user group

Name the group

User group name
Enter a meaningful name to identify this group.
my-user-group
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

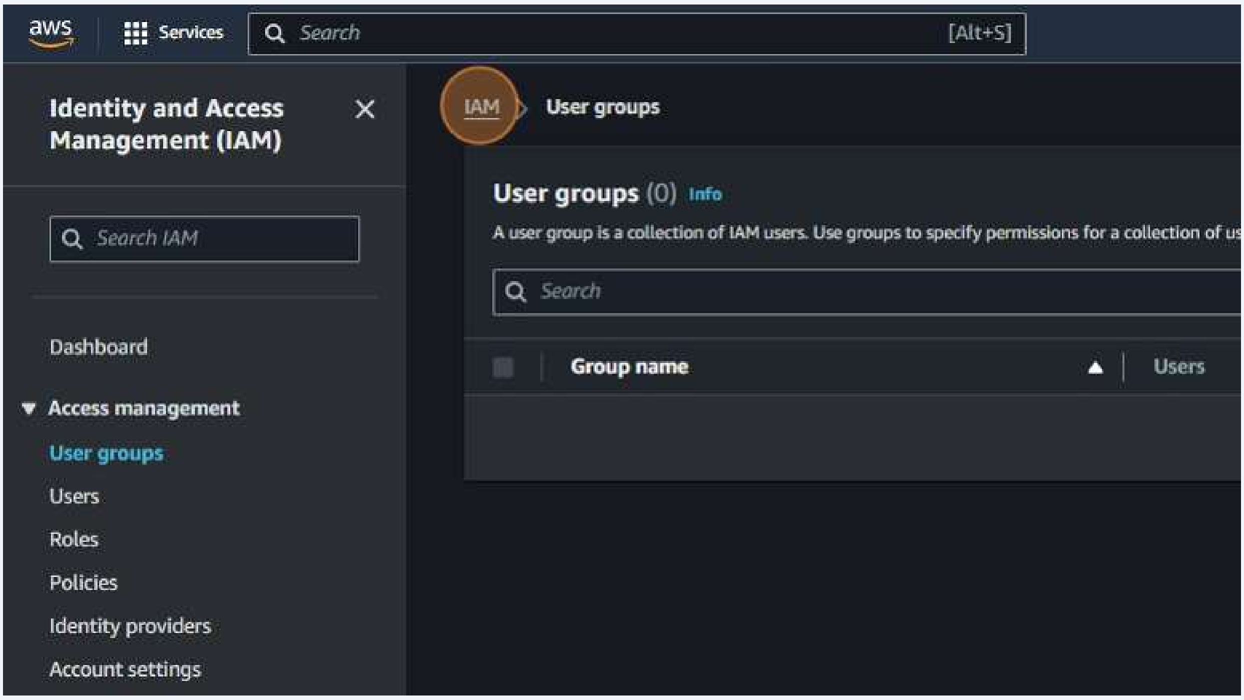
Add users to the group - *Optional* (0) Info
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

72 Click "Continue"



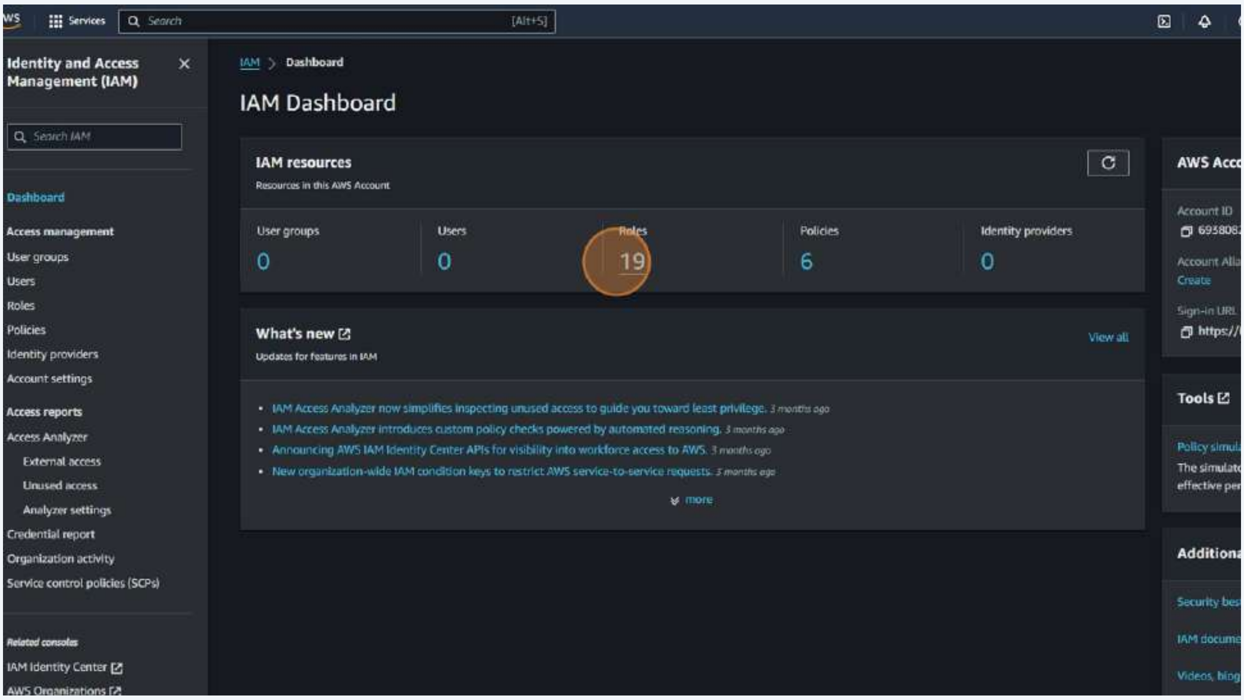
Are you sure you want to leave the current page? The changes that you made won't be saved.

**73** Click "IAM"



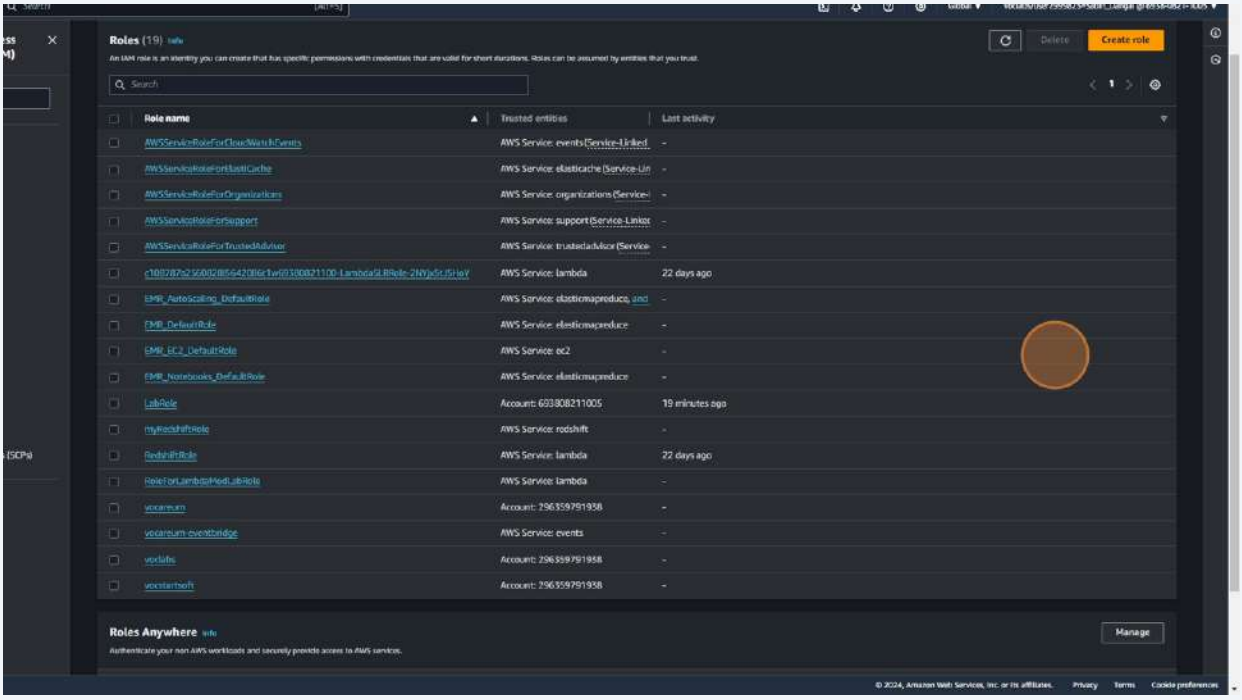
A user group is a collection of IAM users. Use groups to specify permissions for a collection of us

**74** Click on the roles



- IAM Access Analyzer now simplifies inspecting unused access to guide you toward least privilege. 3 months ago
- IAM Access Analyzer introduces custom policy checks powered by automated reasoning. 3 months ago
- Announcing AWS IAM Identity Center APIs for visibility into workforce access to AWS. 3 months ago
- New organization-wide IAM condition keys to restrict AWS service-to-service requests. 3 months ago

## 75 Roles List



**Roles** (19) Info

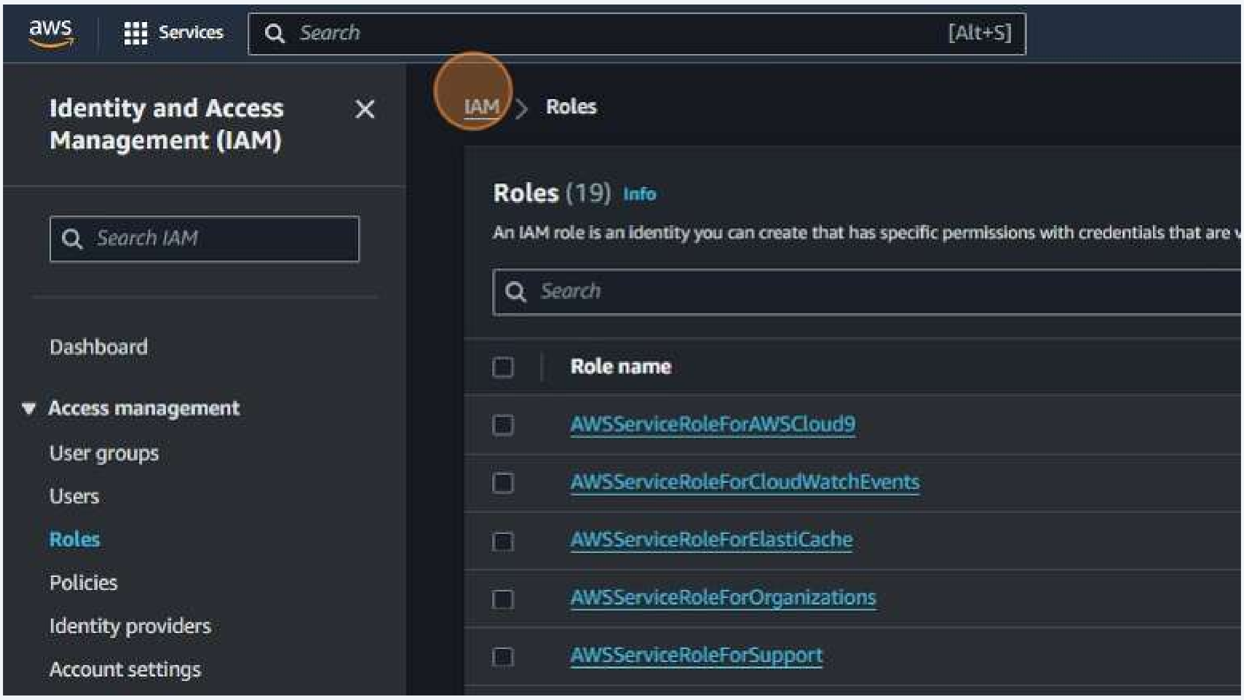
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

| Role name | Trusted entities | Last activity |
|---|---|---|
| AWSServiceRoleForCloudWatchEvents | AWS Service: events (Service-Linked | - |
| AWSServiceRoleForElastiCache | AWS Service: elasticache (Service-Lin | - |
| AWSServiceRoleForOrganizations | AWS Service: organizations (Service-l | - |
| AWSServiceRoleForSupport | AWS Service: support (Service-Linke | - |
| AWSServiceRoleForTrustedAdvisor | AWS Service: trustedadvisor (Service- | - |
| c108787a25600285642086r1w69380821100-LambdaSLRRole-2NYjxSLJ5HeY | AWS Service: lambda | 22 days ago |
| EMR_AutoScaling_DefaultRole | AWS Service: elasticmapreduce, and | - |
| EMR_DefaultRole | AWS Service: elasticmapreduce | - |
| EMR_EC2_DefaultRole | AWS Service: ec2 | - |
| EMR_Notebooks_DefaultRole | AWS Service: elasticmapreduce | - |
| LabRole | Account: 693808211005 | 19 minutes ago |
| myRedshiftRole | AWS Service: redshift | - |
| RedshiftRole | AWS Service: lambda | 22 days ago |
| RoleForLambdaModLabRole | AWS Service: lambda | - |
| vocareum | Account: 296359791938 | - |
| vocareum-eventbridge | AWS Service: events | - |
| voclabs | Account: 296359791938 | - |
| vocstartsoft | Account: 296359791938 | - |

**Roles Anywhere** Info

Authenticate your non AWS workloads and securely provide access to AWS services.

## 76 Click "IAM"

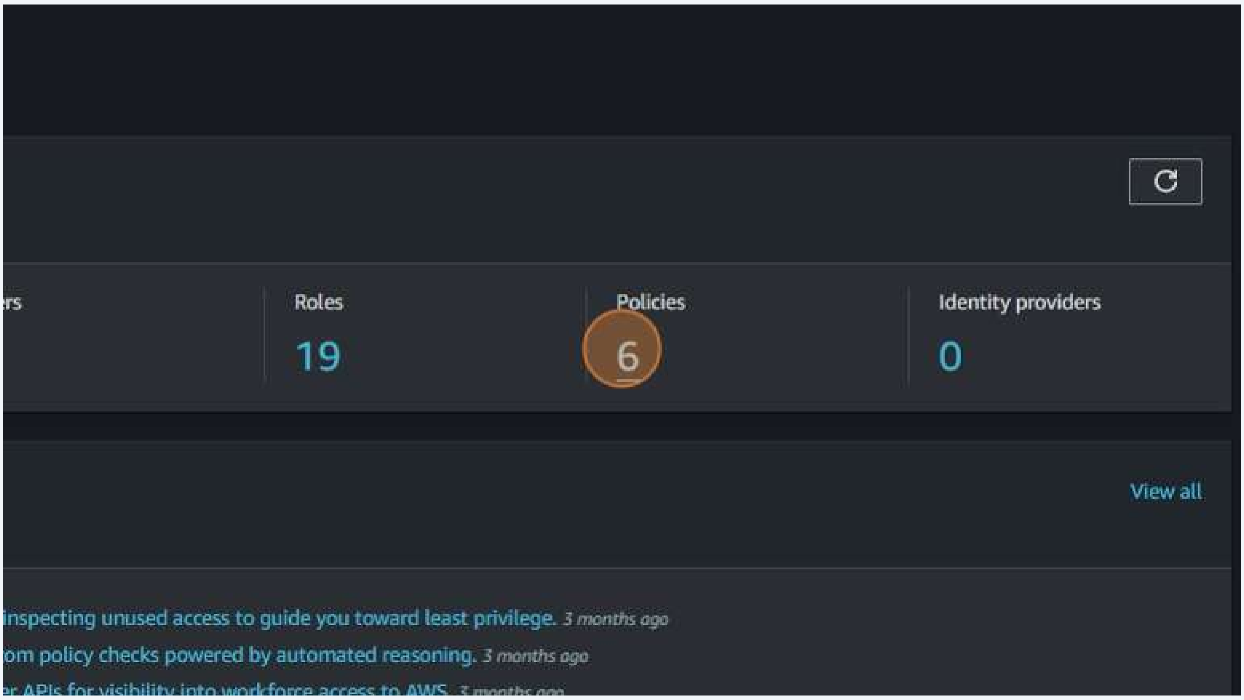


**Roles** (19) Info

An IAM role is an identity you can create that has specific permissions with credentials that are v

| Role name |
|---|
| AWSServiceRoleForAWSCloud9 |
| AWSServiceRoleForCloudWatchEvents |
| AWSServiceRoleForElastiCache |
| AWSServiceRoleForOrganizations |
| AWSServiceRoleForSupport |

77 Click on policies



rs
Roles
19
Policies
6
Identity providers
0
View all
inspecting unused access to guide you toward least privilege. 3 months ago
om policy checks powered by automated reasoning. 3 months ago
r APIs for visibility into workforce access to AWS. 3 months ago

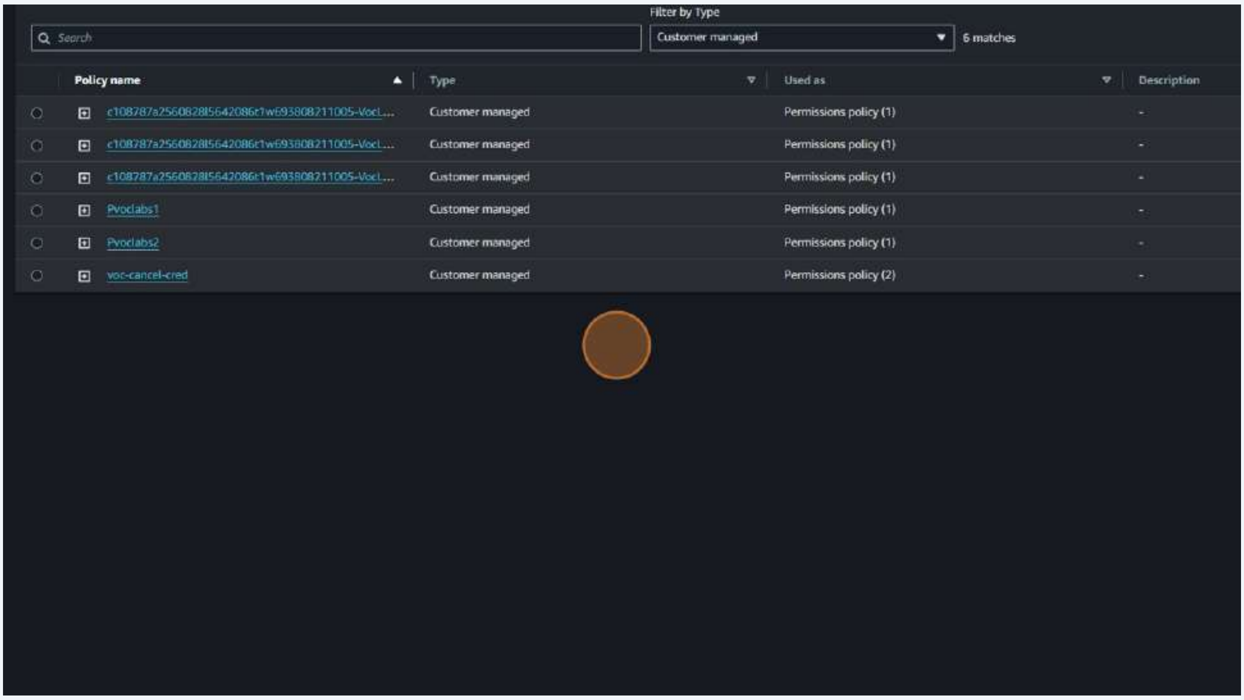
78

Click "IAM
Policies
Policies (1179)

Info
Actions
Delete
Create policy

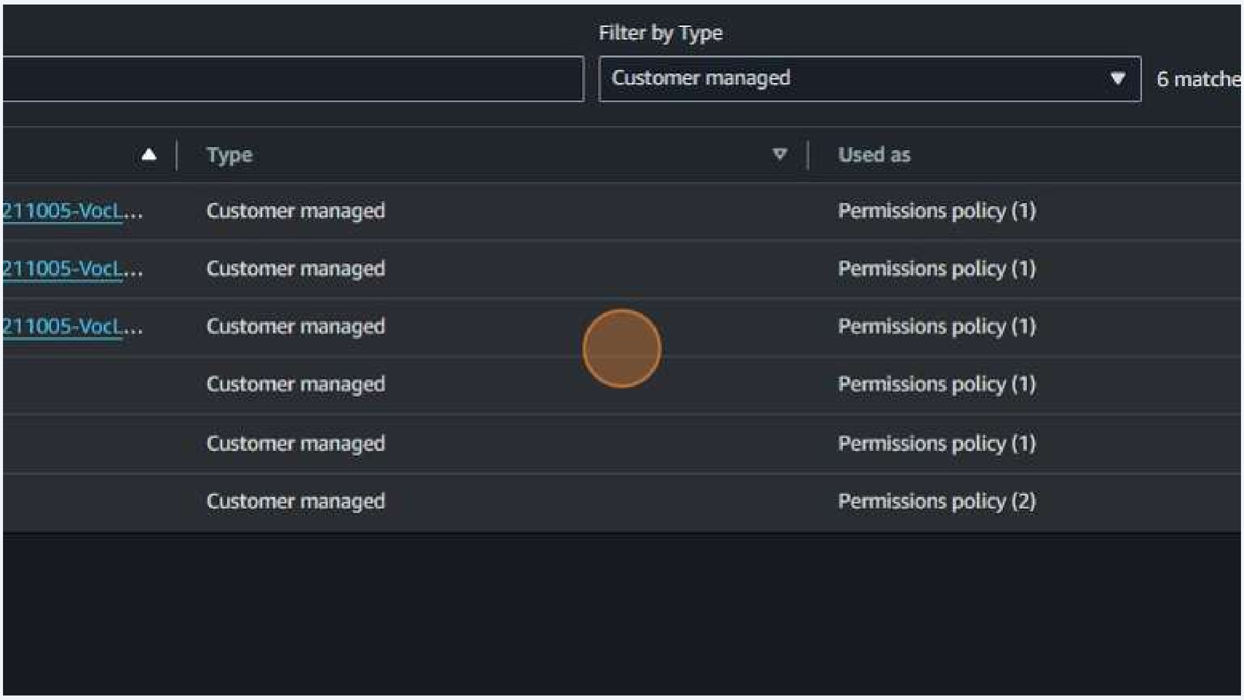
A policy is an object in AWS that defines permissions.

Filter by Type
Custome..."



|  |  | Policy name | Type | Used as | Description |
|---|---|---|---|---|---|
| ○ | ⊞ | c108787a2560828l5642086t1w693808211005-VocL... | Customer managed | Permissions policy (1) | - |
| ○ | ⊞ | c108787a2560828l5642086t1w693808211005-VocL... | Customer managed | Permissions policy (1) | - |
| ○ | ⊞ | c108787a2560828l5642086t1w693808211005-VocL... | Customer managed | Permissions policy (1) | - |
| ○ | ⊞ | Pvoclabs1 | Customer managed | Permissions policy (1) | - |
| ○ | ⊞ | Pvoclabs2 | Customer managed | Permissions policy (1) | - |
| ○ | ⊞ | voc-cancel-cred | Customer managed | Permissions policy (2) | - |

79 Click "Customer managed"

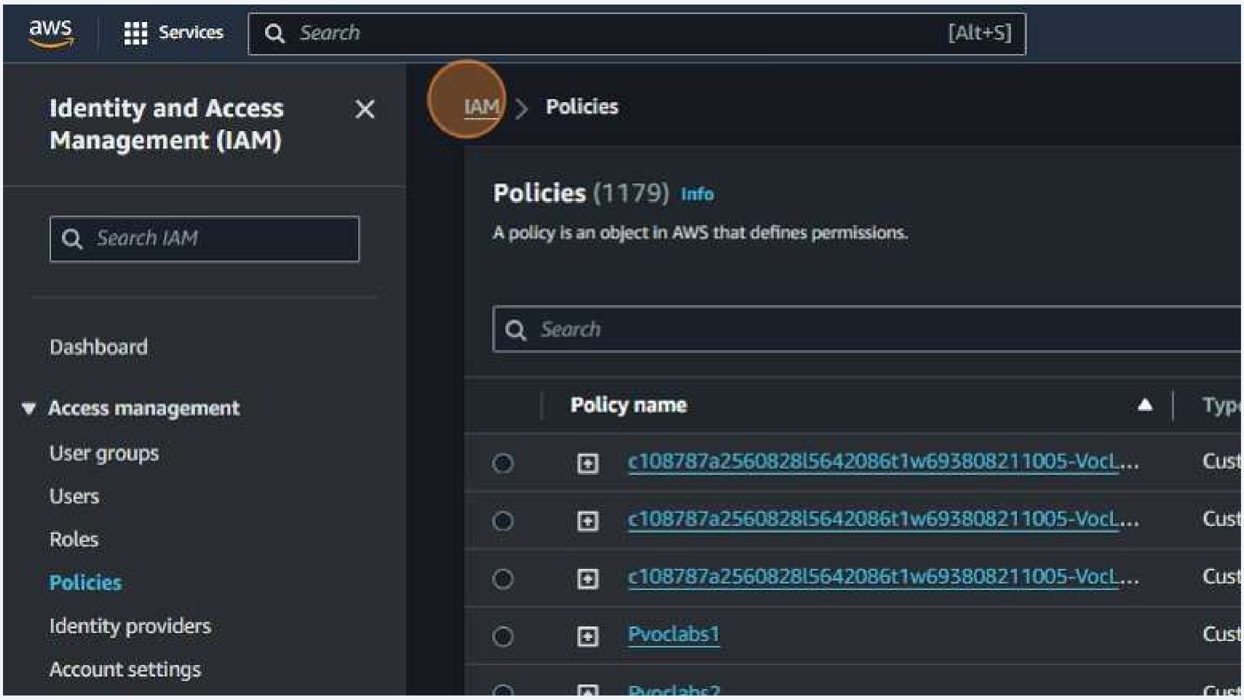


Filter by Type

Customer managed ▼ 6 matche

| ▲ | Type | Used as |
|---|---|---|
| 211005-VocL… | Customer managed | Permissions policy (1) |
| 211005-VocL… | Customer managed | Permissions policy (1) |
| 211005-VocL… | Customer managed | Permissions policy (1) |
| | Customer managed | Permissions policy (1) |
| | Customer managed | Permissions policy (1) |
| | Customer managed | Permissions policy (2) |

80 Click "IAM"



Policies (1179) Info

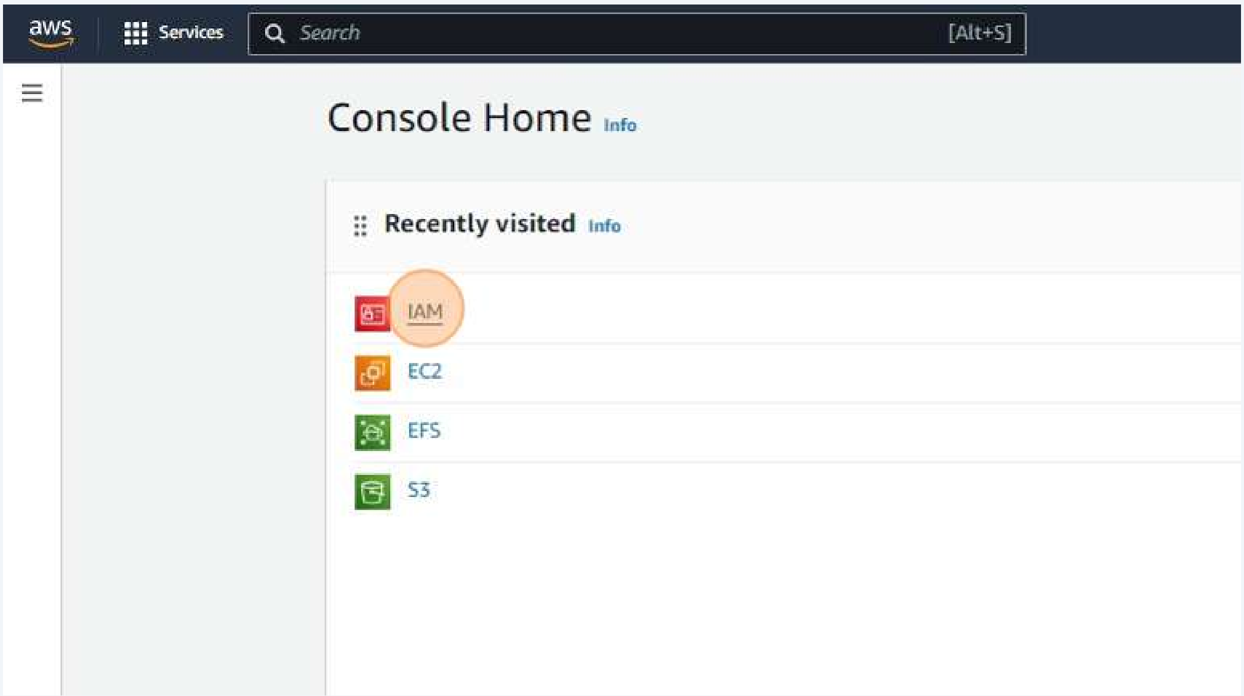
A policy is an object in AWS that defines permissions.

Search

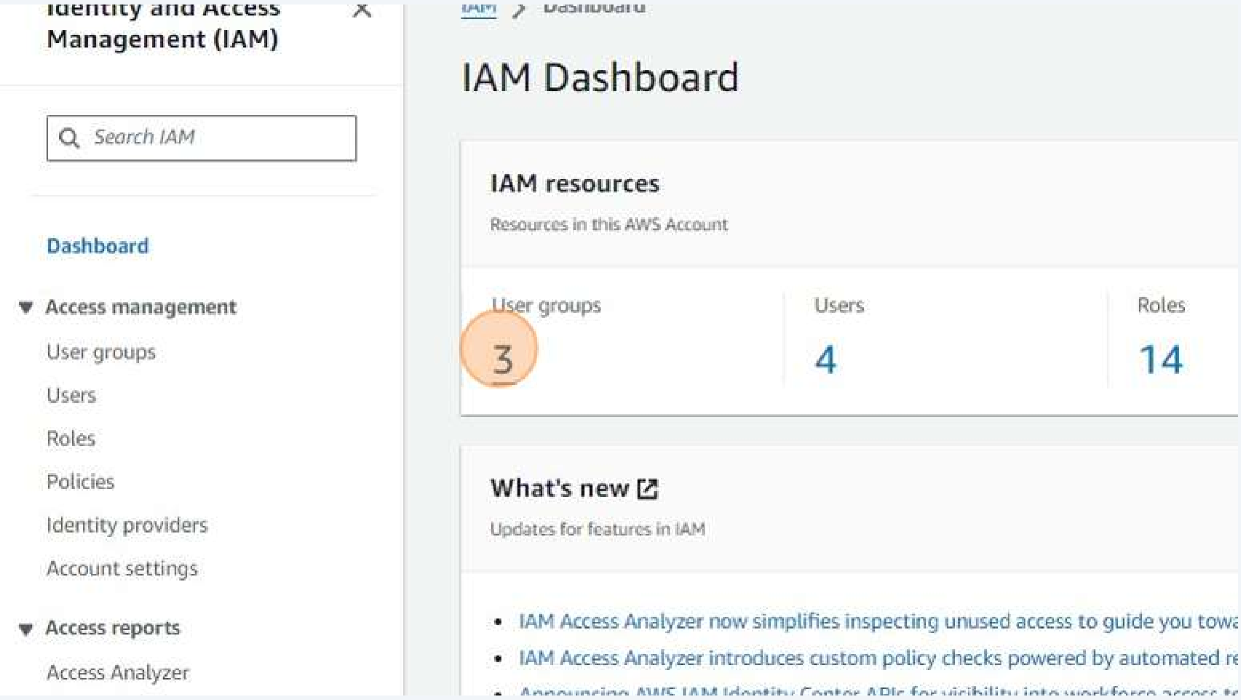
| | | Policy name ▲ | Typ |
|---|---|---|---|
| ○ | ⊞ | c108787a2560828l5642086t1w693808211005-VocL… | Cust |
| ○ | ⊞ | c108787a2560828l5642086t1w693808211005-VocL… | Cust |
| ○ | ⊞ | c108787a2560828l5642086t1w693808211005-VocL… | Cust |
| ○ | ⊞ | Pvoclabs1 | Cust |
| ○ | ⊞ | Pvoclabs2 | Cust |

81 Navigate to [https://us-east-1.console.aws.amazon.com/console/home?region=us-east-1#](https://us-east-1.console.aws.amazon.com/console/home?region=us-east-1#)

82 Click "IAM"



83 Click "3"



Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access Analyzer

IAM > Dashboard

IAM Dashboard

IAM resources

Resources in this AWS Account

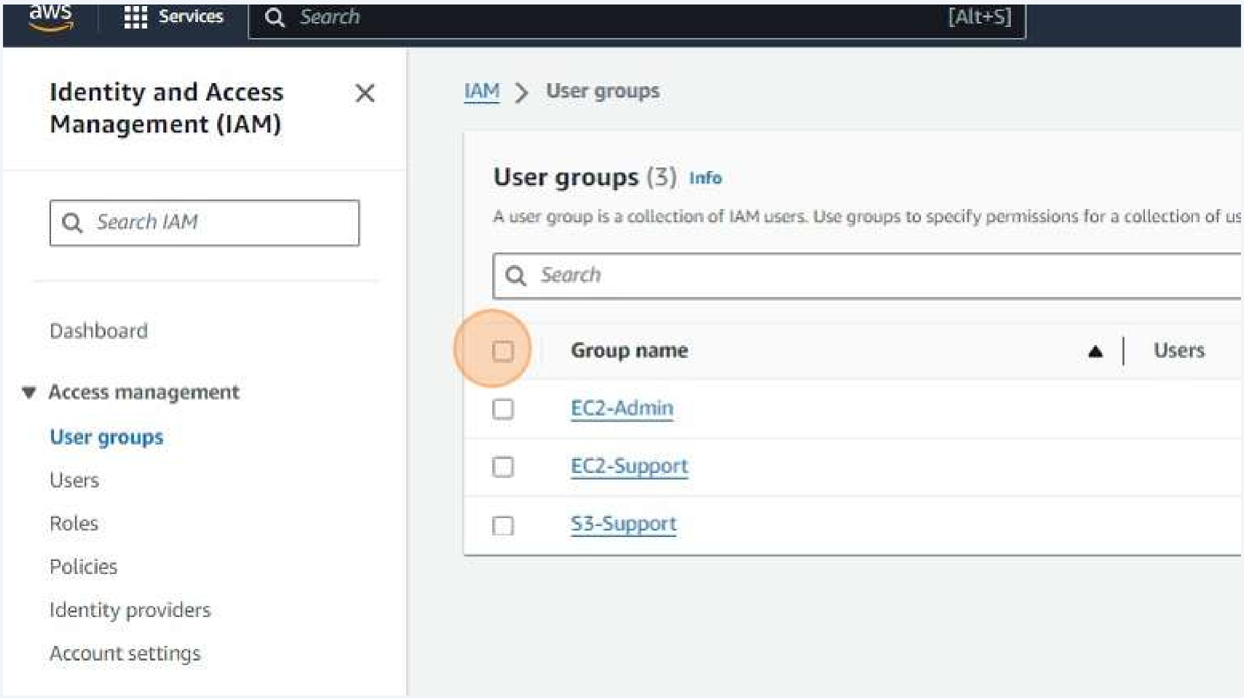
| User groups | Users | Roles |
|---|---|---|
| 3 | 4 | 14 |

What's new

Updates for features in IAM

- IAM Access Analyzer now simplifies inspecting unused access to guide you towa
- IAM Access Analyzer introduces custom policy checks powered by automated re
- Announcing AWS IAM Identity Center APIs for visibility into workforce access to

84 Click this checkbox.



Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

IAM > User groups

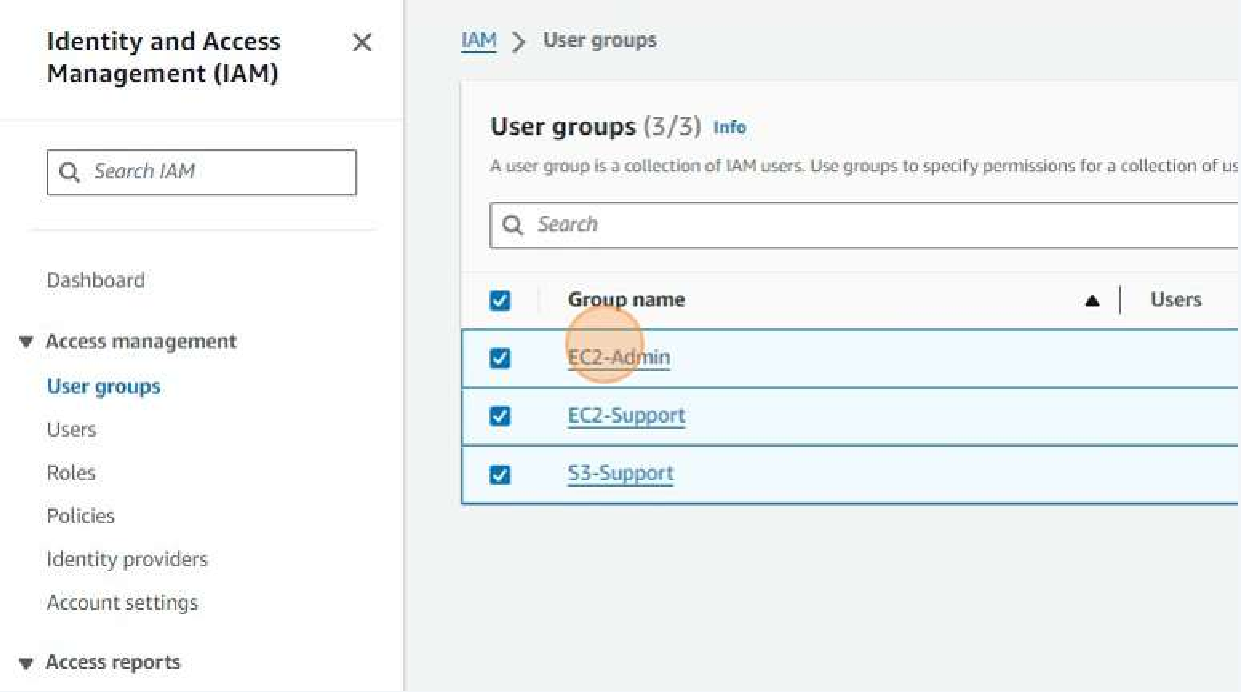
User groups (3) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of us

Search

| □ | Group name ▲ | Users |
|---|---|---|
| □ | EC2-Admin | |
| □ | EC2-Support | |
| □ | S3-Support | |

85 Click "EC2-Admin"



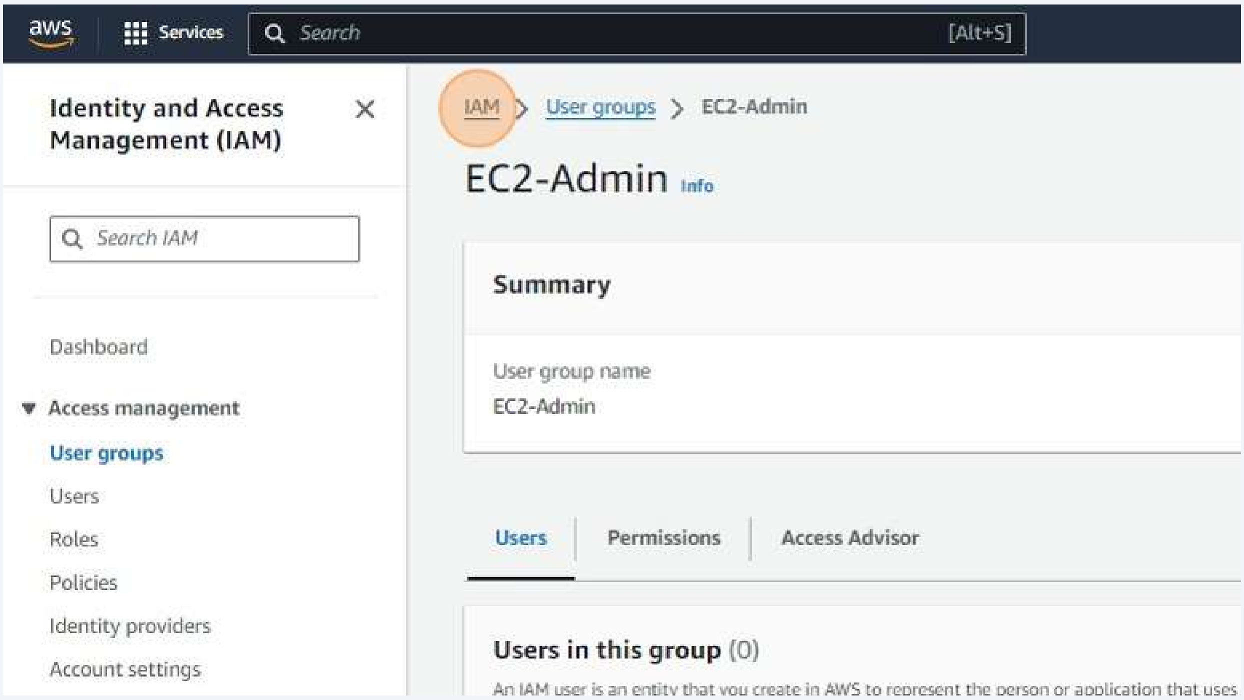
IAM > User groups

User groups (3/3) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of us

| ☑ | Group name | Users |
|---|---|---|
| ☑ | EC2-Admin | |
| ☑ | EC2-Support | |
| ☑ | S3-Support | |

86 Click "IAM"



IAM > User groups > EC2-Admin

EC2-Admin Info

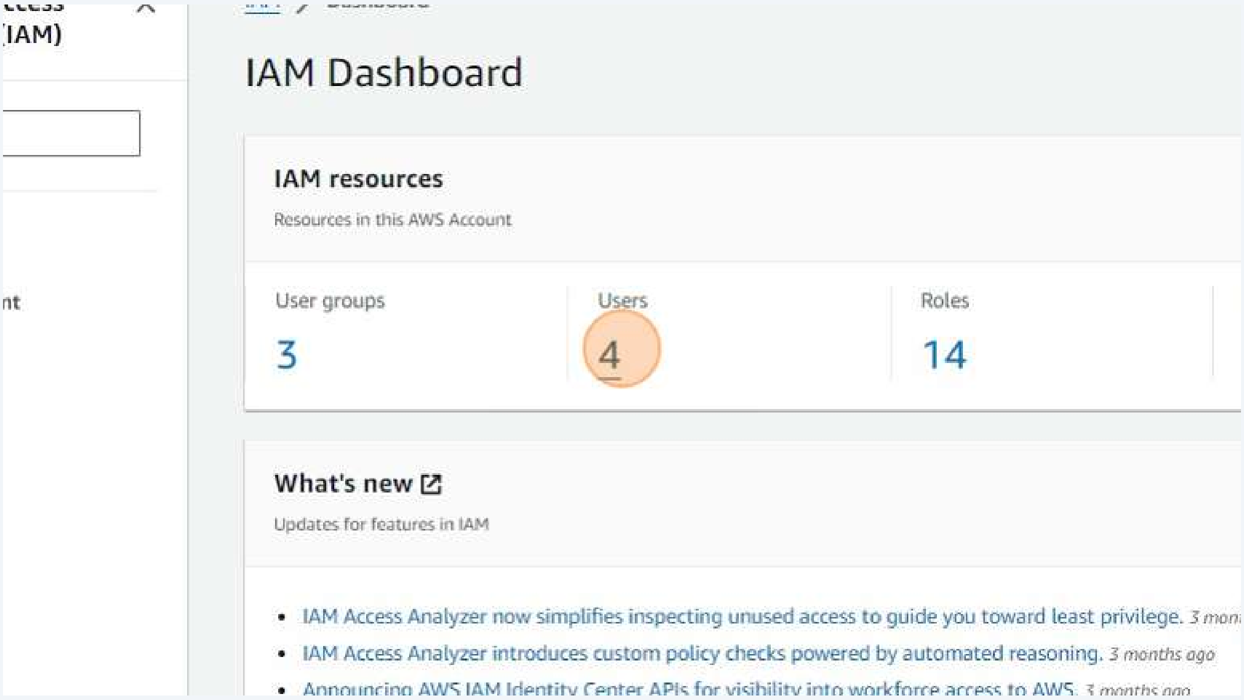
Summary

User group name
EC2-Admin

Users in this group (0)

An IAM user is an entity that you create in AWS to represent the person or application that uses

87 Click "4"



IAM Dashboard

IAM resources

Resources in this AWS Account

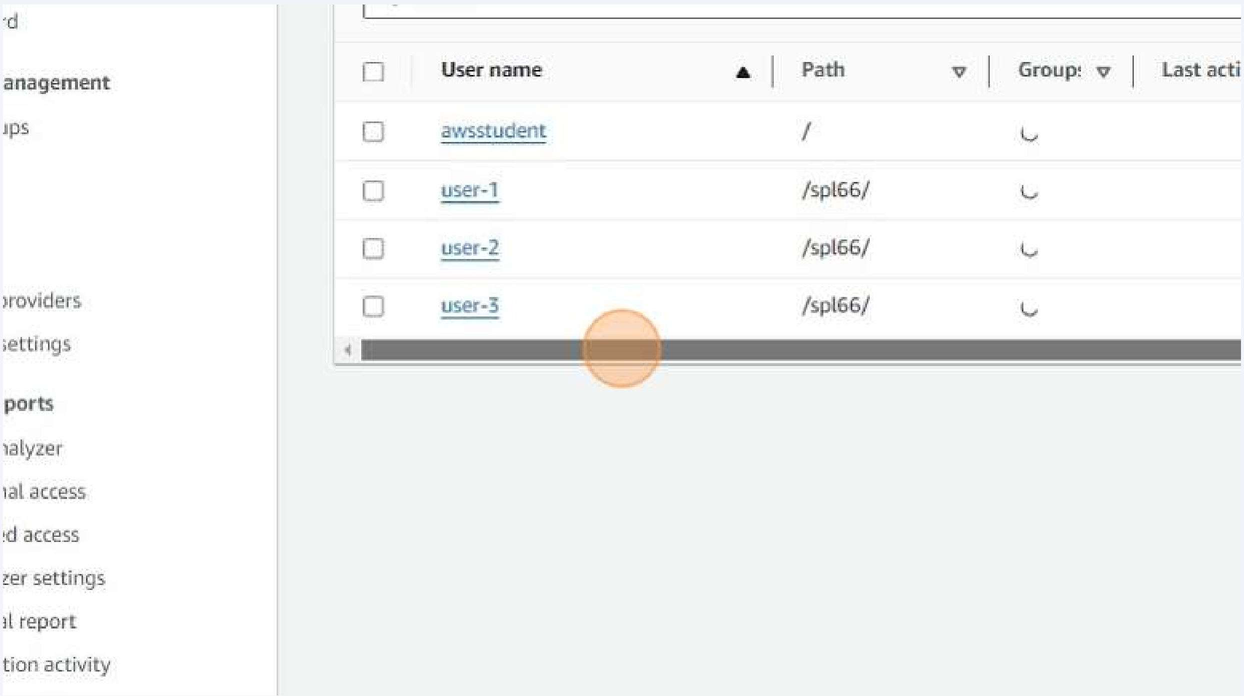
| User groups | Users | Roles |
|---|---|---|
| 3 | 4 | 14 |

What's new

Updates for features in IAM

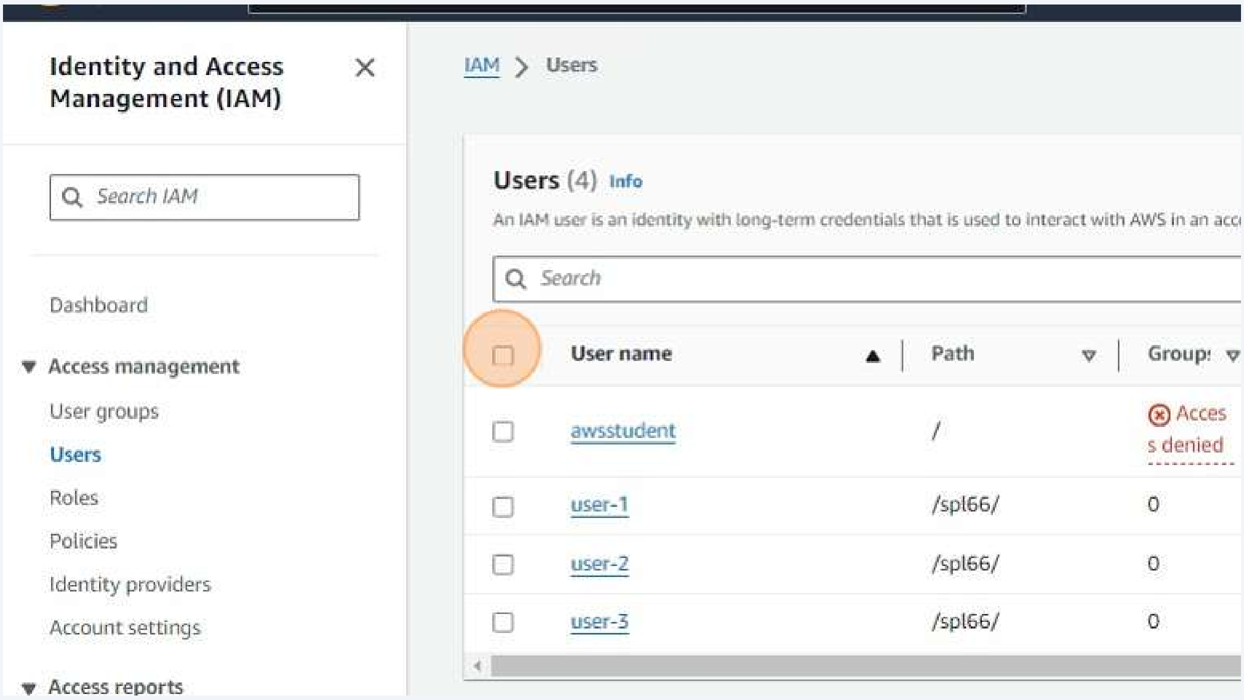
- IAM Access Analyzer now simplifies inspecting unused access to guide you toward least privilege. 3 mon
- IAM Access Analyzer introduces custom policy checks powered by automated reasoning. 3 months ago
- Announcing AWS IAM Identity Center APIs for visibility into workforce access to AWS. 3 months ago

88 Click here.



| ☐ | User name ▲ | Path ▽ | Group: ▽ | Last acti |
|---|---|---|---|---|
| ☐ | awsstudent | / | | |
| ☐ | user-1 | /spl66/ | | |
| ☐ | user-2 | /spl66/ | | |
| ☐ | user-3 | /spl66/ | | |

89 Click this checkbox.

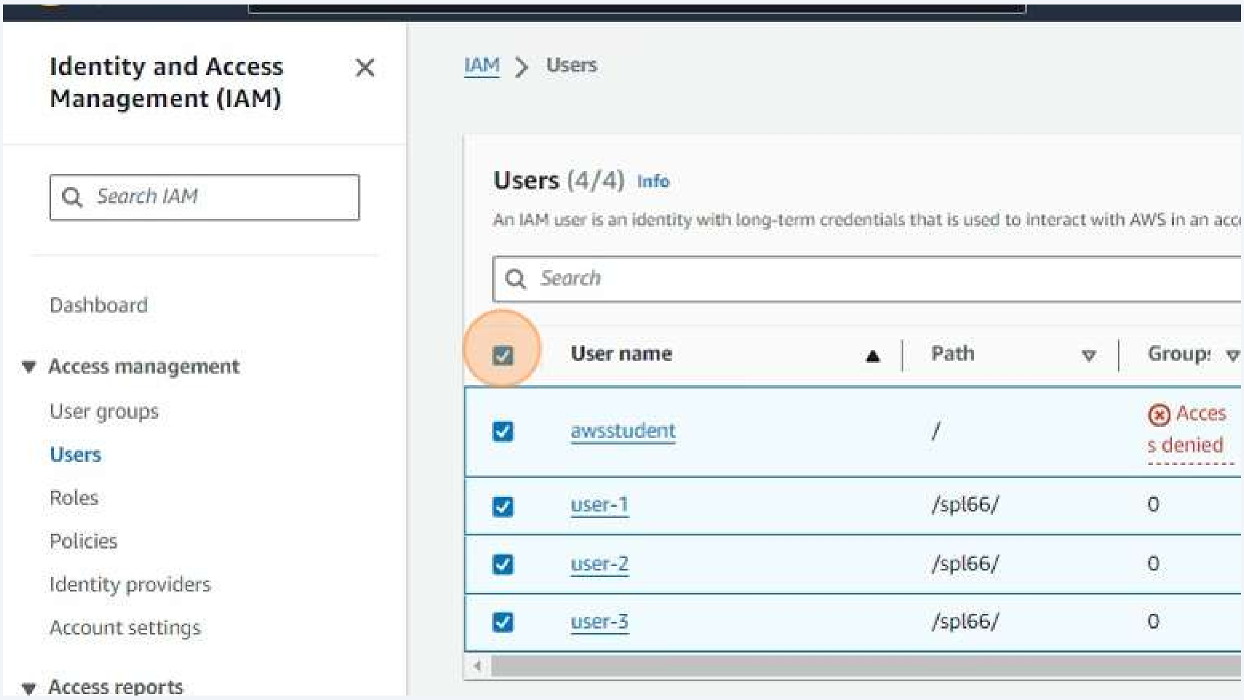


Users (4) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an acc

| □ | User name | Path | Group: |
|---|---|---|---|
| □ | awsstudent | / | Access denied |
| □ | user-1 | /spl66/ | 0 |
| □ | user-2 | /spl66/ | 0 |
| □ | user-3 | /spl66/ | 0 |

90 Click this checkbox.

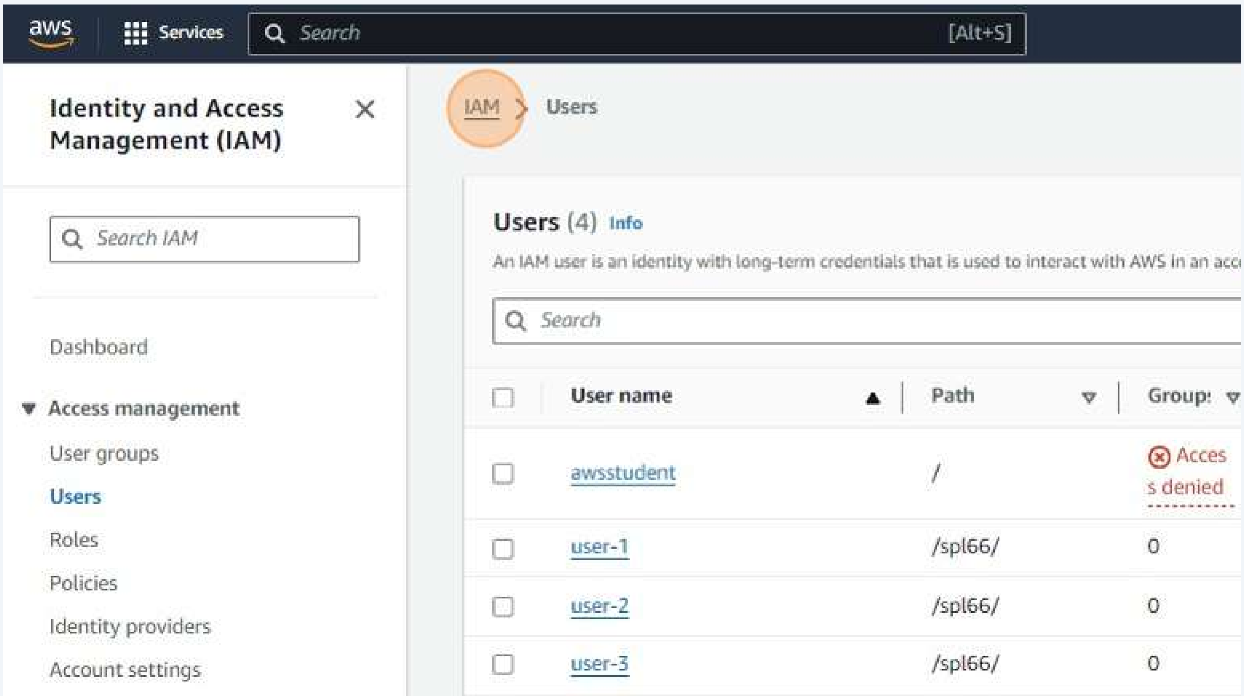


Users (4/4) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an acc

| ☑ | User name | Path | Group: |
|---|---|---|---|
| ☑ | awsstudent | / | Access denied |
| ☑ | user-1 | /spl66/ | 0 |
| ☑ | user-2 | /spl66/ | 0 |
| ☑ | user-3 | /spl66/ | 0 |

91 Click "IAM"



Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

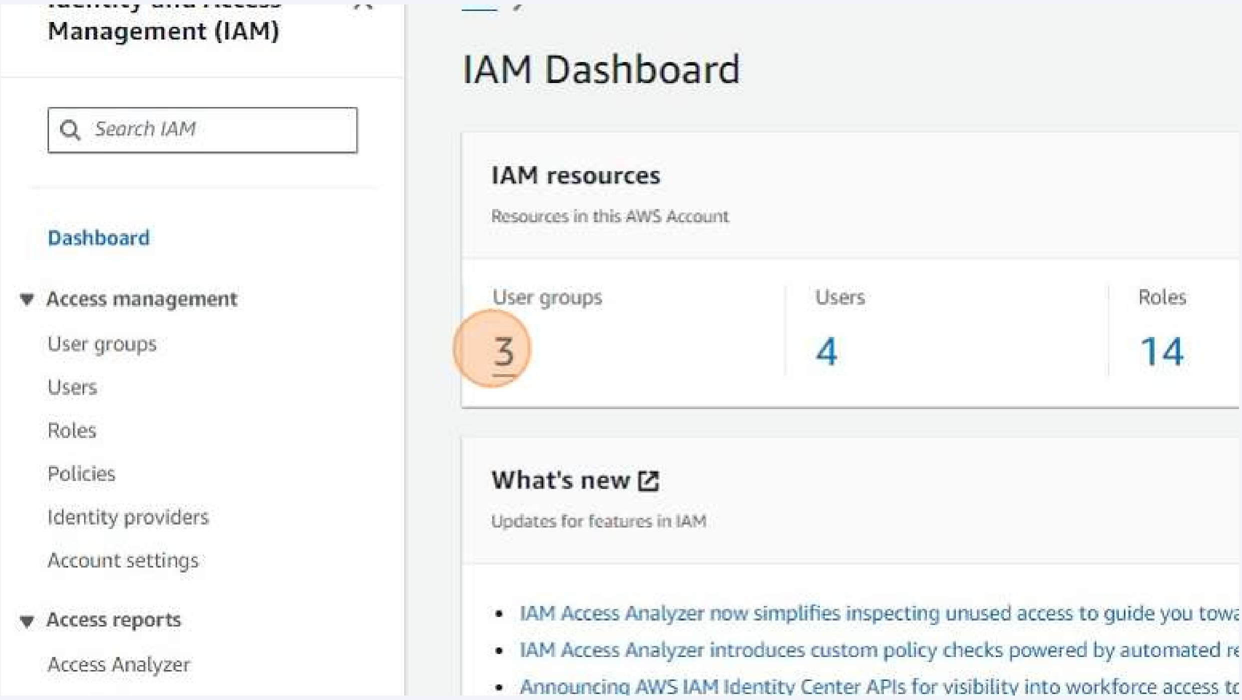
Users (4) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an acc

Search

| □ | User name | Path | Group: |
|---|---|---|---|
| □ | awsstudent | / | Access denied |
| □ | user-1 | /spl66/ | 0 |
| □ | user-2 | /spl66/ | 0 |
| □ | user-3 | /spl66/ | 0 |

92 Click "3"



Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access Analyzer

IAM Dashboard

IAM resources

Resources in this AWS Account

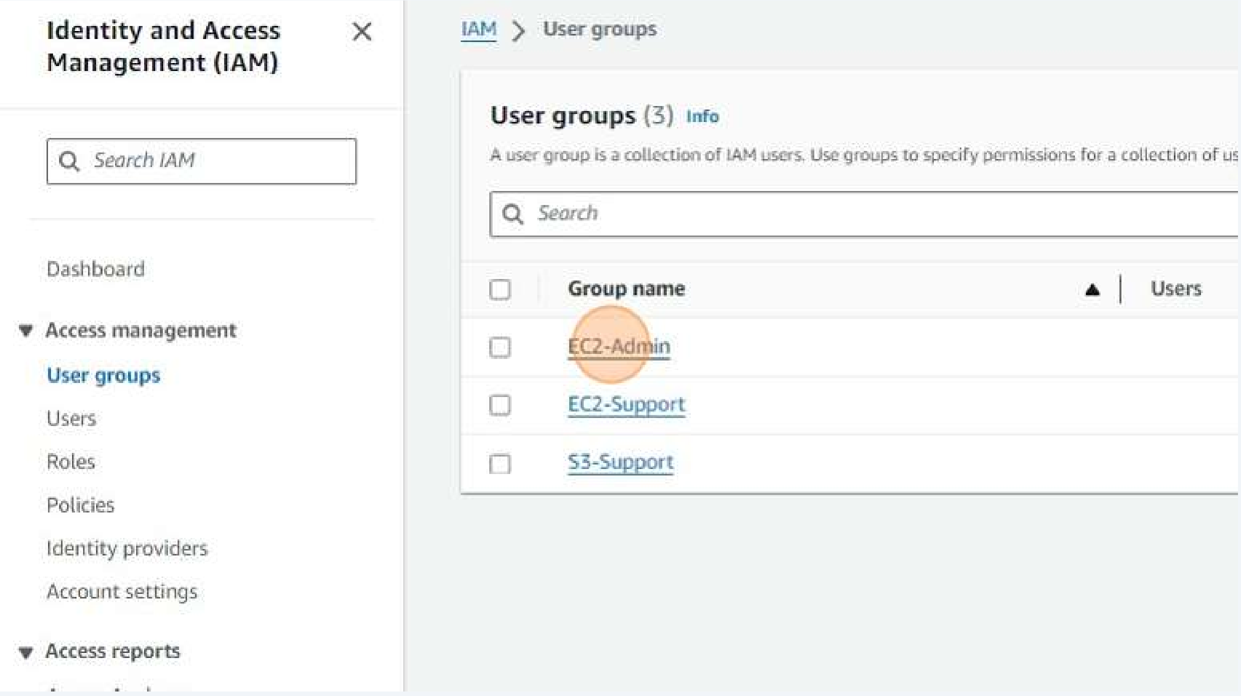
| User groups | Users | Roles |
|---|---|---|
| 3 | 4 | 14 |

What's new

Updates for features in IAM

- IAM Access Analyzer now simplifies inspecting unused access to guide you towa
- IAM Access Analyzer introduces custom policy checks powered by automated re
- Announcing AWS IAM Identity Center APIs for visibility into workforce access to

93 Click "EC2-Admin"

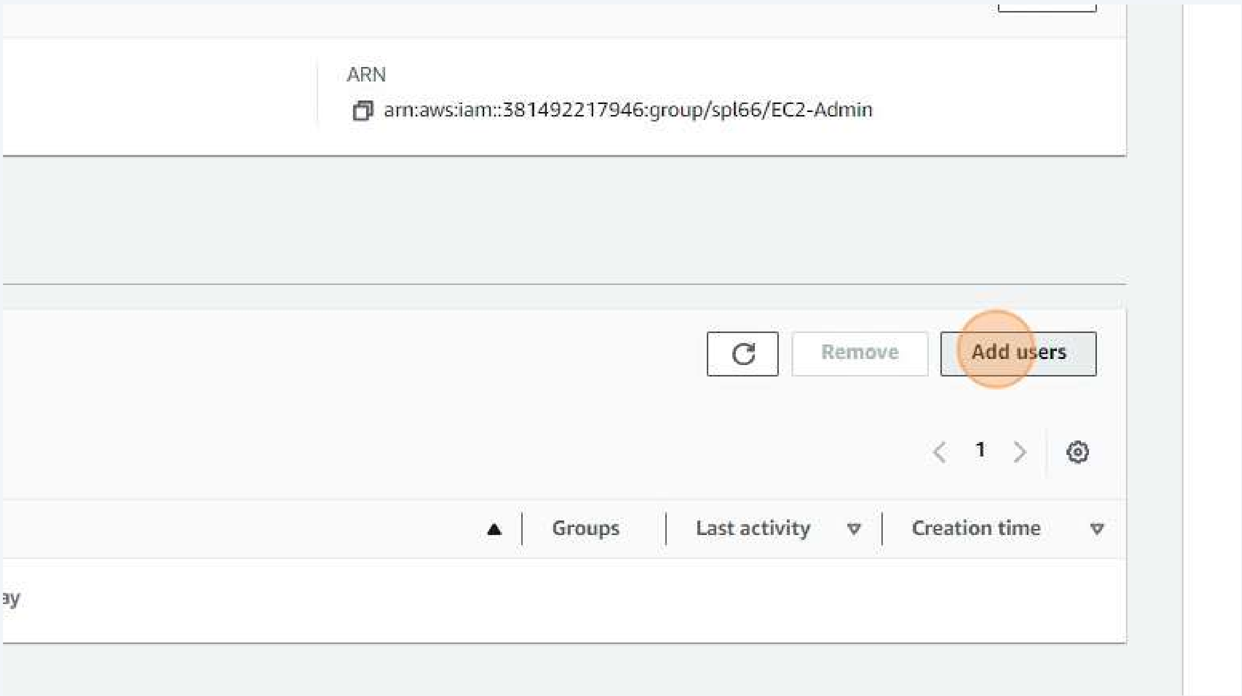


User groups (3) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of us

| ☐ | Group name ▲ | Users |
|---|---|---|
| ☐ | EC2-Admin | |
| ☐ | EC2-Support | |
| ☐ | S3-Support | |

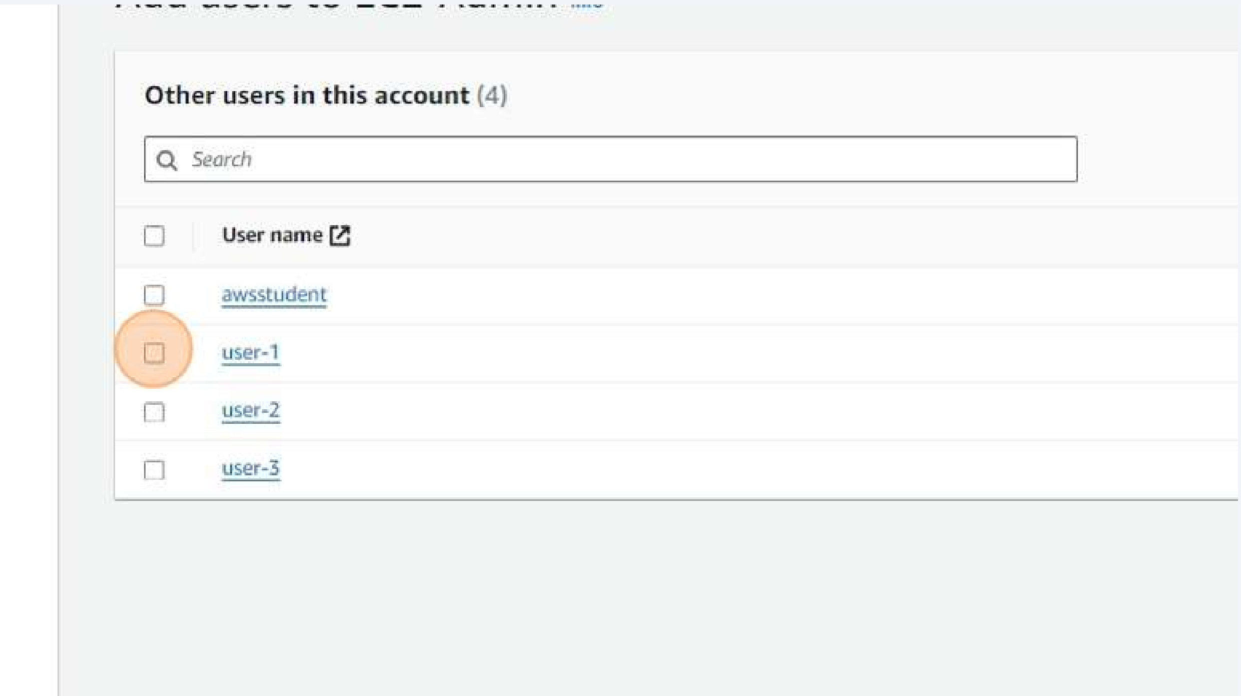
94 Click "Add users"



ARN

arn:aws:iam::381492217946:group/spl66/EC2-Admin

95 Click this checkbox.

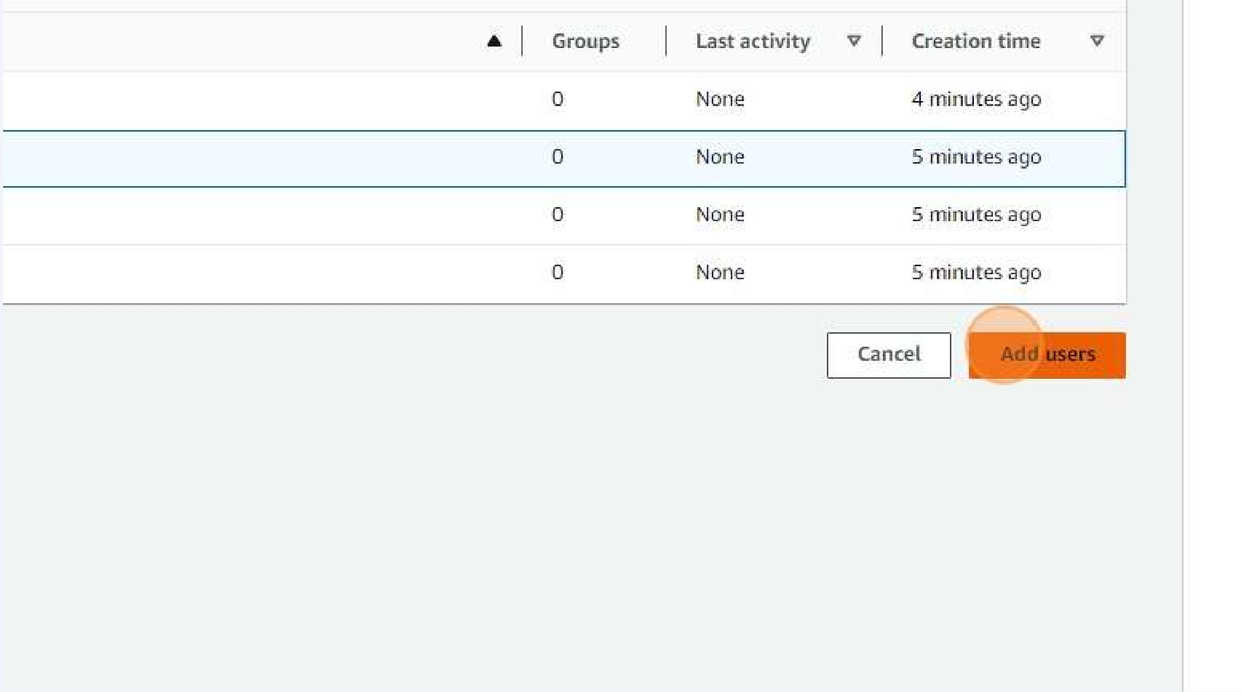


Other users in this account (4)

Search

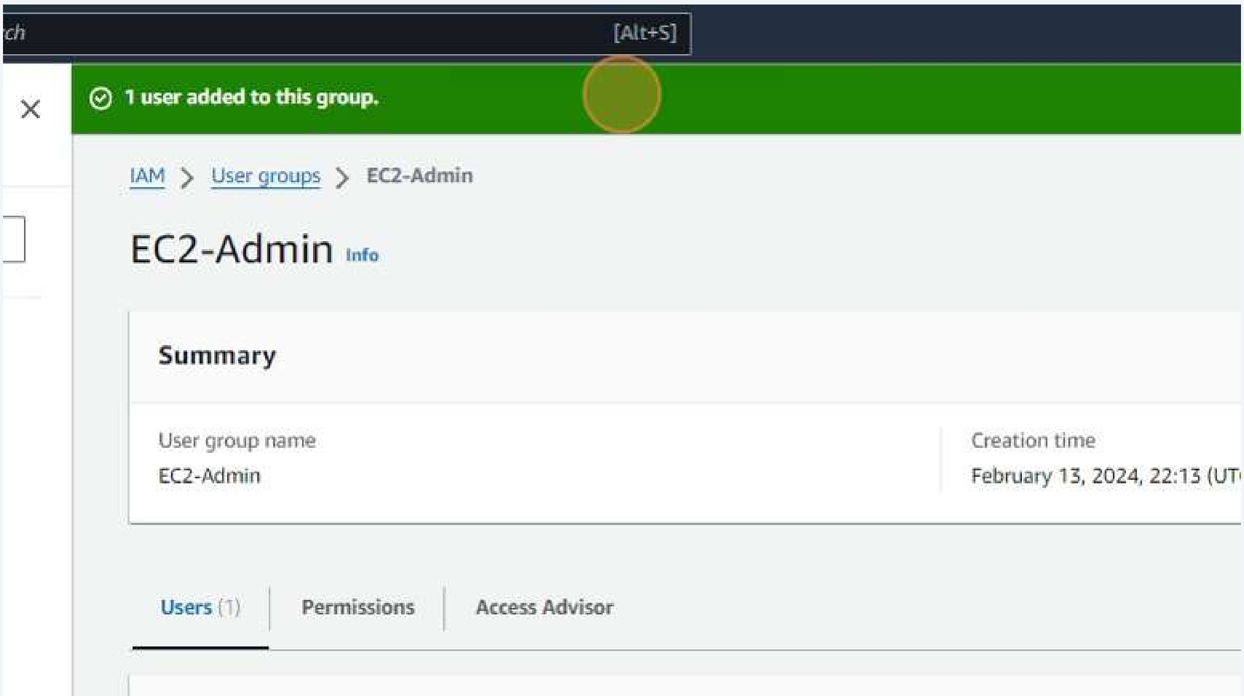
| □ | User name |
|---|---|
| □ | awsstudent |
| □ | user-1 |
| □ | user-2 |
| □ | user-3 |

96 Click "Add users"



| ▲ | Groups | Last activity ▽ | Creation time ▽ |
|---|---|---|---|
| | 0 | None | 4 minutes ago |
| | 0 | None | 5 minutes ago |
| | 0 | None | 5 minutes ago |
| | 0 | None | 5 minutes ago |

97 Click "1 user added to this group."



1 user added to this group.

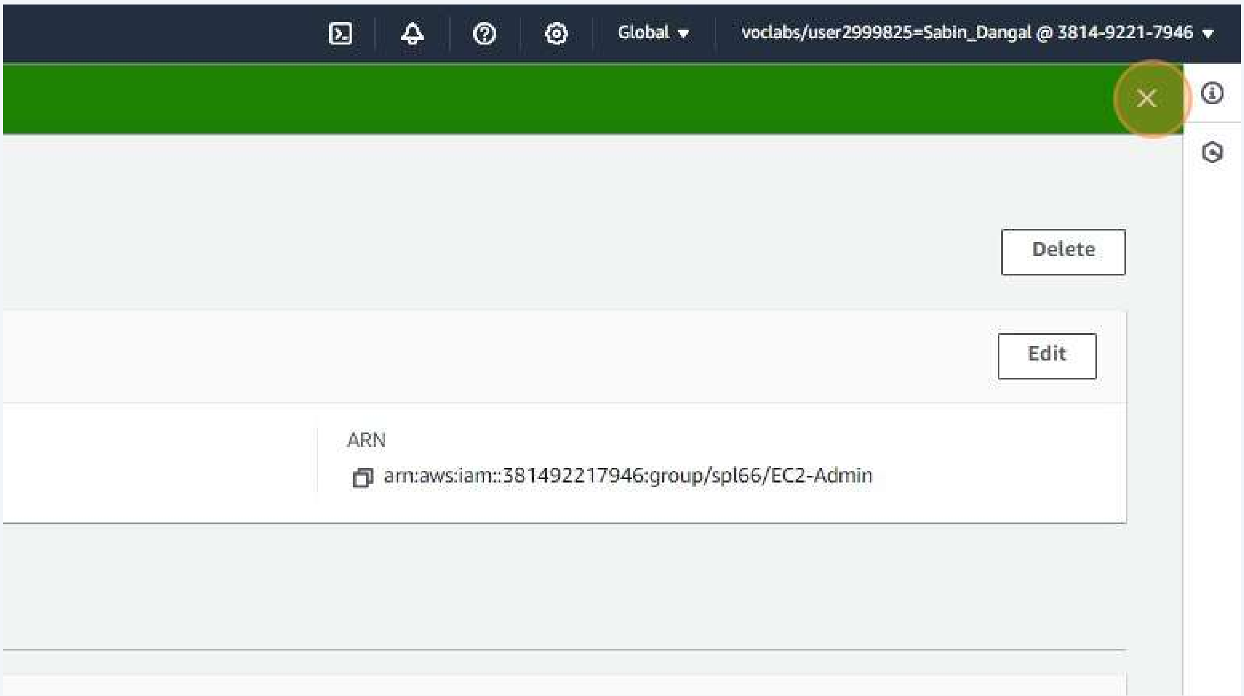
EC2-Admin

Summary

User group name
EC2-Admin

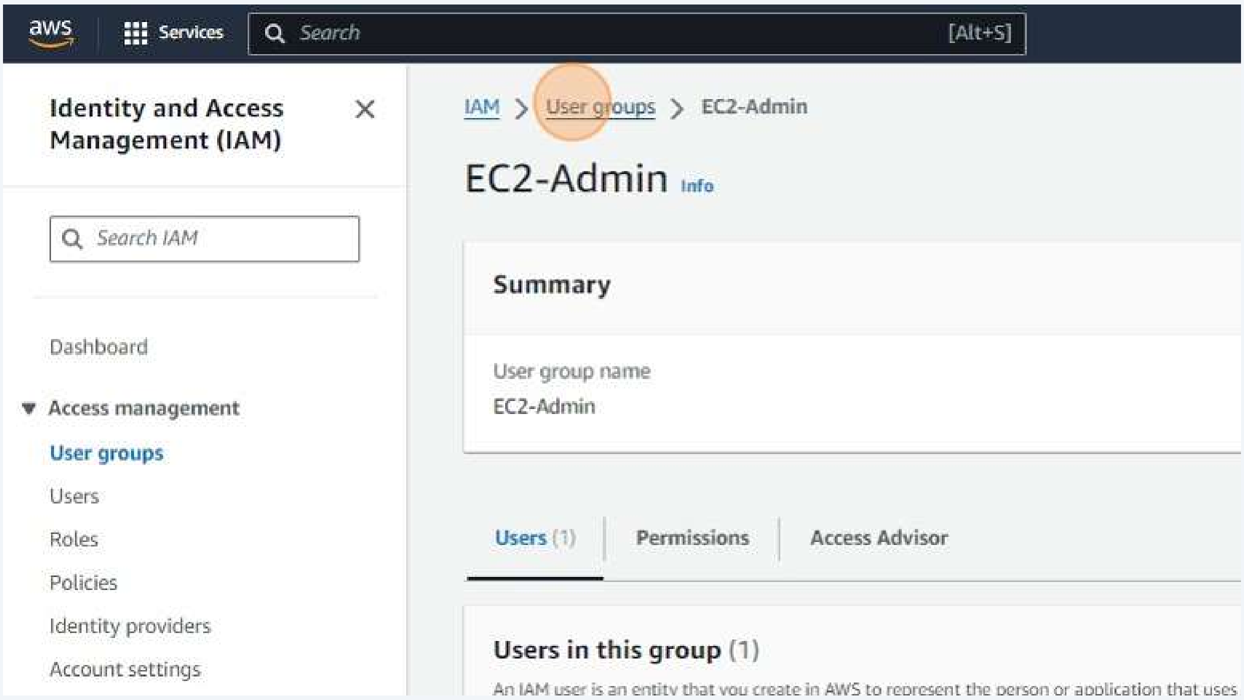
Creation time
February 13, 2024, 22:13 (UT

98 Click here.



ARN
arn:aws:iam::381492217946:group/spl66/EC2-Admin

99 Click "User groups"

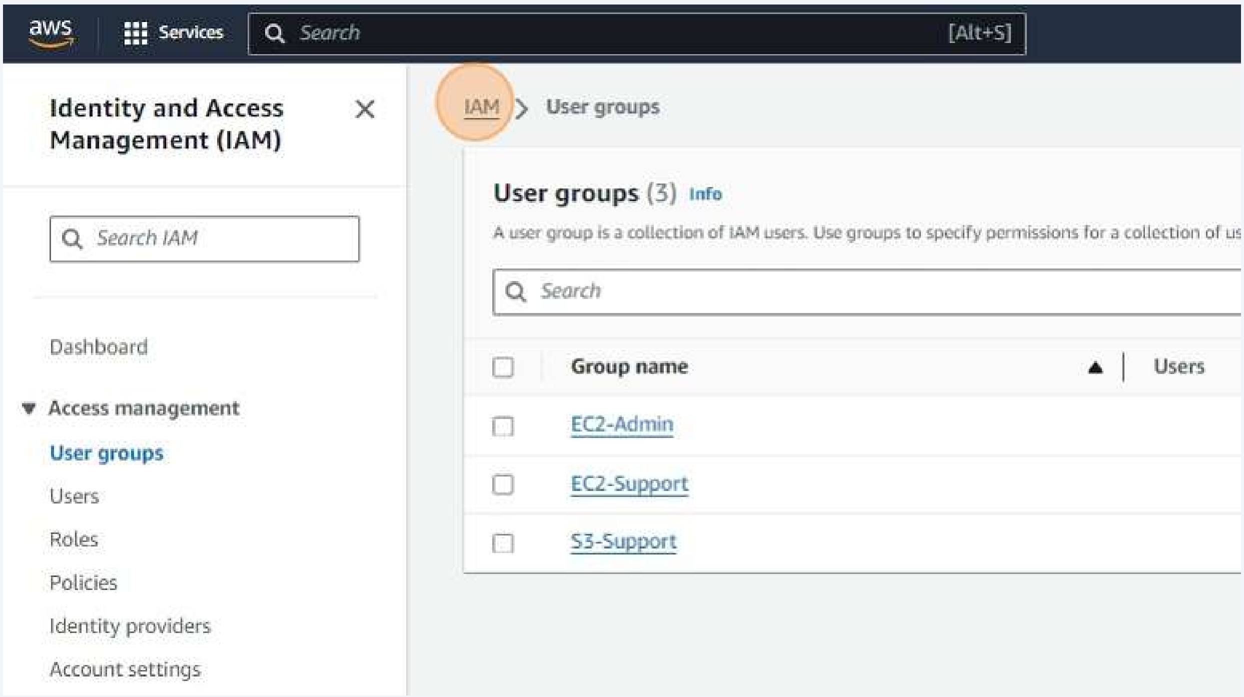


User group name
EC2-Admin

Users in this group (1)

An IAM user is an entity that you create in AWS to represent the person or application that uses

100 Click "IAM"

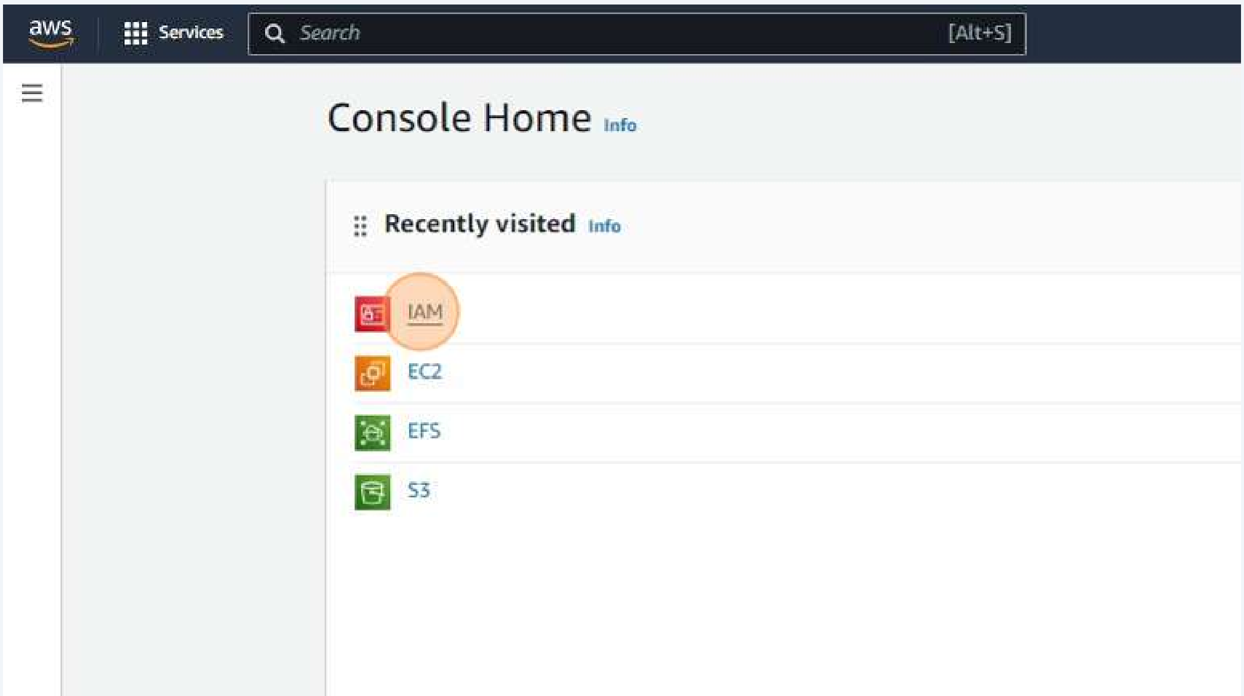


User groups (3)

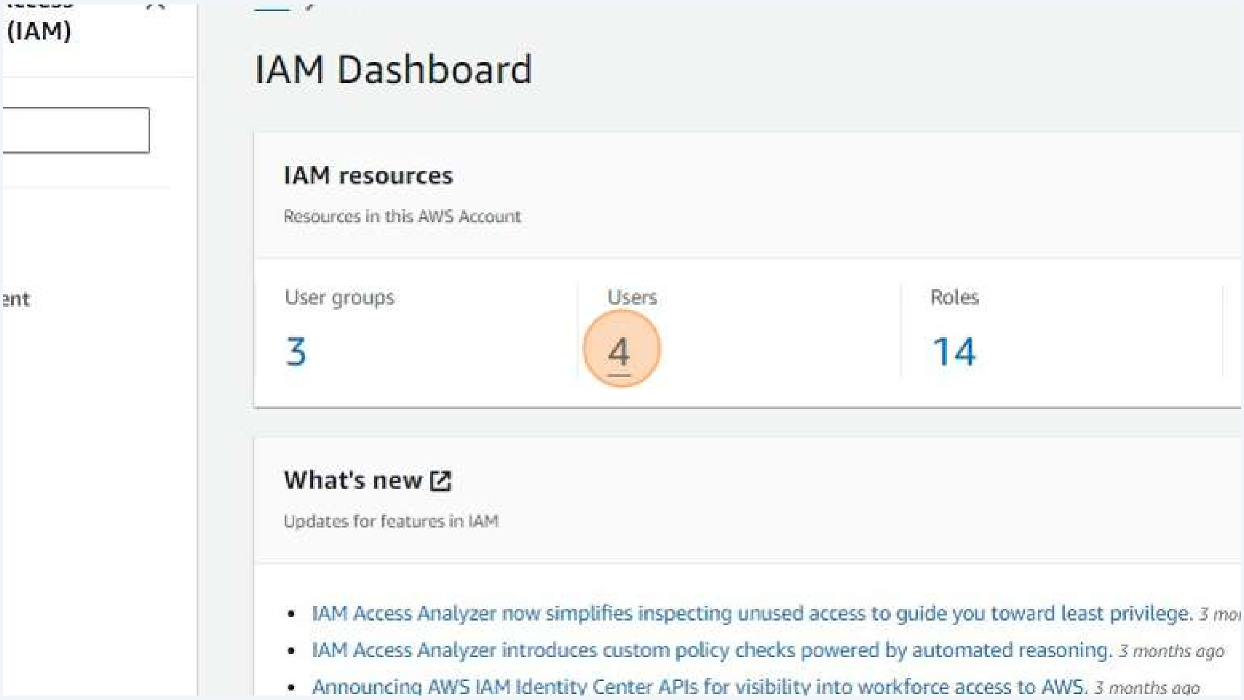
A user group is a collection of IAM users. Use groups to specify permissions for a collection of us

| □ | Group name ▲ | Users |
|---|---|---|
| □ | EC2-Admin | |
| □ | EC2-Support | |
| □ | S3-Support | |

101 Click "IAM"

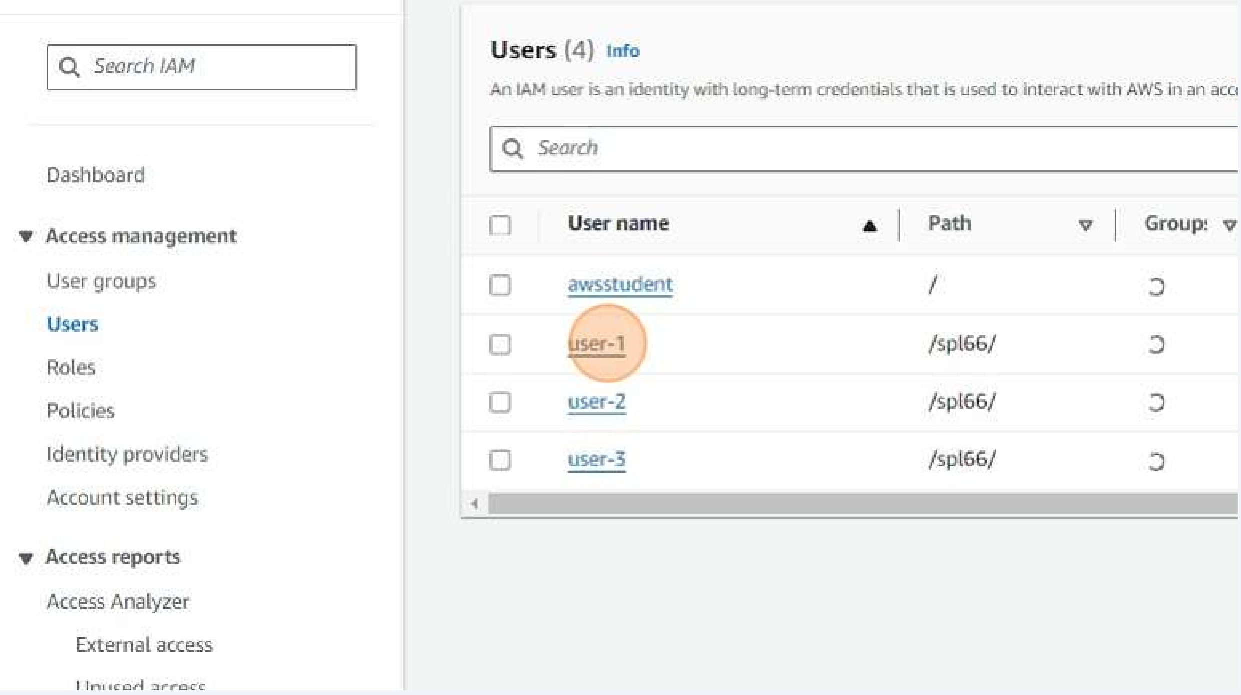


102 Click "4"



- IAM Access Analyzer now simplifies inspecting unused access to guide you toward least privilege. 3 mo
- IAM Access Analyzer introduces custom policy checks powered by automated reasoning. 3 months ago
- Announcing AWS IAM Identity Center APIs for visibility into workforce access to AWS. 3 months ago

**103** Click "user-1"

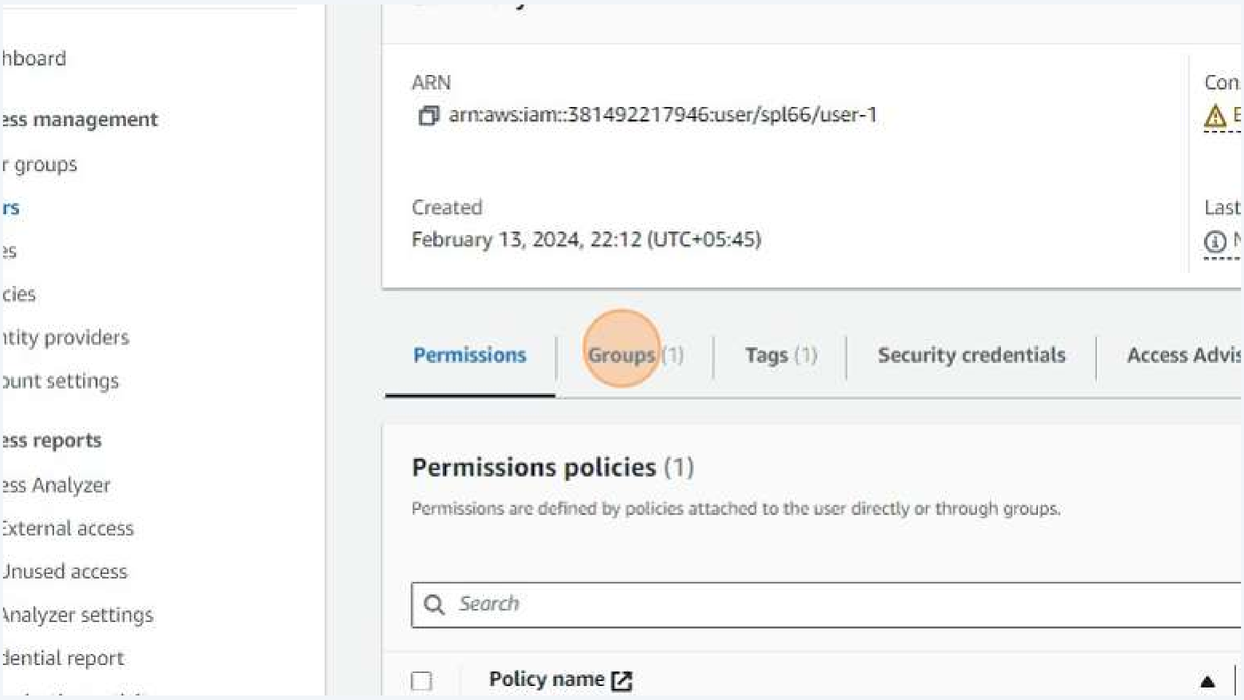


Users (4) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an acc

| □ | User name ▲ | Path | Group: |
|---|---|---|---|
| □ | awsstudent | / | |
| □ | user-1 | /spl66/ | |
| □ | user-2 | /spl66/ | |
| □ | user-3 | /spl66/ | |

**104** Click "Groups (1)"



ARN

arn:aws:iam::381492217946:user/spl66/user-1

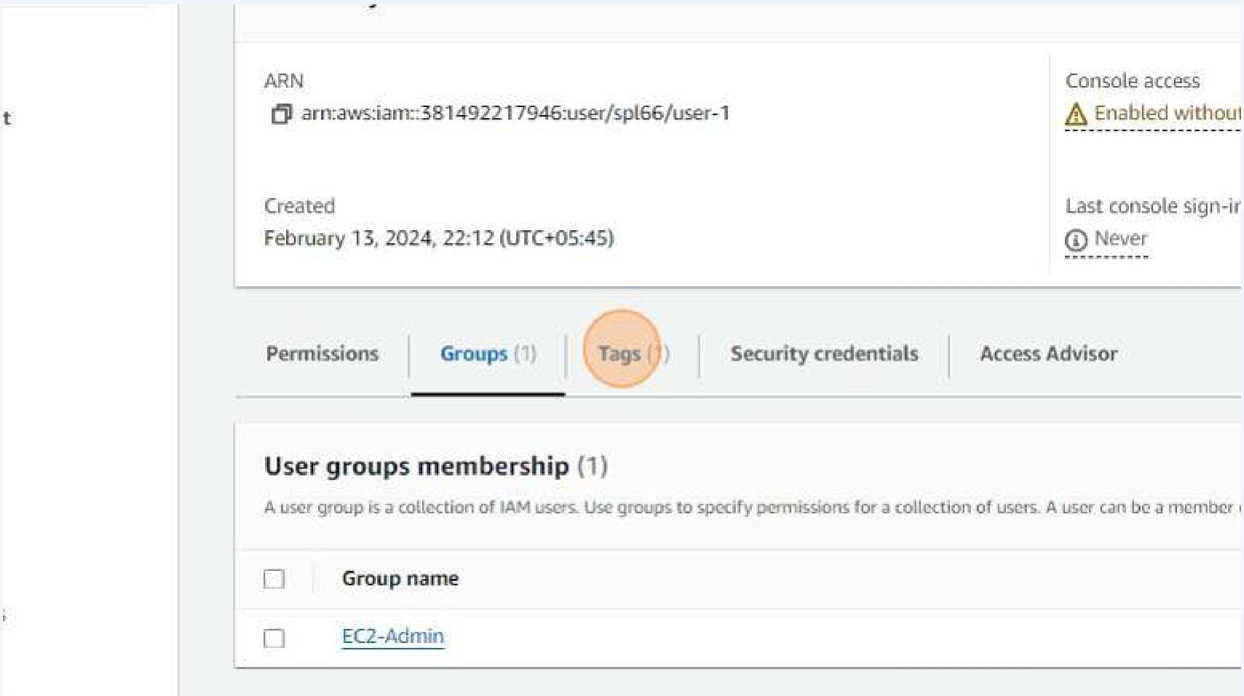
Created

February 13, 2024, 22:12 (UTC+05:45)

Permissions policies (1)

Permissions are defined by policies attached to the user directly or through groups.

105 Click "Tags (1)"



ARN
arn:aws:iam::381492217946:user/spl66/user-1

Created
February 13, 2024, 22:12 (UTC+05:45)

Console access
⚠ Enabled without

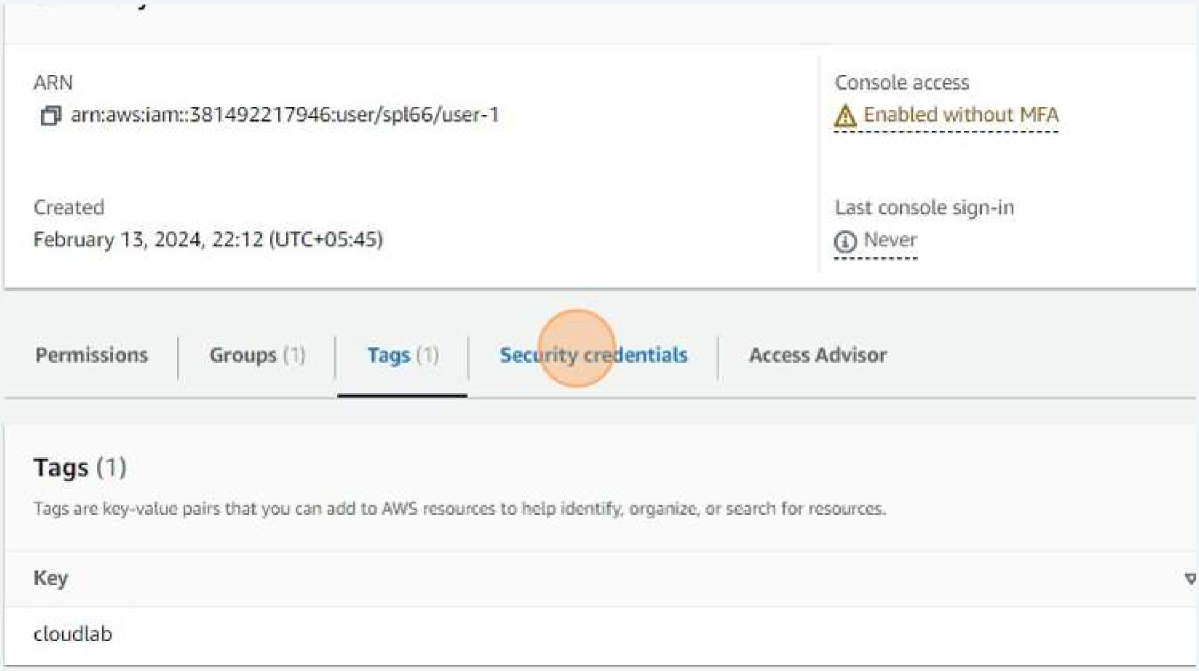
Last console sign-in
Never

User groups membership (1)

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users. A user can be a member

| □ | Group name |
|---|---|
| □ | EC2-Admin |

106 Click "Security credentials"



ARN
arn:aws:iam::381492217946:user/spl66/user-1

Created
February 13, 2024, 22:12 (UTC+05:45)

Console access
⚠ Enabled without MFA

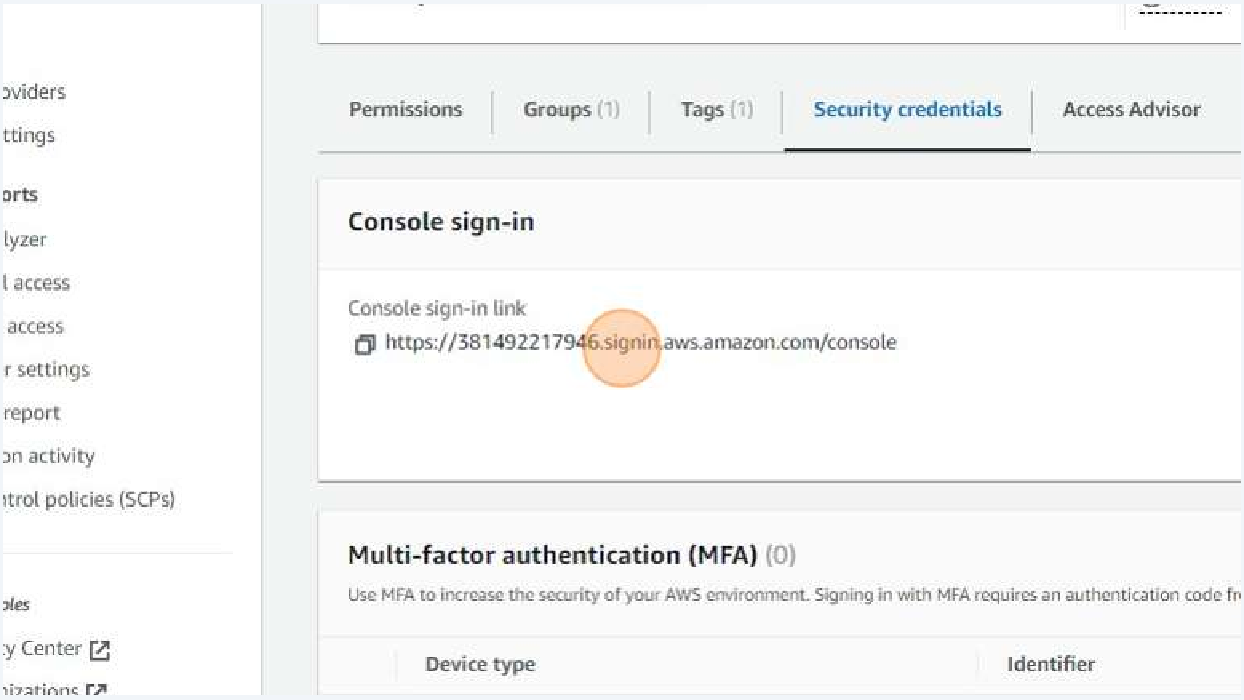
Last console sign-in
Never

Tags (1)

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

| Key |
|---|
| cloudlab |

107 Double-click "https://381492217946.signin.aws.amazon.com/console"



Console sign-in

Console sign-in link
https://381492217946.signin.aws.amazon.com/console

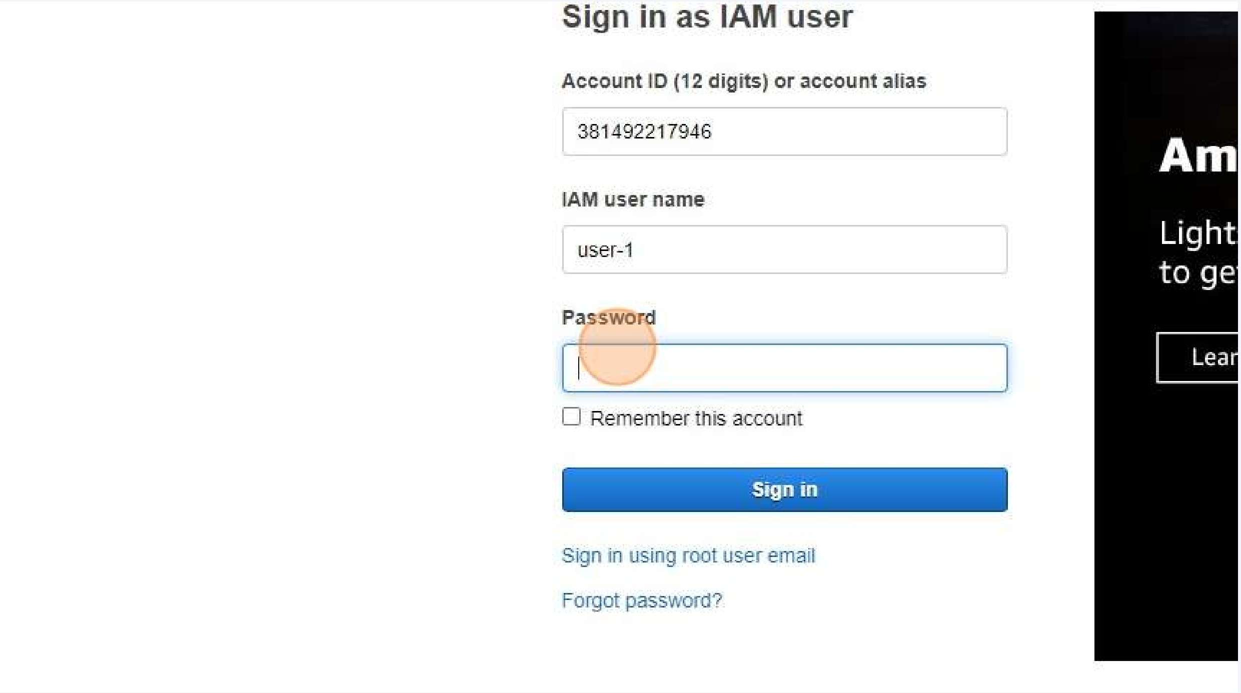
Multi-factor authentication (MFA) (0)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code fr

| Device type | Identifier |
|---|---|

108 Navigate to https://ap-southeast-2.signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code_challenge=20Hlbpqo6a_TwPpf5qaPuE37Ctiz13tuL8mz2zjnGgQ&code_challenge_method=SHA-256&response_type=code&redirect_uri=https%3A%2F%2Fconsole.aws.amazon.com%2Fconsole%2Fhome%3FhashArgs%3D%2523%26isauthcode%3Dtrue%26state%3DhashArgsFromTB_ap-southeast-2_5a40952f95a3eae3&X-Amz-Security-Token=IQoJb3JpZ2luX2VjEKD%2F%2F%2F%2F%2F%2F%2F%2F%2FwEaDmFwLXNvdXRoZWFzdC0yIkcwRQIhAKiOcsQ0bA6aCcPzCT6wztObLwF7B6rixRl6%2BAz8J8srAiB%2B%2BL0eTvnLjYbi4Zxo8pxircPo8hnugfDI%2BqYSBN4RmCqKAgh5EAIaDDQyNjA2MzgxNjU1NCIMVrnzTeuVyeTNaVDSKucBSwroM%2BBAOiylqcsEErYDeObTtrXR8XoLuPOkSqZ6q5OHpqjsxSqzOcOei8bjU93G6uPJY1c0LtJibQYkgBcihIcTcX0M0t%2FVkDYqiSUtCGaohuujCnWklzUxK3BE2lTDglVqCeVHQ36FoZVICPbox8bHKKTu9irSG2q2b9ALyDEaBvbOUvgzQSW%2FwfsKnHbJ4YUpFb7IOPs0FnEK7EN6Buau3%2FJE%2BtCjBzNzSAbnC22cXAMfTmFih31nXLpf3DaiF9N%2F2aCaWsoMb6B4yxrAaoXmPEx0IEIpMgp%2BQHfaHkK1M405mWIpMNKtrq4GOo8Bj6Hm4U7OF7%2BWn2brcvFSUc15WejOJSfvCQRPhERm60D9jr%2BvuDYWthzTflTQRtVBasd6GOptqLUOiEM%2FzpDsTqaXIxU6p%2F7gfSCZbUbFaA4RDdZeF3wpb1fk91QGxJKWeoi%2BI78gk7qAE%2BB6oSIM6gBNJ7qyBawCKw%2FWqJeo6%2BNINU61hA%2Bi8pbj14YsmmI%3D&X-Amz-Date=20240213T163714Z&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=ASIAWGM3B45VAWRBQ6ME%2F20240213%2Fap-southeast-2%2Fsignin%2Faws4_request&X-Amz-SignedHeaders=host&X-Amz-Signature=07223e71f4ea4efa3c290451ad296de450e43b008948940aff1b48ab2fdc6982

109 Click the "Password" field.



Sign in as IAM user

Account ID (12 digits) or account alias

381492217946

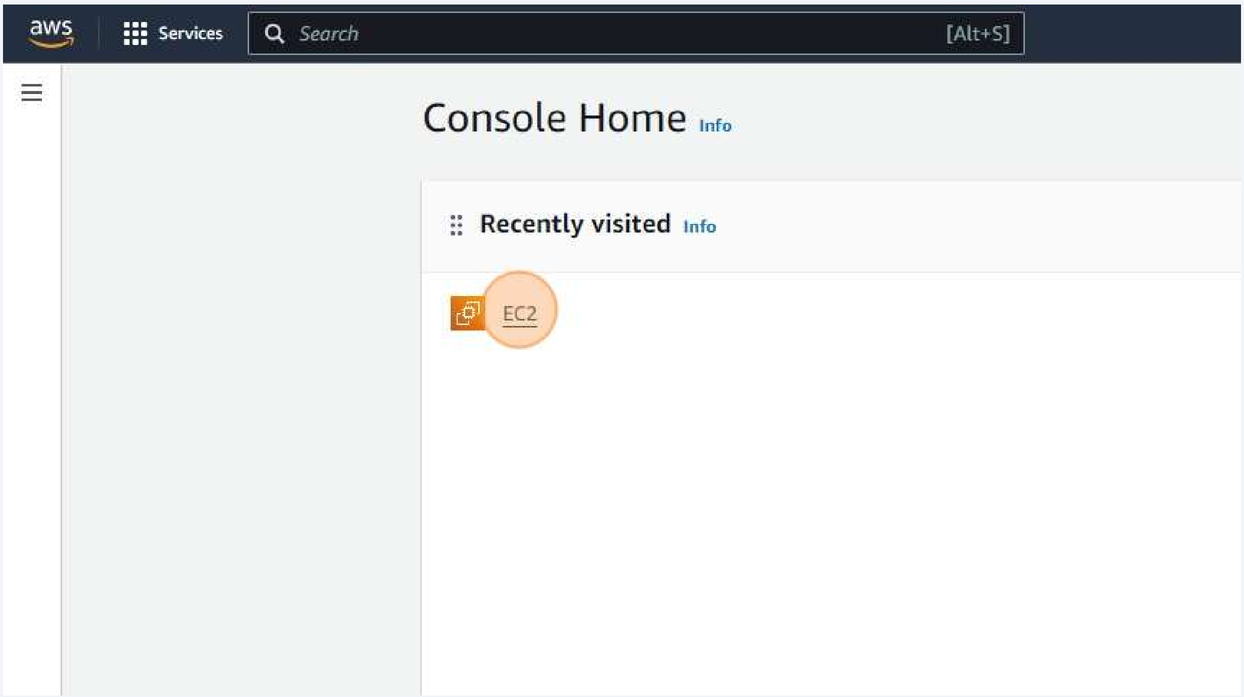
IAM user name

user-1

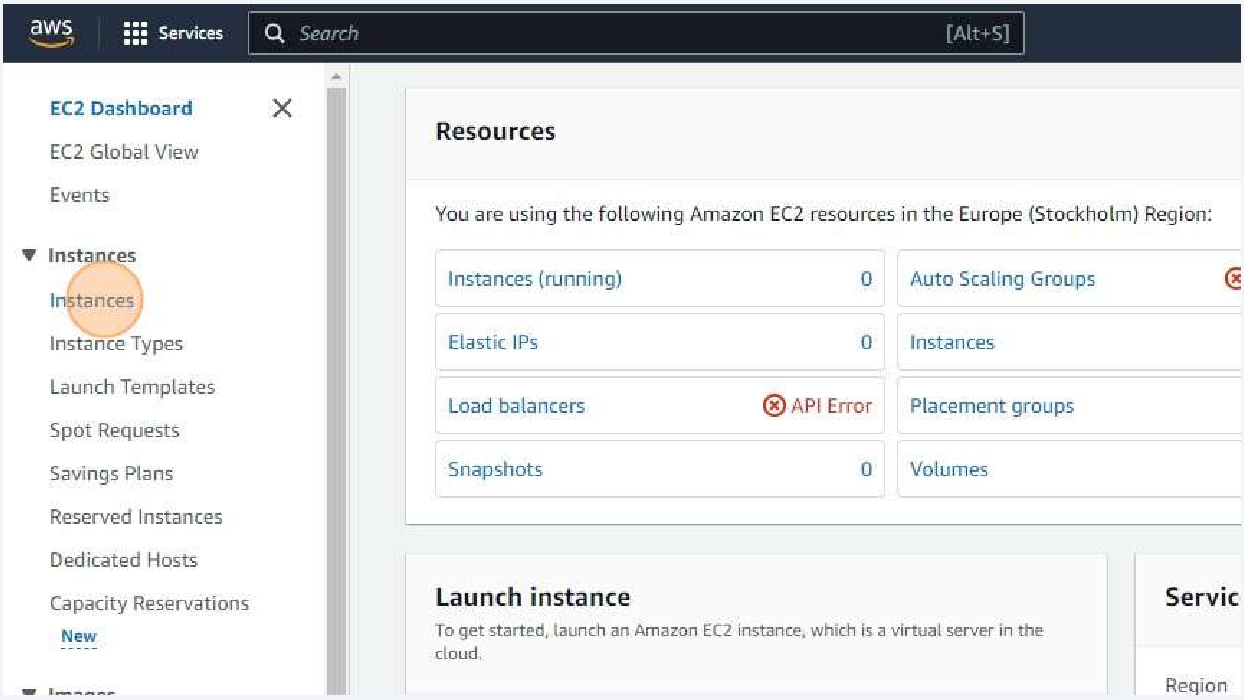
Password

□ Remember this account

110 Click "EC2"



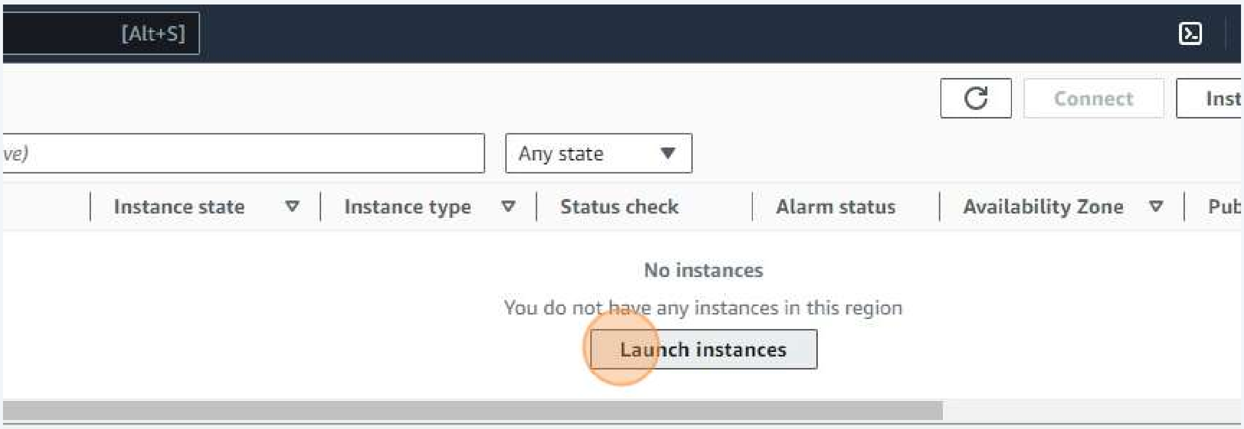
111 Click "Instances"



You are using the following Amazon EC2 resources in the Europe (Stockholm) Region:

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

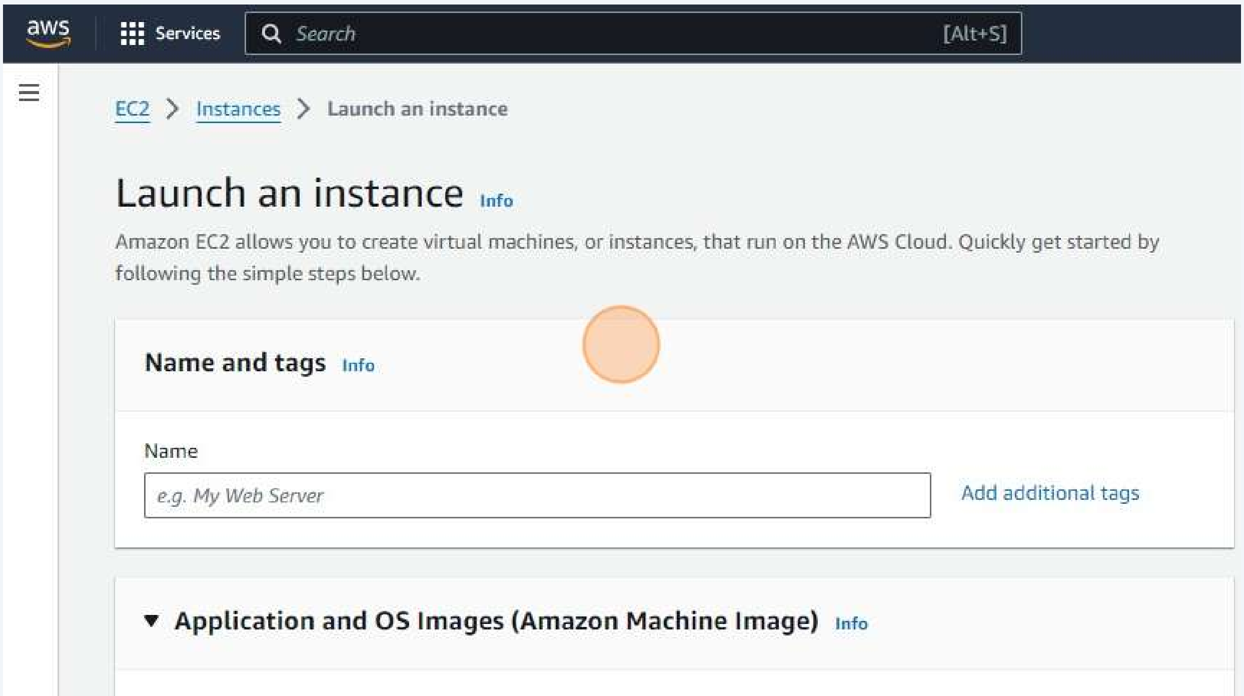
112 Click "Launch instances"



No instances

You do not have any instances in this region

113 Click here.



EC2 > Instances > Launch an instance

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

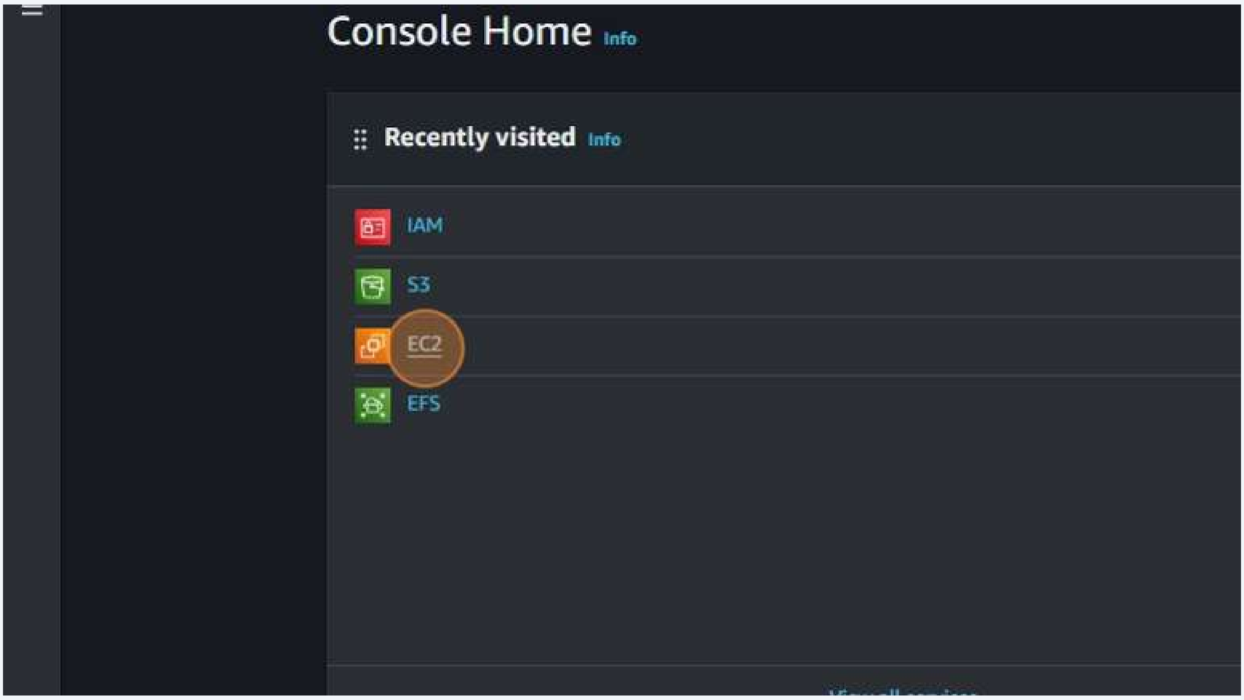
Add additional tags

▼ Application and OS Images (Amazon Machine Image) Info

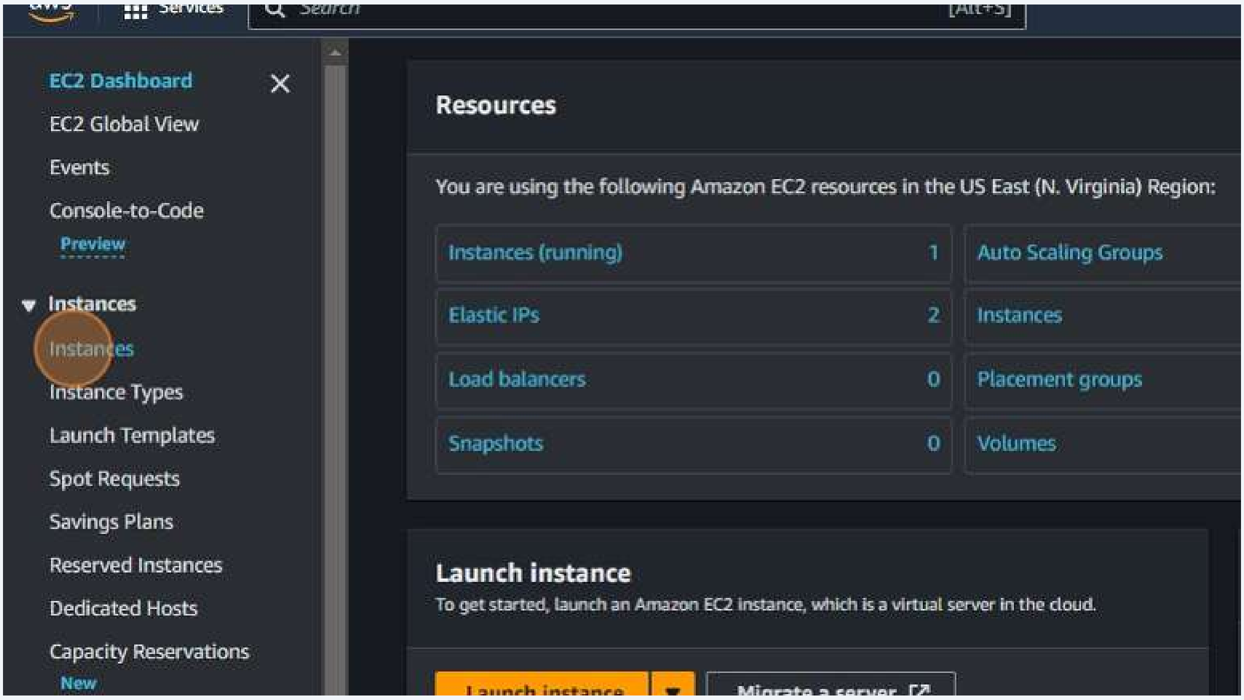
## EC2 Basics Lab

114 Navigate to [https://us-east-1.console.aws.amazon.com/console/home?region=us-east-1#](https://us-east-1.console.aws.amazon.com/console/home?region=us-east-1#)

115 Click "EC2"



116 Click "Instances"



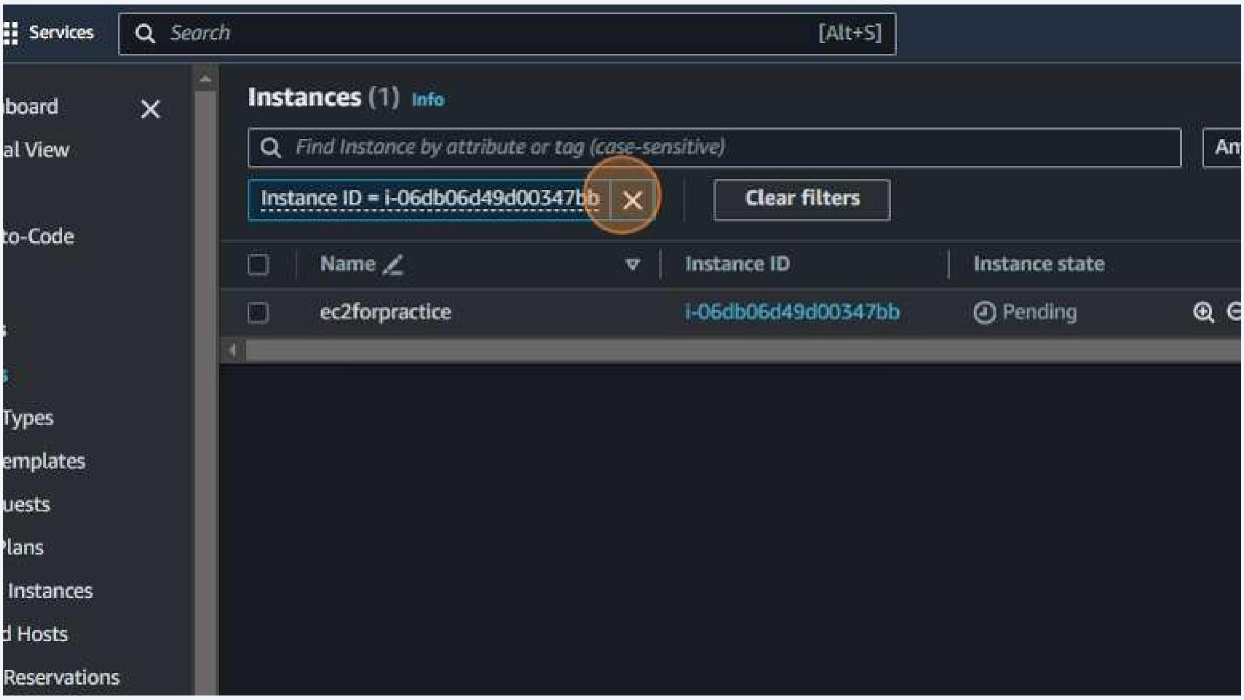
You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

| | | |
|---|---|---|
| Instances (running) | 1 | Auto Scaling Groups |
| Elastic IPs | 2 | Instances |
| Load balancers | 0 | Placement groups |
| Snapshots | 0 | Volumes |

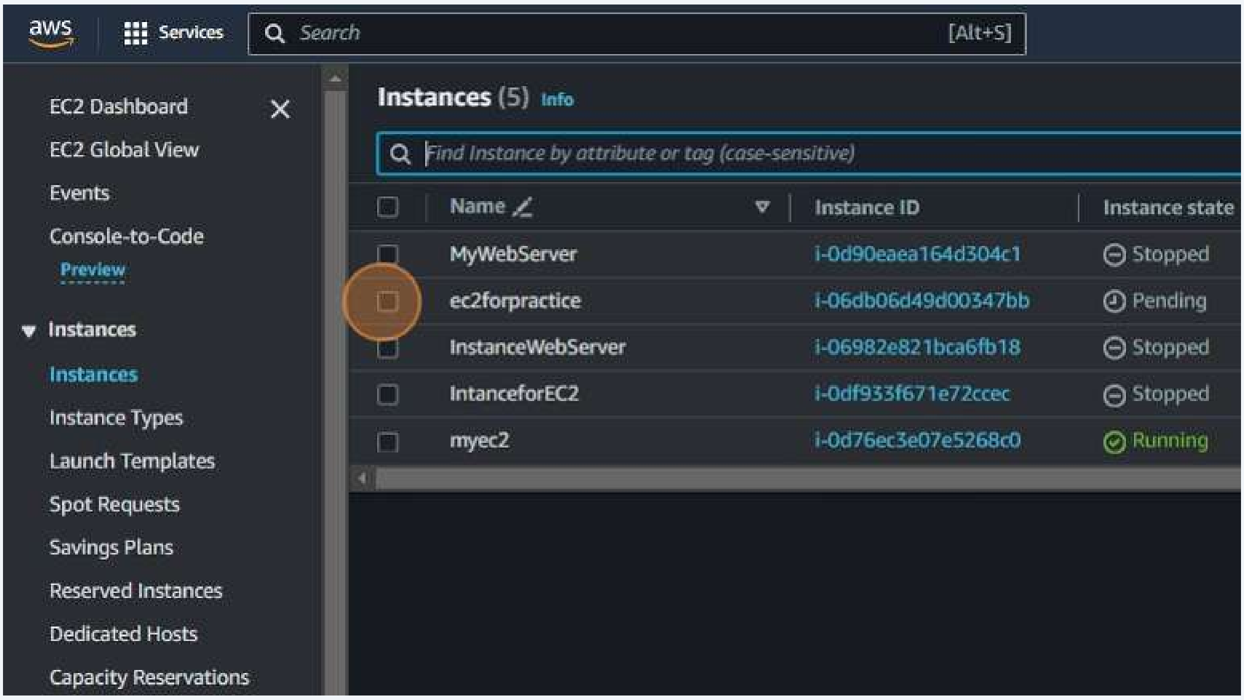
To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

117 Press **ctrl** + **v**

118 Click here.

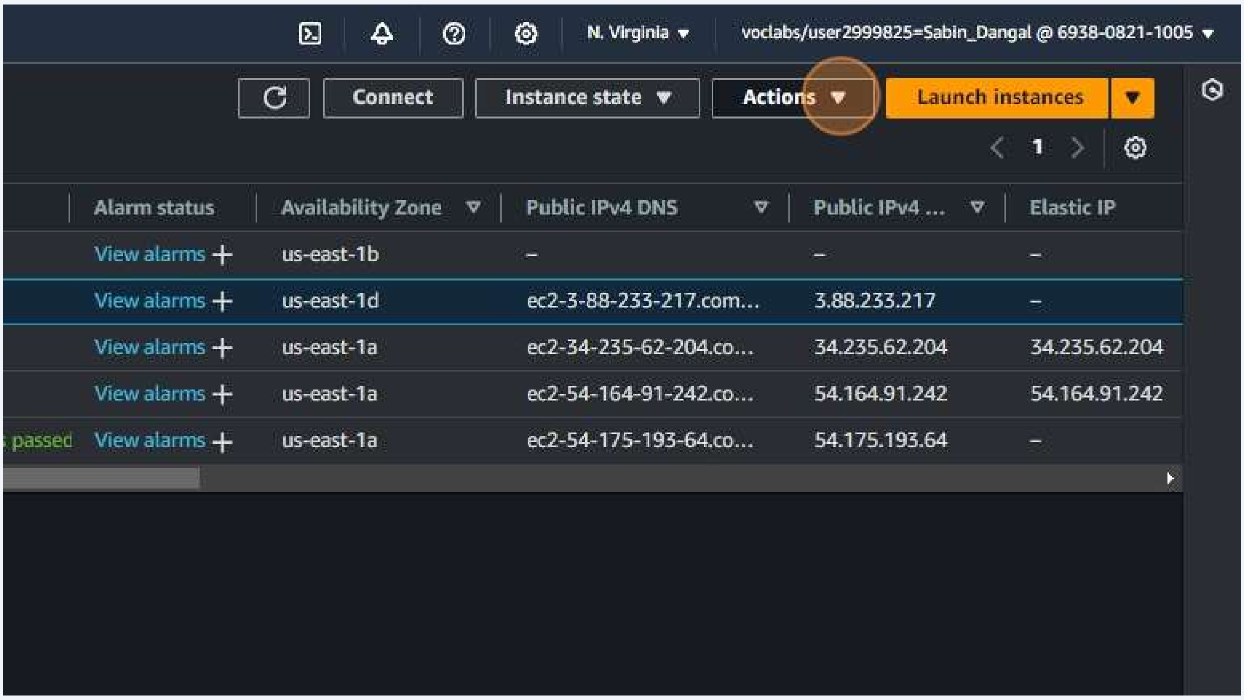


119 Click this checkbox.



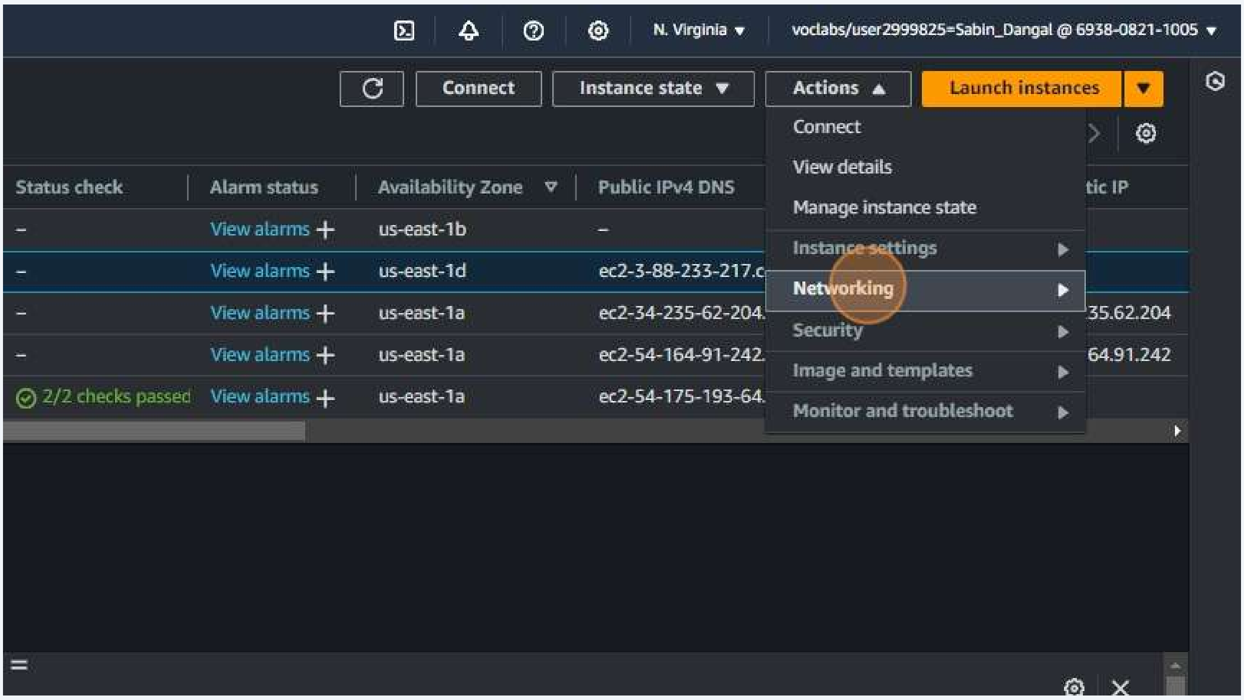
| □ | Name | Instance ID | Instance state |
|---|---|---|---|
| □ | MyWebServer | i-0d90eaea164d304c1 | Stopped |
| □ | ec2forpractice | i-06db06d49d00347bb | Pending |
| □ | InstanceWebServer | i-06982e821bca6fb18 | Stopped |
| □ | IntanceforEC2 | i-0df933f671e72ccec | Stopped |
| □ | myec2 | i-0d76ec3e07e5268c0 | Running |

120 Click here.



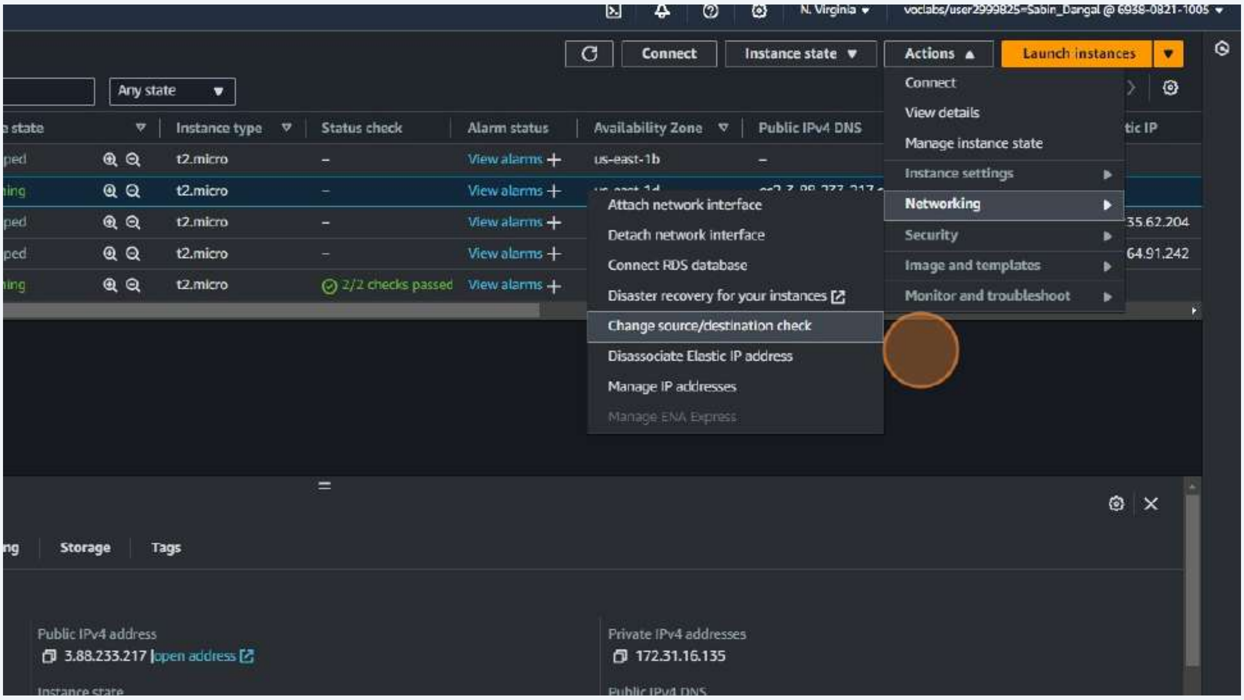
| | Alarm status | Availability Zone | Public IPv4 DNS | Public IPv4 ... | Elastic IP |
|---|---|---|---|---|---|
| | View alarms + | us-east-1b | – | – | – |
| | View alarms + | us-east-1d | ec2-3-88-233-217.com... | 3.88.233.217 | – |
| | View alarms + | us-east-1a | ec2-34-235-62-204.co... | 34.235.62.204 | 34.235.62.204 |
| | View alarms + | us-east-1a | ec2-54-164-91-242.co... | 54.164.91.242 | 54.164.91.242 |
| passed | View alarms + | us-east-1a | ec2-54-175-193-64.co... | 54.175.193.64 | – |

**121** Click "Networking"



| Status check | Alarm status | Availability Zone | Public IPv4 DNS | tic IP |
|---|---|---|---|---|
| – | View alarms + | us-east-1b | – | |
| – | View alarms + | us-east-1d | ec2-3-88-233-217.c | |
| – | View alarms + | us-east-1a | ec2-34-235-62-204. | 35.62.204 |
| – | View alarms + | us-east-1a | ec2-54-164-91-242. | 64.91.242 |
| ✓ 2/2 checks passed | View alarms + | us-east-1a | ec2-54-175-193-64. | |

**122** Click here.



| state | Instance type | Status check | Alarm status | Availability Zone | Public IPv4 DNS | tic IP |
|---|---|---|---|---|---|---|
| ped | t2.micro | – | View alarms + | us-east-1b | – | |
| ning | t2.micro | – | View alarms + | | | |
| ped | t2.micro | – | View alarms + | | | 35.62.204 |
| ped | t2.micro | – | View alarms + | | | 64.91.242 |
| ning | t2.micro | ✓ 2/2 checks passed | View alarms + | | | |

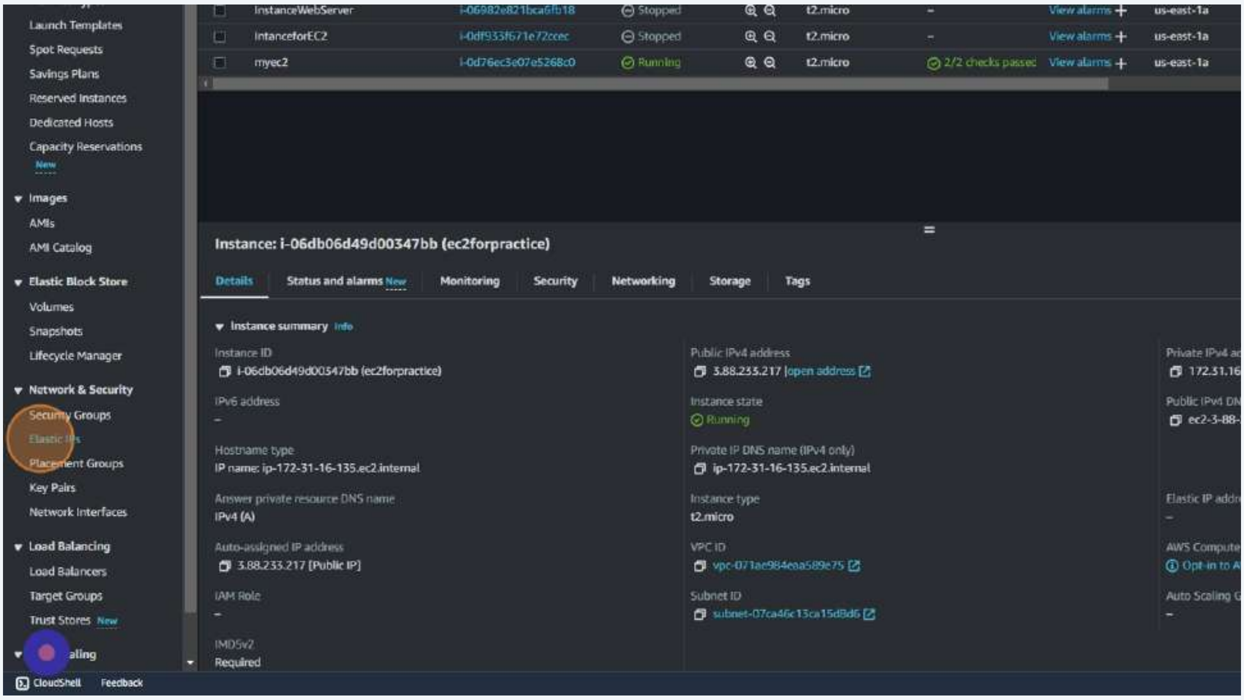
Public IPv4 address
3.88.233.217 | open address

Private IPv4 addresses
172.31.16.135

Instance state

Public IPv4 DNS

**123** Click "Elastic IPs"



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| □ | InstanceWebServer | i-06982e821bca6fb18 | ⊖ Stopped | t2.micro | – | View alarms + | us-east-1a |
| □ | IntanceforEC2 | i-0df933f671e72ccec | ⊖ Stopped | t2.micro | – | View alarms + | us-east-1a |
| □ | myec2 | i-0d76ec3e07e5268c0 | ✓ Running | t2.micro | ✓ 2/2 checks passec | View alarms + | us-east-1a |

Instance: i-06db06d49d00347bb (ec2forpractice)

Instance summary

Instance ID: i-06db06d49d00347bb (ec2forpractice)

IPv6 address: –

Hostname type: IP name: ip-172-31-16-135.ec2.internal

Answer private resource DNS name: IPv4 (A)

Auto-assigned IP address: 3.88.233.217 [Public IP]

IAM Role: –

IMDSv2: Required

Public IPv4 address: 3.88.233.217 |open address

Instance state: Running

Private IP DNS name (IPv4 only): ip-172-31-16-135.ec2.internal

Instance type: t2.micro

VPC ID: vpc-071ae984eaa589e75

Subnet ID: subnet-07ca46c13ca15d8d6

Private IPv4 ad: 172.31.16

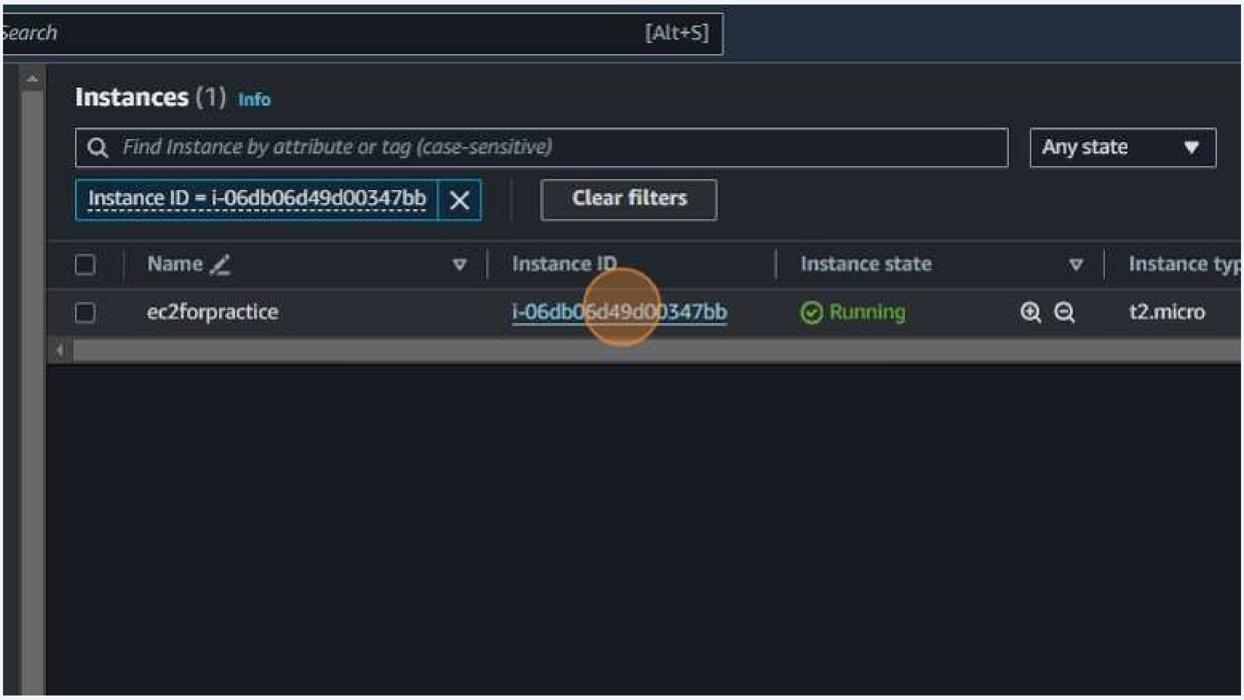
Public IPv4 DN: ec2-3-88-

Elastic IP addr: –

AWS Compute: Opt-in to A

Auto Scaling G: –

**124** Click "i-06db06d49d00347bb"

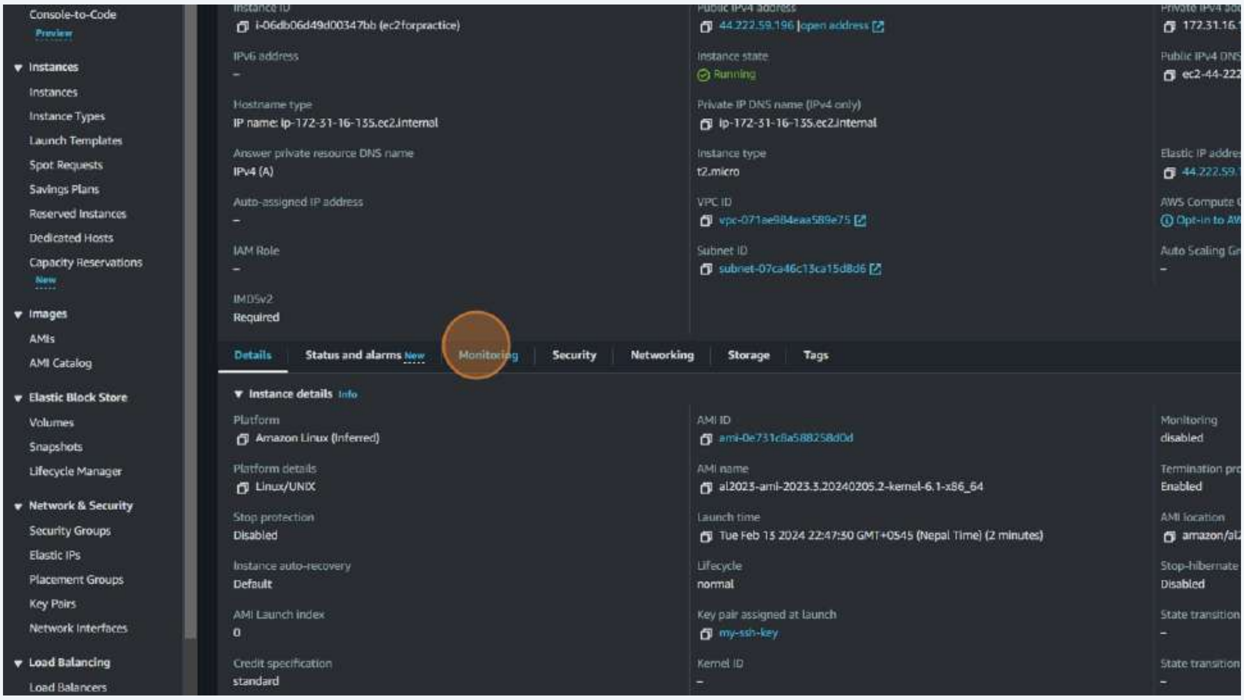


Instances (1) Info

Instance ID = i-06db06d49d00347bb

| □ | Name | Instance ID | Instance state | Instance typ |
|---|---|---|---|---|
| □ | ec2forpractice | i-06db06d49d00347bb | ✓ Running | t2.micro |

**125** Click "Monitoring"



Instance ID
i-06db06d49d00347bb (ec2forpractice)

Public IPv4 address
44.222.59.196 | open address

Private IPv4 add
172.31.16.1

IPv6 address
–

Instance state
Running

Public IPv4 DNS
ec2-44-222

Hostname type
IP name: ip-172-31-16-135.ec2.internal

Private IP DNS name (IPv4 only)
ip-172-31-16-135.ec2.internal

Answer private resource DNS name
IPv4 (A)

Instance type
t2.micro

Elastic IP addre
44.222.59.1

Auto-assigned IP address
–

VPC ID
vpc-071ae984eaa589e75

AWS Compute
Opt-in to AW

IAM Role
–

Subnet ID
subnet-07ca46c13ca15d8d6

Auto Scaling Gr
–

IMDSv2
Required

Instance details Info

Platform
Amazon Linux (Inferred)

AMI ID
ami-0e731c8a588258d0d

Monitoring
disabled

Platform details
Linux/UNIX

AMI name
al2023-ami-2023.3.20240205.2-kernel-6.1-x86_64

Termination pro
Enabled

Stop protection
Disabled

Launch time
Tue Feb 13 2024 22:47:30 GMT+0545 (Nepal Time) (2 minutes)

AMI location
amazon/al2

Instance auto-recovery
Default

Lifecycle
normal

Stop-hibernate
Disabled

AMI Launch index
0

Key pair assigned at launch
my-ssh-key

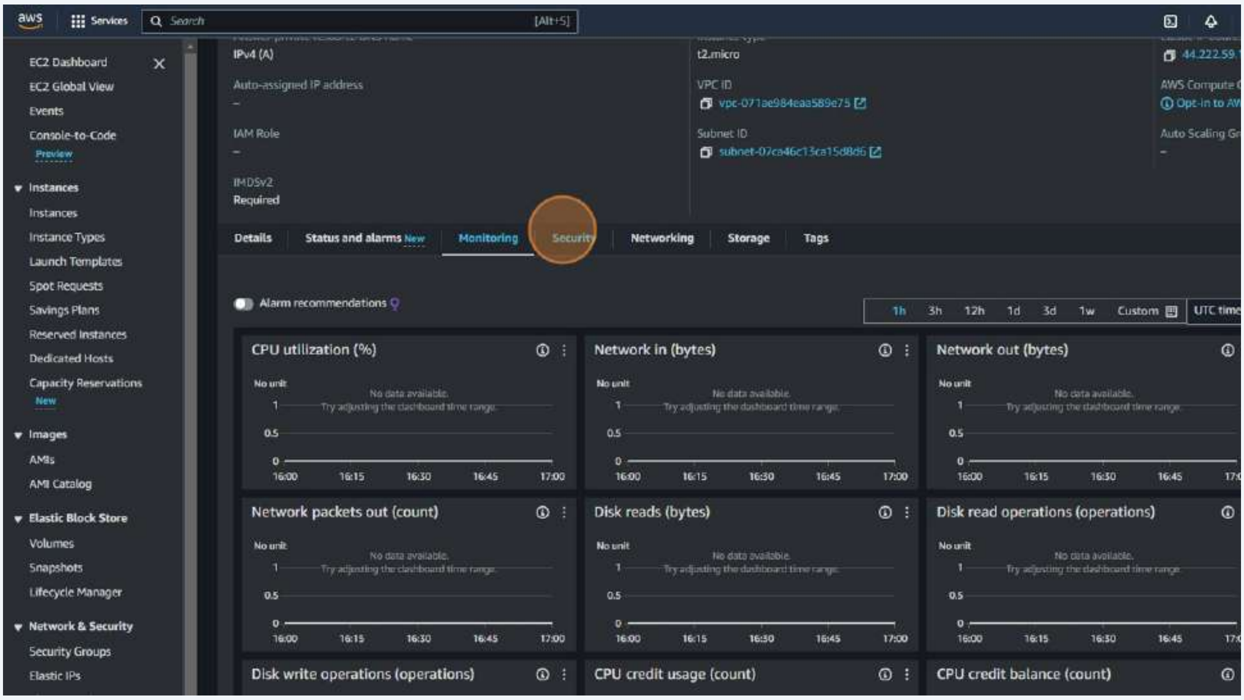
State transition
–

Credit specification
standard

Kernel ID
–

State transition
–

**126** Click "Security"



IPv4 (A)

t2.micro

44.222.59.1

Auto-assigned IP address
–

VPC ID
vpc-071ae984eaa589e75

AWS Compute
Opt-in to AW

IAM Role
–

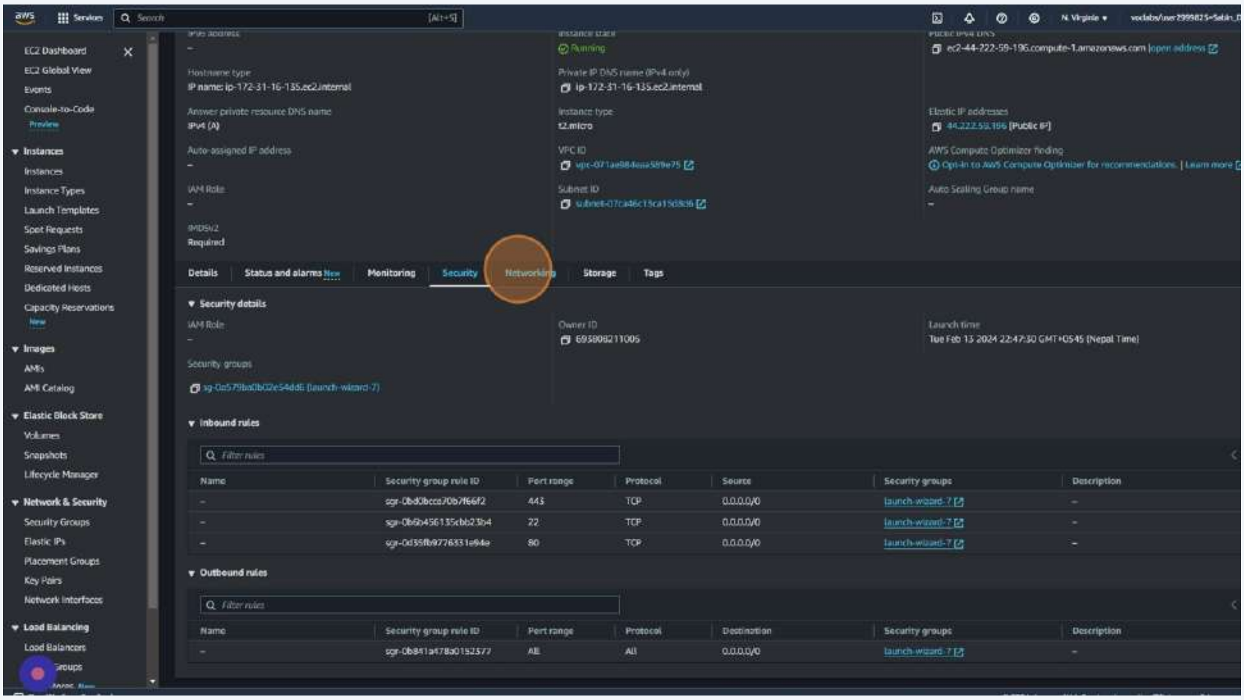
Subnet ID
subnet-07ca46c13ca15d8d6

Auto Scaling Gr
–

IMDSv2
Required

CPU utilization (%)
Network in (bytes)
Network out (bytes)
Network packets out (count)
Disk reads (bytes)
Disk read operations (operations)
Disk write operations (operations)
CPU credit usage (count)
CPU credit balance (count)
No unit
No data available.
Try adjusting the dashboard time range.
1
0.5
0
16:00
16:15
16:30
16:45
17:00

127 Click "Networking"



Instance state
Running

Public IPv4 DNS
ec2-44-222-59-196.compute-1.amazonaws.com |open address

Hostname type
IP name: ip-172-31-16-135.ec2.internal

Private IP DNS name (IPv4 only)
ip-172-31-16-135.ec2.internal

Answer private resource DNS name
IPv4 (A)

Instance type
t2.micro

Elastic IP addresses
44.222.59.196 [Public IP]

Auto-assigned IP address
–

VPC ID
vpc-071ae984eaa589e75

AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. | Learn more

IAM Role
–

Subnet ID
subnet-07ca46c15ca15d8d6

Auto Scaling Group name
–

IMDSv2
Required

▾ Security details

IAM Role
–

Owner ID
693808211005

Launch time
Tue Feb 13 2024 22:47:30 GMT+0545 (Nepal Time)

Security groups
sg-0a579ba0b02e54dd6 (launch-wizard-7)

▾ Inbound rules

Filter rules

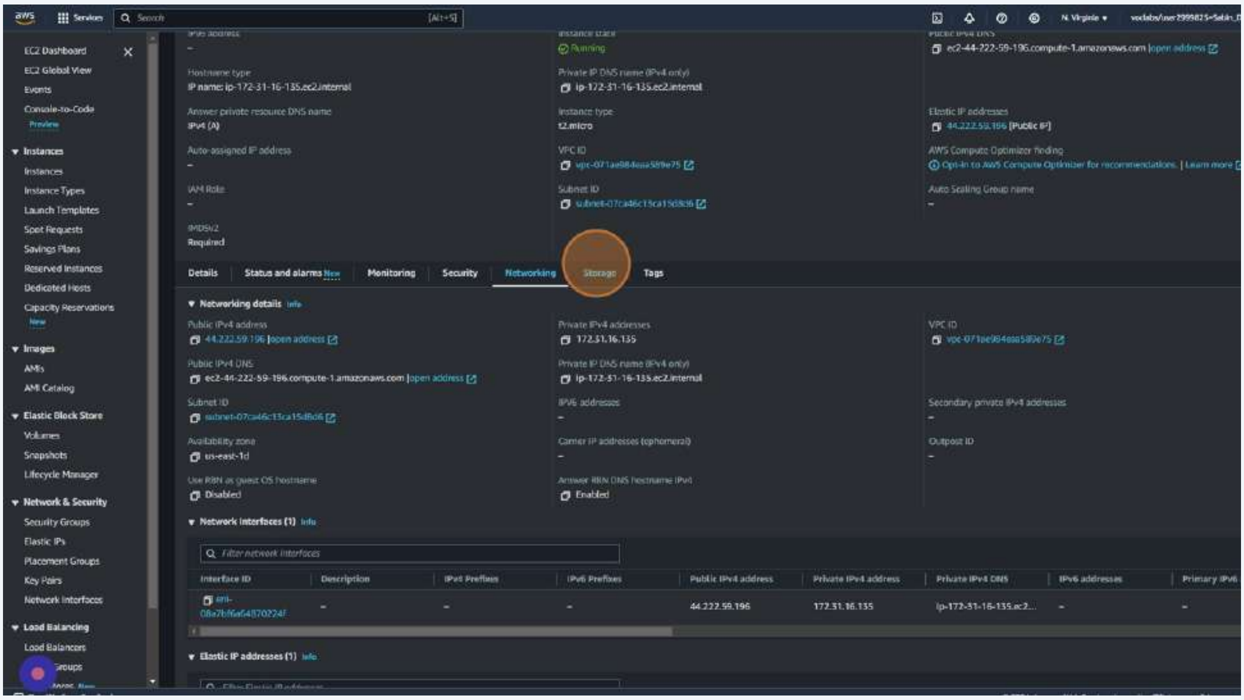
| Name | Security group rule ID | Port range | Protocol | Source | Security groups | Description |
|---|---|---|---|---|---|---|
| – | sgr-0bd0bcca70b7f66f2 | 443 | TCP | 0.0.0.0/0 | launch-wizard-7 | – |
| – | sgr-0b6b456135cbb23b4 | 22 | TCP | 0.0.0.0/0 | launch-wizard-7 | – |
| – | sgr-0d35fb9776331e94e | 80 | TCP | 0.0.0.0/0 | launch-wizard-7 | – |

▾ Outbound rules

Filter rules

| Name | Security group rule ID | Port range | Protocol | Destination | Security groups | Description |
|---|---|---|---|---|---|---|
| – | sgr-0b841a478a0152377 | All | All | 0.0.0.0/0 | launch-wizard-7 | – |

128 Click "Storage"



Instance state
Running

Public IPv4 DNS
ec2-44-222-59-196.compute-1.amazonaws.com |open address

Hostname type
IP name: ip-172-31-16-135.ec2.internal

Private IP DNS name (IPv4 only)
ip-172-31-16-135.ec2.internal

Answer private resource DNS name
IPv4 (A)

Instance type
t2.micro

Elastic IP addresses
44.222.59.196 [Public IP]

Auto-assigned IP address
–

VPC ID
vpc-071ae984eaa589e75

AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. | Learn more

IAM Role
–

Subnet ID
subnet-07ca46c15ca15d8d6

Auto Scaling Group name
–

IMDSv2
Required

▾ Networking details Info

Public IPv4 address
44.222.59.196 |open address

Private IPv4 addresses
172.31.16.135

VPC ID
vpc-071ae984eaa589e75

Public IPv4 DNS
ec2-44-222-59-196.compute-1.amazonaws.com |open address

Private IP DNS name (IPv4 only)
ip-172-31-16-135.ec2.internal

Subnet ID
subnet-07ca46c13ca15d8d6

IPV6 addresses
–

Secondary private IPv4 addresses
–

Availability zone
us-east-1d

Carrier IP addresses (ephemeral)
–

Outpost ID
–

Use RBN as guest OS hostname
Disabled

Answer RBN DNS hostname IPv4
Enabled

▾ Network interfaces (1) Info

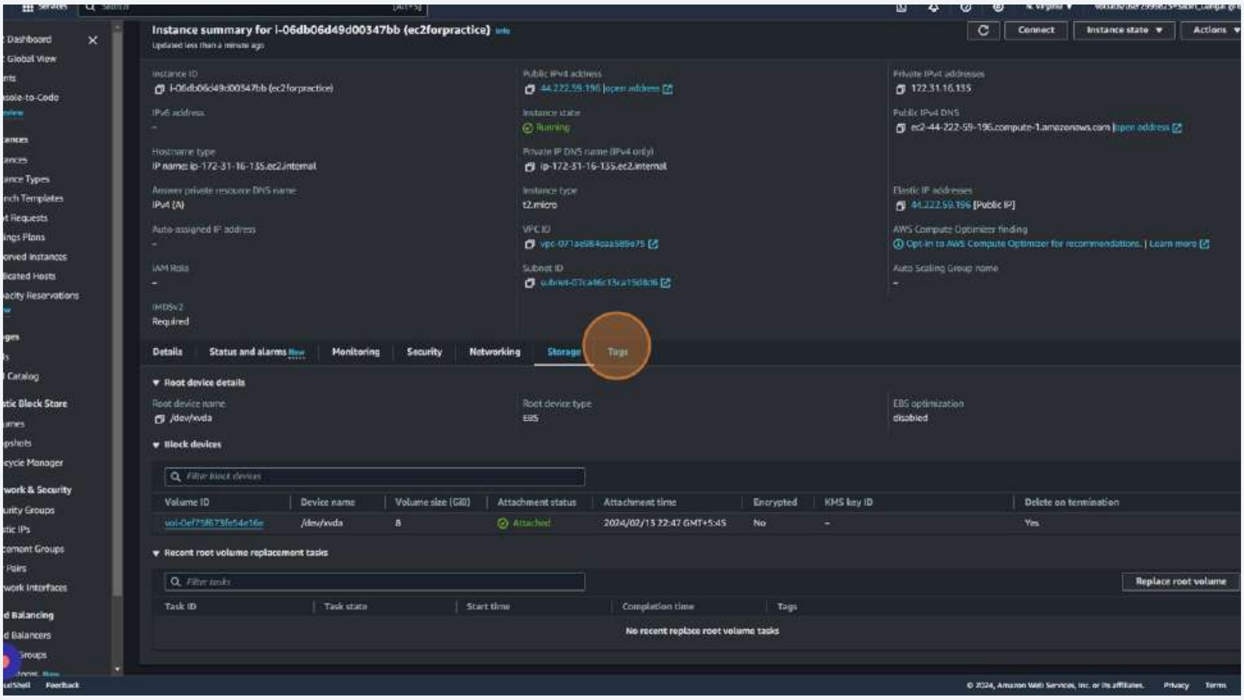
Filter network interfaces

| Interface ID | Description | IPv4 Prefixes | IPv6 Prefixes | Public IPv4 address | Private IPv4 address | Private IPv4 DNS | IPv6 addresses | Primary IPv6 |
|---|---|---|---|---|---|---|---|---|
| eni-08a7bf6a54870224f | – | – | – | 44.222.59.196 | 172.31.16.135 | ip-172-31-16-135.ec2... | – | – |

▾ Elastic IP addresses (1) Info

Filter Elastic IP addresses

129 Click "Tags"



Instance summary for i-06db06d49d00347bb (ec2forpractice)

Updated less than a minute ago

Instance ID: i-06db06d49d00347bb (ec2forpractice)

IPv6 address: –

Hostname type: IP name: ip-172-31-16-135.ec2.internal

Answer private resource DNS name: IPv4 (A)

Auto-assigned IP address: –

IAM Role: –

IMDSv2: Required

Public IPv4 address: 44.222.59.196 | open address

Instance state: Running

Private IP DNS name (IPv4 only): ip-172-31-16-135.ec2.internal

Instance type: t2.micro

VPC ID: vpc-071ae984eaa589e75

Subnet ID: subnet-07ca46c13ca15d8d6

Private IPv4 addresses: 172.31.16.135

Public IPv4 DNS: ec2-44-222-59-196.compute-1.amazonaws.com | open address

Elastic IP addresses: 44.222.59.196 [Public IP]

AWS Compute Optimizer finding: Opt-in to AWS Compute Optimizer for recommendations. | Learn more

Auto Scaling Group name: –

Root device details

Root device name: /dev/xvda

Root device type: EBS

EBS optimization: disabled

Block devices

| Volume ID | Device name | Volume size (GiB) | Attachment status | Attachment time | Encrypted | KMS key ID | Delete on termination |
|---|---|---|---|---|---|---|---|
| vol-0ef75f673fe54e16e | /dev/xvda | 8 | Attached | 2024/02/13 22:47 GMT+5:45 | No | – | Yes |

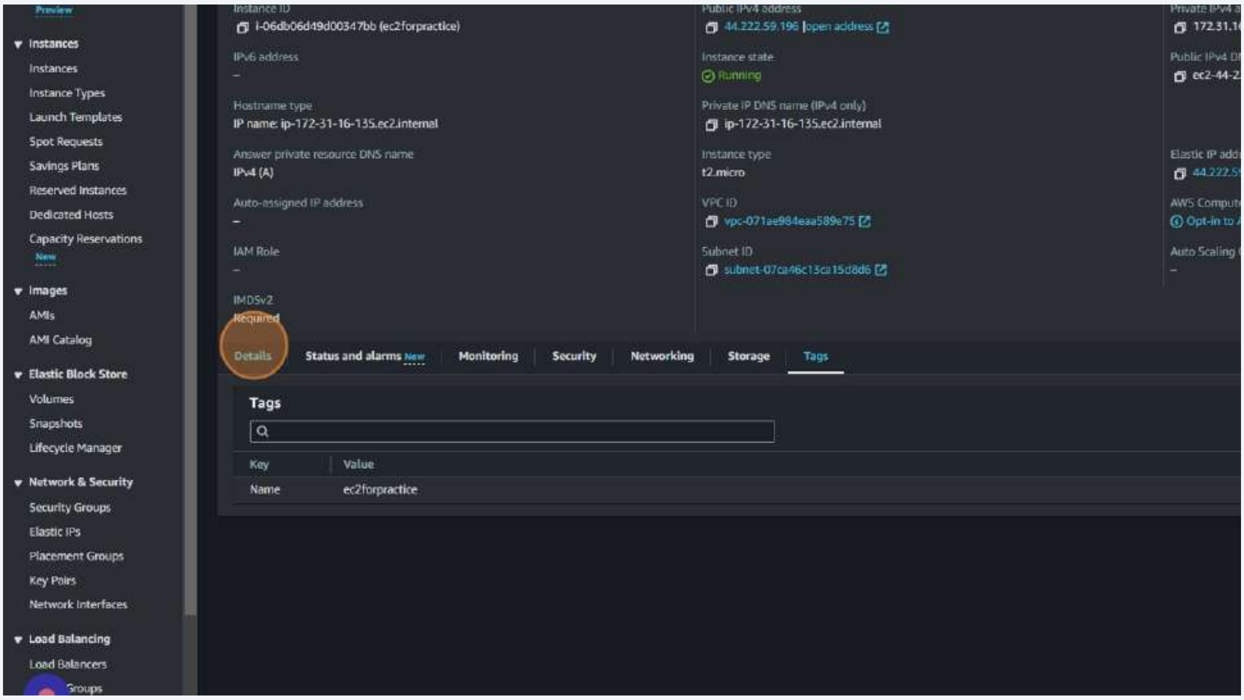
Recent root volume replacement tasks

| Task ID | Task state | Start time | Completion time | Tags |
|---|---|---|---|---|

No recent replace root volume tasks

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

130 Click "Details"



Instance ID: i-06db06d49d00347bb (ec2forpractice)

IPv6 address: –

Hostname type: IP name: ip-172-31-16-135.ec2.internal

Answer private resource DNS name: IPv4 (A)

Auto-assigned IP address: –

IAM Role: –

IMDSv2: Required

Public IPv4 address: 44.222.59.196 | open address

Instance state: Running

Private IP DNS name (IPv4 only): ip-172-31-16-135.ec2.internal

Instance type: t2.micro

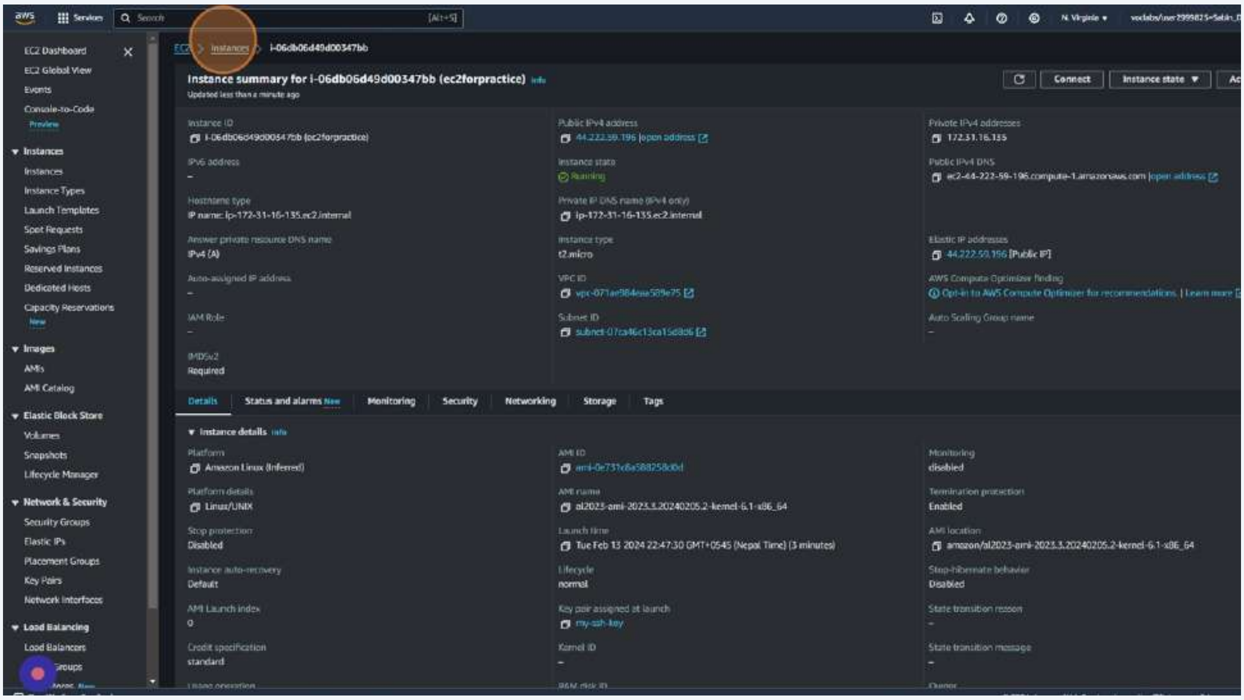
VPC ID: vpc-071ae984eaa589e75

Subnet ID: subnet-07ca46c13ca15d8d6

Tags

| Key | Value |
|---|---|
| Name | ec2forpractice |

131 Click "Instances"



Instance summary for i-06db06d49d00347bb (ec2forpractice) Info
Updated less than a minute ago

Instance ID
i-06db06d49d00347bb (ec2forpractice)

IPv6 address
–

Hostname type
IP name: ip-172-31-16-135.ec2.internal

Answer private resource DNS name
IPv4 (A)

Auto-assigned IP address
–

IAM Role
–

IMDSv2
Required

Public IPv4 address
44.222.59.196 | open address

Instance state
Running

Private IP DNS name (IPv4 only)
ip-172-31-16-135.ec2.internal

Instance type
t2.micro

VPC ID
vpc-071ae984eae589e75

Subnet ID
subnet-07ca46c13ca15d8d6

Private IPv4 addresses
172.31.16.135

Public IPv4 DNS
ec2-44-222-59-196.compute-1.amazonaws.com | open address

Elastic IP addresses
44.222.59.196 [Public IP]

AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. | Learn more

Auto Scaling Group name
–

▾ Instance details Info

Platform
Amazon Linux (Inferred)

Platform details
Linux/UNIX

Stop protection
Disabled

Instance auto-recovery
Default

AMI Launch index
0

Credit specification
standard

AMI ID
ami-0e731c8a588258d0d

AMI name
al2023-ami-2023.3.20240205.2-kernel-6.1-x86_64

Launch time
Tue Feb 13 2024 22:47:30 GMT+0545 (Nepal Time) (3 minutes)

Lifecycle
normal

Key pair assigned at launch
my-ssh-key

Kernel ID
–

Monitoring
disabled

Termination protection
Enabled

AMI location
amazon/al2023-ami-2023.3.20240205.2-kernel-6.1-x86_64

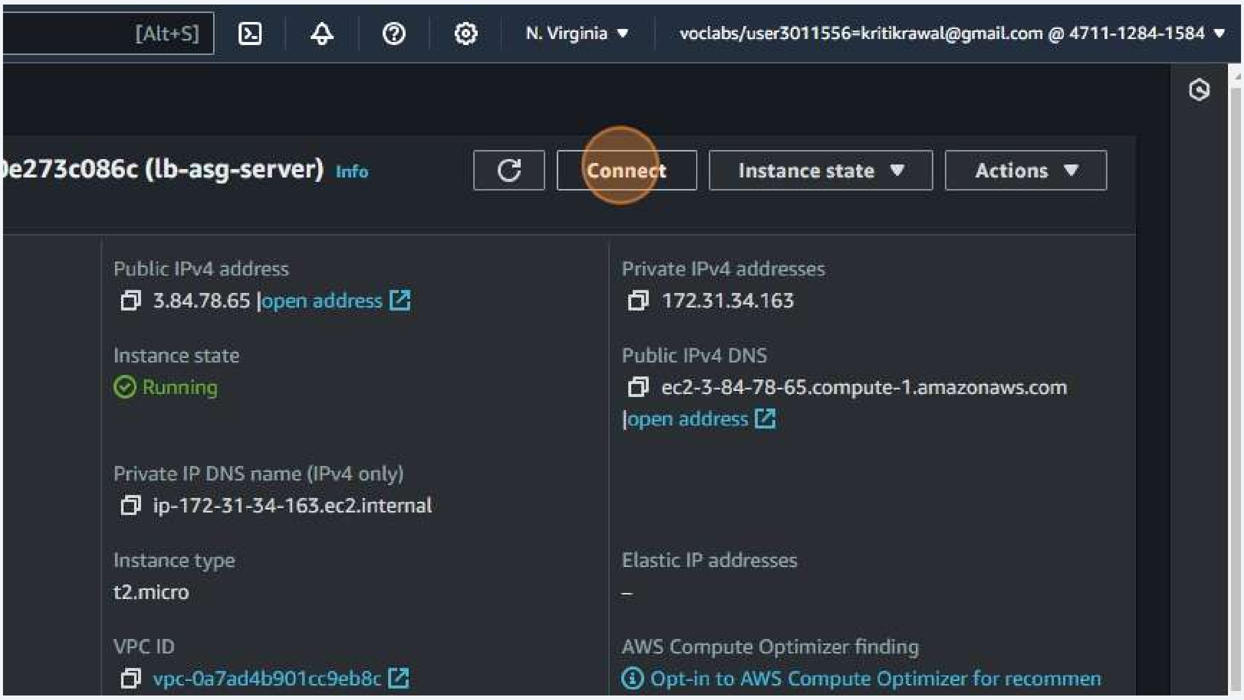
Stop-hibernate behavior
Disabled

State transition reason
–

State transition message
–

132 Navigate to [https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#InstanceDetails:instanceId=i-08cce630e273c086c](https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#InstanceDetails:instanceId=i-08cce630e273c086c)

133 Click "Connect"


[Alt+S]
N. Virginia
voclabs/user3011556=kritikrawal@gmail.com @ 4711-1284-1584
)e273c086c (lb-asg-server) Info
Connect
Instance state
Actions

Public IPv4 address
3.84.78.65 |open address

Private IPv4 addresses
172.31.34.163

Instance state
Running

Public IPv4 DNS
ec2-3-84-78-65.compute-1.amazonaws.com
|open address

Private IP DNS name (IPv4 only)
ip-172-31-34-163.ec2.internal

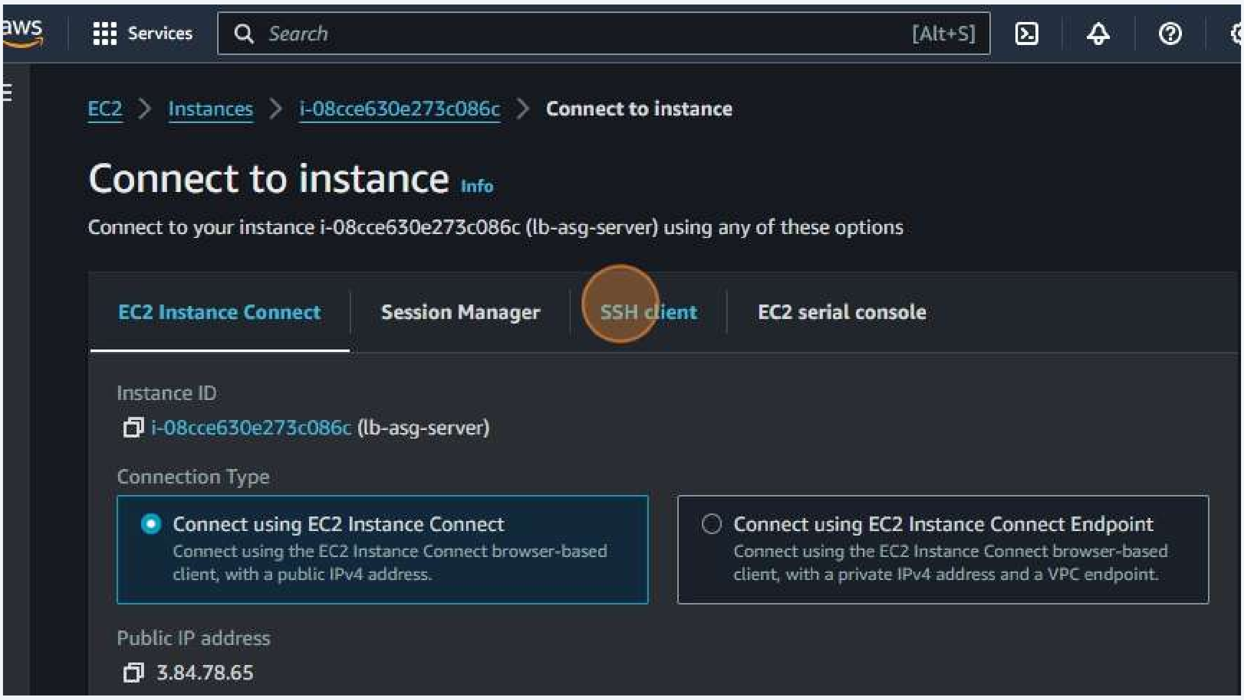
Instance type
t2.micro

Elastic IP addresses
–

VPC ID
vpc-0a7ad4b901cc9eb8c

AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommen

134 Click "SSH client"



Connect to instance Info

Connect to your instance i-08cce630e273c086c (lb-asg-server) using any of these options

Instance ID
i-08cce630e273c086c (lb-asg-server)

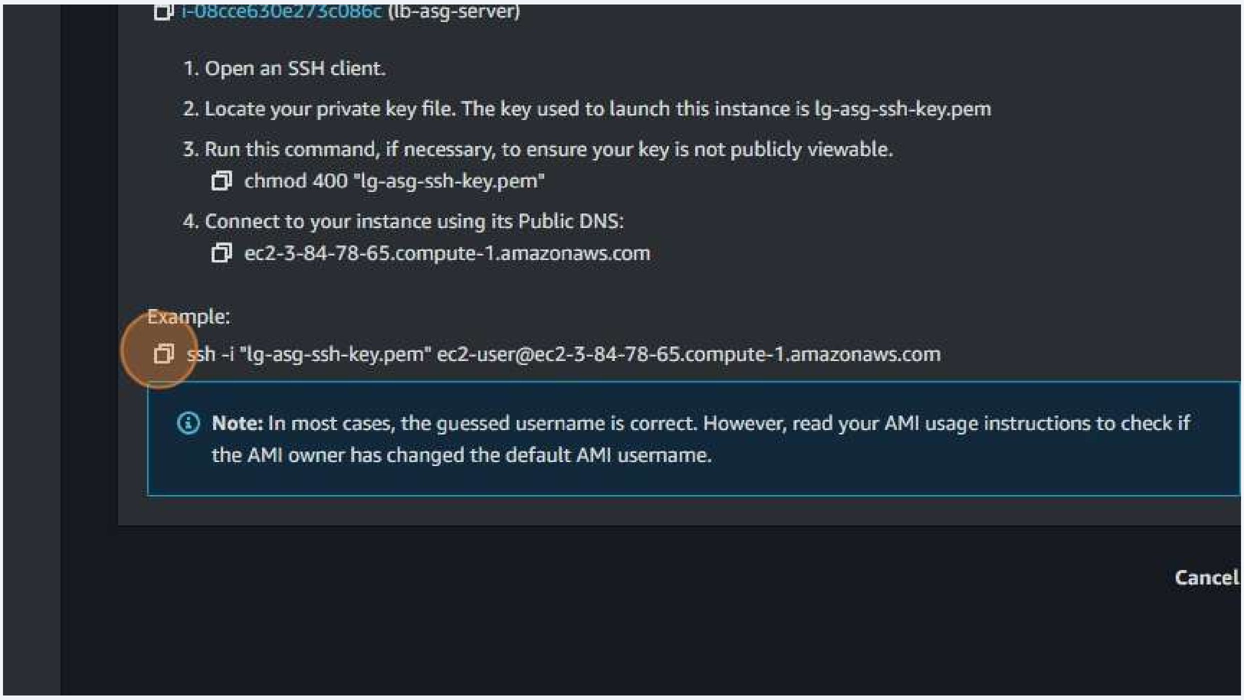
Connection Type

● Connect using EC2 Instance Connect
Connect using the EC2 Instance Connect browser-based client, with a public IPv4 address.

○ Connect using EC2 Instance Connect Endpoint
Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.

Public IP address
3.84.78.65

135 Click here.



i-08cce630e273c086c (lb-asg-server)

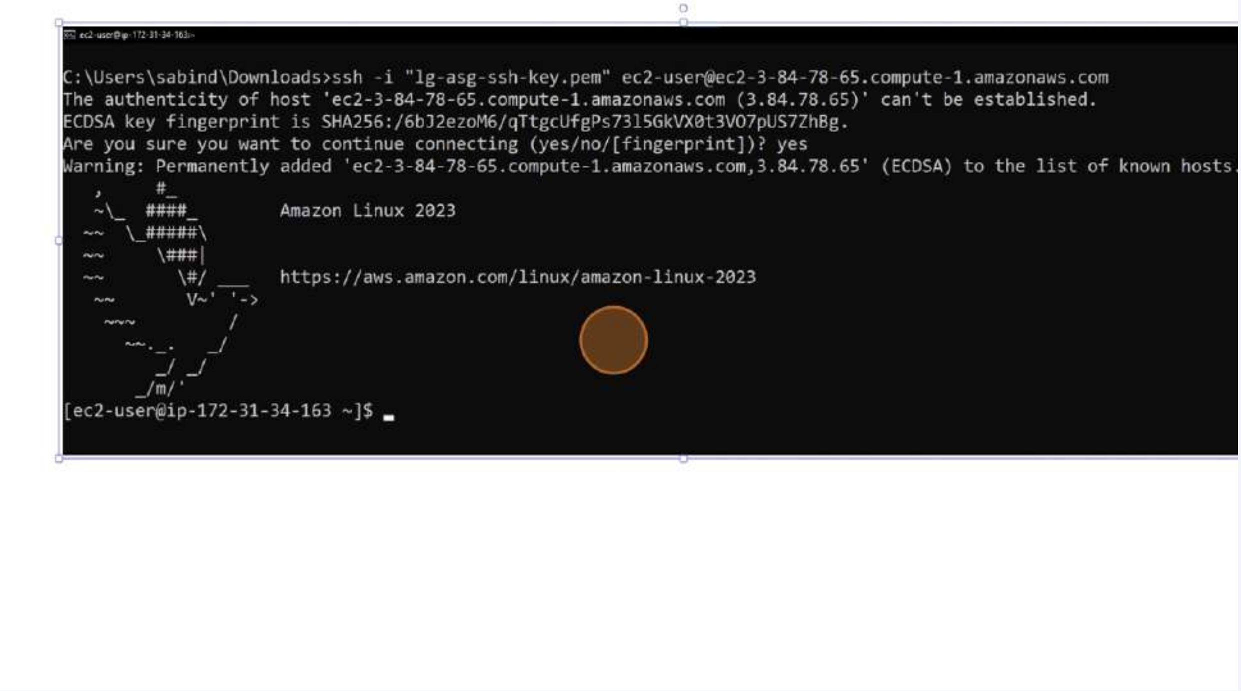
1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is lg-asg-ssh-key.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
   ```
   chmod 400 "lg-asg-ssh-key.pem"
   ```
4. Connect to your instance using its Public DNS:
   ```
   ec2-3-84-78-65.compute-1.amazonaws.com
   ```

Example:

```
ssh -i "lg-asg-ssh-key.pem" ec2-user@ec2-3-84-78-65.compute-1.amazonaws.com
```

**Note:** In most cases, the guessed username is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

136 Click "Drawing canvas"

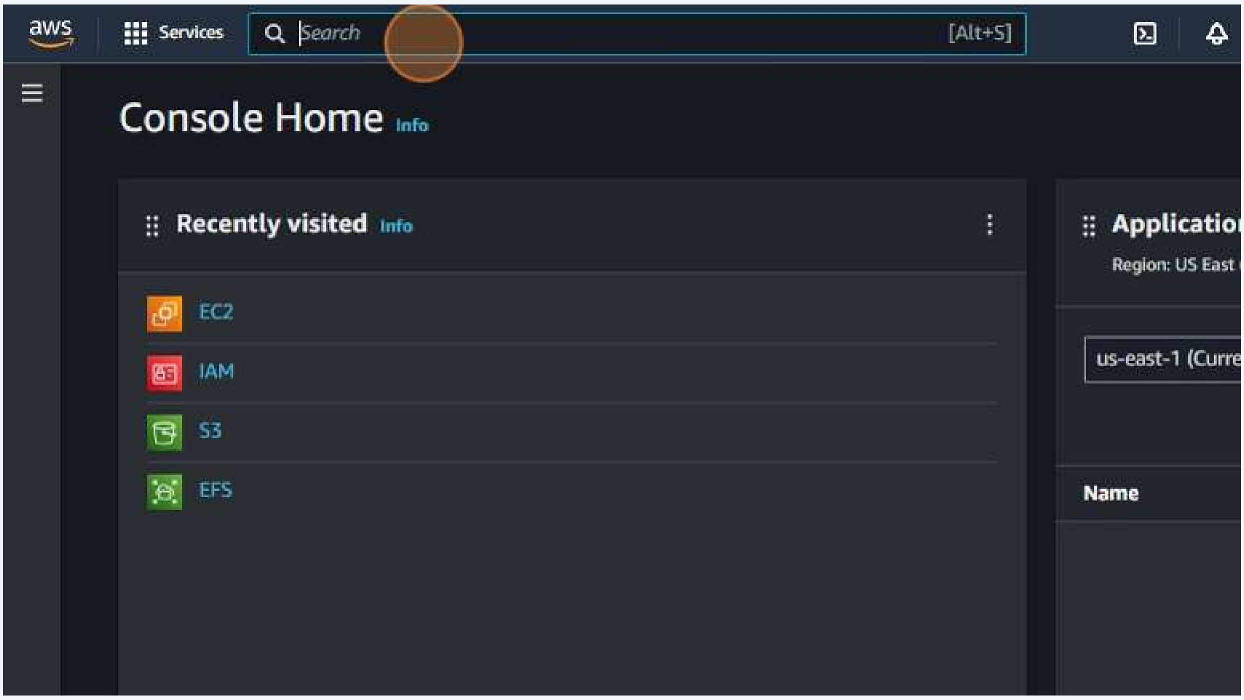


```
C:\Users\sabind\Downloads>ssh -i "lg-asg-ssh-key.pem" ec2-user@ec2-3-84-78-65.compute-1.amazonaws.com
The authenticity of host 'ec2-3-84-78-65.compute-1.amazonaws.com (3.84.78.65)' can't be established.
ECDSA key fingerprint is SHA256:/6bJ2ezoM6/qTtgcUfgPs7315GkVX0t3VO7pUS7ZhBg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-3-84-78-65.compute-1.amazonaws.com,3.84.78.65' (ECDSA) to the list of known hosts.
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-172-31-34-163 ~]$ 
```

## VPC

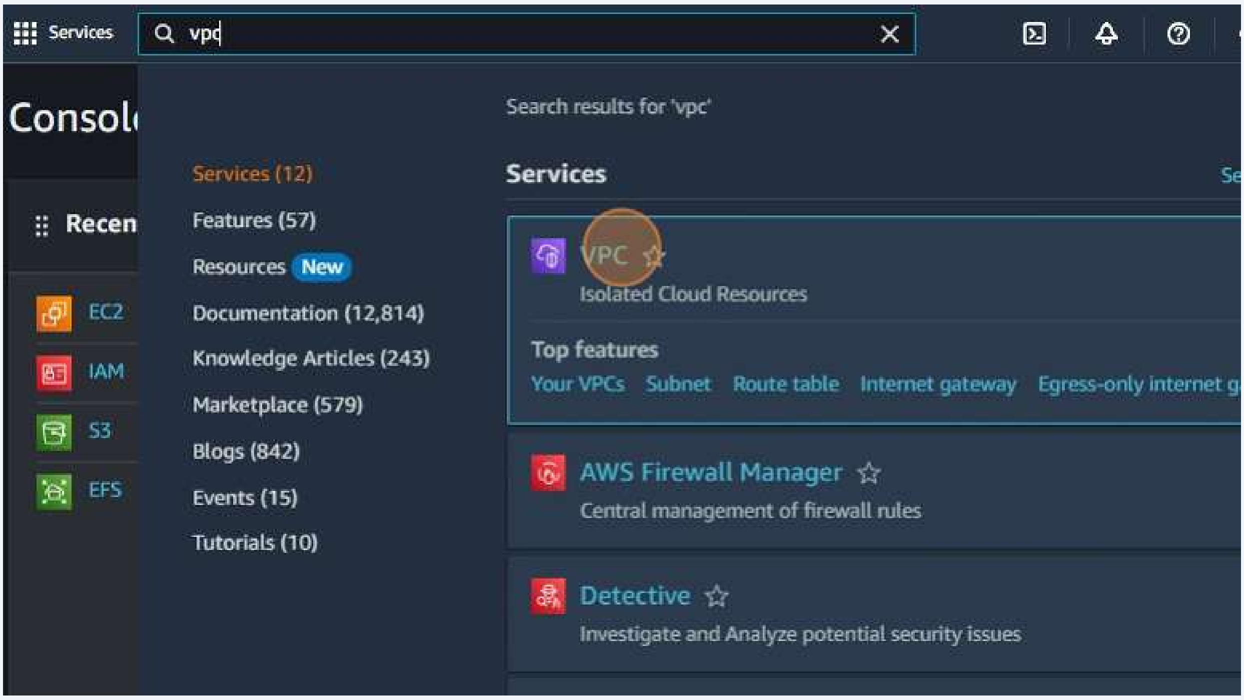
137 Navigate to https://us-east-1.console.aws.amazon.com/console/home?region=us-east-1#

138 Click the "Search" field.

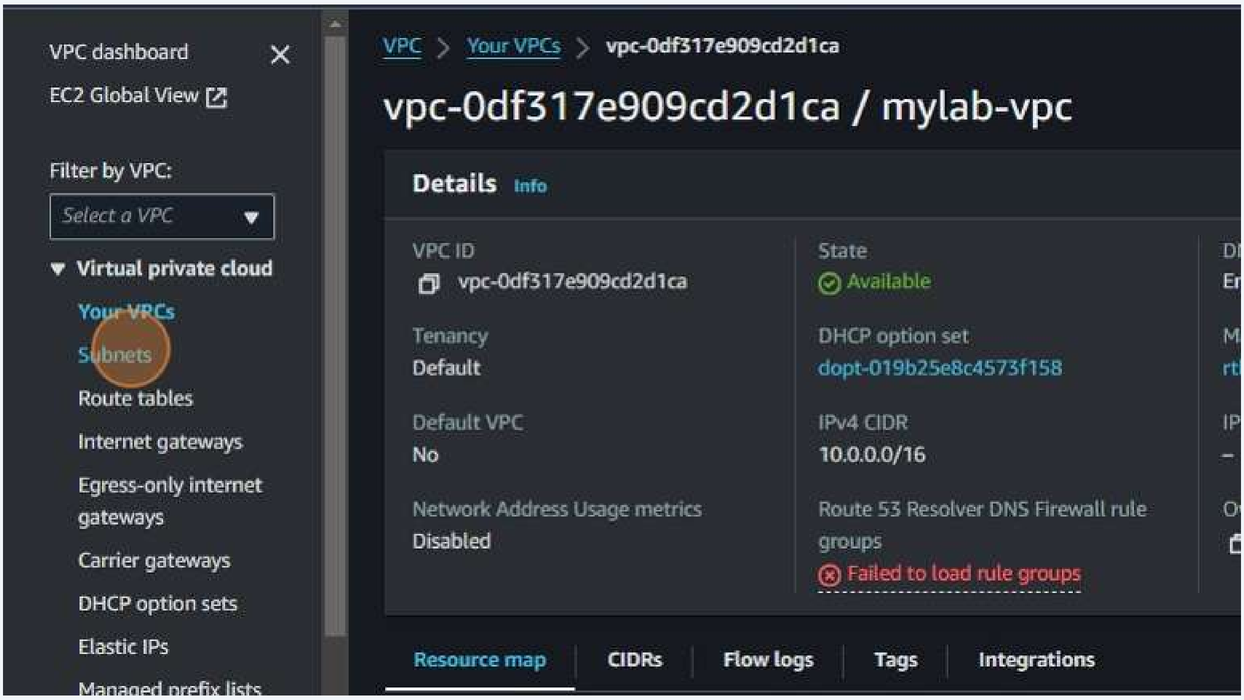


139 Type "vpc"

**140** Click "VPC"



**141** Click "Subnets"



vpc-0df317e909cd2d1ca / mylab-vpc

Details Info

VPC ID
vpc-0df317e909cd2d1ca

State
Available

Tenancy
Default

DHCP option set
dopt-019b25e8c4573f158

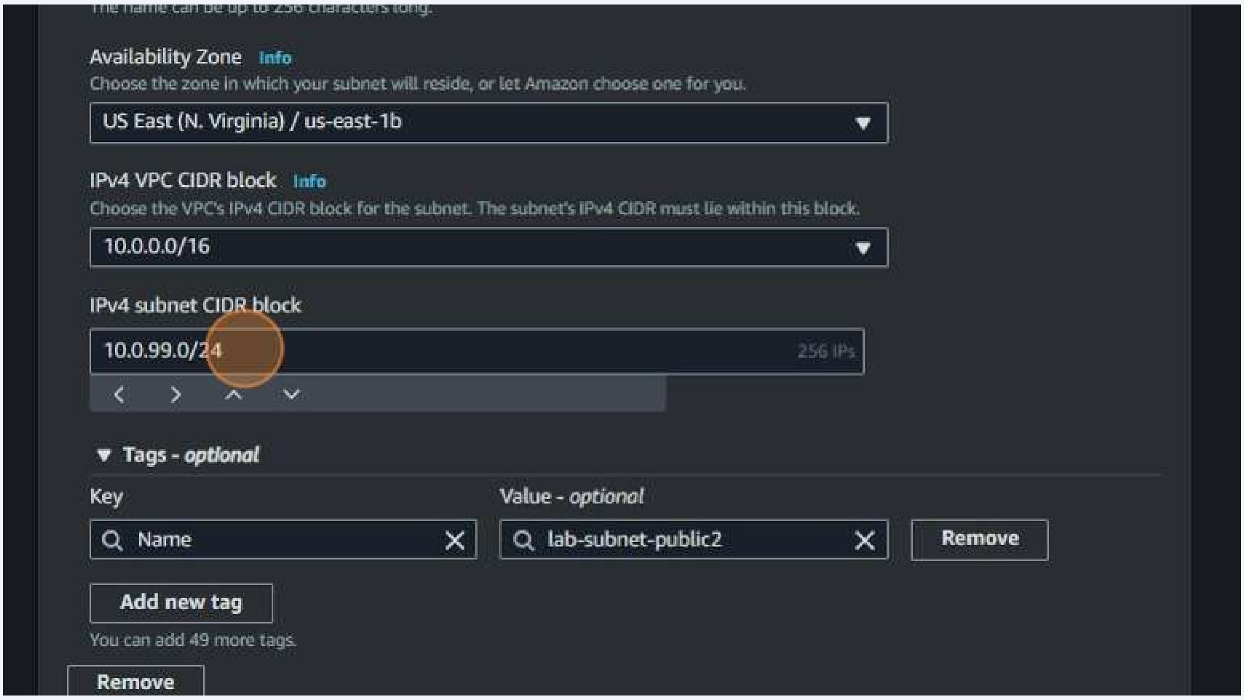
Default VPC
No

IPv4 CIDR
10.0.0.0/16

Network Address Usage metrics
Disabled

Route 53 Resolver DNS Firewall rule groups
Failed to load rule groups

**142** Click the "10.0.0.0/20" field.



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

IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/16

IPv4 subnet CIDR block
10.0.99.0/24 256 IPs

▼ Tags - *optional*

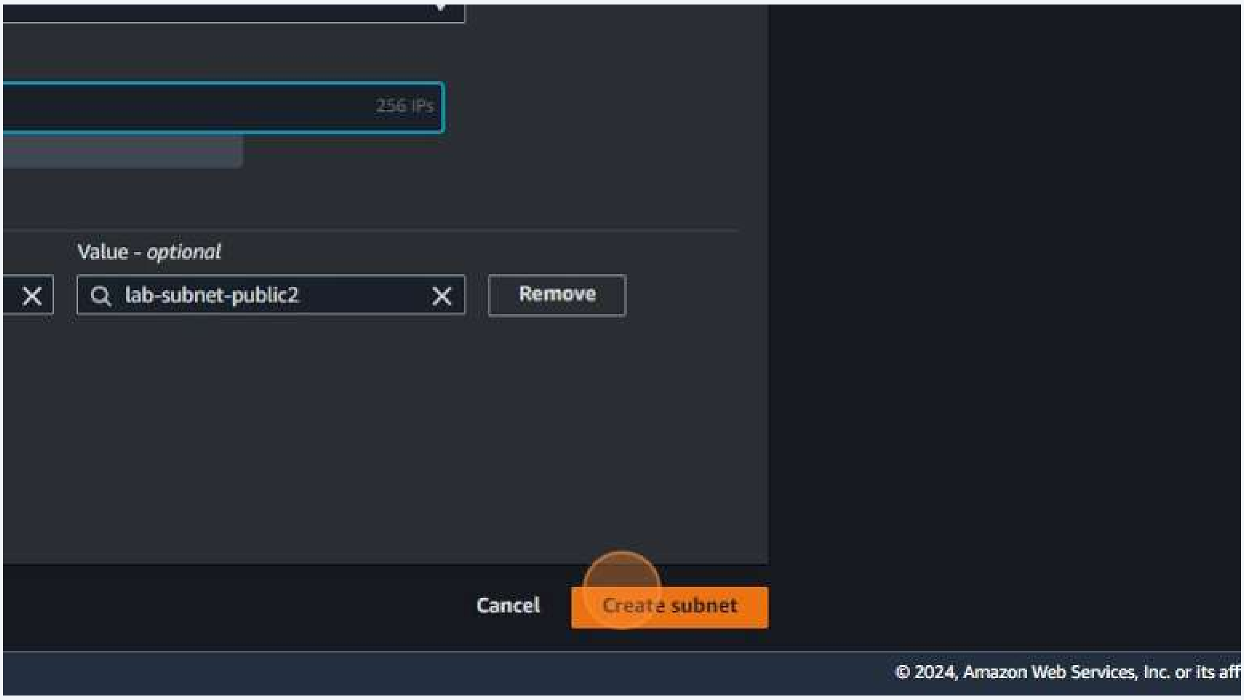
| Key | Value - *optional* | |
|---|---|---|
| Name | lab-subnet-public2 | Remove |

Add new tag

You can add 49 more tags.

Remove

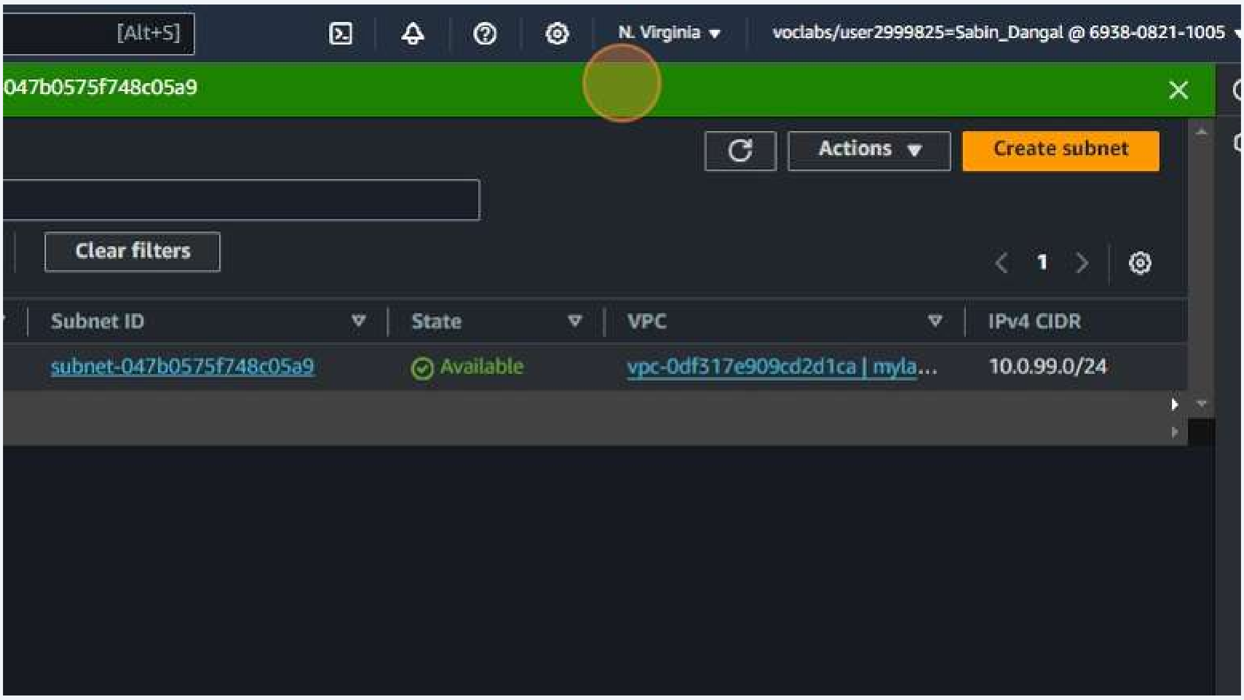
**143** Click "Create subnet"



256 IPs

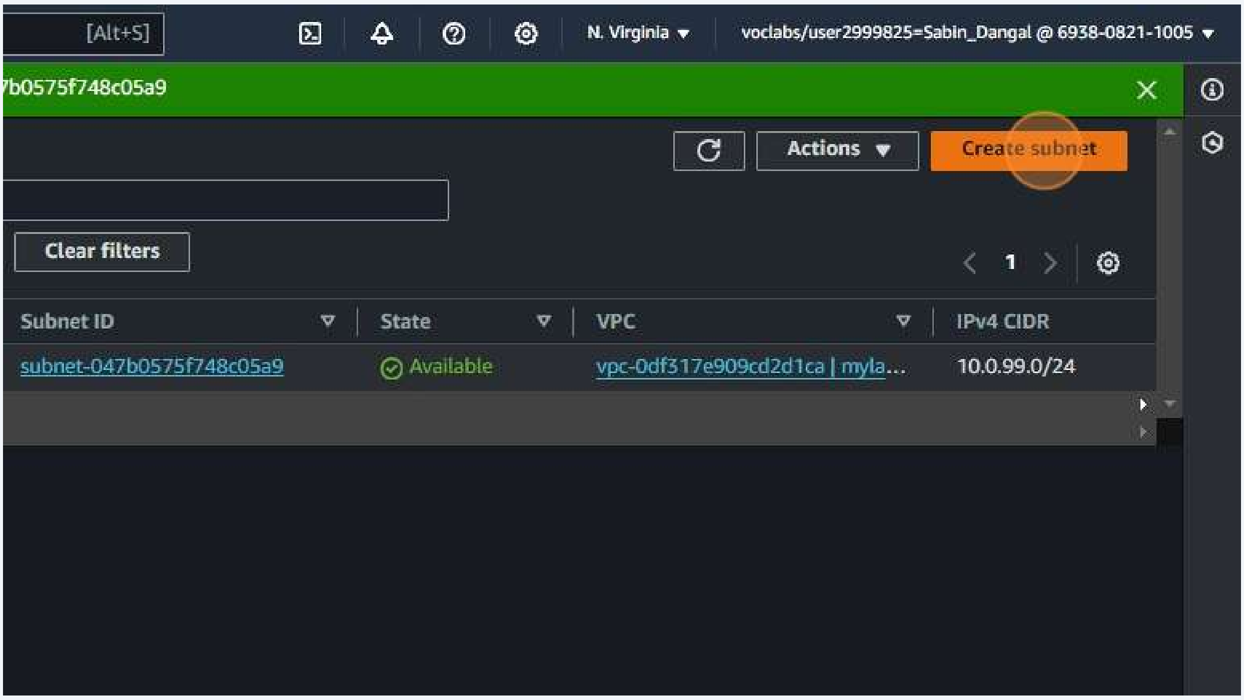
| Value - *optional* | |
|---|---|
| lab-subnet-public2 | Remove |

144 Click "You have successfully created 1 subnet: subnet-047b0575f748c05a9"



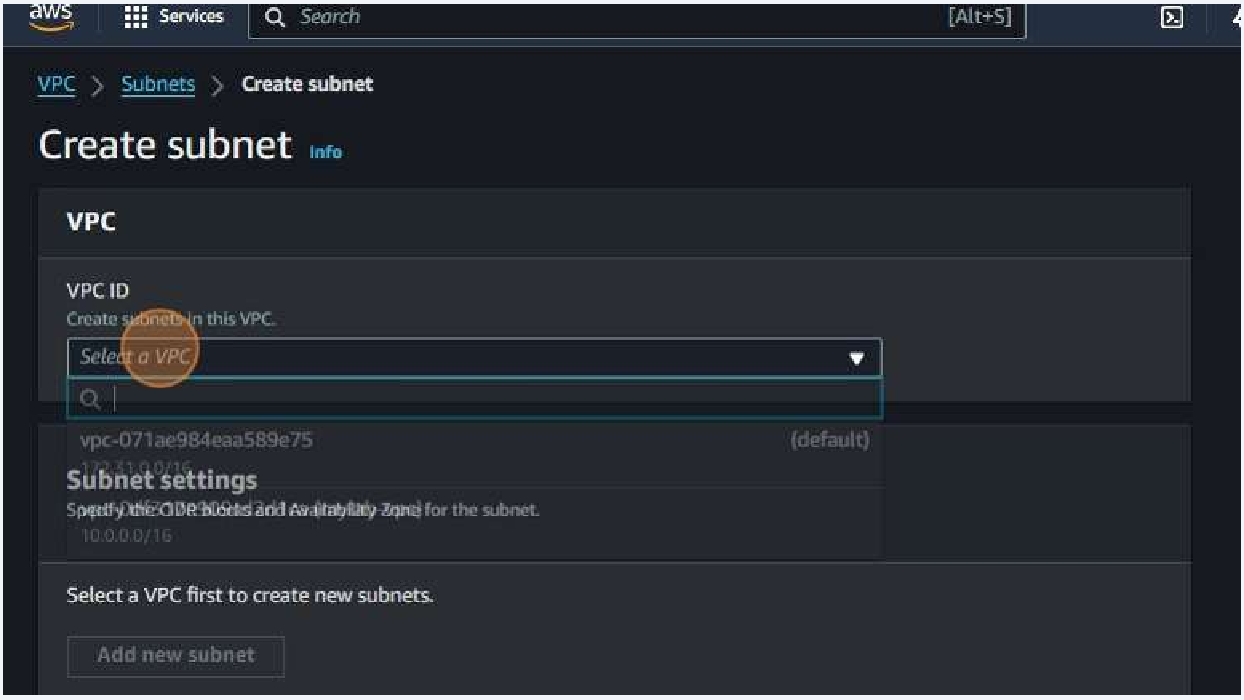
| Subnet ID | State | VPC | IPv4 CIDR |
|---|---|---|---|
| subnet-047b0575f748c05a9 | Available | vpc-0df317e909cd2d1ca \| myla... | 10.0.99.0/24 |

145 Click "Create subnet"



| Subnet ID | State | VPC | IPv4 CIDR |
|---|---|---|---|
| subnet-047b0575f748c05a9 | Available | vpc-0df317e909cd2d1ca \| myla... | 10.0.99.0/24 |

146 Click "Select a VPC"



VPC > Subnets > Create subnet

Create subnet Info

VPC

VPC ID

Create subnets in this VPC.

Select a VPC

vpc-071ae984eaa589e75 (default)

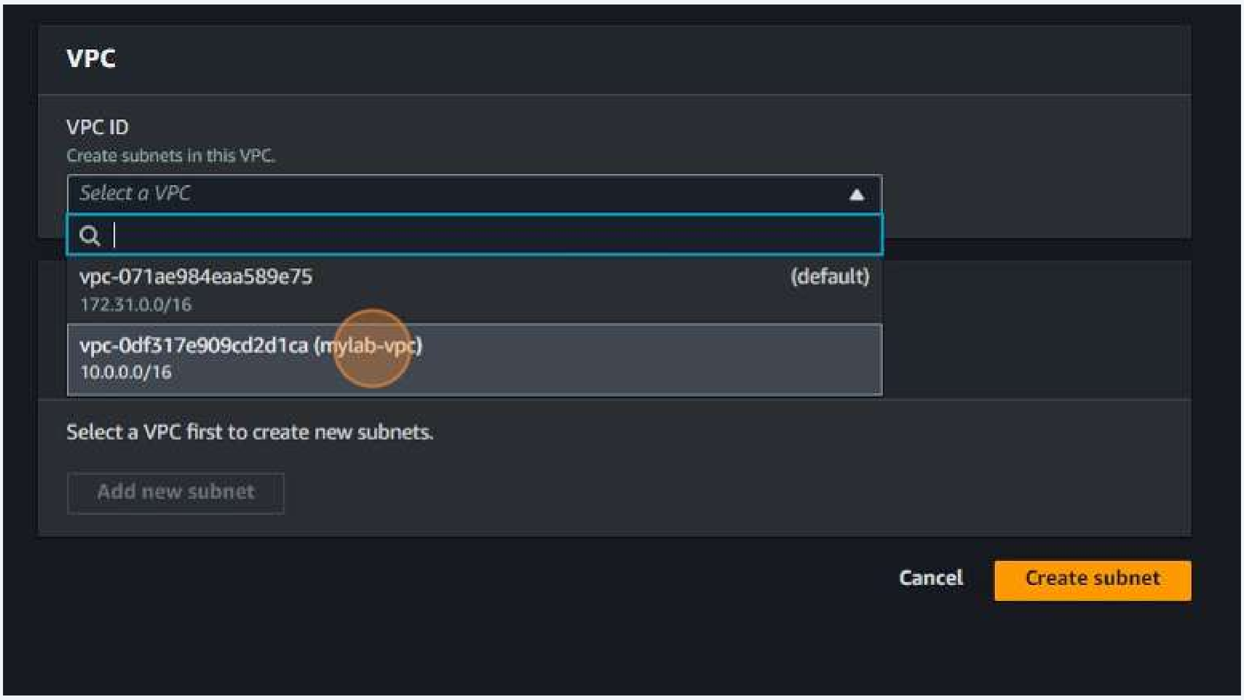
Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Select a VPC first to create new subnets.

Add new subnet

147 Click "vpc-0df317e909cd2d1ca (mylab-vpc)"



VPC

VPC ID

Create subnets in this VPC.

Select a VPC

vpc-071ae984eaa589e75 (default)
172.31.0.0/16

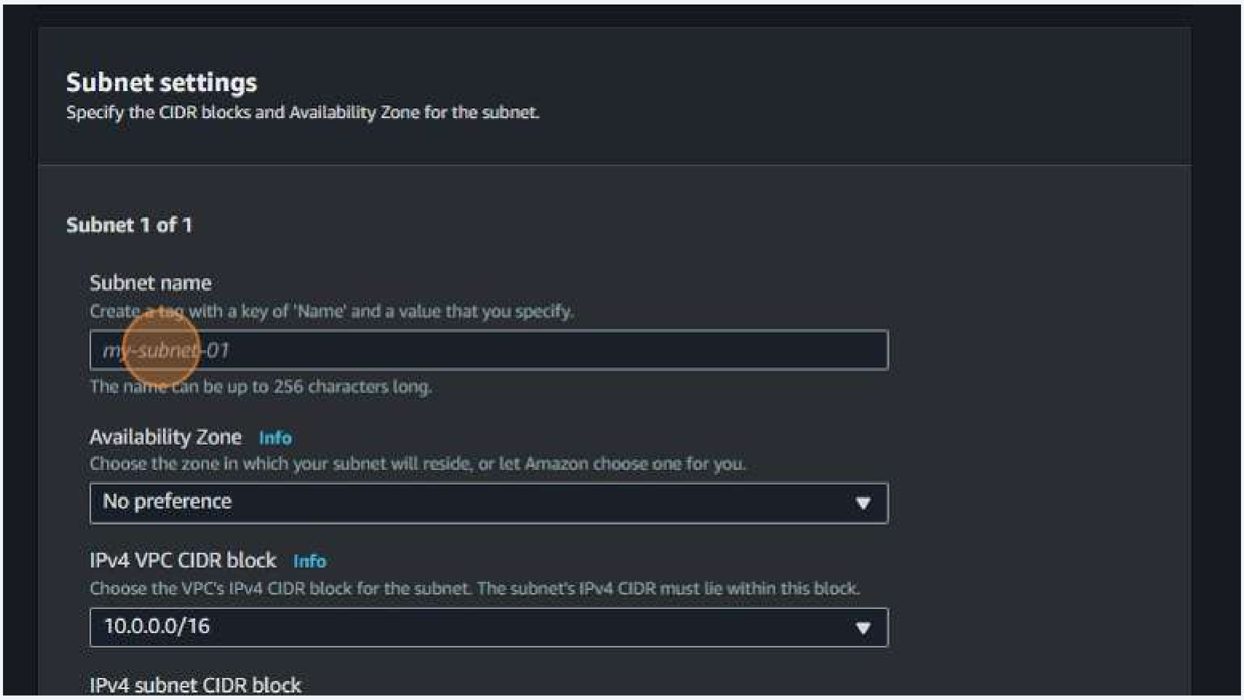
vpc-0df317e909cd2d1ca (mylab-vpc)
10.0.0.0/16

Select a VPC first to create new subnets.

Add new subnet

Cancel Create subnet

148 Click the "Subnet name" field.



**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

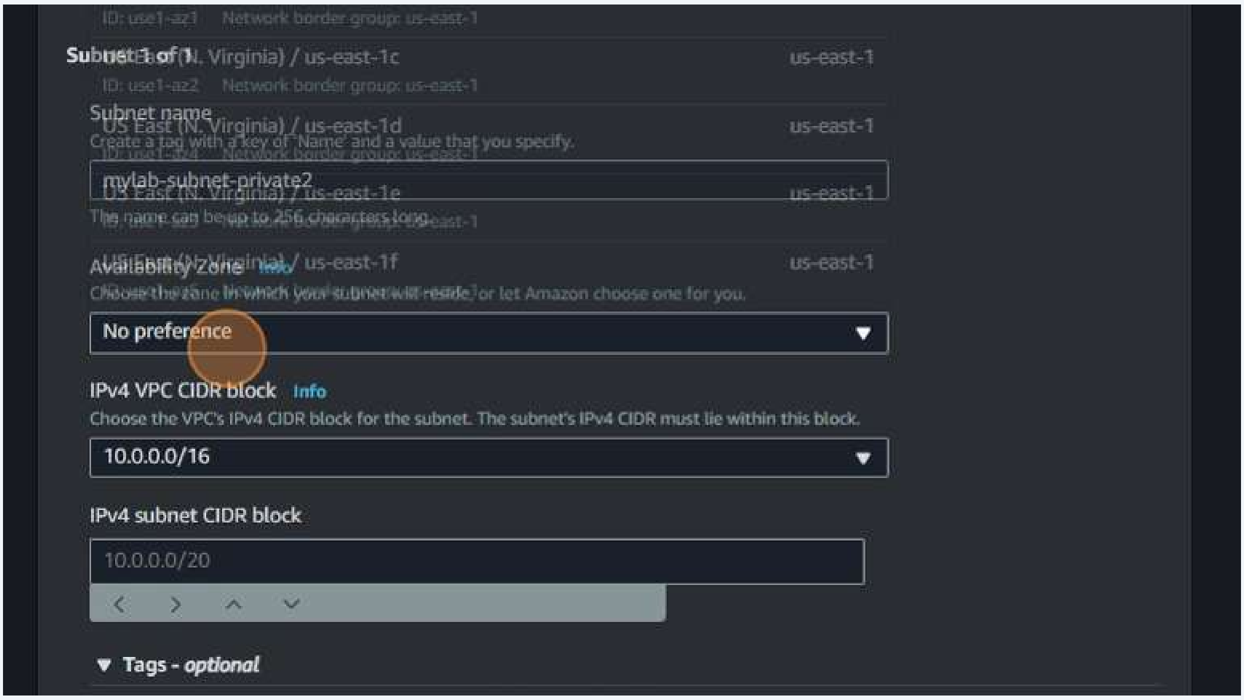
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

10.0.0.0/16 ▼

IPv4 subnet CIDR block

149 Type "mylab-subnet-private2"

**150** Click "No preference"



Subnet 1 of 1

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

mylab-subnet-private2

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 VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

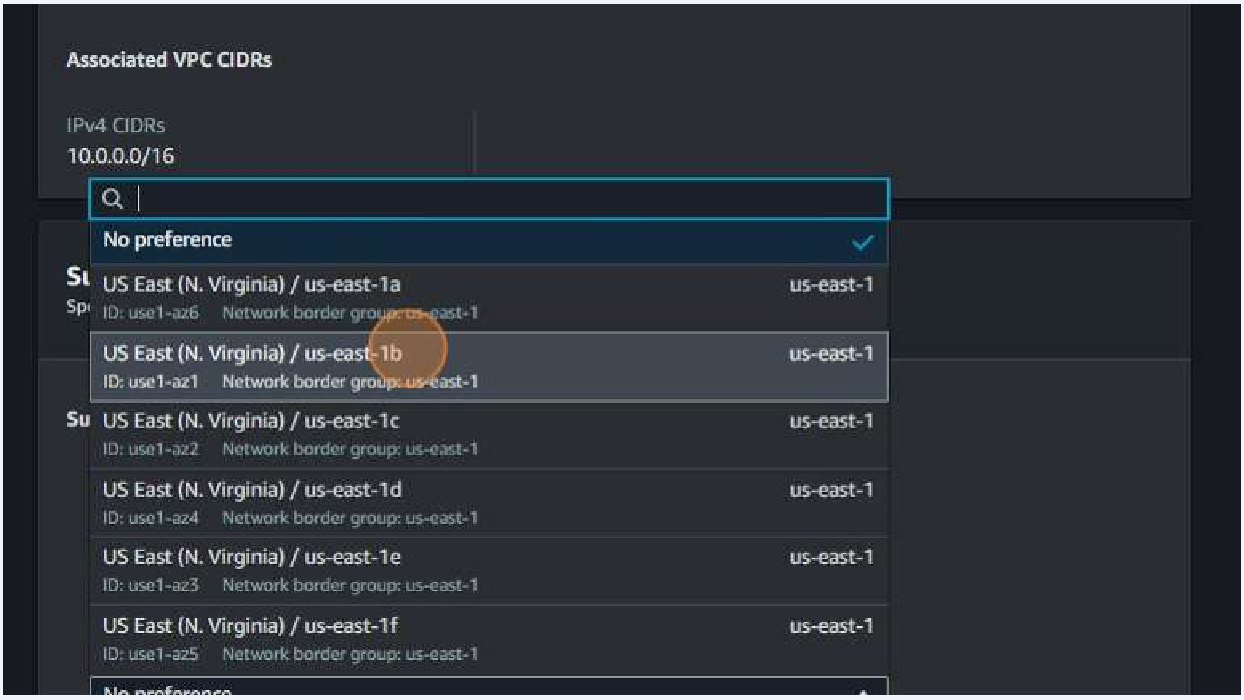
10.0.0.0/16

IPv4 subnet CIDR block

10.0.0.0/20

▼ Tags - *optional*

**151** Click "us-east-1"



Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16

No preference ✓

US East (N. Virginia) / us-east-1a us-east-1
ID: use1-az6 Network border group: us-east-1

US East (N. Virginia) / us-east-1b us-east-1
ID: use1-az1 Network border group: us-east-1

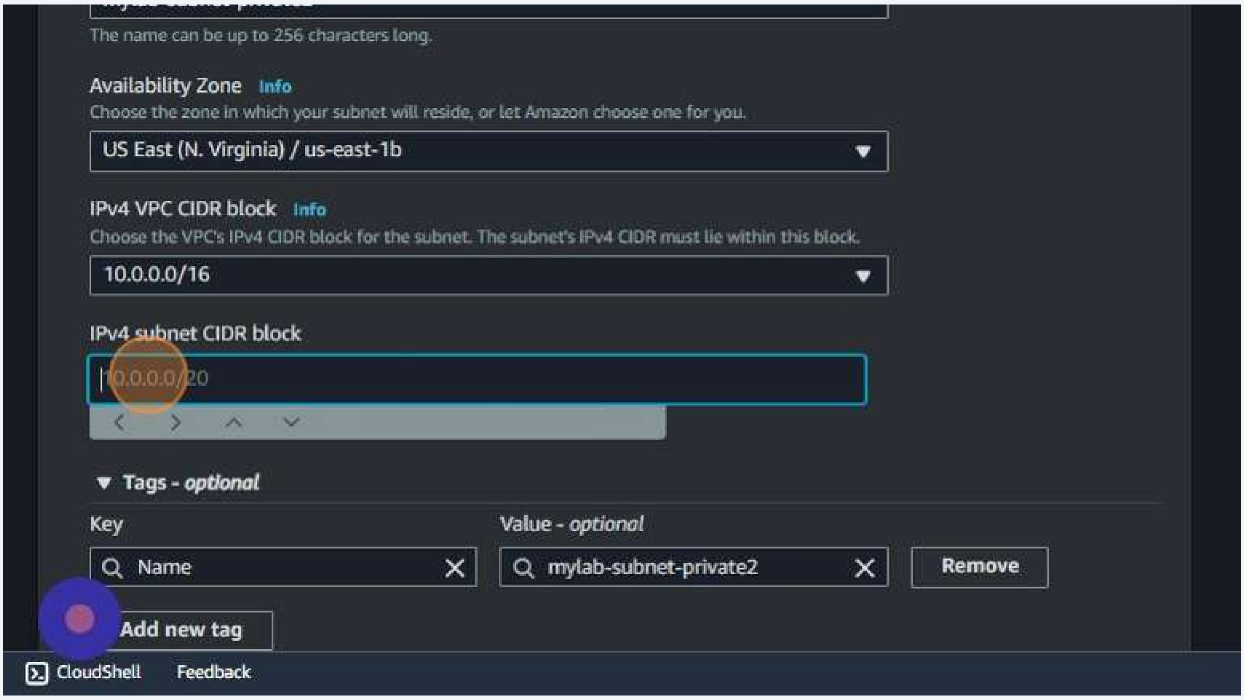
US East (N. Virginia) / us-east-1c us-east-1
ID: use1-az2 Network border group: us-east-1

US East (N. Virginia) / us-east-1d us-east-1
ID: use1-az4 Network border group: us-east-1

US East (N. Virginia) / us-east-1e us-east-1
ID: use1-az3 Network border group: us-east-1

US East (N. Virginia) / us-east-1f us-east-1
ID: use1-az5 Network border group: us-east-1

152 Click the "10.0.0.0/20" field.



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.

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

IPv4 VPC CIDR block Info

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

10.0.0.0/16

IPv4 subnet CIDR block

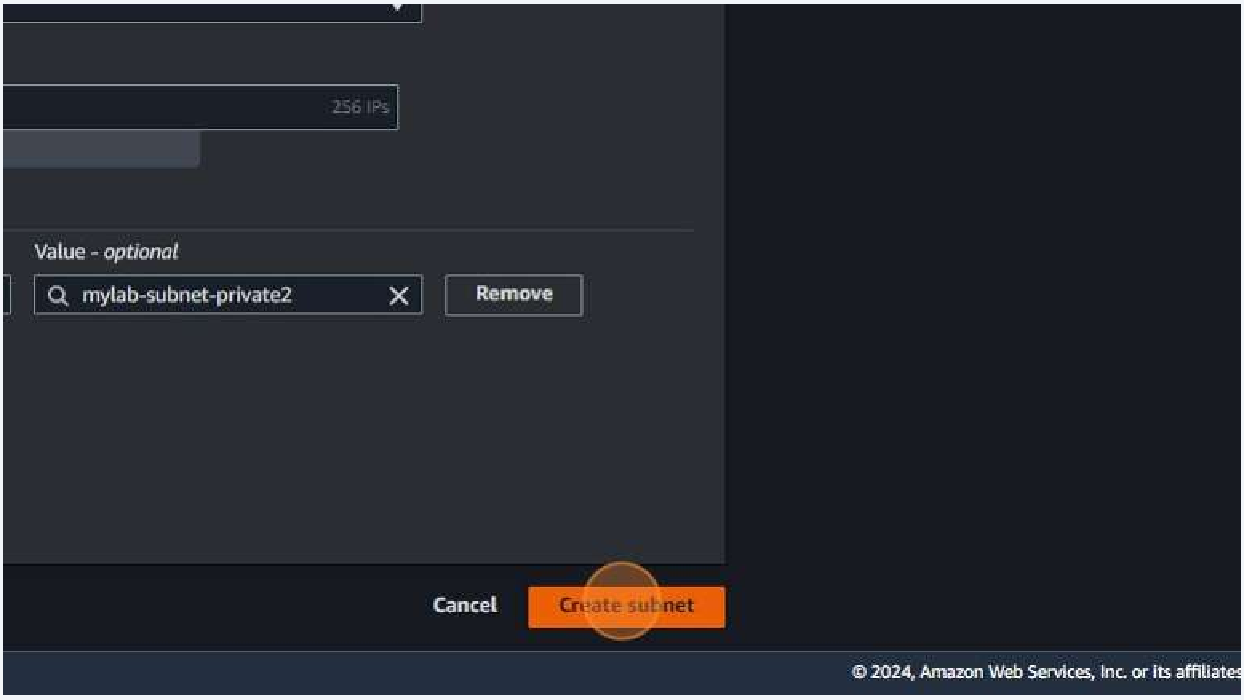
10.0.0.0/20

▼ Tags - *optional*

| Key | Value - *optional* |
|---|---|
| Name | mylab-subnet-private2 |

153 Type "10.0.3.0/24"

**154** Click "Create subnet"

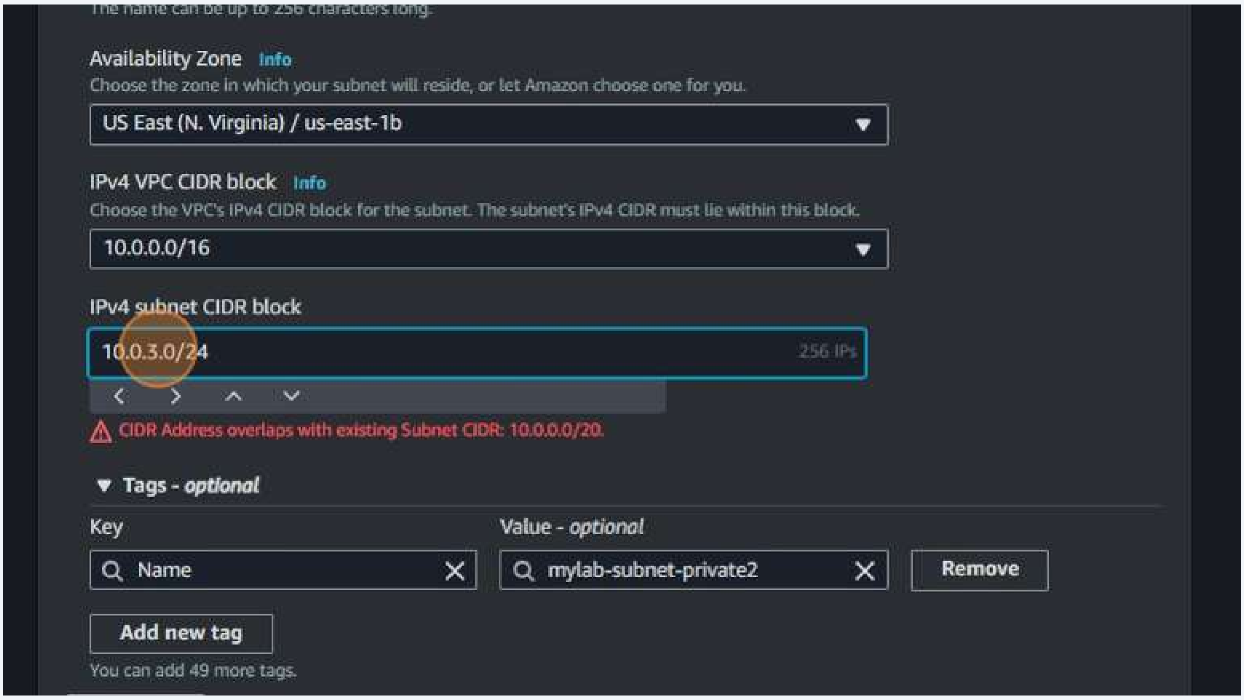


256 IPs

Value - *optional*

mylab-subnet-private2

**155** Click the "10.0.0.0/20" field.



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

IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/16

IPv4 subnet CIDR block
10.0.3.0/24 256 IPs

⚠ CIDR Address overlaps with existing Subnet CIDR: 10.0.0.0/20.

▼ Tags - *optional*

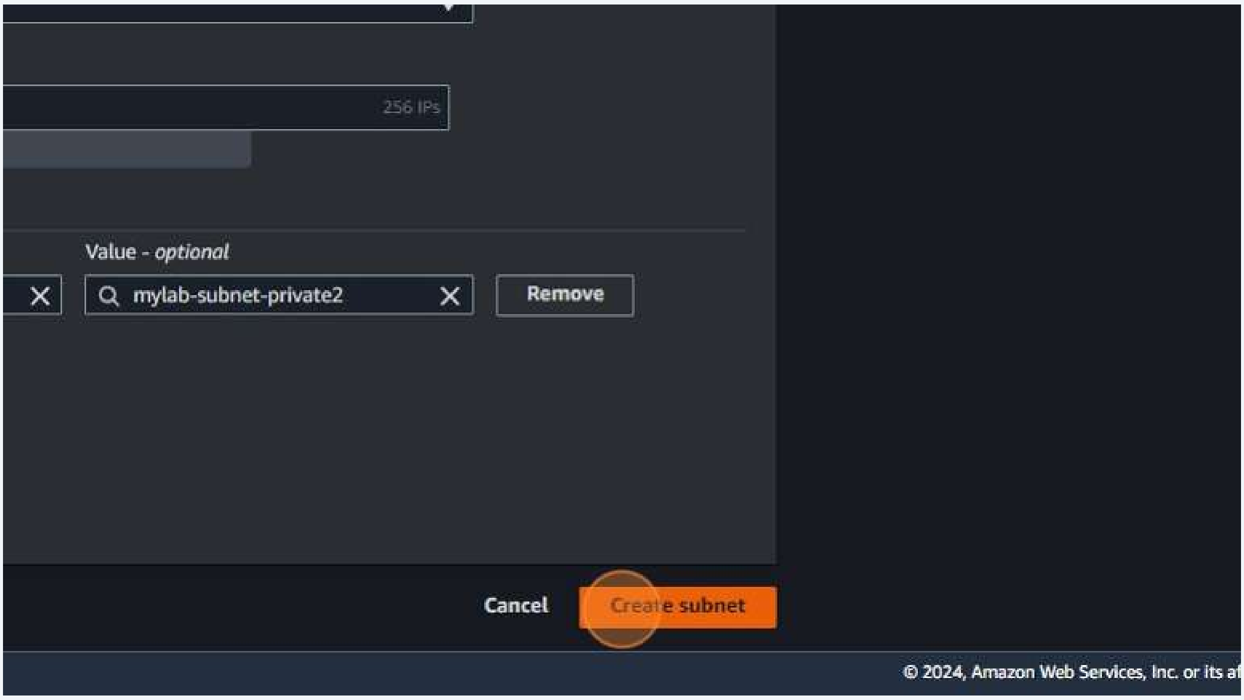
Key: Name

Value - *optional*: mylab-subnet-private2

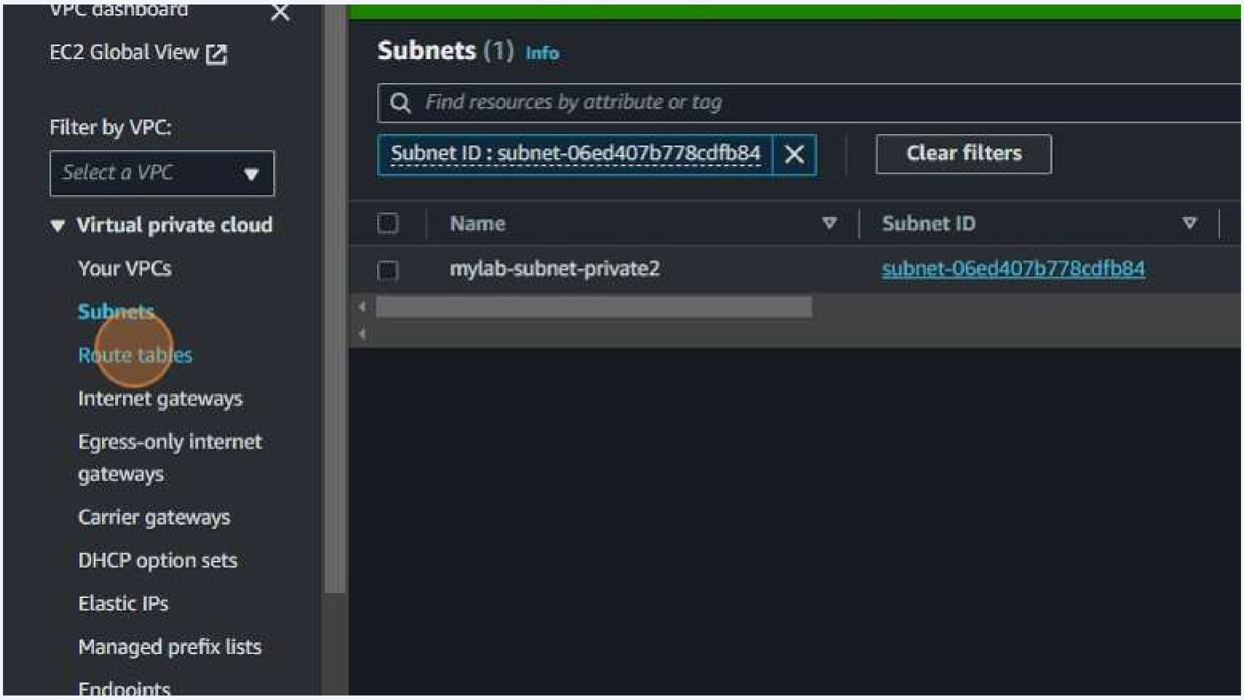
You can add 49 more tags.

156 Type " **Backspace** 98"

157 Click "Create subnet"

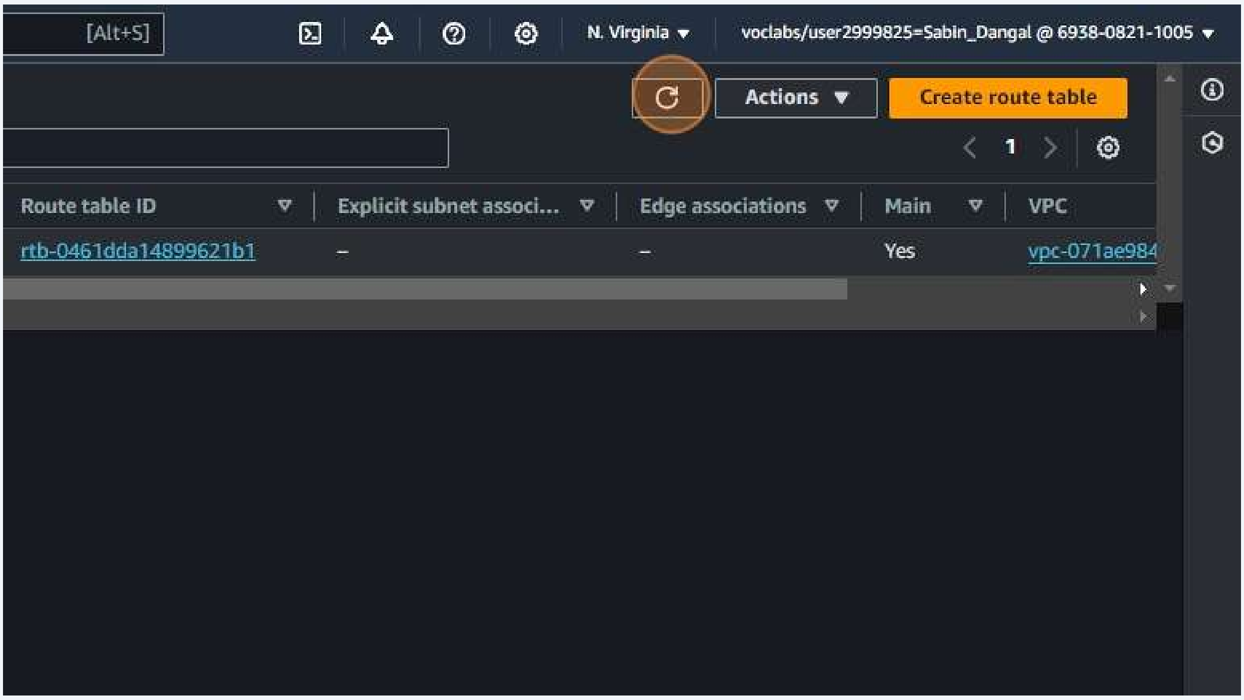


158 Click "Route tables"



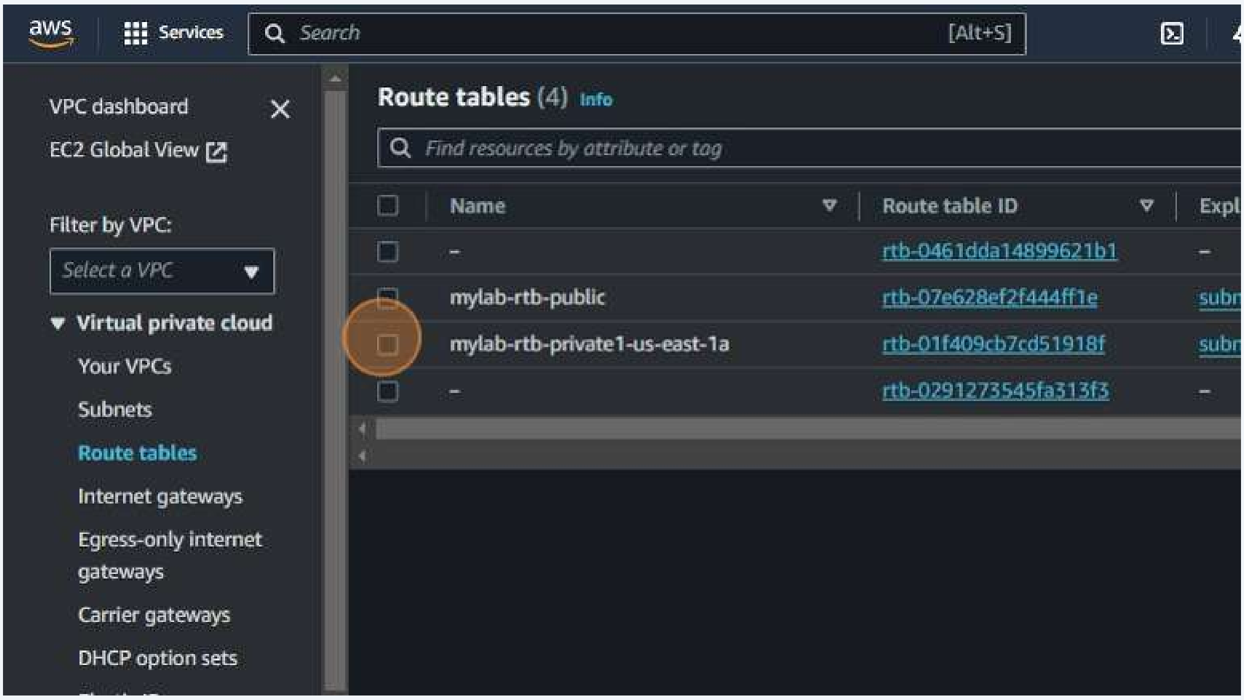
| □ | Name | Subnet ID |
|---|---|---|
| □ | mylab-subnet-private2 | subnet-06ed407b778cdfb84 |

159 Click here.



| Route table ID | Explicit subnet associ... | Edge associations | Main | VPC |
|---|---|---|---|---|
| rtb-0461dda14899621b1 | – | – | Yes | vpc-071ae984 |

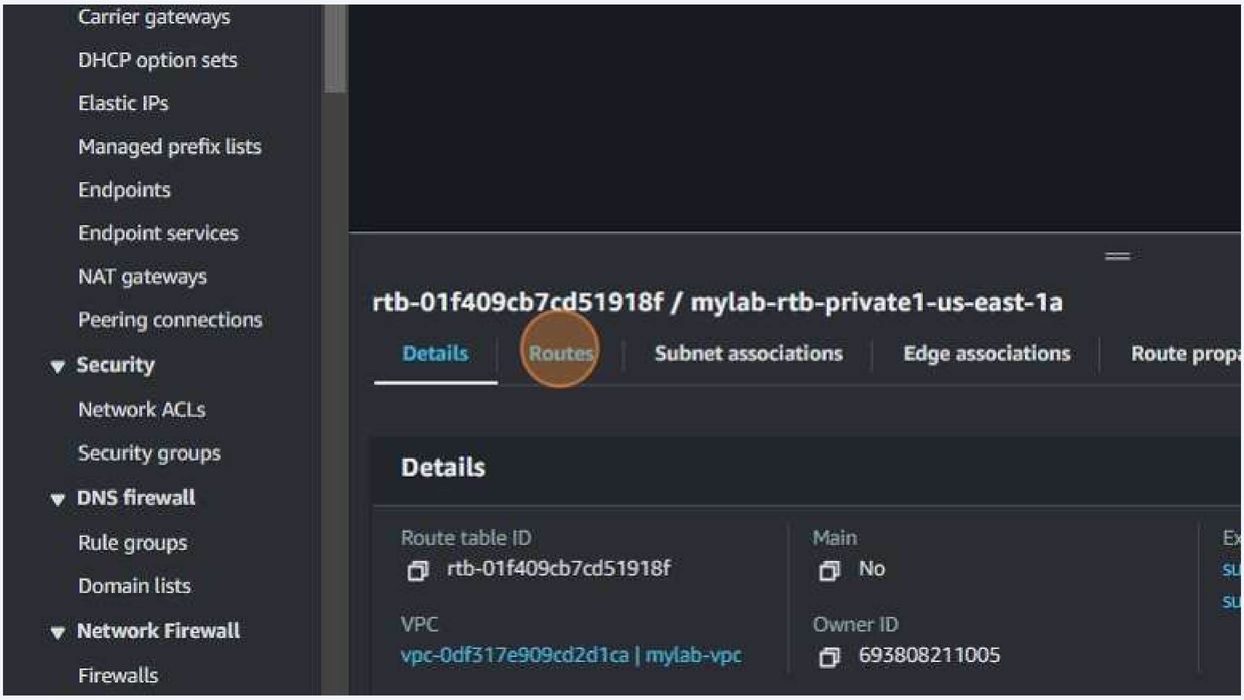
**160** Click this checkbox.



Route tables (4) Info

| □ | Name | Route table ID | Expl |
|---|---|---|---|
| □ | - | rtb-0461dda14899621b1 | – |
| □ | mylab-rtb-public | rtb-07e628ef2f444ff1e | subn |
| □ | mylab-rtb-private1-us-east-1a | rtb-01f409cb7cd51918f | subn |
| □ | - | rtb-0291273545fa313f3 | – |

**161** Click "Routes"



rtb-01f409cb7cd51918f / mylab-rtb-private1-us-east-1a

Details

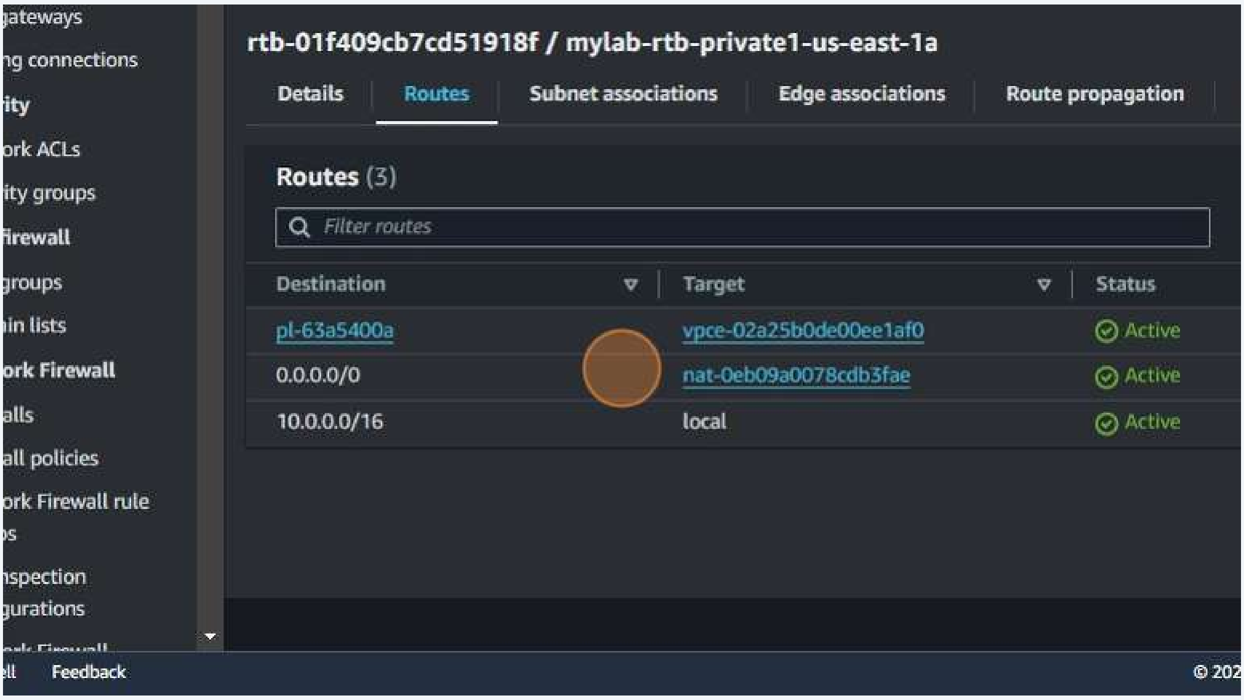
Route table ID
rtb-01f409cb7cd51918f

Main
No

VPC
vpc-0df317e909cd2d1ca | mylab-vpc

Owner ID
693808211005

**162** Click "0.0.0.0/0"

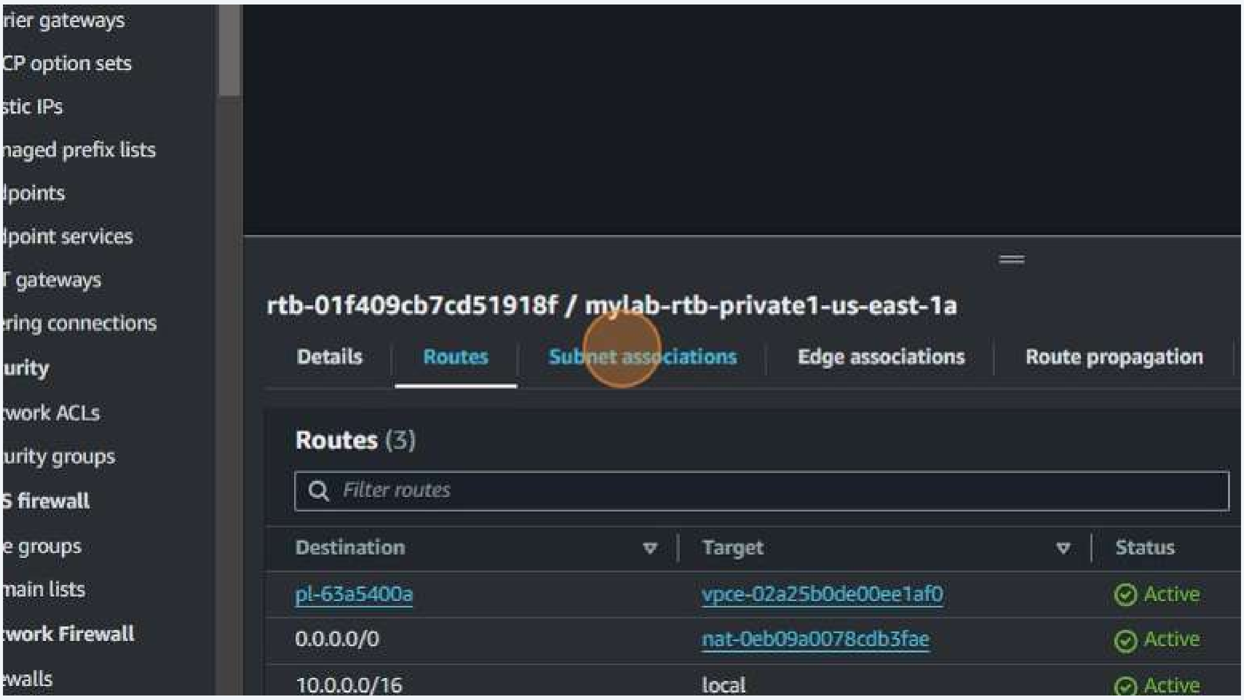


rtb-01f409cb7cd51918f / mylab-rtb-private1-us-east-1a

Routes (3)

| Destination | Target | Status |
|---|---|---|
| pl-63a5400a | vpce-02a25b0de00ee1af0 | Active |
| 0.0.0.0/0 | nat-0eb09a0078cdb3fae | Active |
| 10.0.0.0/16 | local | Active |

**163** Click "Subnet associations"

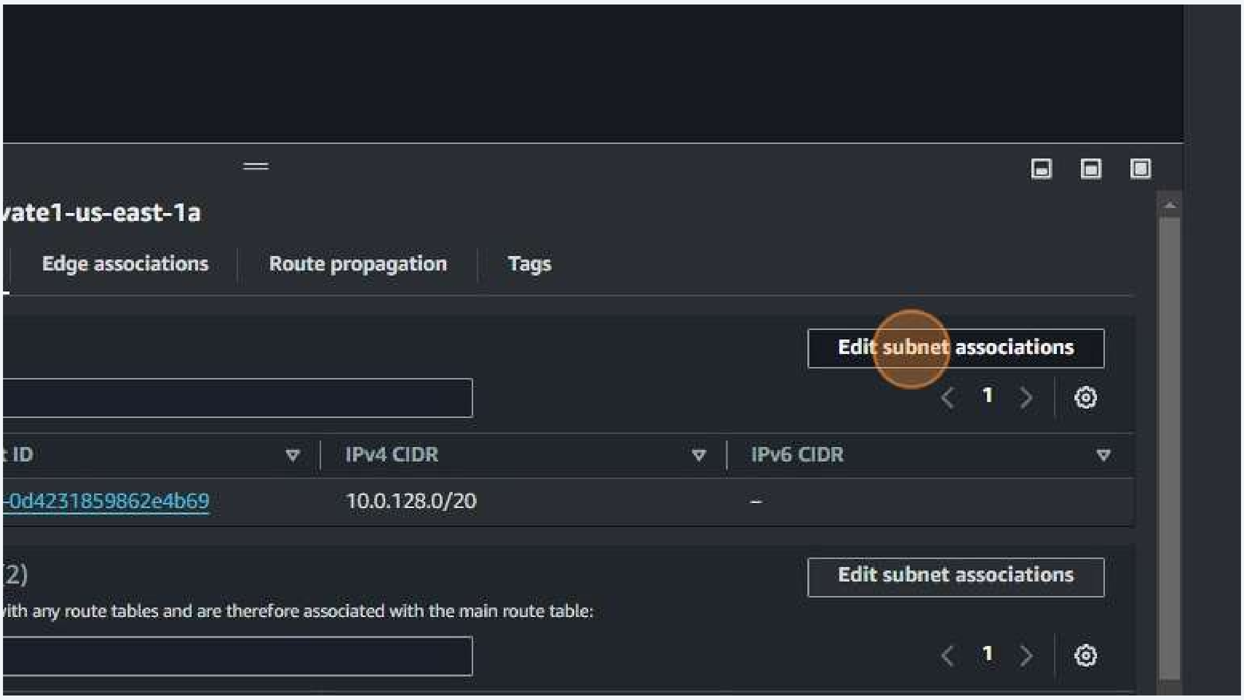


rtb-01f409cb7cd51918f / mylab-rtb-private1-us-east-1a

Routes (3)

| Destination | Target | Status |
|---|---|---|
| pl-63a5400a | vpce-02a25b0de00ee1af0 | Active |
| 0.0.0.0/0 | nat-0eb09a0078cdb3fae | Active |
| 10.0.0.0/16 | local | Active |

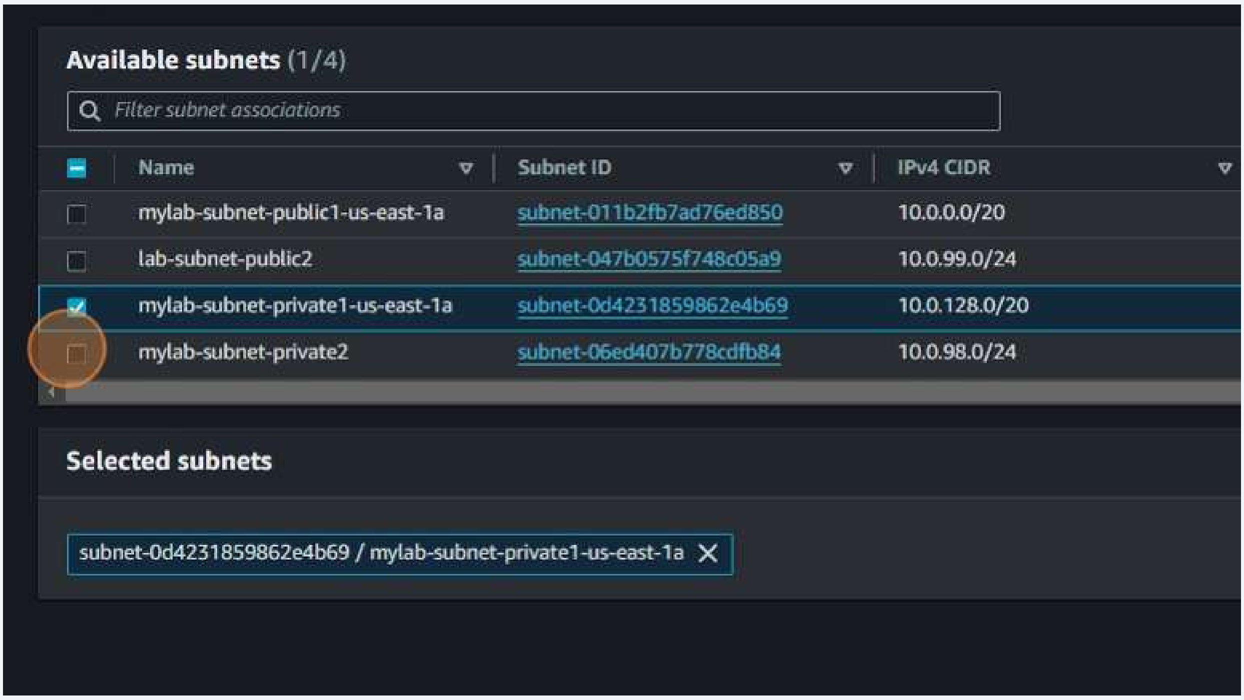
164 Click "Edit subnet associations"



| ID | IPv4 CIDR | IPv6 CIDR |
|---|---|---|
| -0d4231859862e4b69 | 10.0.128.0/20 | – |

ith any route tables and are therefore associated with the main route table:

165 Click this checkbox.



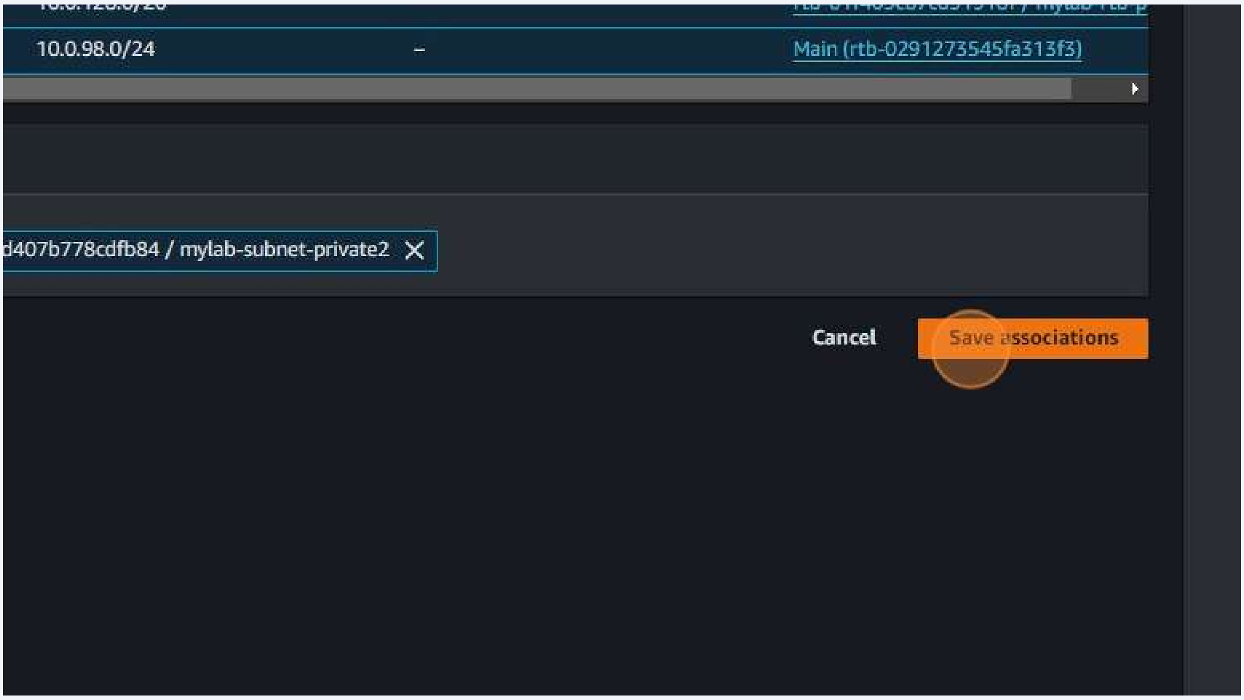
Available subnets (1/4)

| | Name | Subnet ID | IPv4 CIDR |
|---|---|---|---|
| □ | mylab-subnet-public1-us-east-1a | subnet-011b2fb7ad76ed850 | 10.0.0.0/20 |
| □ | lab-subnet-public2 | subnet-047b0575f748c05a9 | 10.0.99.0/24 |
| ☑ | mylab-subnet-private1-us-east-1a | subnet-0d4231859862e4b69 | 10.0.128.0/20 |
| □ | mylab-subnet-private2 | subnet-06ed407b778cdfb84 | 10.0.98.0/24 |

Selected subnets

subnet-0d4231859862e4b69 / mylab-subnet-private1-us-east-1a

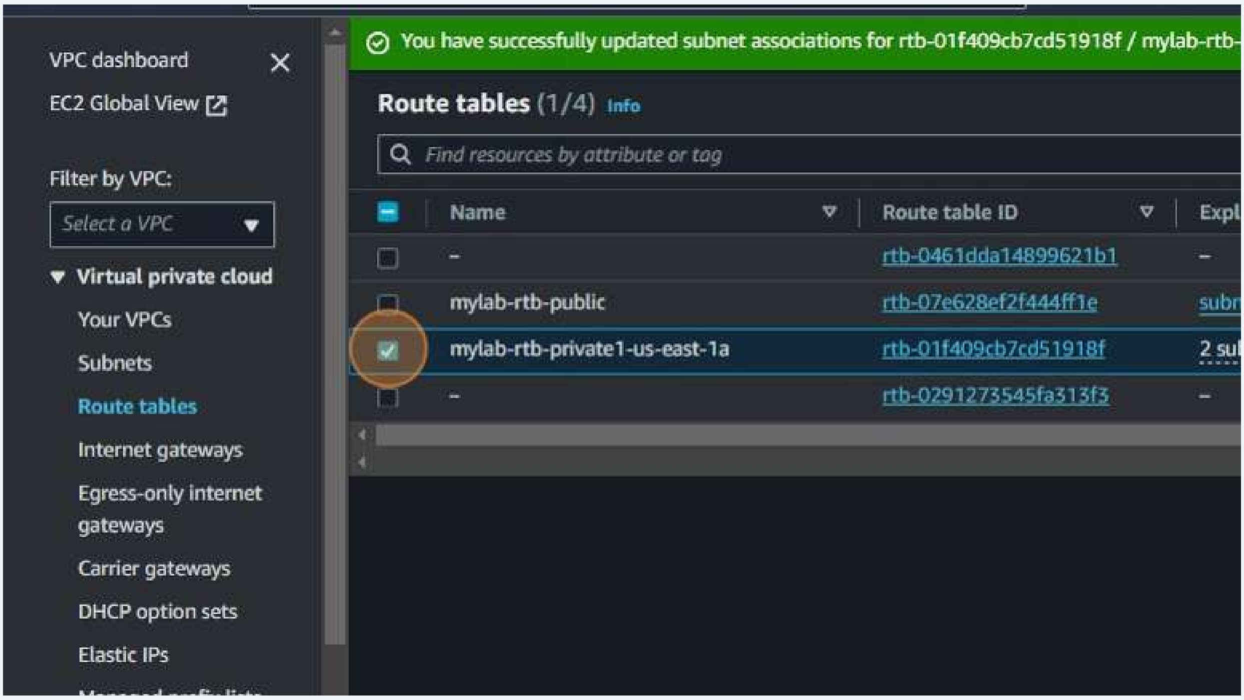
166 Click "Save associations"



10.0.98.0/24 – Main (rtb-0291273545fa313f3)

d407b778cdfb84 / mylab-subnet-private2 ✕

167 Click this checkbox.



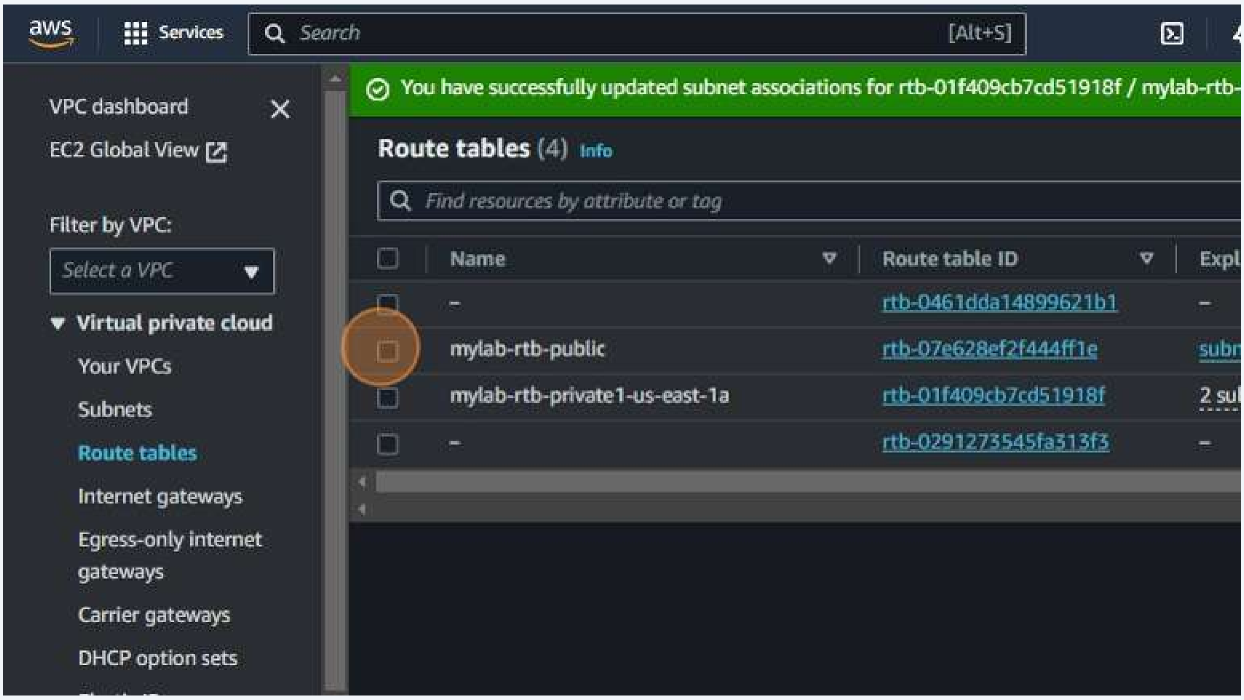
You have successfully updated subnet associations for rtb-01f409cb7cd51918f / mylab-rtb-

Route tables (1/4) Info

Find resources by attribute or tag

| | Name | Route table ID | Expl |
|---|---|---|---|
| □ | – | rtb-0461dda14899621b1 | – |
| □ | mylab-rtb-public | rtb-07e628ef2f444ff1e | subn |
| ☑ | mylab-rtb-private1-us-east-1a | rtb-01f409cb7cd51918f | 2 su |
| □ | – | rtb-0291273545fa313f3 | – |

168 Click this checkbox.

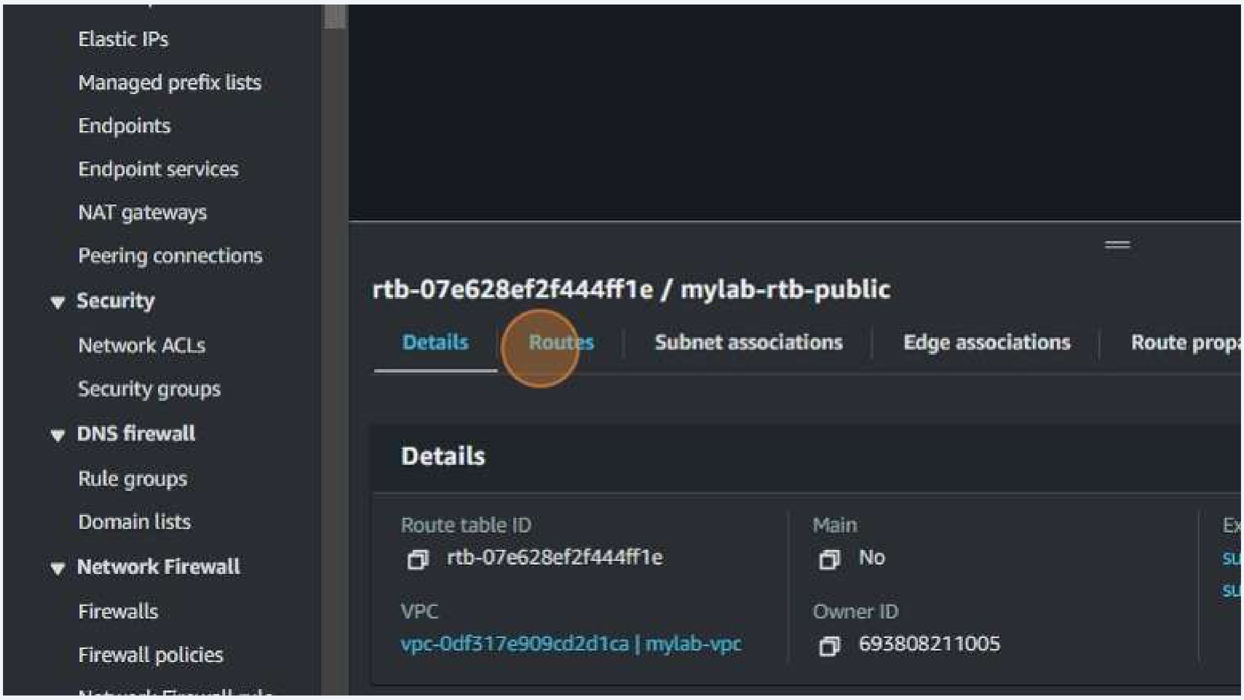


You have successfully updated subnet associations for rtb-01f409cb7cd51918f / mylab-rtb-

Route tables (4) Info

| Name | Route table ID | Expl |
|---|---|---|
| – | rtb-0461dda14899621b1 | – |
| mylab-rtb-public | rtb-07e628ef2f444ff1e | subn |
| mylab-rtb-private1-us-east-1a | rtb-01f409cb7cd51918f | 2 su |
| – | rtb-0291273545fa313f3 | – |

169 Click "Routes"



rtb-07e628ef2f444ff1e / mylab-rtb-public

Details

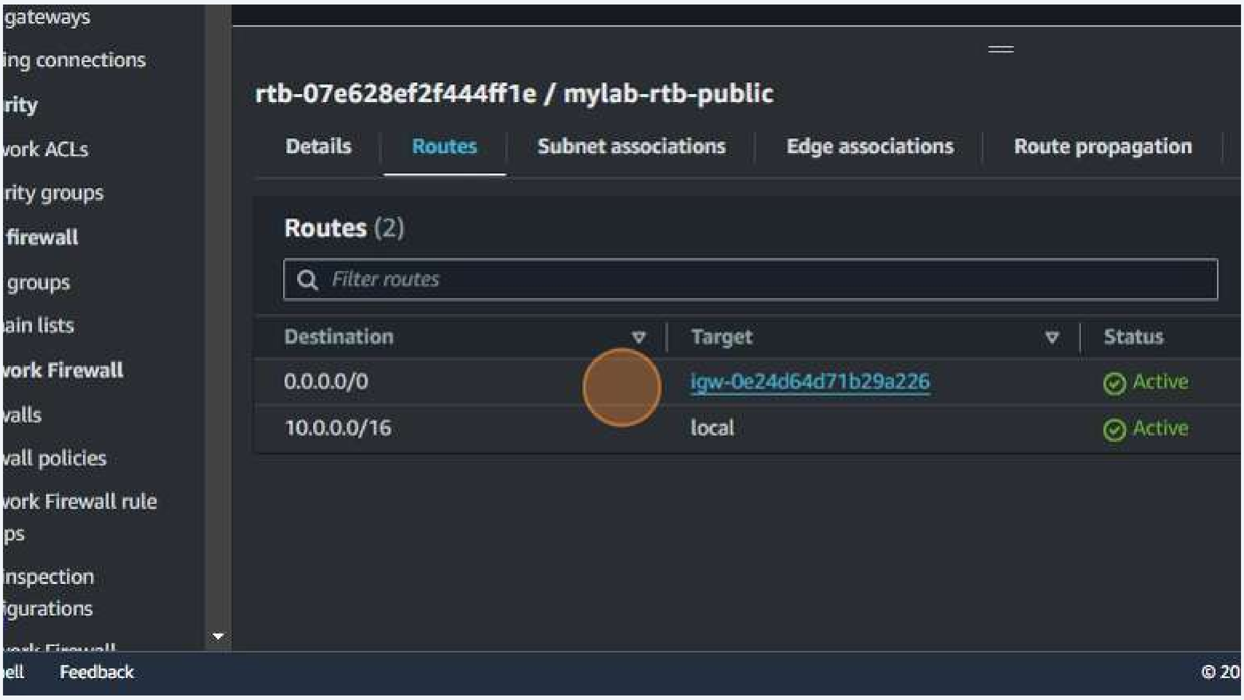
Route table ID: rtb-07e628ef2f444ff1e

Main: No

VPC: vpc-0df317e909cd2d1ca | mylab-vpc

Owner ID: 693808211005

**170** Click "0.0.0.0/0"

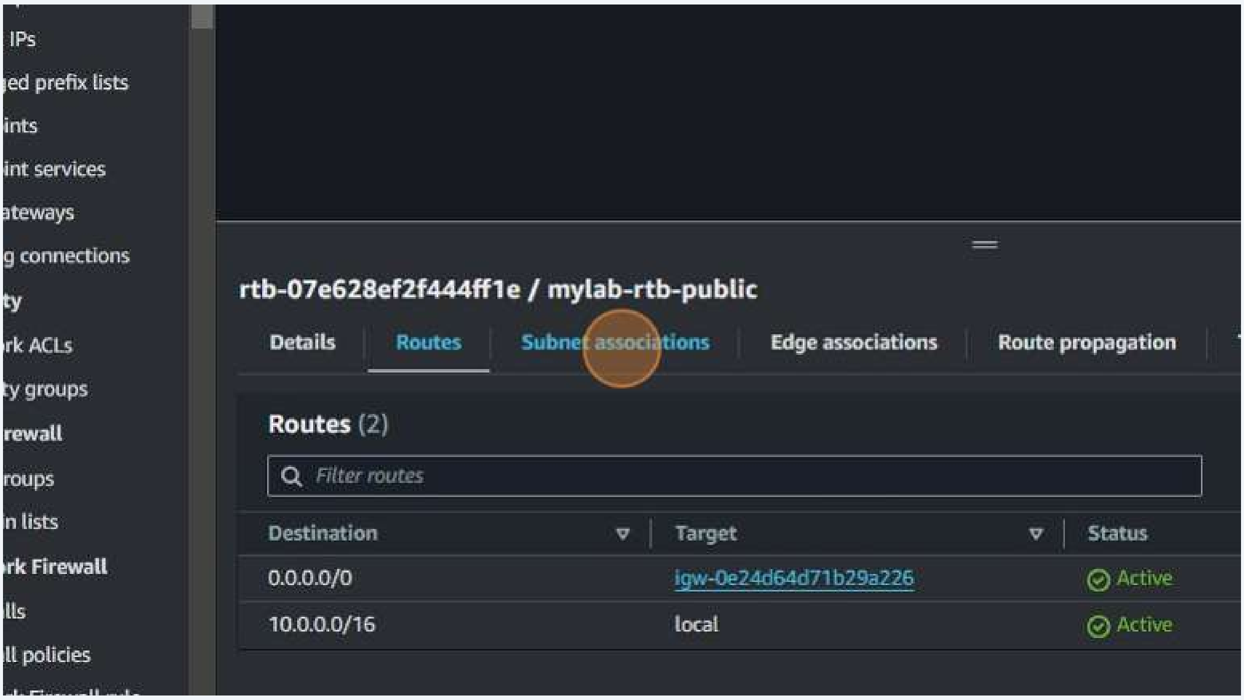


rtb-07e628ef2f444ff1e / mylab-rtb-public

Routes (2)

| Destination | Target | Status |
|---|---|---|
| 0.0.0.0/0 | igw-0e24d64d71b29a226 | Active |
| 10.0.0.0/16 | local | Active |

**171** Click "Subnet associations"

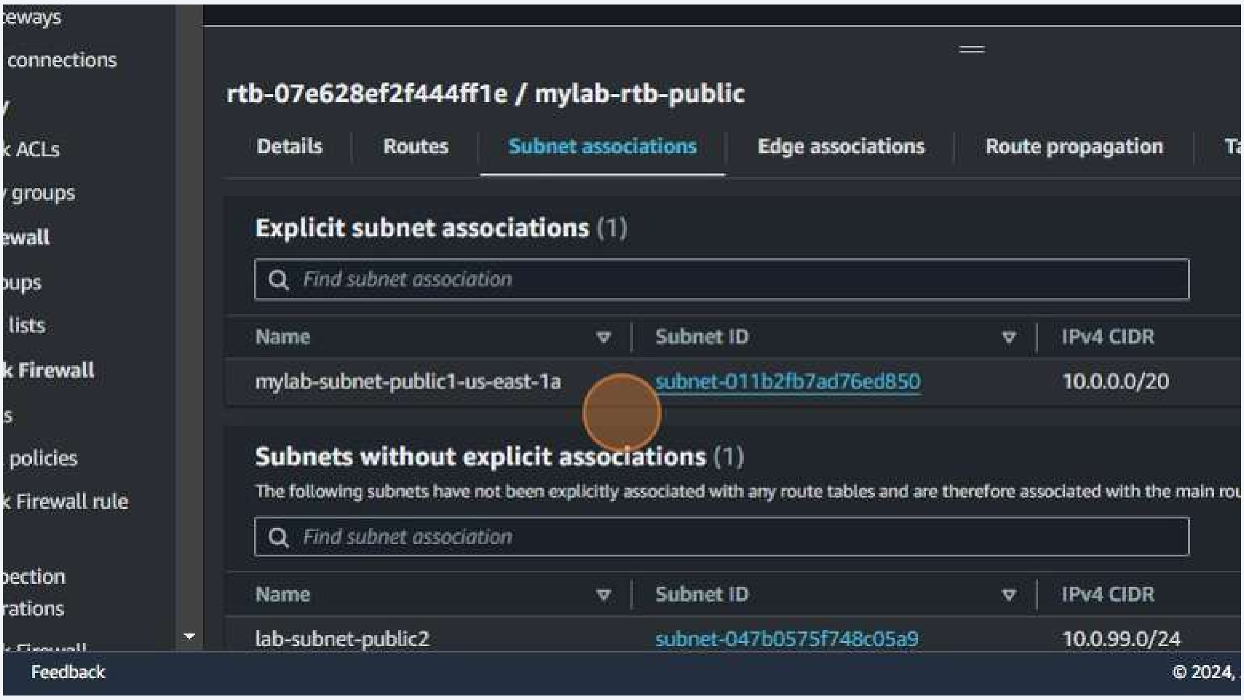


rtb-07e628ef2f444ff1e / mylab-rtb-public

Routes (2)

| Destination | Target | Status |
|---|---|---|
| 0.0.0.0/0 | igw-0e24d64d71b29a226 | Active |
| 10.0.0.0/16 | local | Active |

172 Click here.



rtb-07e628ef2f444ff1e / mylab-rtb-public

Explicit subnet associations (1)

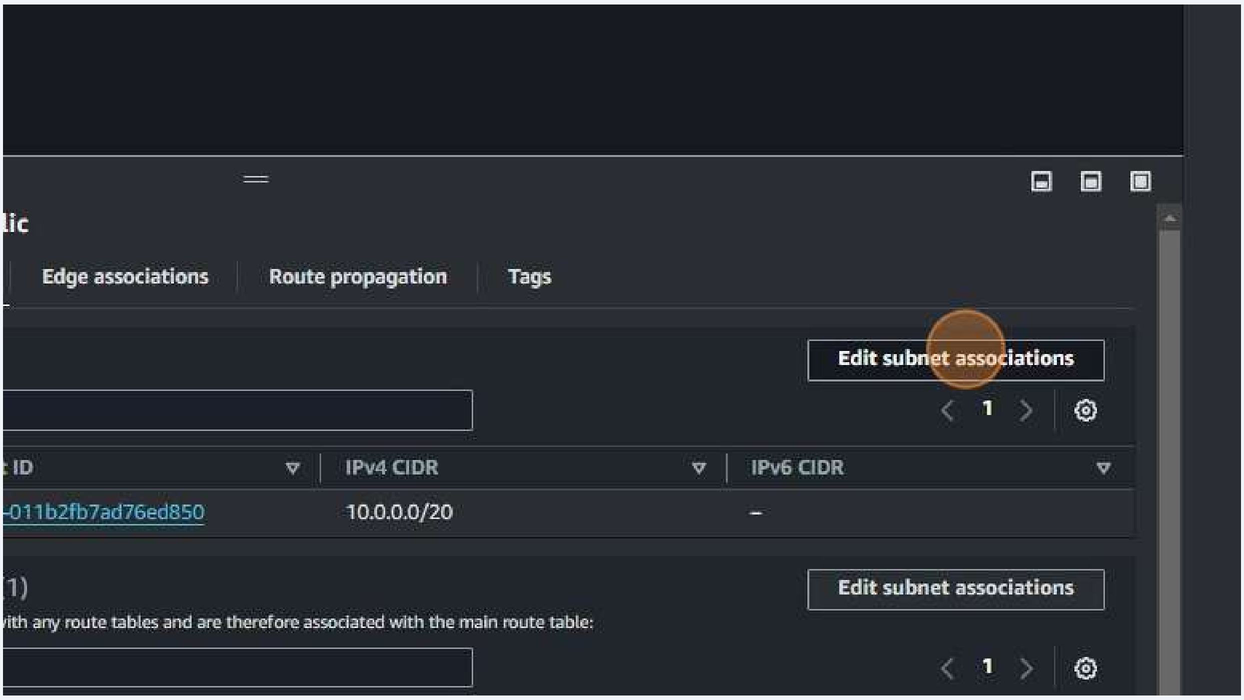
| Name | Subnet ID | IPv4 CIDR |
|---|---|---|
| mylab-subnet-public1-us-east-1a | subnet-011b2fb7ad76ed850 | 10.0.0.0/20 |

Subnets without explicit associations (1)

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main rou

| Name | Subnet ID | IPv4 CIDR |
|---|---|---|
| lab-subnet-public2 | subnet-047b0575f748c05a9 | 10.0.99.0/24 |

173 Click "Edit subnet associations"

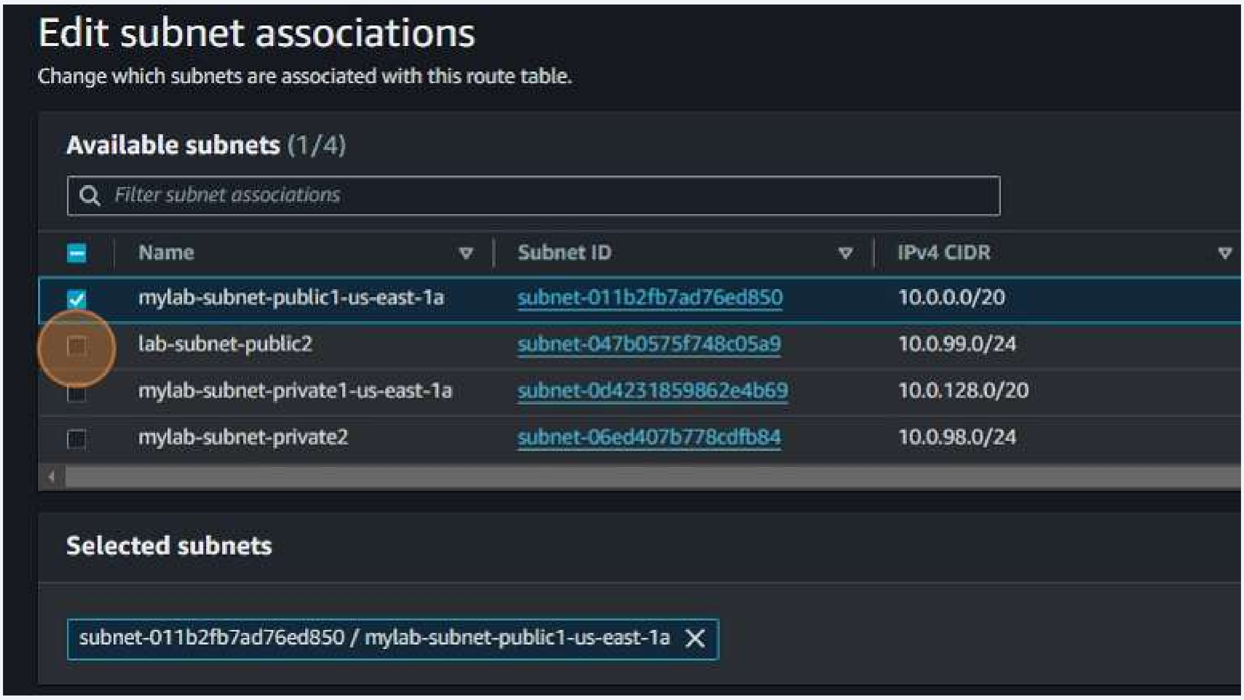


| t ID | IPv4 CIDR | IPv6 CIDR |
|---|---|---|
| -011b2fb7ad76ed850 | 10.0.0.0/20 | – |

(1)

ith any route tables and are therefore associated with the main route table:

174 Click this checkbox.



## Edit subnet associations

Change which subnets are associated with this route table.

**Available subnets** (1/4)

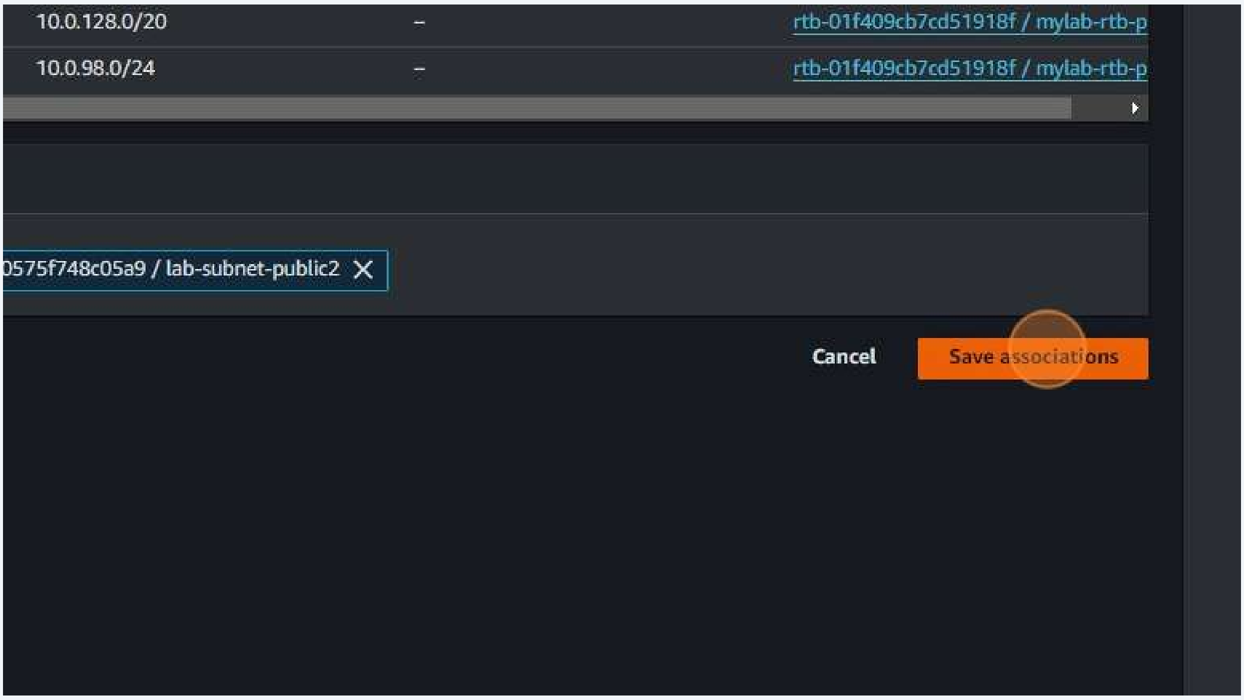
Filter subnet associations

|  | Name | Subnet ID | IPv4 CIDR |
|---|---|---|---|
| ☑ | mylab-subnet-public1-us-east-1a | subnet-011b2fb7ad76ed850 | 10.0.0.0/20 |
| □ | lab-subnet-public2 | subnet-047b0575f748c05a9 | 10.0.99.0/24 |
| □ | mylab-subnet-private1-us-east-1a | subnet-0d4231859862e4b69 | 10.0.128.0/20 |
| □ | mylab-subnet-private2 | subnet-06ed407b778cdfb84 | 10.0.98.0/24 |

**Selected subnets**

subnet-011b2fb7ad76ed850 / mylab-subnet-public1-us-east-1a ✕

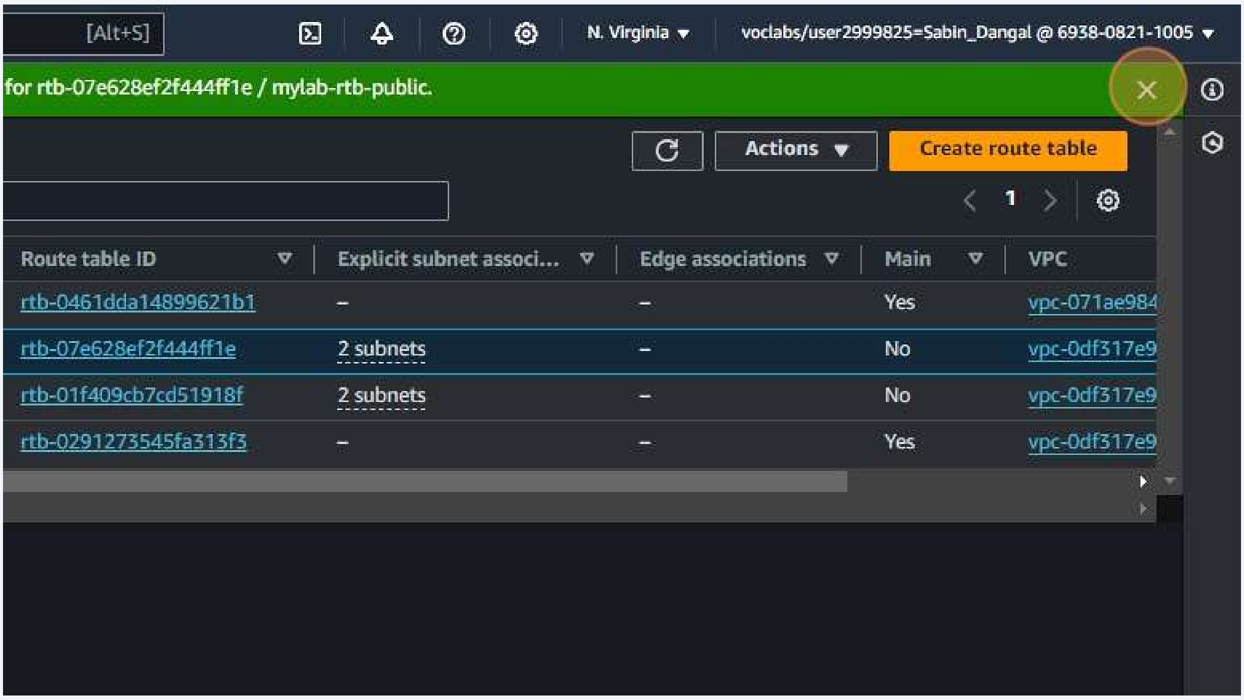
175 Click "Save associations"



| | | |
|---|---|---|
| 10.0.128.0/20 | – | rtb-01f409cb7cd51918f / mylab-rtb-p |
| 10.0.98.0/24 | – | rtb-01f409cb7cd51918f / mylab-rtb-p |

0575f748c05a9 / lab-subnet-public2 ✕

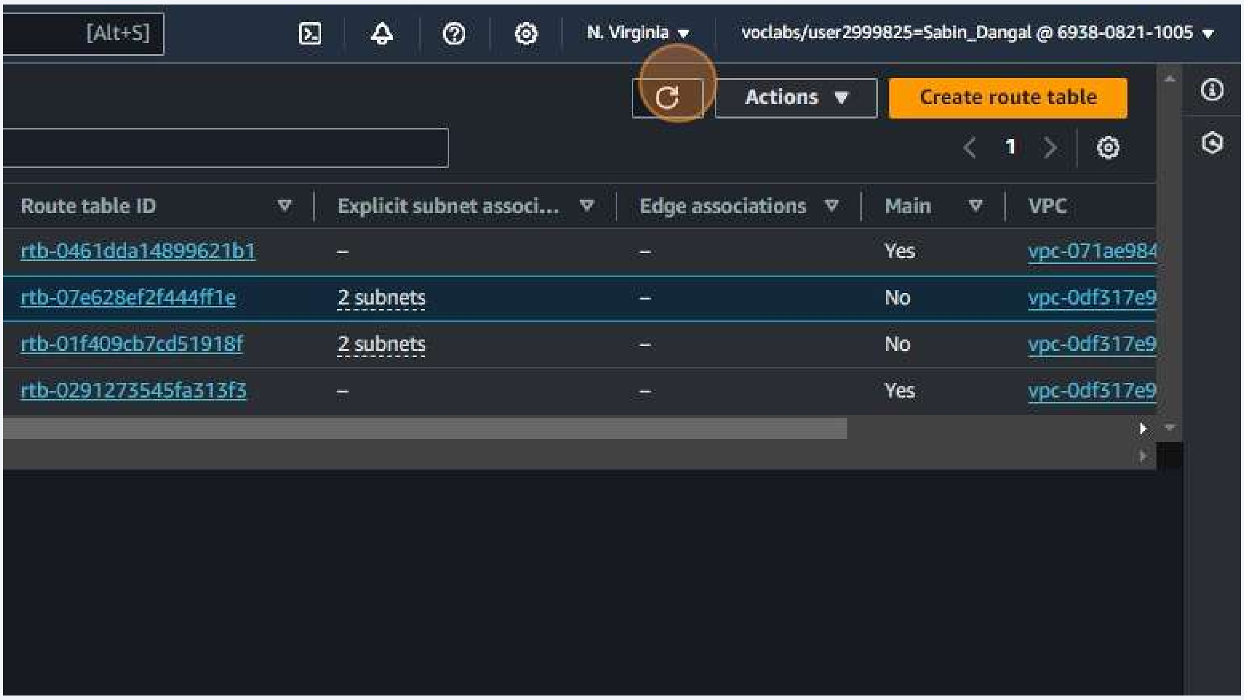
176 Click here.



for rtb-07e628ef2f444ff1e / mylab-rtb-public.

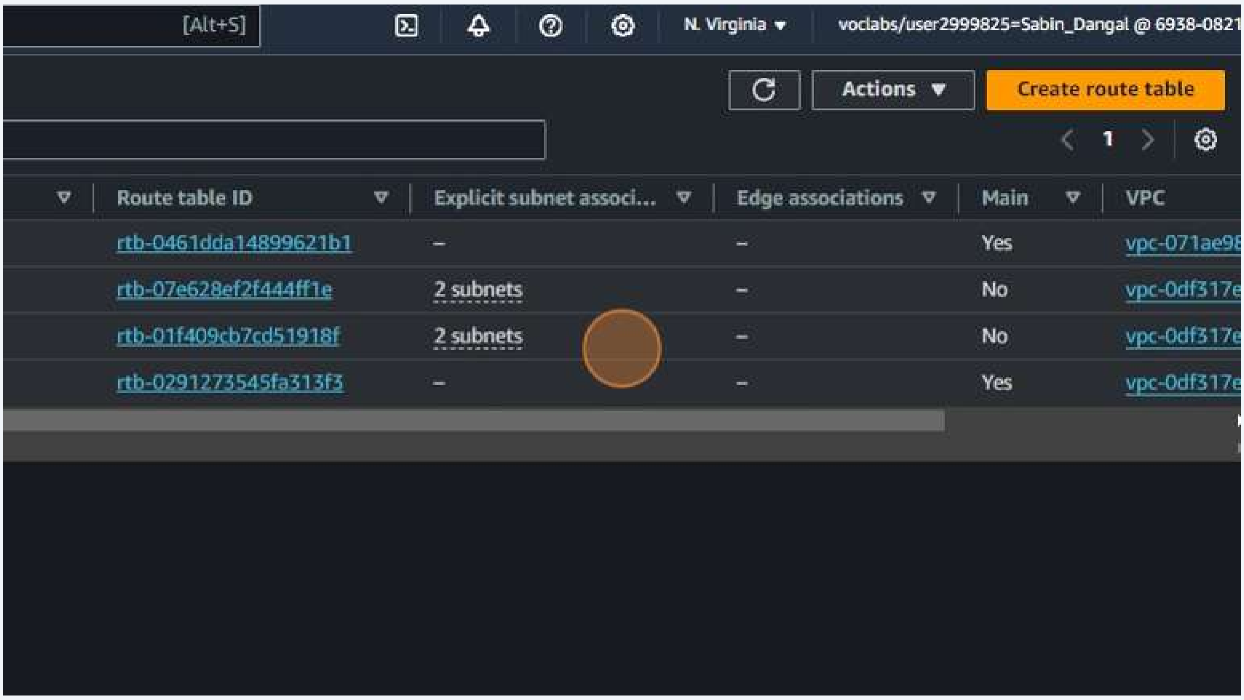
| Route table ID | Explicit subnet associ... | Edge associations | Main | VPC |
|---|---|---|---|---|
| rtb-0461dda14899621b1 | – | – | Yes | vpc-071ae984 |
| rtb-07e628ef2f444ff1e | 2 subnets | – | No | vpc-0df317e9 |
| rtb-01f409cb7cd51918f | 2 subnets | – | No | vpc-0df317e9 |
| rtb-0291273545fa313f3 | – | – | Yes | vpc-0df317e9 |

177 Click this button.



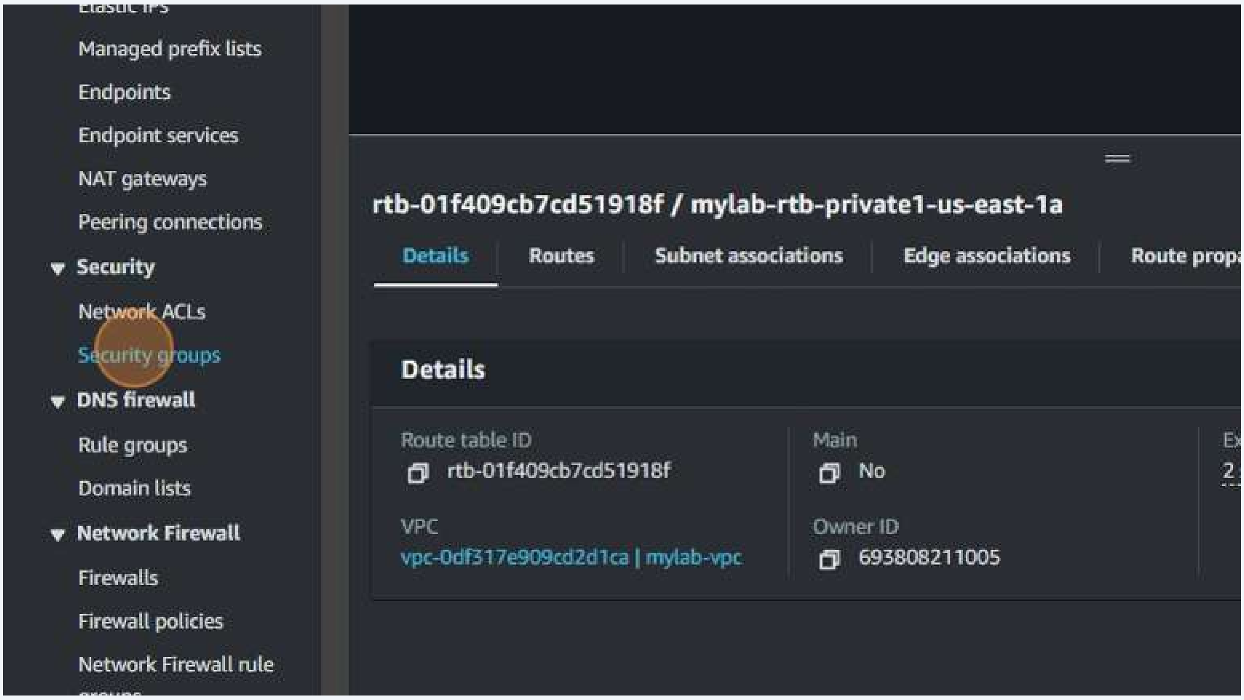
| Route table ID | Explicit subnet associ... | Edge associations | Main | VPC |
|---|---|---|---|---|
| rtb-0461dda14899621b1 | – | – | Yes | vpc-071ae984 |
| rtb-07e628ef2f444ff1e | 2 subnets | – | No | vpc-0df317e9 |
| rtb-01f409cb7cd51918f | 2 subnets | – | No | vpc-0df317e9 |
| rtb-0291273545fa313f3 | – | – | Yes | vpc-0df317e9 |

178 Click "2 subnets"



| | Route table ID | Explicit subnet associ... | Edge associations | Main | VPC |
|---|---|---|---|---|---|
| | rtb-0461dda14899621b1 | – | – | Yes | vpc-071ae98 |
| | rtb-07e628ef2f444ff1e | 2 subnets | – | No | vpc-0df317e |
| | rtb-01f409cb7cd51918f | 2 subnets | – | No | vpc-0df317e |
| | rtb-0291273545fa313f3 | – | – | Yes | vpc-0df317e |

179 Click "Security groups"



rtb-01f409cb7cd51918f / mylab-rtb-private1-us-east-1a

Details

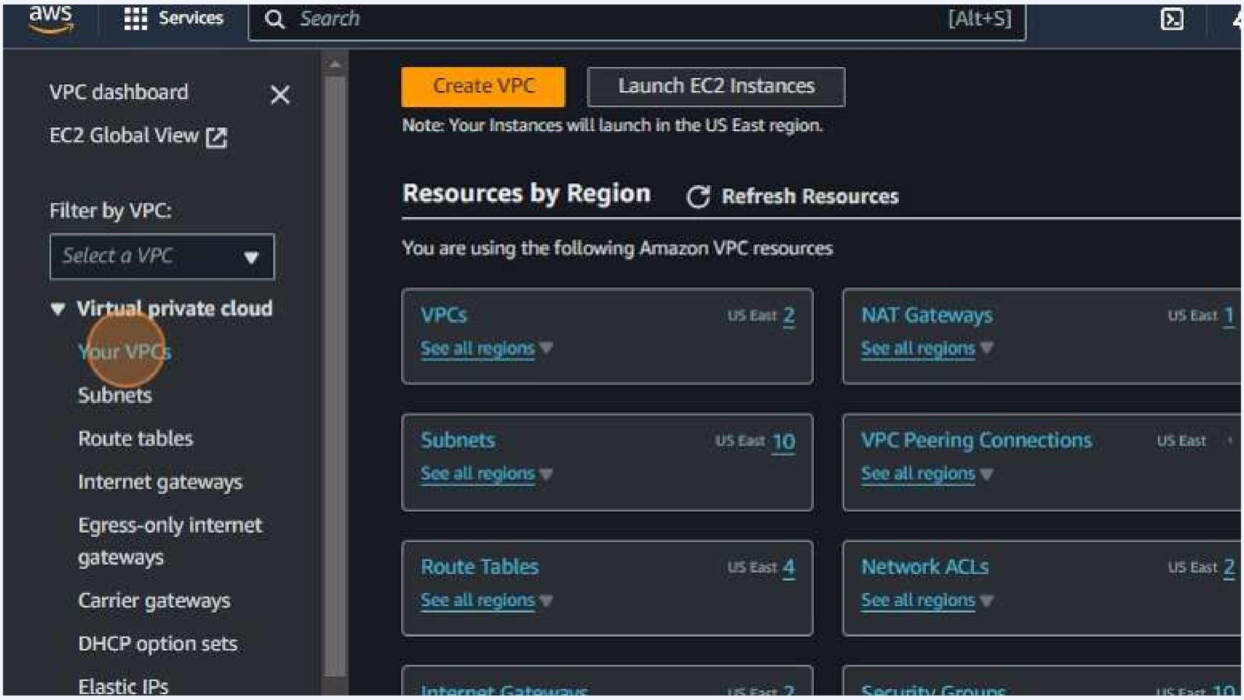
Route table ID: rtb-01f409cb7cd51918f

Main: No

VPC: vpc-0df317e909cd2d1ca | mylab-vpc

Owner ID: 693808211005

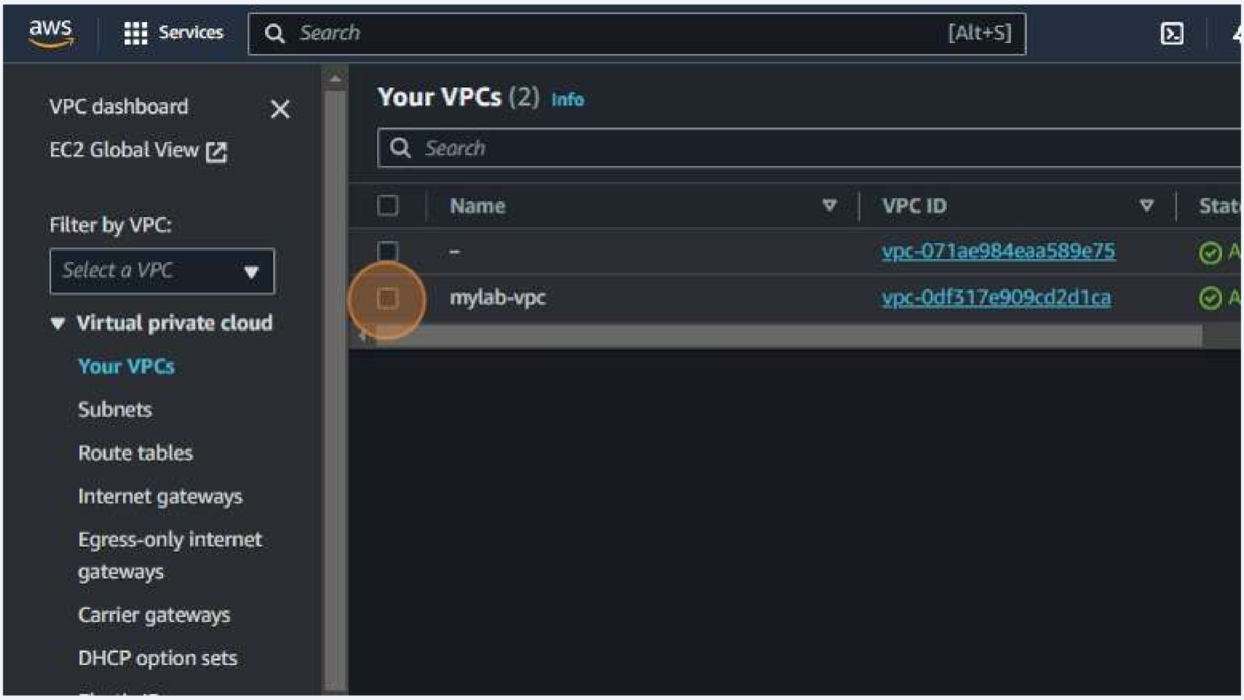
180 Click "Your VPCs"



Note: Your Instances will launch in the US East region.

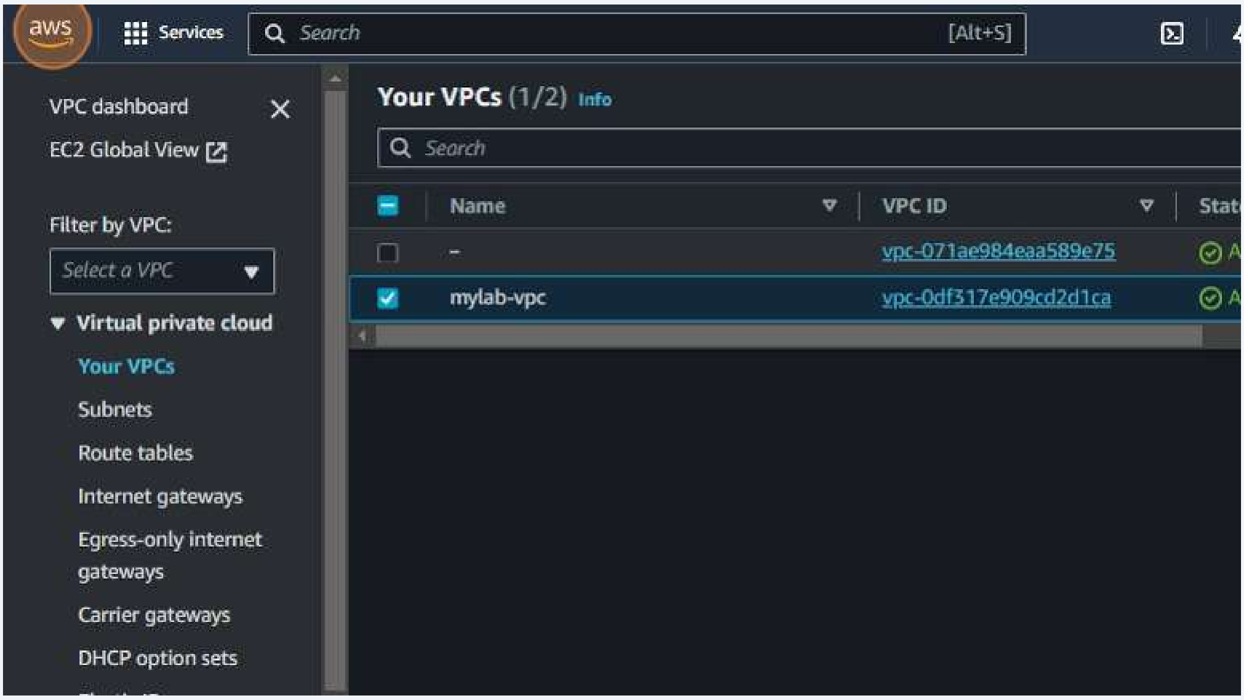
You are using the following Amazon VPC resources

181 Click this checkbox.



| □ | Name | VPC ID | Stat |
|---|---|---|---|
| □ | – | vpc-071ae984eaa589e75 | A |
| □ | mylab-vpc | vpc-0df317e909cd2d1ca | A |

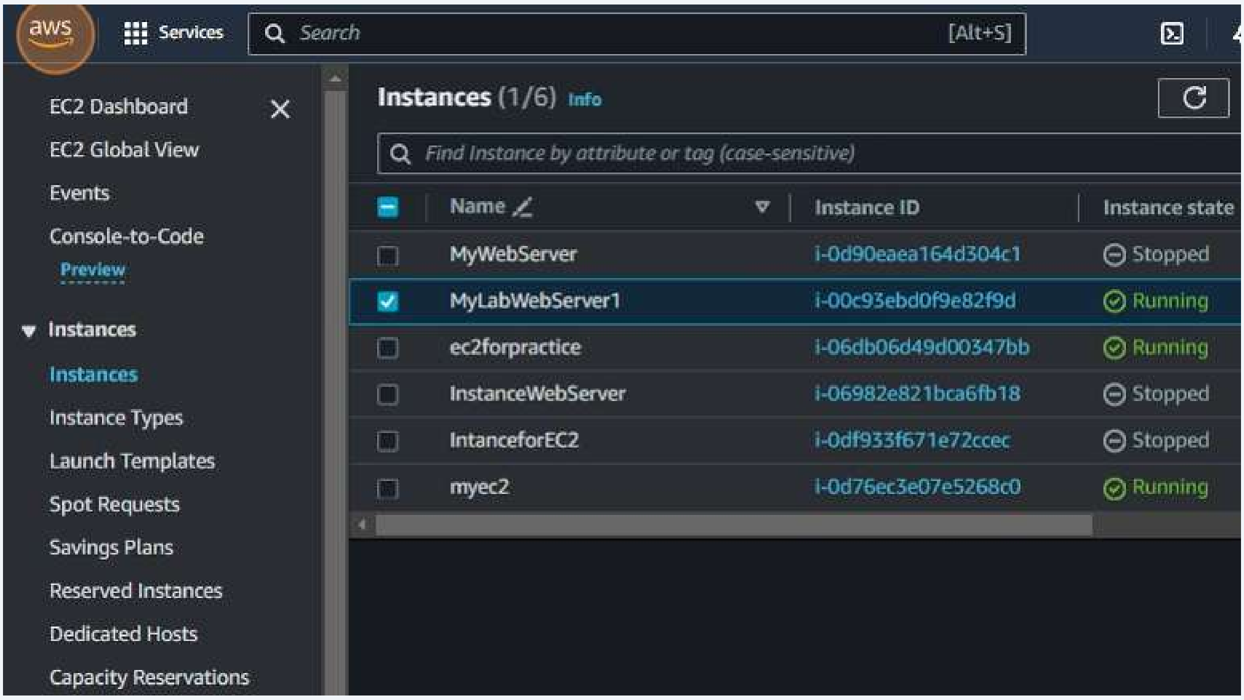
182 Click this link.



| ☑ | Name | VPC ID | Stat |
|---|---|---|---|
| □ | - | vpc-071ae984eaa589e75 | ✓ A |
| ☑ | mylab-vpc | vpc-0df317e909cd2d1ca | ✓ A |

183 Navigate to [https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:v=3;$case=tags:true%5C,client:false;$regex=tags:false%5C,client:false](https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:v=3;$case=tags:true%5C,client:false;$regex=tags:false%5C,client:false)

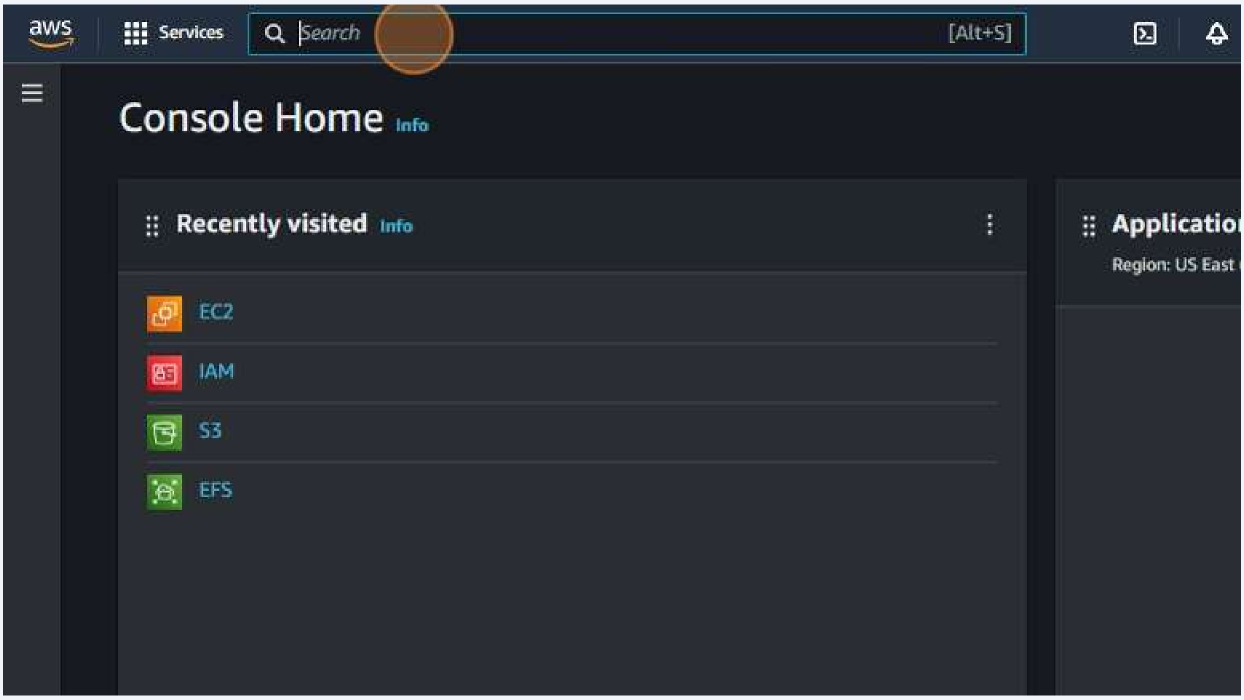
**184** Click this link.



Instances (1/6) Info

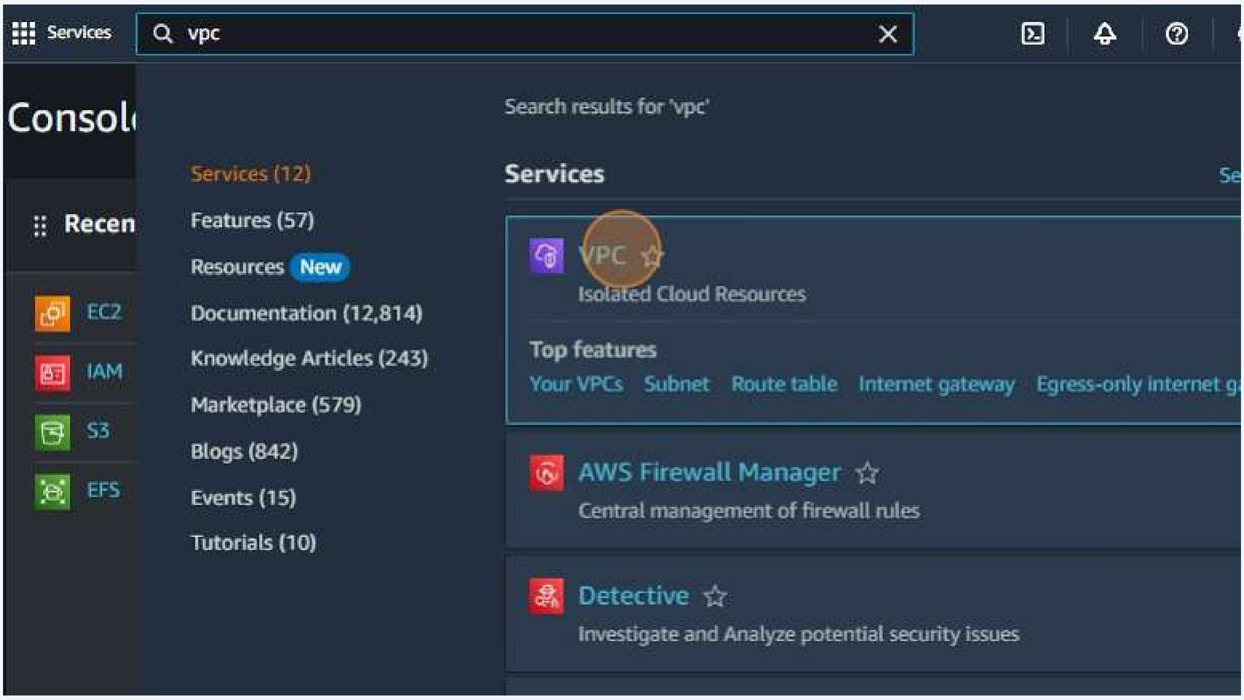
| | Name | Instance ID | Instance state |
|---|---|---|---|
| □ | MyWebServer | i-0d90eaea164d304c1 | Stopped |
| ☑ | MyLabWebServer1 | i-00c93ebd0f9e82f9d | Running |
| □ | ec2forpractice | i-06db06d49d00347bb | Running |
| □ | InstanceWebServer | i-06982e821bca6fb18 | Stopped |
| □ | IntanceforEC2 | i-0df933f671e72ccec | Stopped |
| □ | myec2 | i-0d76ec3e07e5268c0 | Running |

**185** Click the "Search" field.

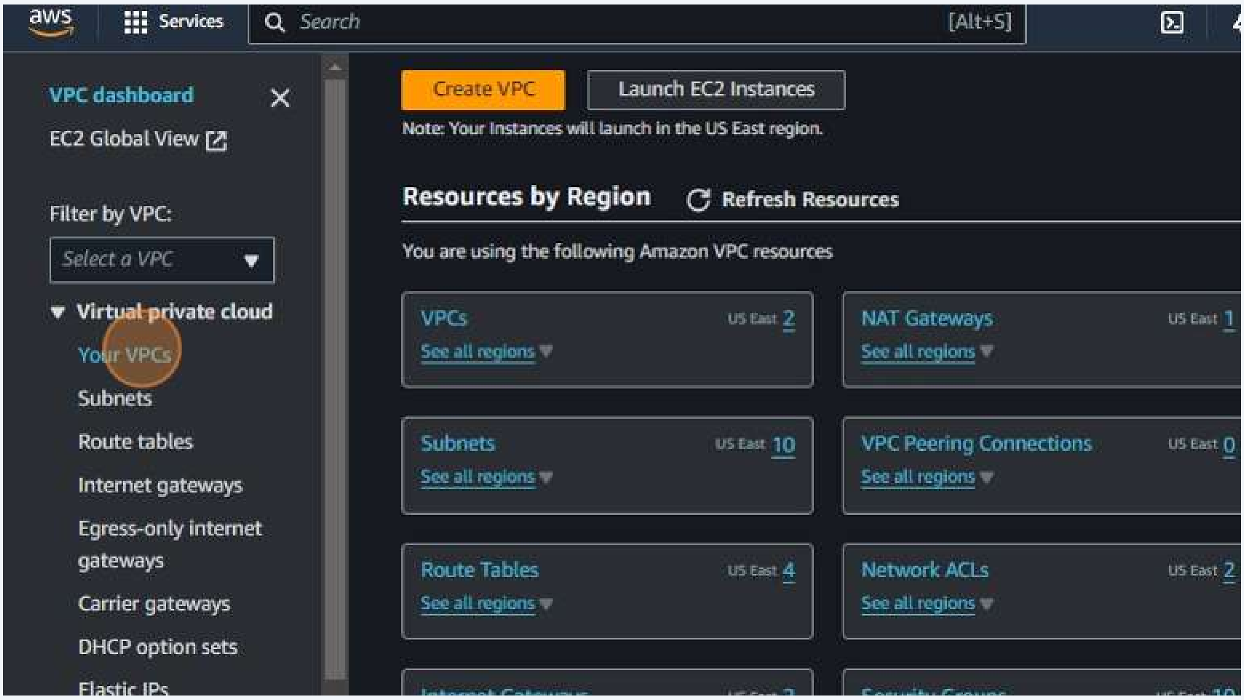


186 Type "vpc"

187 Click "VPC"



188 Click "Your VPCs"

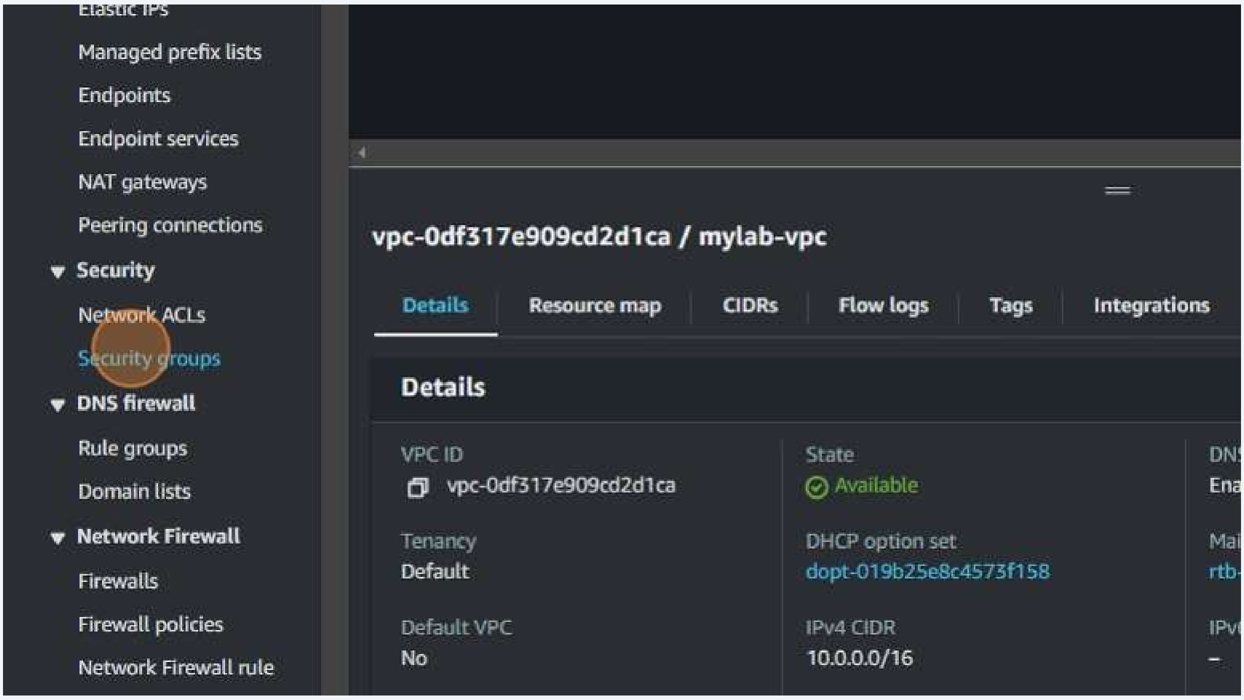


Note: Your Instances will launch in the US East region.

You are using the following Amazon VPC resources

| | | | |
|---|---|---|---|
| VPCs | US East 2 | NAT Gateways | US East 1 |
| Subnets | US East 10 | VPC Peering Connections | US East 0 |
| Route Tables | US East 4 | Network ACLs | US East 2 |

189 Click "Security groups"



vpc-0df317e909cd2d1ca / mylab-vpc

Details

VPC ID: vpc-0df317e909cd2d1ca

State: Available

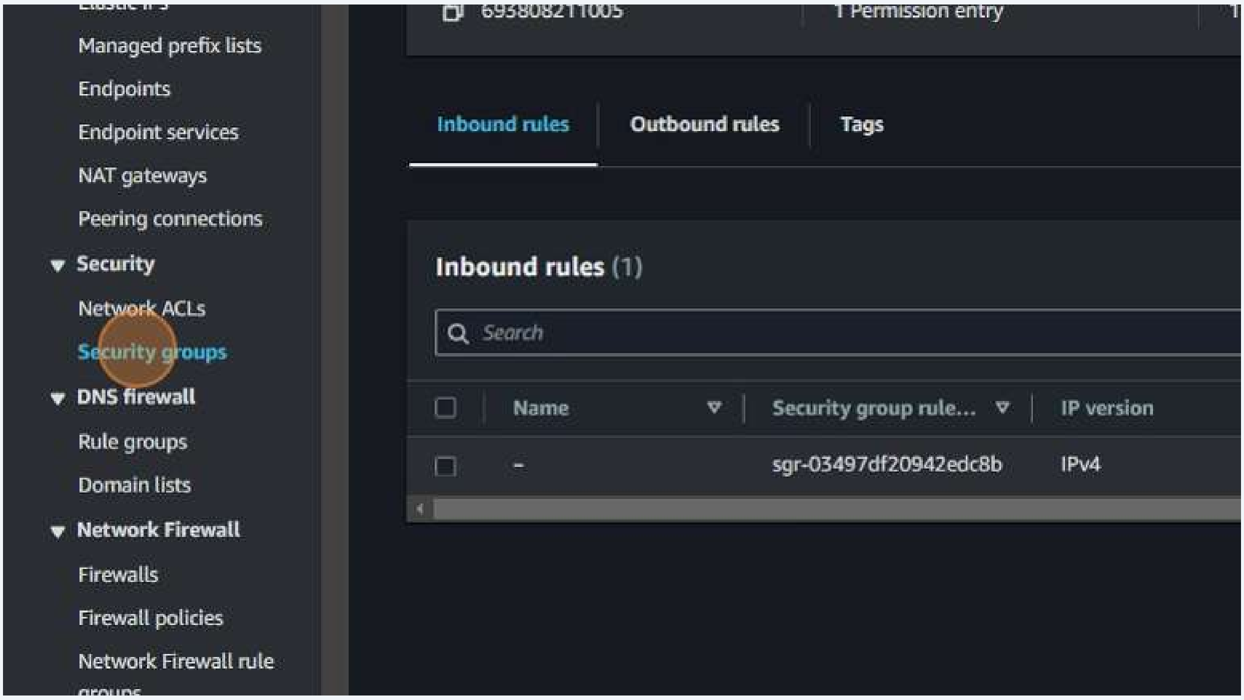
Tenancy: Default

DHCP option set: dopt-019b25e8c4573f158

Default VPC: No

IPv4 CIDR: 10.0.0.0/16

**190** Click "Security groups"



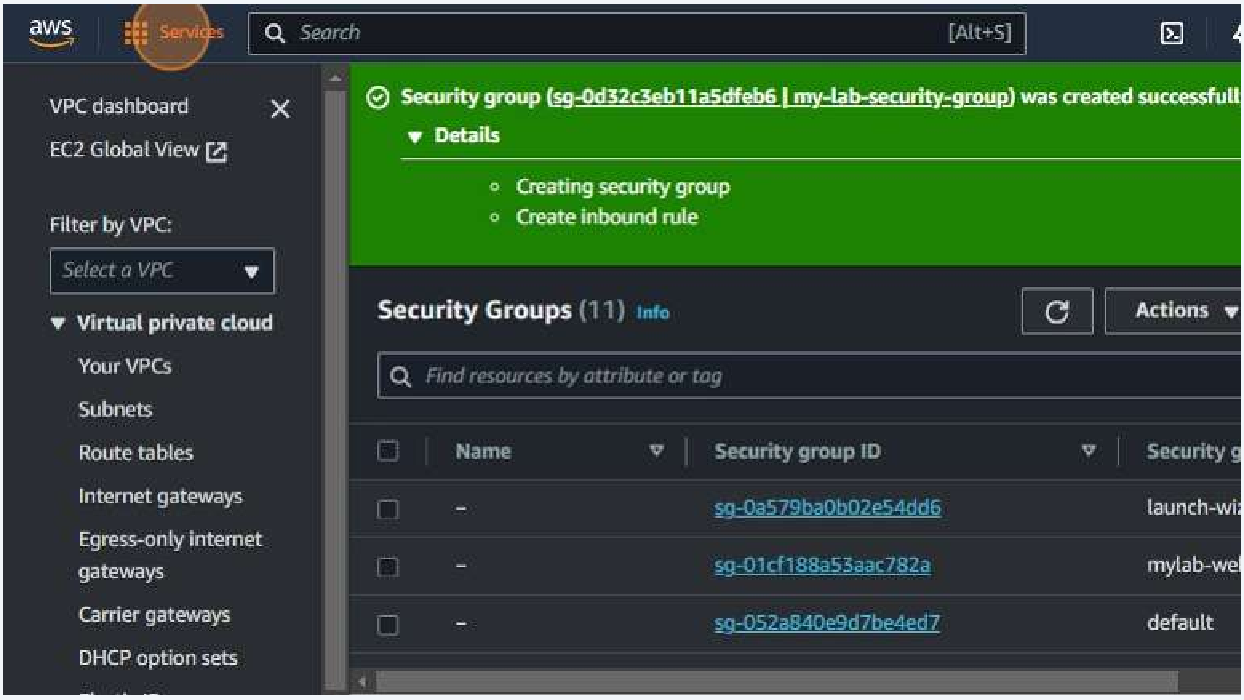
693808211005 | 1 Permission entry

Inbound rules (1)

Search

| ☐ | Name | Security group rule... | IP version |
|---|---|---|---|
| ☐ | - | sgr-03497df20942edc8b | IPv4 |

**191** Click "Services"



Security group (sg-0d32c3eb11a5dfeb6 | my-lab-security-group) was created successfull

Details

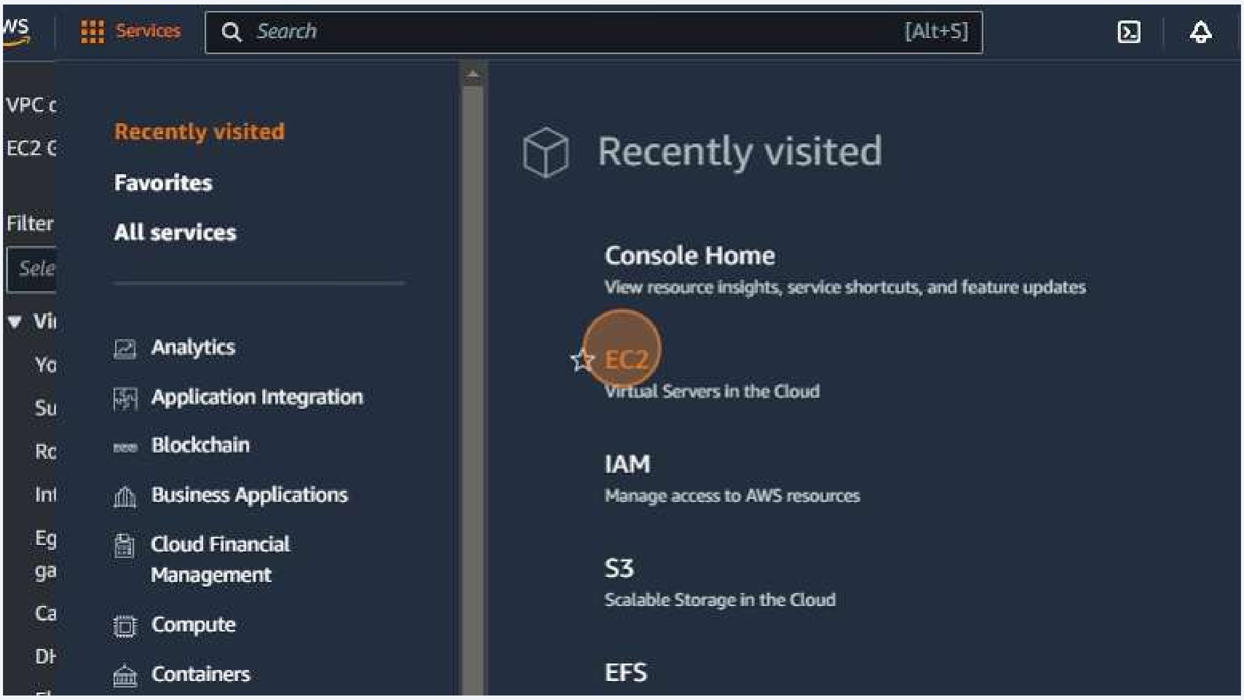
- Creating security group
- Create inbound rule

Security Groups (11) Info

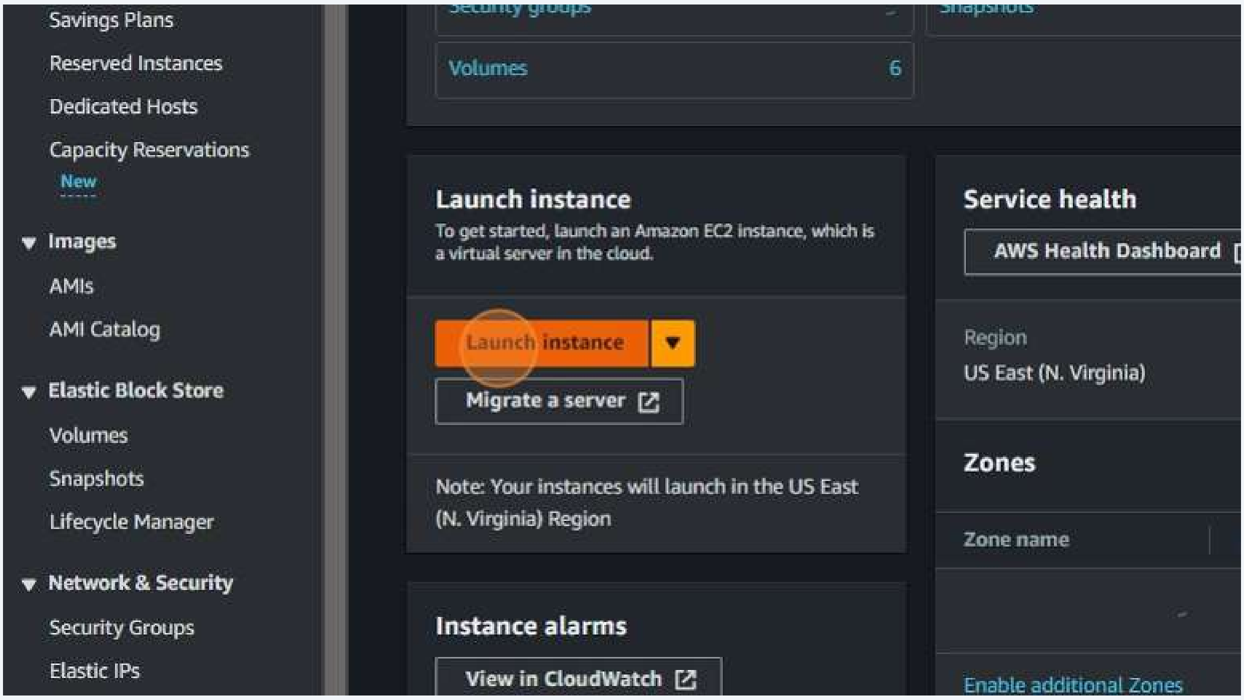
Find resources by attribute or tag

| ☐ | Name | Security group ID | Security g |
|---|---|---|---|
| ☐ | - | sg-0a579ba0b02e54dd6 | launch-wi |
| ☐ | - | sg-01cf188a53aac782a | mylab-we |
| ☐ | - | sg-052a840e9d7be4ed7 | default |

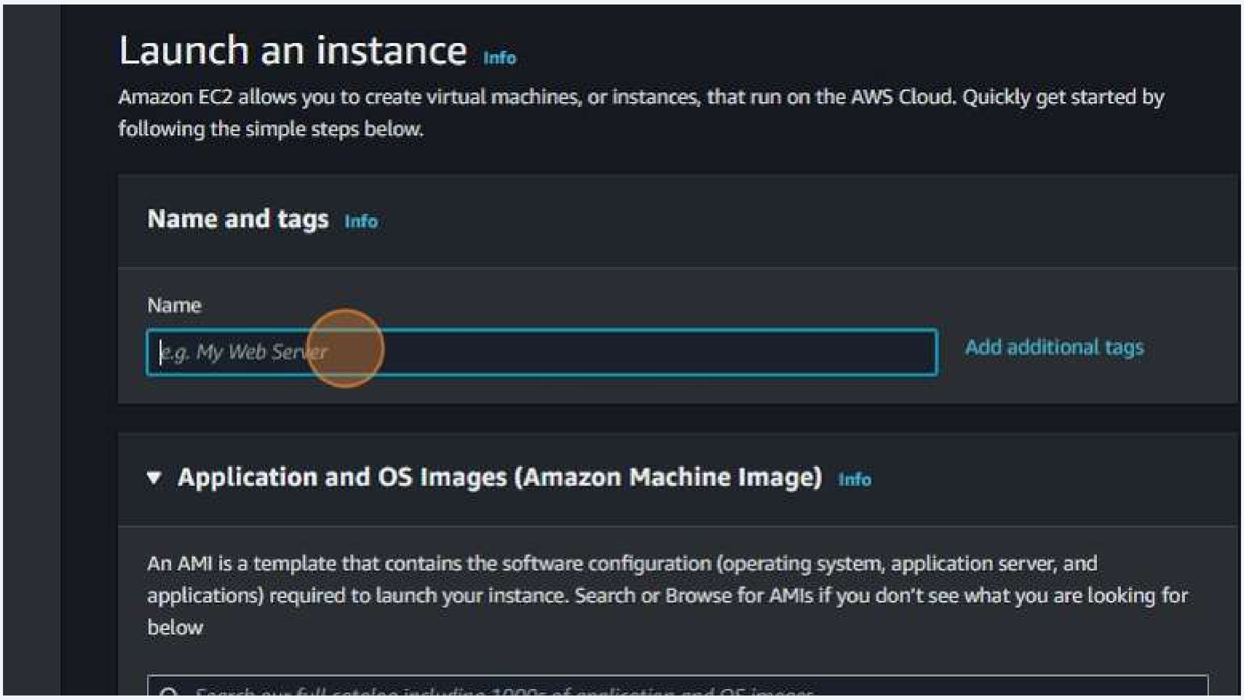
**192** Click "EC2"



**193** Click "Launch instance"



194 Click the "Name" field.



# 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

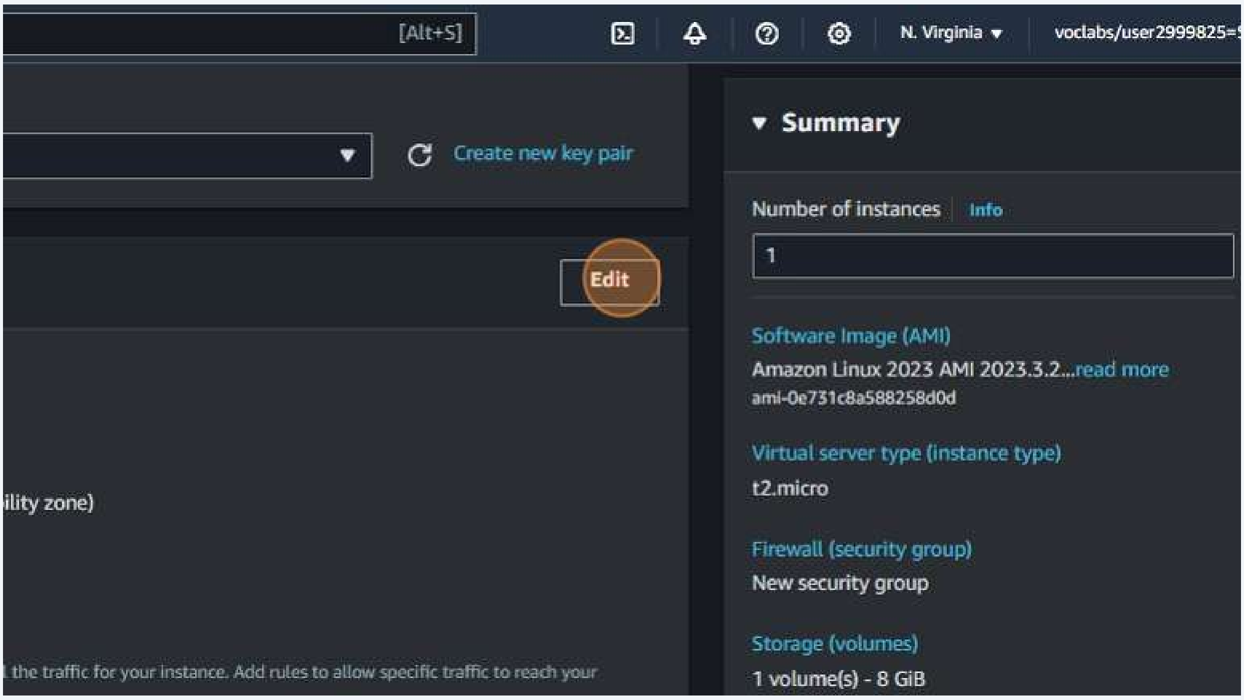
## ▼ Application and OS Images (Amazon Machine Image)

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

195 Type "my-lab-webserver"

**196** Click "Edit"



[Alt+S]

N. Virginia ▾ voclabs/user2999825=

Create new key pair

Edit

ility zone)

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

▾ Summary

Number of instances Info

1

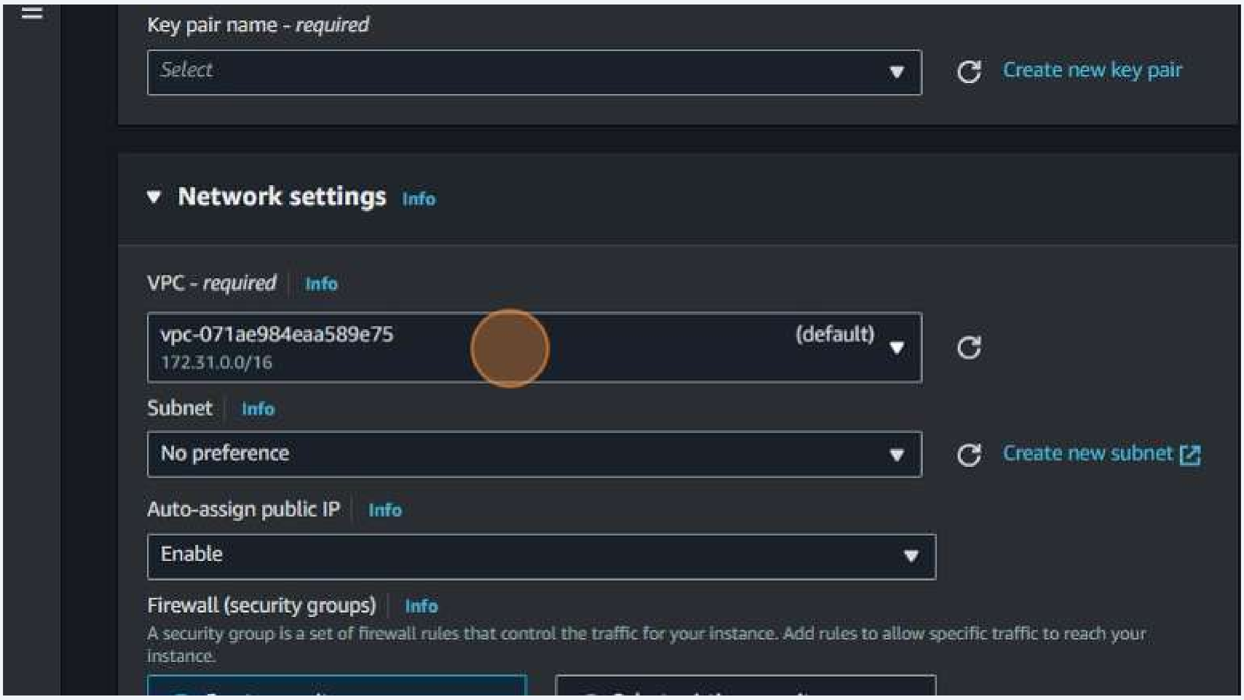
Software Image (AMI)
Amazon Linux 2023 AMI 2023.3.2...read more
ami-0e731c8a588258d0d

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

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

**197** Click "172.31.0.0/16"



Key pair name - *required*

Select ▾ Create new key pair

▾ **Network settings** Info

VPC - *required* Info

vpc-071ae984eaa589e75 (default) ▾
172.31.0.0/16

Subnet Info

No preference ▾ Create new subnet

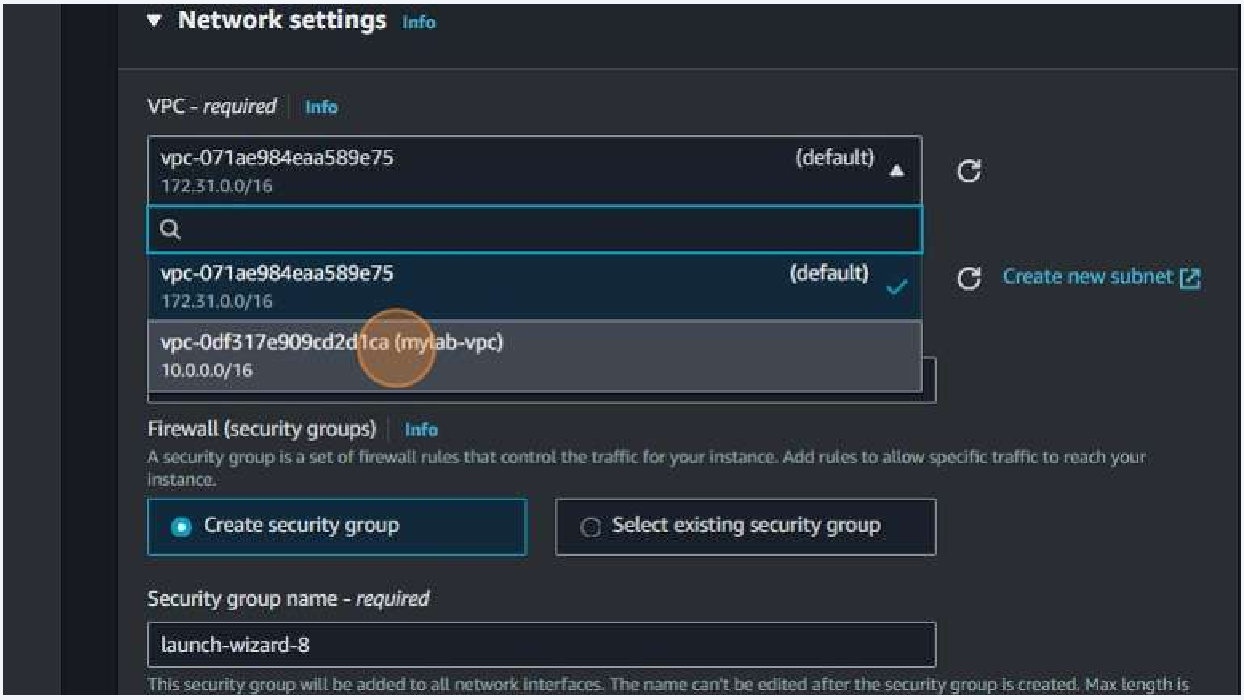
Auto-assign public IP Info

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.

198 Click "vpc-0df317e909cd2d1ca (mylab-vpc)"



▼ Network settings Info

VPC - *required* Info

vpc-071ae984eaa589e75 (default)
172.31.0.0/16

vpc-071ae984eaa589e75 (default) ✓
172.31.0.0/16

vpc-0df317e909cd2d1ca (mylab-vpc)
10.0.0.0/16

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.

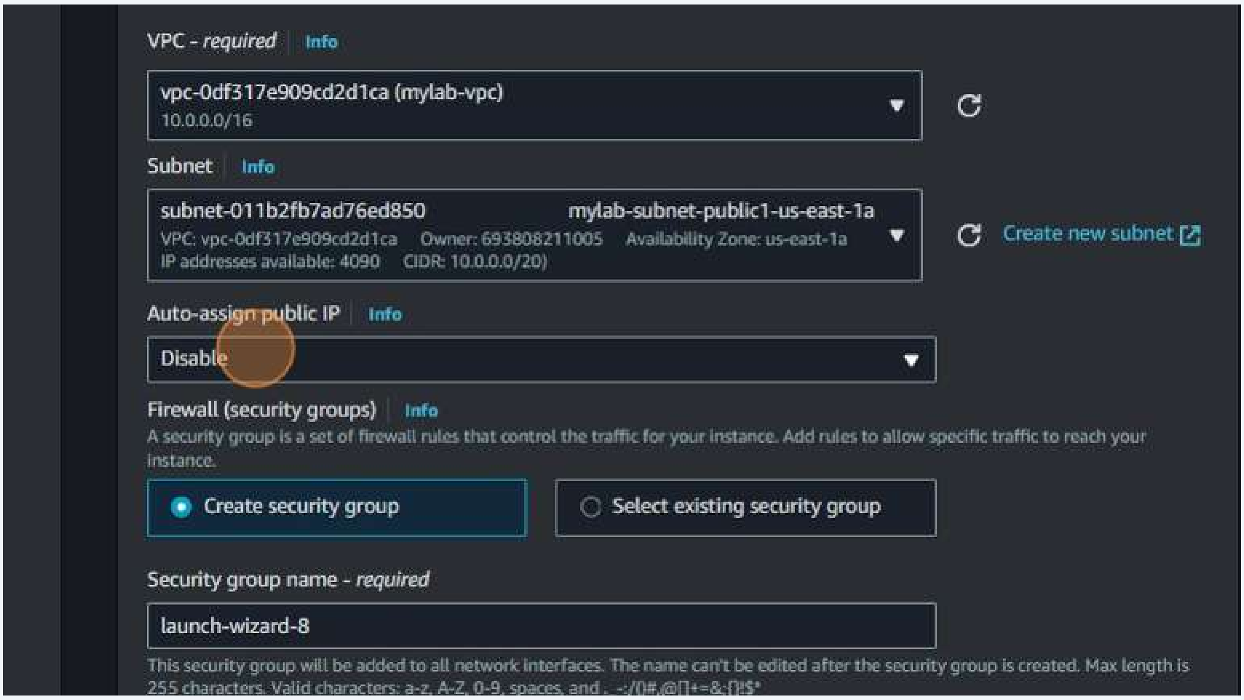
● Create security group ○ Select existing security group

Security group name - *required*

launch-wizard-8

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

199 Click "Disable"



VPC - *required* Info

vpc-0df317e909cd2d1ca (mylab-vpc)
10.0.0.0/16

Subnet Info

subnet-011b2fb7ad76ed850 mylab-subnet-public1-us-east-1a
VPC: vpc-0df317e909cd2d1ca Owner: 693808211005 Availability Zone: us-east-1a
IP addresses available: 4090 CIDR: 10.0.0.0/20)

Auto-assign public IP Info

Disable

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.

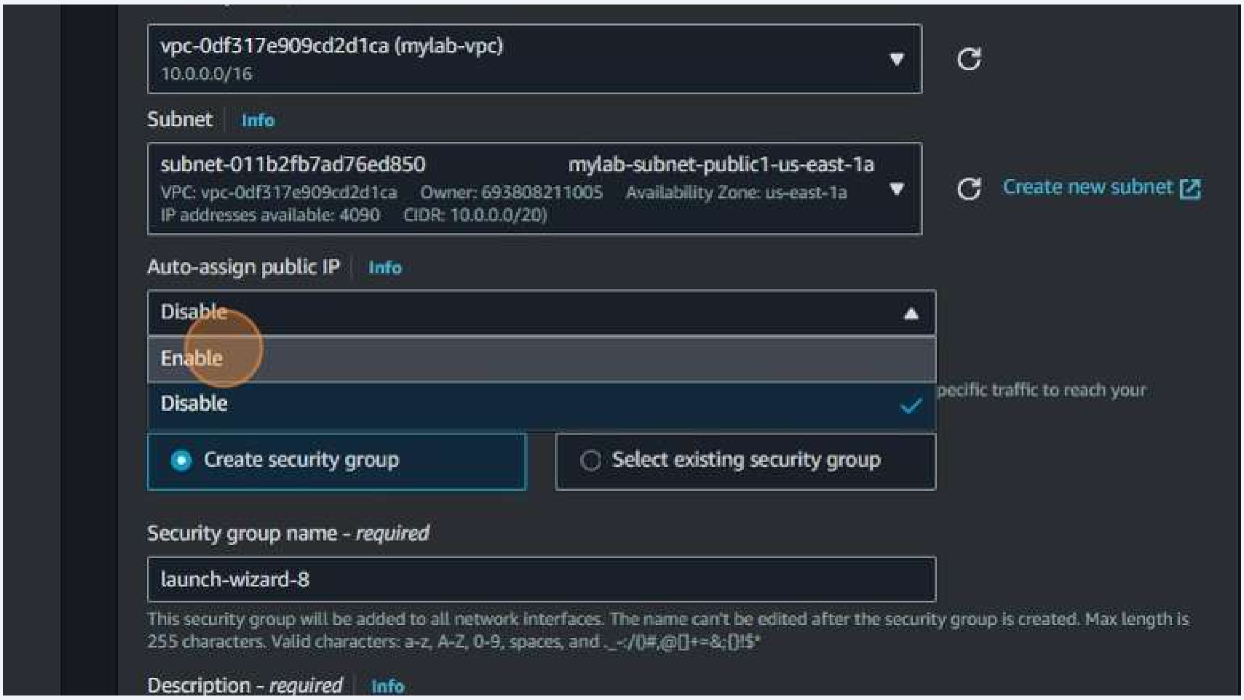
● Create security group ○ Select existing security group

Security group name - *required*

launch-wizard-8

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 . -:/()#,@[]+=&;{}!$*

**200** Click "Enable"



vpc-0df317e909cd2d1ca (mylab-vpc)
10.0.0.0/16

Subnet Info

subnet-011b2fb7ad76ed850 mylab-subnet-public1-us-east-1a
VPC: vpc-0df317e909cd2d1ca Owner: 693808211005 Availability Zone: us-east-1a
IP addresses available: 4090 CIDR: 10.0.0.0/20)

Auto-assign public IP Info

Disable

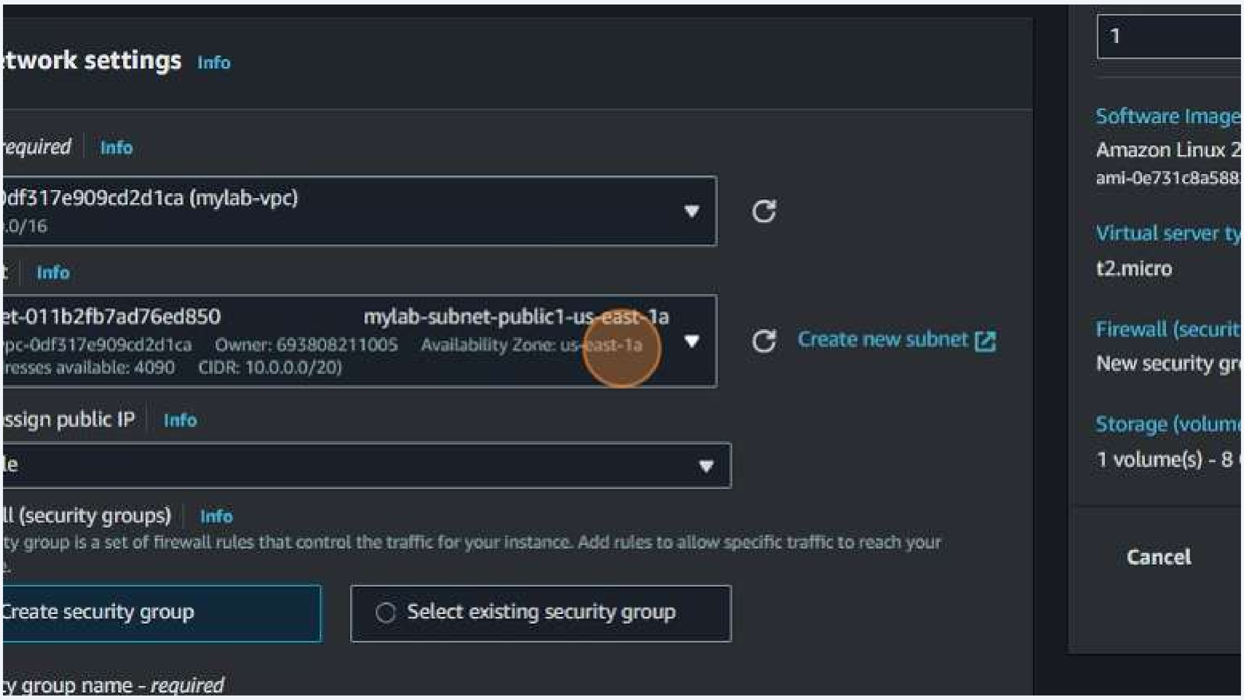
Security group name - *required*

launch-wizard-8

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

**201** Click "Availability Zone: us-east-1a"



twork settings Info

*equired* Info

)df317e909cd2d1ca (mylab-vpc)
.0/16

t Info

et-011b2fb7ad76ed850 mylab-subnet-public1-us-east-1a
pc-0df317e909cd2d1ca Owner: 693808211005 Availability Zone: us-east-1a
resses available: 4090 CIDR: 10.0.0.0/20)

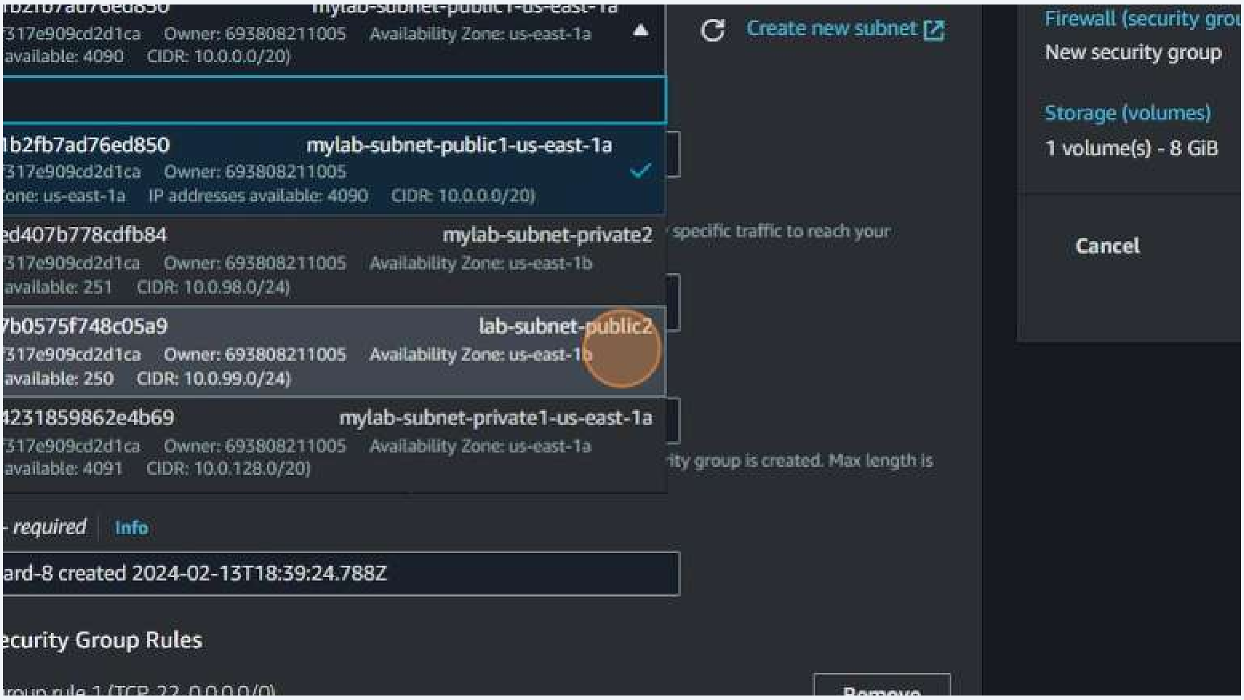
ssign public IP Info

le

ll (security groups) Info
ty group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your
e.

ty group name - *required*

**202** Click "VPC: vpc-0df317e909cd2d1ca
Owner: 693808211005
Availability Zone: us-east-1b
IP addresses available: 250
CIDR: 10.0.99.0/24)"



317e909cd2d1ca Owner: 693808211005 Availability Zone: us-east-1a
available: 4090 CIDR: 10.0.0.0/20)

1b2fb7ad76ed850 mylab-subnet-public1-us-east-1a
317e909cd2d1ca Owner: 693808211005
one: us-east-1a IP addresses available: 4090 CIDR: 10.0.0.0/20) ✓

ed407b778cdfb84 mylab-subnet-private2
317e909cd2d1ca Owner: 693808211005 Availability Zone: us-east-1b
available: 251 CIDR: 10.0.98.0/24)

7b0575f748c05a9 lab-subnet-public2
317e909cd2d1ca Owner: 693808211005 Availability Zone: us-east-1b
available: 250 CIDR: 10.0.99.0/24)

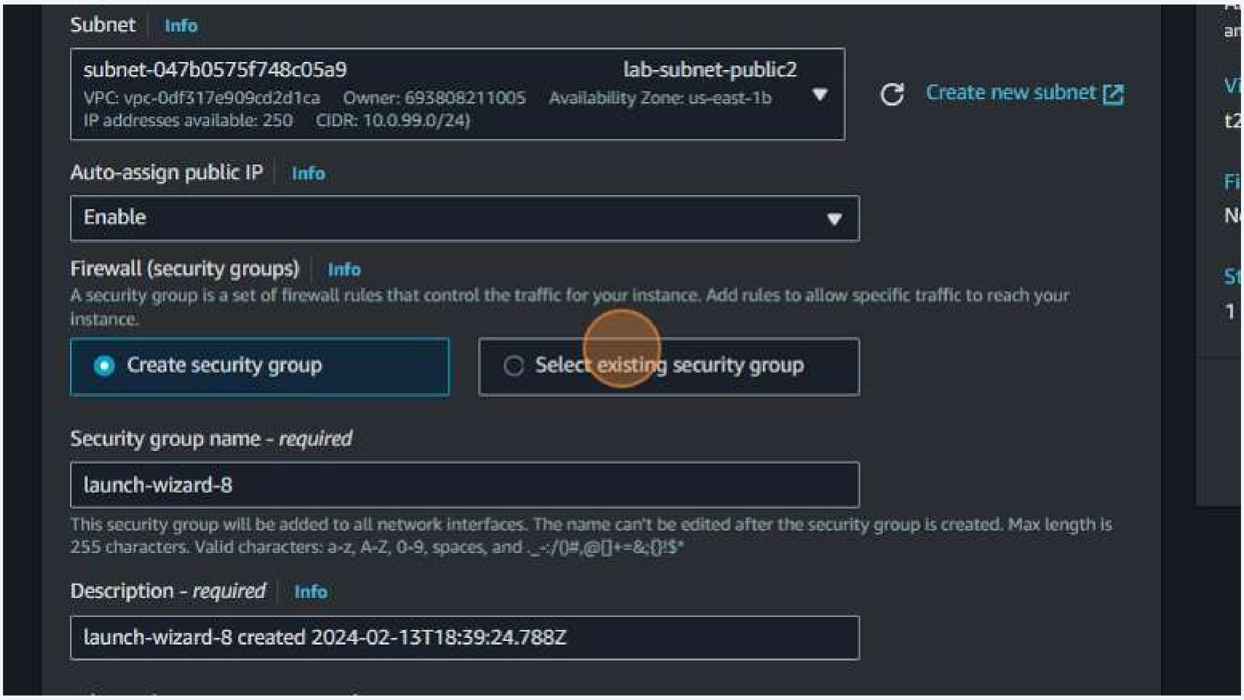
4231859862e4b69 mylab-subnet-private1-us-east-1a
317e909cd2d1ca Owner: 693808211005 Availability Zone: us-east-1a
available: 4091 CIDR: 10.0.128.0/20)

- required Info

ard-8 created 2024-02-13T18:39:24.788Z

ecurity Group Rules

**203** Click "Select existing security group"



Subnet Info

subnet-047b0575f748c05a9 lab-subnet-public2
VPC: vpc-0df317e909cd2d1ca Owner: 693808211005 Availability Zone: us-east-1b
IP addresses available: 250 CIDR: 10.0.99.0/24)

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*

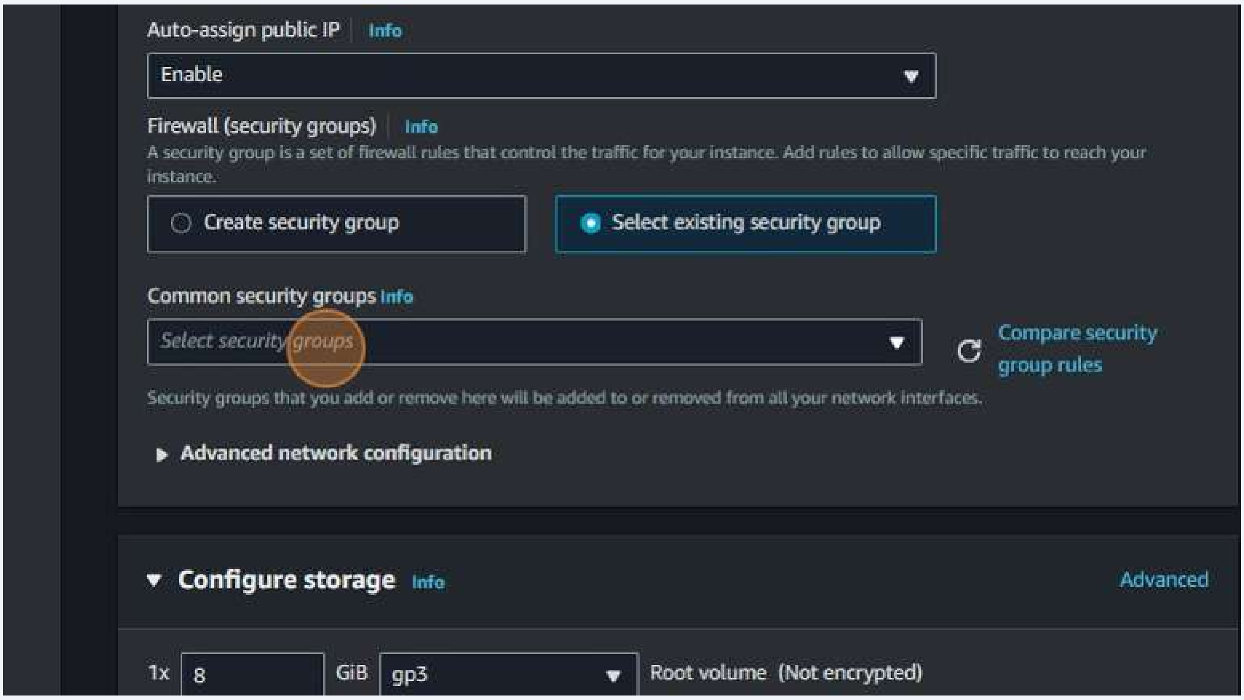
launch-wizard-8

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-8 created 2024-02-13T18:39:24.788Z

**204** Click "Select security groups"



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

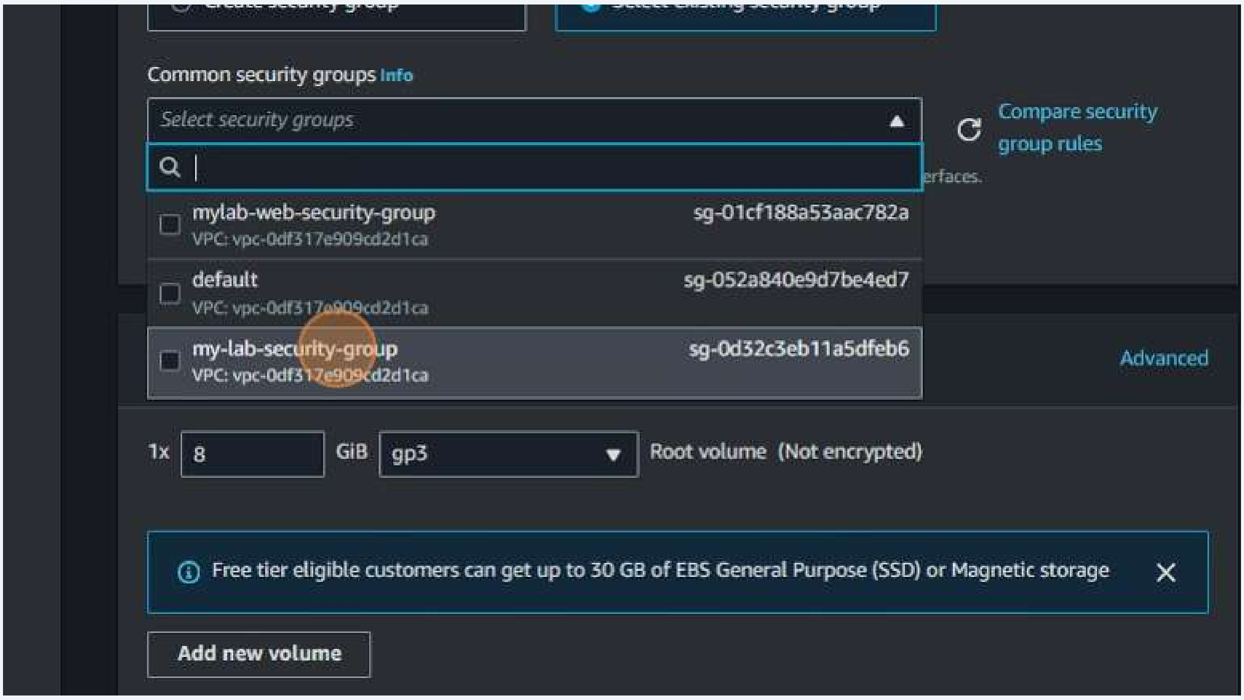
Common security groups Info

Select security groups

Security groups that you add or remove here will be added to or removed from all your network interfaces.

Compare security group rules
Advanced network configuration
Configure storage Info
Advanced
1x 8 GiB gp3 Root volume (Not encrypted)

**205** Click "my-lab-security-group"



Common security groups Info

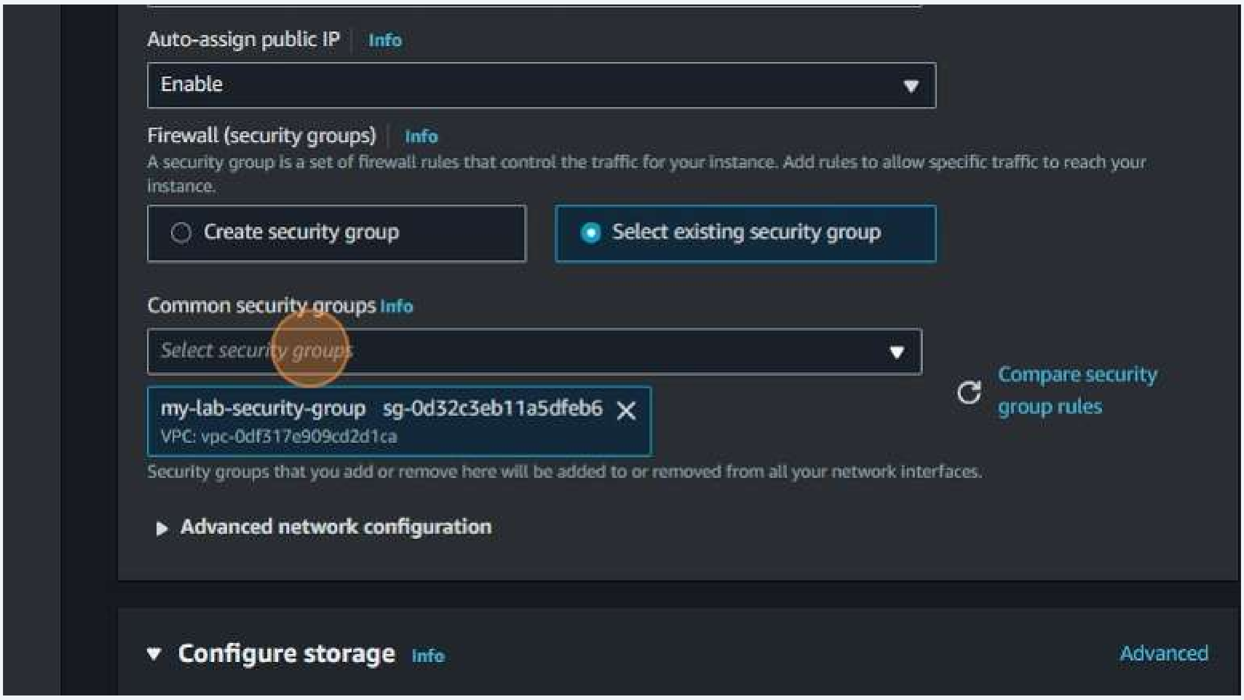
Select security groups

| | |
|---|---|
| □ mylab-web-security-group<br>VPC: vpc-0df317e909cd2d1ca | sg-01cf188a53aac782a |
| □ default<br>VPC: vpc-0df317e909cd2d1ca | sg-052a840e9d7be4ed7 |
| □ my-lab-security-group<br>VPC: vpc-0df317e909cd2d1ca | sg-0d32c3eb11a5dfeb6 |

1x 8 GiB gp3 Root volume (Not encrypted)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

**206** Click "Select security groups"



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

Common security groups Info

Select security groups

my-lab-security-group sg-0d32c3eb11a5dfeb6
VPC: vpc-0df317e909cd2d1ca

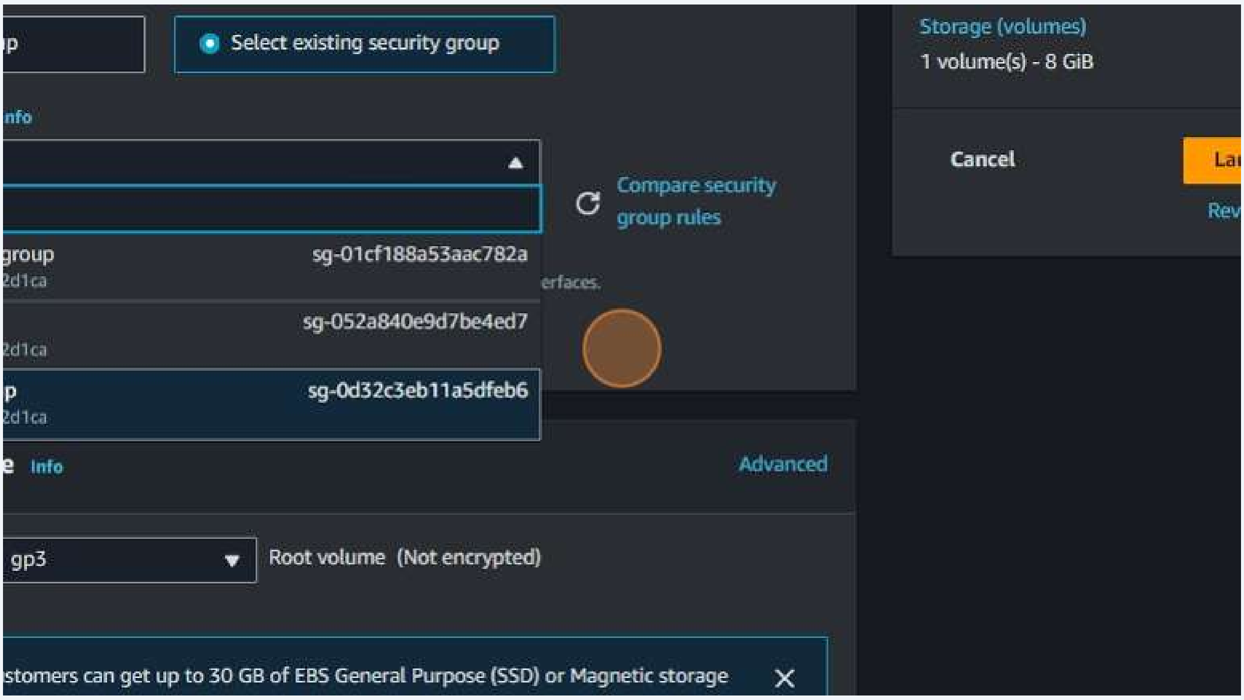
Compare security group rules

Security groups that you add or remove here will be added to or removed from all your network interfaces.

▶ Advanced network configuration

▼ Configure storage Info Advanced

**207** Click here.



● Select existing security group

nfo

group sg-01cf188a53aac782a
2d1ca

sg-052a840e9d7be4ed7
2d1ca

p sg-0d32c3eb11a5dfeb6
2d1ca

Compare security group rules

erfaces.

e Info Advanced

gp3 Root volume (Not encrypted)

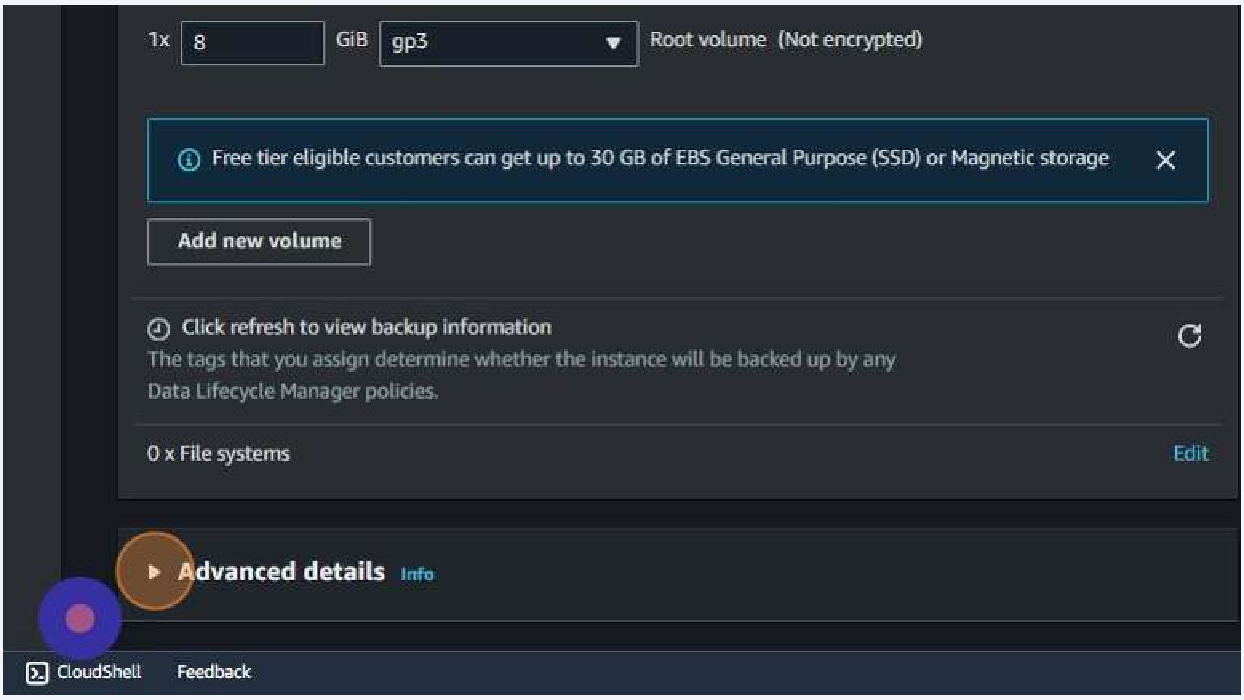
stomers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

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

Cancel La

Rev

208 Click here.



1x 8 GiB gp3 Root volume (Not encrypted)

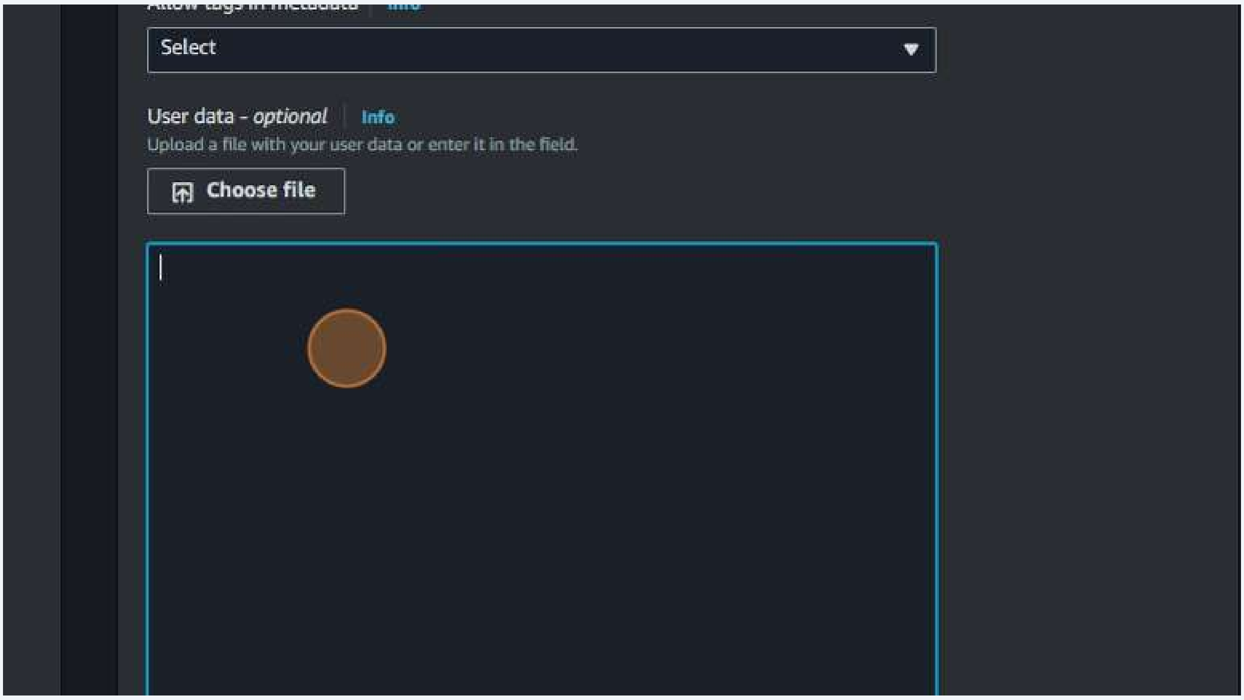
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

Click refresh to view backup information

The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems

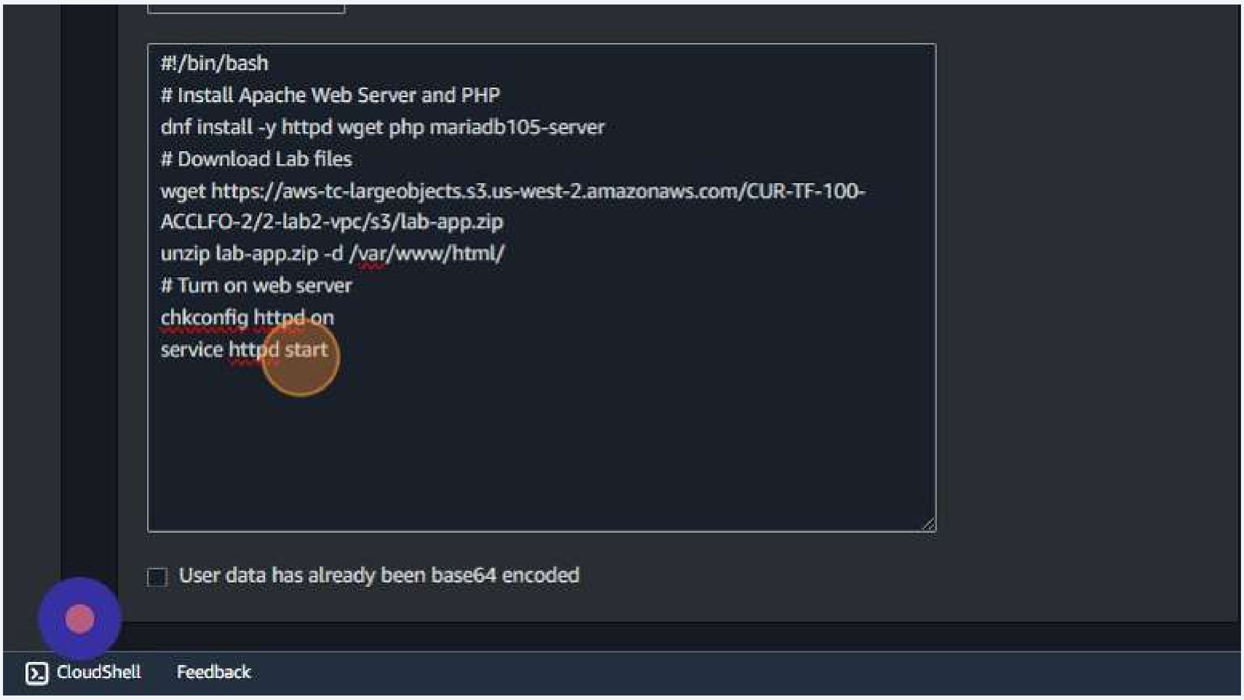
209 Click the "User data - optional" field.



User data - *optional*

Upload a file with your user data or enter it in the field.

210 Click the "User data - optional" field.

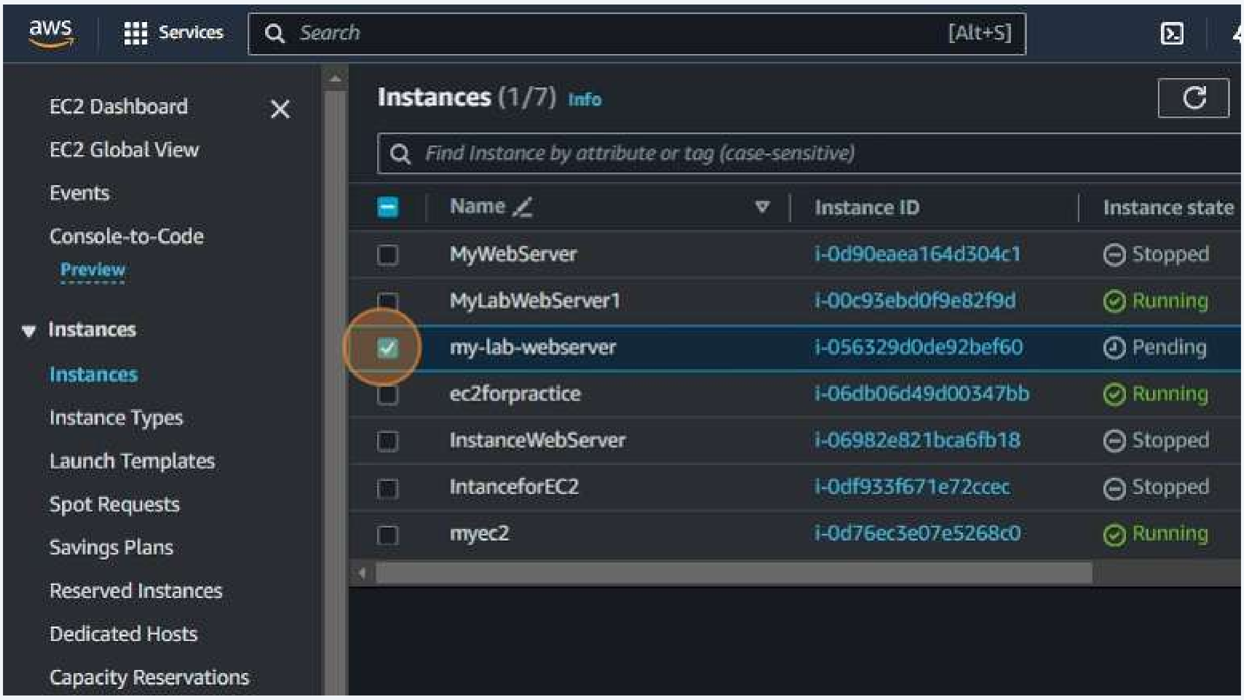


```
#!/bin/bash
# Install Apache Web Server and PHP
dnf install -y httpd wget php mariadb105-server
# Download Lab files
wget https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-100-
ACCLFO-2/2-lab2-vpc/s3/lab-app.zip
unzip lab-app.zip -d /var/www/html/
# Turn on web server
chkconfig httpd on
service httpd start
```

□ User data has already been base64 encoded

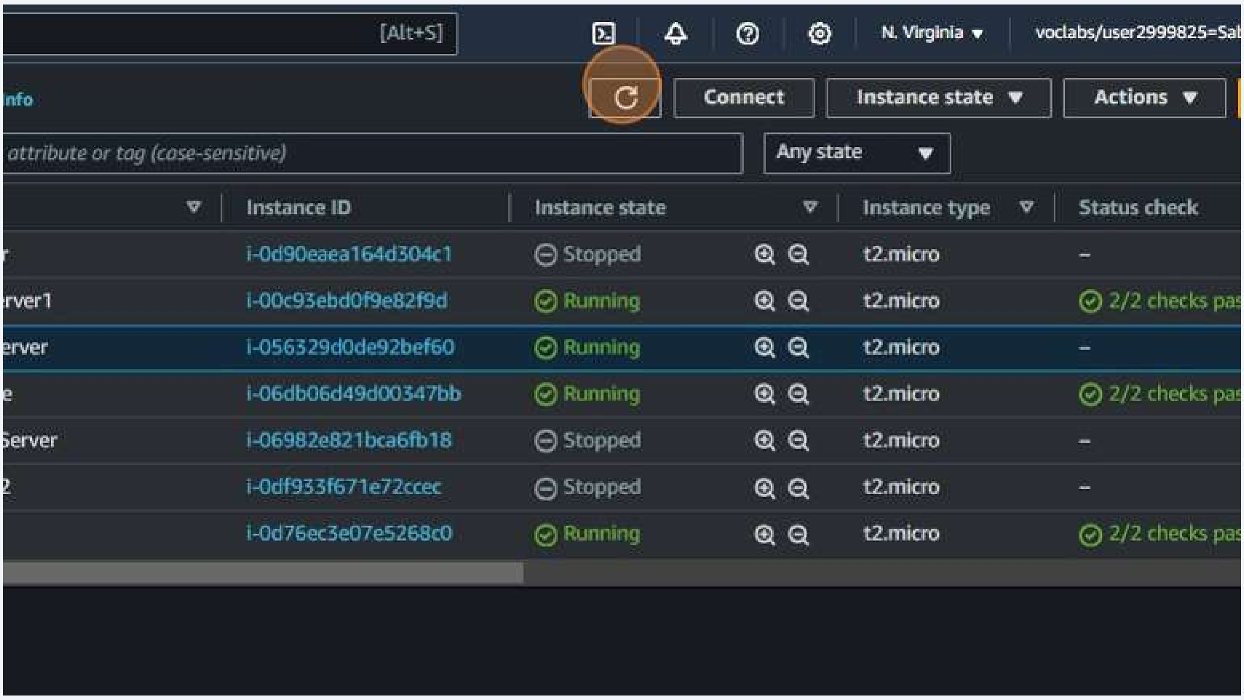
211 Navigate to [https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:v=3;$case=tags:true%5C,client:false;$regex=tags:false%5C,client:false](https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:v=3;$case=tags:true%5C,client:false;$regex=tags:false%5C,client:false)

**212** Click this checkbox.



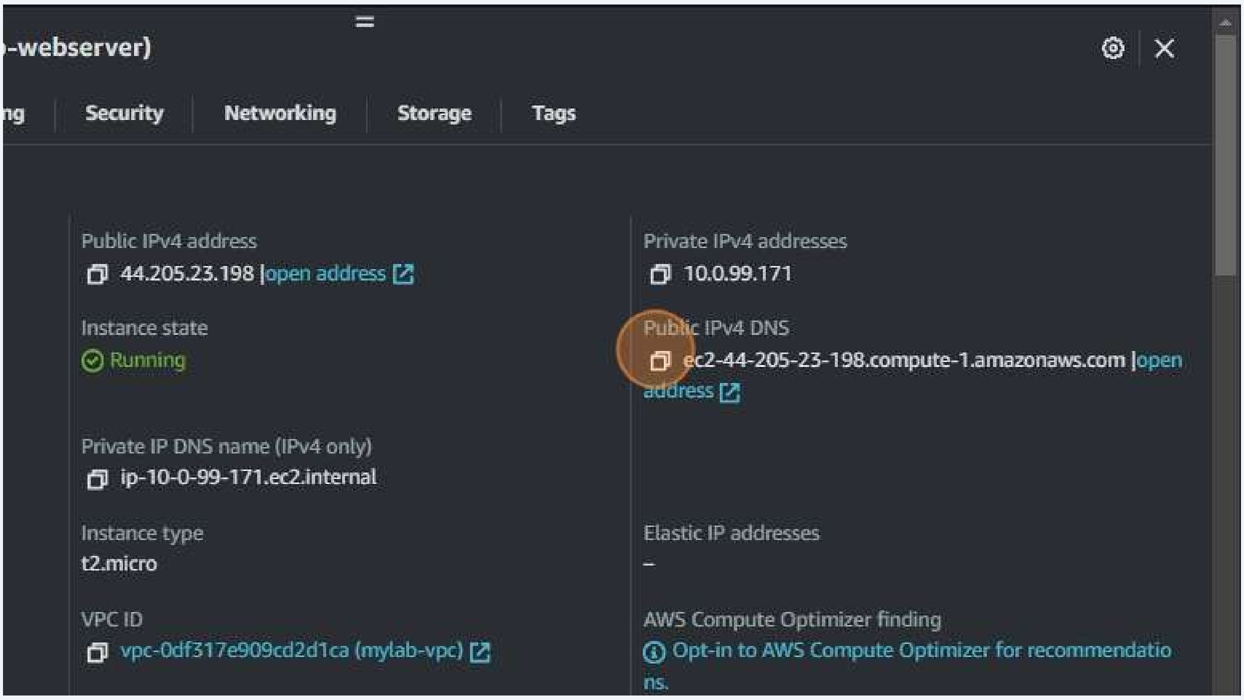
|  | Name | Instance ID | Instance state |
|---|---|---|---|
| □ | MyWebServer | i-0d90eaea164d304c1 | Stopped |
| □ | MyLabWebServer1 | i-00c93ebd0f9e82f9d | Running |
| ☑ | my-lab-webserver | i-056329d0de92bef60 | Pending |
| □ | ec2forpractice | i-06db06d49d00347bb | Running |
| □ | InstanceWebServer | i-06982e821bca6fb18 | Stopped |
| □ | IntanceforEC2 | i-0df933f671e72ccec | Stopped |
| □ | myec2 | i-0d76ec3e07e5268c0 | Running |

**213** Click here.



|  | Instance ID | Instance state | Instance type | Status check |
|---|---|---|---|---|
| r | i-0d90eaea164d304c1 | Stopped | t2.micro | – |
| rver1 | i-00c93ebd0f9e82f9d | Running | t2.micro | 2/2 checks pas |
| erver | i-056329d0de92bef60 | Running | t2.micro | – |
| e | i-06db06d49d00347bb | Running | t2.micro | 2/2 checks pas |
| Server | i-06982e821bca6fb18 | Stopped | t2.micro | – |
| 2 | i-0df933f671e72ccec | Stopped | t2.micro | – |
|  | i-0d76ec3e07e5268c0 | Running | t2.micro | 2/2 checks pas |

214 Click here.



-webserver)

Public IPv4 address
44.205.23.198 |open address

Private IPv4 addresses
10.0.99.171

Instance state
Running

Public IPv4 DNS
ec2-44-205-23-198.compute-1.amazonaws.com |open address

Private IP DNS name (IPv4 only)
ip-10-0-99-171.ec2.internal

Instance type
t2.micro

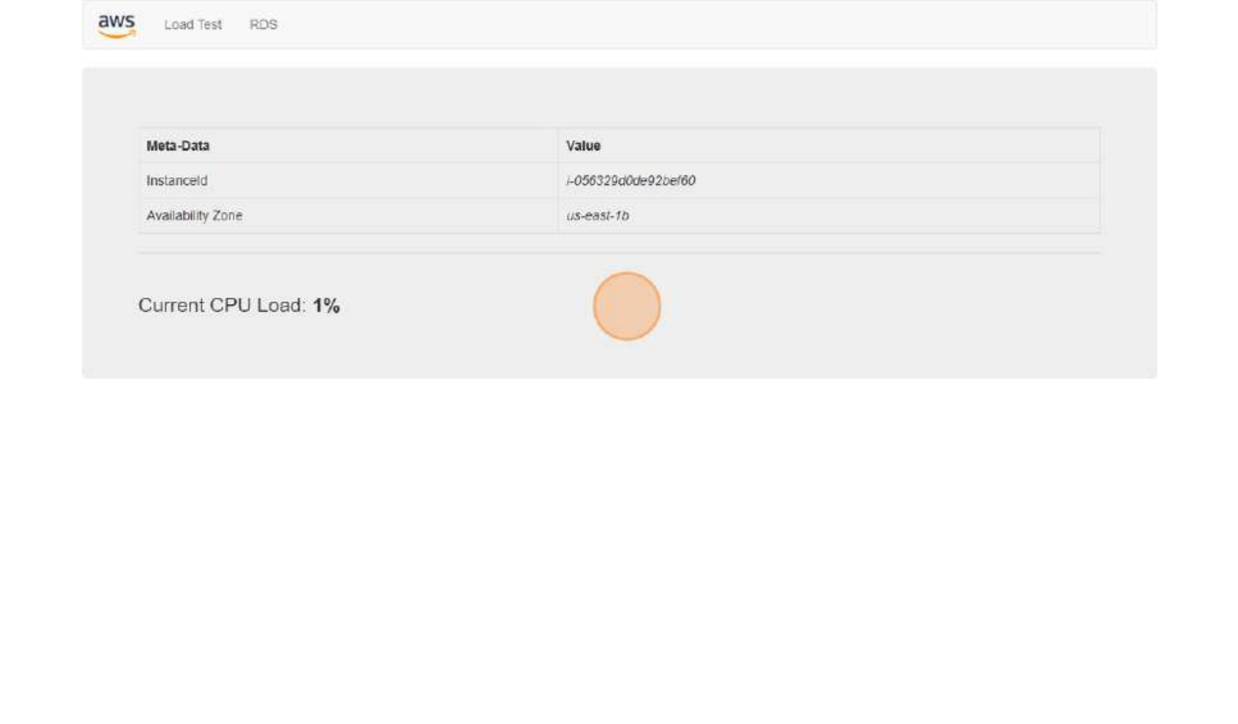
Elastic IP addresses
–

VPC ID
vpc-0df317e909cd2d1ca (mylab-vpc)

AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations.

215 In a new tab, navigate to [http://ec2-44-205-23-198.compute-1.amazonaws.com/](http://ec2-44-205-23-198.compute-1.amazonaws.com/)

**216** Click "Current CPU Load: 1%"



| Meta-Data | Value |
|---|---|
| InstanceId | i-056329d0de92bef60 |
| Availability Zone | us-east-1b |

Current CPU Load: **1%**