

Create a Bucket on AWS S3

Scribe 

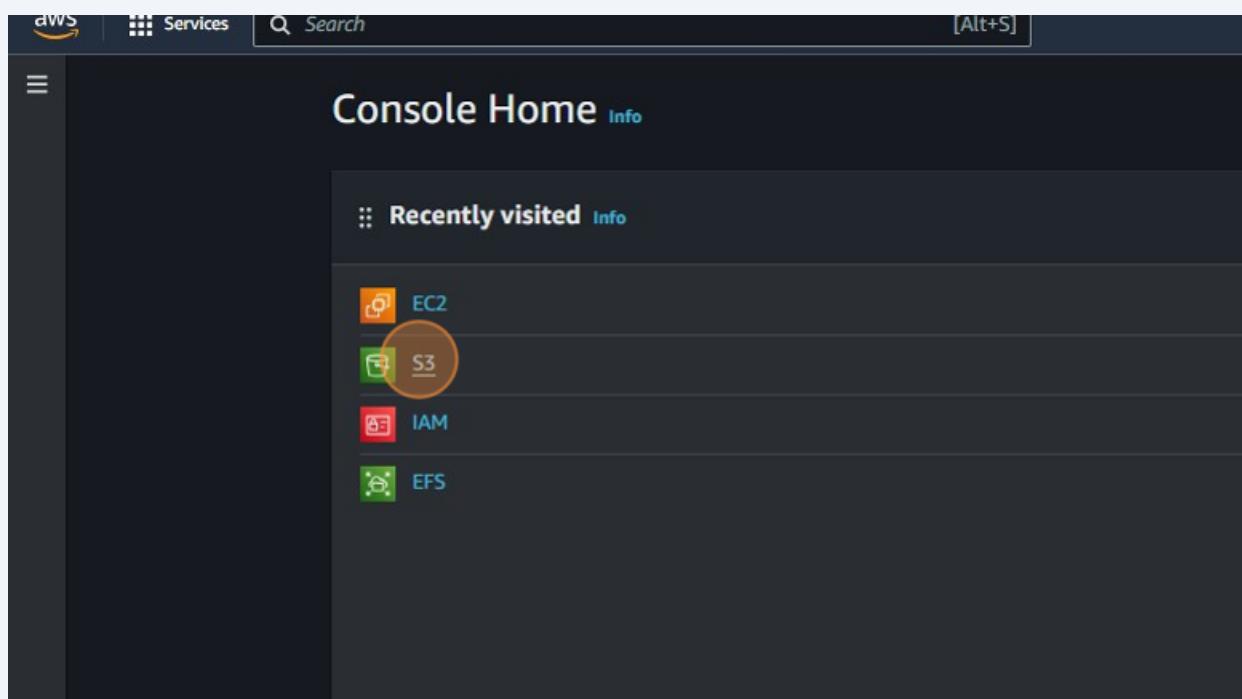
1

Navigate to

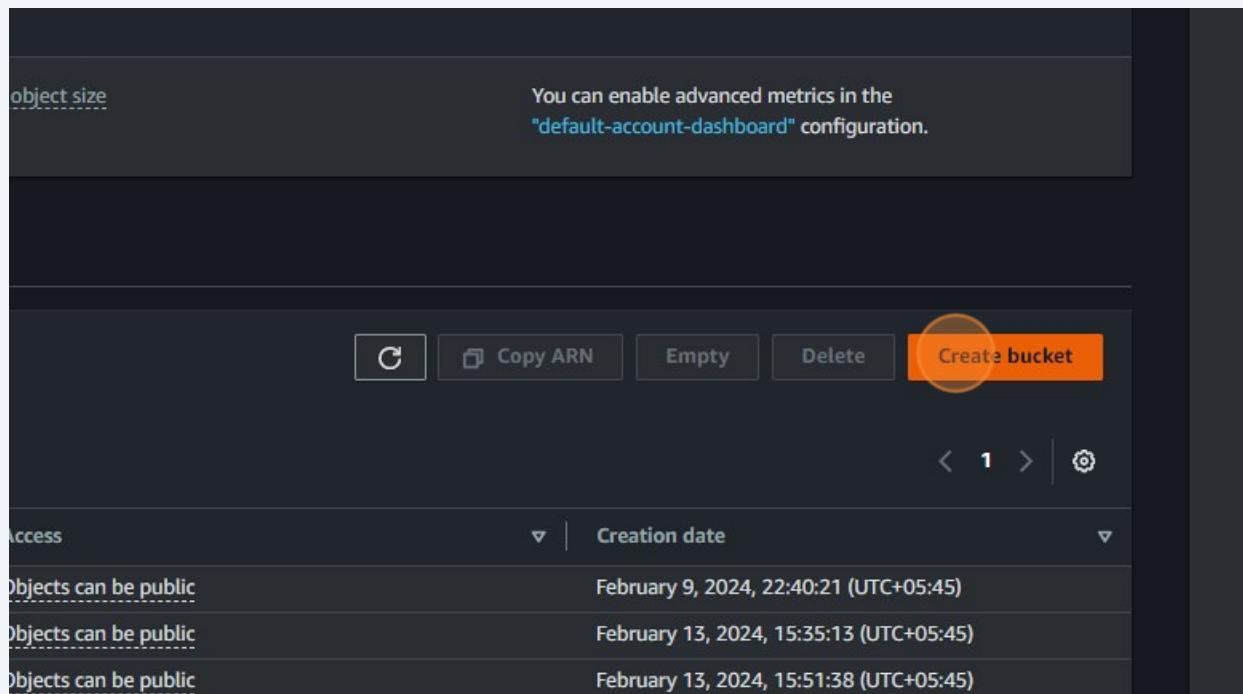
<https://us-east-1.console.aws.amazon.com/console/home?region=us-east-1>

2

Click "S3"

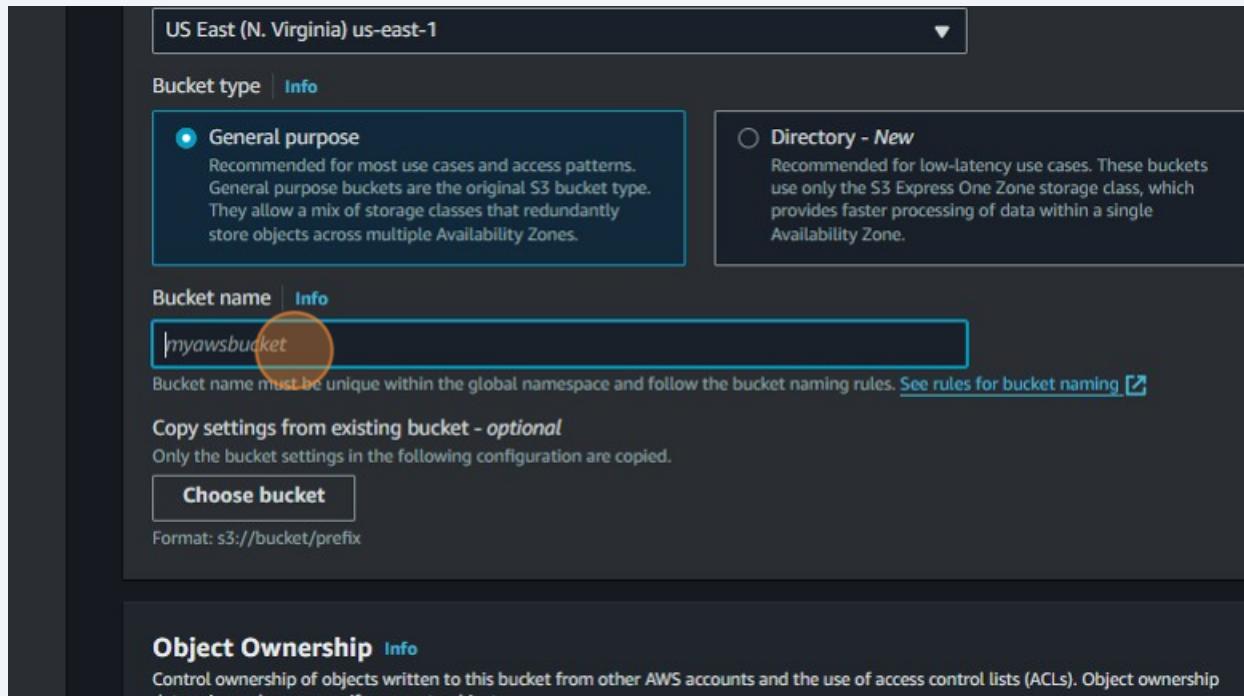


3 Click "Create bucket"



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

- 5 Click the "Bucket name" field.



- 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 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](#)

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

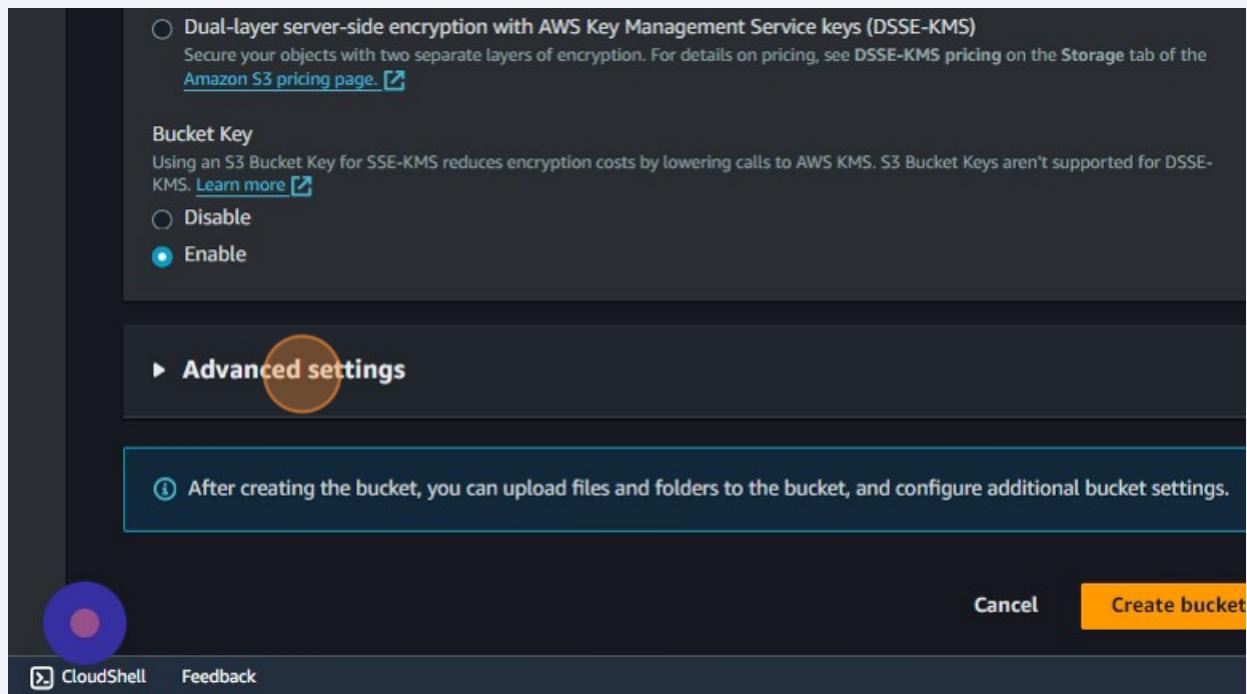
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access 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.

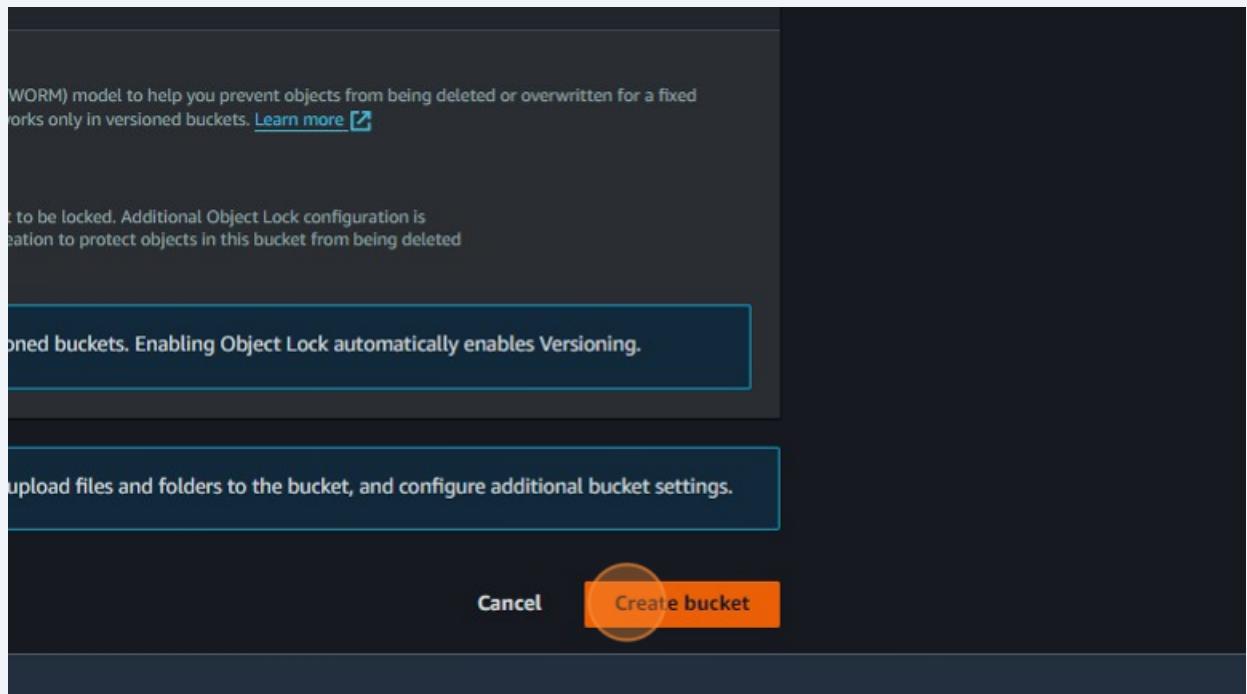
- Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing 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.

 CloudShell [Feedback](#)

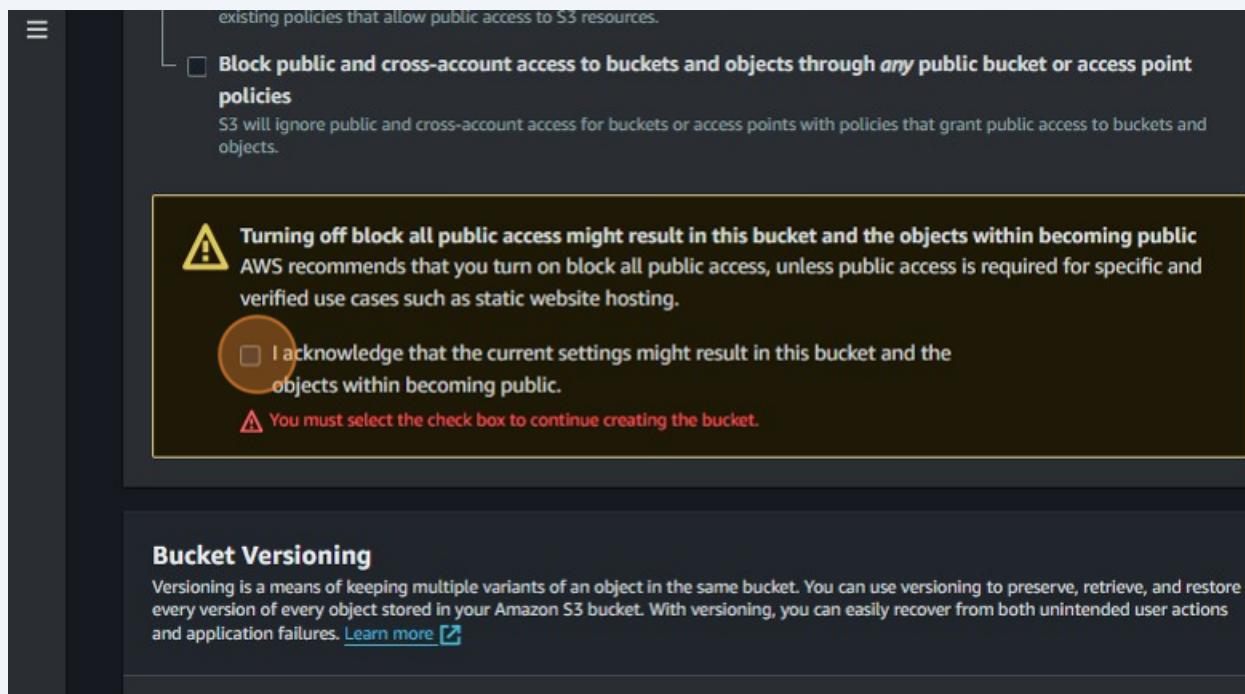
11 Click "Advanced settings"



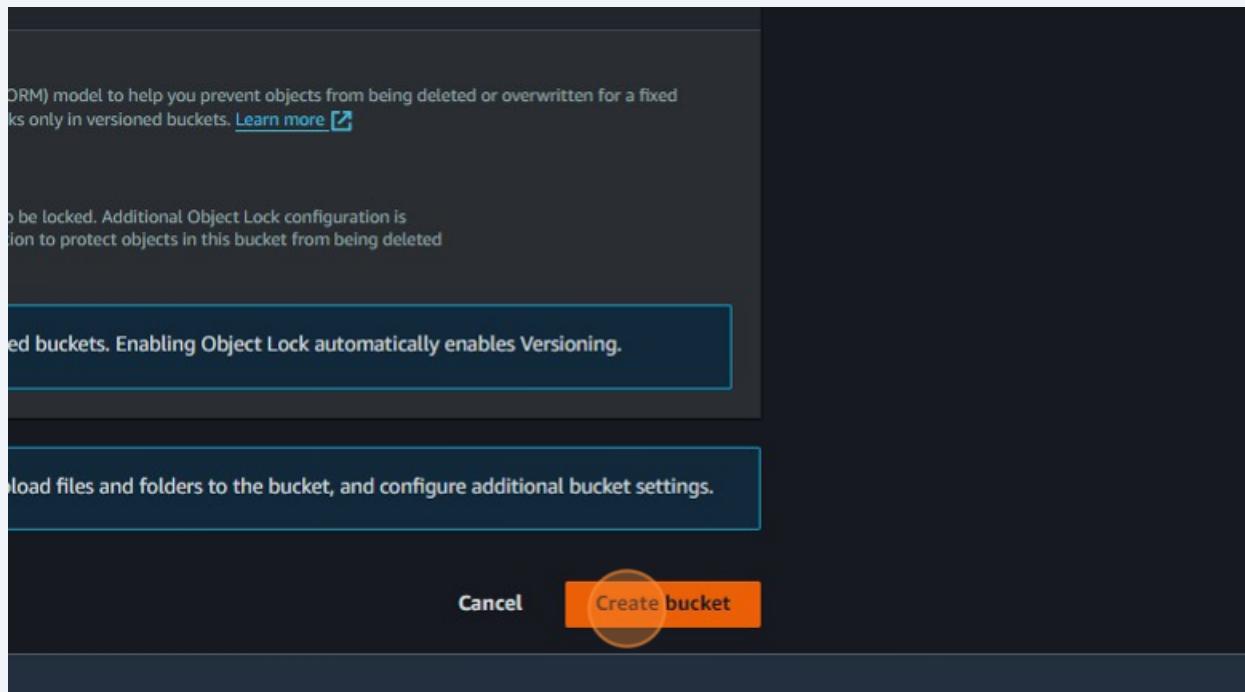
12 Click "Create bucket"



13 Click this checkbox.



14 Click "Create bucket"



15 Click "my-s3-bucket-files"

General purpose buckets (4) [Info](#)
Buckets are containers for data stored in S3. [Learn more](#)

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

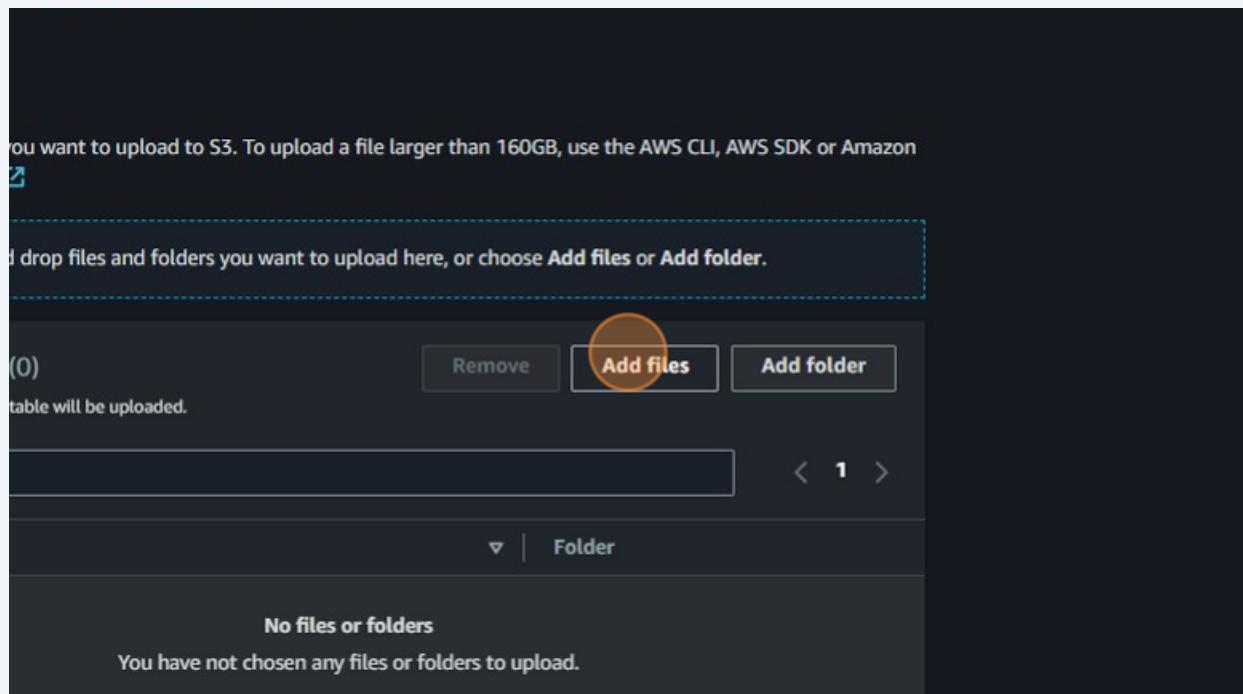
16 Click "Upload"

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](#)

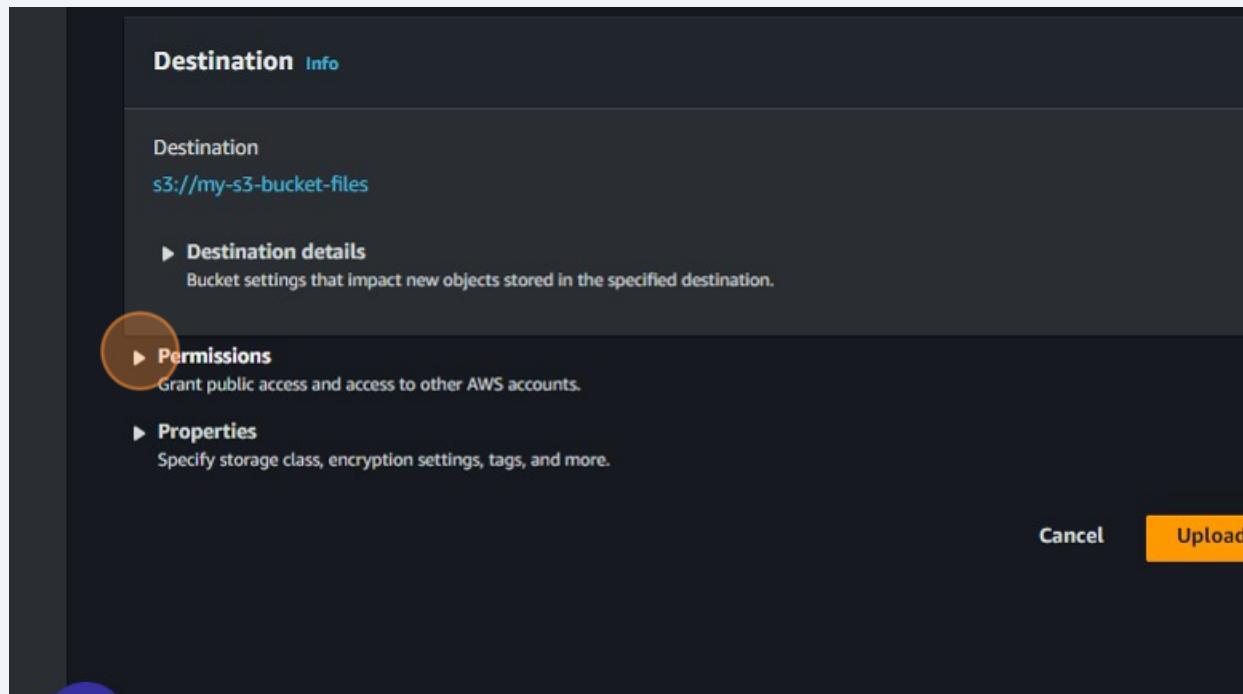
Last modified	Size
No objects	
You don't have any objects in this bucket.	

[Upload](#)

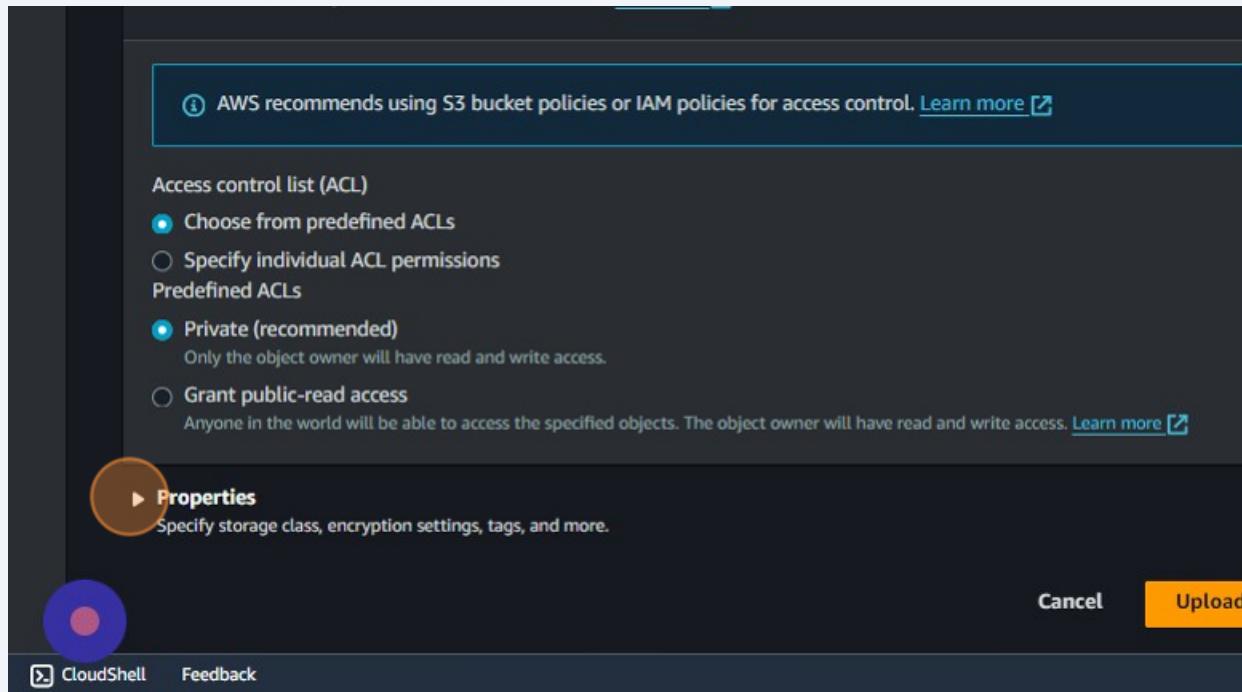
17 Click "Add files"



18 Click here.



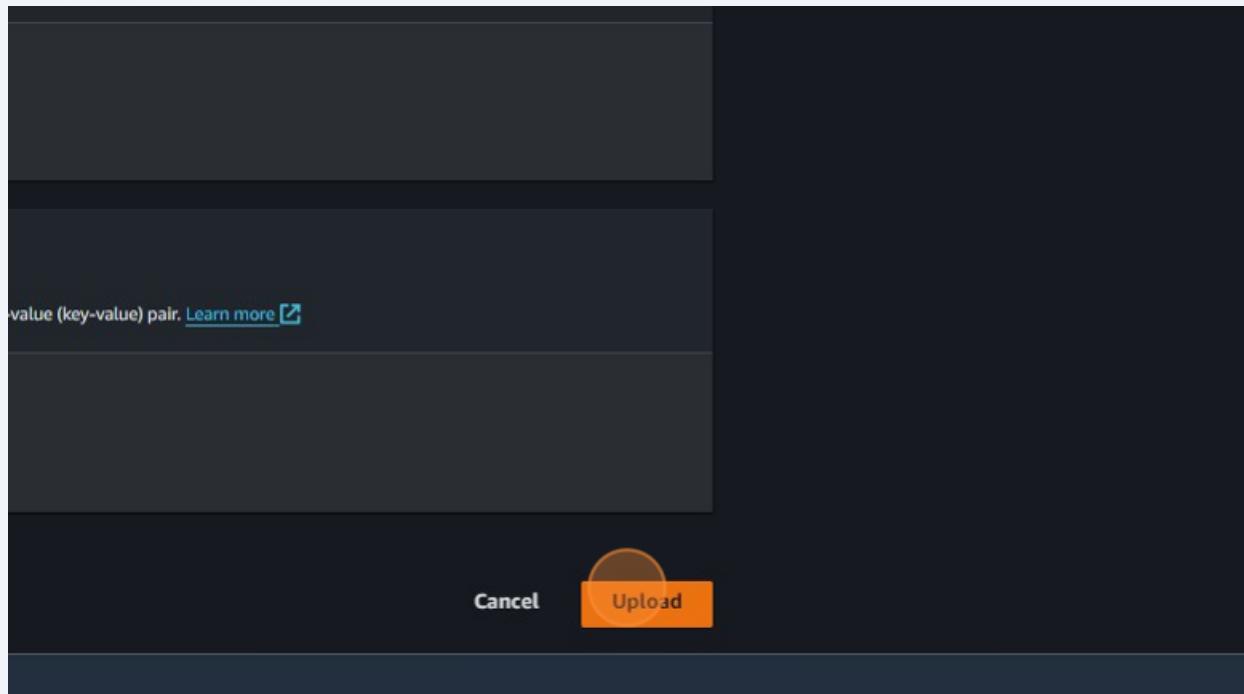
19 Click here.



20 Click "Table Selection Select STANDARD"

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

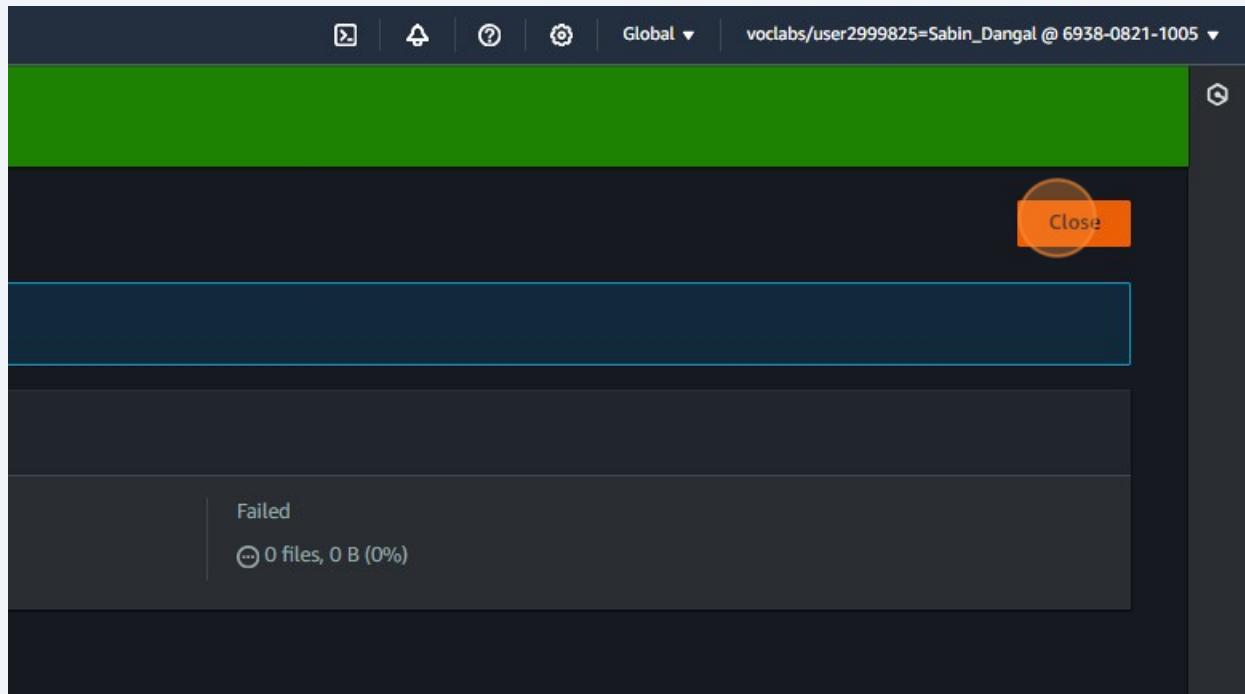
21 Click "Upload"



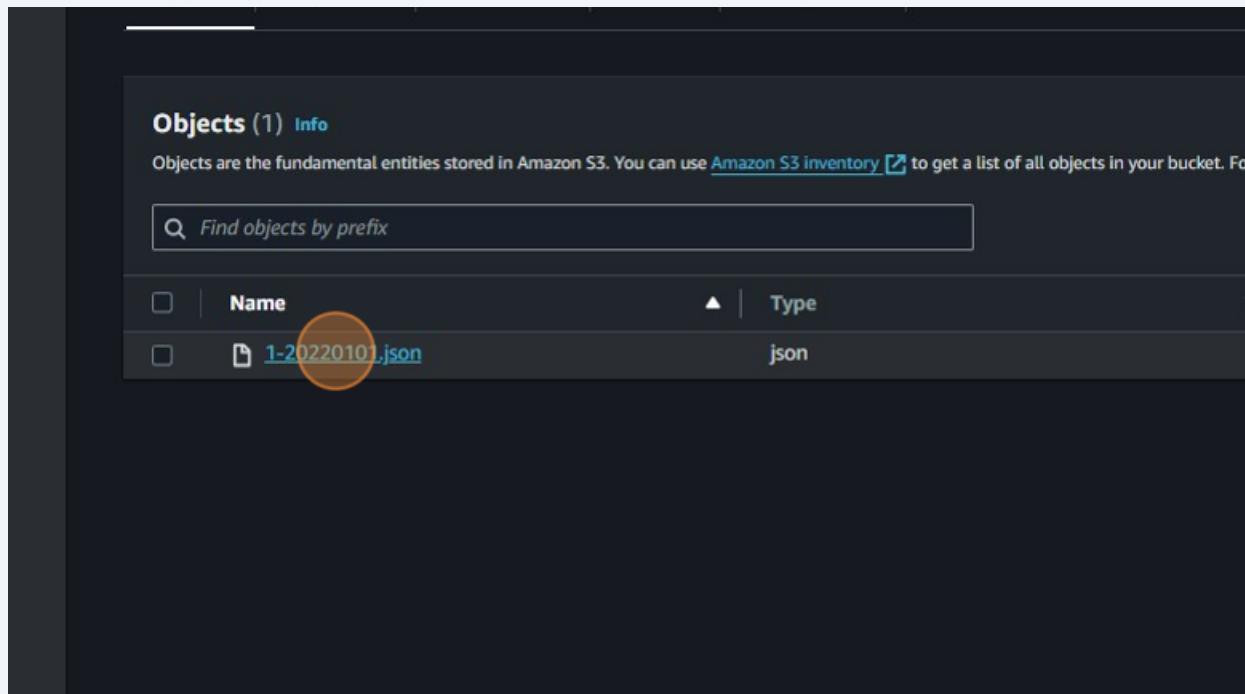
22 Click "View details below."

A screenshot of the AWS S3 "Upload: status" page. The top navigation bar includes the AWS logo, "Services" menu, a search bar, and a keyboard shortcut "[Alt+S]". A green success message box is displayed, stating "Upload succeeded" and "View details below.", with the "View details below" link highlighted by a yellow circle. The main content area is titled "Upload: status" and contains a summary message: "The information below will no longer be available after you navigate away from this page." Below this is a "Summary" section showing the destination as "s3://my-s3-bucket-files" and the result as "Succeeded" with "1 file, 94.0 B (1)". Navigation tabs at the bottom include "Files and folders" and "Configuration".

23 Click "Close"



24 Click "1-20220101.json"



25 Click here.

The screenshot shows the AWS S3 Object Details page for the file '1-20220101.json'. The object details are as follows:

- 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

Below the object details, there is a section titled 'Object management overview' with the subtext: 'The following bucket properties and object management configurations impact the behavior of this object.'

26 Click "Permissions"

The screenshot shows the AWS S3 Object Permissions tab for the file '1-20220101.json'. The navigation path is: Amazon S3 > Buckets > my-s3-bucket-files > 1-20220101.json. The 'Permissions' tab is highlighted with an orange circle. The object overview details are identical to the previous screenshot:

- Owner: awslabsc0w6979671t1703211308
- AWS Region: US East (N. Virginia) us-east-1
- Last modified: February 13, 2024, 22:02:36 (UTC+05:45)

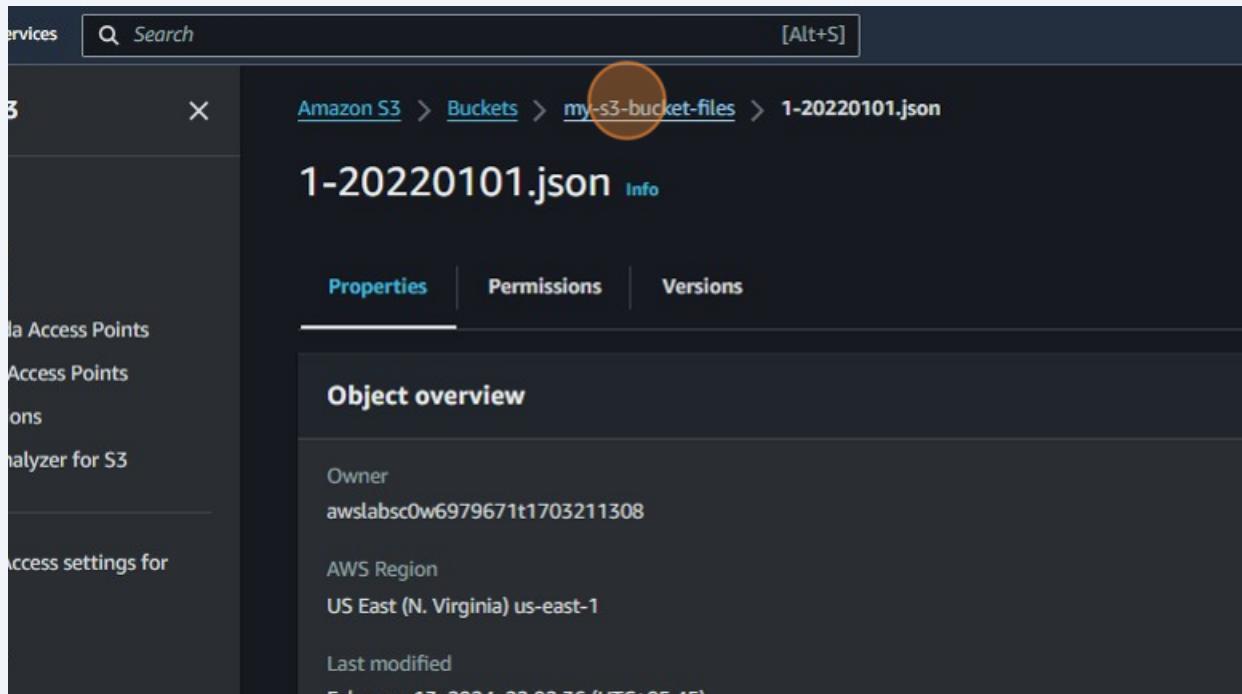
27 Click "Properties"

The screenshot shows the AWS S3 Properties page for the file "1-20220101.json". The navigation bar at the top includes the AWS logo, Services (with Buckets selected), a search bar, and a keyboard shortcut [Alt+S]. The breadcrumb trail shows: Amazon S3 > Buckets > my-s3-bucket-files > 1-20220101.json. Below the breadcrumb trail, the file name "1-20220101.json" is displayed with an "Info" link. A navigation bar at the top of the content area includes "Properties" (which is highlighted with a yellow circle), "Permissions", and "Versions". The main content area is titled "Access control list (ACL)" and contains a sub-section "Grantee" which lists the "Object owner (your AWS account)". It shows the Canonical ID: 193f8c550d7e57aeab690337b3e410585d7e23cf1df44a1ed684ef89af5d8622. There is also a section for "Everyone (public access)".

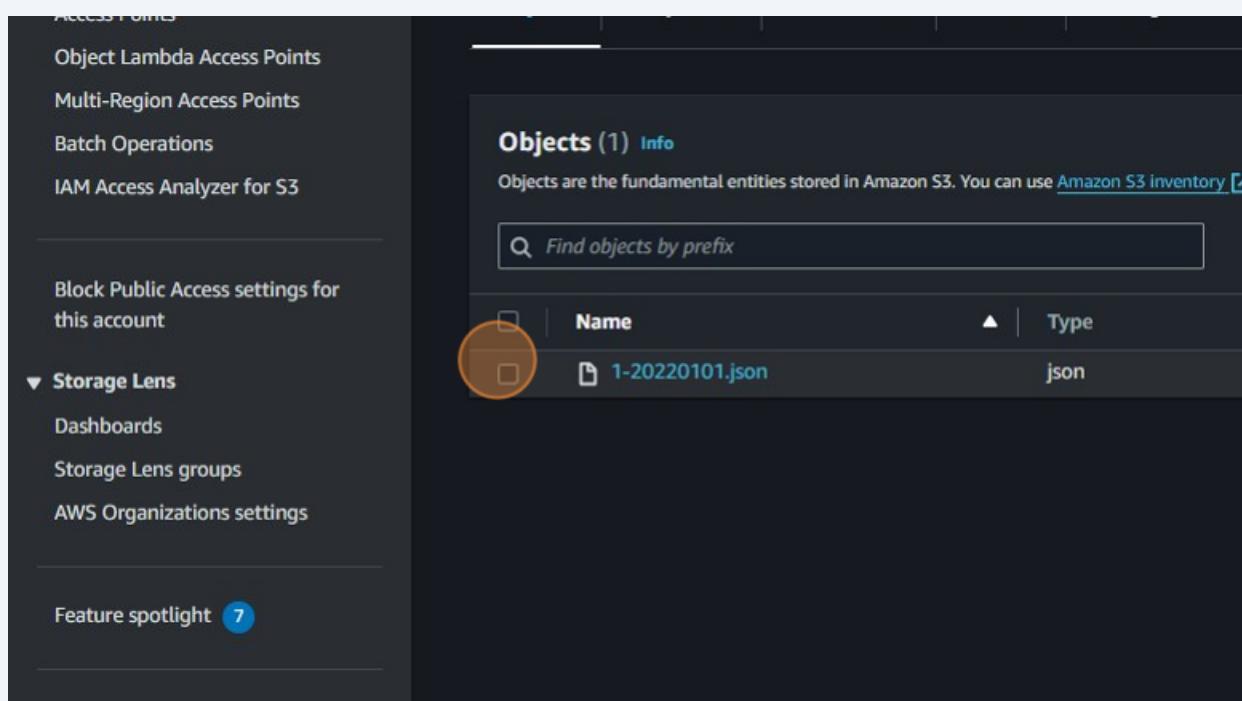
28 Click "<https://my-s3-bucket-files.s3.amazonaws.com/1-20220101.json>"

The screenshot shows the AWS S3 Properties page for the file "1-20220101.json". The left sidebar lists various properties: "s3://my-s3-bucket-files/1-20220101.json" (selected), "Amazon Resource Name (ARN)", "arn:aws:s3:::my-s3-bucket-files/1-20220101.json", "Entity tag (Etag)", "61f924a1b43ad119a7d468f4764cc60f", and "Object URL". The "Object URL" entry is highlighted with a yellow circle and contains the value "<https://my-s3-bucket-files.s3.amazonaws.com/1-20220101.json>".

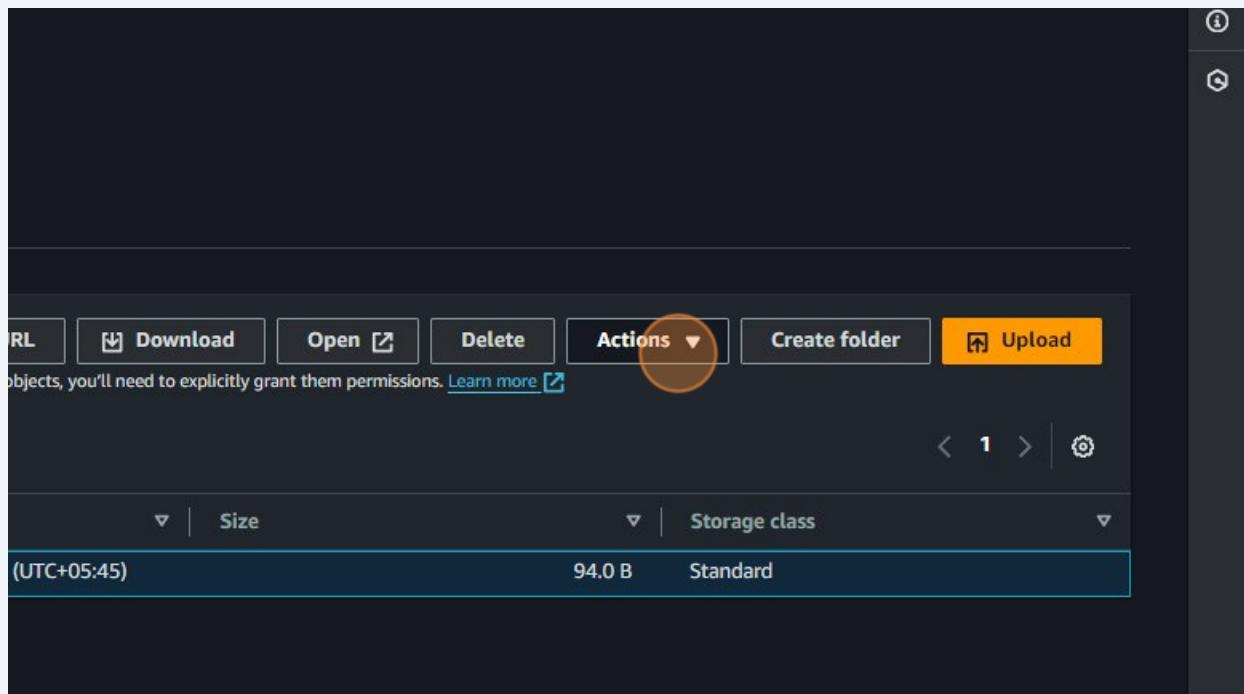
29 Click "my-s3-bucket-files"



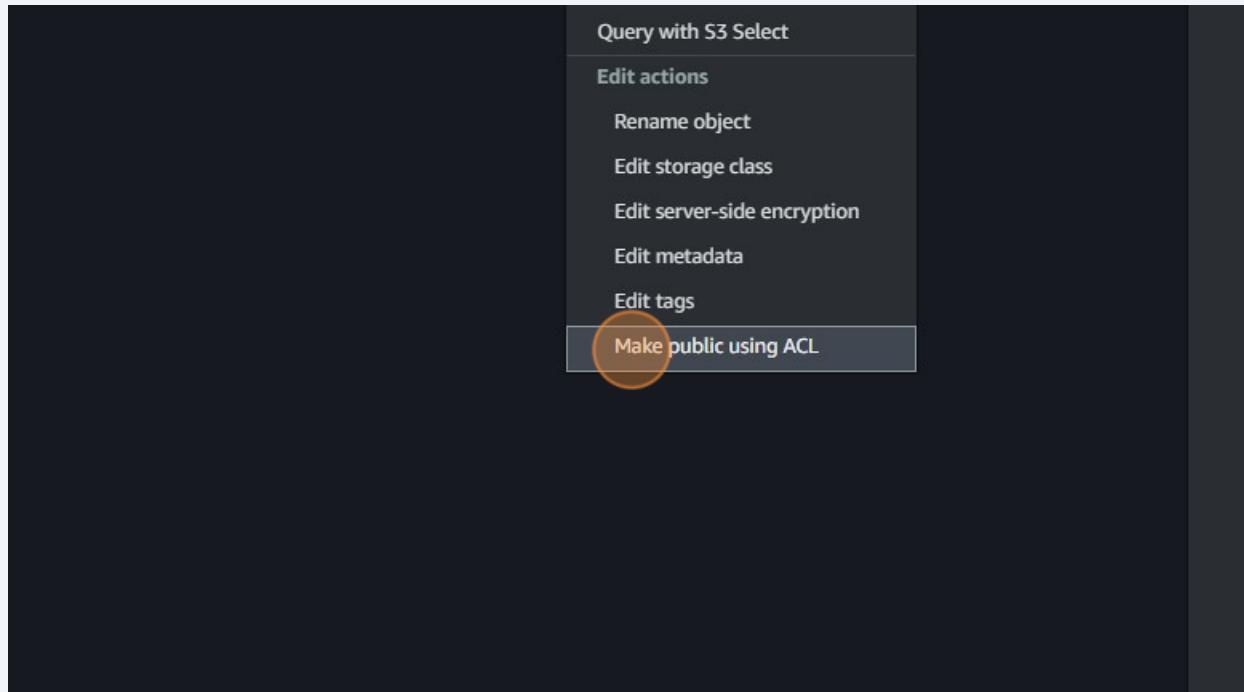
30 Click this checkbox.



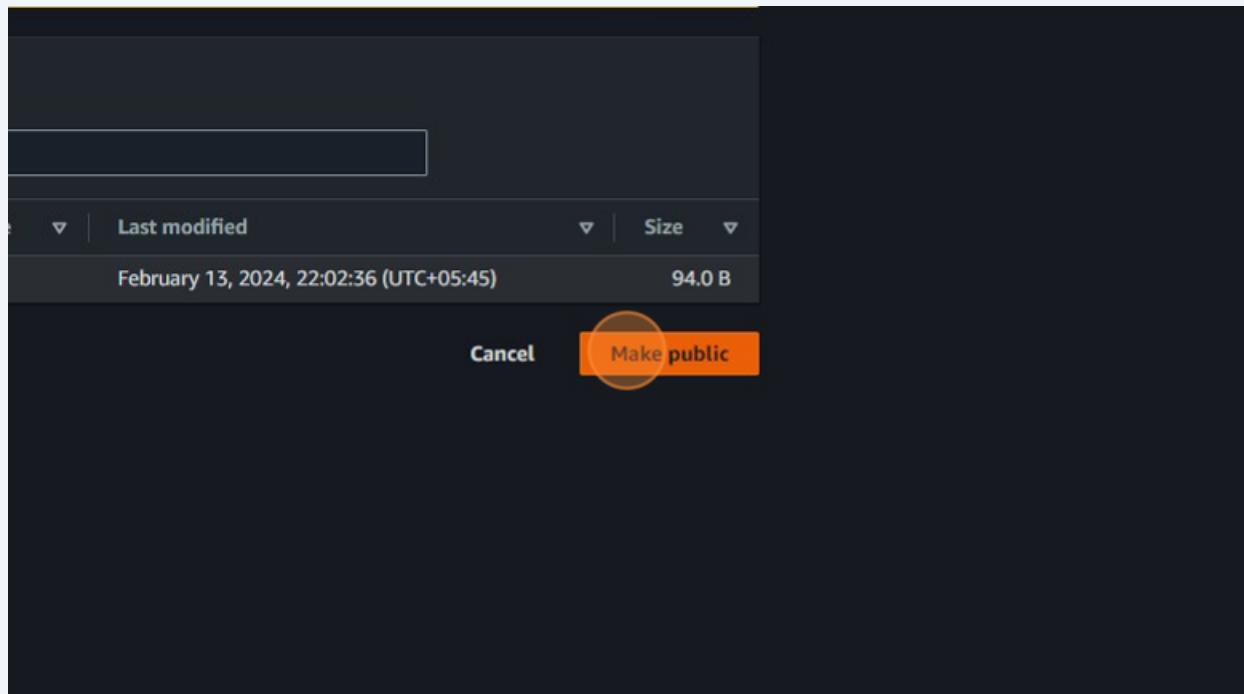
31 Click "Actions"



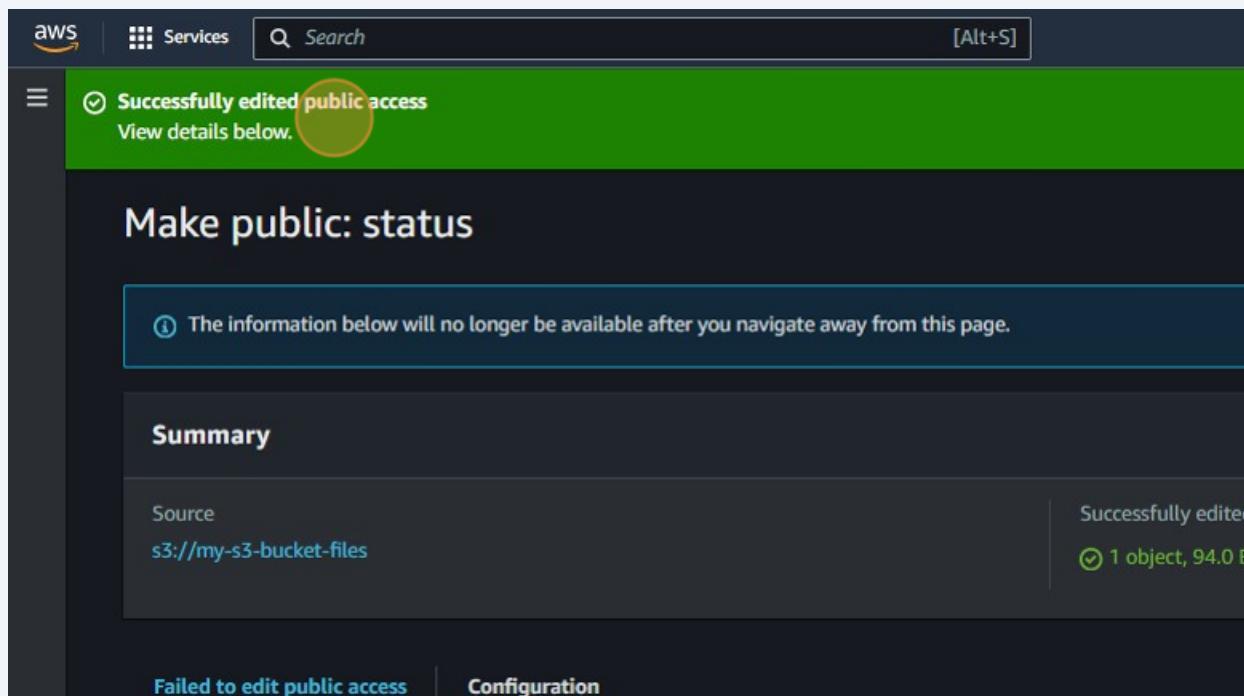
32 Click "Make public using ACL"



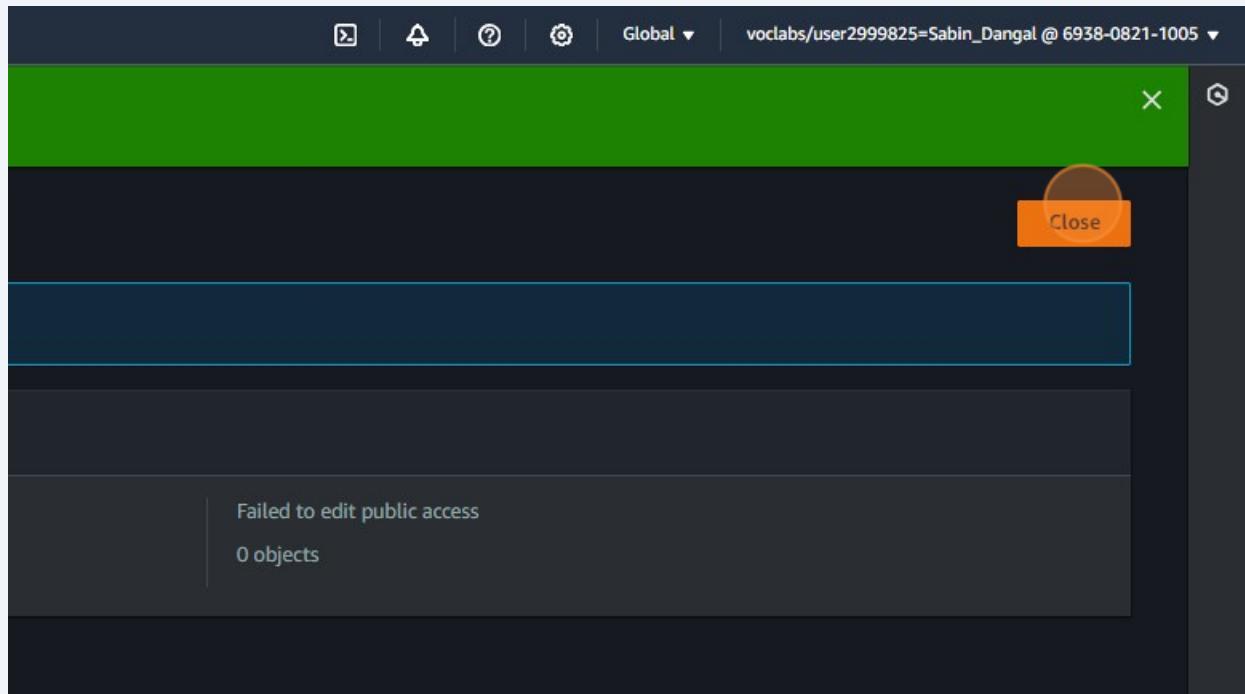
33 Click "Make public"



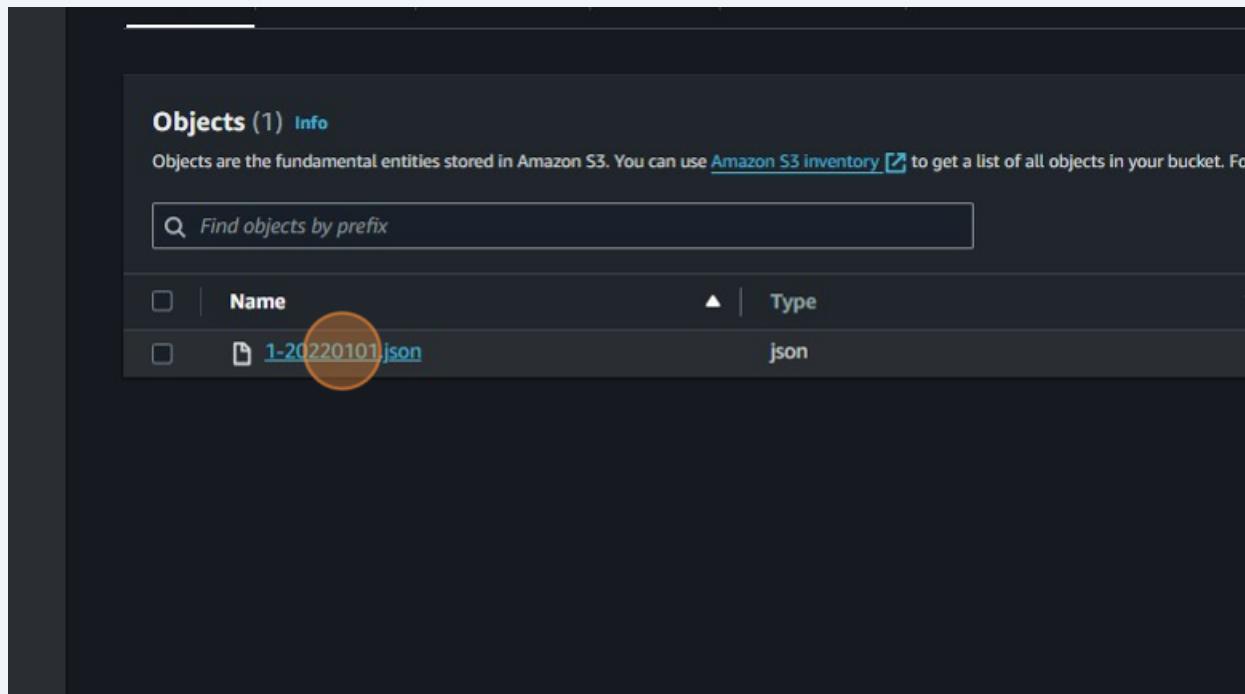
34 Click "View details below."



35 Click "Close"

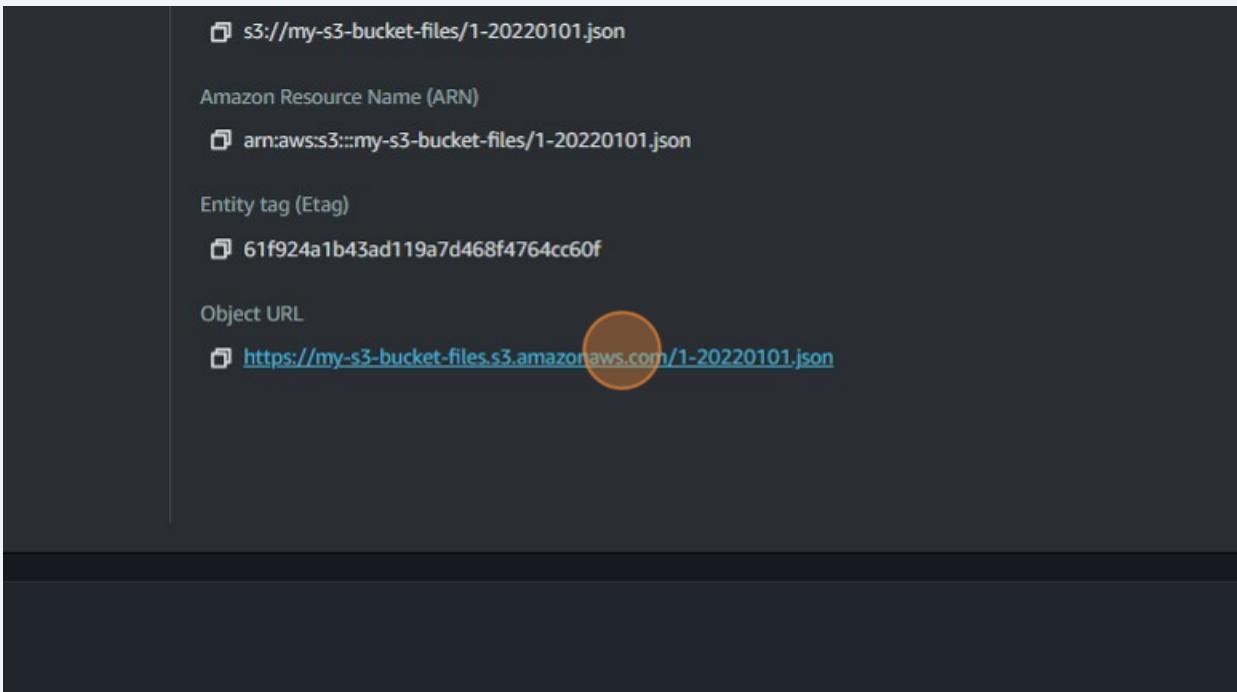


36 Click "1-20220101.json"



37

Click "<https://my-s3-bucket-files.s3.amazonaws.com/1-20220101.json>"



38

Click "age: 30,"



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"

The screenshot shows the AWS S3 console interface. On the left, there's a sidebar with options like Buckets, Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, and IAM Access Analyzer for S3. Below that, there's a section for Block Public Access settings for this account. At the bottom of the sidebar, there's a Storage Lens section with a Storage Lens icon and a link to Dashboards. The main area shows the navigation path: Amazon S3 > Buckets > my-s3-bucket-files > 1-20220101.json. The file name 1-20220101.json is highlighted with a blue oval. Below the path, there are tabs for Properties (which is selected), Permissions, and Versions. Under the Properties tab, there's a section titled 'Object overview' containing the following details:

Owner	awslabsc0w6979671t1703211308
AWS Region	US East (N. Virginia) us-east-1
Last modified	February 17, 2024, 22:02:26 (UTC+05:45)

41 Lists of buckets

The screenshot shows the AWS S3 console interface. On the left, there's a sidebar with navigation links like 'Storage Lens', 'Dashboards', 'Storage Lens groups', 'AWS Organizations settings', 'Feature spotlight' (with a '7' badge), and 'AWS Marketplace for S3'. The main area is titled 'General purpose buckets (4) Info' and contains a table listing four buckets:

Name	AWS Region
bootcampfilesbucket	US East (N. Virginia)
my-bucket-files-techkraft	US East (N. Virginia)
my-s3-bucket-files	US East (N. Virginia)
techkraft-bootcamp-files	US East (N. Virginia)

A search bar at the top right says 'Find buckets by name'.

IAM Users and Roles Lab

42

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

43 Click this link.

The screenshot shows the AWS S3 console. At the top, there's a navigation bar with the AWS logo, a 'Services' dropdown, a search bar containing 'Search', and a keyboard shortcut '[Alt+S]'. Below the navigation bar, the title 'Amazon S3' is displayed next to a close button ('X'). The main content area shows the 'Buckets' page under the 'Amazon S3 > Buckets' breadcrumb. On the left, a sidebar lists various options: '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', and 'Storage Lens' (with 'Dashboards' listed under it). The 'Storage Lens' section has a small orange circle with the number '44' over it. The main content area features an 'Account snapshot' section with a summary: 'Total storage 134.0 B' and 'Object count 1'. Below this, there are two tabs: 'General purpose buckets' (which is selected) and 'Directory buckets'. A section titled 'General purpose buckets (4)' follows, with a note that they are 'Containers for data stored in S3'. A search bar at the bottom allows users to 'Find buckets by name'.

44 Click "IAM"

The screenshot shows the AWS Console Home page. At the top, it says 'Console Home' with an 'Info' link. Below this, there's a section titled ':: Recently visited' with an 'Info' link. This section lists several services: S3 (with a blue icon), EC2 (with an orange icon), IAM (with a red icon and a large orange circle around it), and EFS (with a green icon). To the left of the recently visited section is a dark sidebar with a vertical menu icon (three horizontal lines).

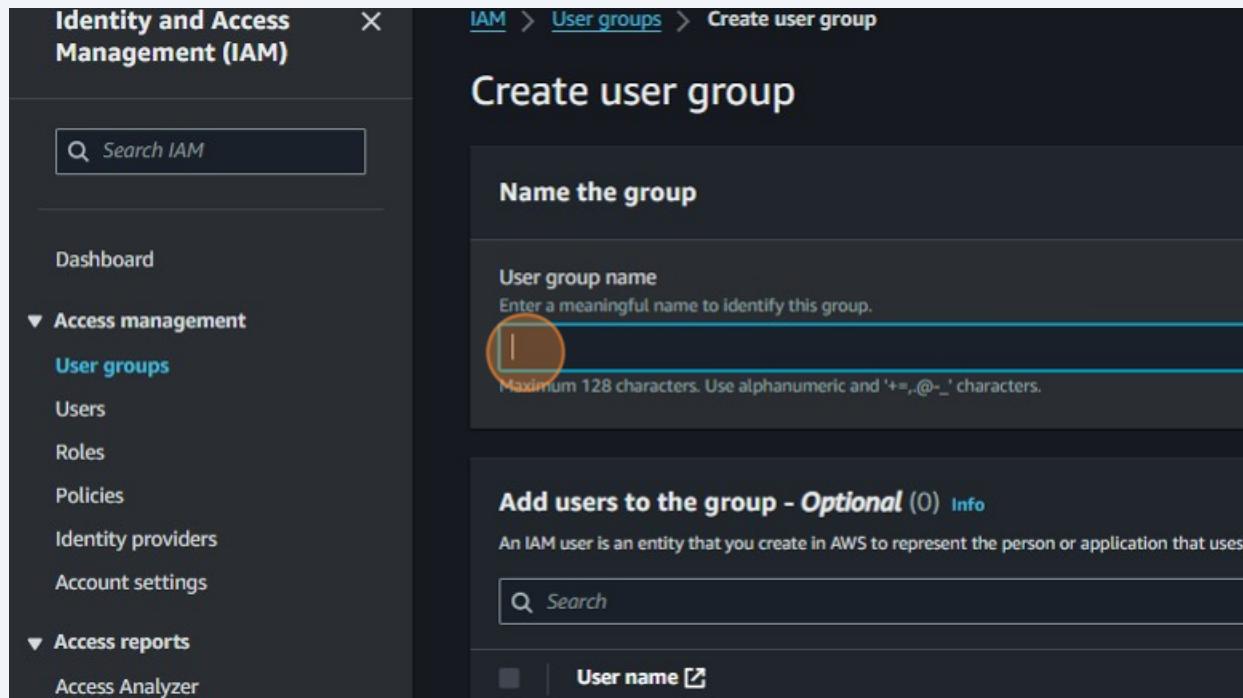
45 Click "0"

The screenshot shows the AWS Management Console with the IAM service selected. The left sidebar has a 'Management (IAM)' header and a search bar. Under 'Access management', it lists 'User groups' (with a value of 0 highlighted in orange), 'Users', 'Roles', 'Policies', 'Identity providers', and 'Account settings'. Under 'Access reports', it lists 'Access Analyzer'. The main area is titled 'IAM Dashboard' and contains a section for 'IAM resources' with a table showing 0 User groups, 0 Users, and 19 Roles. Below this is a 'What's new' section with a link to updates for features in IAM.

46 Click "Create group"

The screenshot shows the 'User groups' page in the IAM service. At the top, there are navigation icons and a dropdown for 'Global'. The main area displays a table of user groups. A modal dialog is open over the table, containing a 'Create group' button which is highlighted with an orange circle. Other buttons in the dialog include 'C' (cancel) and 'Delete'. Below the table, there are sorting options for 'Creation time'.

- 47 Click the "User group name" field.



- 48 Type "my-user-group"

49 Click this checkbox.

The screenshot shows the AWS Identity and Access Management (IAM) console. On the left, there's a sidebar with a search bar and links for Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings), and a large 'Attach permissions policies' section. The main area displays a list of policies under 'Policy name' with checkboxes to the left of each. One specific checkbox for the 'AdministratorAccess' policy is highlighted with a red circle, indicating it should be clicked. The list includes:

Policy name	Type
AdministratorAccess	AWS
AdministratorAccess-Amplify	AWS
AdministratorAccess-AWSElasticBeanstalk	AWS
AlexaForBusinessDeviceSetup	AWS
AlexaForBusinessFullAccess	AWS
AlexaForBusinessGatewayExecution	AWS

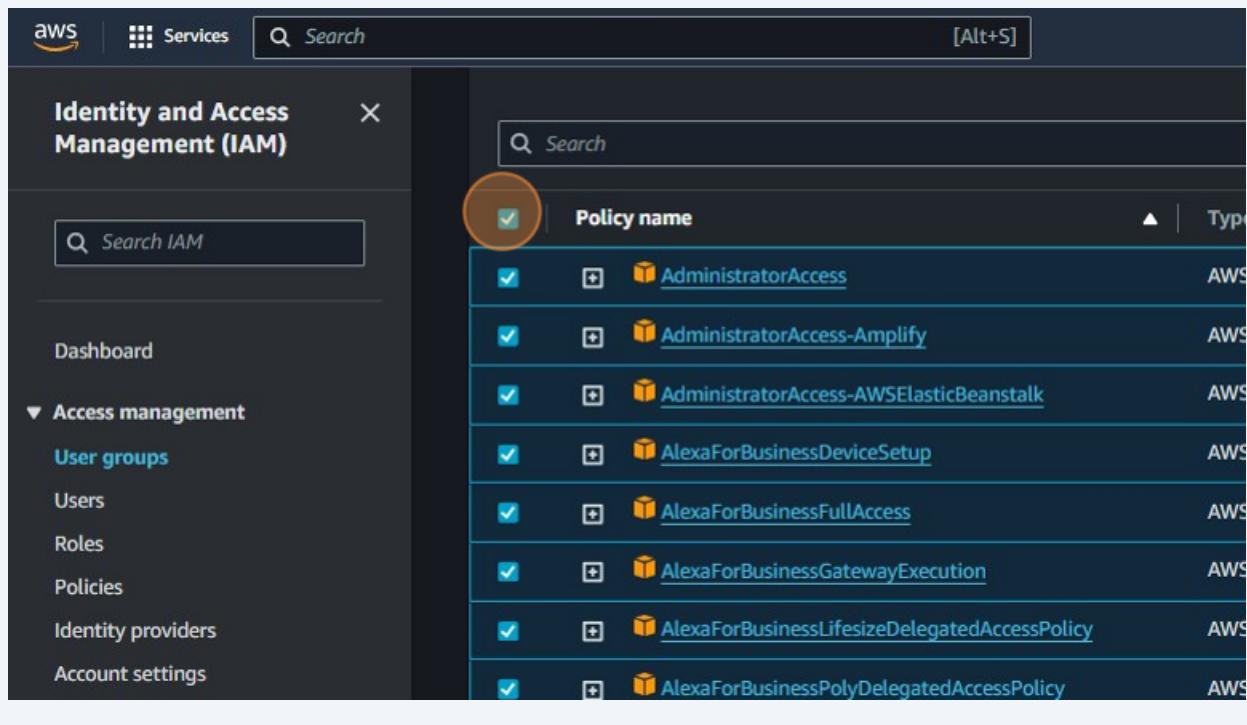
50 Click "Create group"

The screenshot shows a 'Create group' dialog box. It lists several AWS services with their corresponding default policies. At the bottom right, there are 'Cancel' and 'Create group' buttons, with the 'Create group' button being highlighted with a red circle. The list of services and their descriptions is as follows:

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...

At the bottom of the dialog, there are links for '© 2024, Amazon Web Services, Inc. or its affiliates.', 'Privacy', 'Terms', and 'Cookie preferences'.

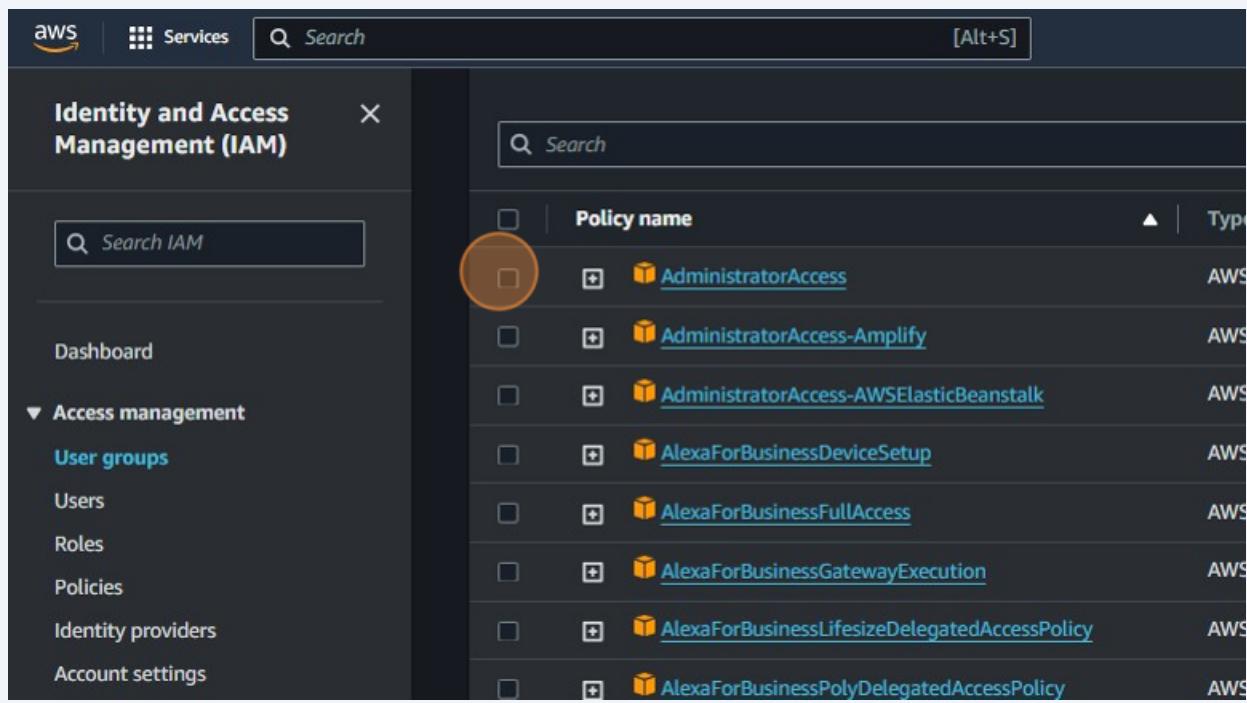
51 Click this checkbox.



The screenshot shows the AWS Identity and Access Management (IAM) Policies page. On the left, there's a sidebar with a search bar and a list of navigation options under 'Access management': User groups, Users, Roles, Policies, Identity providers, and Account settings. The 'Policies' option is selected. On the right, a table lists various AWS managed policies. The first policy, 'AdministratorAccess', has its checkbox checked and is highlighted with a yellow circle. The table columns include 'Policy name', 'Type', and 'AWS'. Other policies listed include 'AdministratorAccess-Amplify', 'AdministratorAccess-AWSElasticBeanstalk', 'AlexaForBusinessDeviceSetup', 'AlexaForBusinessFullAccess', 'AlexaForBusinessGatewayExecution', 'AlexaForBusinessLifesizeDelegatedAccessPolicy', and 'AlexaForBusinessPolyDelegatedAccessPolicy'.

Policy name	Type	AWS
AdministratorAccess	AWS	
AdministratorAccess-Amplify	AWS	
AdministratorAccess-AWSElasticBeanstalk	AWS	
AlexaForBusinessDeviceSetup	AWS	
AlexaForBusinessFullAccess	AWS	
AlexaForBusinessGatewayExecution	AWS	
AlexaForBusinessLifesizeDelegatedAccessPolicy	AWS	
AlexaForBusinessPolyDelegatedAccessPolicy	AWS	

52 Click this checkbox.



This screenshot is identical to the one above it, showing the same AWS IAM Policies page. However, the first policy, 'AdministratorAccess', now has its checkbox unchecked. The yellow circle highlighting the checkbox is also gone. The rest of the table and sidebar are identical to the previous screenshot.

Policy name	Type	AWS
AdministratorAccess	AWS	
AdministratorAccess-Amplify	AWS	
AdministratorAccess-AWSElasticBeanstalk	AWS	
AlexaForBusinessDeviceSetup	AWS	
AlexaForBusinessFullAccess	AWS	
AlexaForBusinessGatewayExecution	AWS	
AlexaForBusinessLifesizeDelegatedAccessPolicy	AWS	
AlexaForBusinessPolyDelegatedAccessPolicy	AWS	

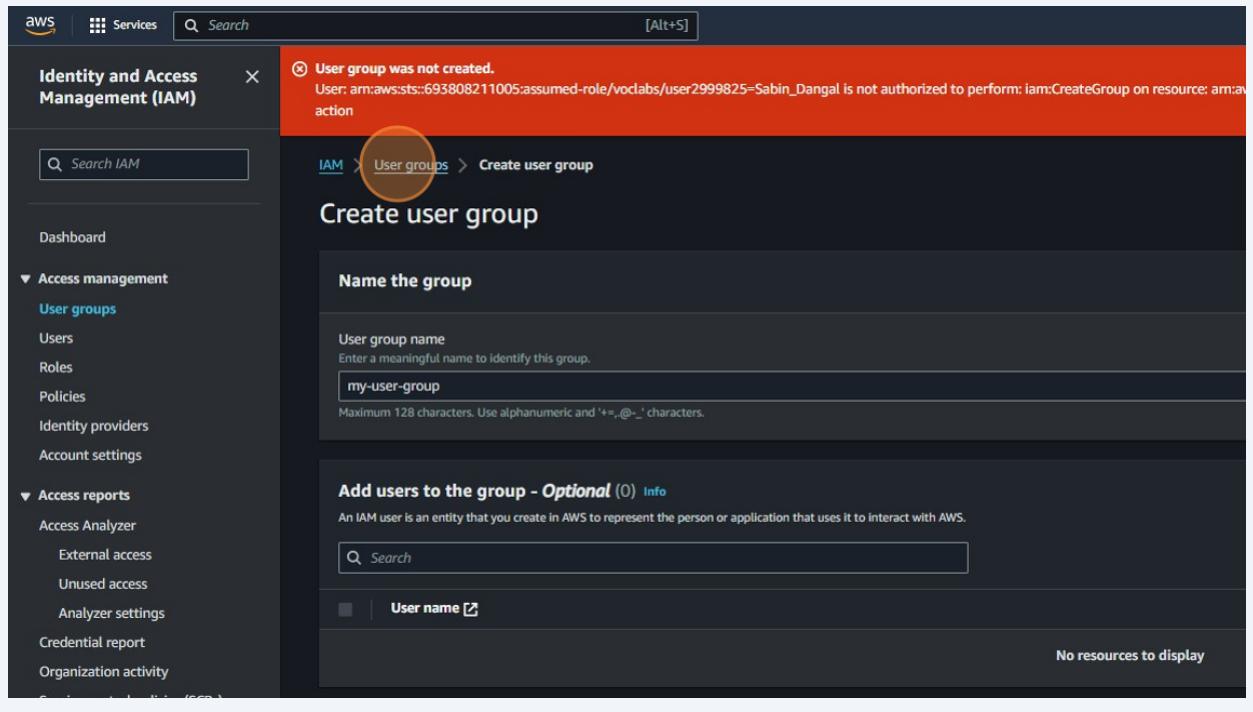
53 Click "Create group"

The screenshot shows the AWS IAM Policies page. A search bar at the top has 'Search' and '[Alt+S]' placeholder text. Below it is a table with columns: Policy name, Type, Used as, and Description. The 'AdministratorAccess' policy is selected (indicated by a checked checkbox). Other policies listed include 'AdministratorAccess-Amplify', 'AdministratorAccess-AWSElasticBeanstalk', 'AlexaForBusinessDeviceSetup', 'AlexaForBusinessFullAccess', 'AlexaForBusinessGatewayExecution', 'AlexaForBusinessLifesizeDelegatedAccessPolicy', 'AlexaForBusinessPolyDelegatedAccessPolicy', 'AlexaForBusinessReadOnlyAccess', 'AmazonAPIGatewayAdministrator', 'AmazonAPIGatewayInvokeFullAccess', 'AmazonAPIGatewayPushToCloudWatchLogs', 'AmazonAppFlowFullAccess', 'AmazonAppFlowReadOnlyAccess', 'AmazonAppStreamFullAccess', 'AmazonAppStreamPAAccess', 'AmazonAppStreamReadOnlyAccess', 'AmazonAppStreamServiceAccess', 'AmazonAthenaFullAccess', and 'AmazonAugmentedAIFullAccess'. The 'AdministratorAccess' row is highlighted in blue. A note at the bottom left says '⚠ Number of policies to be attached exceeds the limit.' At the bottom right are links for 'Privacy', 'Terms', and 'Cookie preferences'.

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

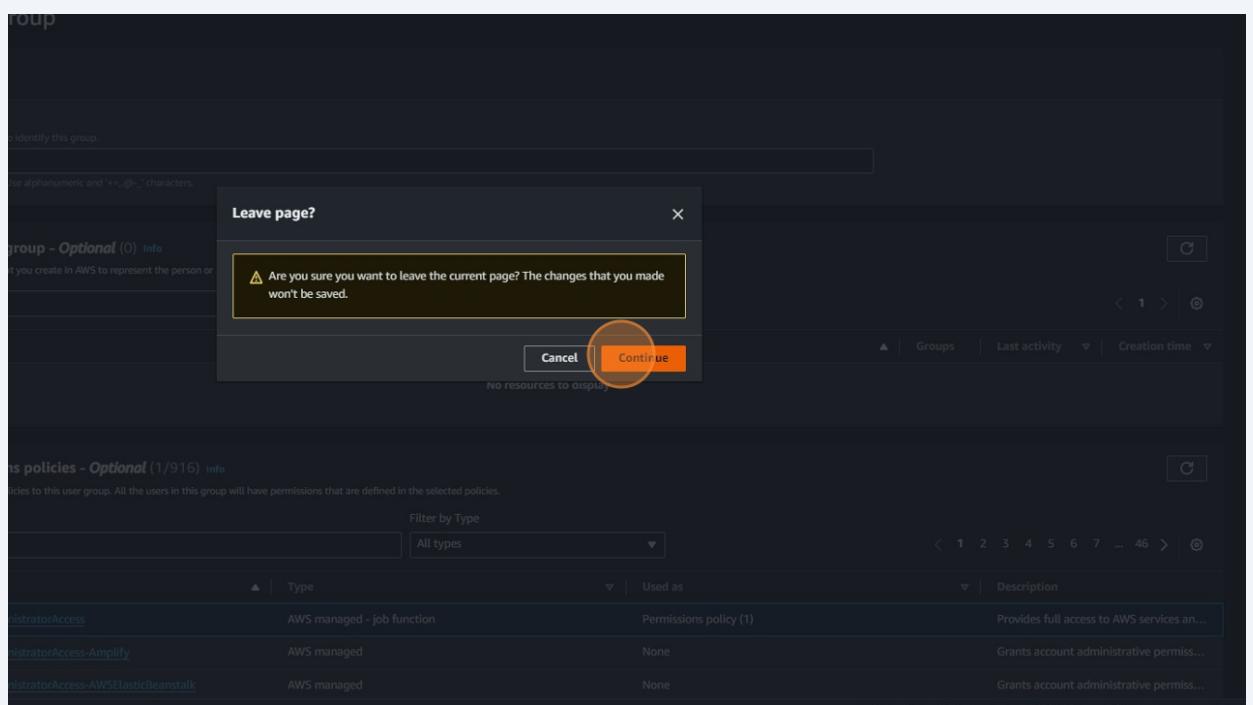
The screenshot shows the AWS IAM Policies page. A search bar at the top has 'Search' and '[Alt+S]' placeholder text. On the left, there's a sidebar with 'Access Management (IAM)' and other tabs like 'Management', 'Users', and 'Groups'. A red error banner at the top center says '✖ User group was not created.' followed by 'User: arn:aws:sts::693808211005:assumed-role/voclabs/user2999825=Sabin_Dangal is not authorized to perform action'. Below the banner is a table with columns: Policy name, Type, and Description. The 'AdministratorAccess' policy is selected (indicated by a checked checkbox). Other policies listed include 'AdministratorAccess-Amplify', 'AdministratorAccess-AWSElasticBeanstalk', 'AlexaForBusinessDeviceSetup', 'AlexaForBusinessFullAccess', 'AlexaForBusinessGatewayExecution', 'AlexaForBusinessLifesizeDelegatedAccessPolicy', 'AlexaForBusinessPolyDelegatedAccessPolicy', 'AlexaForBusinessReadOnlyAccess', 'AmazonAPIGatewayAdministrator', 'AmazonAPIGatewayInvokeFullAccess', 'AmazonAPIGatewayPushToCloudWatchLogs', 'AmazonAppFlowFullAccess', 'AmazonAppFlowReadOnlyAccess', 'AmazonAppStreamFullAccess', 'AmazonAppStreamPAAccess', 'AmazonAppStreamServiceAccess', 'AmazonAthenaFullAccess', and 'AmazonAugmentedAIFullAccess'. The 'AdministratorAccess' row is highlighted in blue. At the bottom right are links for 'Privacy', 'Terms', and 'Cookie preferences'.

55 Click "User groups"



The screenshot shows the AWS Identity and Access Management (IAM) console. In the top-left corner, there's a circular icon with the number 55. The main title is "Create user group". On the left side, there's a navigation menu with "User groups" highlighted. The main content area has a heading "Name the group" and a "User group name" input field containing "my-user-group". Below this, there's a section titled "Add users to the group - Optional (0)" with a "User name" search bar and a message "No resources to display". At the top, there's an error message: "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:aws:iam::693808211005:group/my-user-group".

56 Click "Continue"



The screenshot shows a confirmation dialog box titled "Leave page?". It contains a warning message: "Are you sure you want to leave the current page? The changes that you made won't be saved." There are two buttons at the bottom: "Cancel" and "Continue". The "Continue" button is highlighted with a red circle. In the background, there's a list of policies for the user group, with one policy named "AdministratorAccess" selected.

57 Click "IAM"

The screenshot shows the AWS Identity and Access Management (IAM) console. The left sidebar is titled 'Identity and Access Management (IAM)' and includes links for Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings), and other sections like Access reports, Credential report, Organization activity, and Service control policies (SCPs). The main content area is titled 'User groups (0) Info' and contains a table header with columns for Group name and Users. A search bar is at the top of the main content area.

58 Click on the roles

The screenshot shows the AWS IAM Dashboard. The left sidebar includes links for Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings), Access reports, Credential report, Organization activity, and Service control policies (SCPs). The main content area is titled 'IAM Dashboard' and features a summary table for IAM resources: User groups (0), Users (0), Roles (19), Policies (6), and Identity providers (0). Below this is a 'What's new' section with a list of recent updates. On the right side, there are sections for AWS Account (Account ID, Sign-in URL) and Tools (Policy simulator, IAM document, Videos, blog).

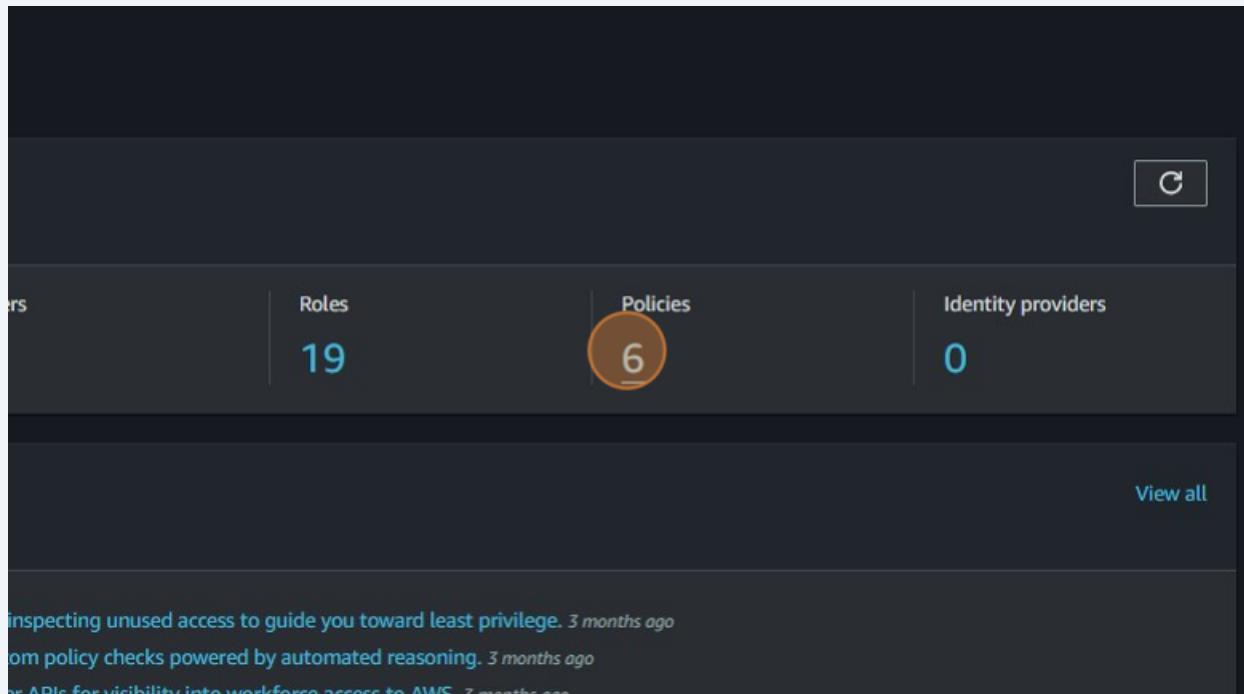
59 Roles List

The screenshot shows the AWS IAM Roles List page. At the top, there is a search bar and a 'Create role' button. Below the header, a table lists 19 IAM roles. The columns are 'Role name', 'Trusted entities', and 'Last activity'. A large orange circle highlights the 'Role name' column header. The roles listed include: AWSServiceRoleForCloudWatchEvents, AWSServiceRoleForElastiCache, AWSServiceRoleForOrganizations, AWSServiceRoleForSupport, AWSServiceRoleForTrustedAdvisor, c108787a256087856420861w69380821100-LambdaSLRRole-2NYjxStJSHoY, EMR_AutoScaling_DefaultRole, EMR_DefaultRole, EMR_EC2_DefaultRole, EMR_Notebooks_DefaultRole, LabRole, myRedshiftRole, RedshiftRole, RoleForLambdaModLabRole, vocareum, vocareum-eventbridge, vodabs, and vocatsoft. The last activity for most roles is '22 days ago', except for LabRole which was '19 minutes ago'.

60 Click "IAM"

The screenshot shows the AWS IAM dashboard. The left sidebar has a 'Dashboard' section and a 'Access management' section with links for 'User groups', 'Users', 'Roles', 'Policies', 'Identity providers', and 'Account settings'. The 'Roles' link is highlighted with an orange circle. The main content area is titled 'Roles (19) Info' and contains a table with the same 19 roles as the previous screenshot. The 'Role name' column header is also highlighted with an orange circle. The roles listed are: AWSServiceRoleForAWSCloud9, AWSServiceRoleForCloudWatchEvents, AWSServiceRoleForElastiCache, AWSServiceRoleForOrganizations, and AWSServiceRoleForSupport.

61 Click on policies



62

Click "IAM Policies Policies (1179)

Info
Actions
Delete
Create policy

A policy is an object in AWS that defines permissions.

Filter by Type
Custome..."

Search		Filter by Type			
		Customer managed		▼ 6 matches	
	Policy name	Type	Used as		Description
○	c108787a2560828l56420861w693808211005-VocL...	Customer managed	Permissions policy (1)	-	
○	c108787a2560828l56420861w693808211005-VocL...	Customer managed	Permissions policy (1)	-	
○	c108787a2560828l56420861w693808211005-VocL...	Customer managed	Permissions policy (1)	-	
○	Pvclabs1	Customer managed	Permissions policy (1)	-	
○	Pvclabs2	Customer managed	Permissions policy (1)	-	
○	voc-cancel-cred	Customer managed	Permissions policy (2)	-	

63 Click "Customer managed"

Filter by Type		
Type	Used as	Count
Customer managed	Permissions policy (1)	1
Customer managed	Permissions policy (1)	1
Customer managed	Permissions policy (1)	1
Customer managed	Permissions policy (1)	1
Customer managed	Permissions policy (1)	1
Customer managed	Permissions policy (2)	1

64 Click "IAM"

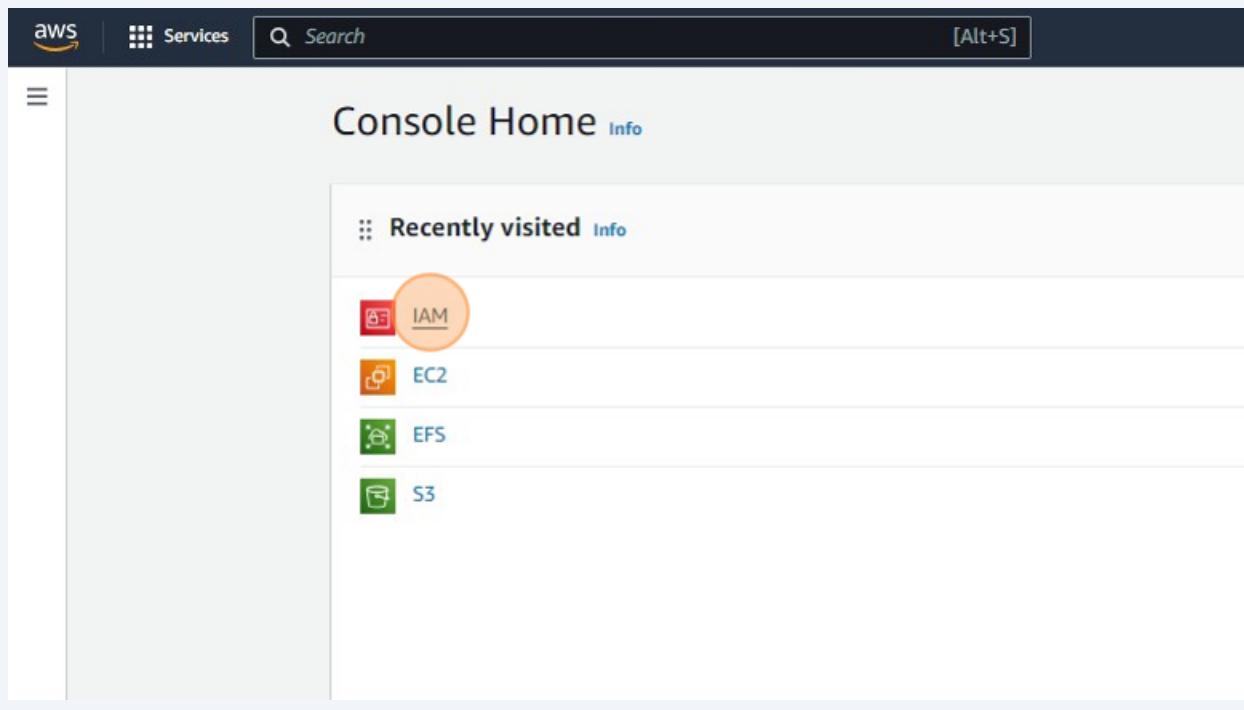
Identity and Access Management (IAM)		
Search IAM		
Dashboard		
Access management		
User groups		
Users		
Roles		
Policies		
Identity providers		
Account settings		
Policies (1179) Info		
A policy is an object in AWS that defines permissions.		
Search		
Policy name		
c108787a2560828l5642086t1w693808211005-VocL...	Cust	
c108787a2560828l5642086t1w693808211005-VocL...	Cust	
c108787a2560828l5642086t1w693808211005-VocL...	Cust	
Pvoclabs1	Cust	
Pvoclabs2	Cust	

65

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

66

Click "IAM"



67 Click "3"

The screenshot shows the AWS Identity and Access Management (IAM) dashboard. On the left, there's a sidebar with navigation links like Dashboard, Access management, and Access reports. The main area is titled "IAM Dashboard" and contains a section titled "IAM resources" with a sub-section "User groups". A large orange circle highlights the number "3" next to "User groups", indicating the count of user groups. Below this, there are sections for "Users" (4) and "Roles" (14). To the right, there's a "What's new" section with a link to updates for features in IAM.

68 Click this checkbox.

The screenshot shows the "User groups" page within the AWS IAM service. At the top, there's a navigation bar with the AWS logo, services menu, and search bar. The main content area is titled "User groups (3) Info" and describes what user groups are. It includes a search bar and a table with three rows. The first row, which has a checkbox highlighted with an orange circle next to it, is labeled "EC2-Admin". The other two rows are "EC2-Support" and "S3-Support".

69 Click "EC2-Admin"

The screenshot shows the AWS Identity and Access Management (IAM) console. On the left, the navigation pane is visible with options like Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings), and Access reports. The 'User groups' option under 'Access management' is selected. On the right, the 'User groups (3/3) Info' page is displayed, showing a list of user groups: EC2-Admin, EC2-Support, and S3-Support. The 'EC2-Admin' group is highlighted with a red circle around its name in the list.

70 Click "IAM"

The screenshot shows the AWS IAM console with the 'IAM' service selected in the top navigation bar. The left sidebar shows the same navigation options as the previous screenshot. The right panel displays the 'EC2-Admin' user group details. The 'Summary' section shows the user group name as 'EC2-Admin'. Below it, there are tabs for 'Users', 'Permissions', and 'Access Advisor', with 'Users' currently selected. A section titled 'Users in this group (0)' indicates that no users are associated with this group.

71 Click "4"

The screenshot shows the AWS IAM Dashboard. On the left, there's a sidebar with navigation links like Home, IAM, Policies, Groups, Roles, and User management. The main area is titled "IAM Dashboard" and contains a section titled "IAM resources" with the sub-section "Users". It displays three categories: "User groups" (3), "Users" (4, highlighted with an orange circle), and "Roles" (14). Below this, there's a "What's new" section with a link to updates for features in IAM.

User groups	Users	Roles
3	4	14

72 Click here.

The screenshot shows the "User management" page under the "Users" section of the IAM dashboard. On the left, there's a sidebar with navigation links. The main area lists four users: "awsstudent" (selected), "user-1", "user-2", and "user-3". Each user entry includes a checkbox, a "User name" column, a "Path" column (all show "/"), and a "Actions" column with a downward arrow icon. A large orange circle highlights the "Actions" column for the first user, "awsstudent".

User name	Path	Actions
awsstudent	/	▼
user-1	/spl66/	▼
user-2	/spl66/	▼
user-3	/spl66/	▼

73 Click this checkbox.

The screenshot shows the AWS Identity and Access Management (IAM) service. On the left, there's a sidebar with a search bar and a navigation menu under 'Access management' which includes 'User groups', 'Users' (which is selected), 'Roles', 'Policies', 'Identity providers', and 'Account settings'. On the right, the main panel shows the 'Users (4) Info' section. It contains a table with four rows, each representing a user: 'awsstudent', 'user-1', 'user-2', and 'user-3'. The 'User name' column lists the names, and the 'Path' and 'Groups' columns show their respective paths and group counts. The first row, 'awsstudent', has its checkbox highlighted with an orange circle.

User name	Path	Groups
awsstudent	/	Access denied
user-1	/spl66/	0
user-2	/spl66/	0
user-3	/spl66/	0

74 Click this checkbox.

This screenshot is similar to the previous one but shows a different state. The 'Users' section now displays 'Users (4/4) Info'. The table shows the same four users ('awsstudent', 'user-1', 'user-2', 'user-3') with their checkboxes all checked (indicated by blue checkmarks). The first row, 'awsstudent', still has 'Access denied' status.

User name	Path	Groups
awsstudent	/	Access denied
user-1	/spl66/	0
user-2	/spl66/	0
user-3	/spl66/	0

75 Click "IAM"

The screenshot shows the AWS Identity and Access Management (IAM) service. In the top navigation bar, the 'Services' tab is selected. Below it, the 'Identity and Access Management (IAM)' service is open. On the left sidebar, under 'Access management', the 'Users' option is highlighted and circled in orange. The main content area displays a table titled 'Users (4) Info'. The table lists four users: 'awsstudent' (Path: /), 'user-1' (Path: /spl66/), 'user-2' (Path: /spl66/), and 'user-3' (Path: /spl66/). A red note next to 'awsstudent' states 'Access denied'.

	User name	Path	Group:
<input type="checkbox"/>	awsstudent	/	Access denied
<input type="checkbox"/>	user-1	/spl66/	0
<input type="checkbox"/>	user-2	/spl66/	0
<input type="checkbox"/>	user-3	/spl66/	0

76 Click "3"

The screenshot shows the AWS IAM Dashboard. The left sidebar includes 'Management (IAM)' and 'Access management' sections. Under 'Access management', the 'User groups' option is highlighted and circled in orange. The main content area features a summary card titled 'IAM resources' showing 'User groups: 3', 'Users: 4', and 'Roles: 14'. Below this, a 'What's new' section lists recent updates.

User groups	Users	Roles
3	4	14

What's new

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

77 Click "EC2-Admin"

The screenshot shows the AWS Identity and Access Management (IAM) console. On the left, the navigation pane includes options like Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings), and Access reports. The 'User groups' option under 'Access management' is selected. The main content area is titled 'User groups (3) Info' and contains a table with three rows:

	Group name	Users
<input type="checkbox"/>	<u>EC2-Admin</u>	
<input type="checkbox"/>	<u>EC2-Support</u>	
<input type="checkbox"/>	<u>S3-Support</u>	

A search bar is at the top of the main content area.

78 Click "Add users"

The screenshot shows the AWS IAM Groups page. At the top, there is an ARN field containing 'arn:aws:iam::381492217946:group/spl66/EC2-Admin'. Below this, there is a table with one row. The table includes columns for Groups, Last activity, and Creation time. At the bottom right of the table, there are buttons for 'C' (Create), 'Remove', and 'Add users'. The 'Add users' button is highlighted with an orange circle.

79 Click this checkbox.

The screenshot shows a list titled "Other users in this account (4)". A search bar is at the top. Below it is a table with columns: "User name" and "Groups". The table contains four rows:

User name	Groups
awsstudent	0
user-1	0
user-2	0

The row for "user-1" has an orange circle around its checkbox column, indicating it is the target for step 79.

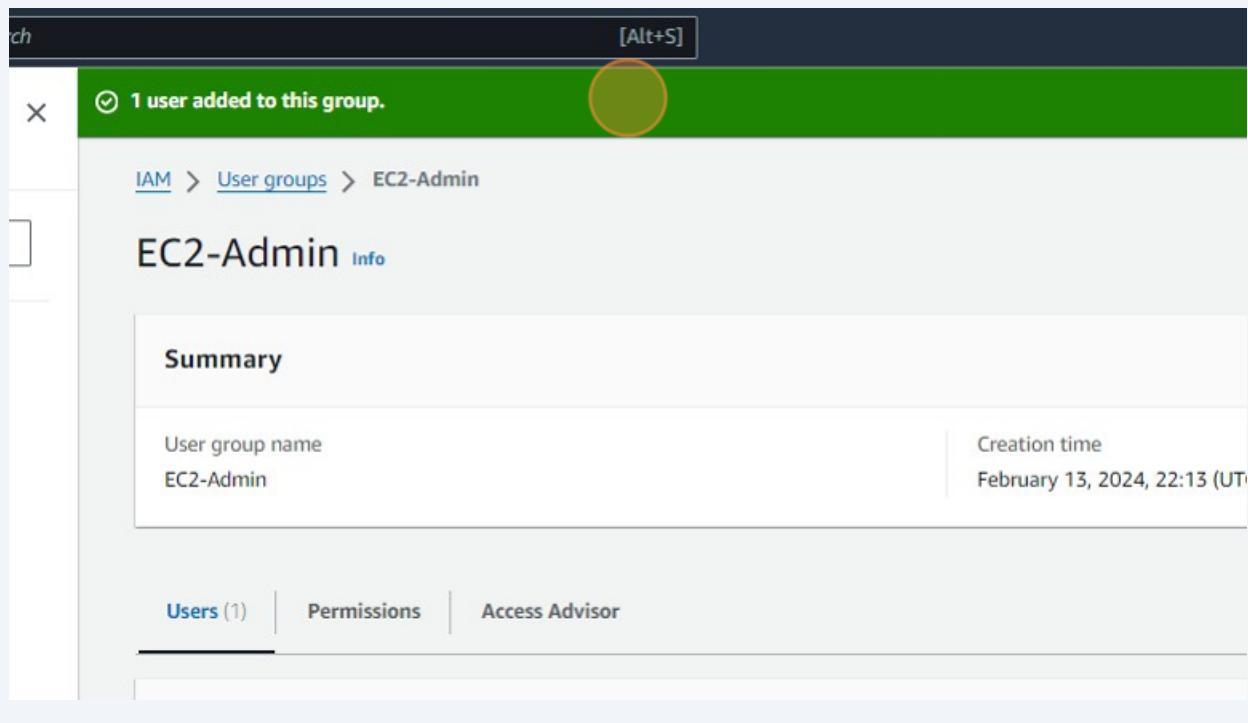
80 Click "Add users"

The screenshot shows a table with columns: "Groups", "Last activity", and "Creation time". The table contains four rows:

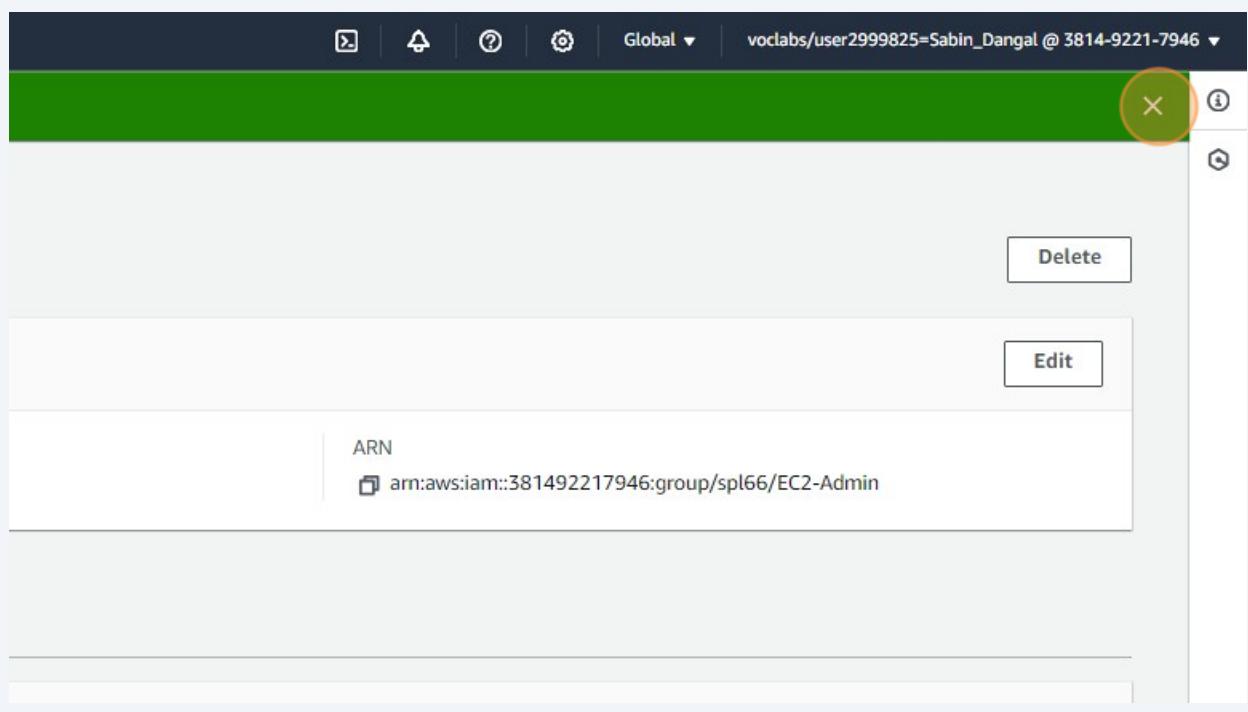
Groups	Last activity	Creation time
0	None	4 minutes ago
0	None	5 minutes ago
0	None	5 minutes ago

At the bottom right, there are two buttons: "Cancel" and "Add users". The "Add users" button is highlighted with an orange circle, indicating it is the target for step 80.

81 Click "1 user added to this group."



82 Click here.



83 Click "User groups"

The screenshot shows the AWS Identity and Access Management (IAM) console. On the left, the navigation pane is visible with the following structure:

- Identity and Access Management (IAM)
- Dashboard
- Access management
 - User groups (selected)
 - Users
 - Roles
 - Policies
 - Identity providers
 - Account settings

The main content area displays the details for the "EC2-Admin" user group. The breadcrumb navigation at the top right shows: IAM > User groups > EC2-Admin. The "User groups" link is highlighted with a yellow circle. The "EC2-Admin" name is also highlighted with a yellow circle. The "Summary" section shows the user group name as "EC2-Admin". Below it, there are tabs for "Users (1)", "Permissions", and "Access Advisor". The "Users (1)" tab is selected, showing a single user entry: "Users in this group (1)". A note below states: "An IAM user is an entity that you create in AWS to represent the person or application that uses".

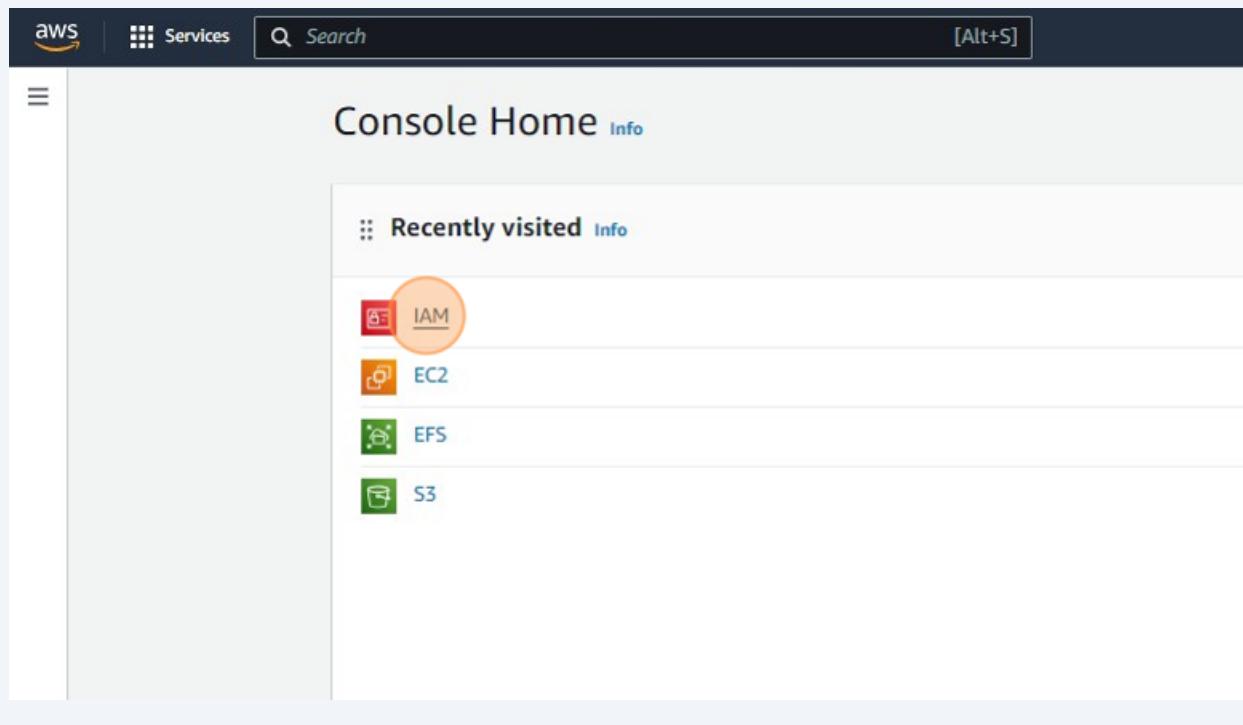
84 Click "IAM"

The screenshot shows the AWS Identity and Access Management (IAM) console. The navigation pane on the left is identical to the previous screenshot, with the "User groups" option selected.

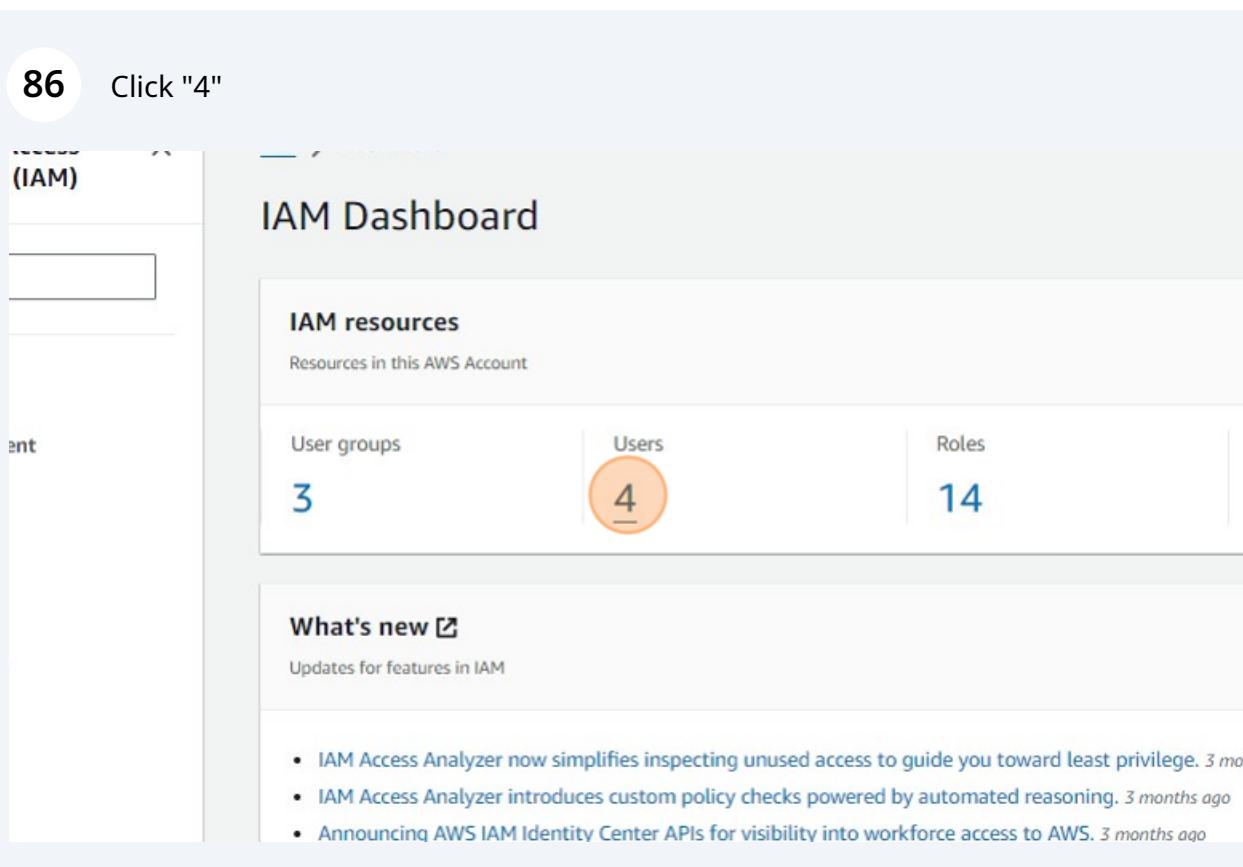
The main content area displays the "User groups (3)" list. The "User groups" link is highlighted with a yellow circle. The "EC2-Admin" group is also highlighted with a yellow circle. The list shows three entries:

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

85 Click "IAM"



86 Click "4"



87 Click "user-1"

The screenshot shows the AWS IAM console. On the left, there's a sidebar with navigation links like Dashboard, Access management, and Access reports. The main area is titled "Users (4) Info" and contains a table with four rows:

	User name	Path	Groups
<input type="checkbox"/>	awsstudent	/	
<input type="checkbox"/>	user-1	/spl66/	
<input type="checkbox"/>	user-2	/spl66/	
<input type="checkbox"/>	user-3	/spl66/	

88 Click "Groups (1)"

The screenshot shows the "User Details" page for the user "user-1". The sidebar on the left has the same navigation as the previous screenshot. The main content area shows the user's ARN and creation date. Below that, there are tabs: "Permissions" (selected), "Groups" (1), "Tags (1)", "Security credentials", and "Access Adviser". The "Groups" tab is highlighted with an orange circle.

Permissions policies (1)
Permissions are defined by policies attached to the user directly or through groups.

Search Policy name

89 Click "Tags (1)"

The screenshot shows the AWS IAM User details page for a user named 'user-1'. At the top, there are sections for ARN (arn:aws:iam::381492217946:user/spl66/user-1), Created (February 13, 2024, 22:12 (UTC+05:45)), Console access (Enabled without MFA), and Last console sign-in (Never). Below these, there are tabs for Permissions, Groups (1), Tags (1) (which is highlighted with an orange circle), Security credentials, and Access Advisor. Under the 'User groups membership' section, it shows one group: EC2-Admin.

90 Click "Security credentials"

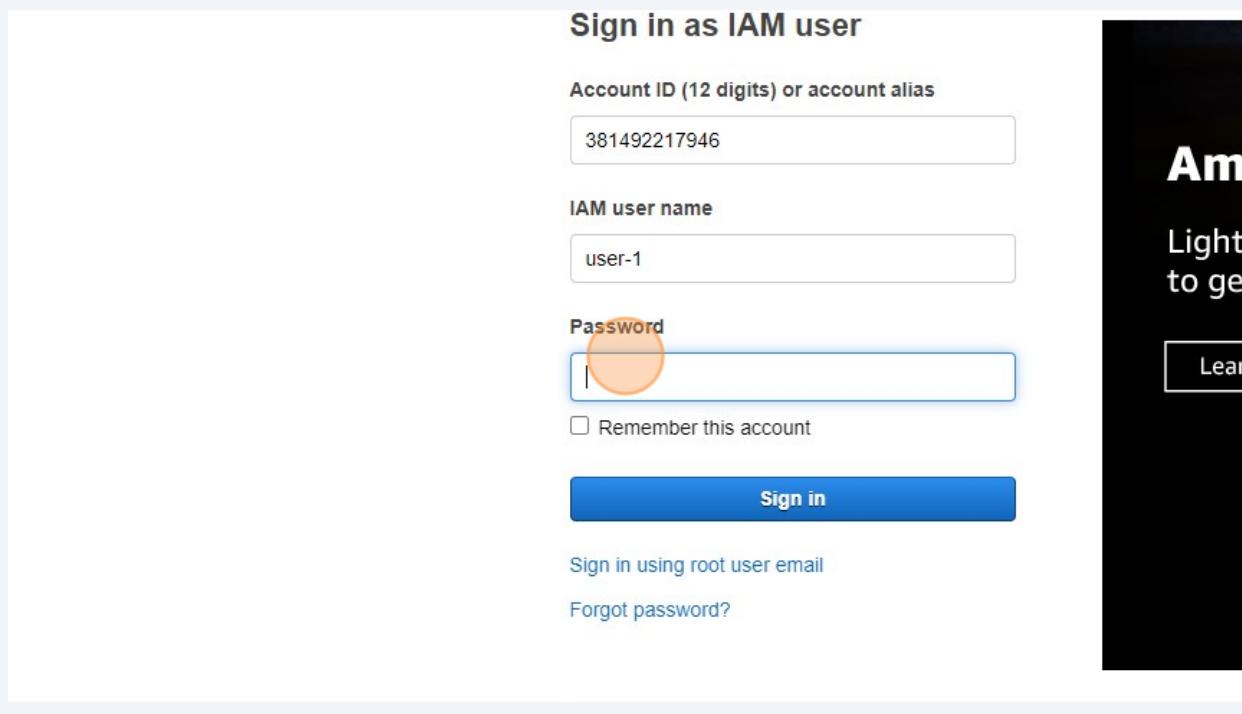
The screenshot shows the AWS IAM User details page for the same user 'user-1'. The tabs at the top are now Permissions, Groups (1), Tags (1), Security credentials (which is highlighted with an orange circle), and Access Advisor. Under the 'Tags (1)' section, it shows one tag: Key 'cloudlab'.

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

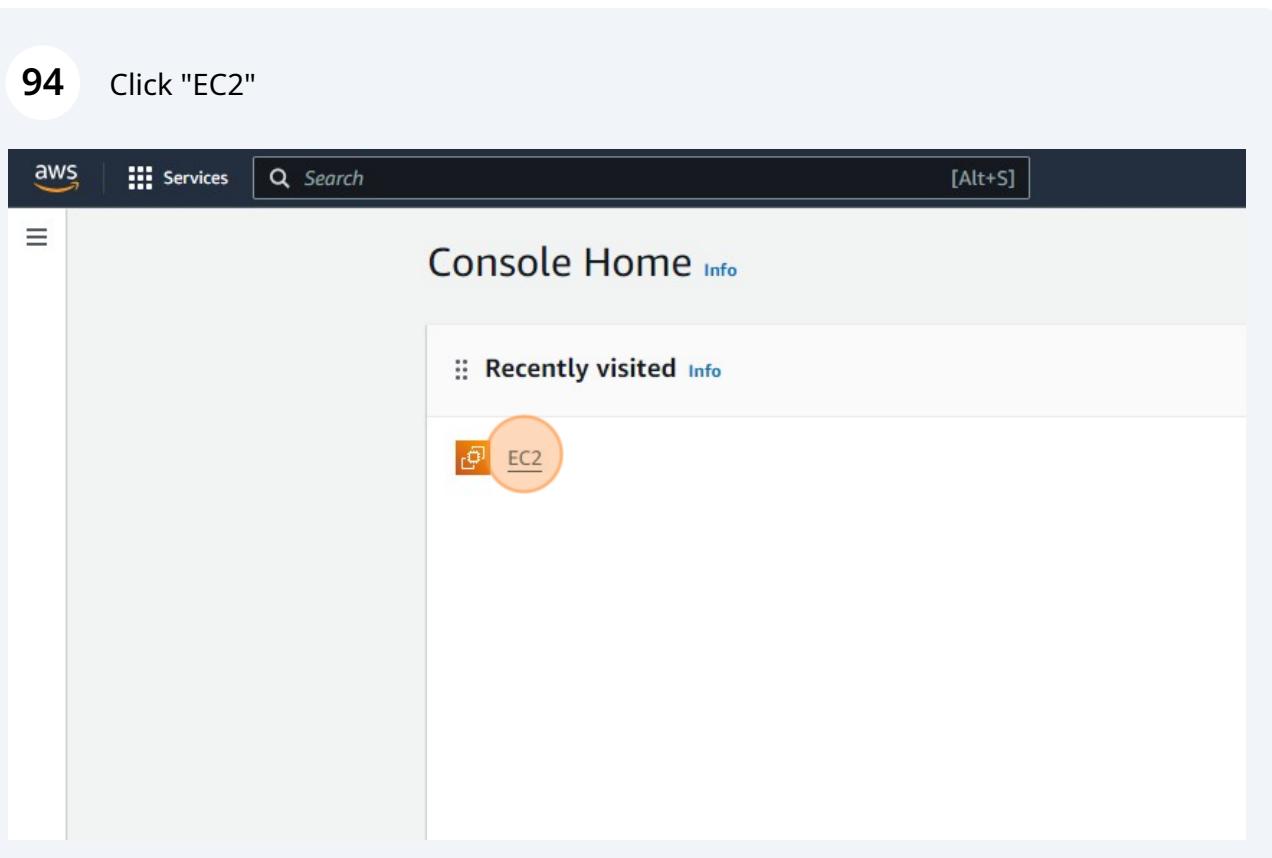
Actions	ARN	Name	Type	Status	Last updated
Edit	arn:aws:iam::123456789012:role/test-role	test-role	Role	Active	2023-01-12T12:00:00Z
Edit	arn:aws:iam::123456789012:role/test-role-with-mfa	test-role-with-mfa	Role	Active	2023-01-12T12:00:00Z
Edit	arn:aws:iam::123456789012:role/test-role-with-signin-link	test-role-with-signin-link	Role	Active	2023-01-12T12:00:00Z
Edit	arn:aws:iam::123456789012:role/test-role-with-signin-link-and-mfa	test-role-with-signin-link-and-mfa	Role	Active	2023-01-12T12:00:00Z

- 92 Navigate to https://ap-southeast-2.signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3Aconsole%2Fcanvas&code_challenge=20Hlbpq06a_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%2F%2FwEaDmFwLXNvdXR0ZWFrzDc0yIkcwRQIhAKiOcsQ0bA6aCcPzCT6wztObLwF7B6rixRl6%2BAz8J8srAiB%2B%2BL0eTvnLjYbi4Zxo8pxircPo8hnugfDI%2BqYSBN4RmCqKAgh5EAiDDQyNjA2MzgxNjU1NCIMVrnzTeuVyeTNaVDSKucBSwroM%2BBAOiyqlqcsEErYDeObTtrXR8XoLuPOkSqZ6q50HpqjsxSqzOcOei8bjU93G6uPJY1c0LtlibQYkgBcihIcTcX0M0t%2FVkdYqiSUtCGaohuujCnWklzUxK3BE2ITDglVqCeVHQ36FoZVCPbox8bHKKTu9irSG2q2b9ALyDEaBvbOUvqzQSW%2FwfssKnHbj4YUpFb7IOPs0FnEK7EN6Buau3%2FJE%2BtCjBzNzSAbnC22cXAMfTmFih31nXLpf3DaiF9N%2F2aCaWsoMb6B4yxrAaoXmPEx0IEIpMgp%2BQHfaHkK1M405mWIpmMNKtrq4GOo8Bj6Hm4U7OF7%2BWn2brcvFSUc15WejOJSfvCQRPhERm60D9jr%2BvuDYWthzTflTQRtVBasd6GOptqLUOiEM%2FzpDsTqaXIxU6p%2F7gfSCZbUbFa4RddZeF3wpb1fk91QGxJKWeoi%2BI78gk7qAE%2BB6oSIM6gBNJ7qyBawCKw%2FWqle06%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

- 93 Click the "Password" field.



- 94 Click "EC2"



95 Click "Instances"

The screenshot shows the AWS EC2 Dashboard. On the left, a sidebar menu has 'Instances' expanded, with 'Instances' highlighted by a red circle. The main content area is titled 'Resources' and displays statistics for the Europe (Stockholm) Region. It includes sections for Instances (running), Auto Scaling Groups, Elastic IPs, Instances, Load balancers (with an API Error notice), Placement groups, Snapshots, and Volumes. Below this is a 'Launch instance' section with a note: 'To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.' A 'Service' dropdown and 'Region' selector are visible on the right.

96 Click "Launch instances"

The screenshot shows the AWS EC2 Instances page. At the top, there are search and filter fields for 've)' and 'Any state'. Below these are filters for 'Instance state', 'Instance type', 'Status check', 'Alarm status', 'Availability Zone', and 'Pub'. The main content area displays a message: 'No instances' and 'You do not have any instances in this region'. A large orange circle highlights the 'Launch instances' button. The top navigation bar includes '[Alt+S]' and other buttons for 'Connect' and 'Inst'.

97

Click here.

The screenshot shows the 'Launch an instance' step in the AWS EC2 wizard. At the top, there's a navigation bar with the AWS logo, 'Services' (with a dropdown arrow), a search bar containing 'Search', and a keyboard shortcut '[Alt+S]'. Below the navigation is a breadcrumb trail: 'EC2 > Instances > Launch an instance'. The main title 'Launch an instance' has an 'Info' link. A descriptive text below says: 'Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.' The first step, 'Name and tags', is selected and has an orange circle highlighting it. It contains a 'Name' field with the placeholder 'e.g. My Web Server' and a 'Add additional tags' link. The second step, 'Application and OS Images (Amazon Machine Image)', is collapsed, indicated by a downward arrow icon.

EC2 Basics Lab

98

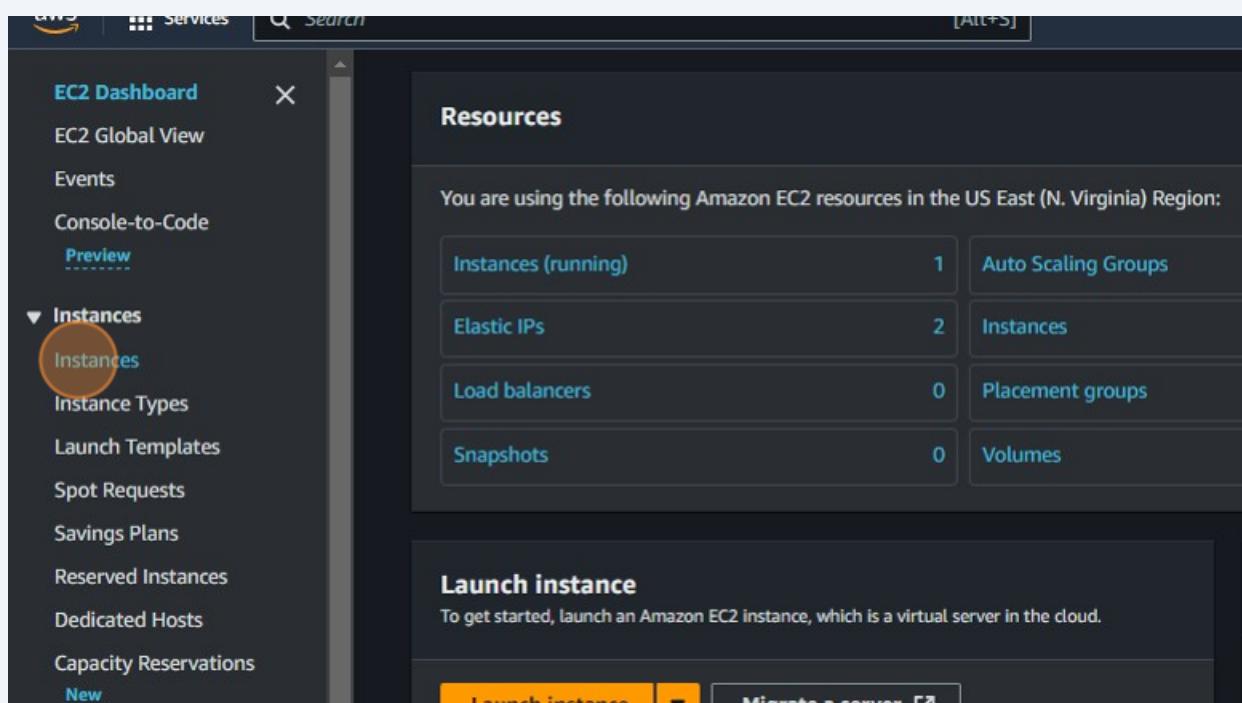
Navigate to

<https://us-east-1.console.aws.amazon.com/console/home?region=us-east-1#>

99 Click "EC2"

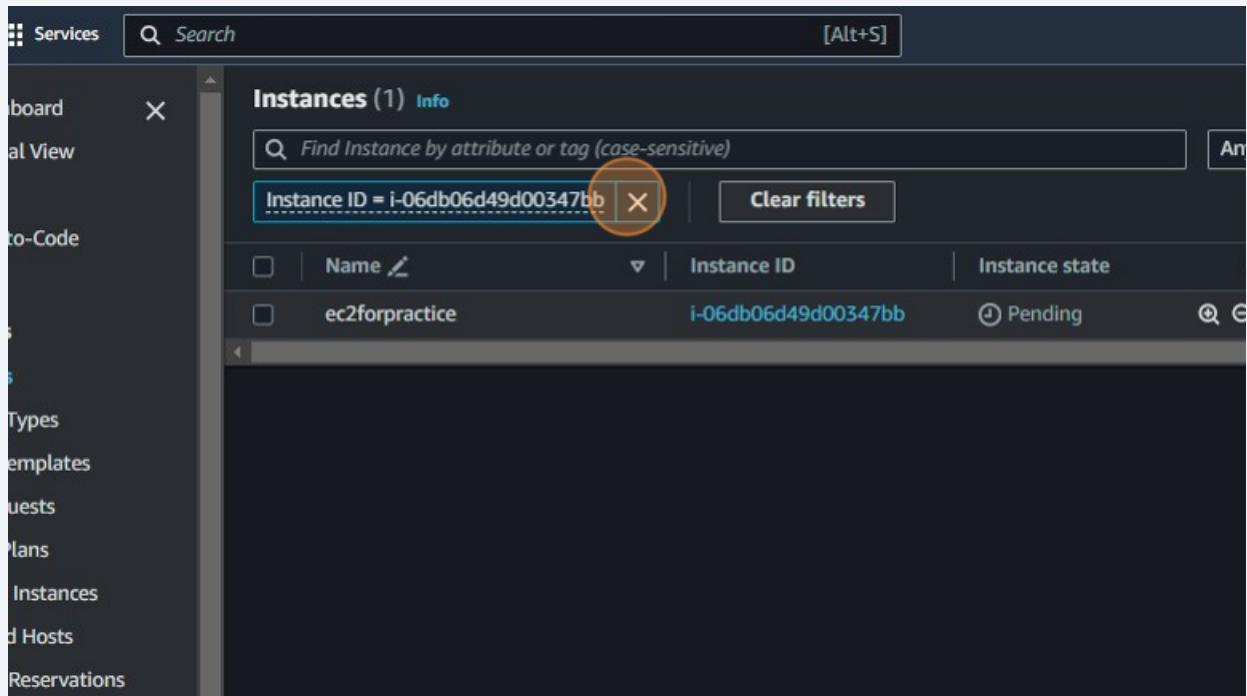


100 Click "Instances"



101 Press **ctrl + v**

102 Click here.



103 Click this checkbox.

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with various EC2-related options like Dashboard, Global View, Events, etc. The main area is titled 'Instances (5)' and lists five instances:

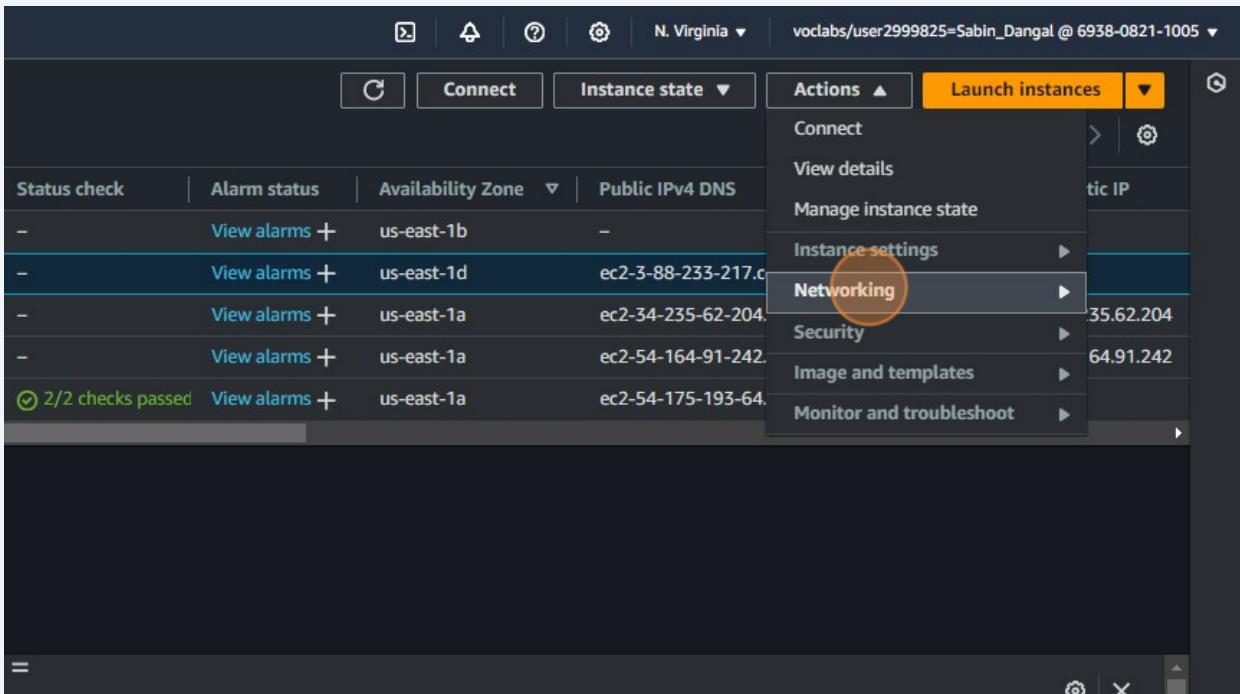
Name	Instance ID	Instance state
MyWebServer	i-0d90eaea164d304c1	Stopped
ec2forpractice	i-06db06d49d00347bb	Pending
InstanceWebServer	i-06982e821bca6fb18	Stopped
IntanceforEC2	i-0df933f671e72ccce	Stopped
myec2	i-0d76ec3e07e5268c0	Running

104 Click here.

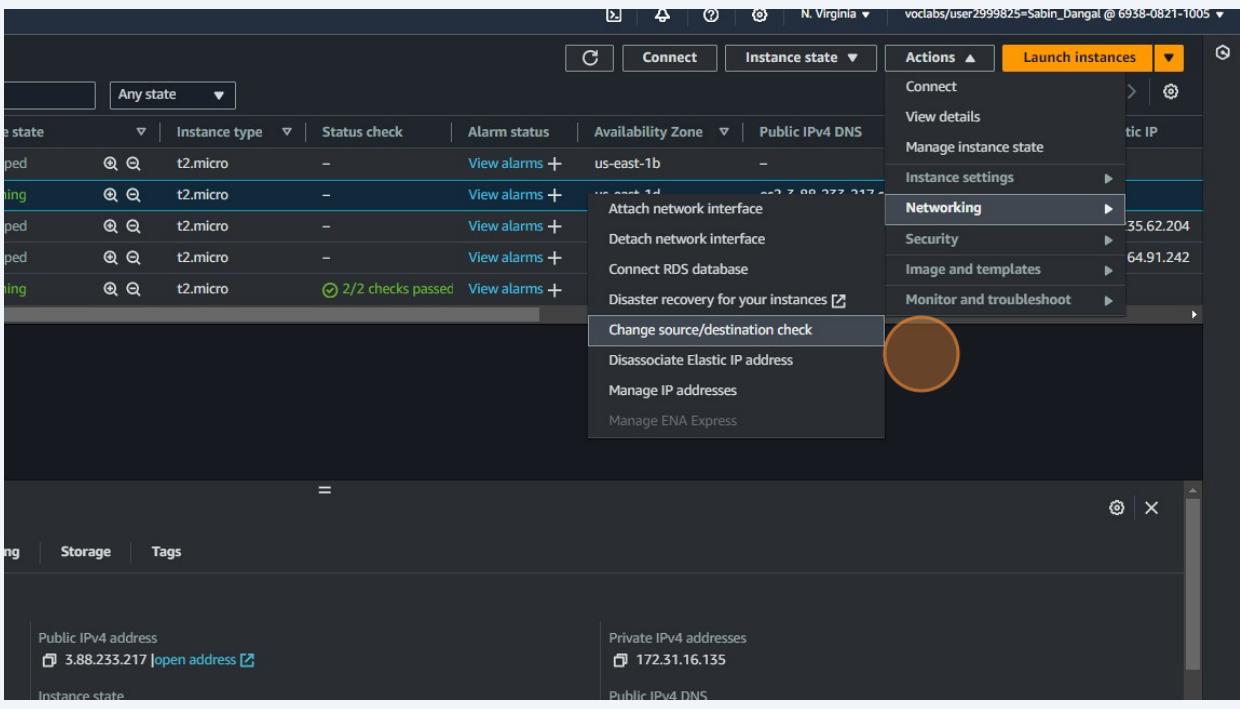
The screenshot shows the AWS EC2 Instances page. At the top, there are several buttons: a magnifying glass, a cloud icon, a question mark, and a gear icon. To the right of these is the region 'N. Virginia'. Further right is a user info bar 'voclabs/user2999825=Sabin_Dangal @ 6938-0821-1005'. The main area displays a table of instances:

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 +	ec2-54-175-193-64.co...	54.175.193.64	-

105 Click "Networking"



106 Click here.



107 Click "Elastic IPs"

The screenshot shows the AWS CloudWatch Metrics interface. On the left, there's a sidebar with navigation links like Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images, AMIs, AMI Catalog, Elastic Block Store, Volumes, Snapshots, Lifecycle Manager, Network & Security (with 'Elastic IPs' highlighted by a red circle), Security Groups, Placement Groups, Key Pairs, Network Interfaces, Load Balancing, Load Balancers, Target Groups, Trust Stores, and CloudWatch Metrics (with a red circle around it). The main area displays a table of metrics. One row is selected, showing details for an instance with the ID i-06db06d49d00347bb. The instance is named 'ec2forpractice', has an auto-assigned IP address of 3.88.233.217, and is running in a t2.micro instance type. It is associated with a VPC ID (vpc-071ae984eaa589e75) and a subnet ID (subnet-07ca46c13ca15d8d6).

108 Click "i-06db06d49d00347bb"

The screenshot shows the AWS Lambda console. At the top, there's a search bar and a button labeled [Alt+S]. Below it, a header says 'Instances (1) Info'. A search bar contains the placeholder 'Find Instance by attribute or tag (case-sensitive)'. To the right is a dropdown menu set to 'Any state'. Underneath, there are filter buttons for 'Instance ID = i-06db06d49d00347bb' and 'Clear filters'. The main table lists one instance: 'ec2forpractice' with the Instance ID 'i-06db06d49d00347bb'. The instance is shown as 'Running' in the 'Instance state' column and 't2.micro' in the 'Instance type' column.

109 Click "Monitoring"

The screenshot shows the AWS EC2 Instances details page for an instance named 'i-06db06d49d00347bb'. The 'Monitoring' tab is highlighted with a red circle. The page displays various instance details such as Public IP, Instance State, and VPC ID.

Category	Value
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
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) (2 minutes)
Lifecycle	normal
Key pair assigned at launch	my-ssh-key
Kernel ID	-

110 Click "Security"

The screenshot shows the AWS CloudWatch Metrics Dashboard for an instance. The 'Security' tab is highlighted with a red circle. The dashboard displays various metrics including CPU utilization, Network in, Network out, Disk reads, Disk write operations, and CPU credit usage.

Metric	Value
CPU utilization (%)	No unit 1 0.5 0
Network in (bytes)	No unit 1 0.5 0
Network out (bytes)	No unit 1 0.5 0
Network packets out (count)	No unit 1 0.5 0
Disk reads (bytes)	No unit 1 0.5 0
Disk read operations (operations)	No unit 1 0.5 0
Disk write operations (operations)	No unit 1 0.5 0
CPU credit usage (count)	No unit 1 0.5 0
CPU credit balance (count)	No unit 1 0.5 0

111 Click "Networking"

The screenshot shows the AWS EC2 instance networking details page. The instance state is Running. The Networking tab is highlighted with a yellow circle. The page displays inbound and outbound security group rules.

Name	Security group rule ID	Port range	Protocol	Source	Security groups	Description
sgr-0bd0bcce70b7f66f2	443	TCP	0.0.0.0/0	launch-wizard-7		-
sgr-0b6b456135ccb23b4	22	TCP	0.0.0.0/0	launch-wizard-7		-
sgr-0d35fb9776331e94e	80	TCP	0.0.0.0/0	launch-wizard-7		-

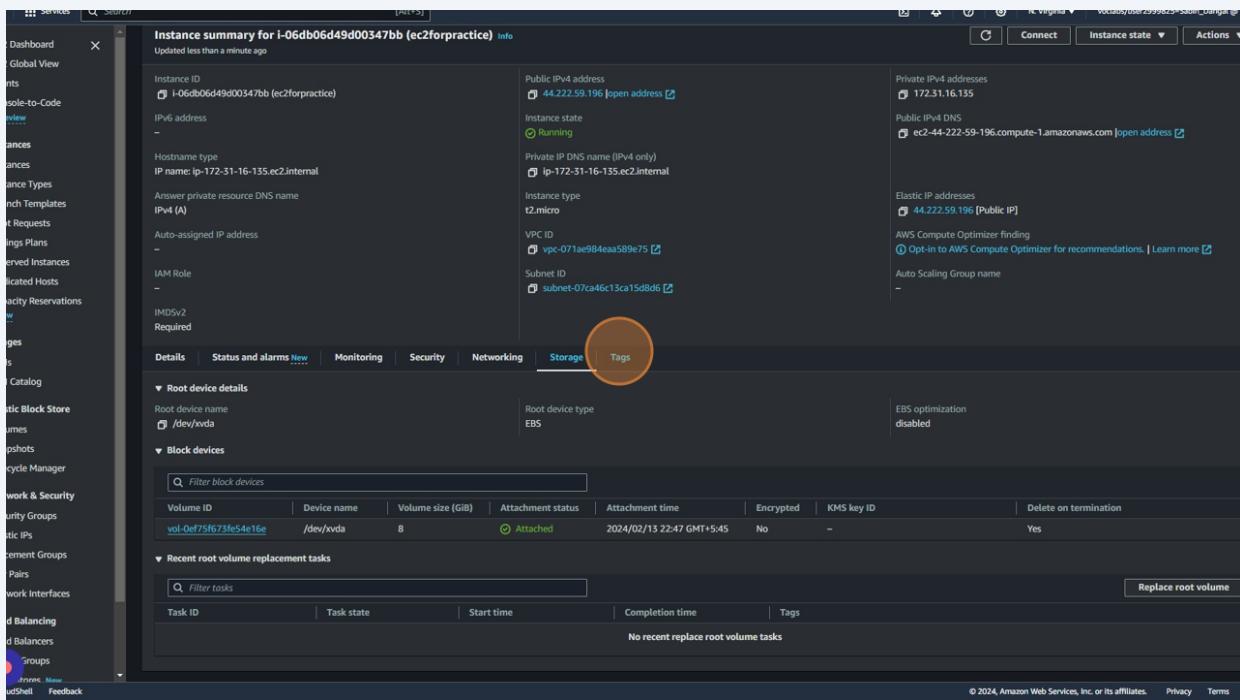
Name	Security group rule ID	Port range	Protocol	Destination	Security groups	Description
sgr-0b841a478a0152377	All	All	0.0.0.0/0	launch-wizard-7		-

112 Click "Storage"

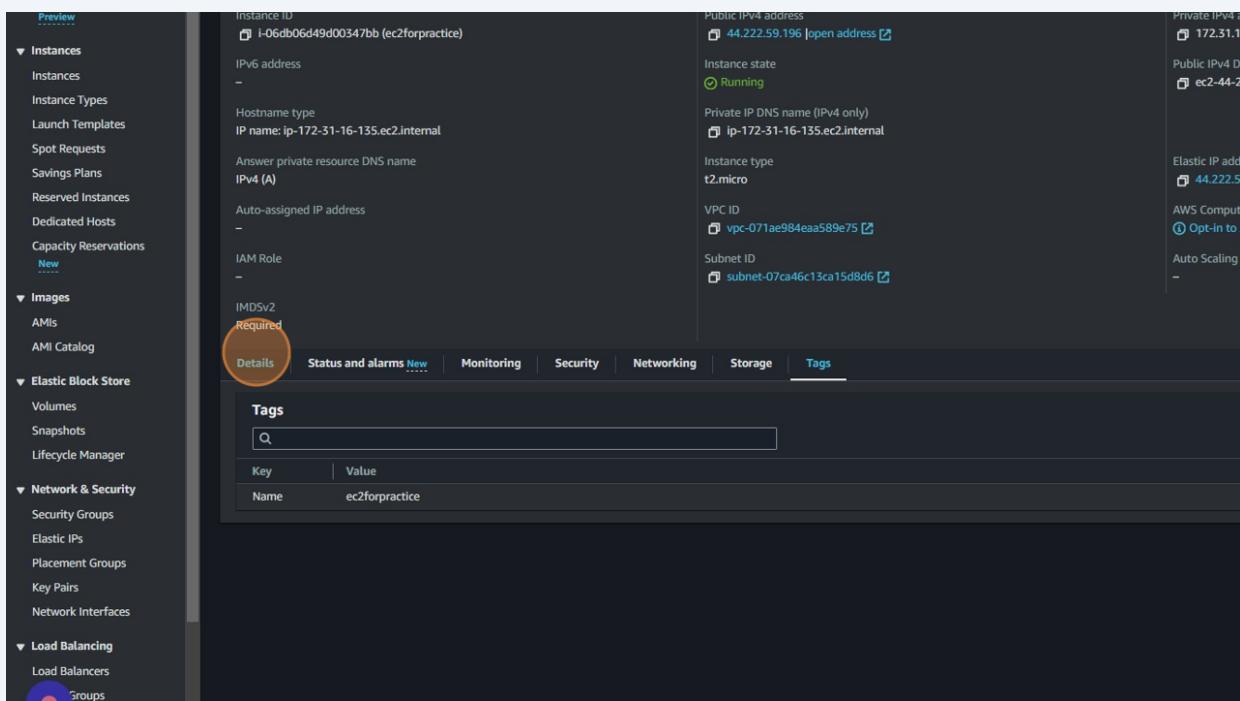
The screenshot shows the AWS EC2 instance storage details page. The instance state is Running. The Storage tab is highlighted with a yellow circle. The page displays networking details, network interfaces, and elastic IP addresses.

Interface ID	Description	IPv4 Prefixes	IPv6 Prefixes	Public IPv4 address	Private IPv4 address	Private IPv4 DNS	IPv6 addresses	Primary IPv6
eni-08a7bf5a64870224f	-	-	-	44.222.59.196	172.31.16.135	ip-172-31-16-135.ec2...	-	-

113 Click "Tags"



114 Click "Details"



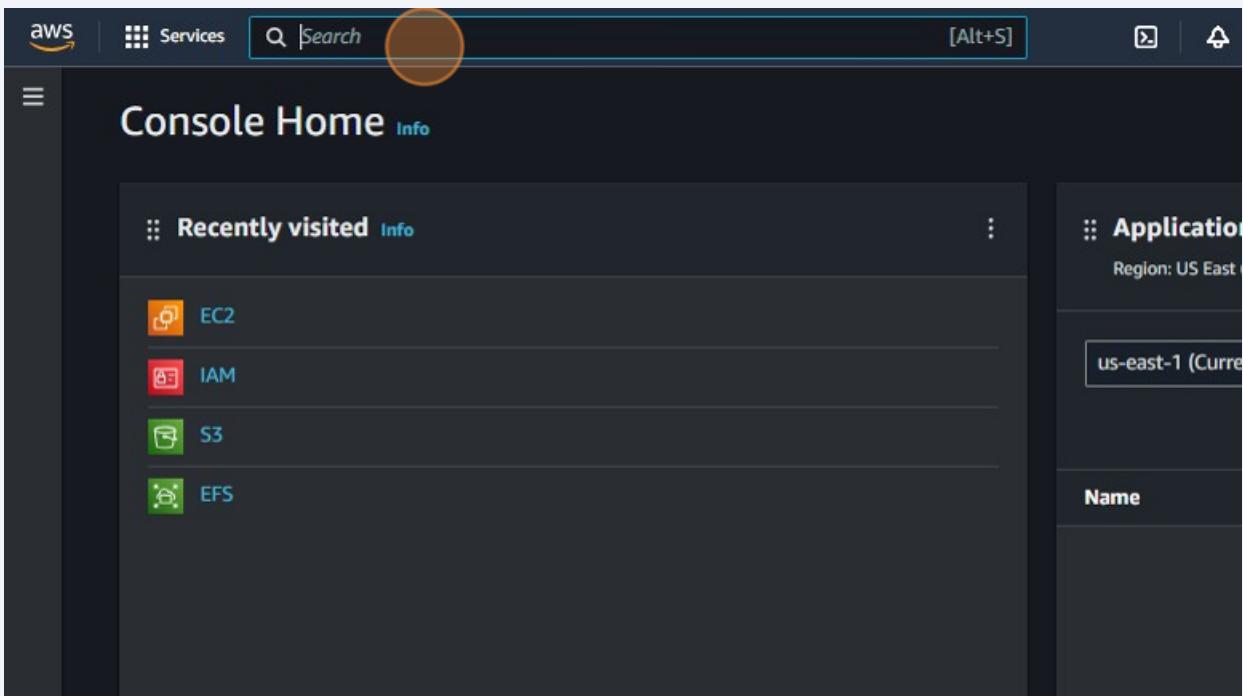
115 Click "Instances"

The screenshot shows the AWS EC2 Instances page. A blue circle highlights the 'Instances' link in the left navigation bar. The main content area displays detailed information for a single instance, 'i-06db06d49d00347bb (ec2forpractice)'. The instance is currently running. Key details include its public IP address (44.222.59.196), private IP address (172.31.16.135), and AMI ID (ami-0e731c8a58825bd0). The instance was launched on February 13, 2024, at 22:47:30 GMT+0545 (Nepal Time). The status bar at the bottom indicates the instance was created 3 minutes ago.

VPC

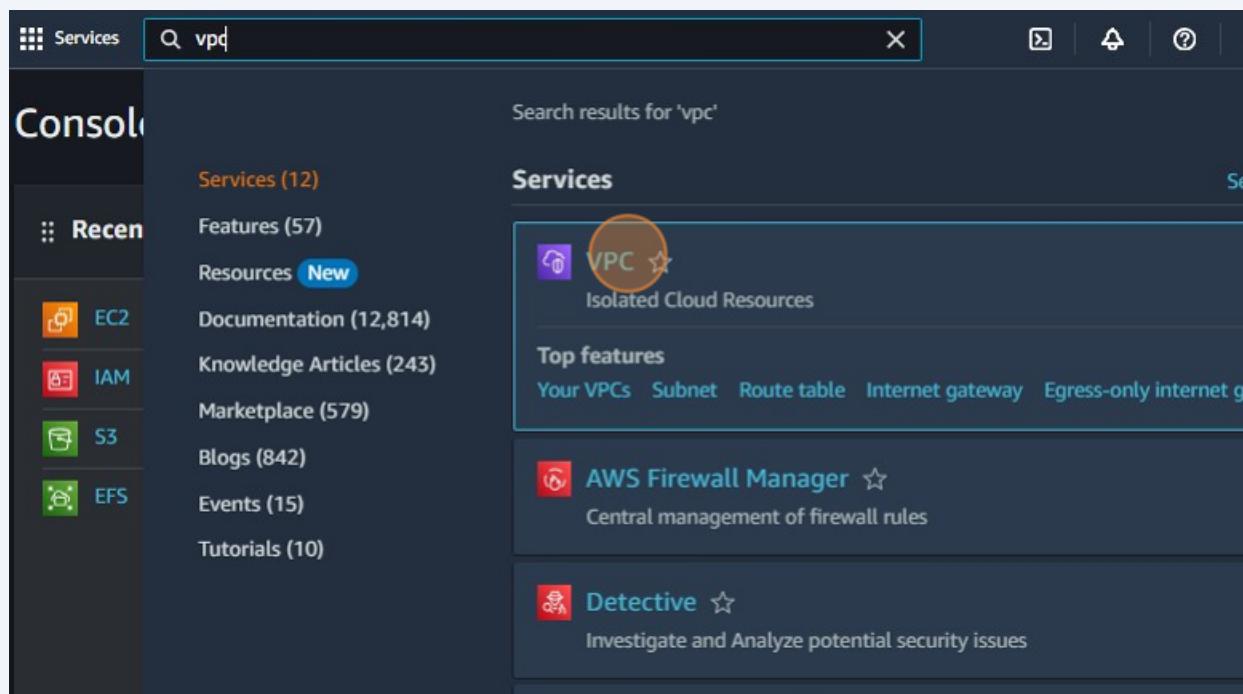
116 Navigate to <https://us-east-1.console.aws.amazon.com/console/home?region=us-east-1#>

117 Click the "Search" field.

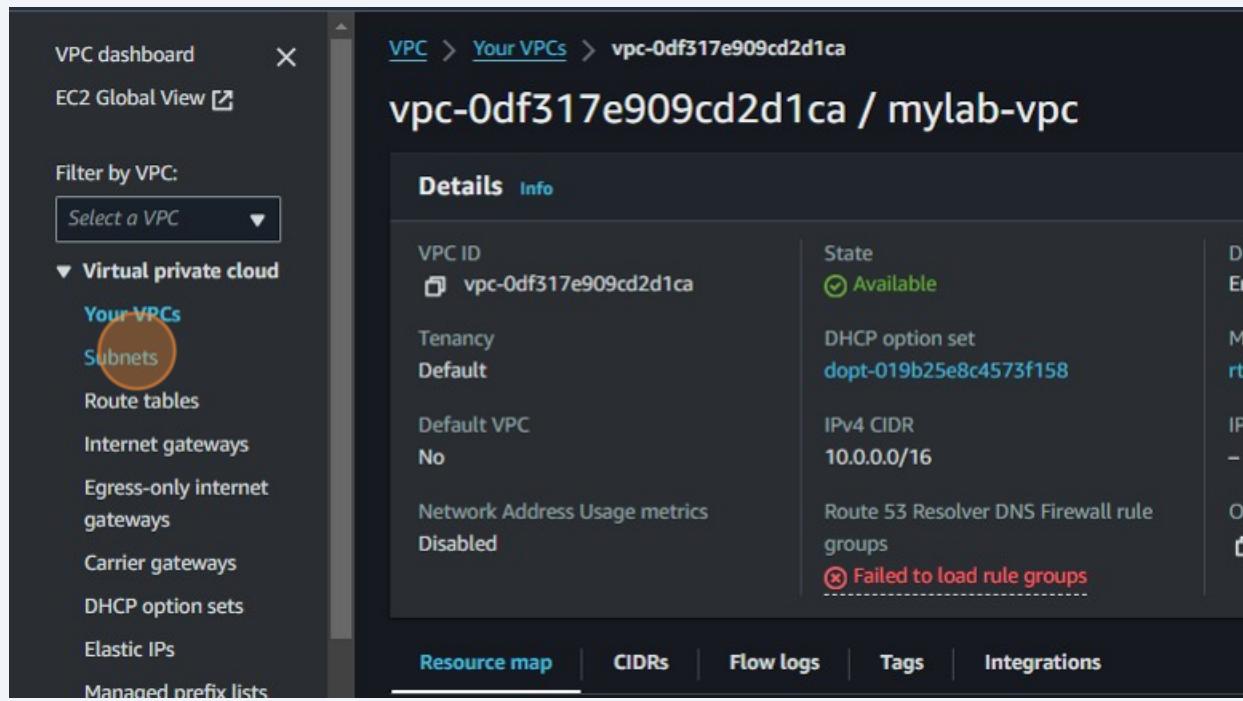


118 Type "vpc"

119 Click "VPC"



120 Click "Subnets"



- 121 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 ▾

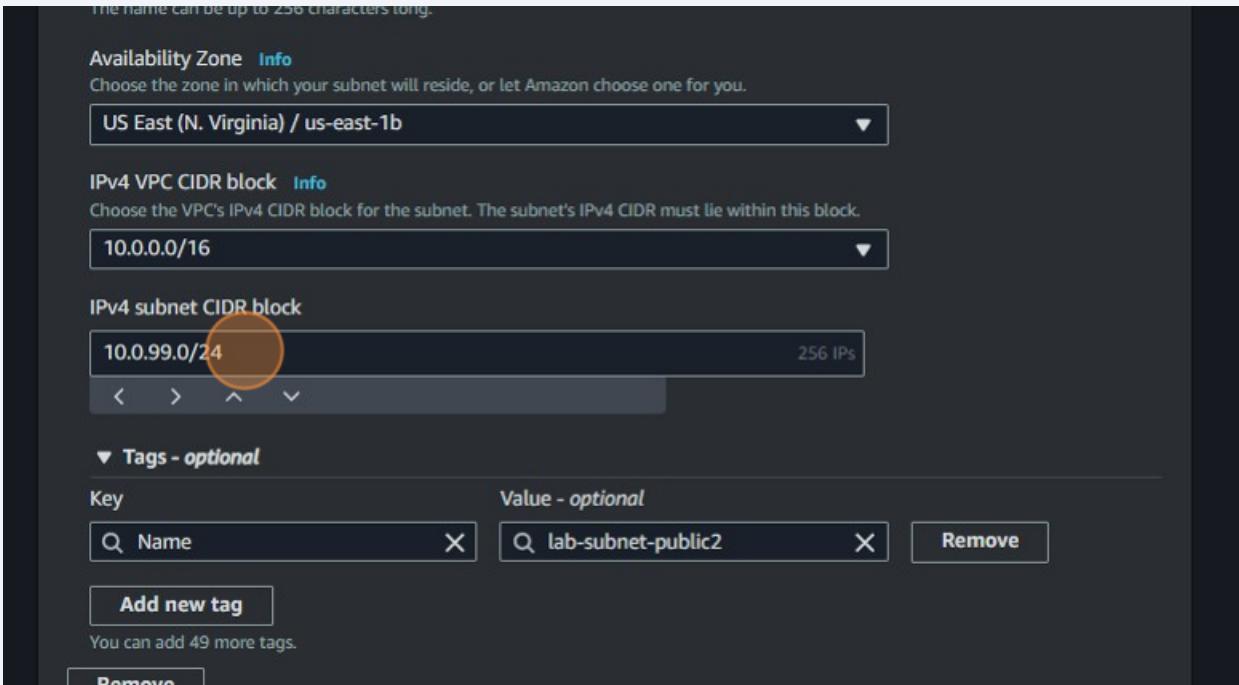
IPv4 VPC CIDR block [Info](#)
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/16 ▾

IPv4 subnet CIDR block
10.0.99.0/24 256 IPs
< > ^ v

Tags - optional

Key	Value - optional	Remove
<input type="text" value="Name"/> X	<input type="text" value="lab-subnet-public2"/> X	Remove

Add new tag
You can add 49 more tags.
Remove



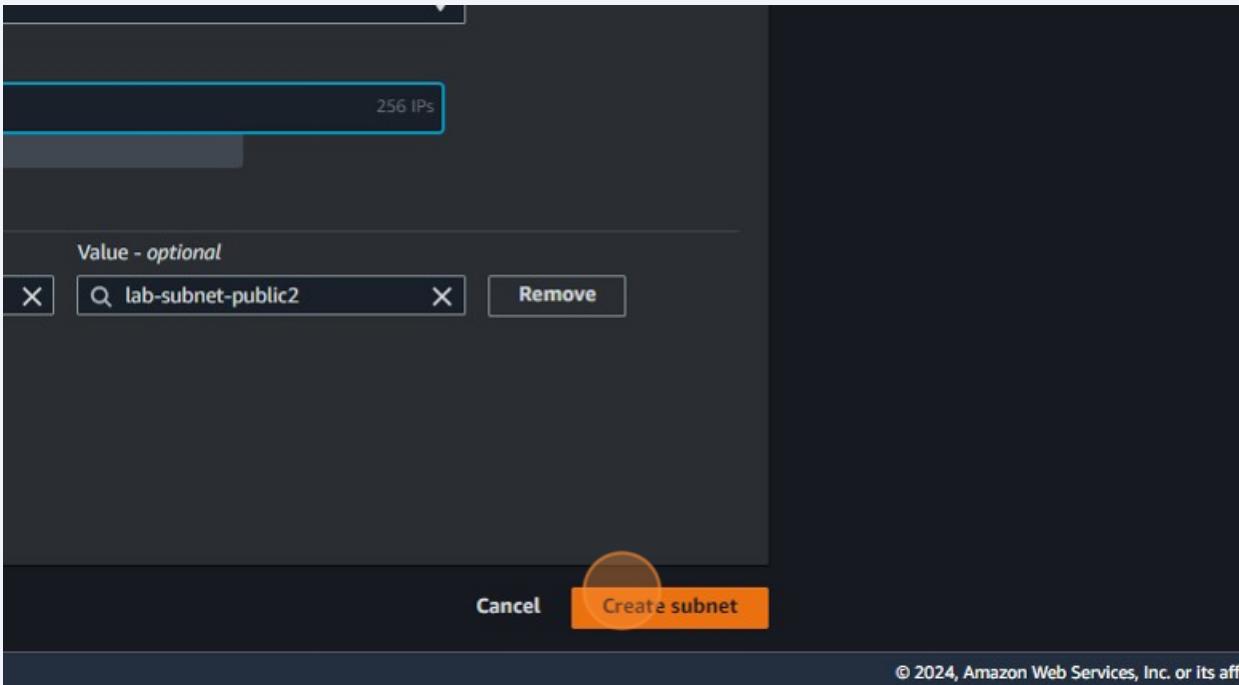
- 122 Click "Create subnet"

256 IPs

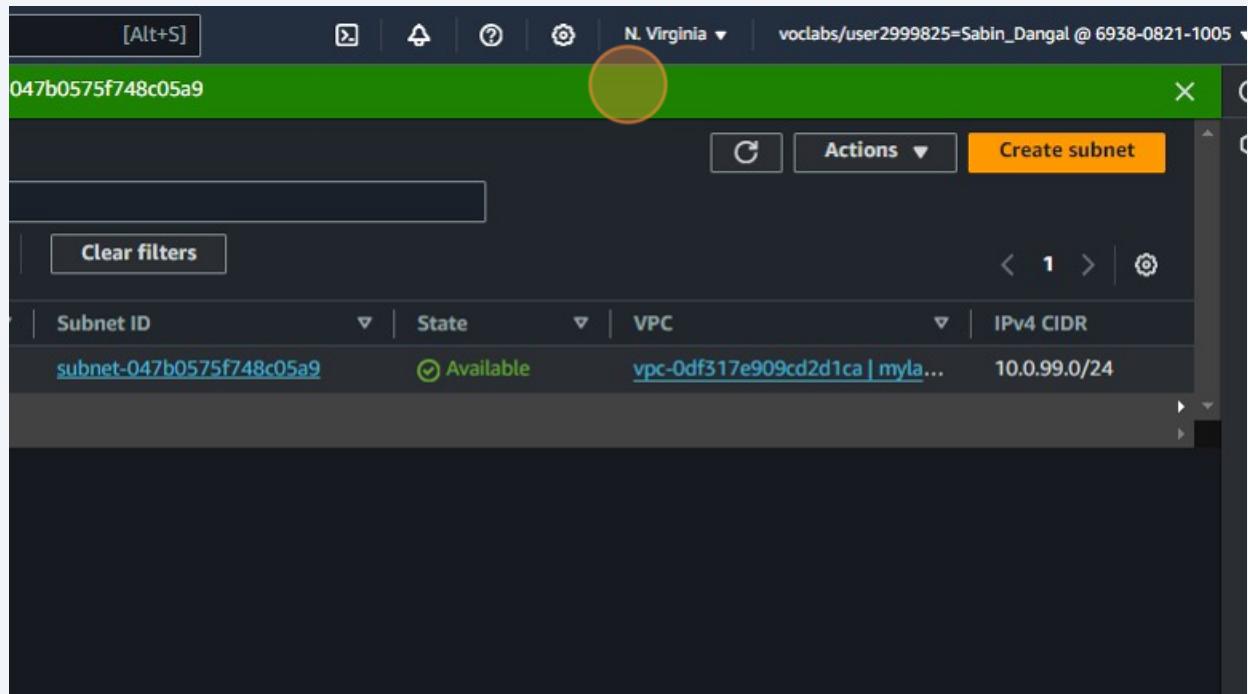
Value - optional
 X Remove

Cancel Create subnet

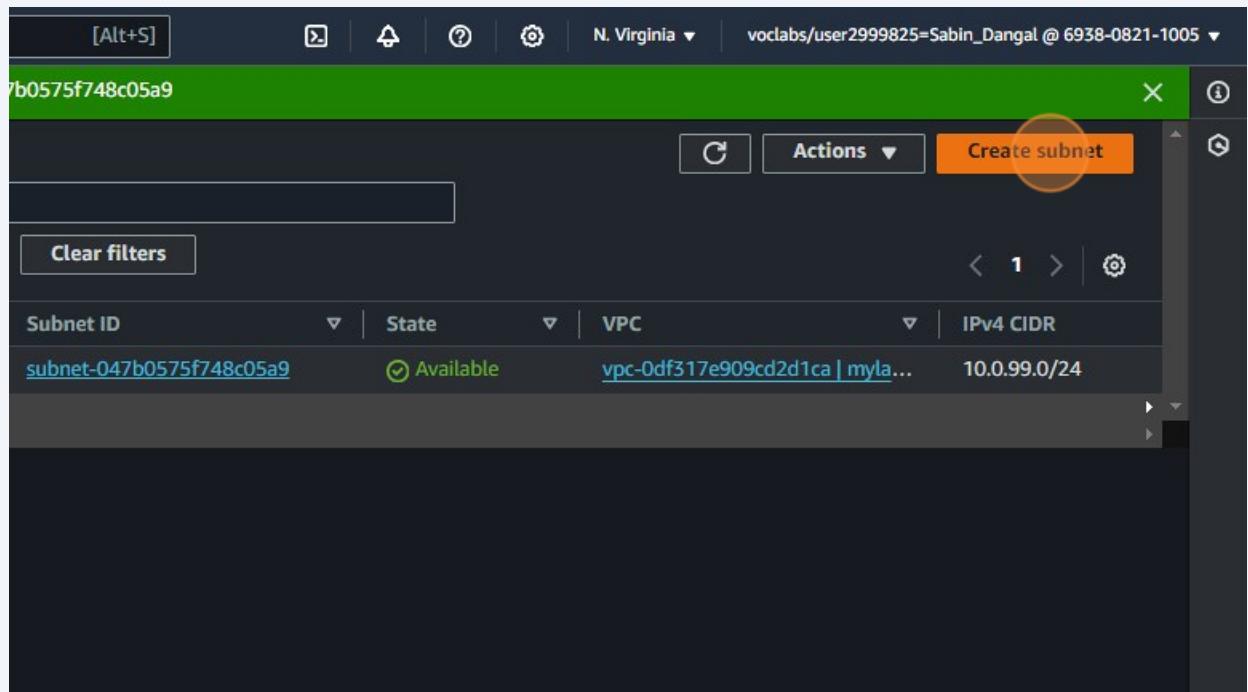
© 2024, Amazon Web Services, Inc. or its affiliates



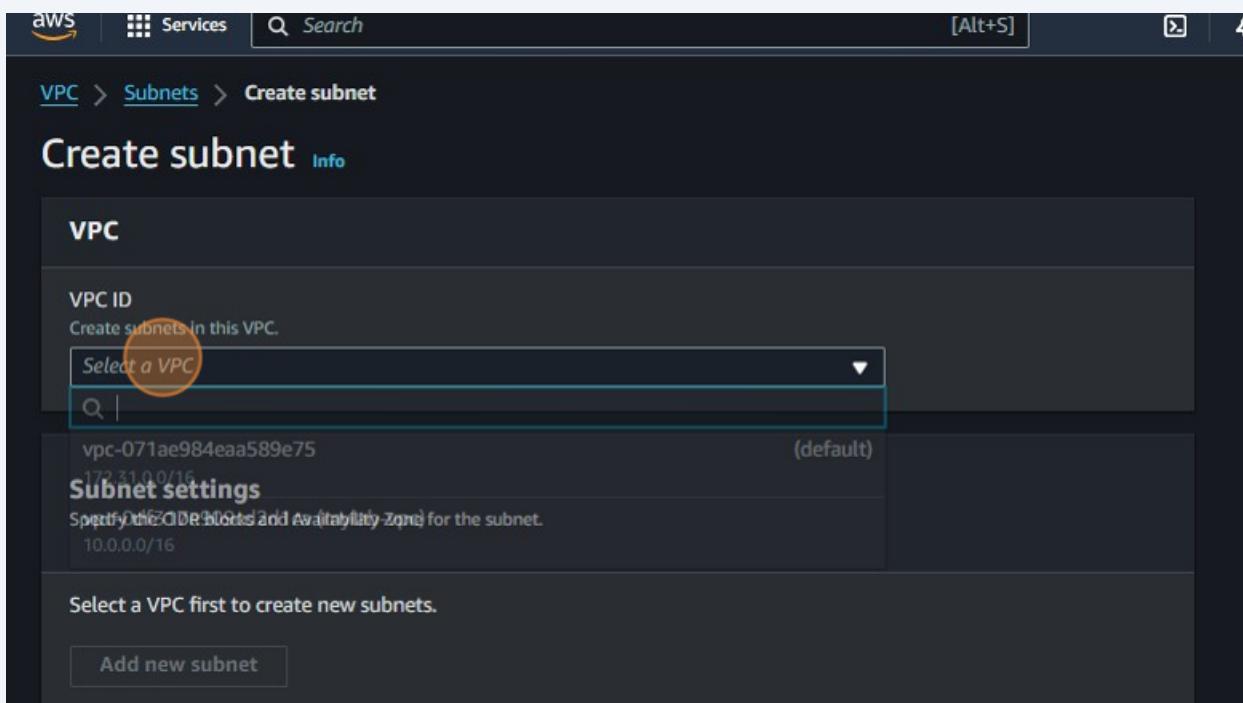
123 Click "You have successfully created 1 subnet: subnet-047b0575f748c05a9"



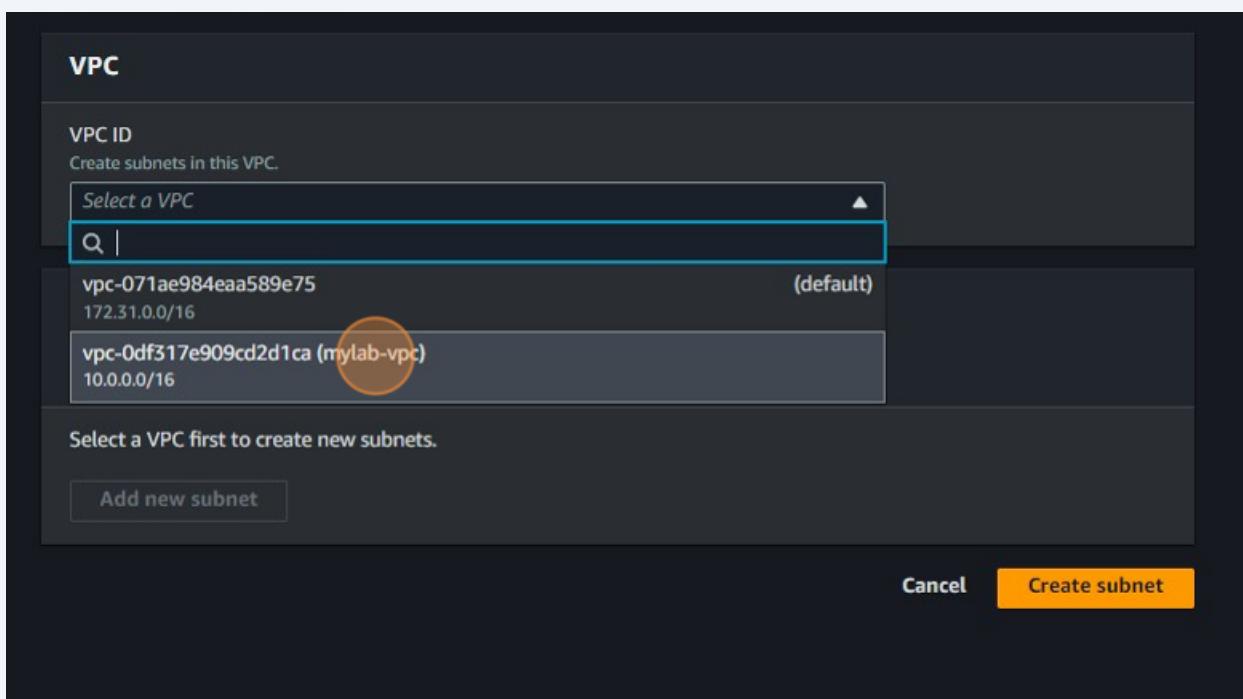
124 Click "Create subnet"



125 Click "Select a VPC"



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



127 Click the "Subnet name" field.

The screenshot shows the 'Subnet settings' page for creating a new subnet. The 'Subnet 1 of 1' section is displayed. The 'Subnet name' field contains the value 'my-subnet-01', which is circled in red. Below the field, a note states: 'The name can be up to 256 characters long.' The 'Availability Zone' dropdown is set to 'No preference'. The 'IPv4 VPC CIDR block' dropdown is set to '10.0.0.0/16'. The 'IPv4 subnet CIDR block' field is empty.

128 Type "mylab-subnet-private2"

129 Click "No preference"

The screenshot shows the AWS VPC console interface for creating a new subnet. The 'Availability zone' dropdown menu is open, displaying several options. The option 'No preference' is highlighted and circled in red. Other visible options include 'us-east-1a', 'us-east-1b', 'us-east-1c', 'us-east-1d', 'us-east-1e', and 'us-east-1f'. The 'Availability zone' label is preceded by a question mark icon.

ID: use1-az1 Network border group: us-east-1

Subnet 1 of 1 (N. Virginia) / us-east-1c us-east-1

ID: use1-az2 Network border group: us-east-1

Subnet name us-east-1

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

ID: use1-az4 Network border group: us-east-1

mylab-subnet-private2 us-east-1

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

The name can be up to 256 characters long.

Availability zone **No preference** us-east-1

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

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

< > ^ v

▼ Tags - optional

130 Click "us-east-1"

The screenshot shows the AWS VPC console interface for associating a CIDR block with a subnet. The 'Associated VPC CIDRs' dropdown menu is open, displaying several options. The option 'us-east-1' is highlighted and circled in red. Other visible options include 'No preference', 'us-east-1a', 'us-east-1b', 'us-east-1c', 'us-east-1d', 'us-east-1e', and 'us-east-1f'. The 'Associated VPC CIDRs' label is preceded by a question mark icon.

Associated VPC CIDRs

IPv4 CIDRs

10.0.0.0/16

Q |

No preference ✓

us-east-1 us-east-1

us-east-1a us-east-1

us-east-1b us-east-1

us-east-1c us-east-1

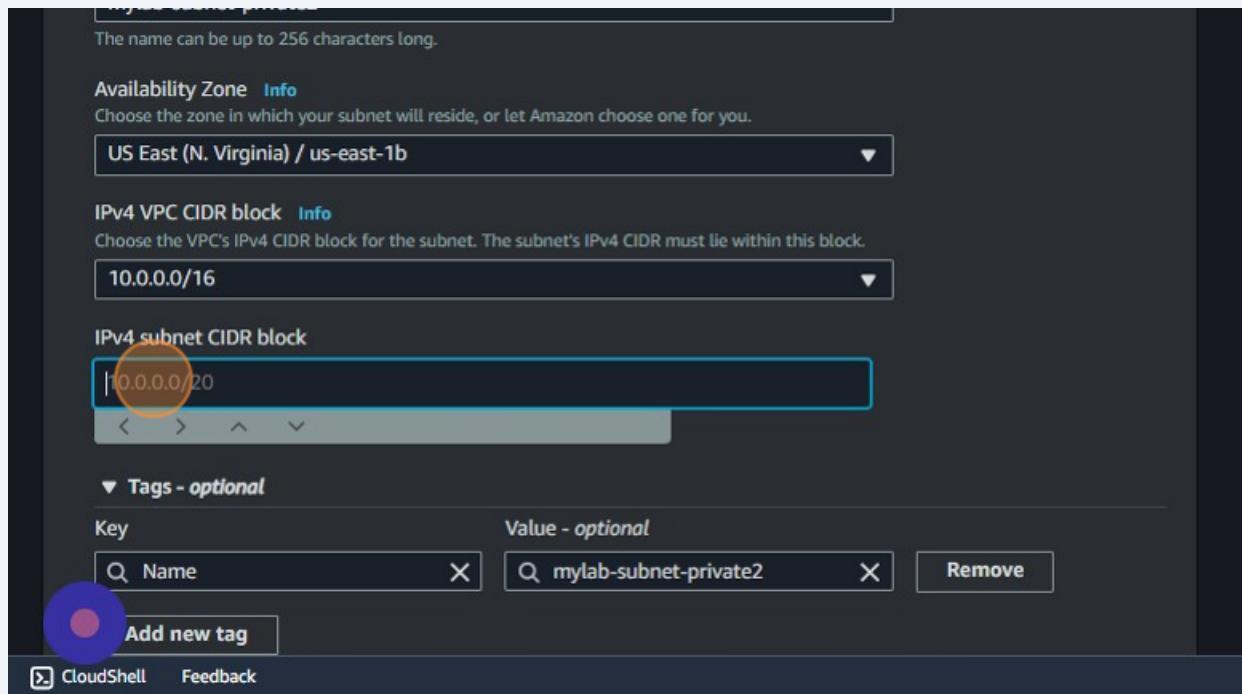
us-east-1d us-east-1

us-east-1e us-east-1

us-east-1f us-east-1

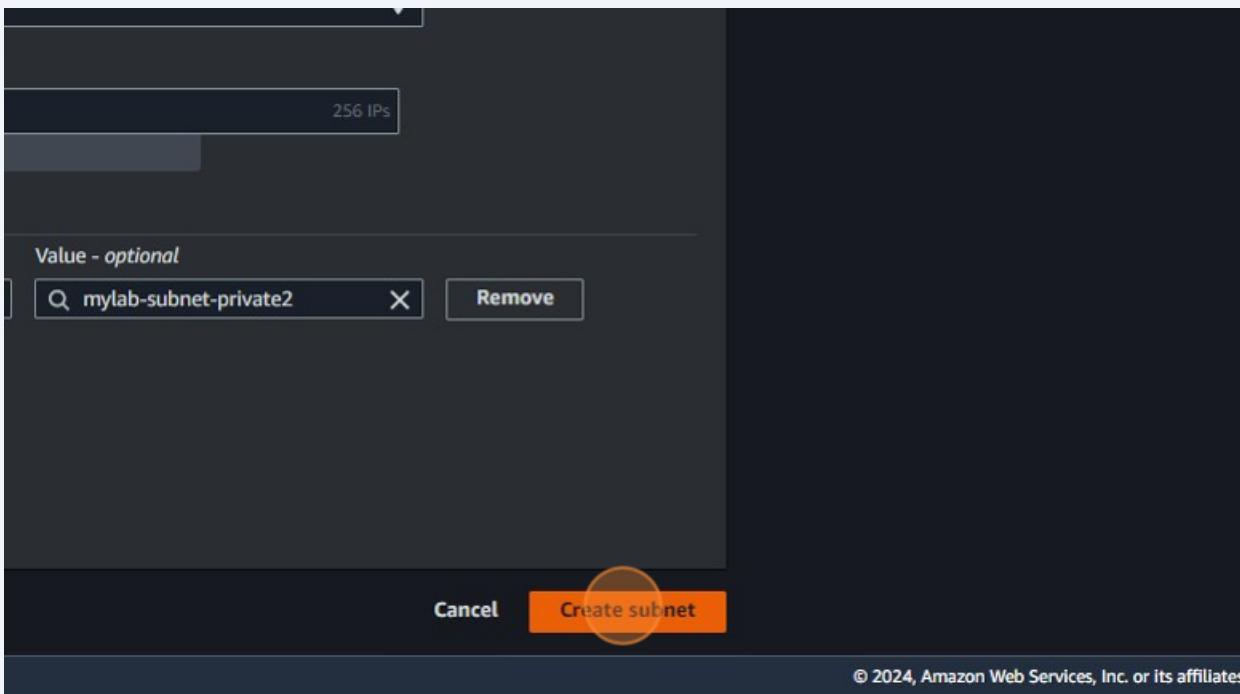
No preference

131 Click the "10.0.0.0/20" field.

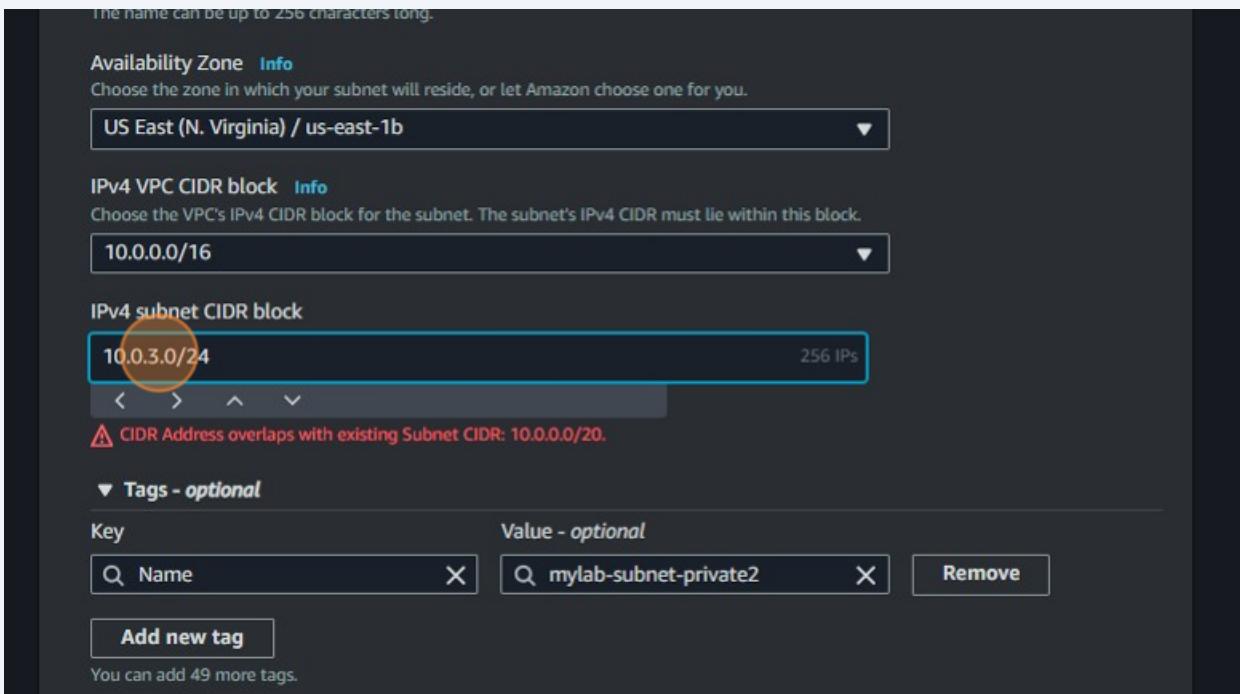


132 Type "10.0.3.0/24"

133 Click "Create subnet"

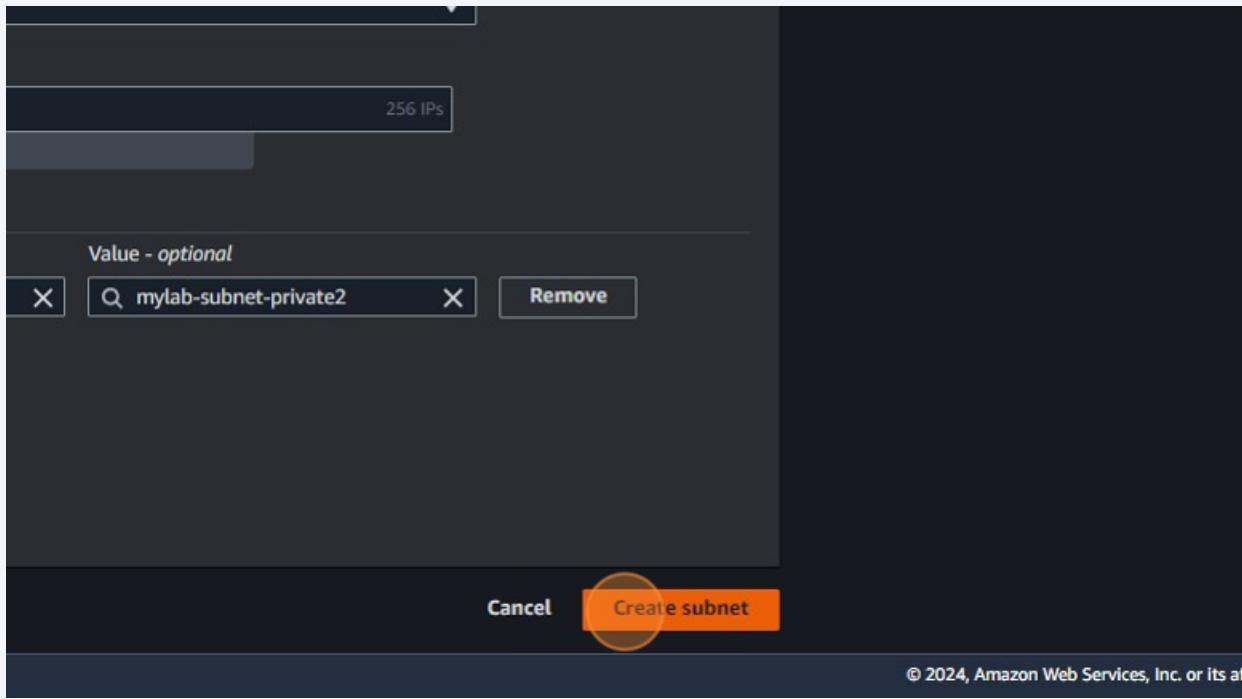


134 Click the "10.0.0.0/20" field.

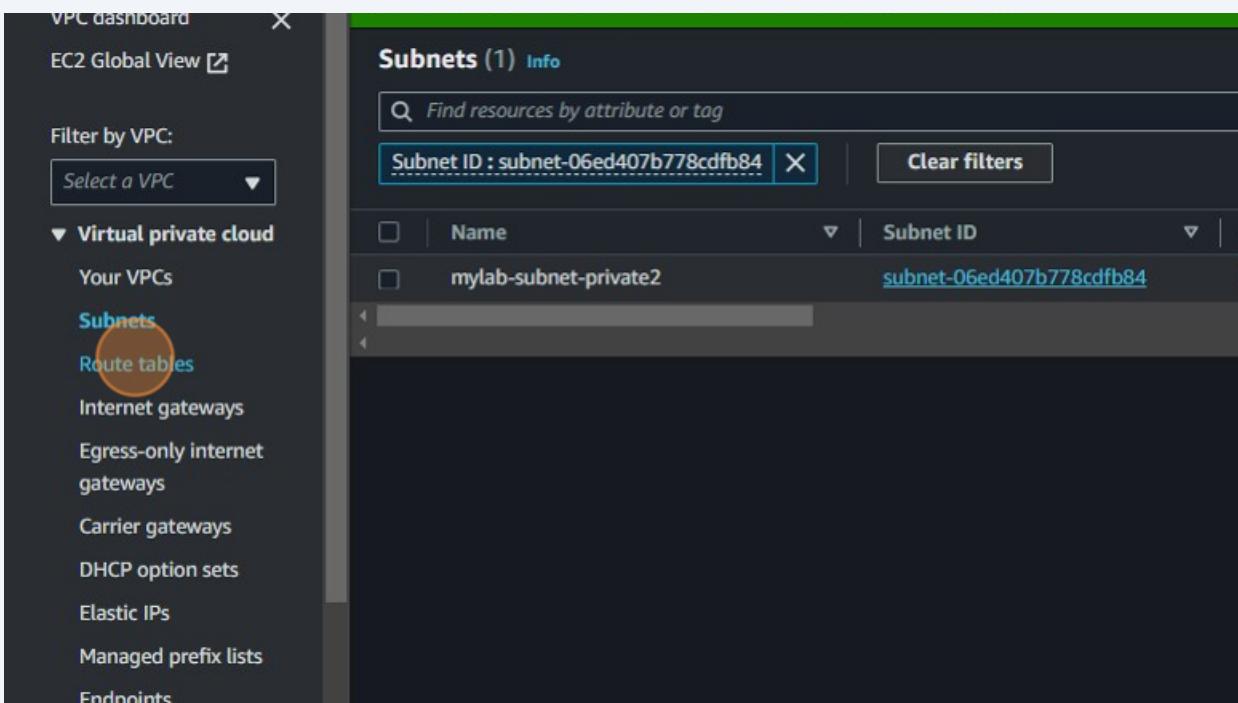


135 Type " Backspace 98"

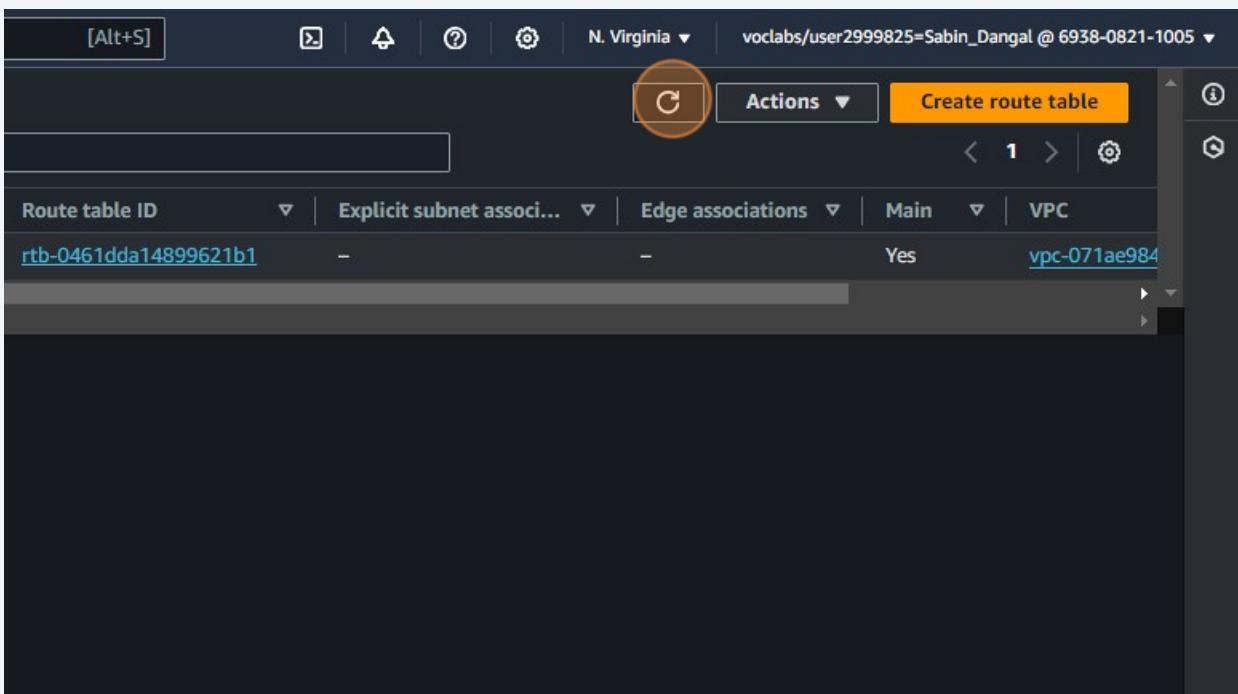
136 Click "Create subnet"



137 Click "Route tables"



138 Click here.



139 Click this checkbox.

The screenshot shows the AWS VPC dashboard. On the left, there's a sidebar with 'Virtual private cloud' selected, which has 'Route tables' highlighted. The main area shows a table titled 'Route tables (4)'. The first row, which is 'mylab-rtb-public', has its checkbox circled in orange. The table columns are 'Name', 'Route table ID', and 'Expl'.

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

140 Click "Routes"

The screenshot shows the details for a specific route table. The sidebar on the left lists various network components, and 'Security' is expanded to show 'Network ACLs' and 'Security groups'. The main panel displays the route table details for 'rtb-01f409cb7cd51918f / mylab-rtb-private1-us-east-1a'. The 'Routes' tab is highlighted with an orange circle. Below it, the 'Details' tab is active, showing information like Route table ID, Main, VPC, and Owner ID.

Route table ID	Main
rtb-01f409cb7cd51918f	No

VPC: [vpc-0df317e909cd2d1ca | mylab-vpc](#)

Owner ID: 693808211005

141 Click "0.0.0.0/0"

The screenshot shows the AWS CloudFormation console with a sidebar containing navigation links like 'Carrier gateways', 'CP option sets', 'Static IPs', etc. The main area displays a route table named 'rtb-01f409cb7cd51918f / mylab-rtb-private1-us-east-1a'. The 'Routes' tab is selected, showing three routes:

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

142 Click "Subnet associations"

The screenshot shows the AWS CloudFormation console with a sidebar containing navigation links like 'Carrier gateways', 'CP option sets', 'Static IPs', etc. The main area displays a route table named 'rtb-01f409cb7cd51918f / mylab-rtb-private1-us-east-1a'. The 'Subnet associations' tab is selected, showing three subnet associations:

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

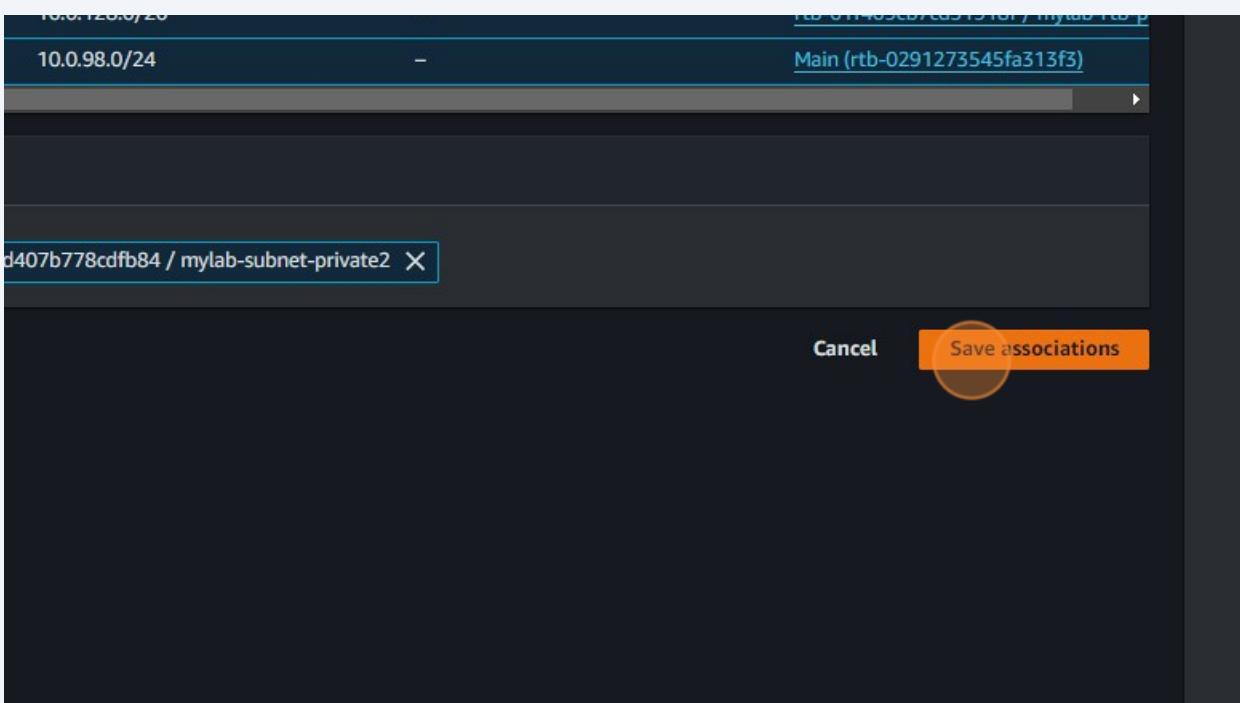
143 Click "Edit subnet associations"

The screenshot shows the AWS Lambda console with the Route propagation tab selected for a specific route table. At the top right of the main content area, there is a button labeled "Edit subnet associations". This button is highlighted with a yellow circle. Below it, there is a table with two columns: "Subnet ID" and "IPv4 CIDR". One row is selected, showing "subnet-0d4231859862e4b69" and "10.0.128.0/20". Further down, there is another section with a table and a "Edit subnet associations" button, also highlighted with a yellow circle.

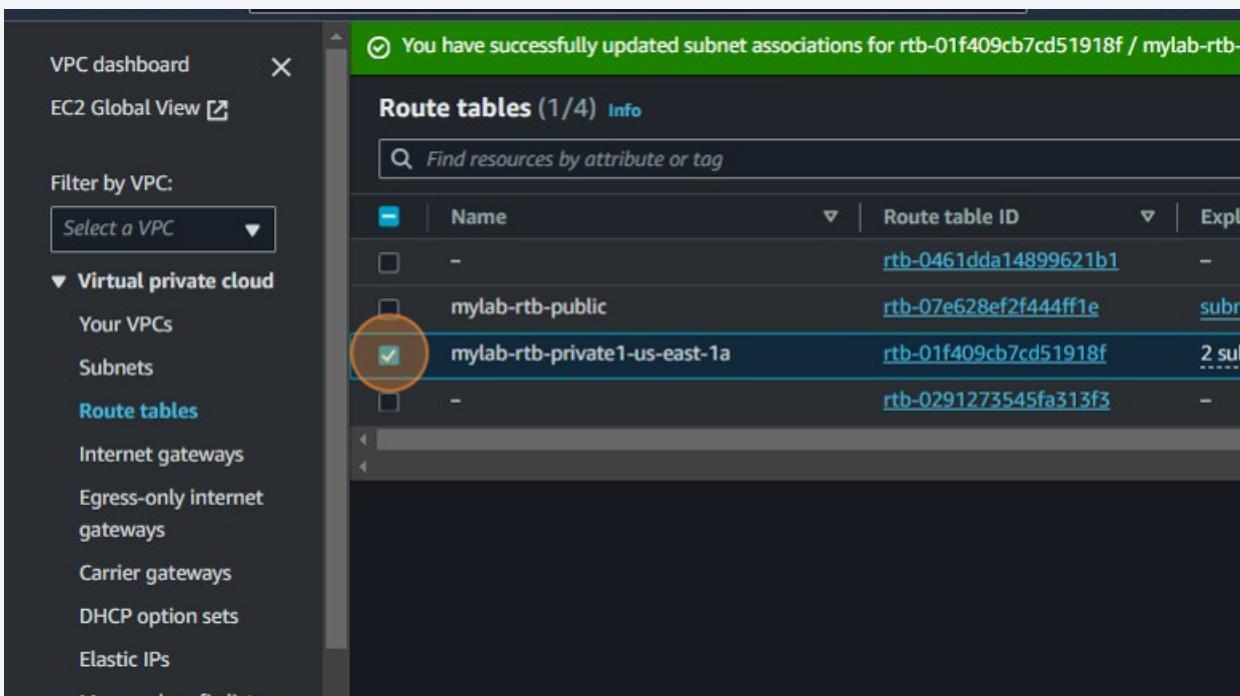
144 Click this checkbox.

The screenshot shows the AWS Lambda console with the Available subnets section. There is a table with columns: Name, Subnet ID, and IPv4 CIDR. Several subnets are listed, including "mylab-subnet-public1-us-east-1a", "lab-subnet-public2", "mylab-subnet-private1-us-east-1a" (which has a checked checkbox and is highlighted with a yellow circle), and "mylab-subnet-private2". Below the table, there is a section titled "Selected subnets" containing a single item: "subnet-0d4231859862e4b69 / mylab-subnet-private1-us-east-1a".

145 Click "Save associations"



146 Click this checkbox.



147 Click this checkbox.

The screenshot shows the AWS VPC dashboard. On the left, there's a sidebar with 'Virtual private cloud' selected. Under 'Route tables', a checkbox is highlighted with a red circle. The main area shows a table of route tables with columns for Name, Route table ID, and Subnets. One row for 'mylab-rtb-public' has its checkbox highlighted.

Name	Route table ID	Subnets
-	rtb-0461dda14899621b1	-
mylab-rtb-public	rtb-07e628ef2f444ff1e	sub
mylab-rtb-private1-us-east-1a	rtb-01f409cb7cd51918f	2 sub
-	rtb-0291273545fa313f3	-

148 Click "Routes"

The screenshot shows the details page for a specific route table. The left sidebar lists various network components like Elastic IPs, Managed prefix lists, and Network ACLs. The main panel displays the route table details for 'rtb-07e628ef2f444ff1e / mylab-rtb-public'. The 'Routes' tab is selected and highlighted with a red circle. Below it, the 'Details' section shows information such as Route table ID, Main status, VPC, and Owner ID.

Route table ID	Main
rtb-07e628ef2f444ff1e	No

VPC: [vpc-0df317e909cd2d1ca | mylab-vpc](#)

Owner ID: 693808211005

149 Click "0.0.0.0/0"

Details Routes Subnet associations Edge associations Route propagation

Routes (2)

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

150 Click "Subnet associations"

Details Routes **Subnet associations** Edge associations Route propagation

Routes (2)

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

151 Click here.

The screenshot shows the AWS Route Tables interface for a specific route table. The left sidebar includes options like 'Connections', 'ACLs', 'Groups', 'Firewall', 'Policies', and 'Feedback'. The main content area displays the route table details: 'rtb-07e628ef2f444ff1e / mylab-rtb-public'. Below this, there are tabs for 'Details', 'Routes', 'Subnet associations' (which is selected), 'Edge associations', 'Route propagation', and 'Tags'. The 'Subnet associations' section contains two sections: 'Explicit subnet associations (1)' and 'Subnets without explicit associations (1)'. The first section lists a single association: 'mylab-subnet-public1-us-east-1a' with Subnet ID 'subnet-011b2fb7ad76ed850' and IPv4 CIDR '10.0.0.0/20'. The second section lists a single subnet: 'lab-subnet-public2' with Subnet ID 'subnet-047b0575f748c05a9' and IPv4 CIDR '10.0.99.0/24'. A search bar labeled 'Find subnet association' is present in both sections. The bottom right corner of the interface shows the date '© 2024'.

152 Click "Edit subnet associations"

This screenshot shows the same AWS Route Tables interface as the previous one, but with a different focus. The 'Edit subnet associations' button in the 'Subnet associations' section of the 'Subnets without explicit associations' table is highlighted with a large orange circle. The table structure is identical to the previous screenshot, showing the subnet 'lab-subnet-public2' with Subnet ID 'subnet-047b0575f748c05a9' and IPv4 CIDR '10.0.99.0/24'. The interface also includes tabs for 'Edge associations', 'Route propagation', and 'Tags'.

153 Click this checkbox.

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/4)

	Name	Subnet ID	IPv4 CIDR
<input checked="" type="checkbox"/>	mylab-subnet-public1-us-east-1a	subnet-011b2fb7ad76ed850	10.0.0.0/20
<input type="checkbox"/>	lab-subnet-public2	subnet-047b0575f748c05a9	10.0.99.0/24
<input type="checkbox"/>	mylab-subnet-private1-us-east-1a	subnet-0d4231859862e4b69	10.0.128.0/20
<input type="checkbox"/>	mylab-subnet-private2	subnet-06ed407b778cd84	10.0.98.0/24

Selected subnets

[subnet-011b2fb7ad76ed850 / mylab-subnet-public1-us-east-1a X](#)

154 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 X](#)

Cancel **Save associations**

155 Click here.

The screenshot shows the AWS Route Tables page. At the top, there's a header bar with various icons and the text "N. Virginia". Below it, a green banner displays the message "for rtb-07e628ef2f444ff1e / mylab-rtb-public.". The main area is a table with the following columns: Route table ID, Explicit subnet associations, Edge associations, Main, and VPC. There are four rows in the table:

Route table ID	Explicit subnet associations	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

156 Click this button.

The screenshot shows the AWS Route Tables page. At the top, there's a header bar with various icons and the text "N. Virginia". Below it, a green banner displays the message "for rtb-07e628ef2f444ff1e / mylab-rtb-public.". The main area is a table with the following columns: Route table ID, Explicit subnet associations, Edge associations, Main, and VPC. There are four rows in the table:

Route table ID	Explicit subnet associations	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

157 Click "2 subnets"

Route table ID	Explicit subnet associations	Main	VPC
rtb-0461dda14899621b1	-	Yes	vpc-071ae98
rtb-07e628ef2f444ff1e	<u>2 subnets</u>	No	vpc-0df317e
rtb-01f409cb7cd51918f	<u>2 subnets</u>	No	vpc-0df317e
rtb-0291273545fa313f3	-	Yes	vpc-0df317e

158 Click "Security groups"

The screenshot shows the AWS Lambda service configuration page. On the left, there's a sidebar with various navigation options: Elastic IPs, Managed prefix lists, Endpoints, Endpoint services, NAT gateways, Peering connections, Security (which is expanded), Network ACLs, Security groups (which is also expanded and circled in orange), DNS firewall, Rule groups, Domain lists, Network Firewall (which is expanded), Firewalls, Firewall policies, and Network Firewall rule. The main pane displays the details for the security group associated with the route table. The title is "rtb-01f409cb7cd51918f / mylab-rtb-private1-us-east-1a". The "Details" tab is selected, showing the following information:

Route table ID	Main
rtb-01f409cb7cd51918f	No

Other tabs visible include Routes, Subnet associations, Edge associations, and Route properties.

159 Click "Your VPCs"

The screenshot shows the AWS VPC dashboard. On the left, a sidebar menu under 'Virtual private cloud' includes 'Your VPCs' (which is circled in orange), 'Subnets', 'Route tables', 'Internet gateways', 'Egress-only internet gateways', 'Carrier gateways', 'DHCP option sets', and 'Elastic IPs'. At the top right, there are buttons for 'Create VPC' and 'Launch EC2 Instances'. A note says 'Note: Your Instances will launch in the US East region.' Below this, a section titled 'Resources by Region' lists various Amazon VPC resources with counts: VPCs (2), Subnets (10), Route Tables (4), Internet Gateways (2), NAT Gateways (1), VPC Peering Connections (1), Network ACLs (2), and Security Groups (10). All counts are for the 'US East' region.

160 Click this checkbox.

The screenshot shows the 'Your VPCs' list page. The sidebar on the left is identical to the previous screenshot. The main area displays a table titled 'Your VPCs (2)'. The table has columns for 'Name', 'VPC ID', and 'Status'. It lists two entries: 'mylab-vpc' (VPC ID: [vpc-0df317e909cd2d1ca](#)) and another entry (VPC ID: [vpc-071ae984eaa589e75](#)). The first row, 'mylab-vpc', has its first column checkbox circled in orange.

	Name	VPC ID	Status
<input type="checkbox"/>	-	vpc-071ae984eaa589e75	<input checked="" type="checkbox"/> A
<input type="checkbox"/>	mylab-vpc	vpc-0df317e909cd2d1ca	<input checked="" type="checkbox"/> A

161 Click this link.

Name	VPC ID	Status
-	vpc-071ae984eaa589e75	✓ A
mylab-vpc	vpc-0df317e909cd2d1ca	✓ A

162 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)

163 Click this link.

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with links like EC2 Dashboard, EC2 Global View, Events, Console-to-Code (with a Preview link), Instances (which is expanded to show Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, and Capacity Reservations), and an X button. The main area is titled "Instances (1/6)" with an "Info" link. It includes a search bar with placeholder text "Find Instance by attribute or tag (case-sensitive)". A table lists six instances:

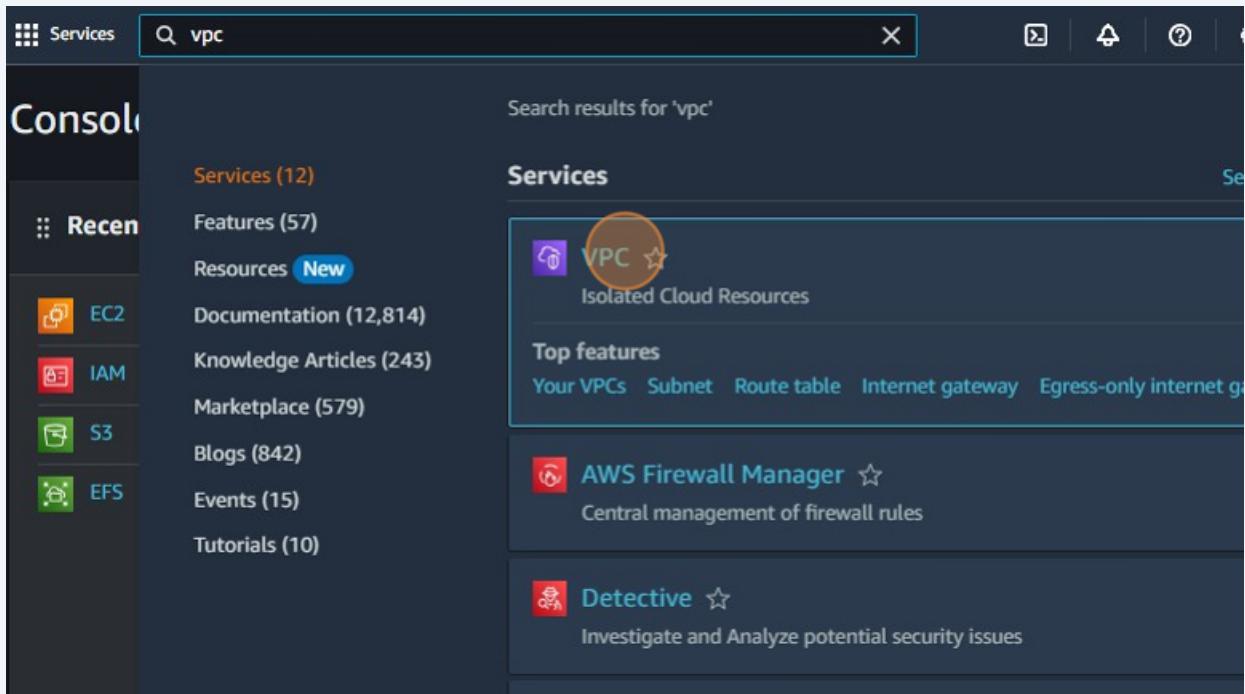
Name	Instance ID	Instance state
MyWebServer	i-0d90eaea164d304c1	Stopped
MyLabWebServer1	i-00c93ebd0f9e82f9d	Running
ec2forpractice	i-06db06d49d00347bb	Running
InstanceWebServer	i-06982e821bca6fb18	Stopped
IntanceforEC2	i-0df933f671e72cced	Stopped
myec2	i-0d76ec3e07e5268c0	Running

164 Click the "Search" field.

The screenshot shows the AWS Console Home page. At the top, there's a navigation bar with the AWS logo, a Services icon, a search bar containing the placeholder text "Search" (which is highlighted with a yellow circle), and other icons. Below the search bar, the title "Console Home" is displayed with an "Info" link. To the left, there's a sidebar with a "Recently visited" section showing links to EC2, IAM, S3, and EFS. To the right, there's a "Applications" section with a note "Region: US East".

165 Type "vpc"

166 Click "VPC"



167 Click "Your VPCs"

The screenshot shows the AWS VPC dashboard. On the left, there's a sidebar with a 'Virtual private cloud' section containing 'Your VPCs' (which is circled in orange), 'Subnets', 'Route tables', 'Internet gateways', 'Egress-only internet gateways', 'Carrier gateways', 'DHCP option sets', and 'Elastic IPs'. At the top right, there are buttons for 'Create VPC' and 'Launch EC2 Instances'. Below these buttons, a note says 'Note: Your Instances will launch in the US East region.' The main area is titled 'Resources by Region' and shows the following counts for the US East region:

Resource Type	Count
VPCs	2
NAT Gateways	1
Subnets	10
VPC Peering Connections	0
Route Tables	4
Network ACLs	2
Internet Gateways	2
Security Groups	10

168 Click "Security groups"

The screenshot shows the 'Details' tab for a VPC named 'mylab-vpc'. The VPC ID is 'vpc-0df317e909cd2d1ca'. The 'Security' section of the sidebar is expanded, showing 'Network ACLs' and 'Security groups' (which is circled in orange). The 'Details' table contains the following information:

Attribute	Value	Actions
VPC ID	vpc-0df317e909cd2d1ca	DNS Enabled
Tenancy	Default	DHCP option set dopt-019b25e8c4573f158
Default VPC	No	IPv4 CIDR 10.0.0.0/16

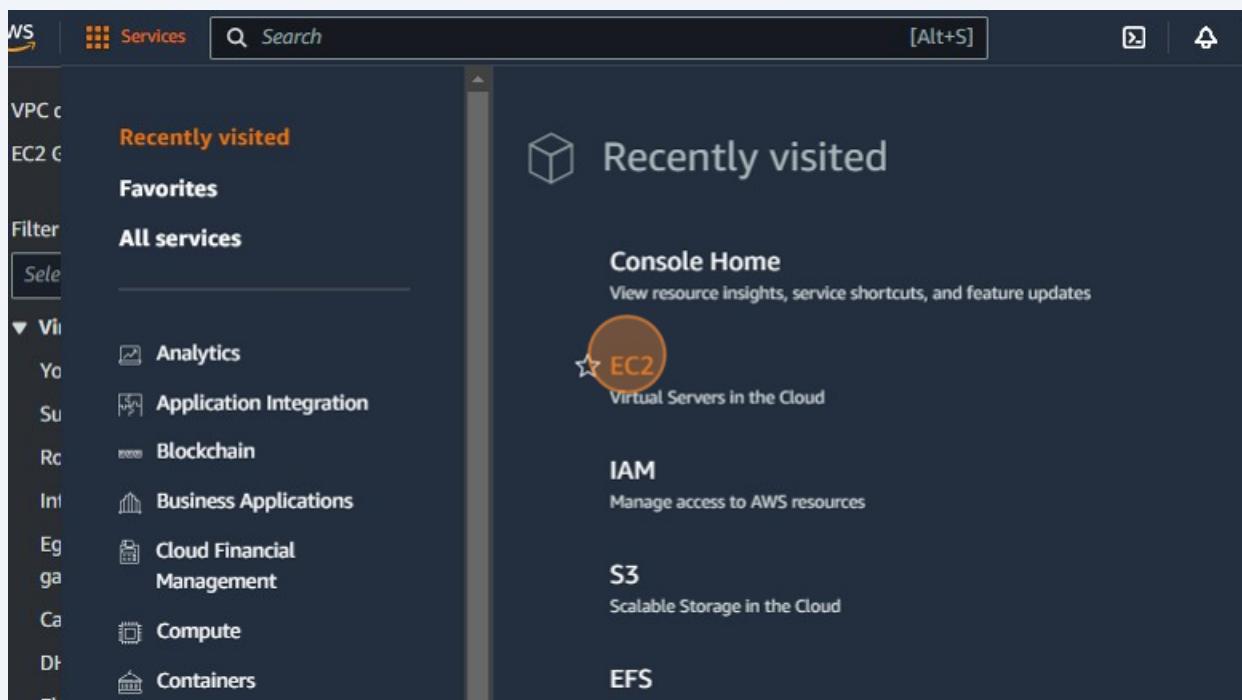
169 Click "Security groups"

The screenshot shows the AWS VPC console. On the left, a sidebar menu includes options like Managed prefix lists, Endpoints, Endpoint services, NAT gateways, Peering connections, Security (with Security groups highlighted and circled in orange), DNS firewall, Rule groups, Domain lists, Network Firewall, Firewalls, Firewall policies, and Network Firewall rule groups. The main content area displays the 'Inbound rules' tab for a security group with ID 693808211005. It shows one inbound rule named 'sgr-03497df20942edc8b' for IPv4.

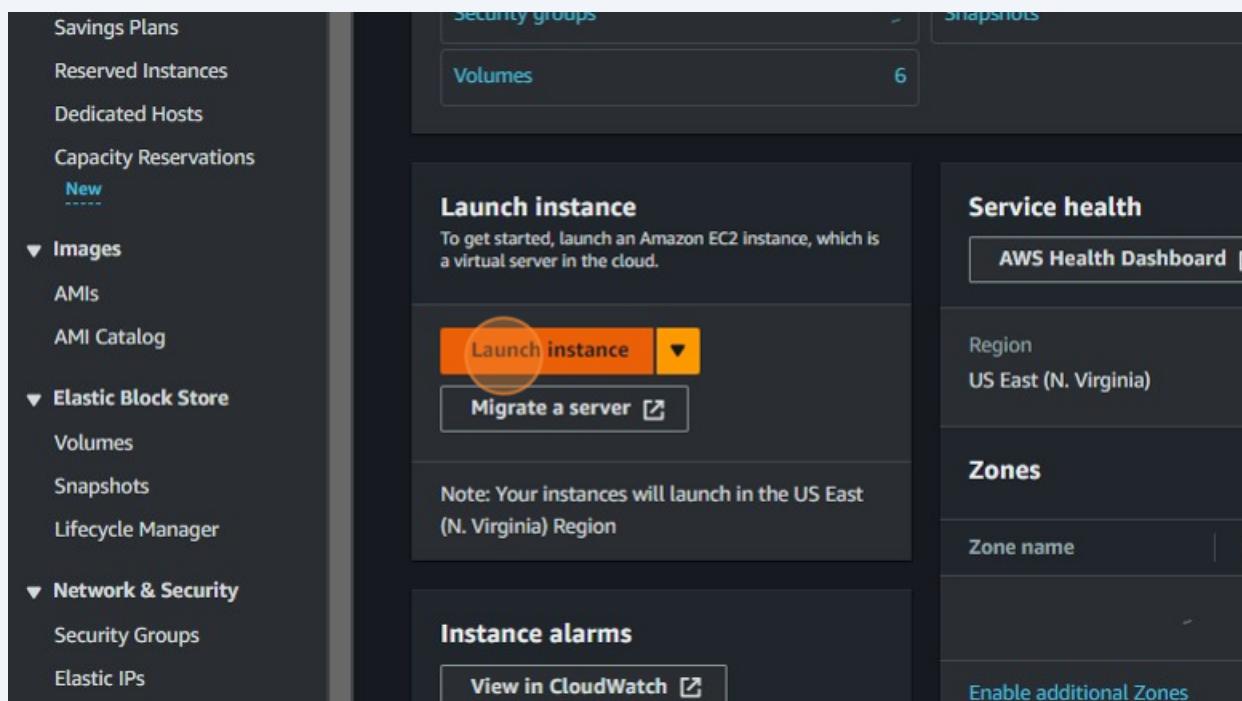
170 Click "Services"

The screenshot shows the AWS Services dashboard. The 'Services' button is highlighted and circled in orange. The main content area shows a success message: 'Security group (sg-0d32c3eb11a5dfb6 | my-lab-security-group) was created successfully'. Below it, the 'Details' section lists 'Creating security group' and 'Create inbound rule'. Further down, the 'Security Groups (11)' section is displayed, showing a table of security groups with columns for Name, Security group ID, and Description. The first few rows are: sg-0a579ba0b02e54dd6 (Description: launch-wizard-1), sg-01cf188a53aac782a (Description: mylab-wizard-1), and sg-052a840e9d7be4ed7 (Description: default).

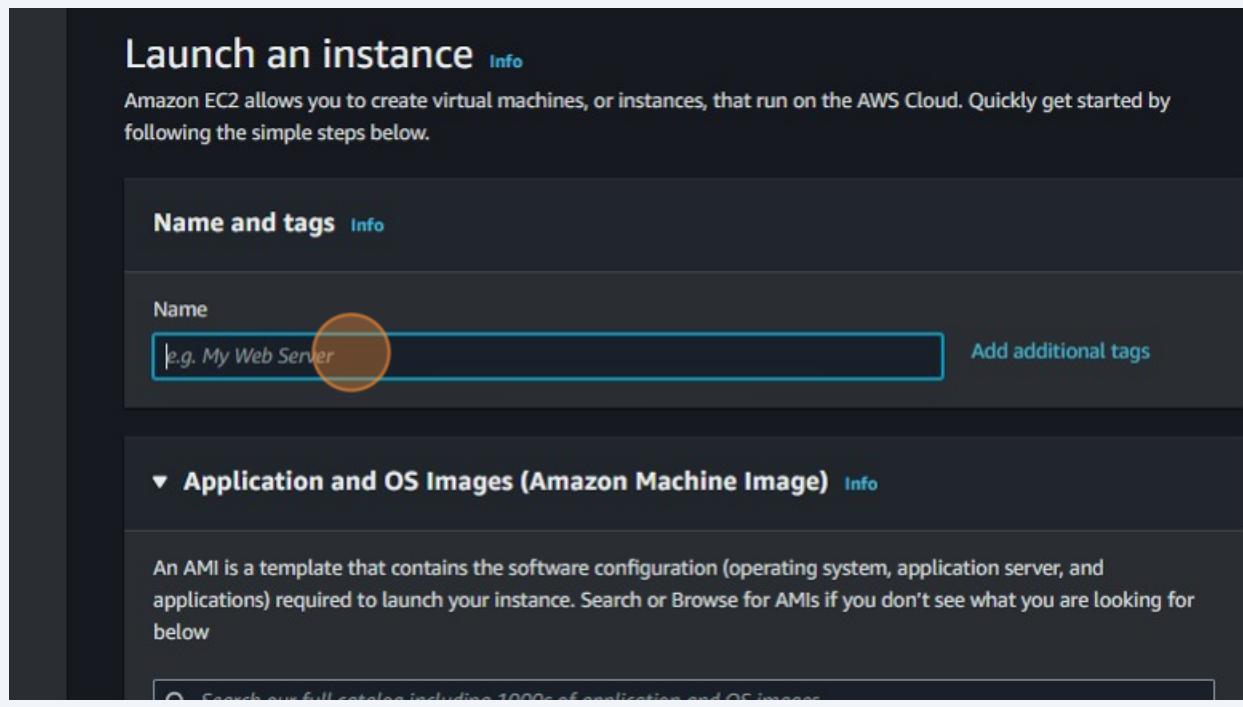
171 Click "EC2"



172 Click "Launch instance"

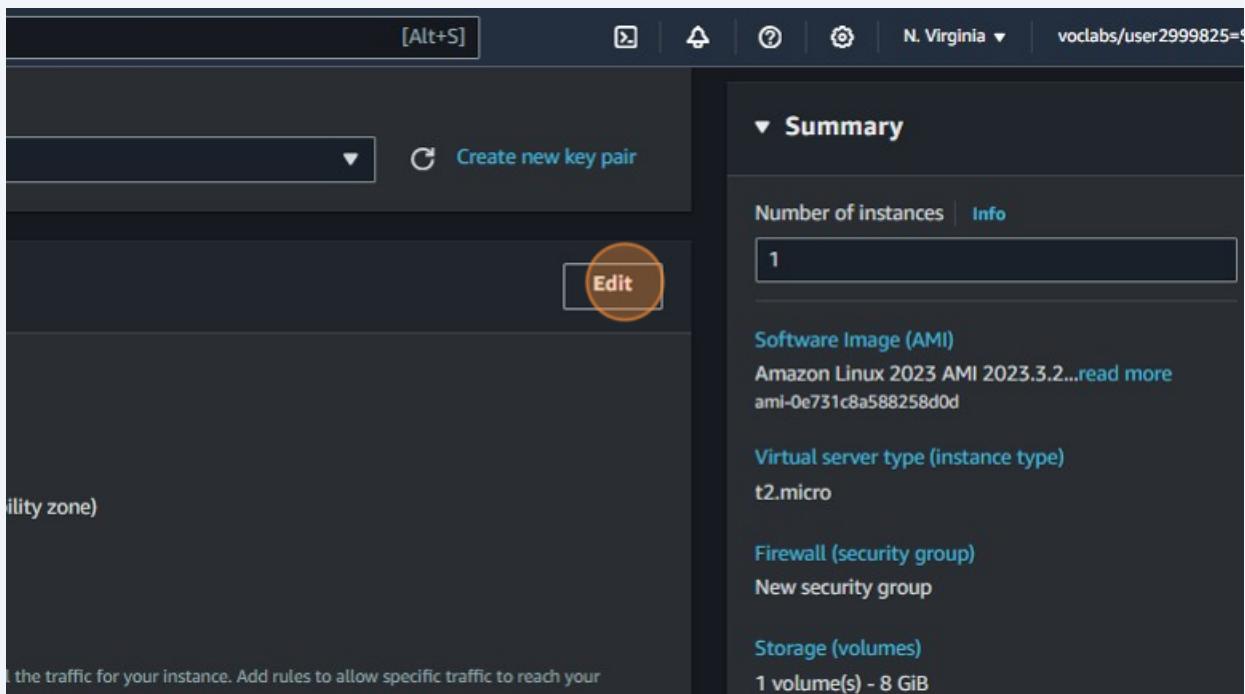


173 Click the "Name" field.

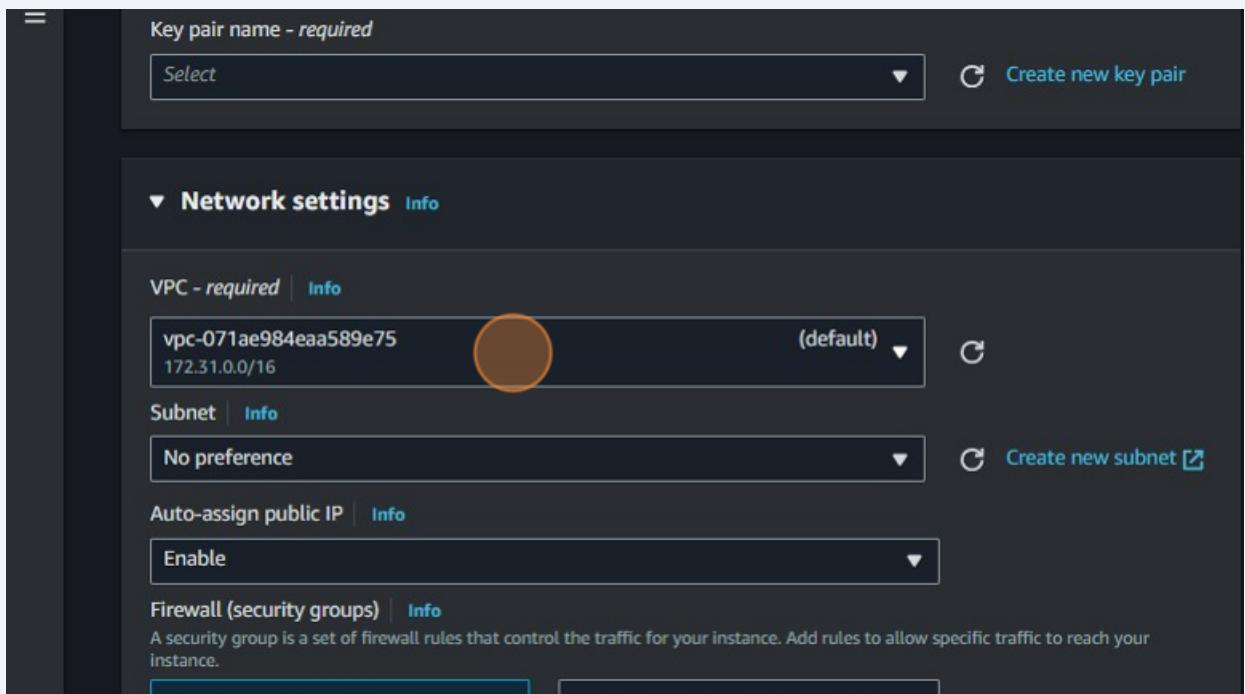


174 Type "my-lab-webserver"

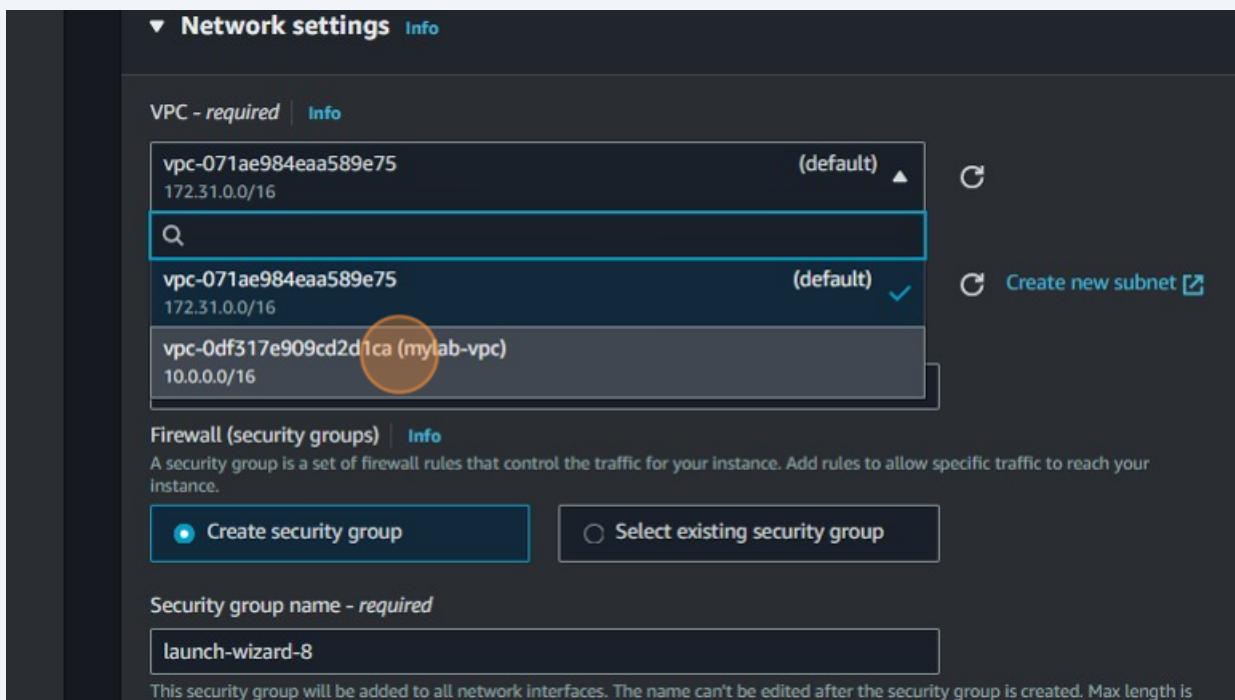
175 Click "Edit"



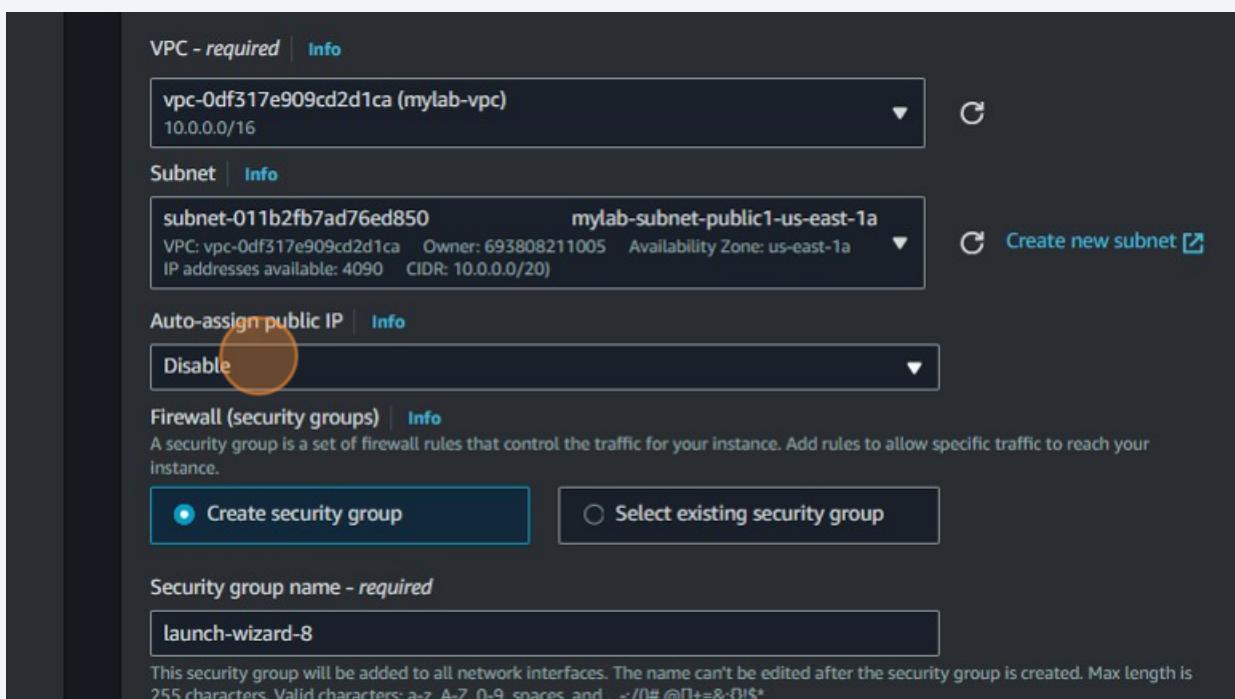
176 Click "172.31.0.0/16"



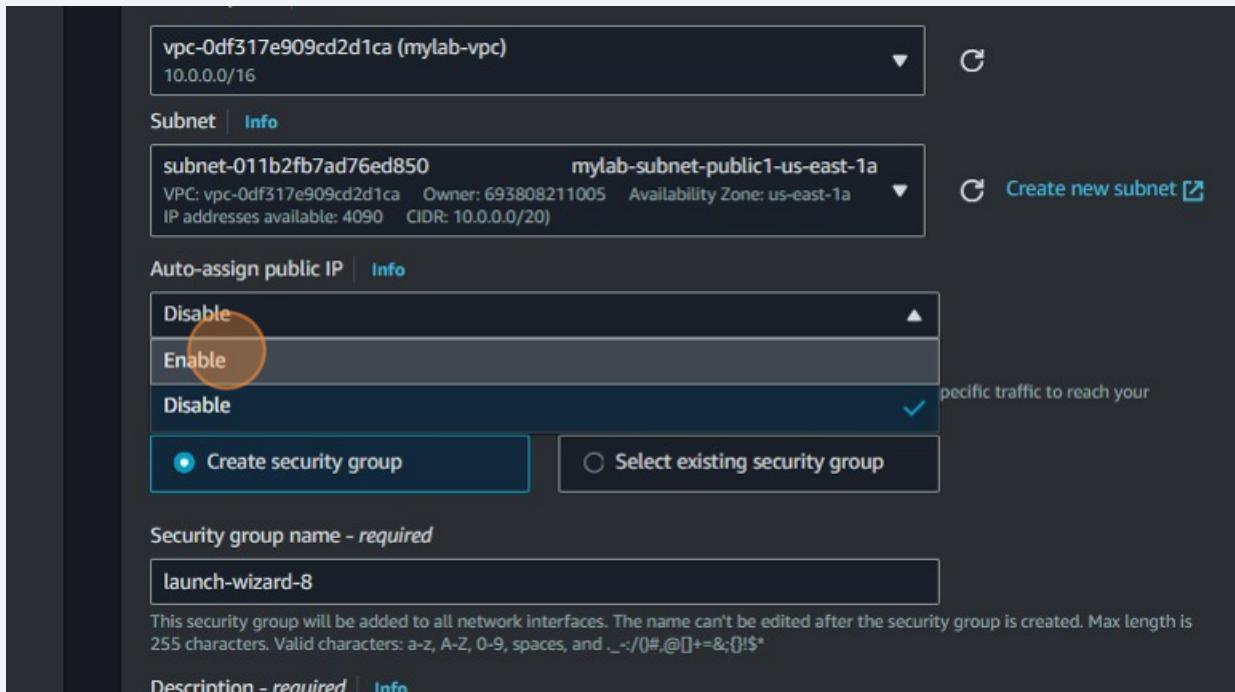
177 Click "vpc-0df317e909cd2d1ca (mylab-vpc)"



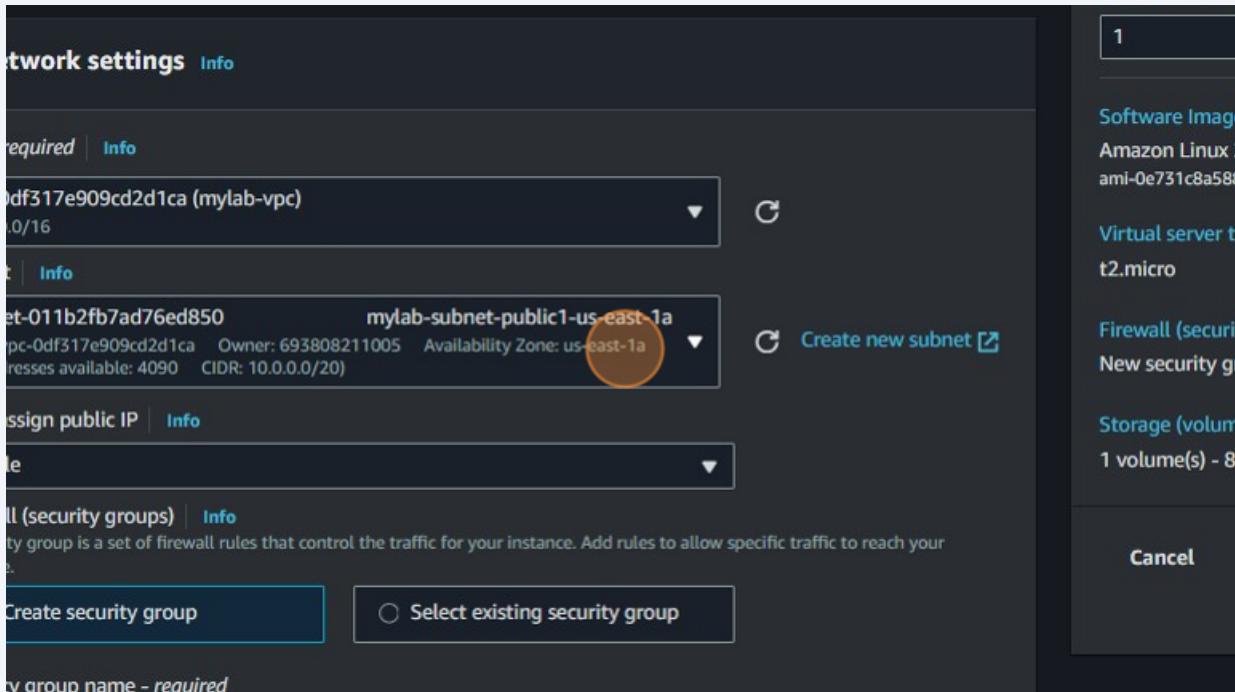
178 Click "Disable"



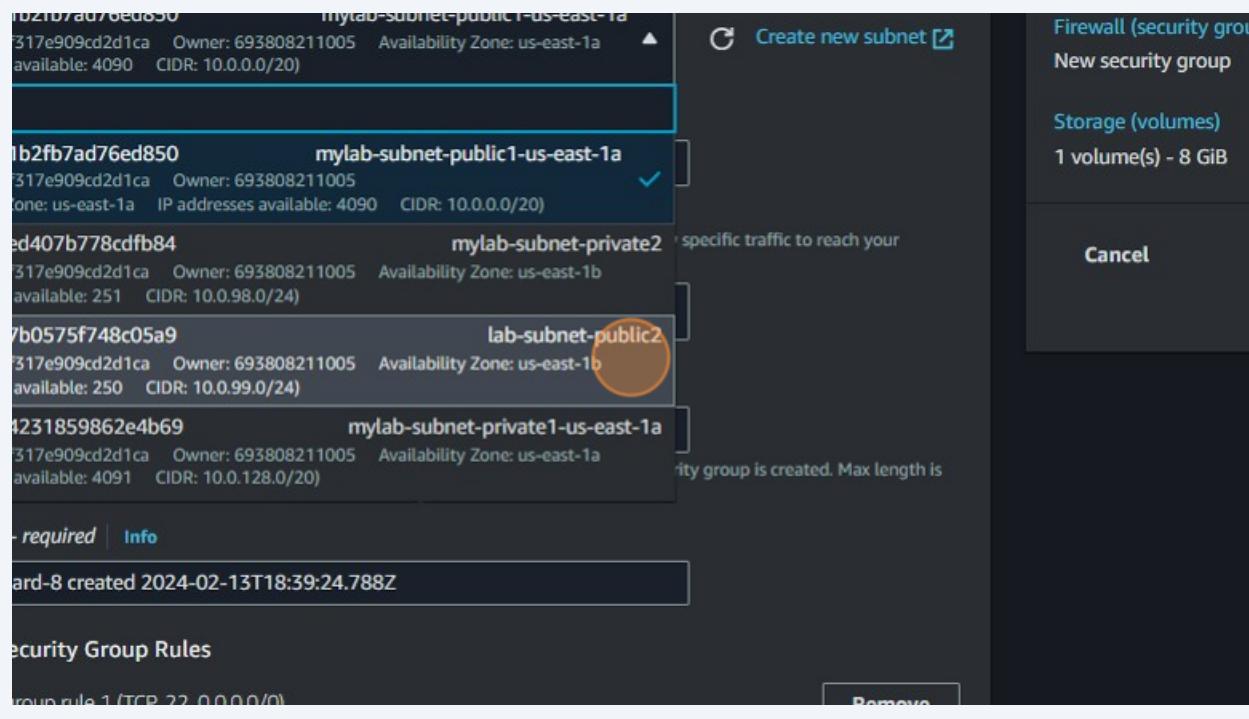
179 Click "Enable"



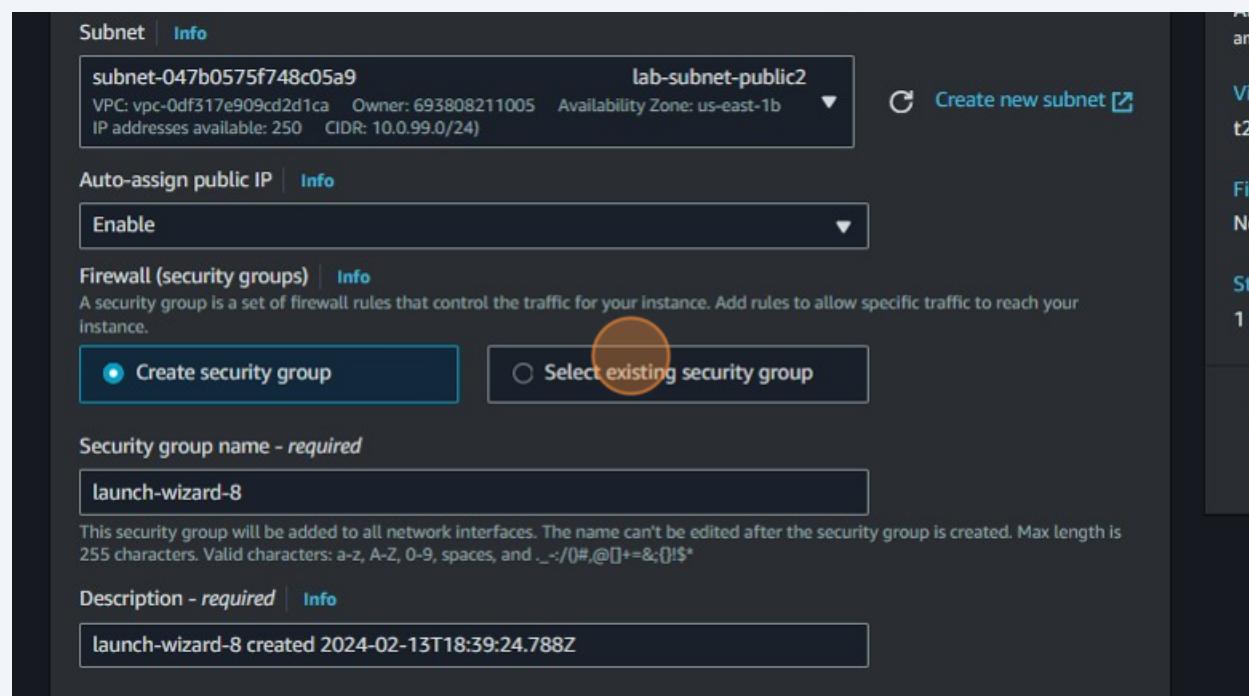
180 Click "Availability Zone: us-east-1a"



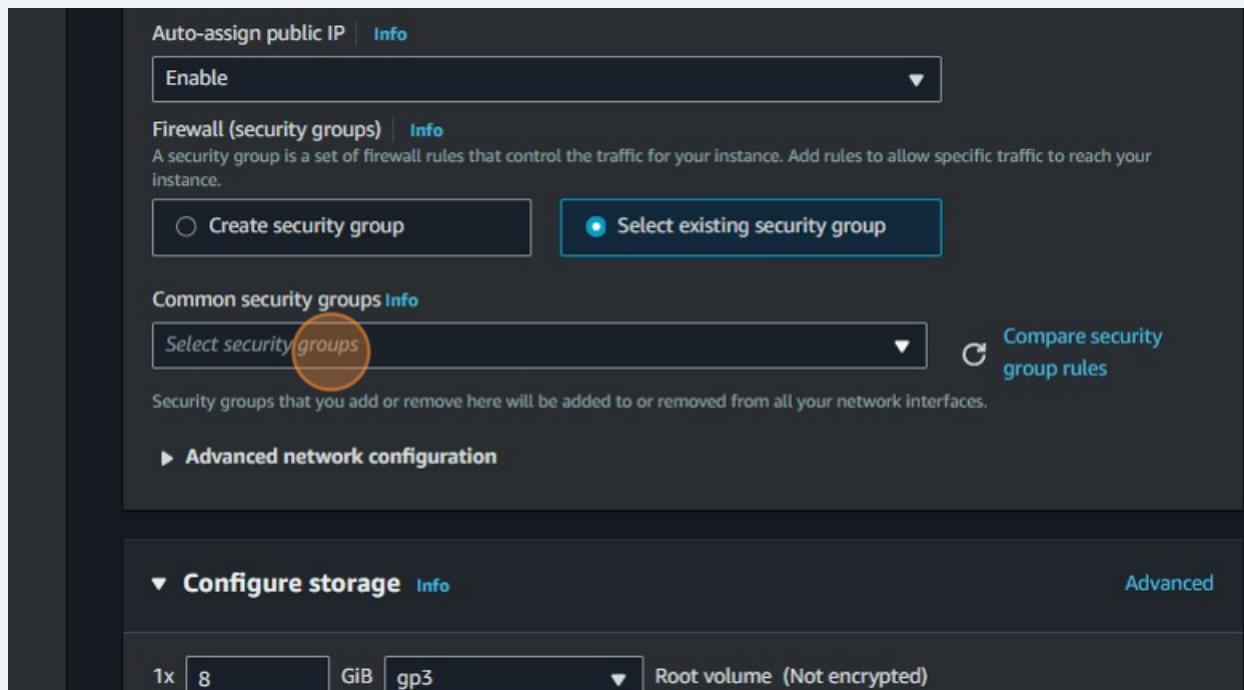
- 181** Click "VPC: vpc-0df317e909cd2d1ca
Owner: 693808211005
Availability Zone: us-east-1b
IP addresses available: 250
CIDR: 10.0.99.0/24)"



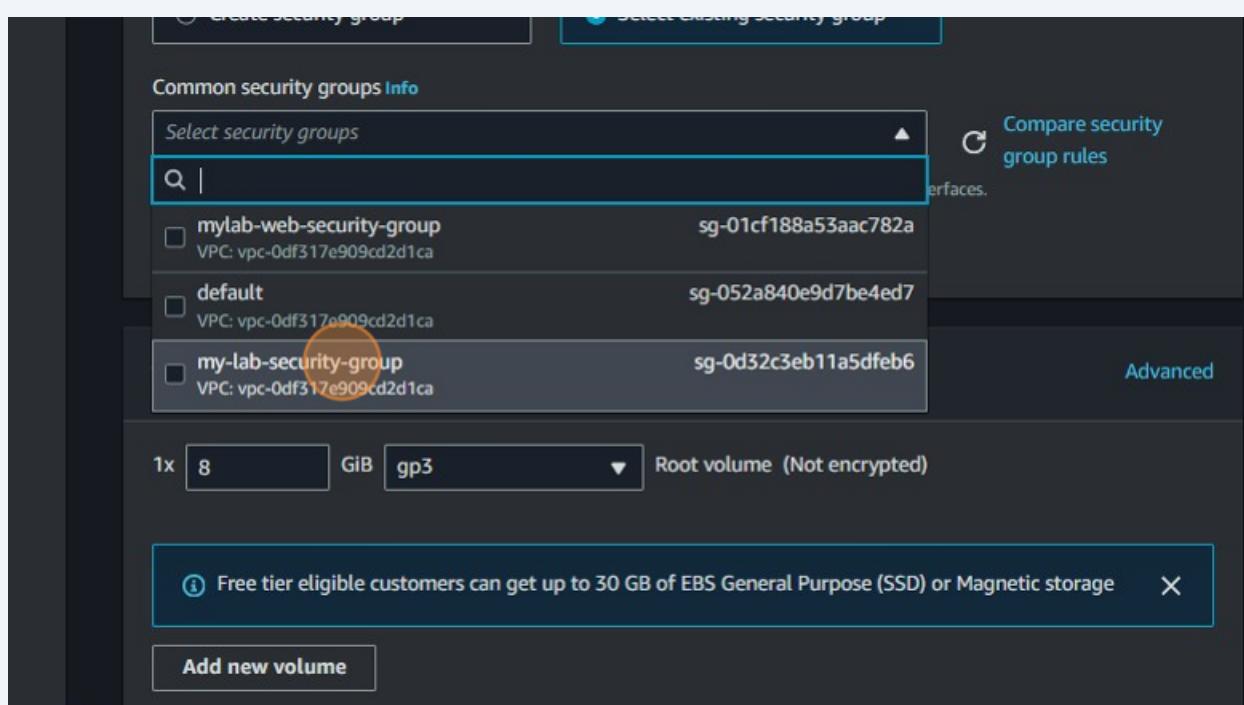
- 182** Click "Select existing security group"



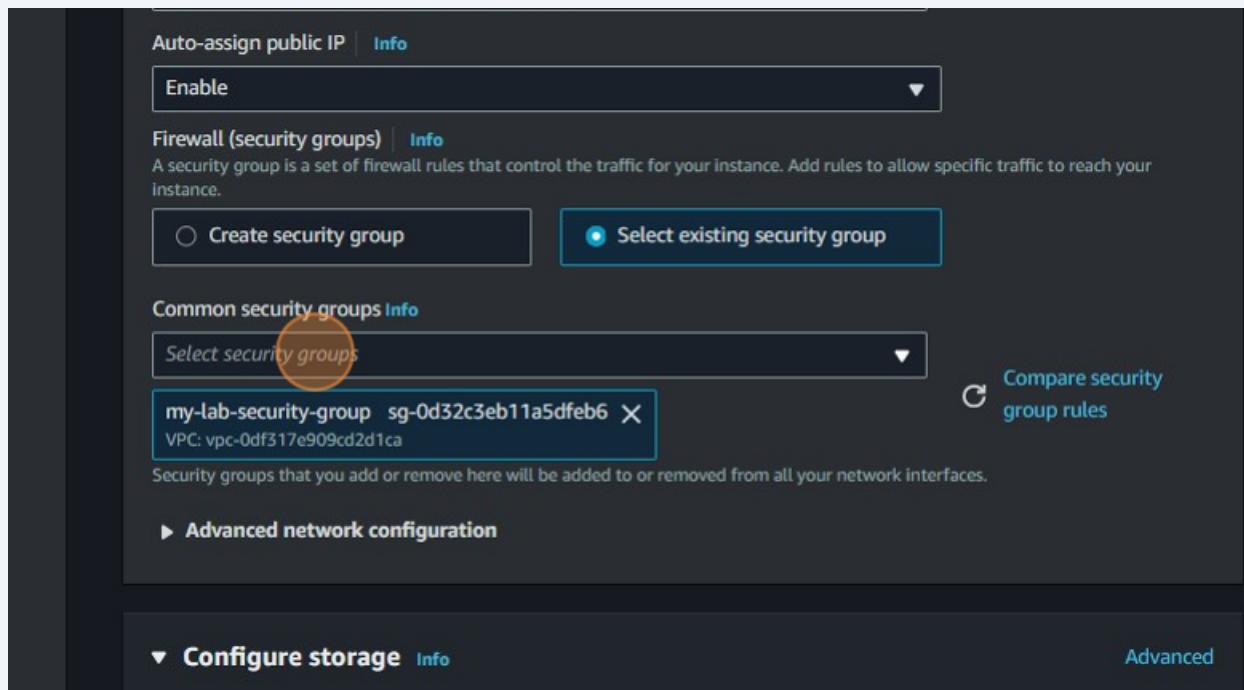
183 Click "Select security groups"



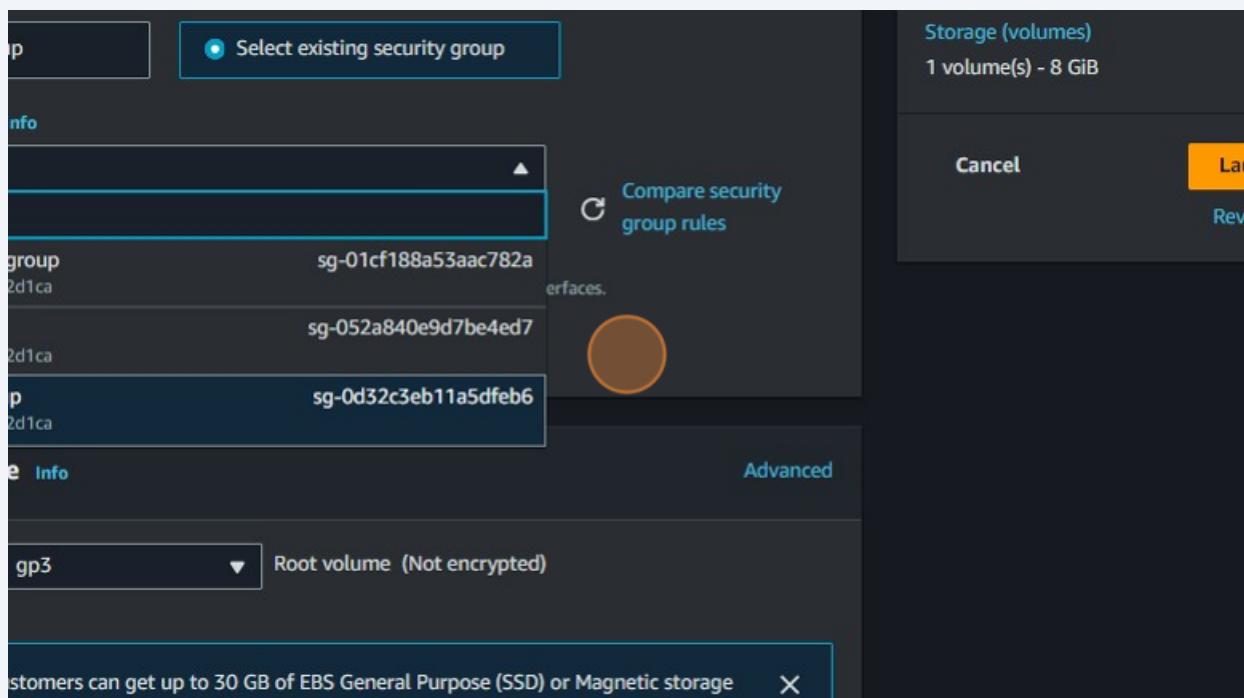
184 Click "my-lab-security-group"



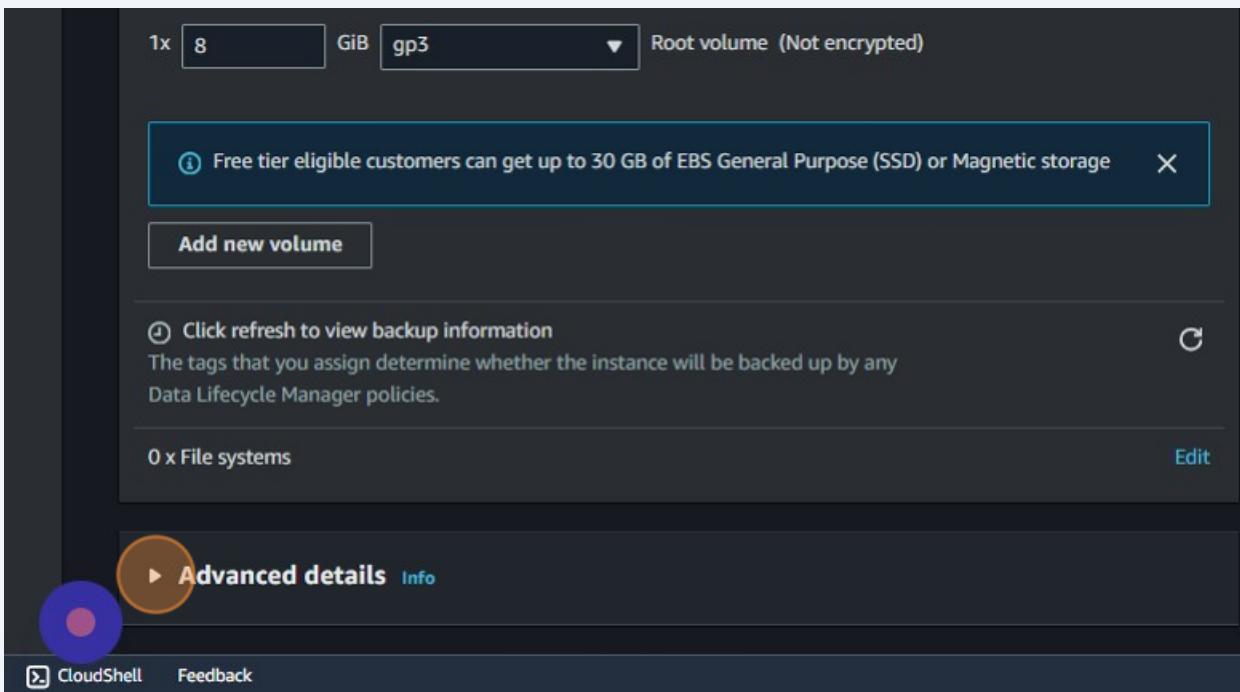
185 Click "Select security groups"



186 Click here.

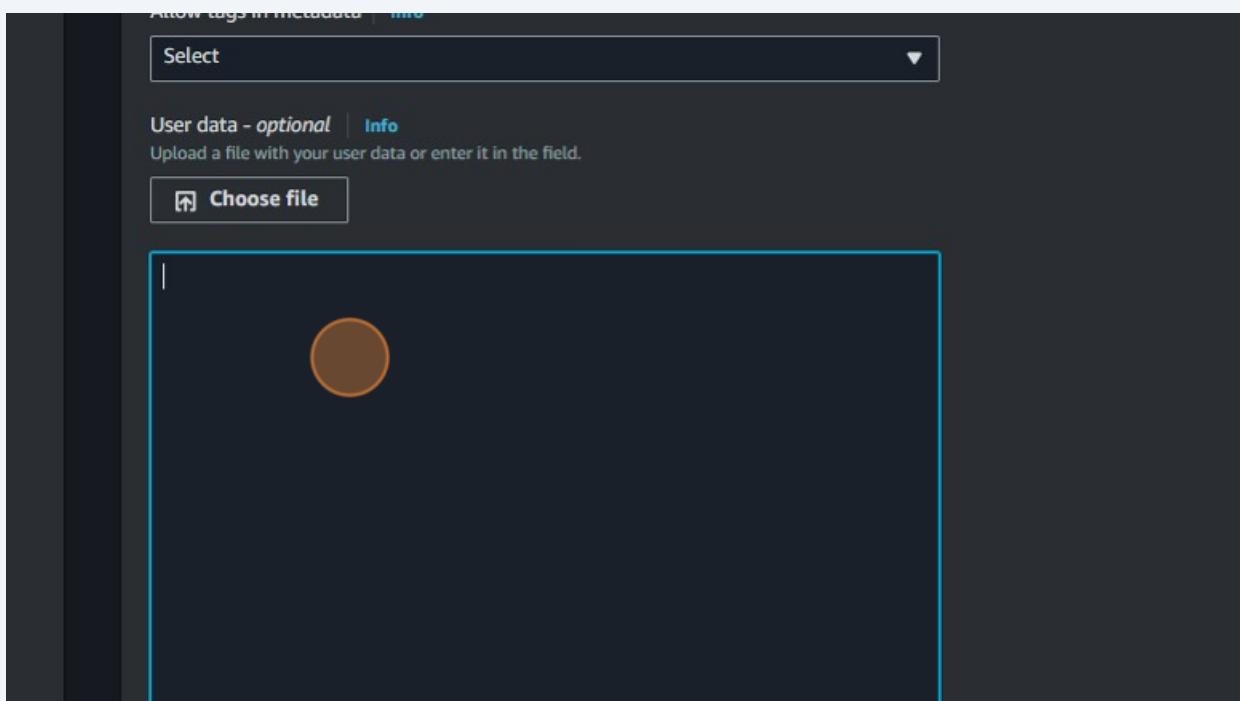


187 Click here.

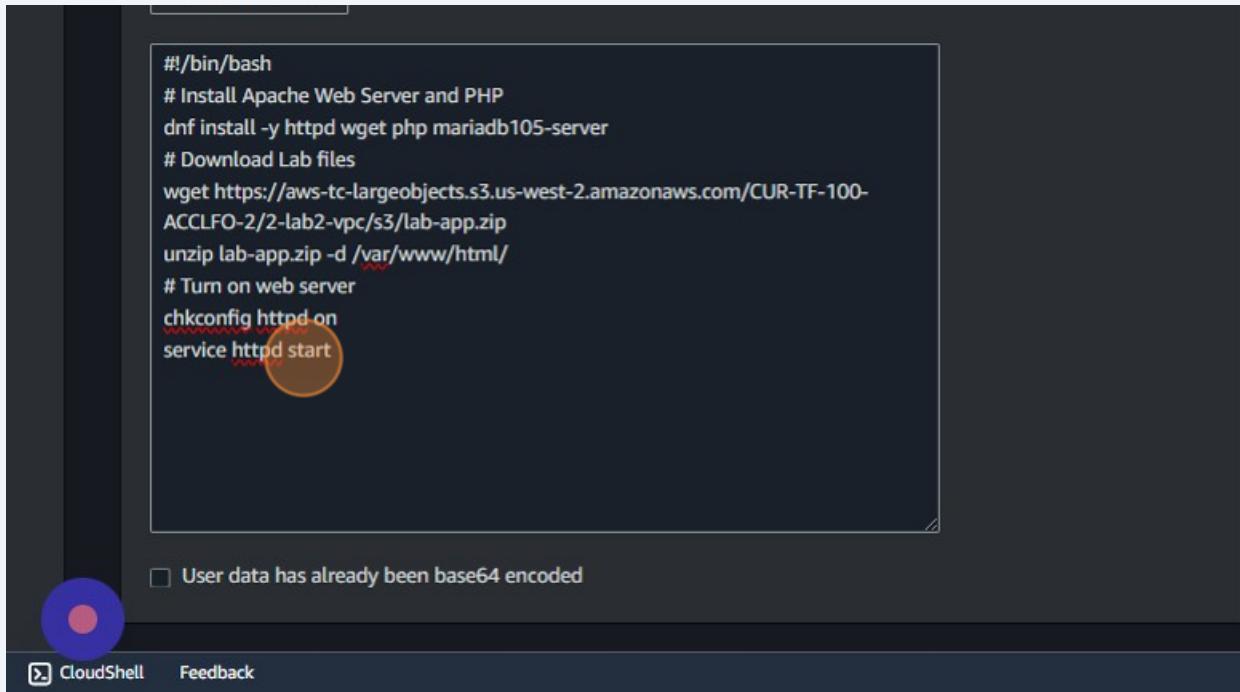


188 Switch to tab "Workbench - Vocareum"

189 Click the "User data - optional" field.



190 Click the "User data - optional" field.

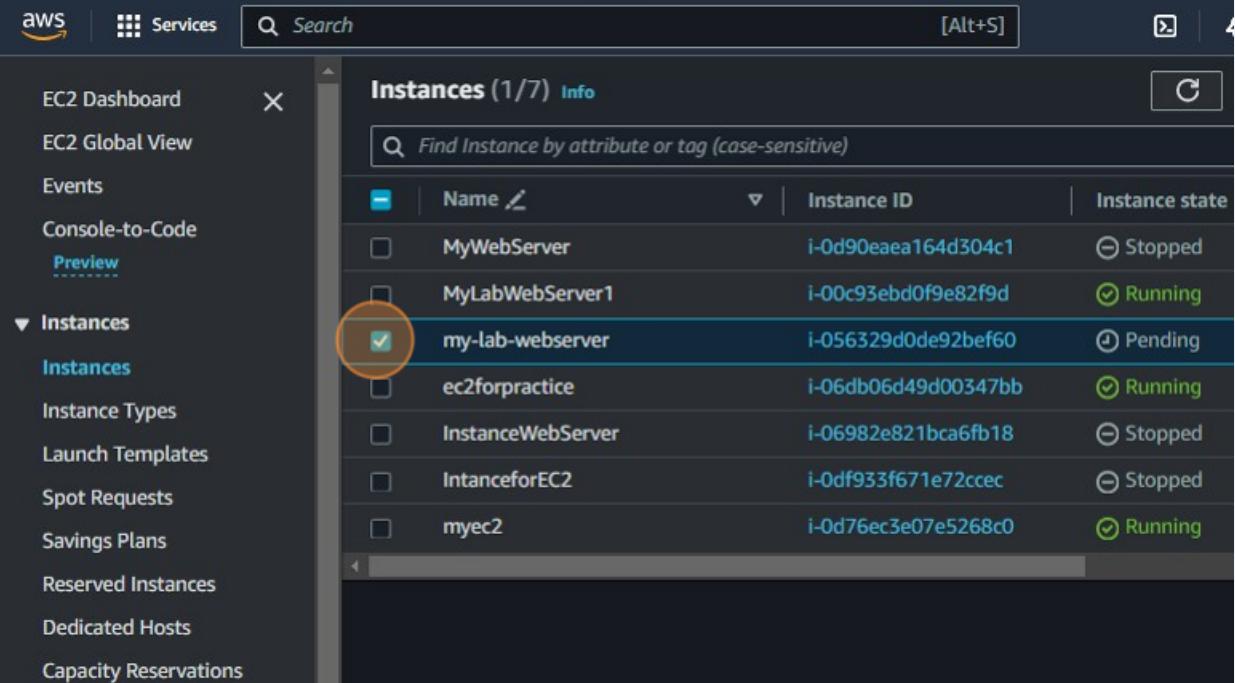


191

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)

192

Click this checkbox.

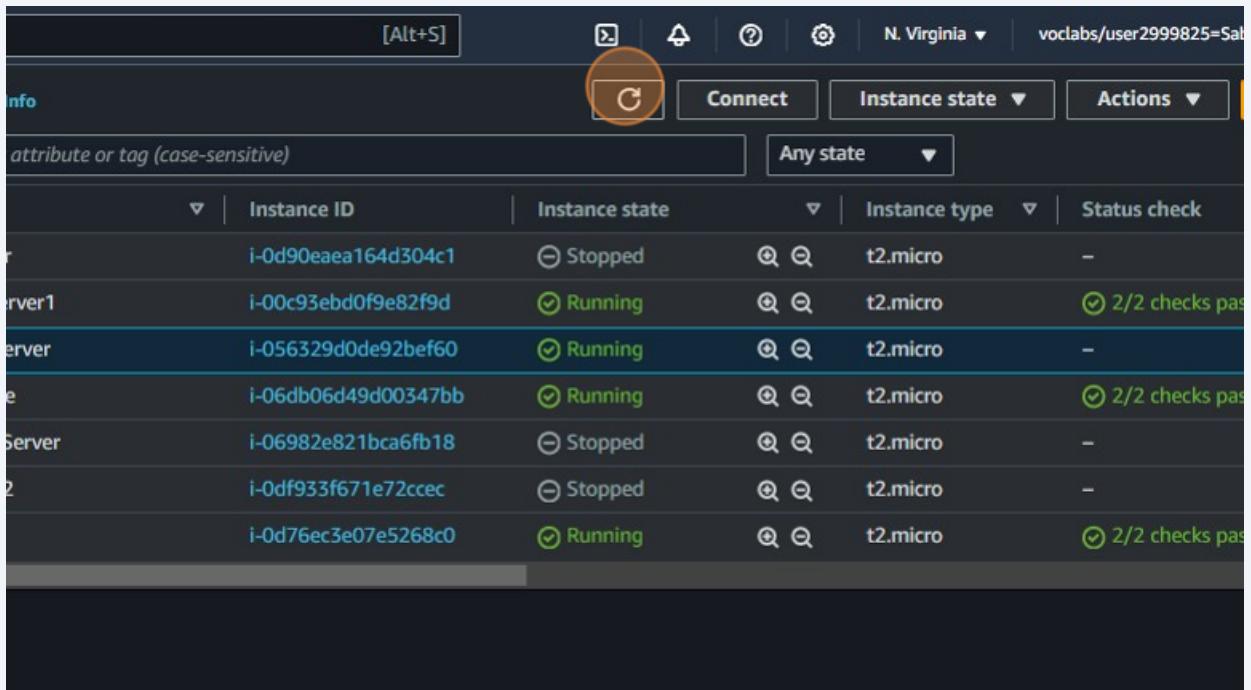


The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with various EC2-related options like Dashboard, Global View, Events, and Instances. Under Instances, 'Instances' is selected. The main area displays a table of 7 instances:

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-0df933f671e72cc6c	Stopped
myec2	i-0d76ec3e07e5268c0	Running

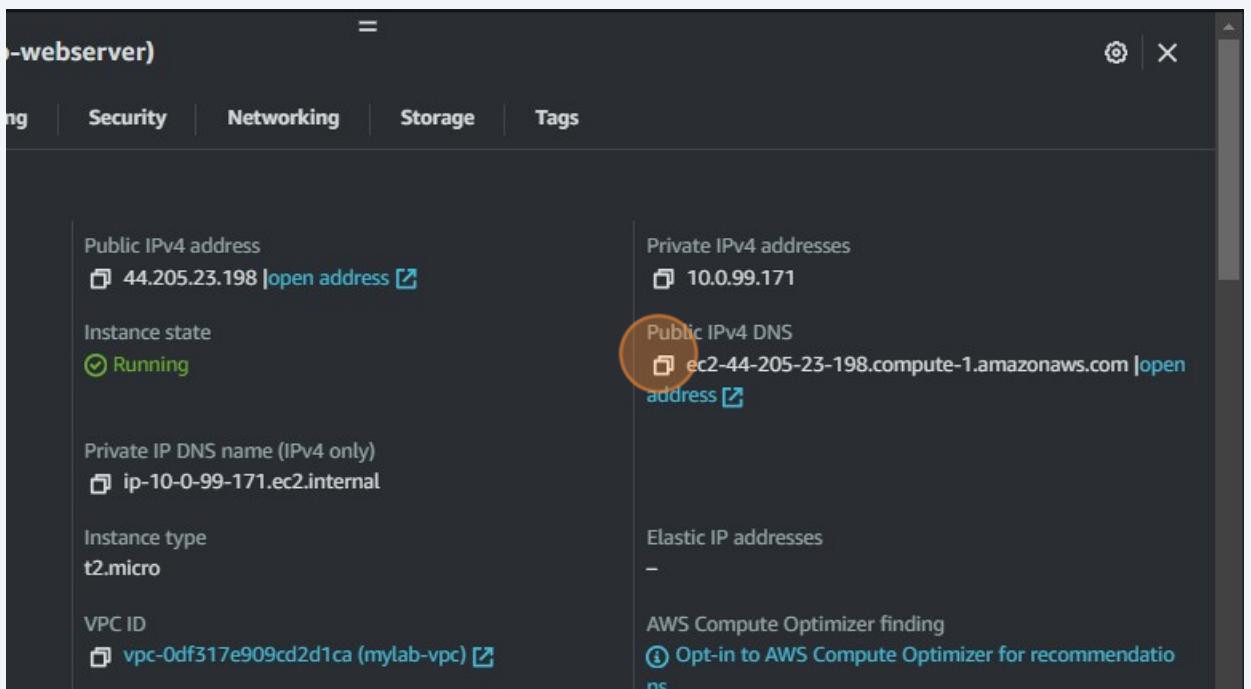
The row for 'my-lab-webserver' has a checked checkbox in the first column, which is circled in red.

193 Click here.



Info		[Alt+S]	Actions	N. Virginia	voclabs/user2999825=Sat
		Connect	Instance state	Actions	
attribute or tag (case-sensitive)			Any state		
▼	Instance ID	Instance state	▼	Instance type	▼
1	i-0d90eaea164d304c1	Stopped	Q Q	t2.micro	-
Server1	i-00c93ebd0f9e82f9d	Running	Q Q	t2.micro	✓ 2/2 checks pass
Server	i-056329d0de92bef60	Running	Q Q	t2.micro	-
e	i-06db06d49d00347bb	Running	Q Q	t2.micro	✓ 2/2 checks pass
Server	i-06982e821bca6fb18	Stopped	Q Q	t2.micro	-
2	i-0df933f671e72ccce	Stopped	Q Q	t2.micro	-
	i-0d76ec3e07e5268c0	Running	Q Q	t2.micro	✓ 2/2 checks pass

194 Click here.



my-lab-webserver	
Setting	Value
Public IPv4 address	44.205.23.198 [open address]
Instance state	✓ Running
Private IP DNS name (IPv4 only)	ip-10-0-99-171.ec2.internal
Instance type	t2.micro
VPC ID	vpc-0df317e909cd2d1ca (mylab-vpc) [open]
Private IPv4 addresses	10.0.99.171
Public IPv4 DNS	ec2-44-205-23-198.compute-1.amazonaws.com [open address]
Elastic IP addresses	-
AWS Compute Optimizer finding	Opt-in to AWS Compute Optimizer for recommendations.

195 In a new tab, navigate to <http://ec2-44-205-23-198.compute-1.amazonaws.com/>

196 Click "Current CPU Load: 1%"

The screenshot shows a web browser window with the AWS Lambda console. At the top, there are tabs for 'aws' (selected), 'Load Test', and 'RDS'. Below the tabs, there's a table titled 'Meta-Data' with two rows: 'InstanceId' (Value: i-056329d0de92bef60) and 'Availability Zone' (Value: us-east-1b). Underneath the table, the text 'Current CPU Load: 1%' is displayed next to a large orange circular progress bar.

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

Current CPU Load: 1%