

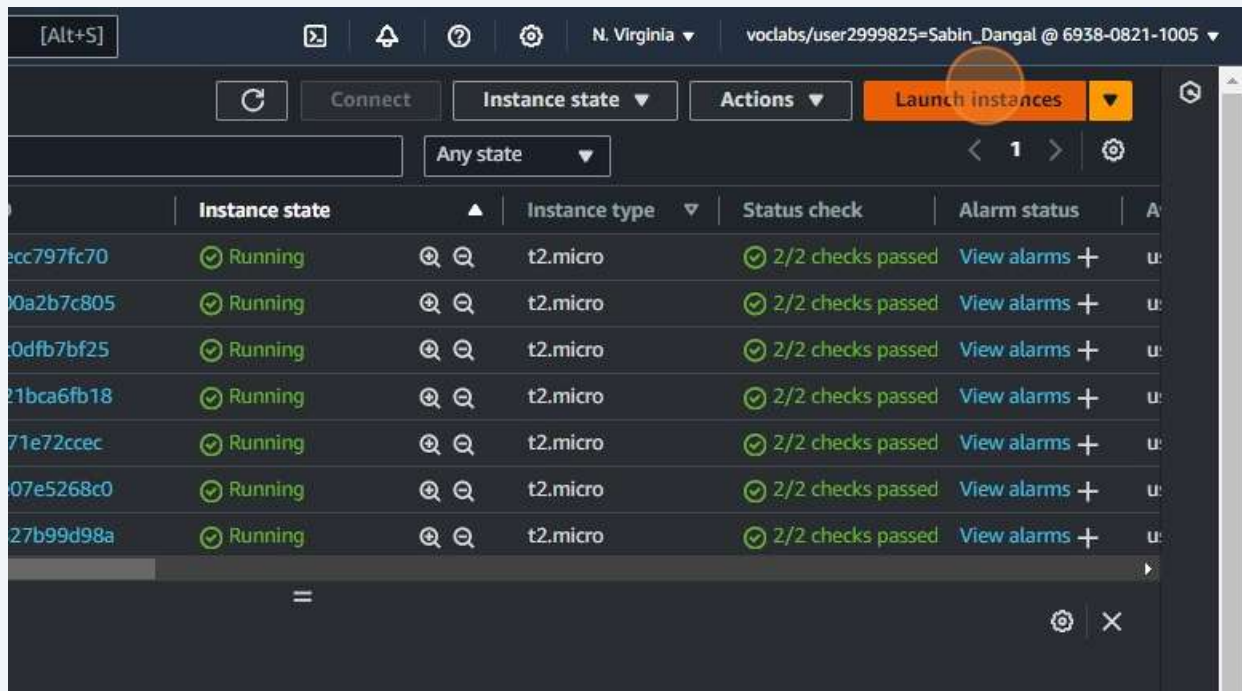
EC2 with ELB and ASG

1

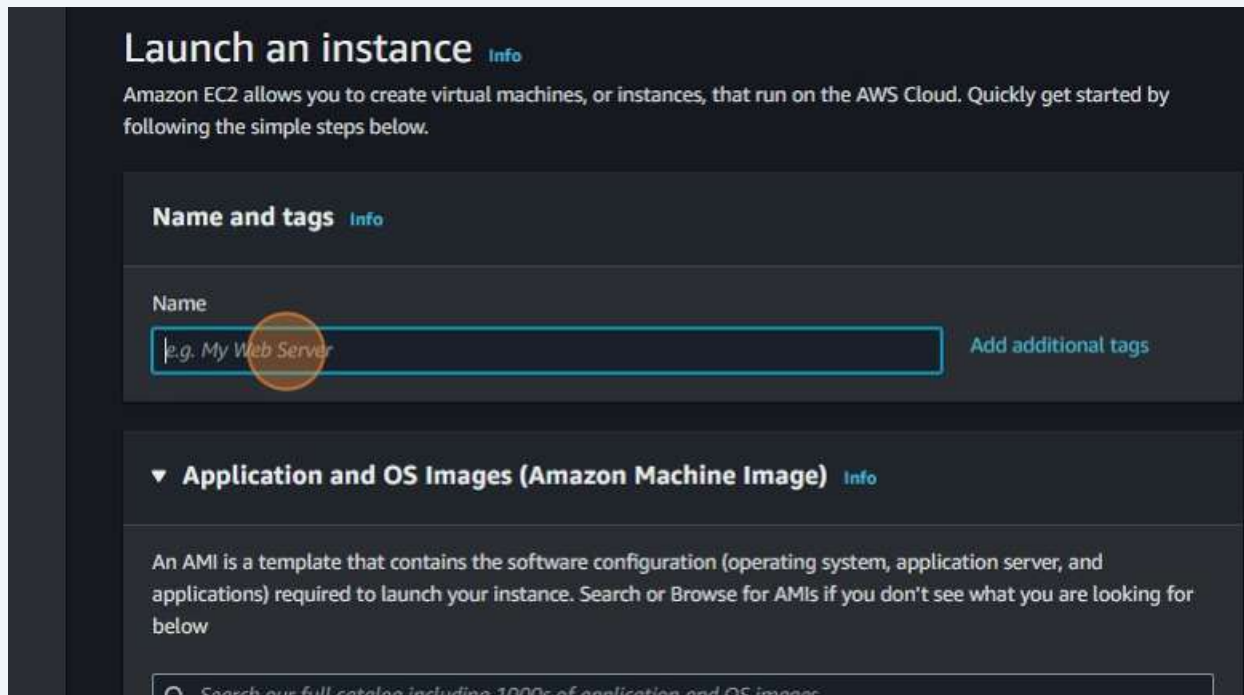
Navigate to [https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:v=3;\\$case=tags:true%5C,client:false;\\$regex=tags:false%5C,client:false;sort=instanceState](https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:v=3;$case=tags:true%5C,client:false;$regex=tags:false%5C,client:false;sort=instanceState)

2

Click "Launch instances"



- 3 Click the "Name" field.



Launch an instance Info

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

Name and tags Info

Name

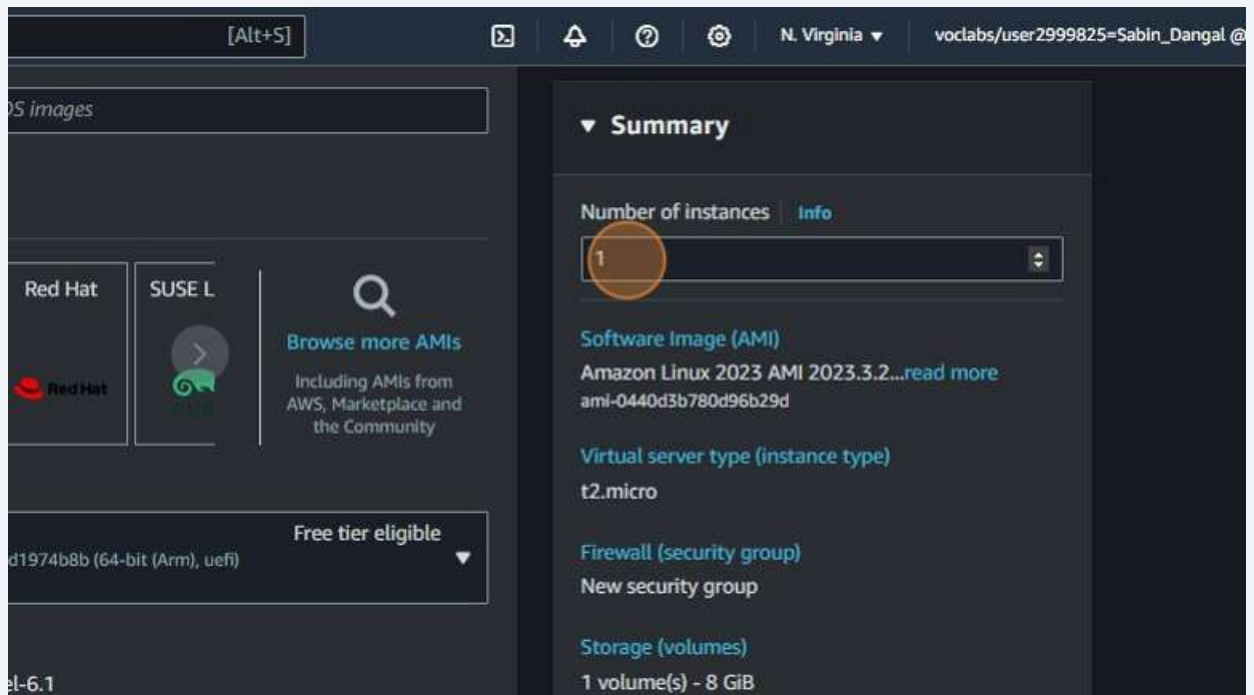
[Add additional tags](#)

▼ Application and OS Images (Amazon Machine Image) Info

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

- 4 Type "lb-asg-webserver"

- 5 Click the "Number of instances" field.



- 6 Type "up up"

7 Click "Select"

Additional costs apply for AMIs with pre-installed software

▼ **Key pair (login)** [Info](#)

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

Key pair name - *required*

Select ▼ [Create new key pair](#)

▼ **Network settings** [Info](#) [Edit](#)

Network [Info](#)
vpc-071ae984eaa589e75

Subnet [Info](#)

8 Click "ssh-key"

Key pair (login) [Info](#)

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

Key pair name - *required*

Select ▼ [Create new key pair](#)

Q |

Proceed without a key pair (Not recommended) [Default value](#)

ssh-key
Type: rsa

rsa-ssh-key
Type: rsa

vockey
Type: rsa

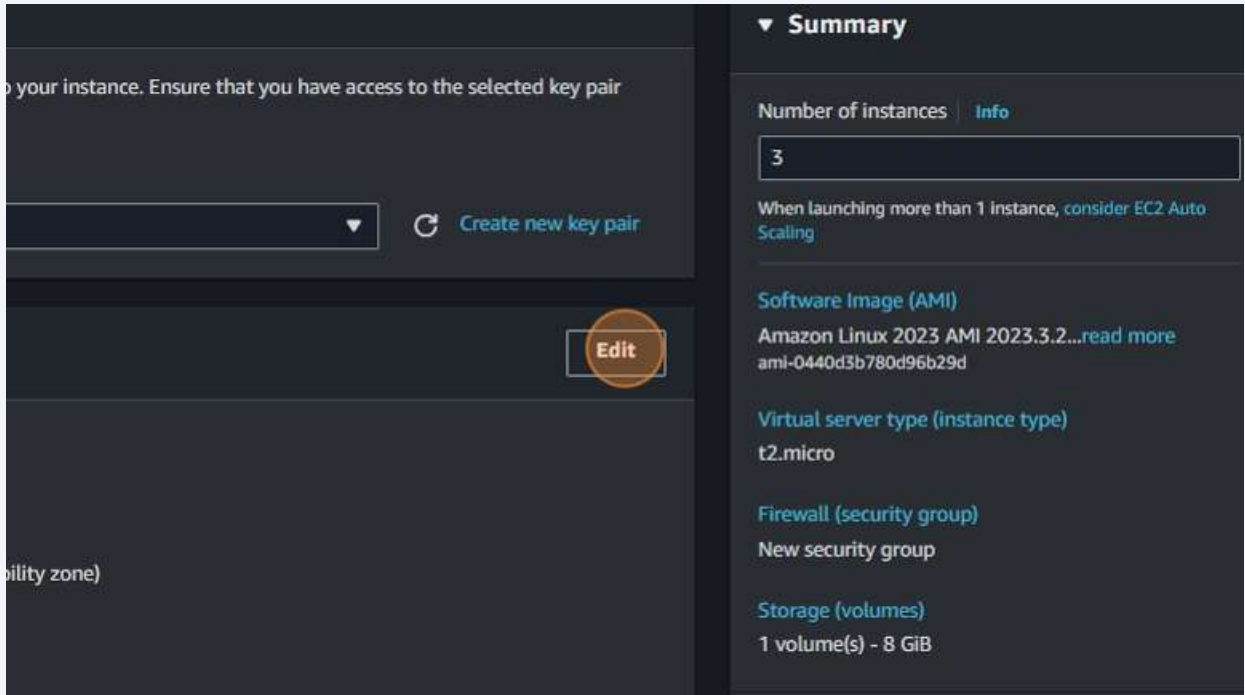
my-ssh-key

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

[CloudShell](#) [Feedback](#)

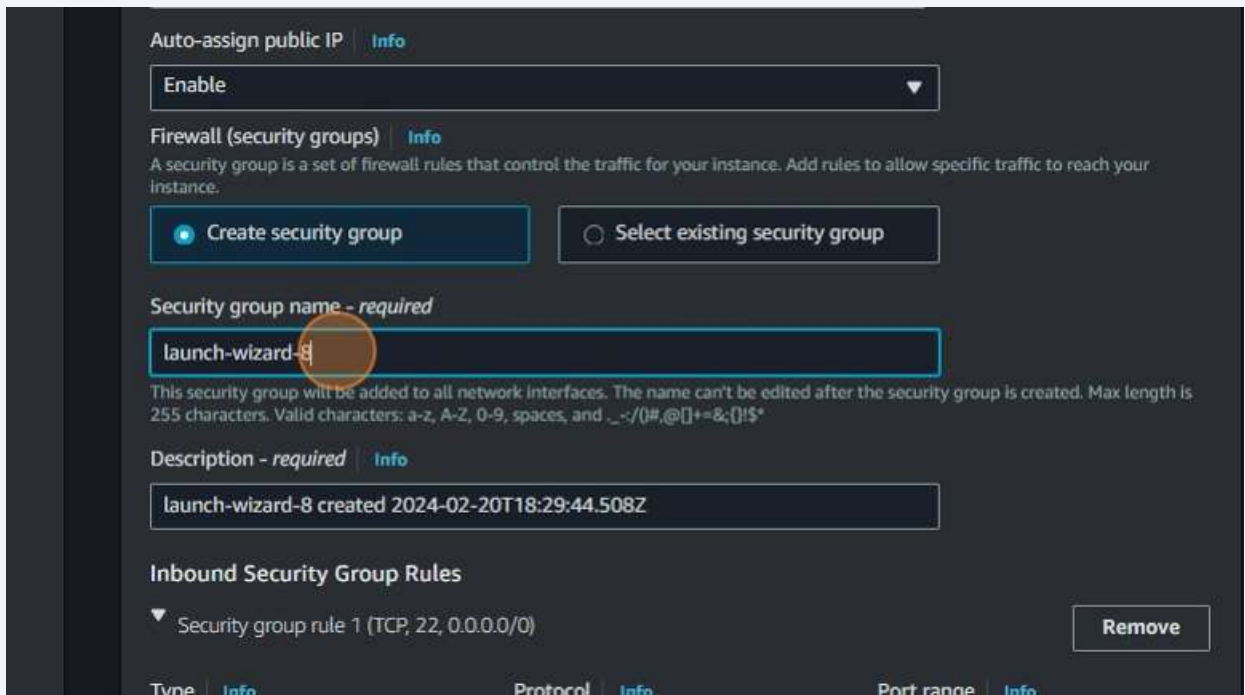
9

Click "Edit"

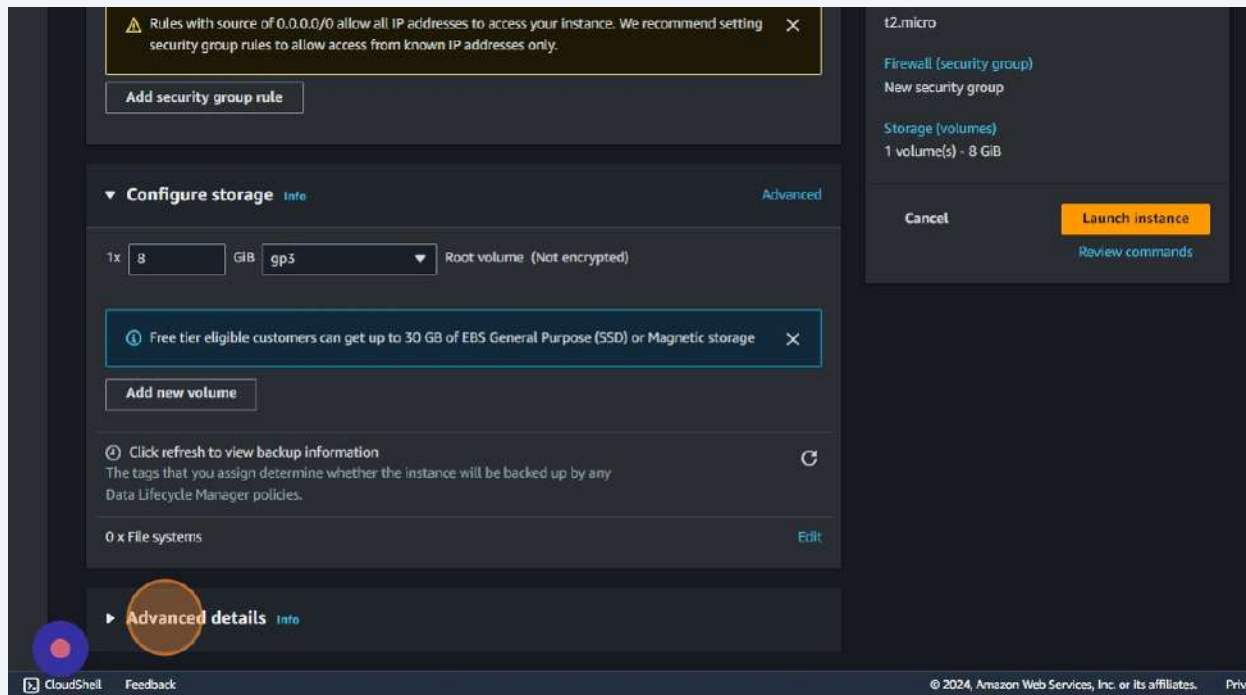


10

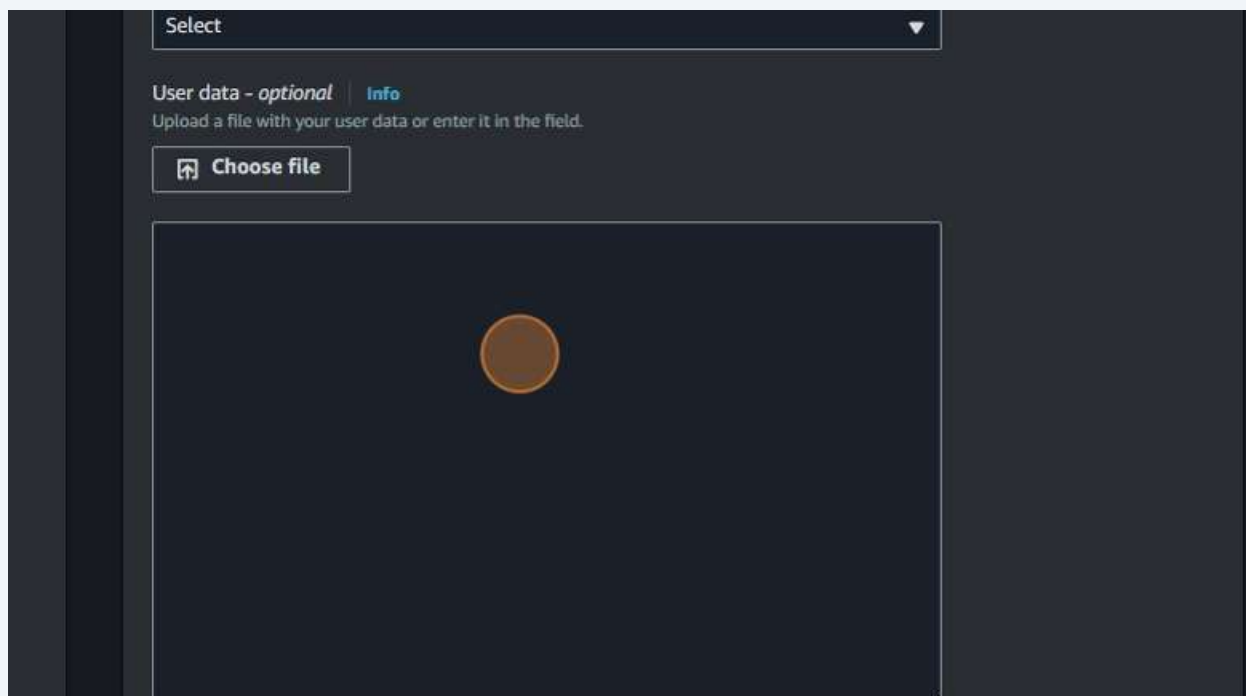
Click the "Security group name - required" field.



11 Click "Advanced details"



12 Click the "User data - optional" field.



13

Click "security-group-lb-asg
sg-03c131377be591833
VPC: vpc-071ae984eaa589e75"

able

ewall (security groups) [Info](#)

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

☐ Create security group ☒ Select existing security group

Common security groups [Info](#)

Select security groups

security-group-lb-asg sg-03c131377be591833 X
VPC: vpc-071ae984eaa589e75

Compare security group rules

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

Configure storage [Info](#) [Advanced](#)

8 GiB gp3 Root volume (Not encrypted)

When launched
Scaling
Software
Amazon Lin
ami-0440d3b
Virtual serv
t2.micro
Firewall (se
security-gr
Storage (vo
1 volume(s)
Cancel

14

Click the "User data - optional" field.

2

Allow tags in metadata [Info](#)

Select

User data - optional [Info](#)

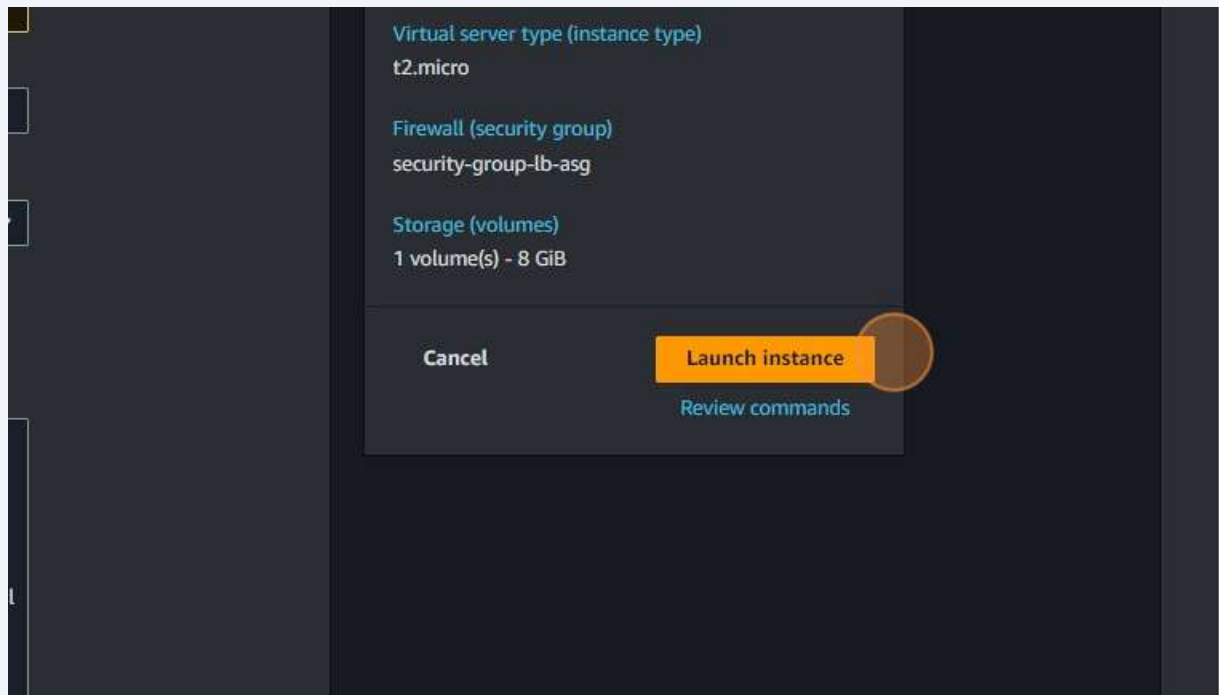
Upload a file with your user data or enter it in the field.

Choose file

```
#!/bin/bash
yum update -y
yum install -y httpd
systemctl start httpd
systemctl enable httpd
echo "<h1> Hello World from $(hostname -f)</h1>" > /var/www/html/index.html
```

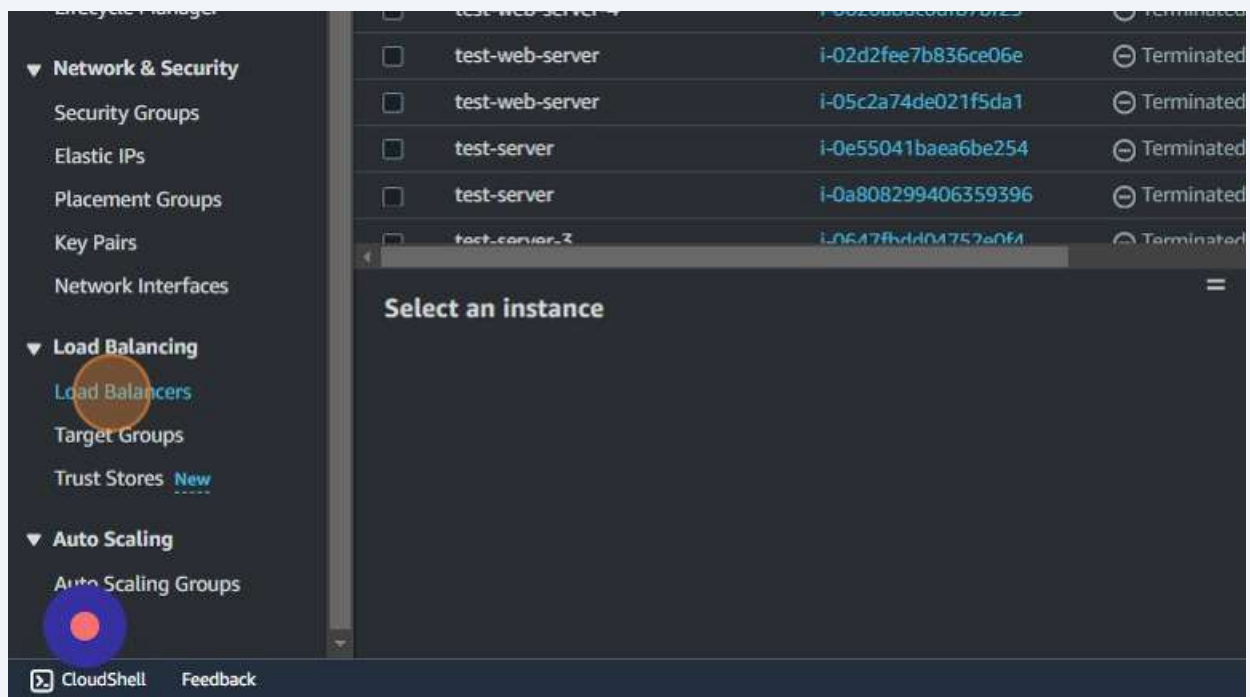
When launched
Scaling
Software
Amazon Lin
ami-0440d3b
Virtual serv
t2.micro
Firewall (se
security-gr
Storage (vo
1 volume(s)
Cancel

15 Click here.

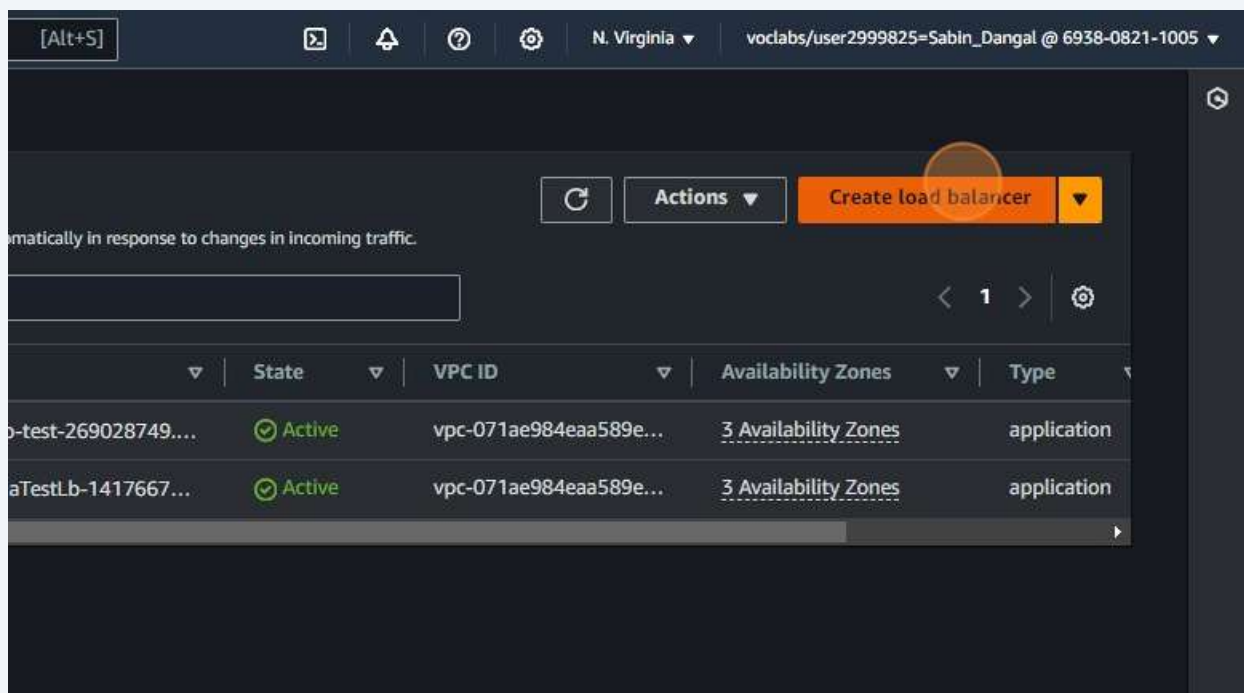


16 Navigate to <https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:sort=instanceState>

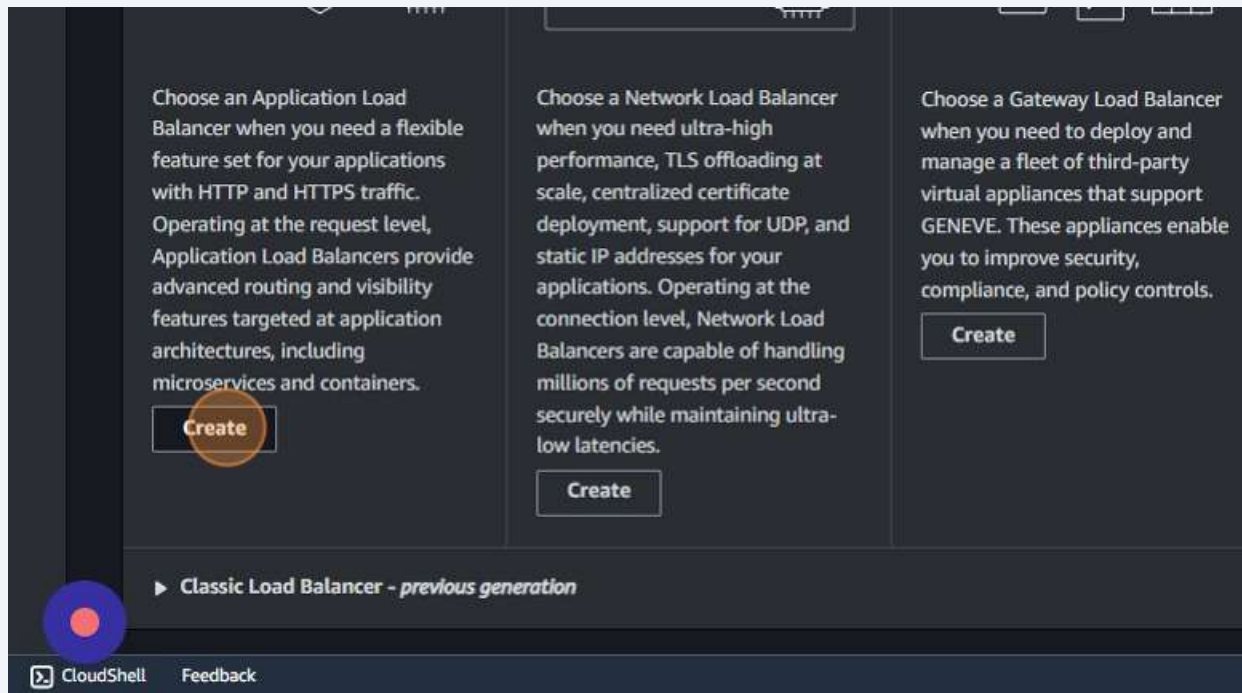
17 Click "Load Balancers"



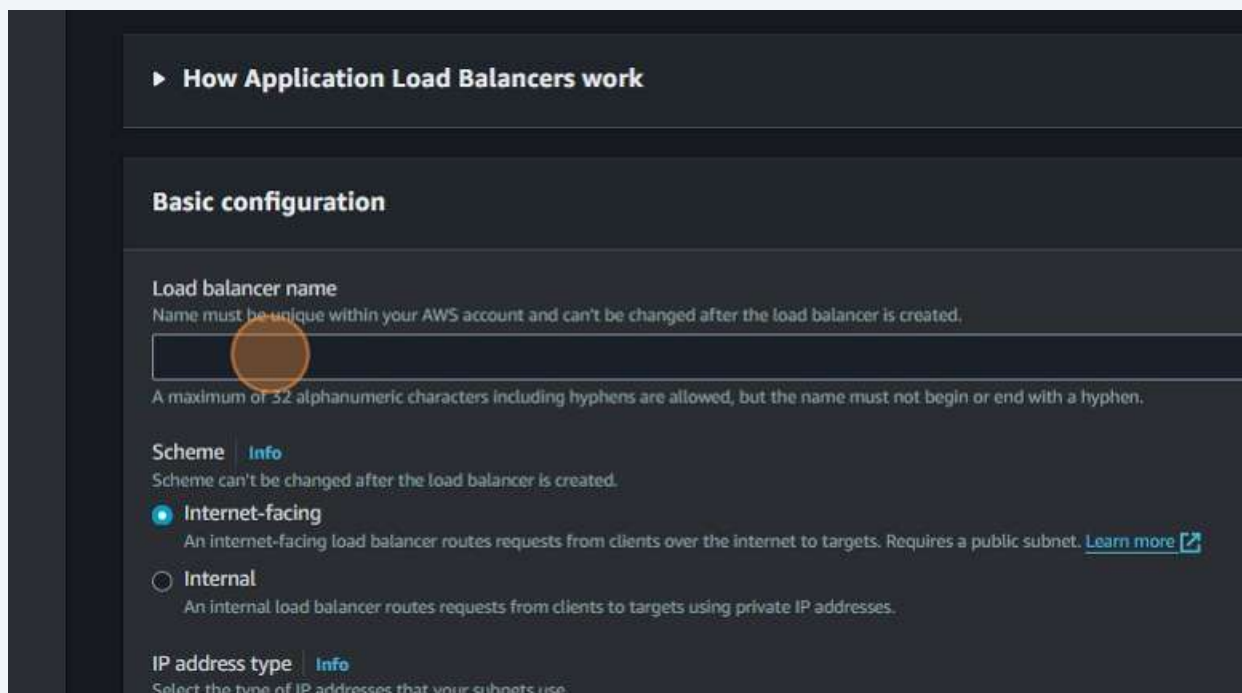
18 Click "Create load balancer"



19 Click "Create"

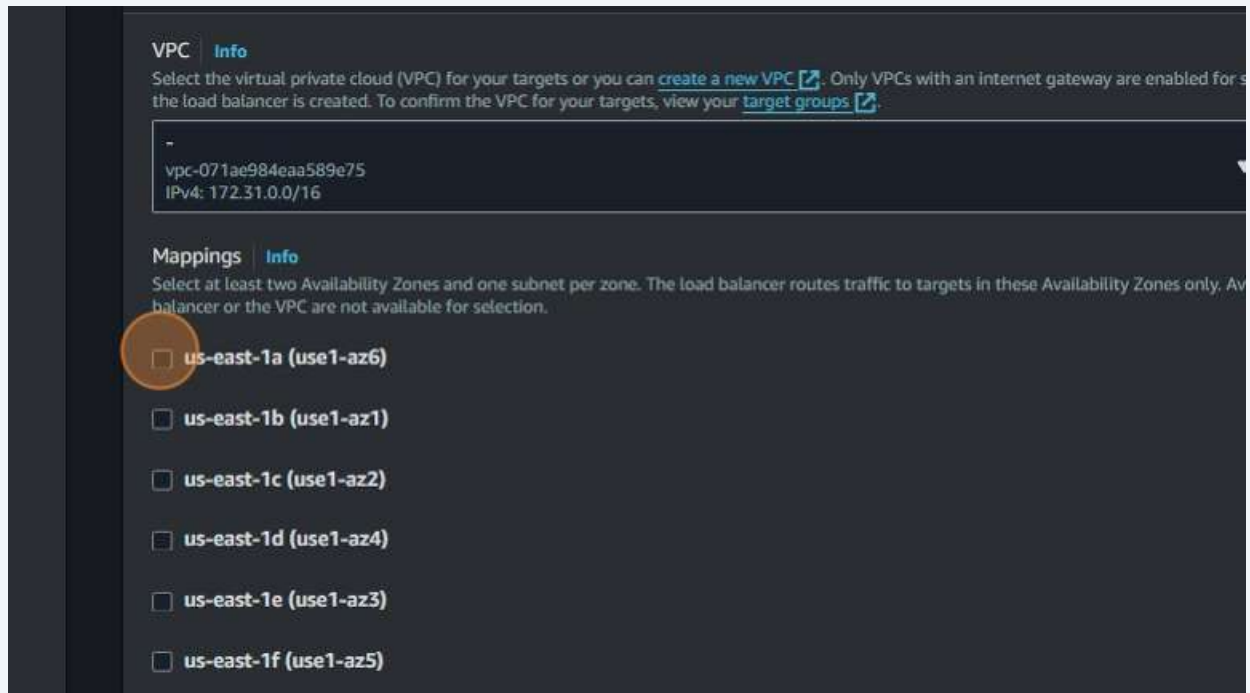


20 Click the "Load balancer name" field.

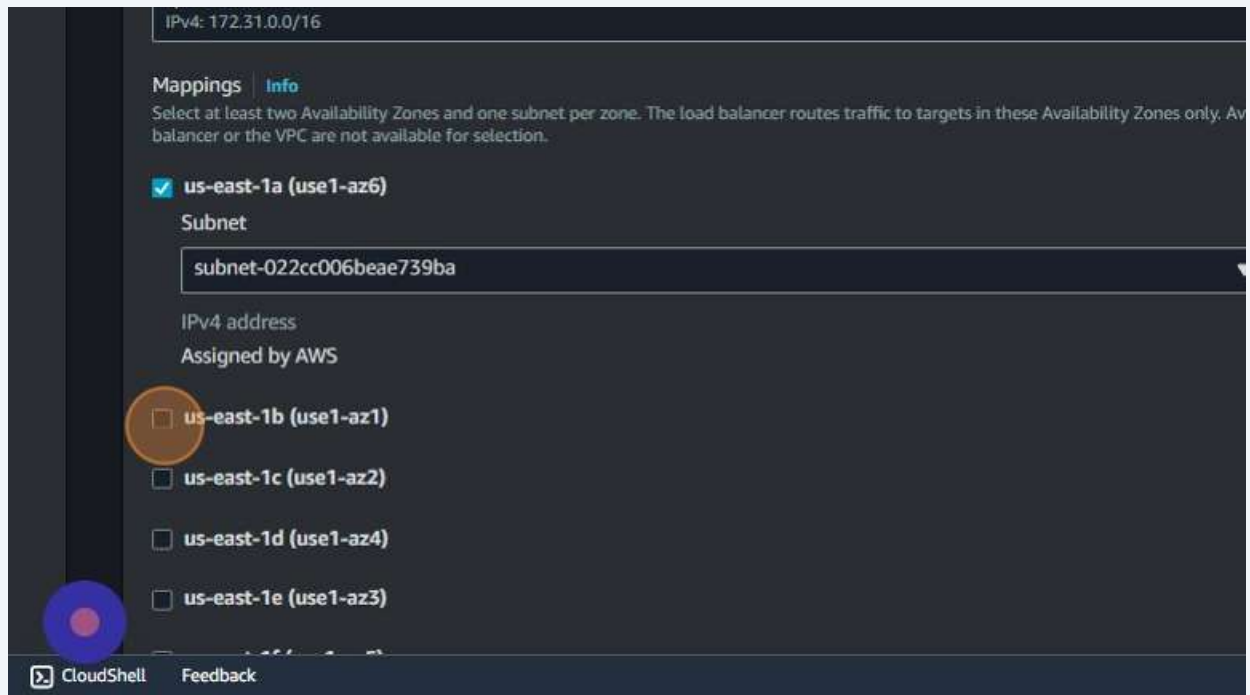


21 Type "load-balancer-adv"

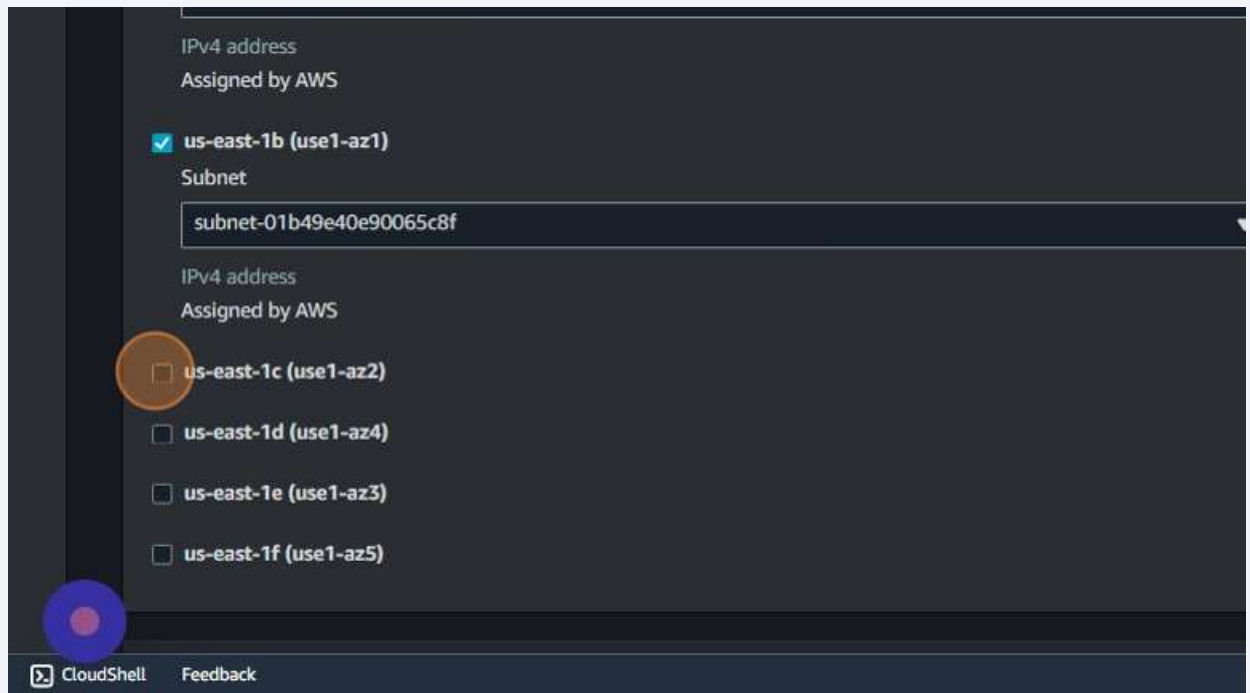
22 Click this checkbox.



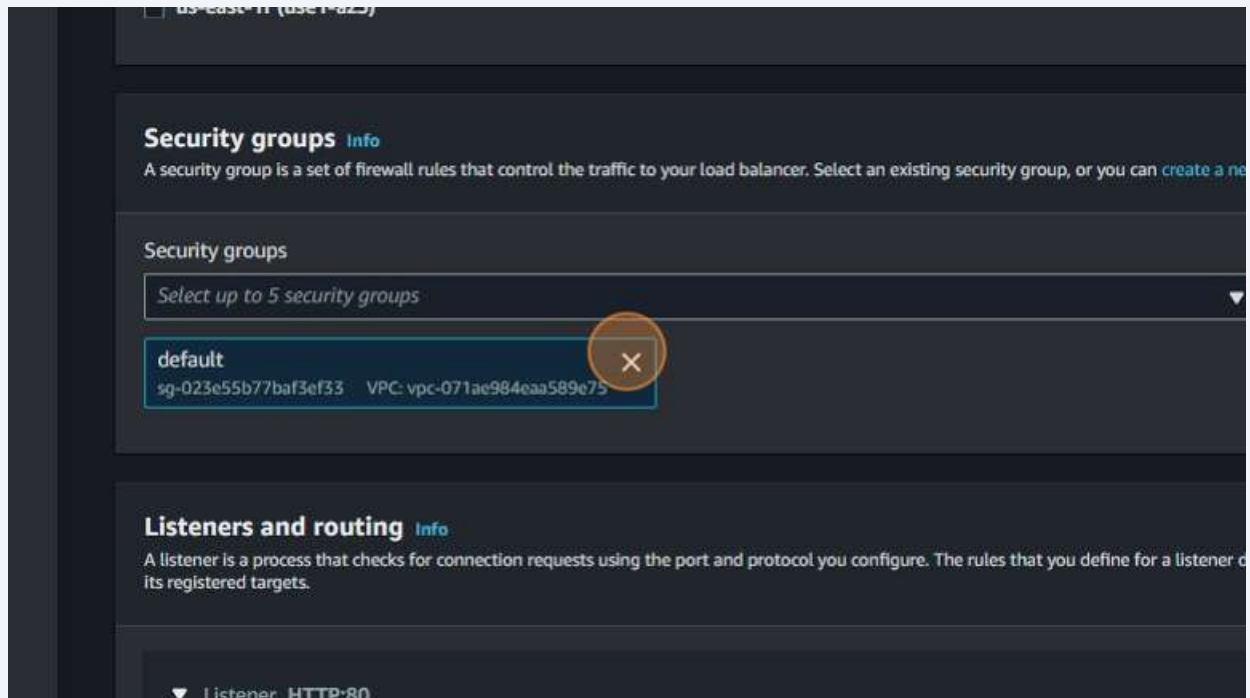
23 Click "us-east-1b (use1-az1)"



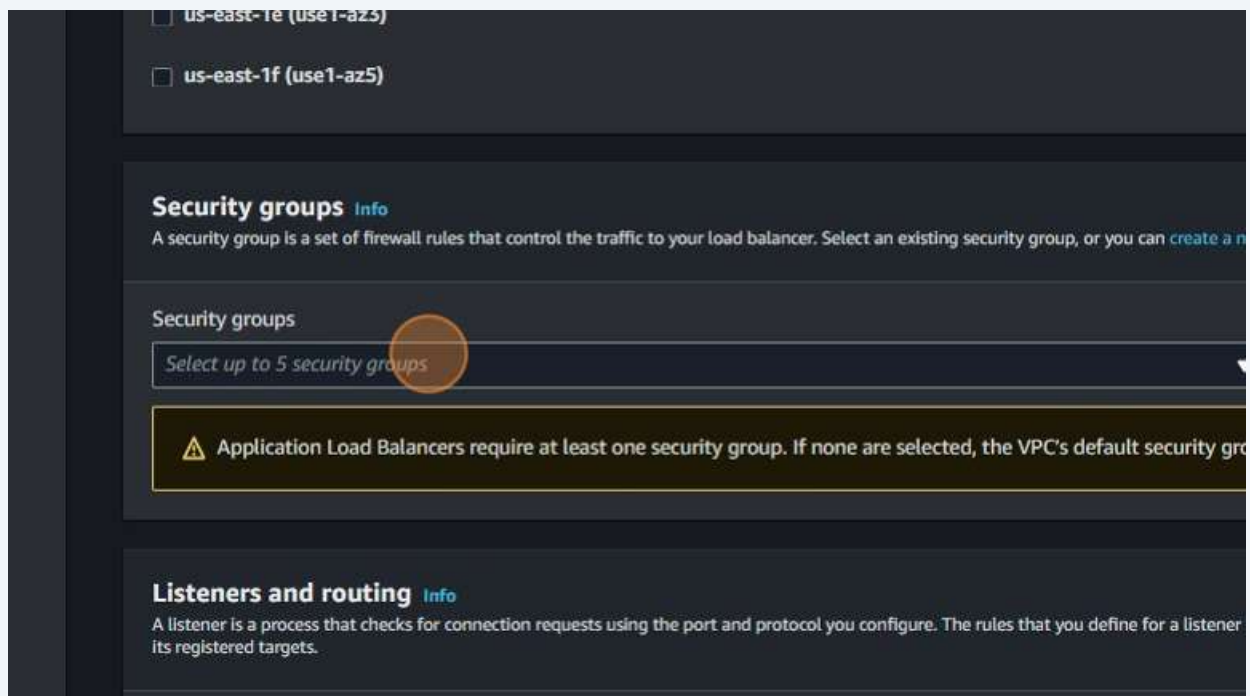
24 Click this checkbox.



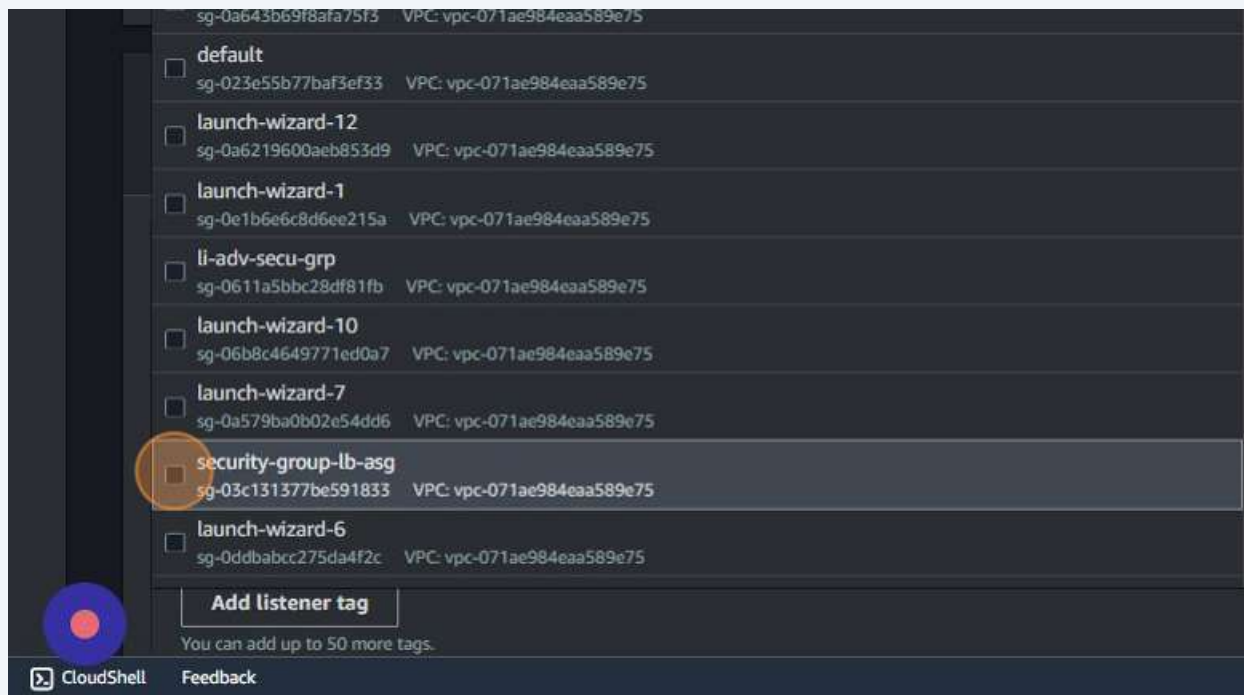
25 Click here.



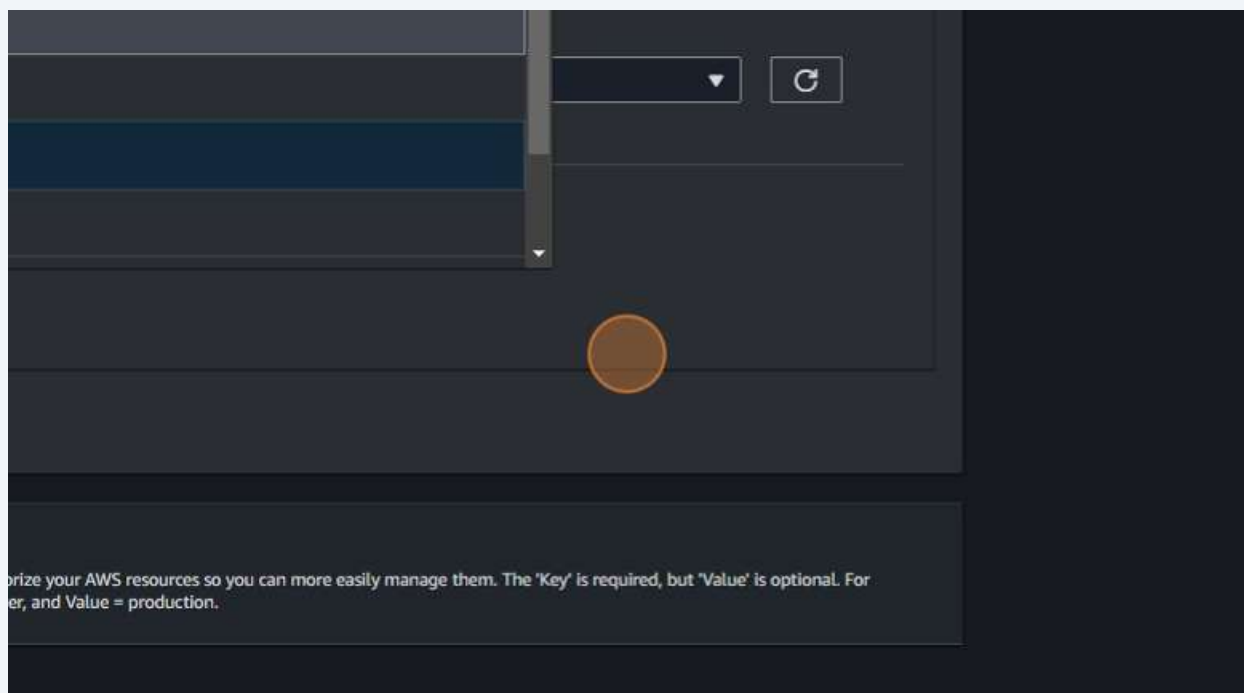
26 Click "Select up to 5 security groups"



27 Click here.



28 Click here.



29 Click "Create target group"

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the traffic is routed to its registered targets.

▼ Listener HTTP:80

Protocol: HTTP Port: 80

Default action: Forward to Select a target group

[Create target group](#)

Listener tags - optional
Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.

[Add listener tag](#)

You can add up to 50 more tags.

[Add listener](#)

30 Click the "Target group name" field.

• Facilitates routing to a single Lambda function.
• Accessible to Application Load Balancers only.

☐ Application Load Balancer

• Offers the flexibility for a Network Load Balancer to accept and route TCP requests.
• Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.

Target group name

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must start with a letter and end with a letter or digit.

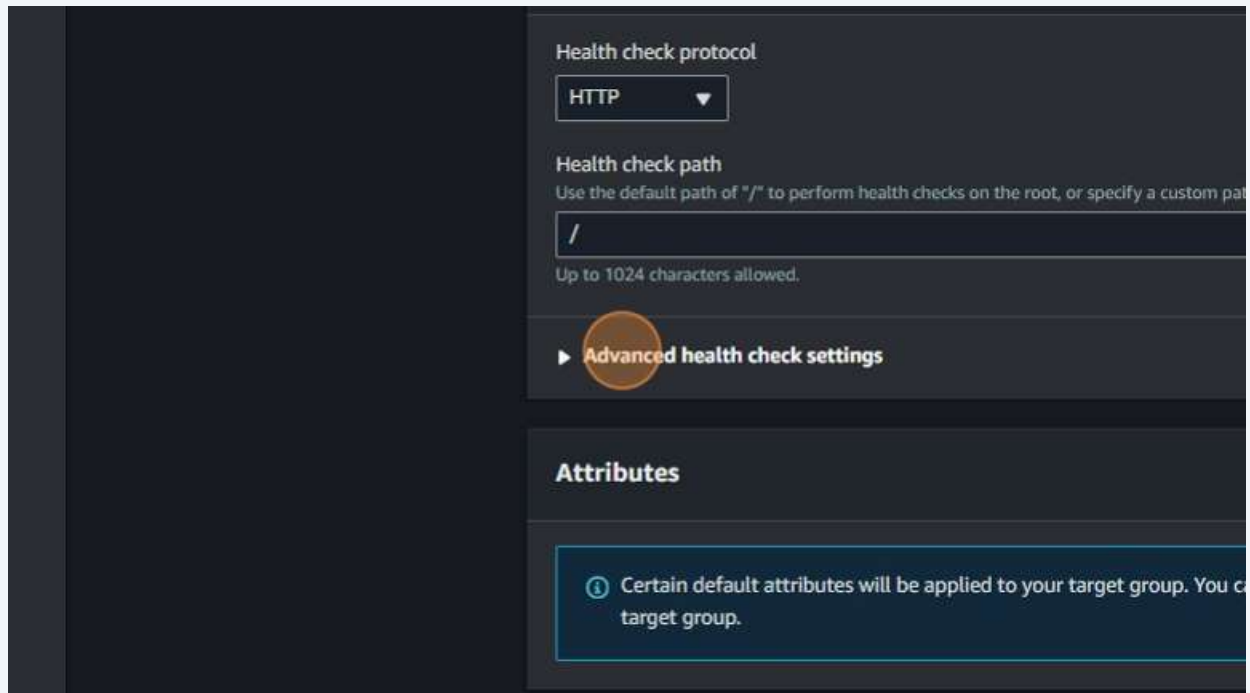
Protocol : Port
Choose a protocol for your target group that corresponds to the Load Balancer type that will be used to route traffic to the targets and you can set mitigation options once your target group is created.

HTTP 80

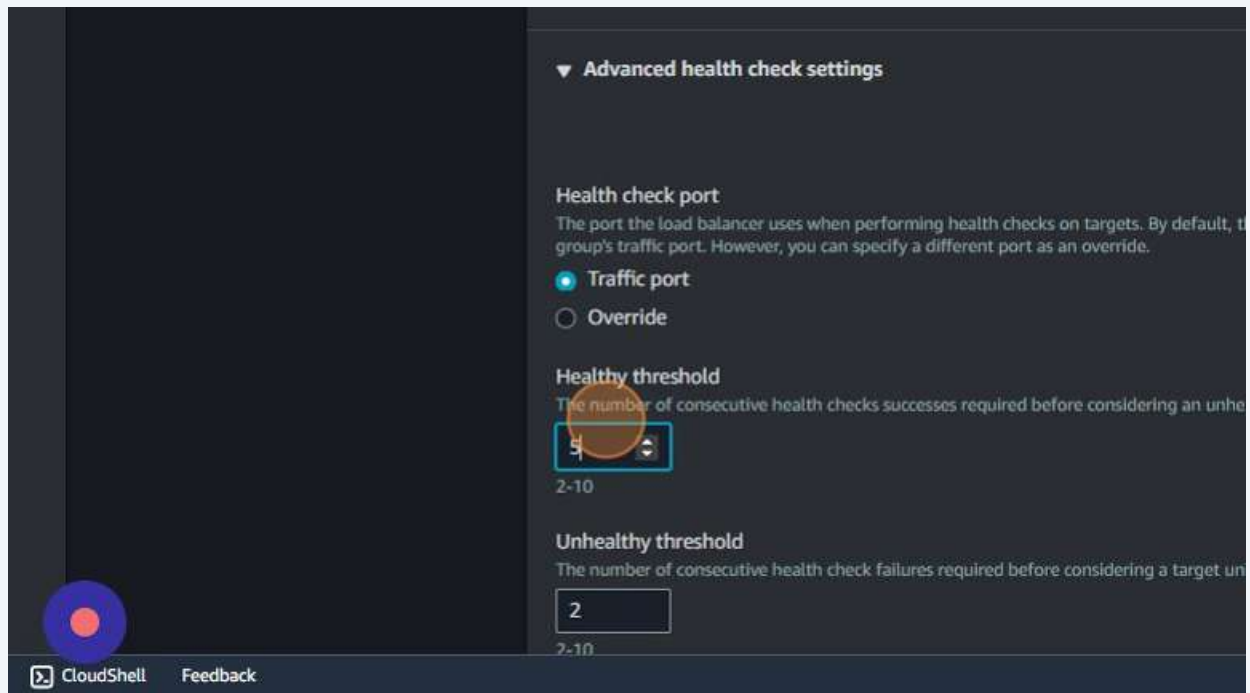
IP address type
Only targets with the indicated IP address type can be registered to this target group.

31 Type "target-grp-adv"

32 Click "Advanced health check settings"

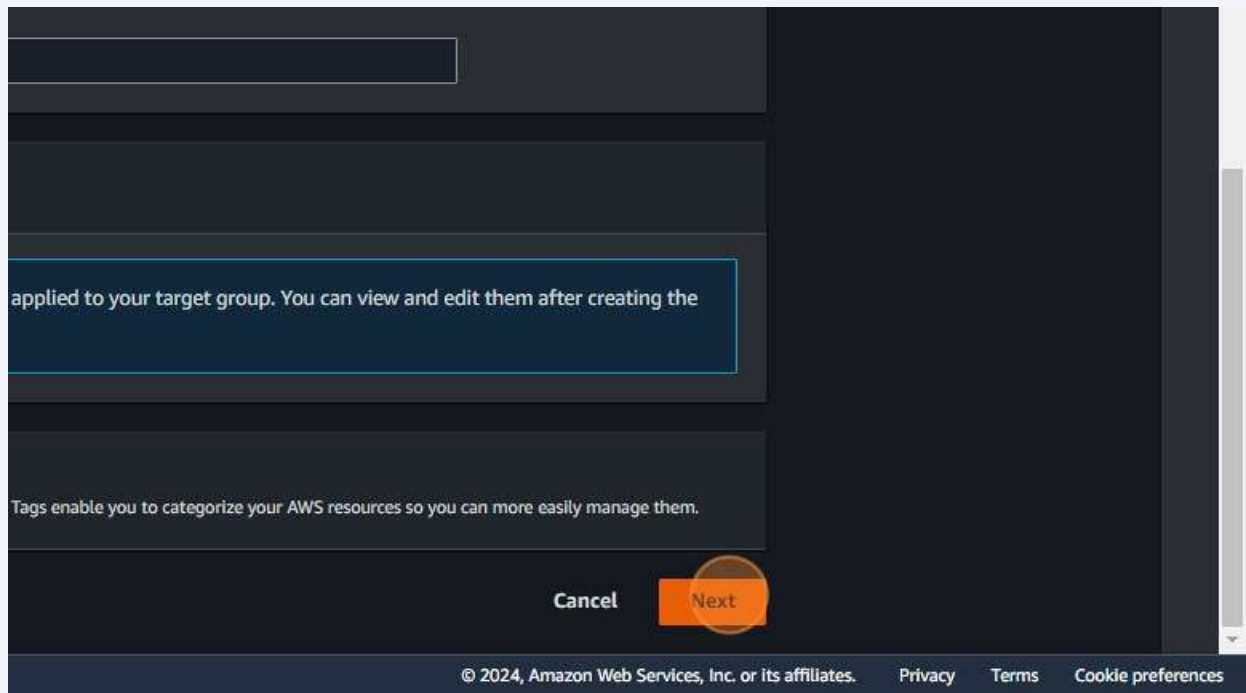


33 Click the "Healthy threshold" field.

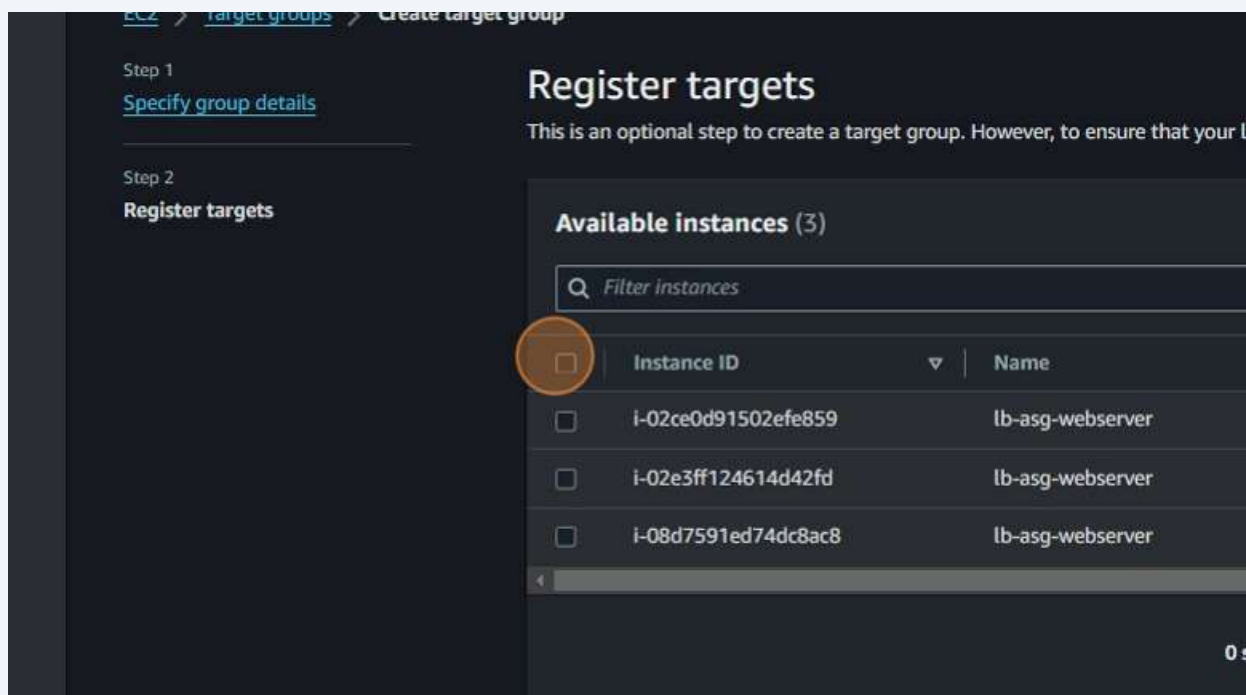


34 Type " **Backspace** 3"

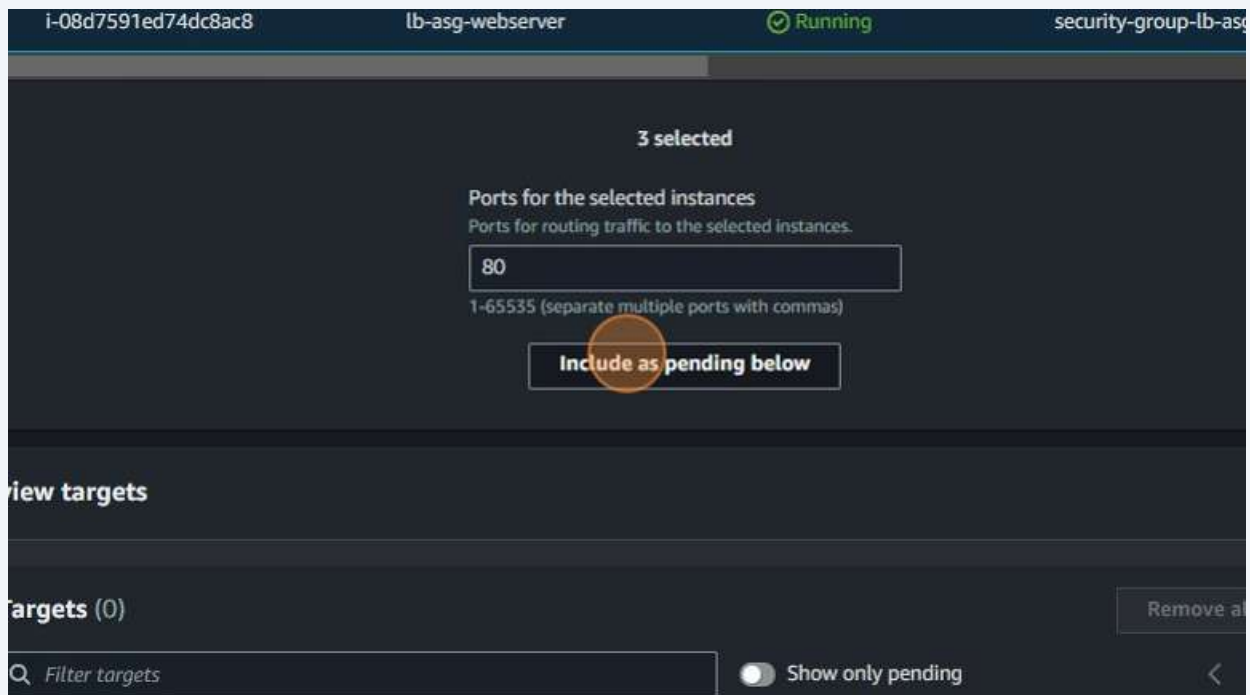
35 Click "Next"



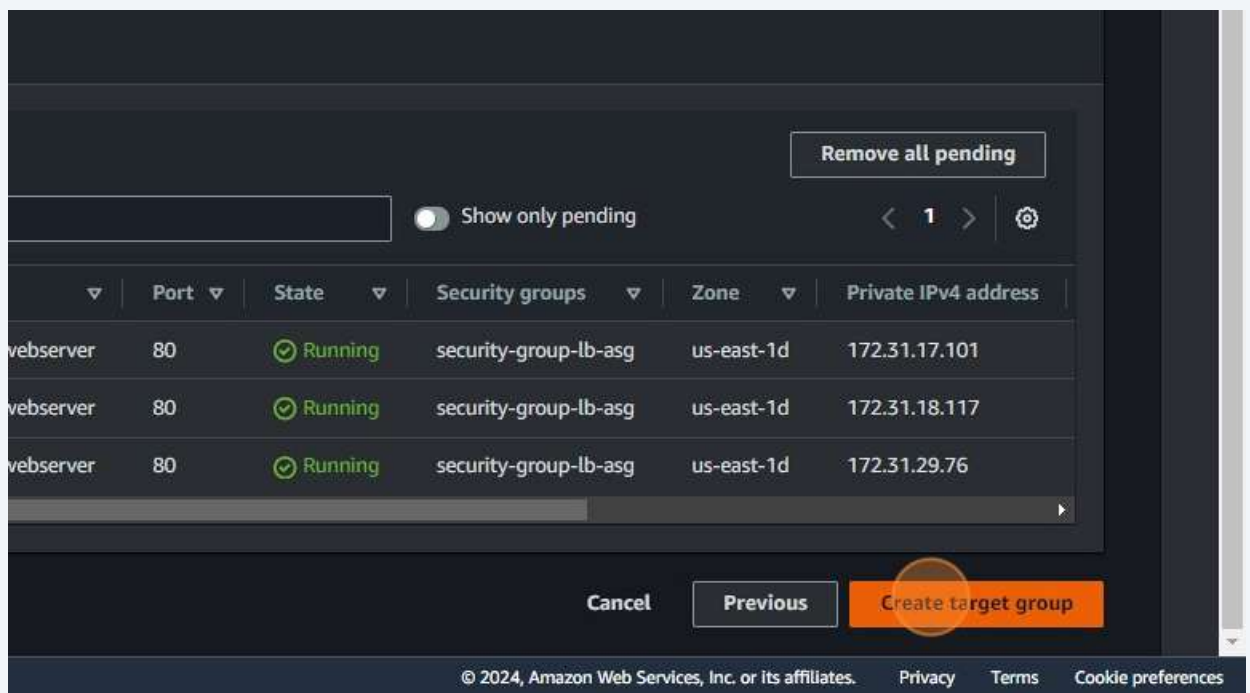
36 Click this checkbox.



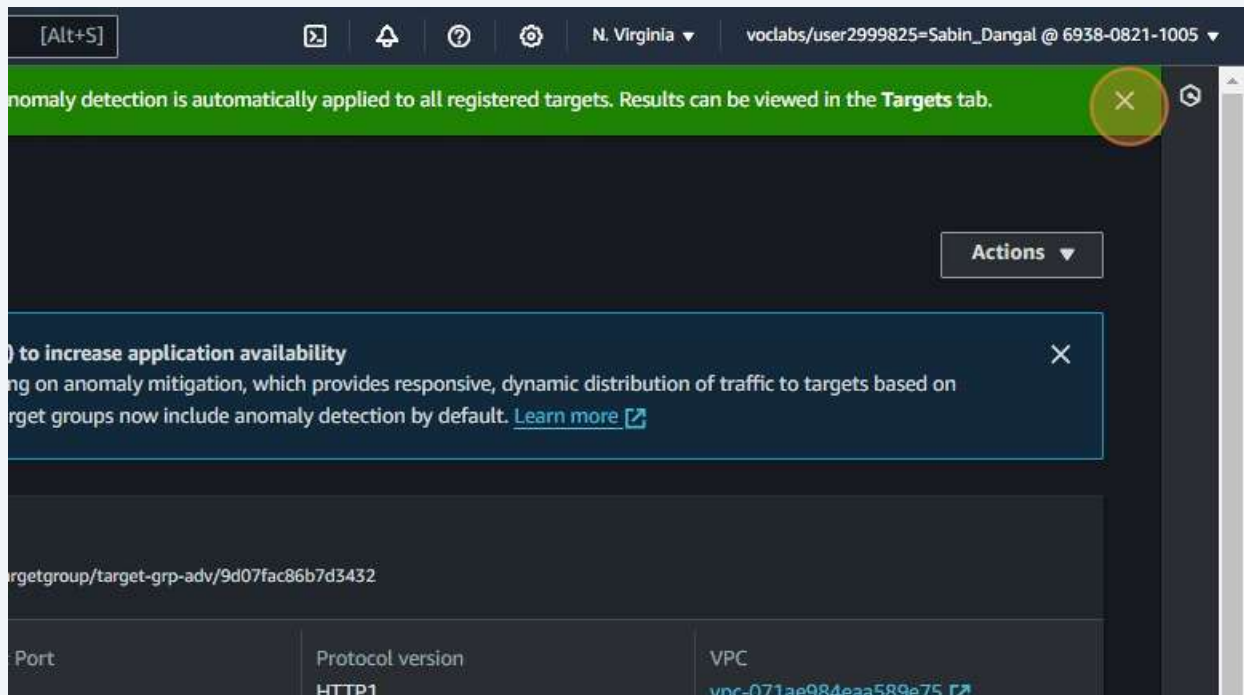
37 Click "Include as pending below"



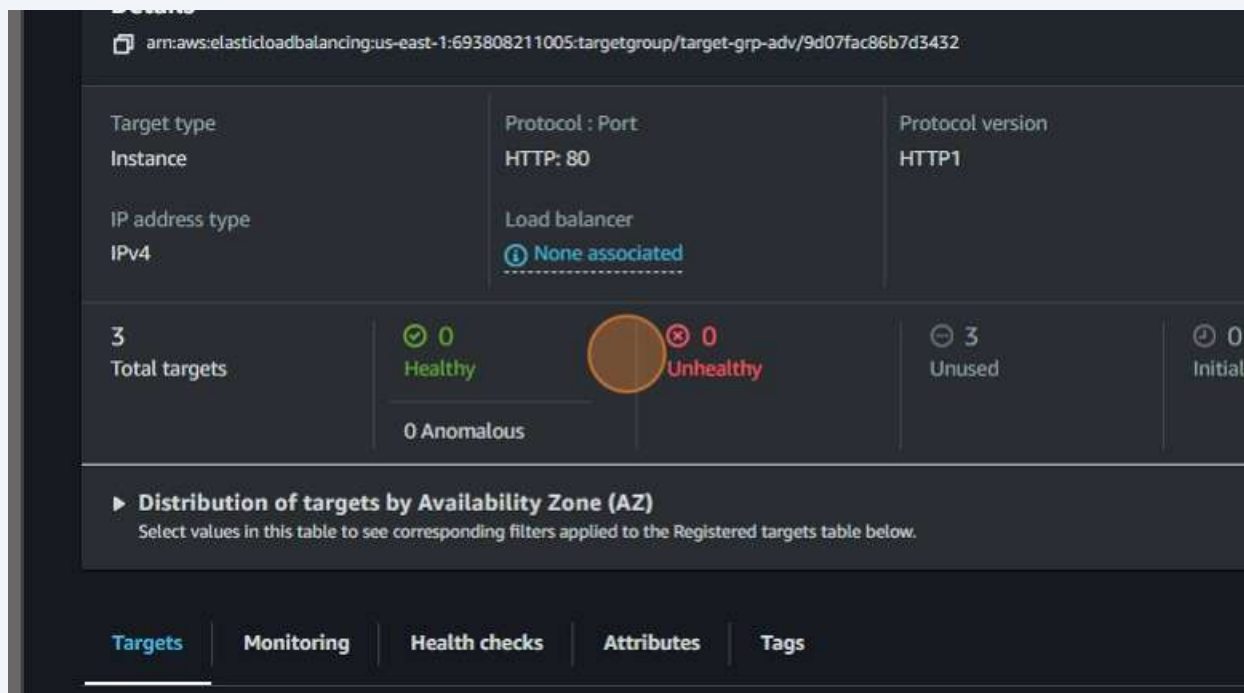
38 Click "Create target group"



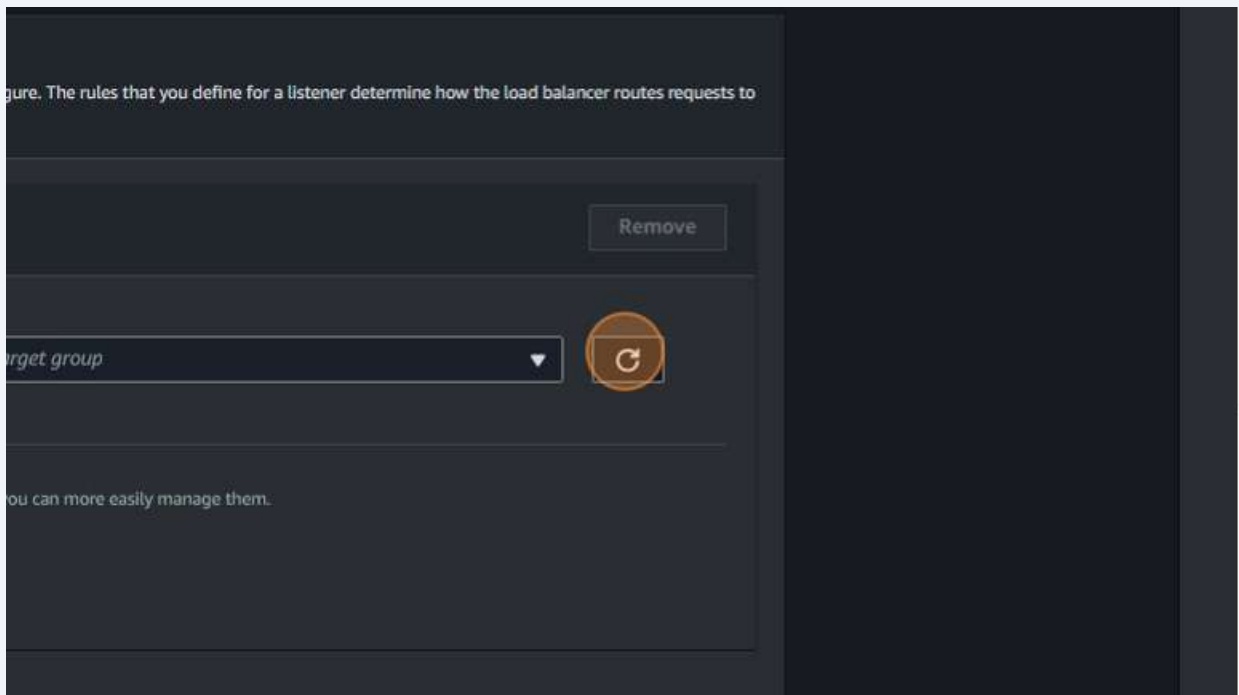
39 Click here.



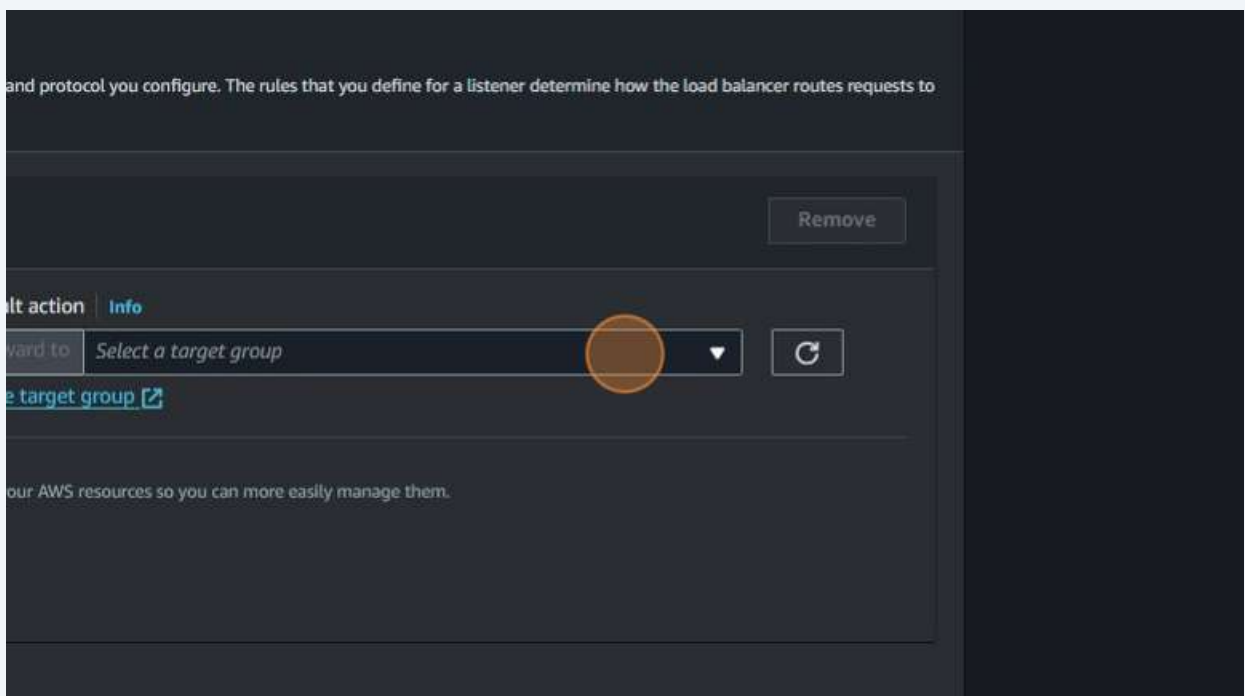
40 Click here.



41 Click here.



42 Click "Select a target group"



43 Click "Target type: Instance, IPv4"

The screenshot shows the AWS Management Console interface for configuring a load balancer. The 'Forward to' dropdown menu is open, displaying a list of target groups. The target group 'target-grp-adv' is highlighted, and its 'Target type: Instance, IPv4' is visible. The 'Default action' is set to 'HTTP'. The 'Port' is set to '80'. The 'Create target' button is visible below the dropdown menu.

Port: 80

Default action: HTTP

Forward to: Select a target group

Create target

lit-adv-test-tg-grp
Target type: Instance, IPv4

myTestLamdaTg
Target type: Lambda, IPv4

target-grp-adv
Target type: Instance, IPv4

HTTP

HTTP

tags - optional

to your load balancer. Tags enable you to categorize your AWS resources so you can more easily manage them. The 'Key' is required, but 'Value' is optional. For example, Key = production-webserver, or Key = webserver, and Value = production.

44 Click "Create load balancer"

The screenshot shows the AWS Management Console interface for creating a load balancer. The 'Create load balancer' button is highlighted. The 'Tags' section is visible, showing a list of tags. The 'Create load balancer' button is located at the bottom right of the console.

Tags Edit

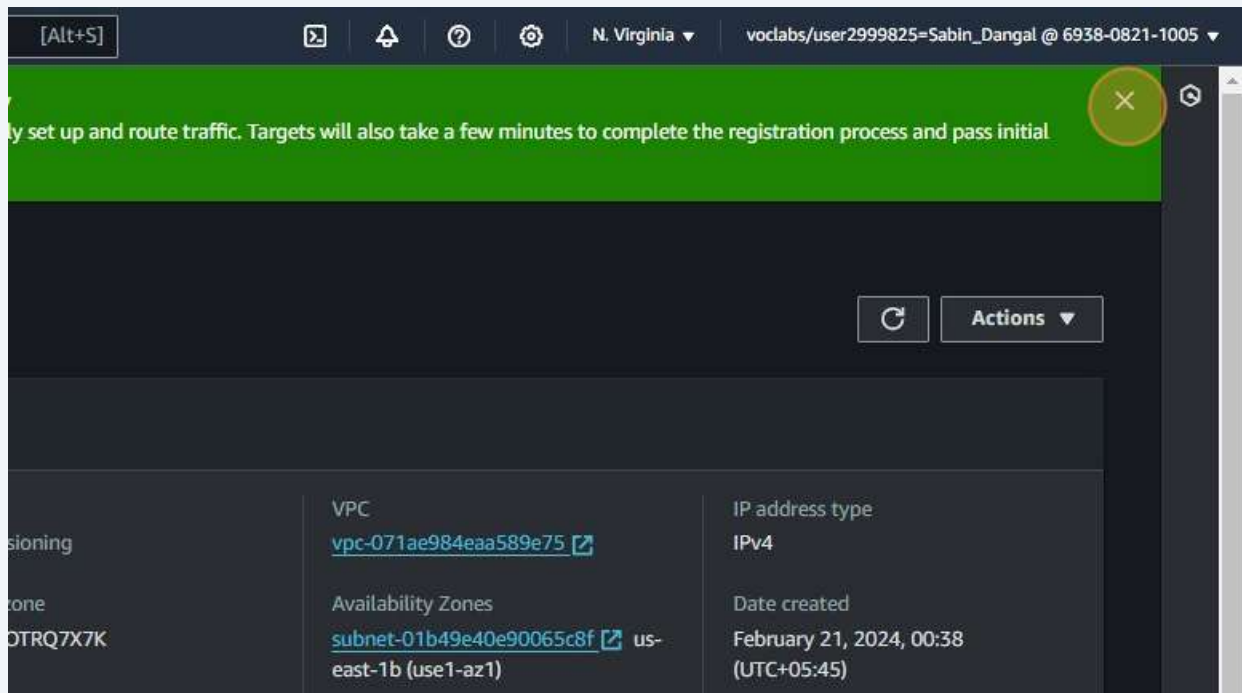
None

and edit them after creating the load balancer.

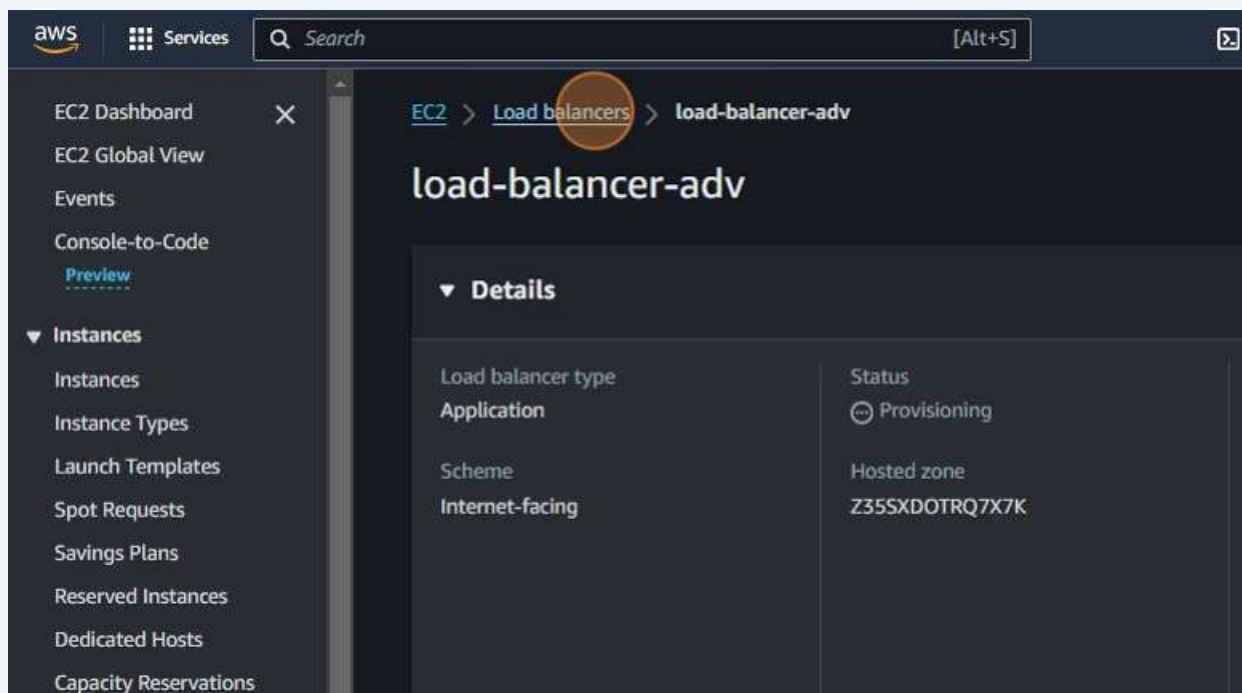
Cancel Create load balancer

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

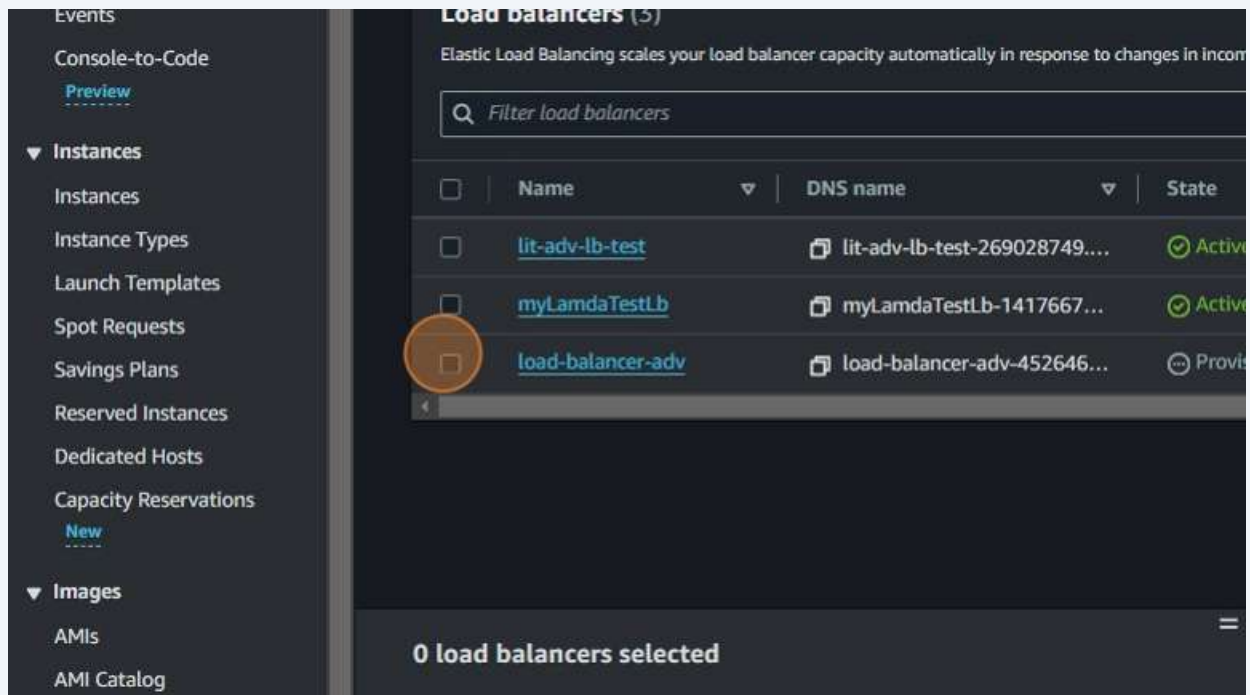
45 Click here.



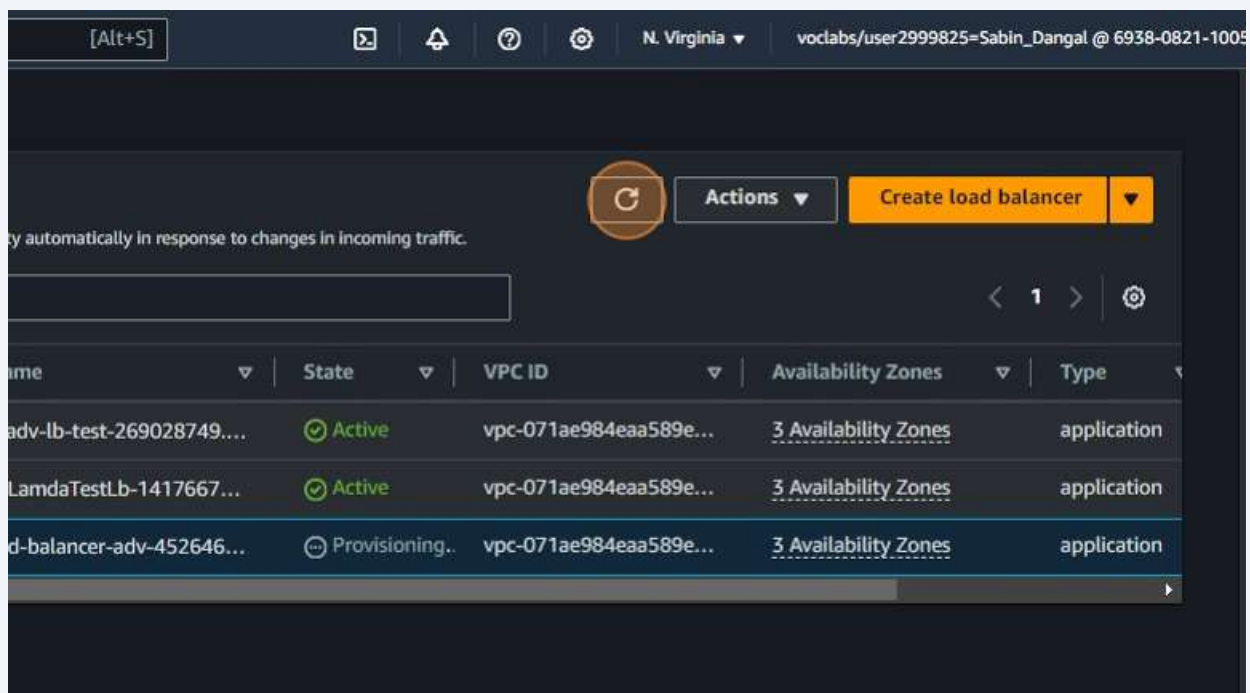
46 Click "Load balancers"



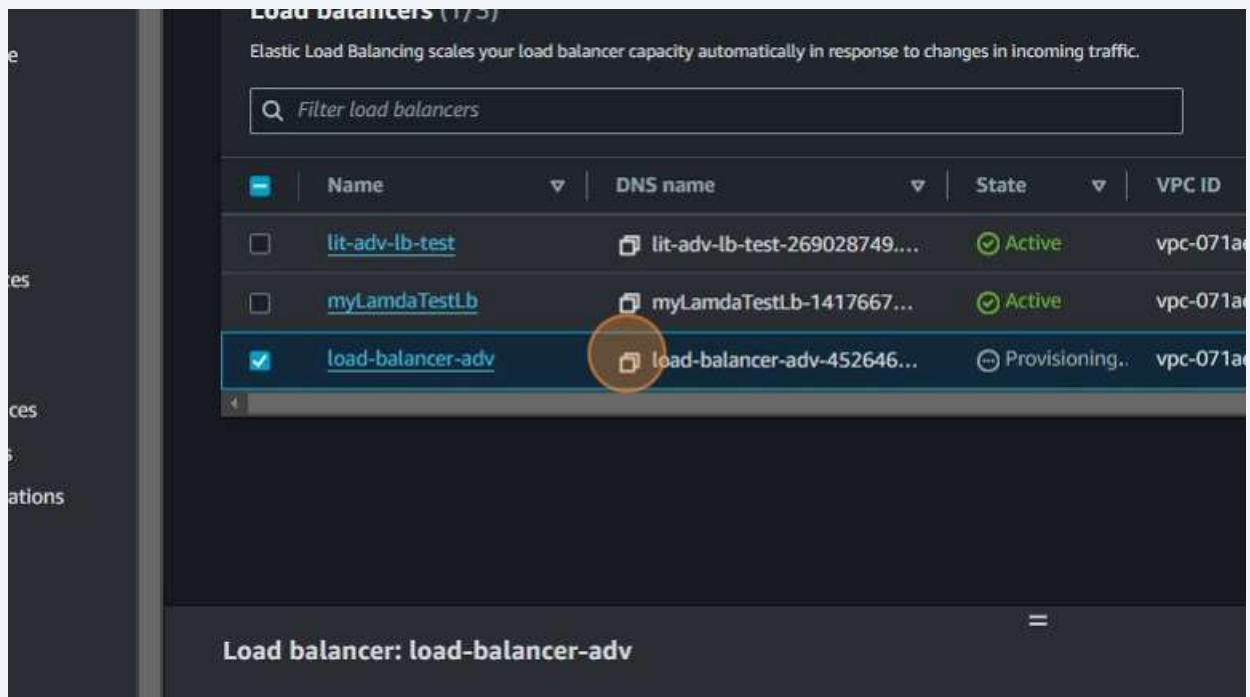
47 Click this checkbox.



48 Click here.

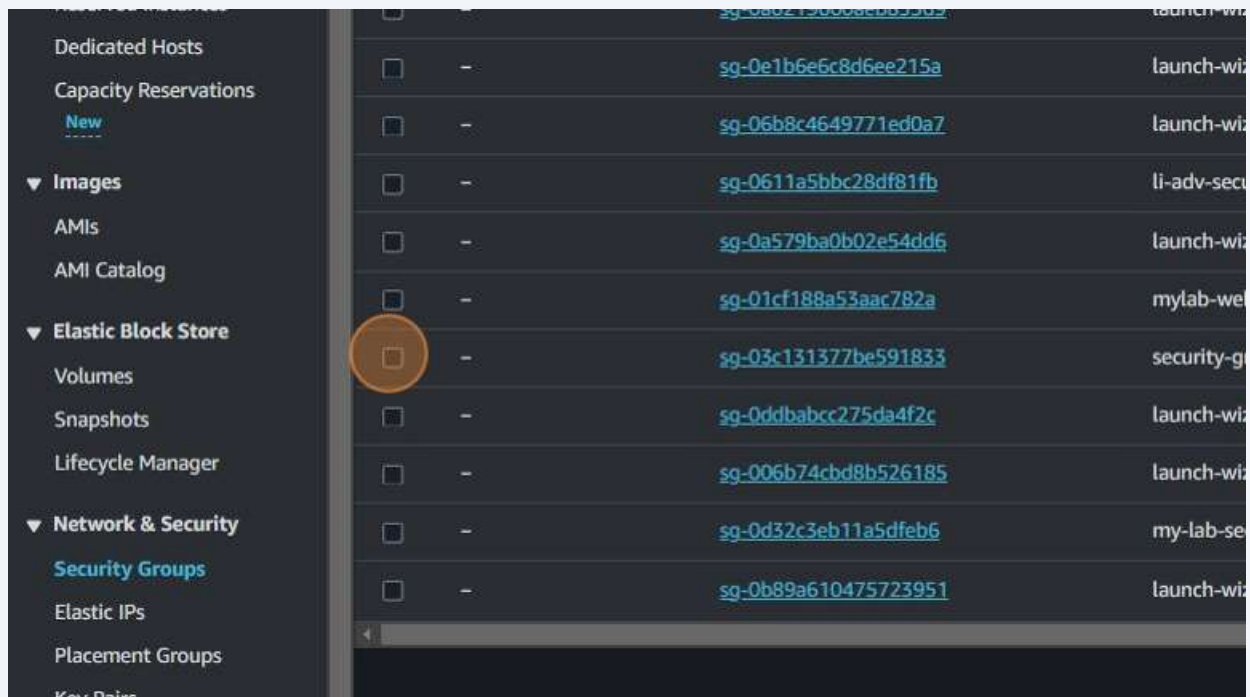


49 Click here.

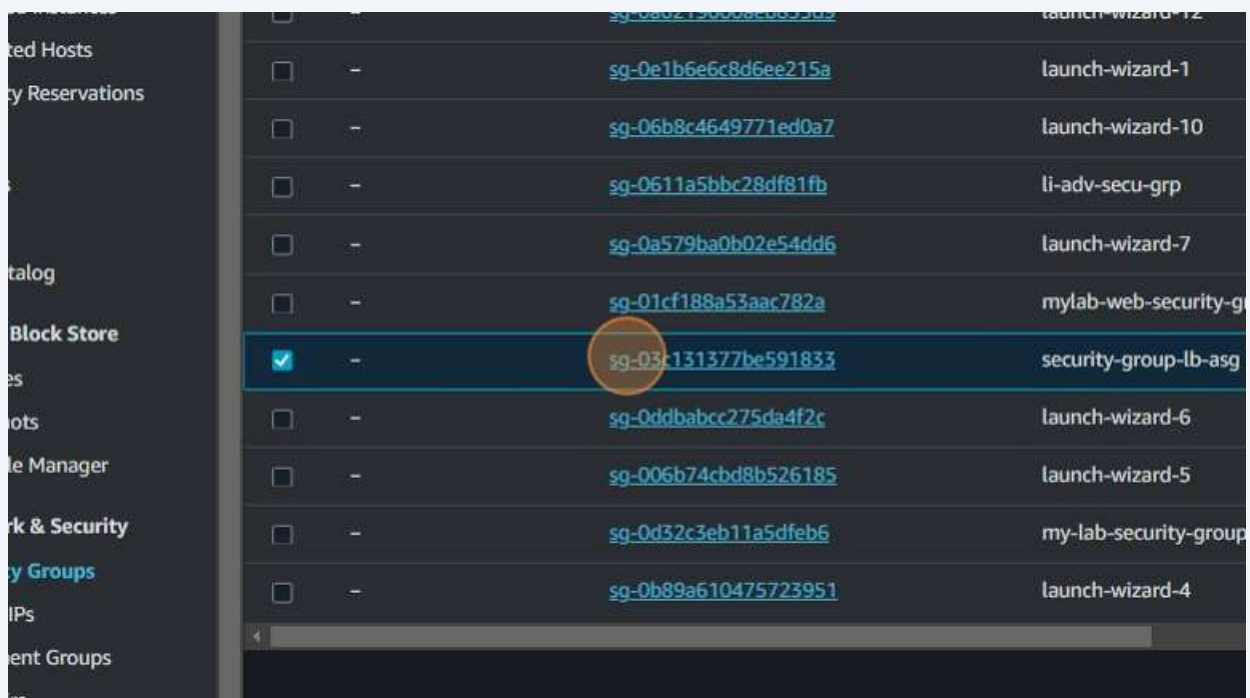


50 Navigate to <https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#SecurityGroups:>

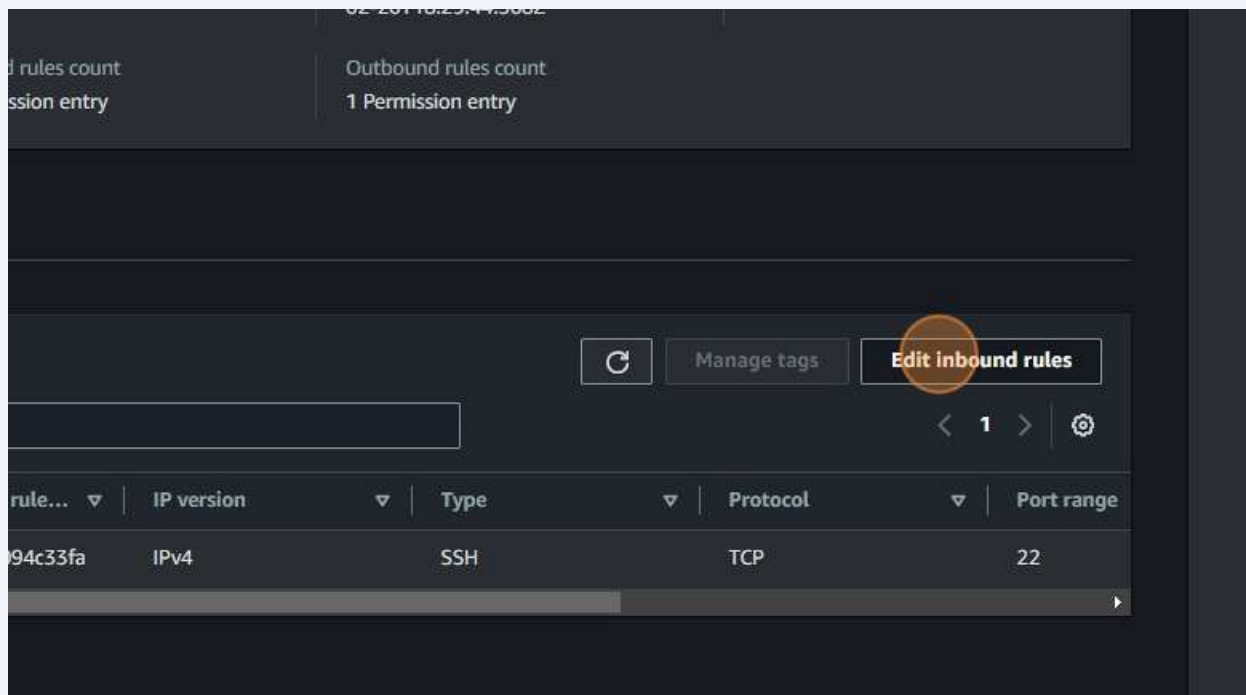
51 Click this checkbox.



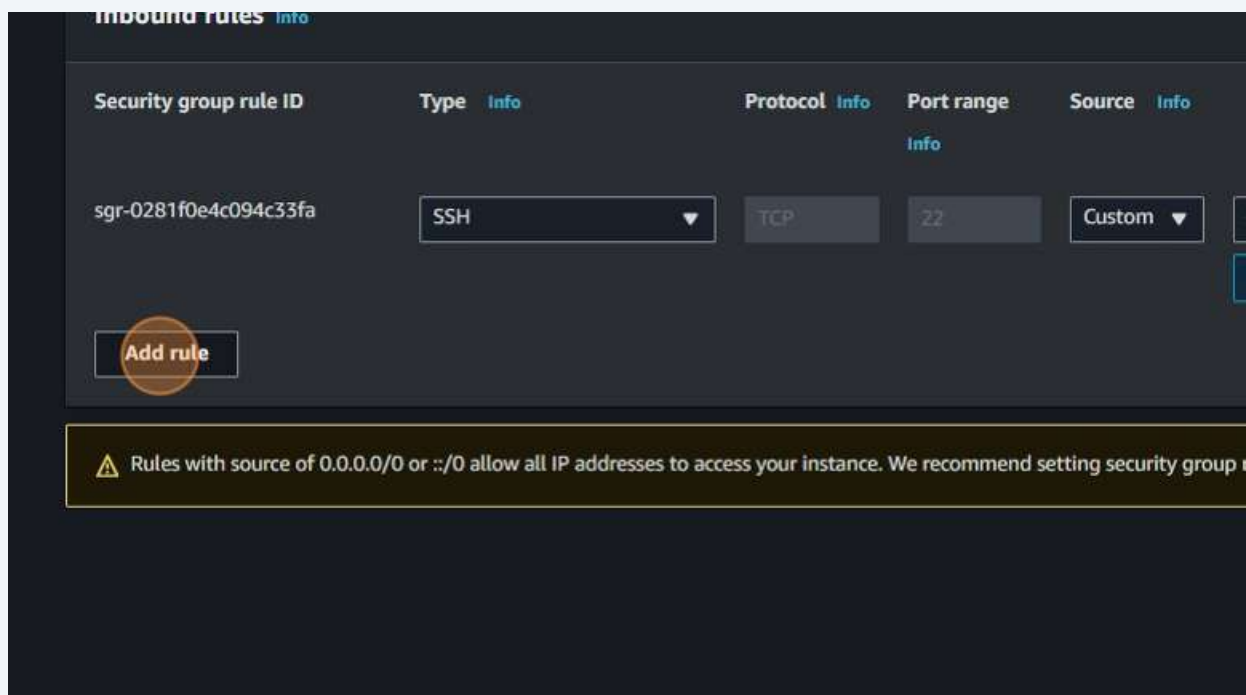
52 Click "sg-03c131377be591833"



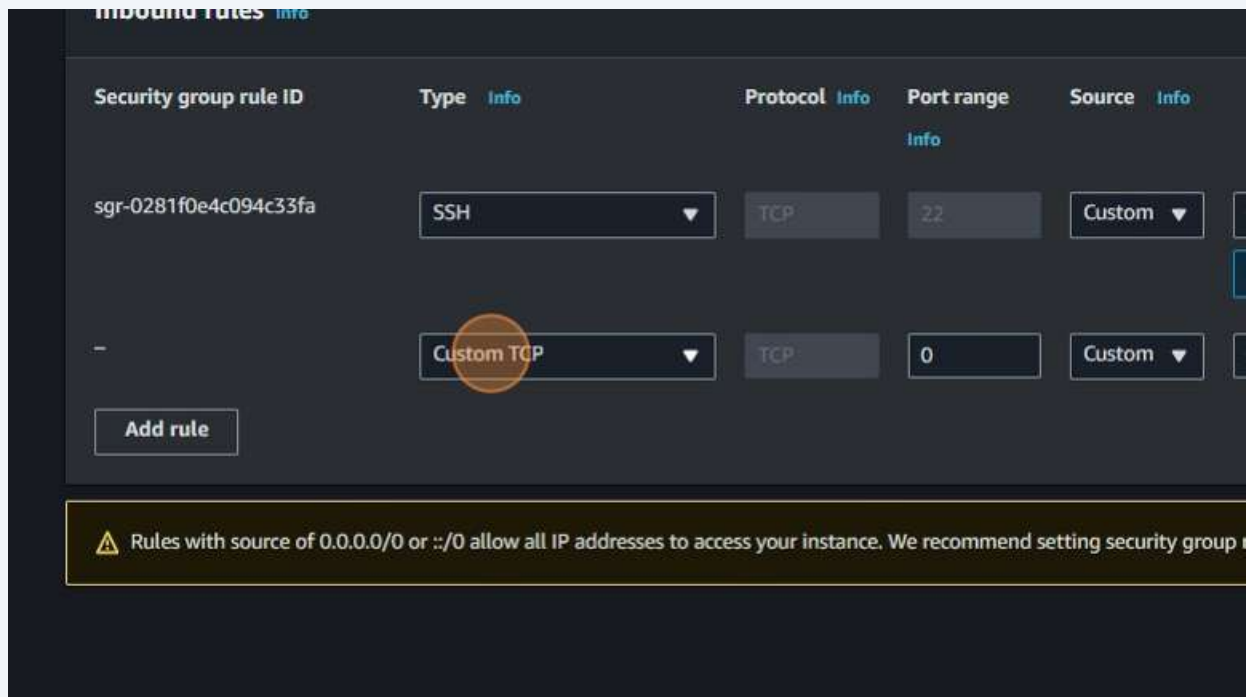
53 Click "Edit inbound rules"



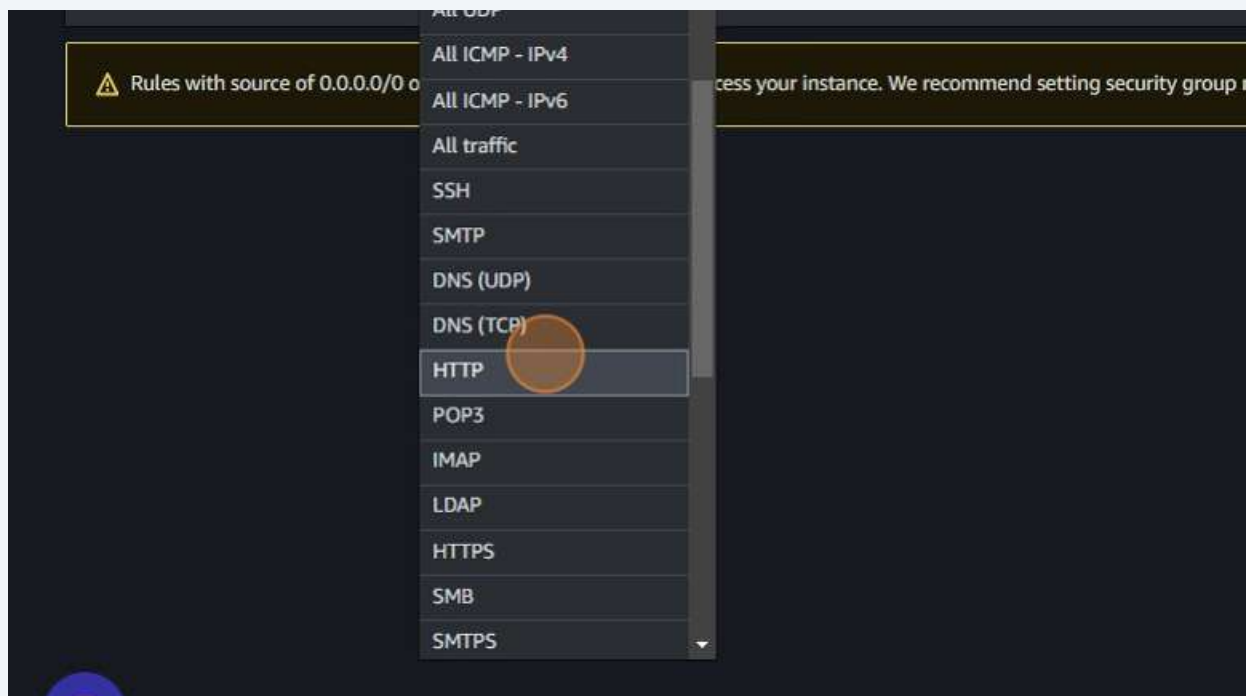
54 Click "Add rule"



55 Click "Custom TCP"



56 Click "HTTP"



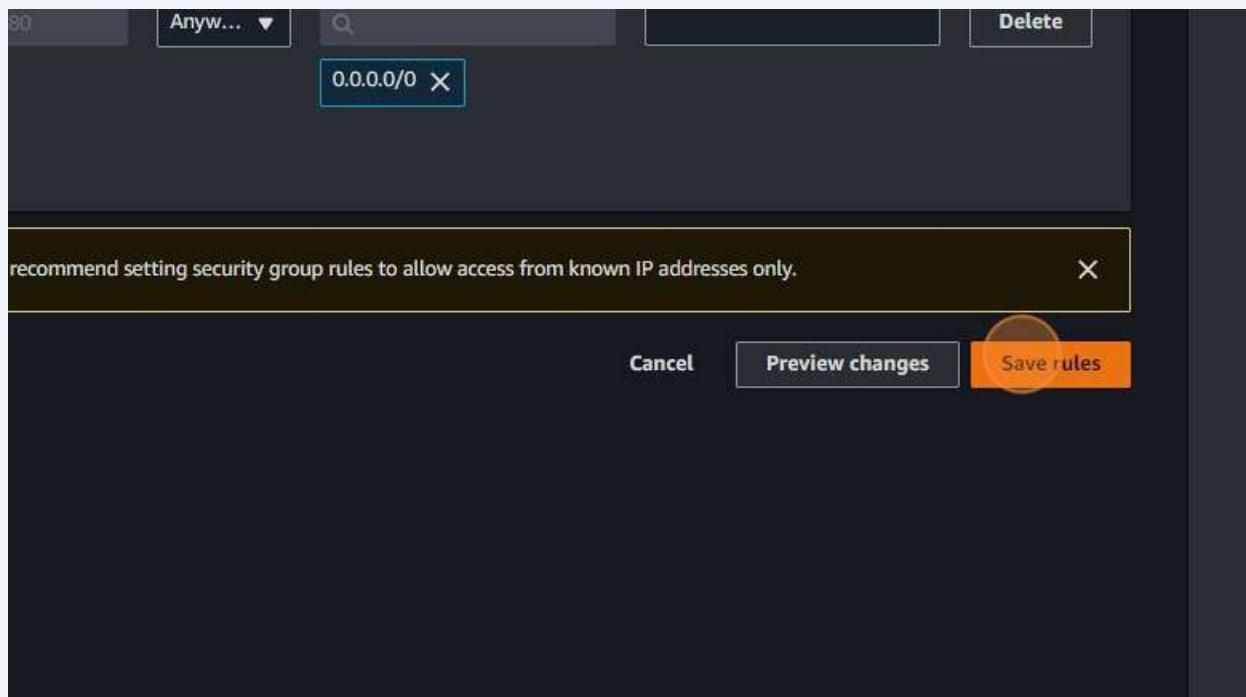
57 Click "Custom"

The screenshot shows the AWS Security Groups configuration interface. The 'Source' dropdown menu is open, displaying options: 'Custom' (selected with a checkmark), 'Anywhere-IPv4', and 'Anywhere-IPv6'. The 'Protocol' is set to 'TCP' and the 'Port range' is '22'. A search bar with '0.0.0.0/0' and a close button is visible. The interface includes columns for 'Protocol', 'Port range', 'Source', and 'Description - optional'. At the bottom, there are 'Cancel' and 'Preview' buttons.

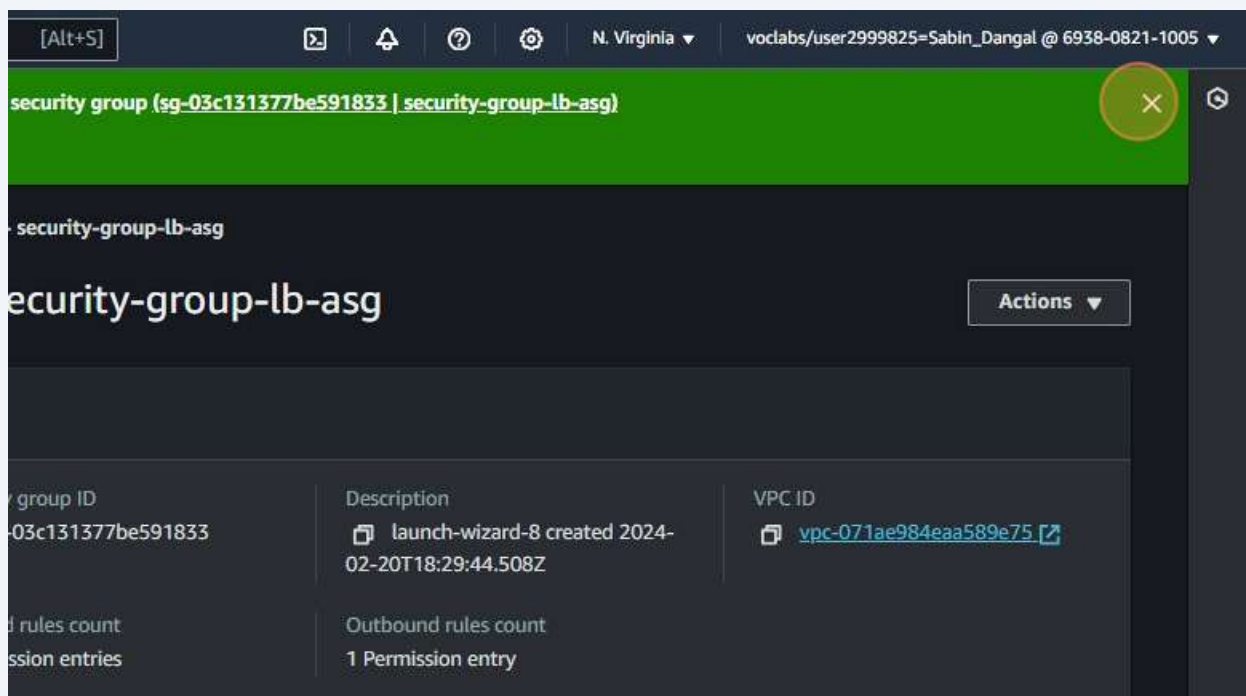
58 Click "Anywhere-IPv4"

The screenshot shows the AWS Security Groups configuration interface. The 'Source' dropdown menu is open, displaying options: 'Custom' (with a checkmark), 'Anywhere-IPv4' (highlighted with an orange circle), 'Anywhere-IPv6', and 'My IP'. The 'Protocol' is set to 'TCP' and the 'Port range' is '80'. A search bar with '0.0.0.0/0' and a close button is visible. The interface includes columns for 'Protocol', 'Port range', 'Source', and 'Description - optional'. At the bottom, there are 'Cancel' and 'Preview' buttons.

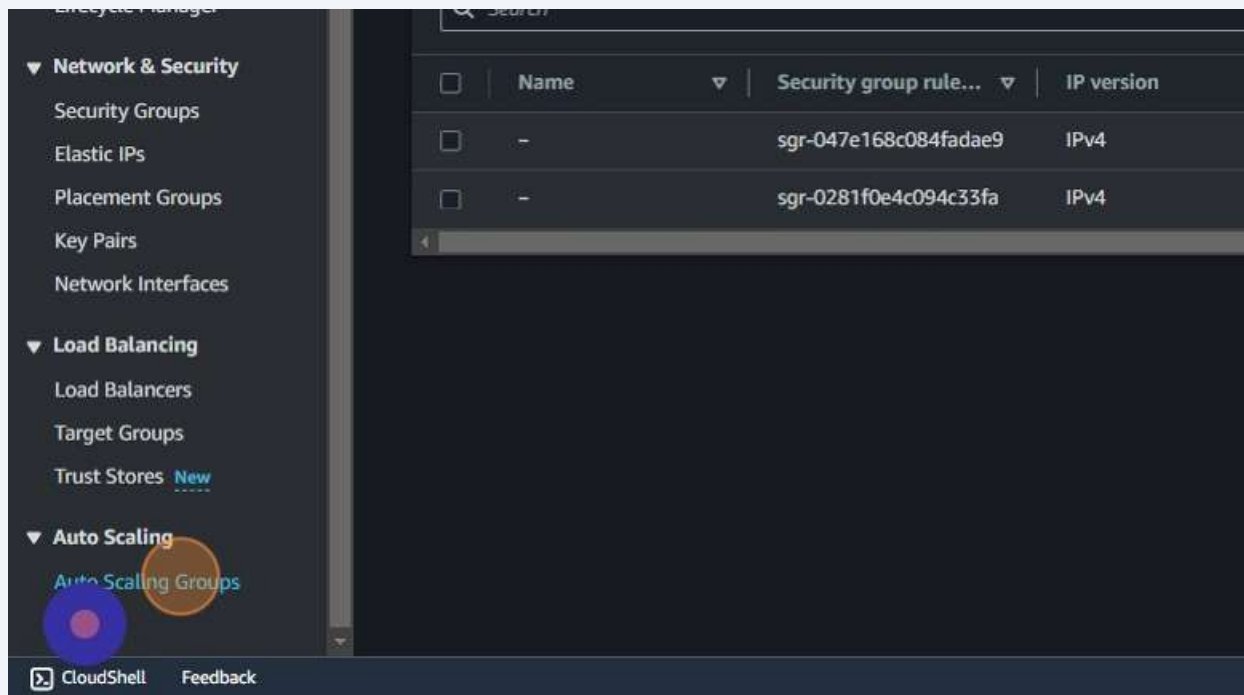
59 Click "Save rules"



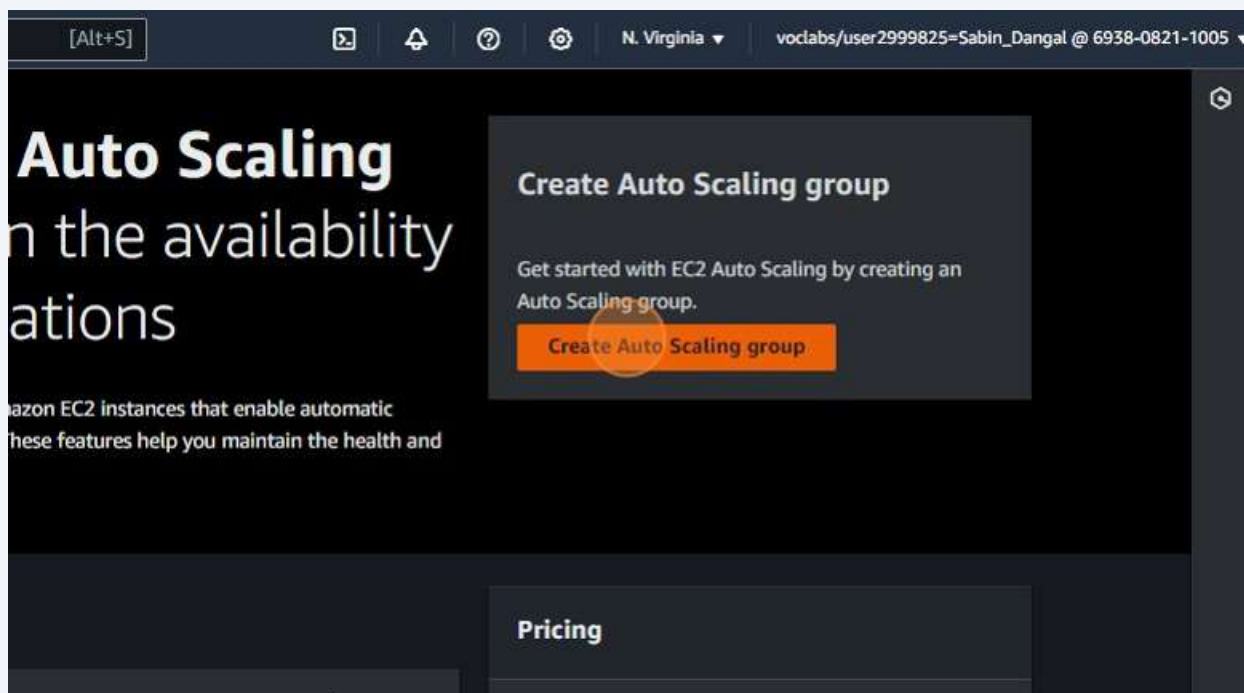
60 Click here.



61 Click "Auto Scaling Groups"



62 Click "Create Auto Scaling group"



63 Click the "Auto Scaling group name" field.

The screenshot shows the AWS Management Console interface for creating an Auto Scaling group. On the left, a sidebar lists the steps: Step 1: Choose launch template, Step 2: Choose instance launch options, Step 3 - optional: Configure advanced options, Step 4 - optional: Configure group size and scaling, Step 5 - optional: Add notifications, and Step 6 - optional: Add tags. The main content area is titled 'Choose launch template' with a subtitle 'Specify a launch template that contains settings common to all EC2 instances t'. Below the title, there is a section for 'Name' with a sub-section 'Auto Scaling group name' that says 'Enter a name to identify the group.' A text input field is present, and the first character 'I' is highlighted with a red circle. Below the input field, a note states 'Must be unique to this account in the current Region and no more than 255 characters.' Further down, there is a 'Launch template' section with an 'Info' icon and a note: 'For accounts created after May 31, 2023, the EC2 console only supports launch templates. Creating Auto Scaling groups with launch configurations is available via the CLI and API until December 31, 2023.'



64 Type "auto-scaling-grp-adv"


65 Click "Select a launch template"

Launch template [Info](#)

Info For accounts created after May 31, 2023, the EC2 console only supports creating Auto Scaling groups with launch templates. Creating Auto Scaling groups with launch configurations is not recommended but still available via the CLI and API until December 31, 2023.

Launch template
Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.

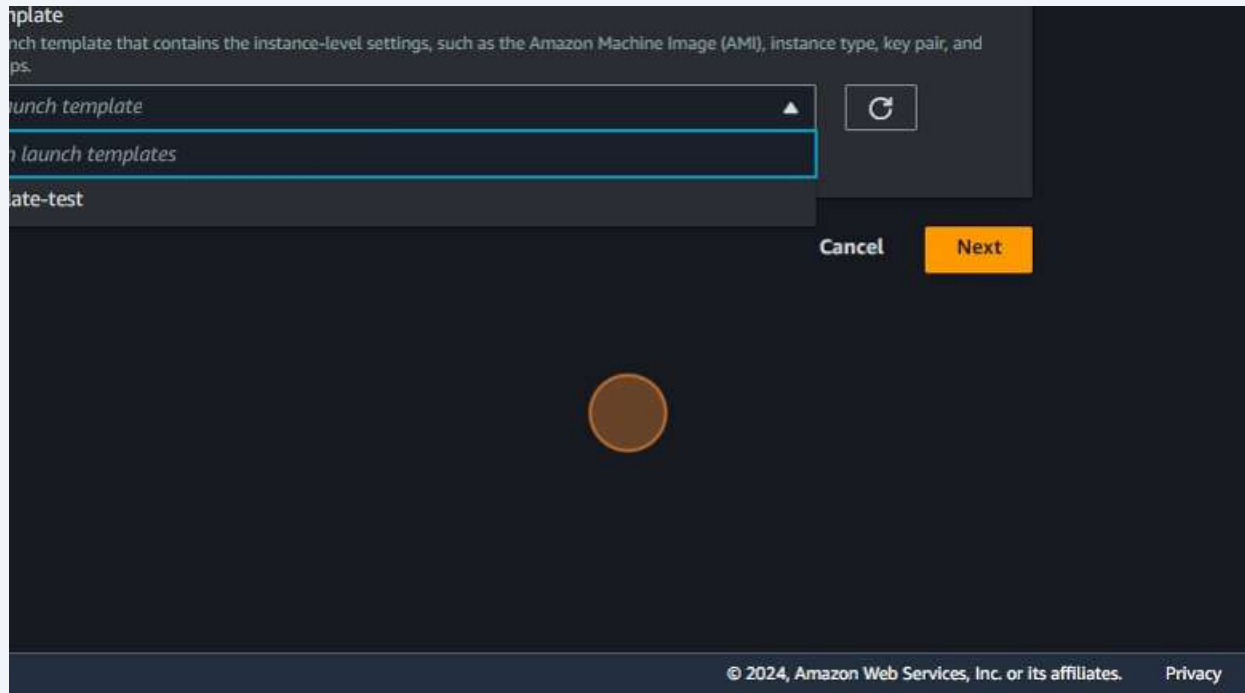
Select a launch template  

[Create a launch template](#) 

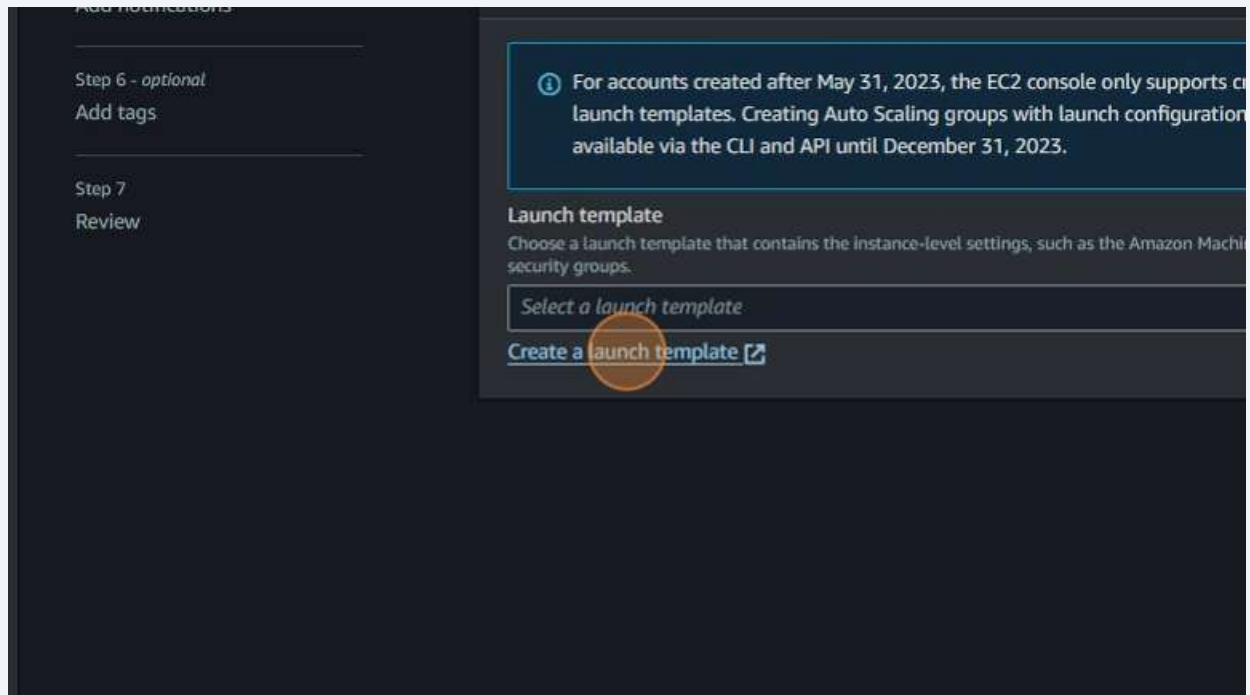
Cancel **Next**

66

Click "EC2
Auto Scaling groups
Create Auto Scaling group
Step 1
Choose launch template
Step 2
Choose instance launch options
Step 3 - optional
Configur..."

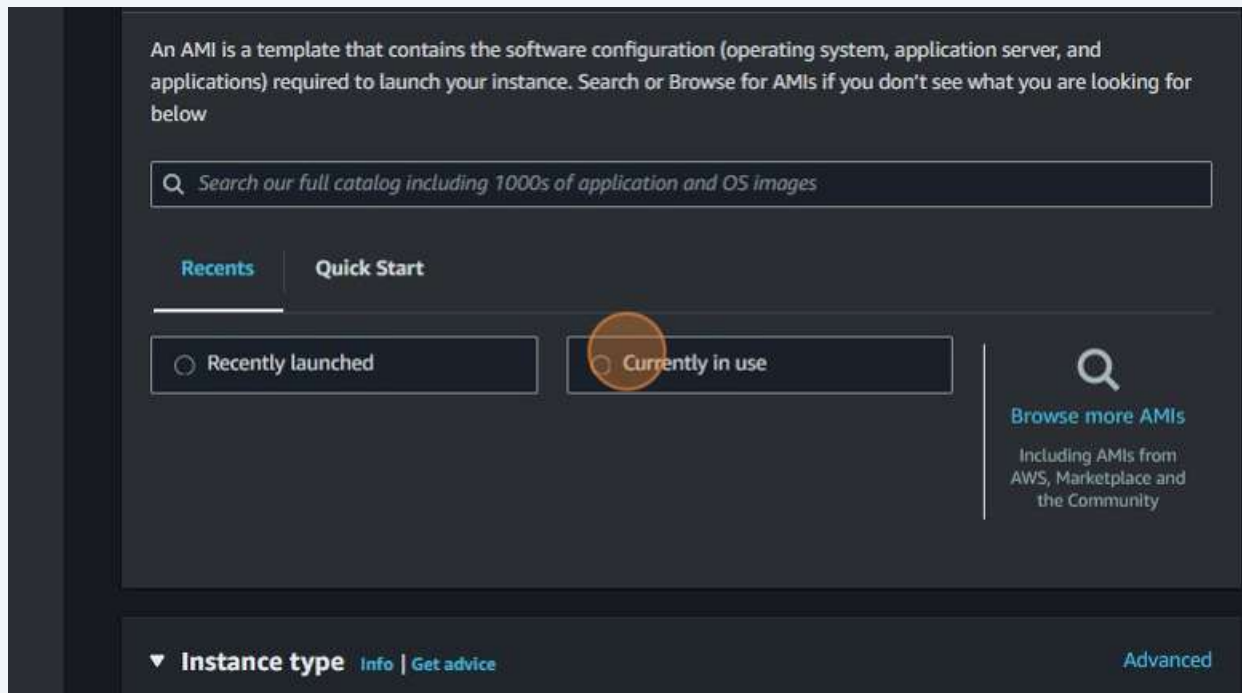


67 Click "Create a launch template"

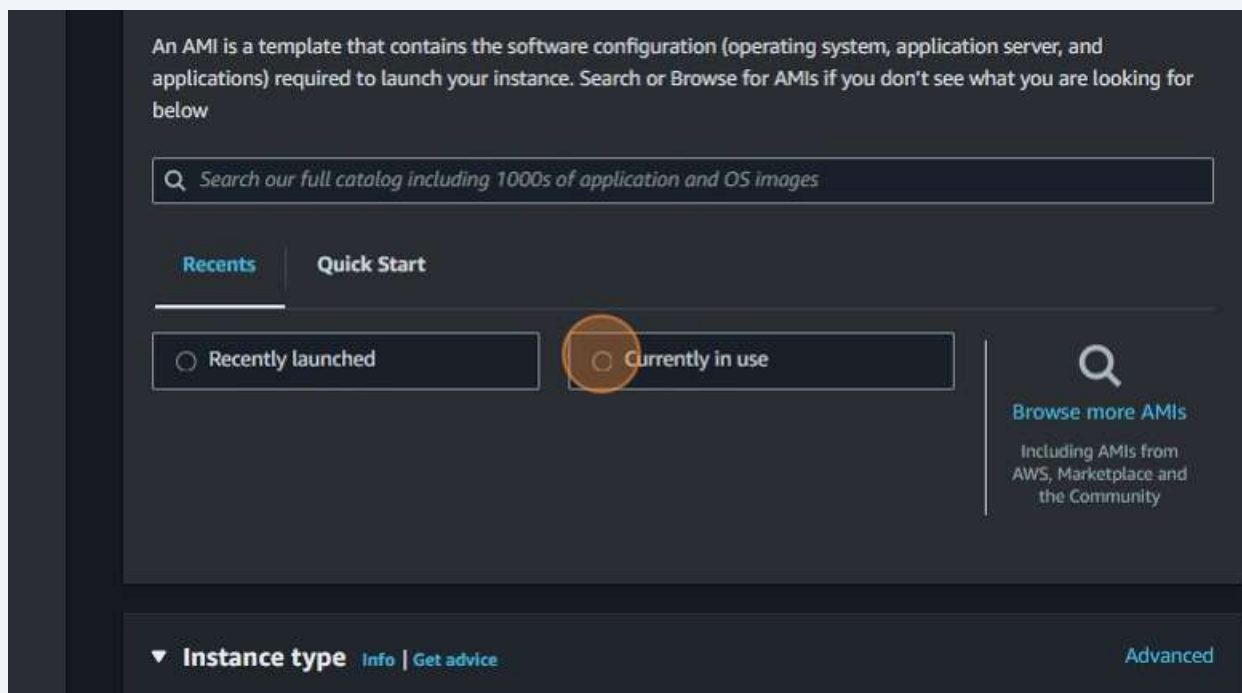


68 Type "template-lit-adv"

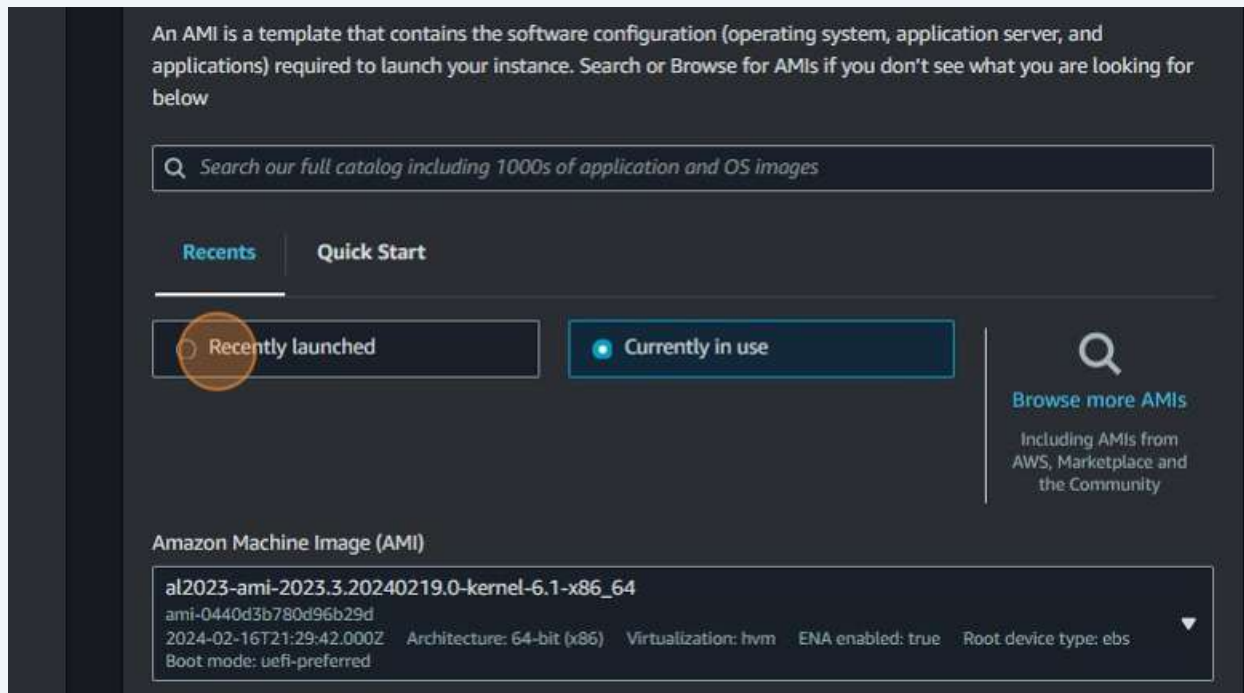
69 Click "Currently in use"



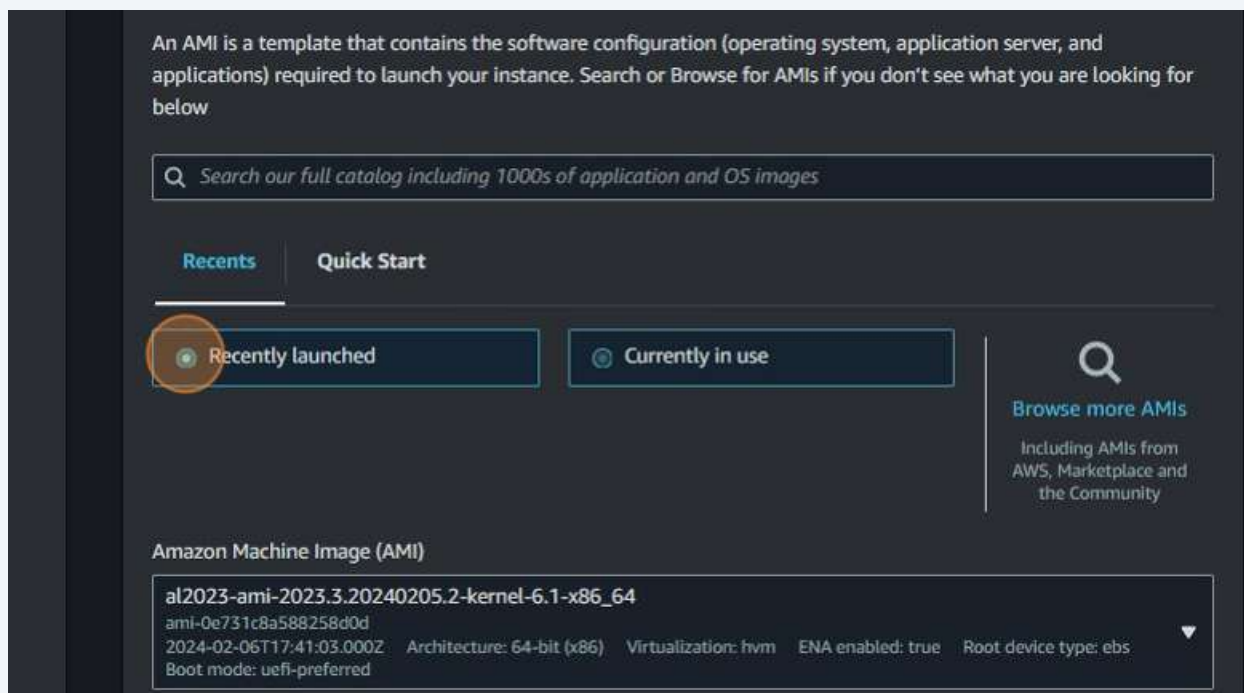
70 Click this radio button.



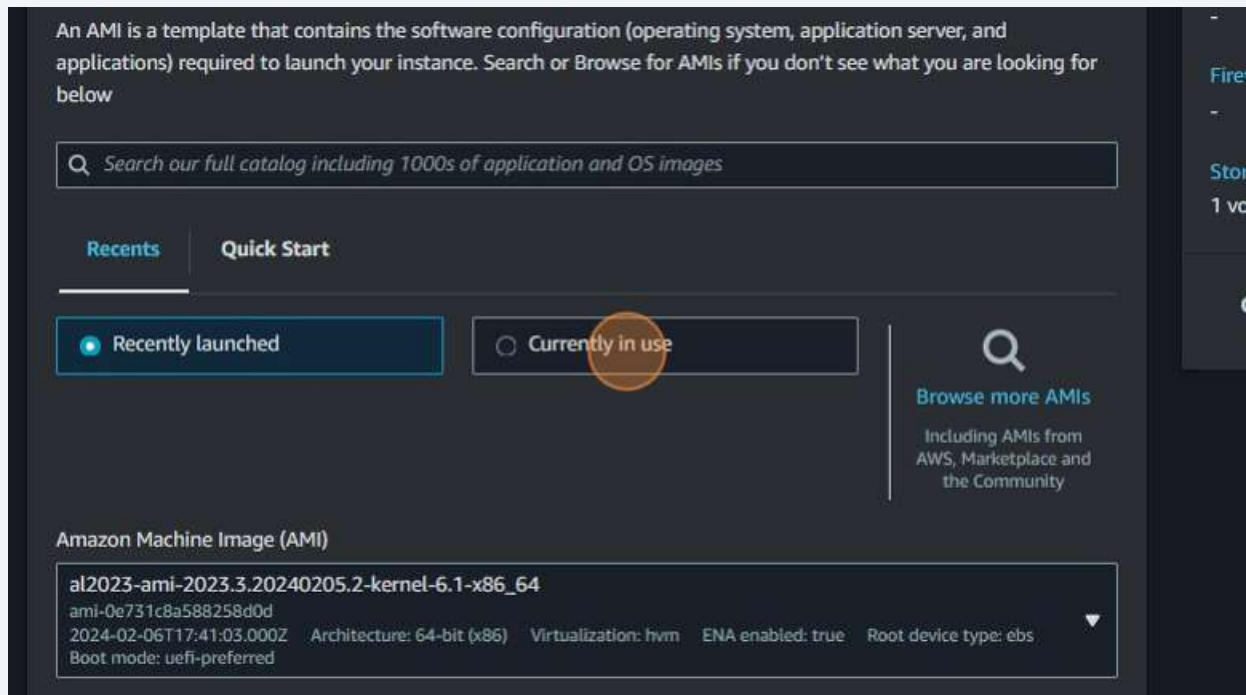
71 Click "Recently launched"



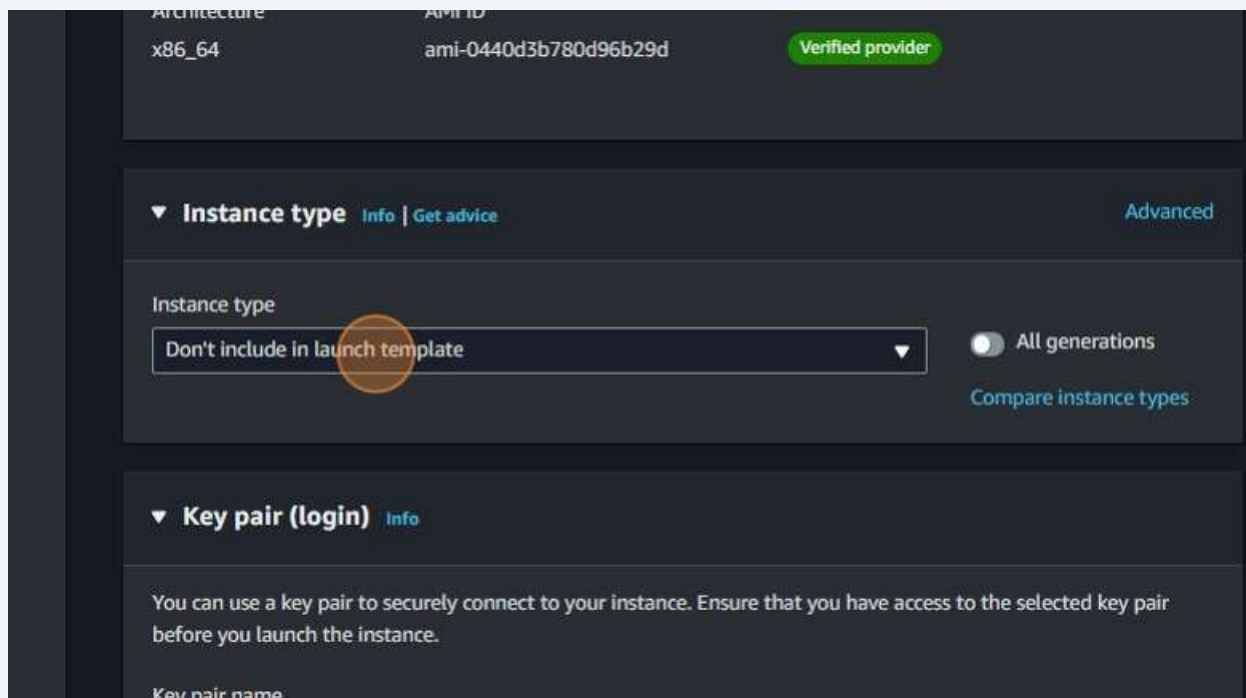
72 Click this radio button.



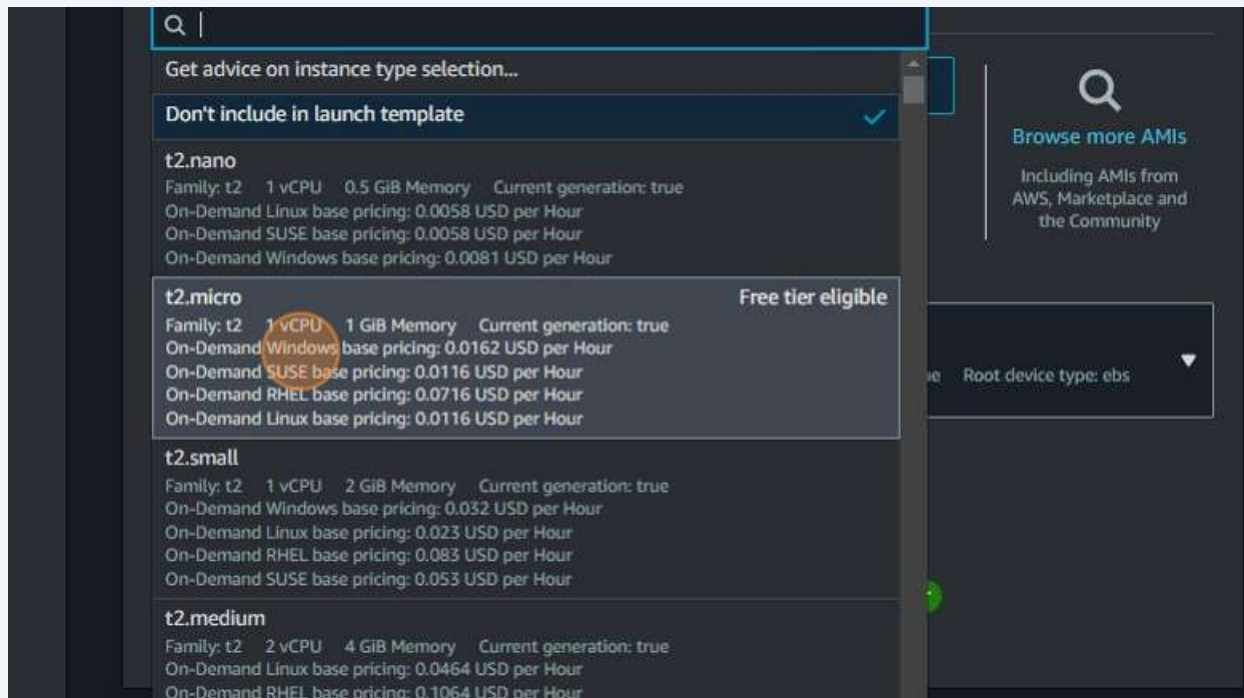
73 Click "Currently in use"



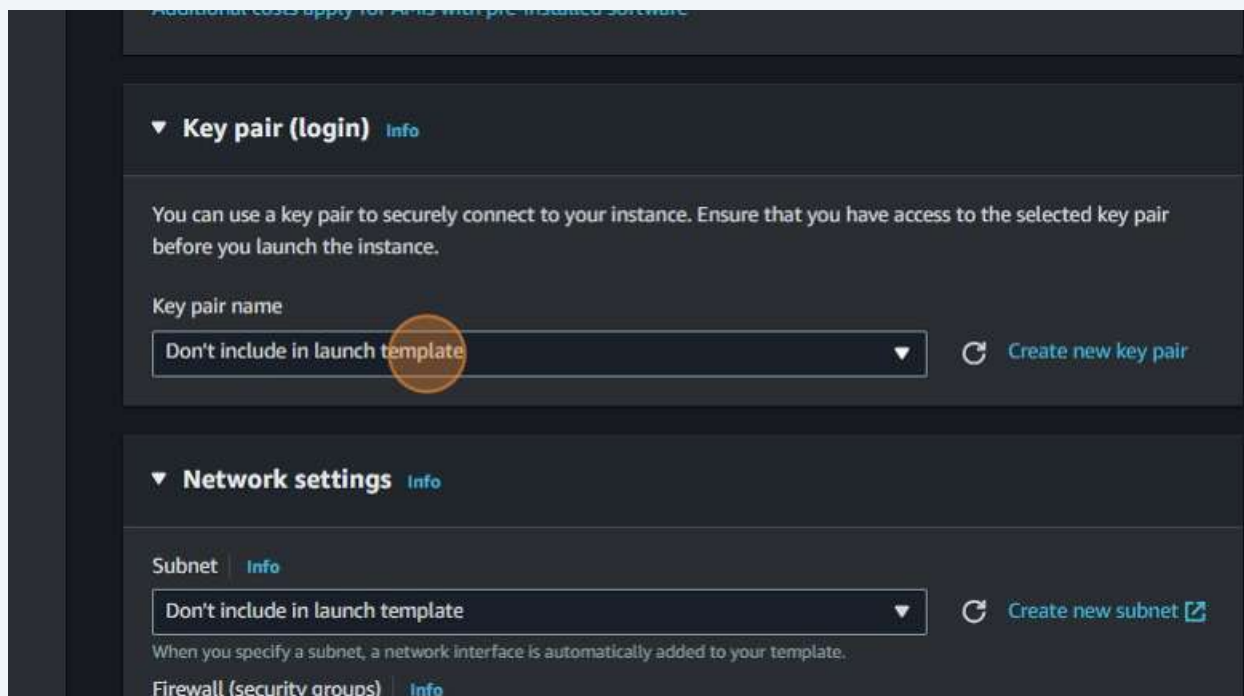
74 Click "Don't include in launch template"



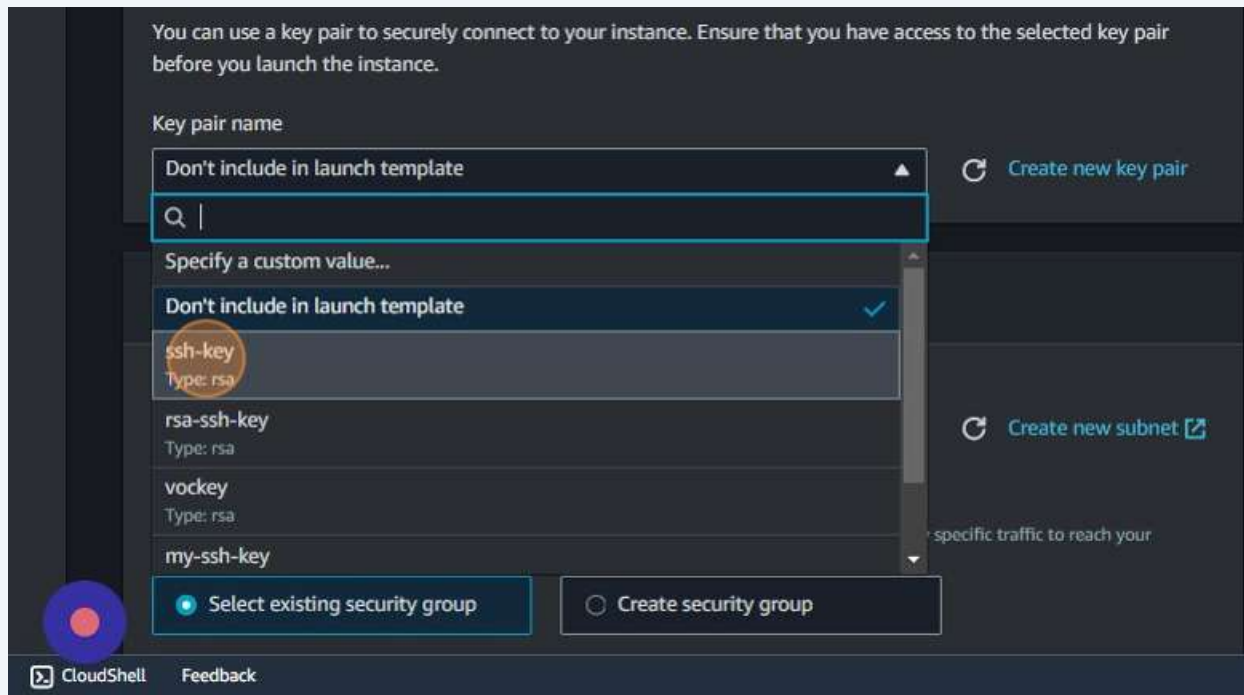
75 Click "On-Demand Windows base pricing: 0.0162 USD per Hour"



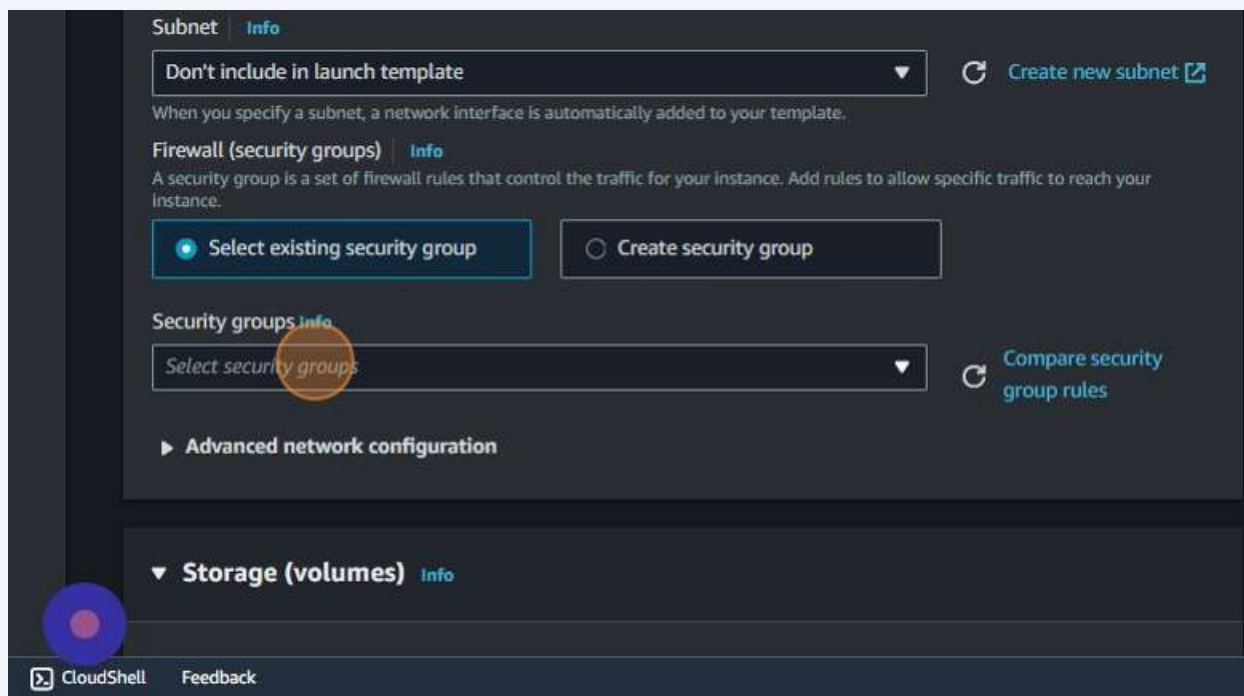
76 Click "Don't include in launch template"



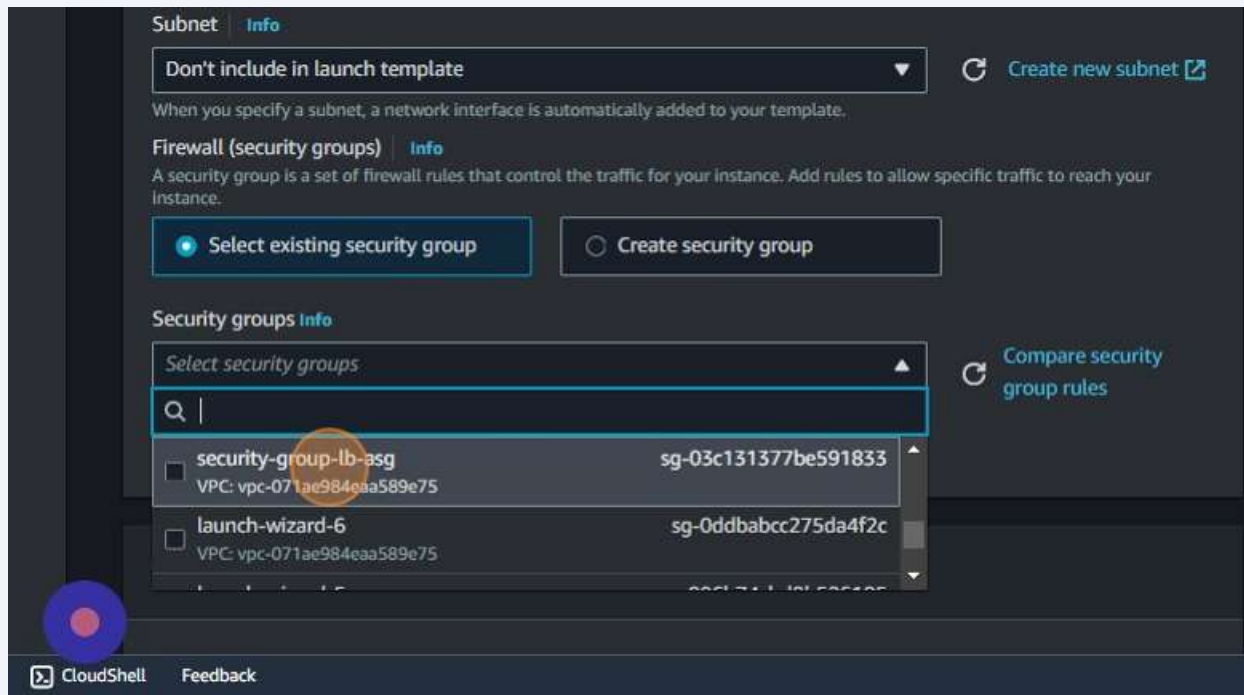
77 Click "ssh-key"



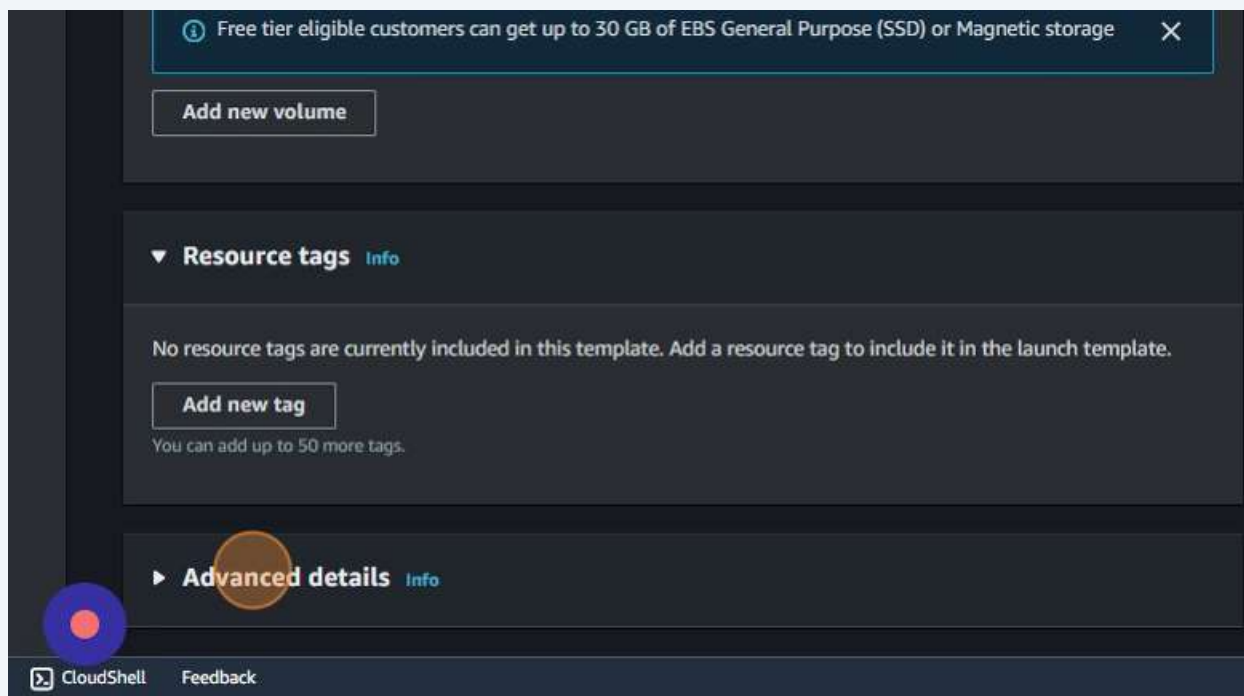
78 Click "Select security groups"



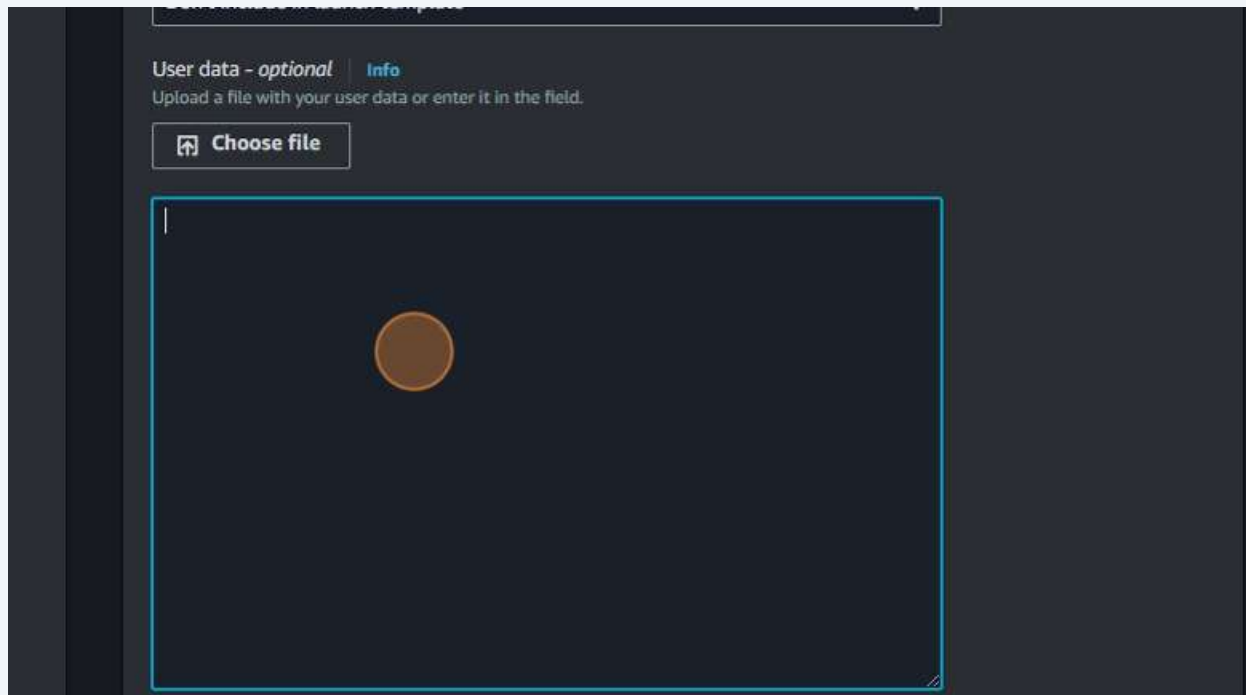
79 Click "security-group-lb-asg"



80 Click "Advanced details"



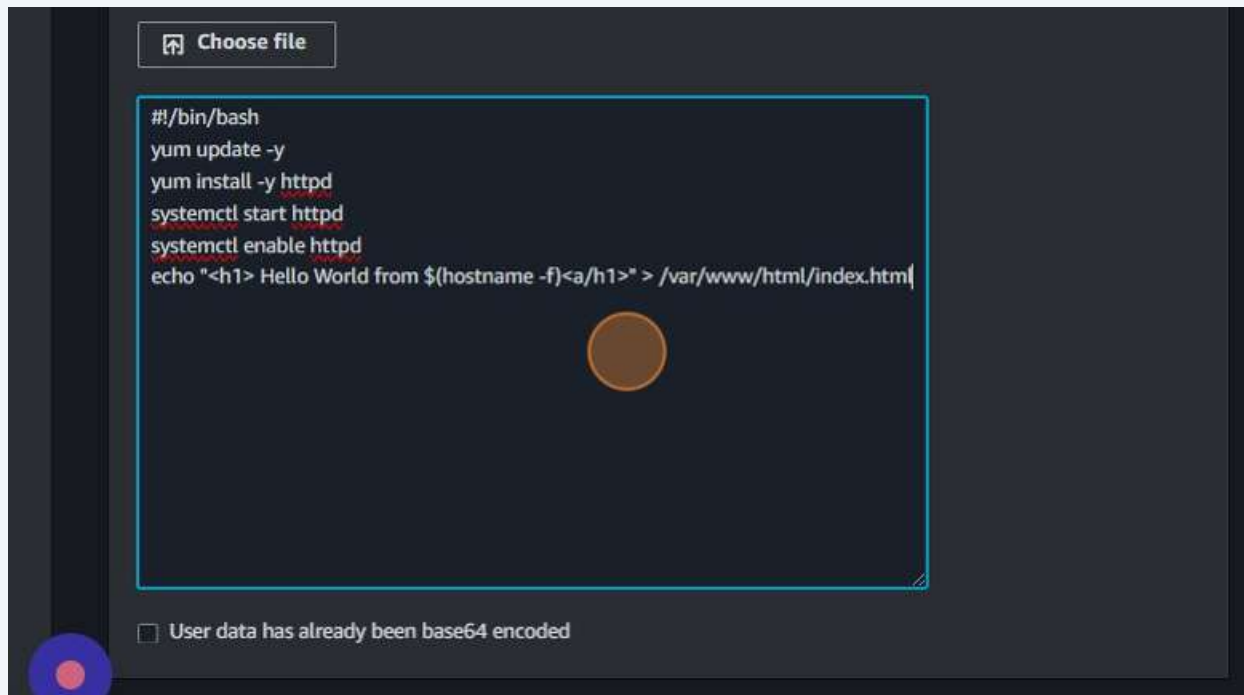
81 Click the "User data - optional" field.



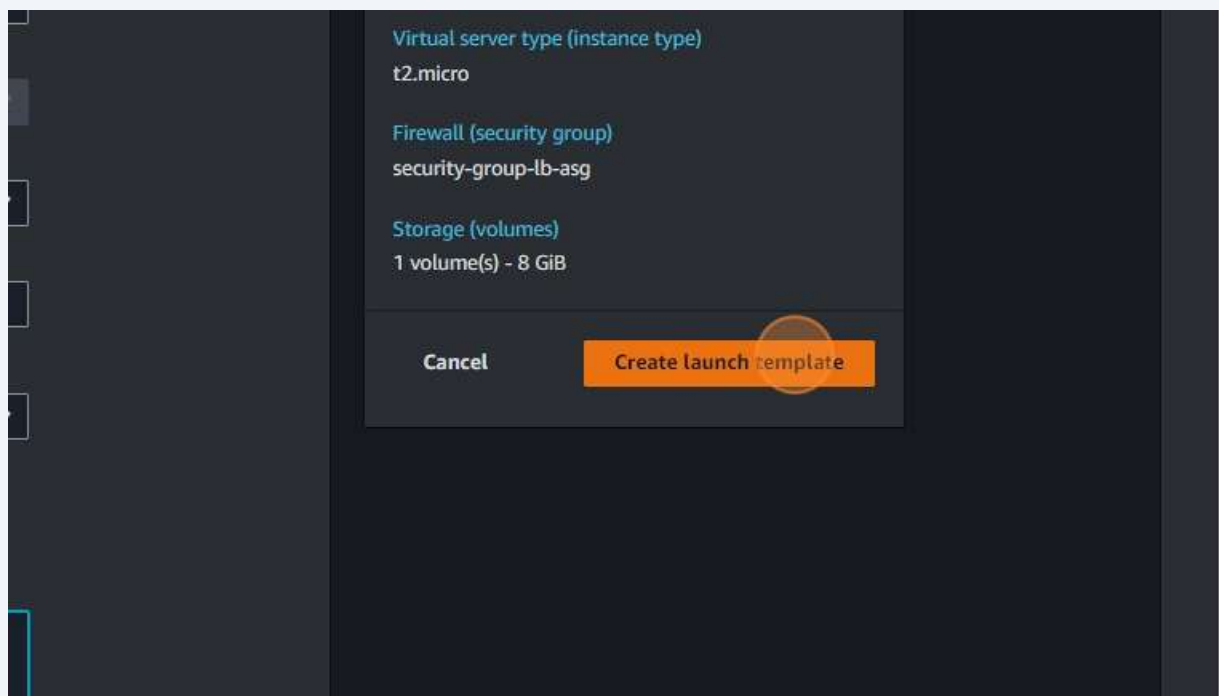
82 Press **ctrl + v**

83 Press **ctrl + v**

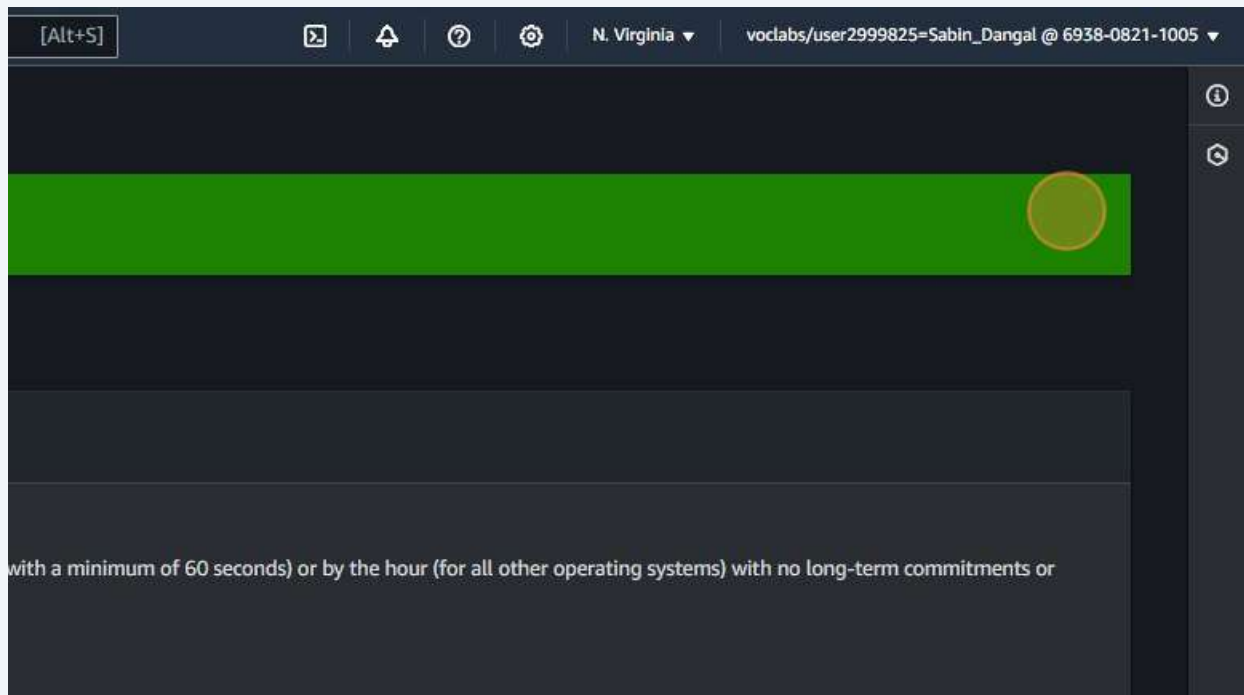
84 Click the "User data - optional" field.



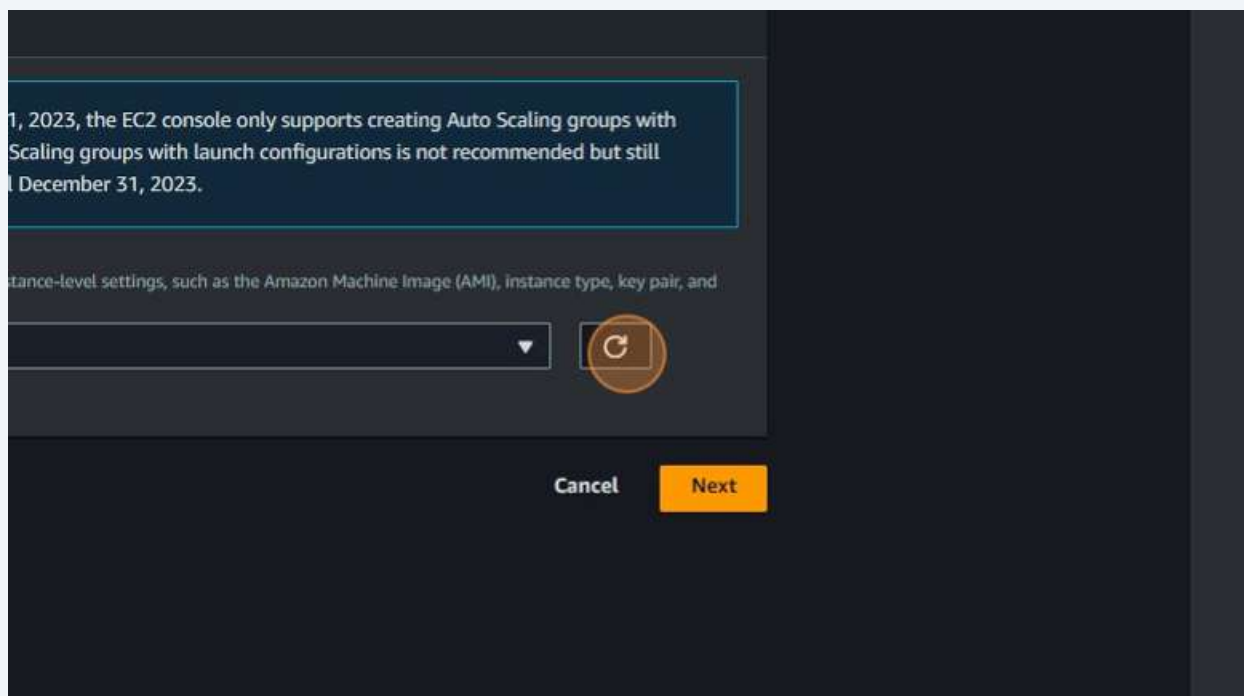
85 Click "Create launch template"



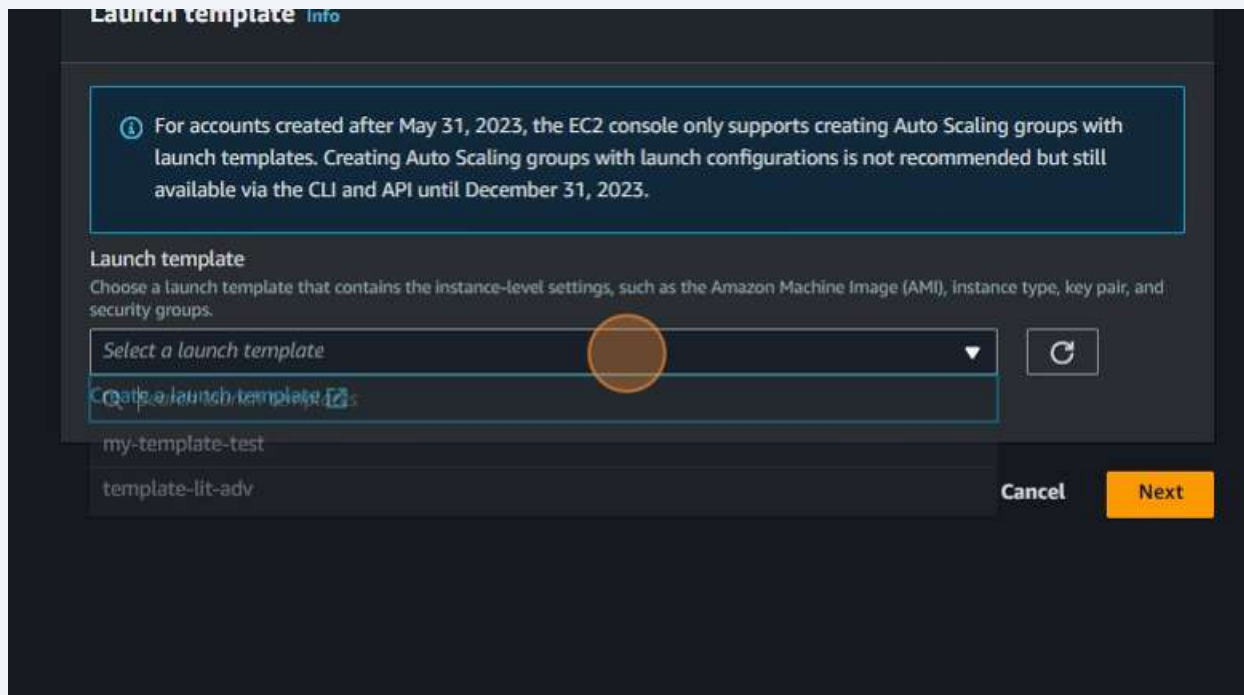
86 Click "Success"



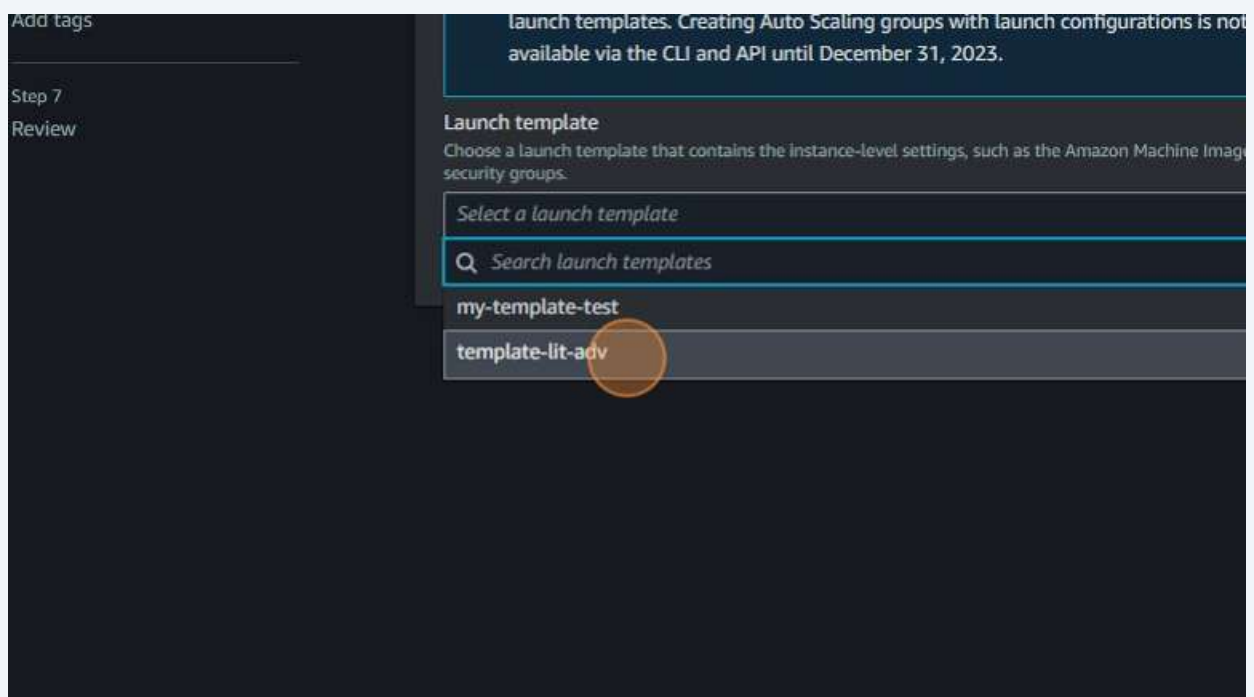
87 Click this button.



88 Click "Select a launch template"



89 Click "template-lit-adv"



90 Click "Default (1)"

Add tags

Step 7
Review

launch templates. Creating Auto Scaling groups with launch configurations is not available via the CLI and API until December 31, 2023.



Launch template

Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image, security groups.


template-lit-adv

Create a launch template [↗](#)

Version

Default (1)  

Create a launch template version [↗](#)

Default (1) 

1

| | | | | |
|---------------|-----------------------|--------------------|------------------------------------|------|
| AMI ID | ami-0440d3b780d96b29d | Launch template | template-lit-adv ↗ | Inst |
| Key pair name | | Security groups | - | t2.r |
| | | Security group IDs | | Req |
| | | | | No |

91 Click "Default (1)"

Add tags

Step 7
Review

launch templates. Creating Auto Scaling groups with launch configurations is not available via the CLI and API until December 31, 2023.



Launch template

Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image, security groups.


template-lit-adv

Create a launch template [↗](#)

Version

Default (1)  

Latest (1) [↗](#)

Default (1) 

1

| | | | | |
|---------------|-----------------------|--------------------|------------------------------------|------|
| AMI ID | ami-0440d3b780d96b29d | Launch template | template-lit-adv ↗ | Inst |
| Key pair name | | Security groups | - | t2.r |
| | | Security group IDs | | Req |
| | | | | No |

92 Click "Next"

Launch template
template-lit-adv [link](#)
lt-0de1446fec168bc64

Security groups
-

Security group IDs
sg-03c131377be591833 [link](#)

Instance type
t2.micro

Request Spot Instances
No

Date created
Wed Feb 21 2024 00:46:42
GMT+0545 (Nepal Time)

Cancel Next

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

93 Click "172.31.0.0/16 Default"

Network [Info](#)

For most applications, you can use multiple Availability Zones and let EC2 Auto Scaling balance your instances across the zones. The default VPC and default subnets are suitable for getting started quickly.

VPC
Choose the VPC that defines the virtual network for your Auto Scaling group.

vpc-071ae984eaa589e75
172.31.0.0/16 Default

[Create a VPC](#)

vpc-071ae984eaa589e75
172.31.0.0/16 Default

Availability Zones and subnets
Define which Availability Zones and subnets your Auto Scaling group can use in the chosen VPC.

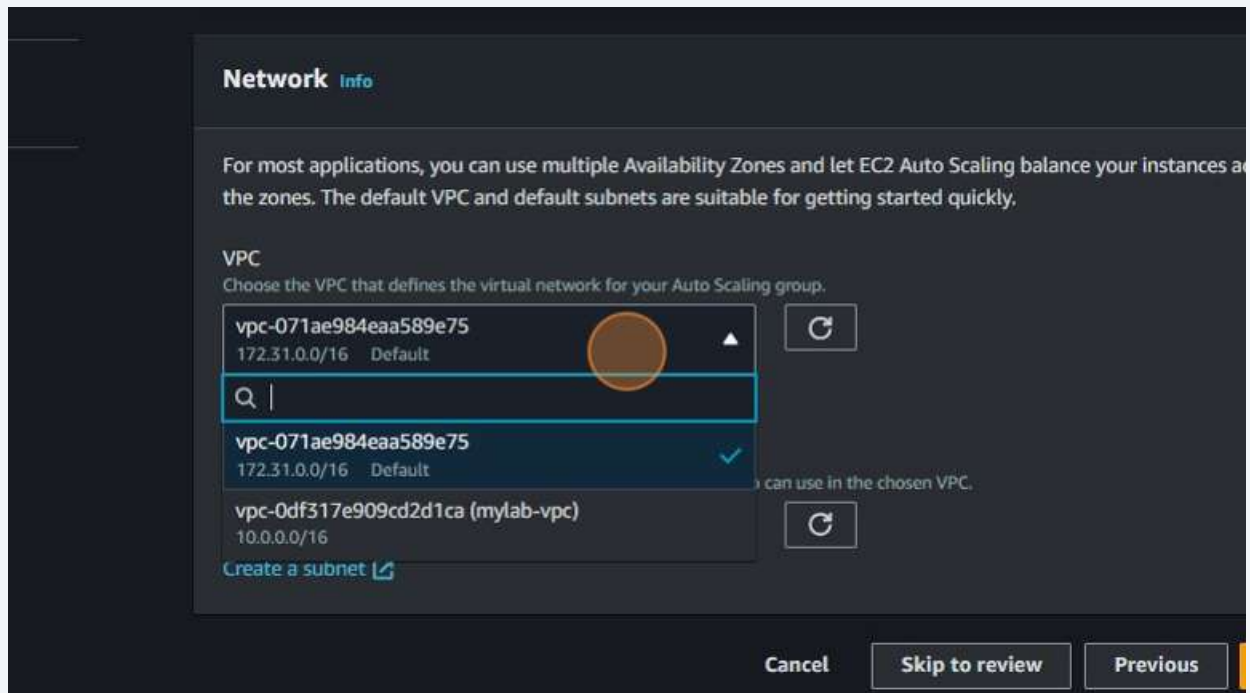
vpc-0df317e9109cd2d1ca (mylab-vpc)
10.0.0.0/16

[Create a subnet](#)

Cancel Skip to review Previous

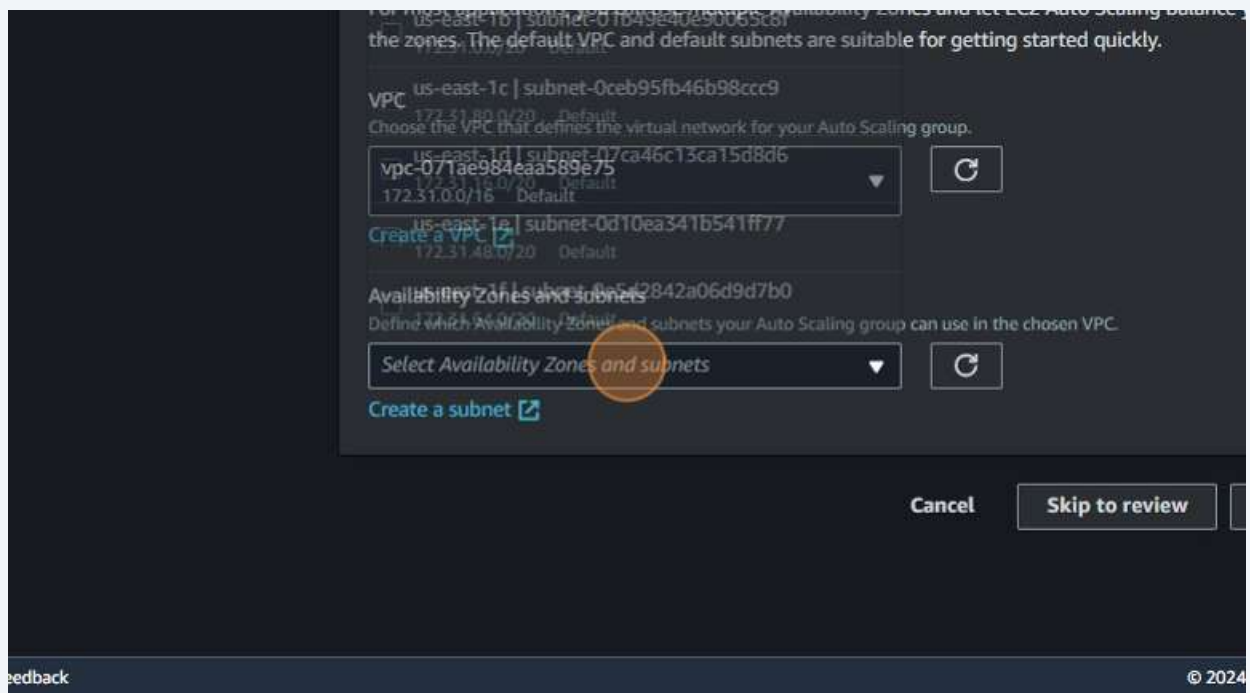
94

Click "172.31.0.0/16
Default"

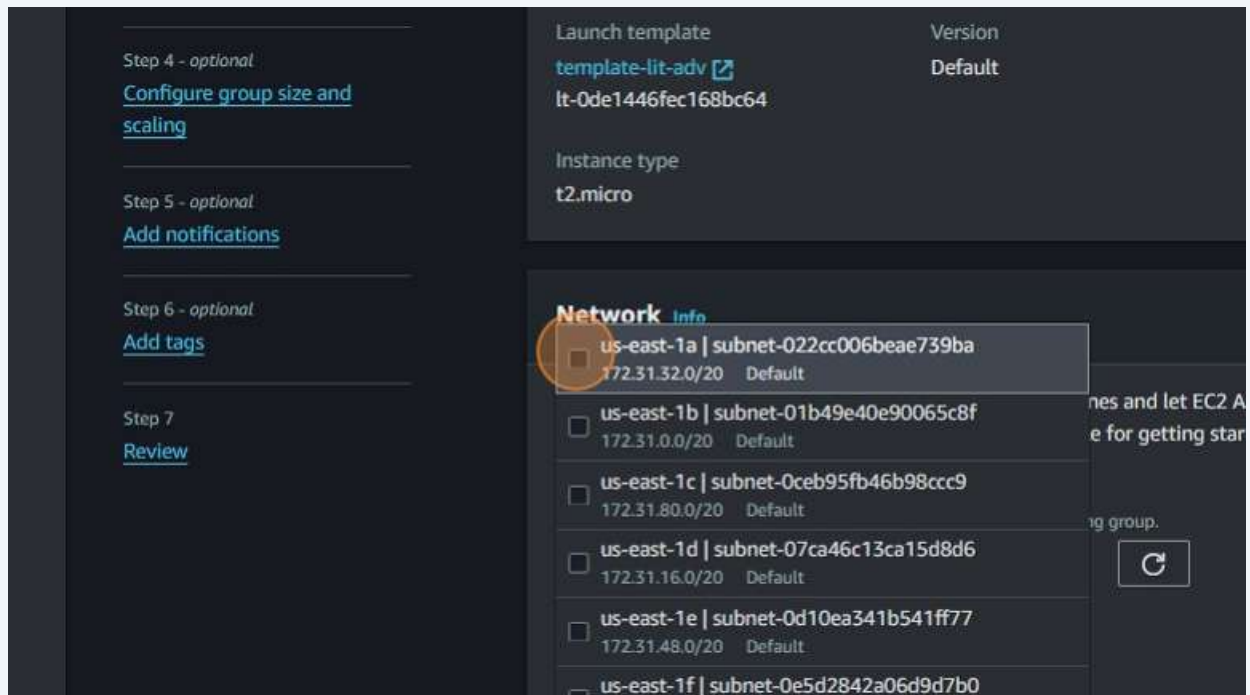


95

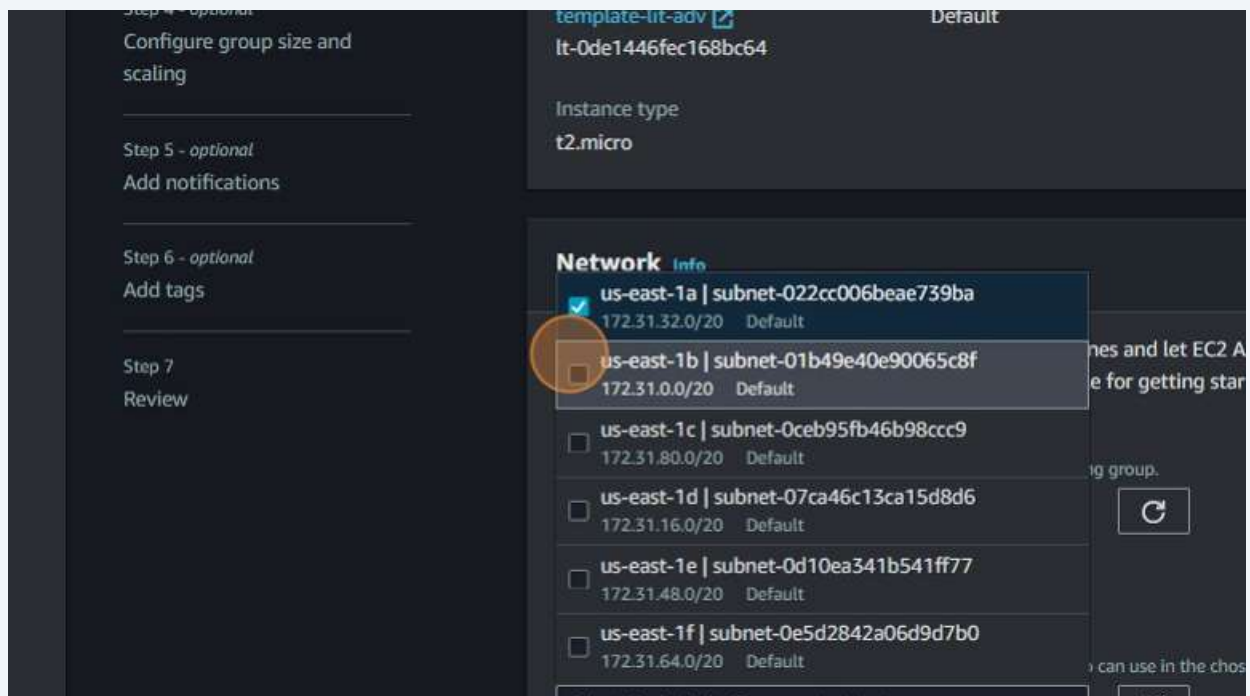
Click "Select Availability Zones and subnets"



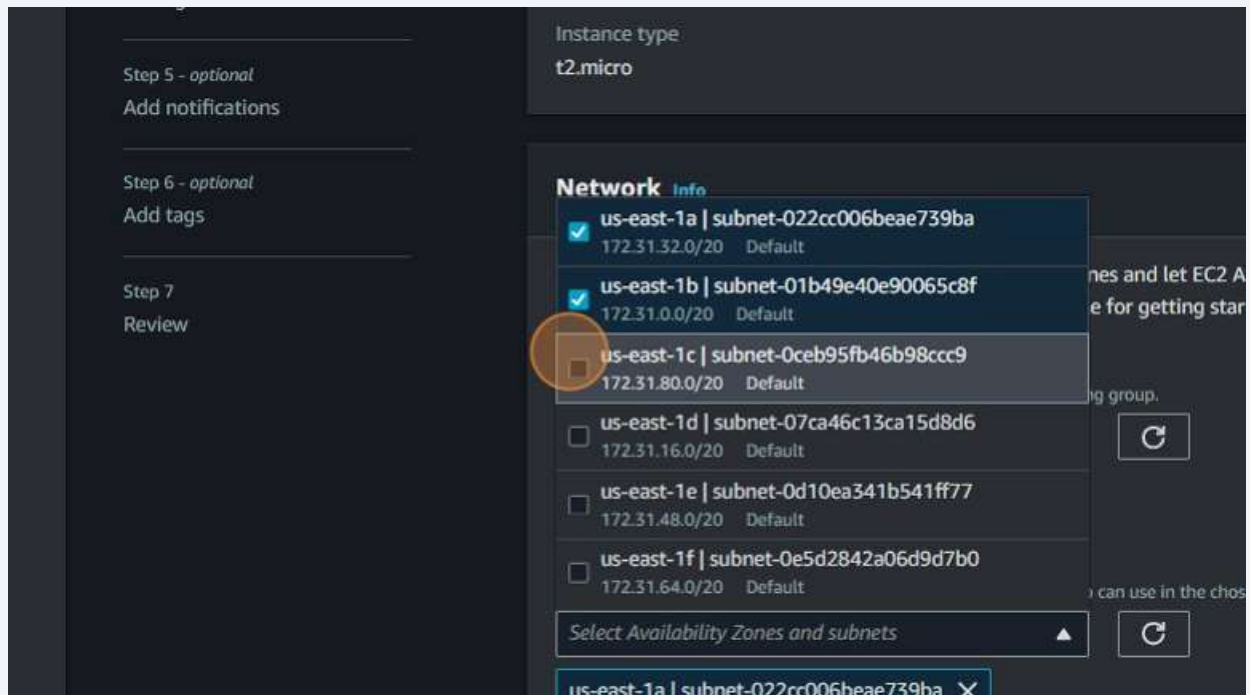
96 Click here.



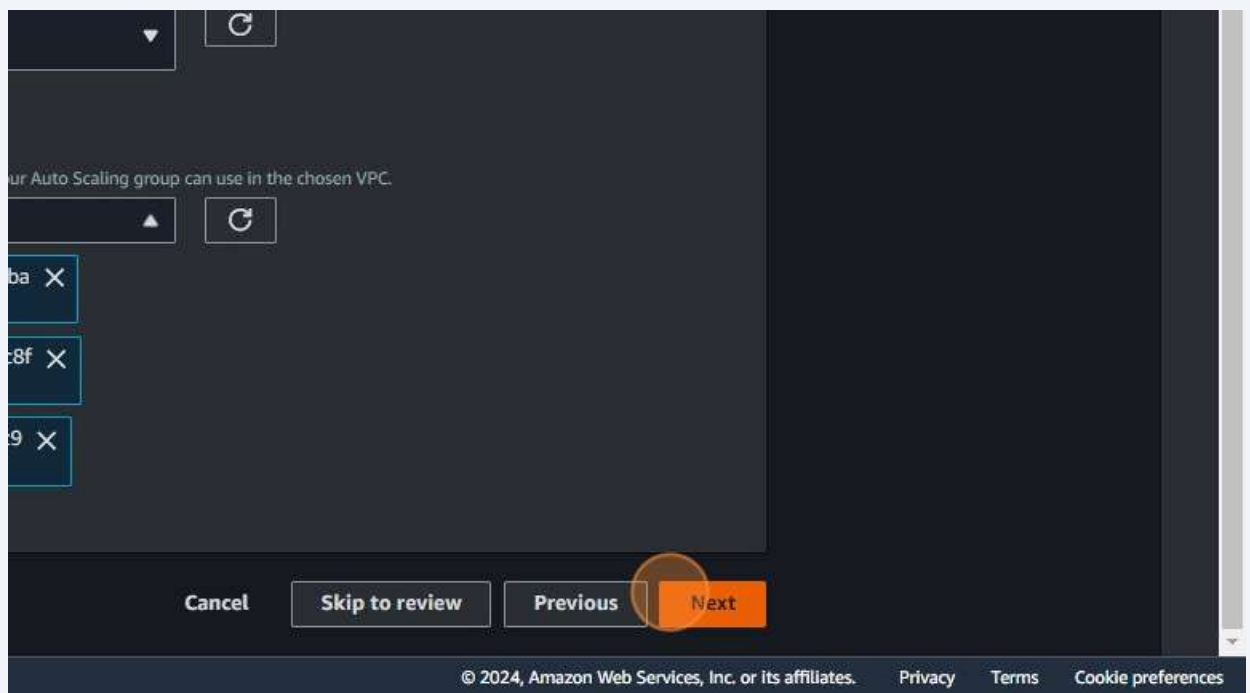
97 Click here.



98 Click here.



99 Click "Next"



100 Click "Attach to an existing load balancer"

Integrate your Auto Scaling group with other services to distribute network traffic across multiple servers using a load balancer or to establish service-to-service communications using VPC Lattice. You can also set options that give you more control over health check replacements and monitoring.

Load balancing [Info](#)

Use the options below to attach your Auto Scaling group to an existing load balancer, or to a new load balancer that you define.

☒ No load balancer

Traffic to your Auto Scaling group will not be fronted by a load balancer.

☐ Attach to an existing load balancer

Choose from your existing load balancers.

☐ Attach to a new load balancer

Quickly create a basic load balancer to attach to your Auto Scaling group.

VPC Lattice integration options [Info](#)

To improve networking capabilities and scalability, integrate your Auto Scaling group with VPC Lattice. VPC Lattice facilitates communications between AWS services and helps you connect and manage your applications across compute services in AWS.

101 Click "Select target groups"

Step 6 - optional

[Add tags](#)

Step 7

[Review](#)

Attach to an existing load balancer

Select the load balancers that you want to attach to your Auto Scaling group.

☒ Choose from your load balancer target groups

This option allows you to attach Application, Network, or Gateway Load Balancers.

☐ Choose from Classic

Existing load balancer target groups

Only instance target groups that belong to the same VPC as your Auto Scaling group are available for

[Select target groups](#)

VPC Lattice integration options [Info](#)

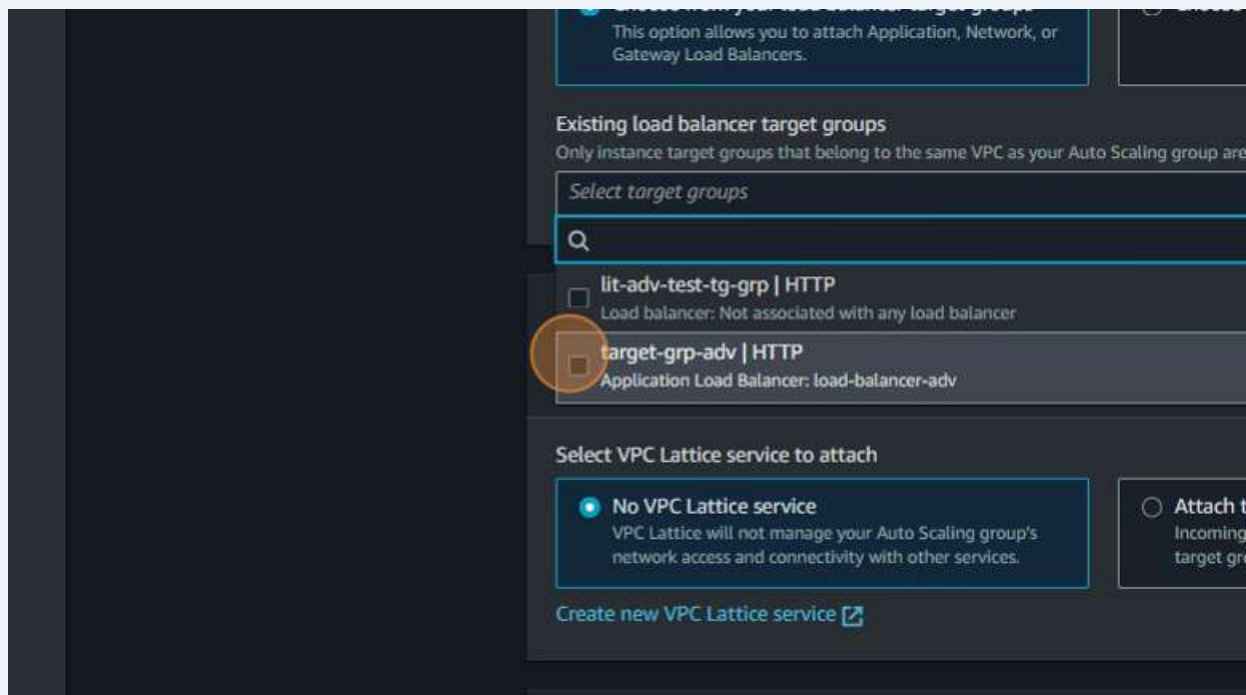
To improve networking capabilities and scalability, integrate your Auto Scaling group with VPC Lattice. VPC Lattice facilitates communications between AWS services and helps you connect and manage your applications across compute services in AWS.

Select VPC Lattice service to attach

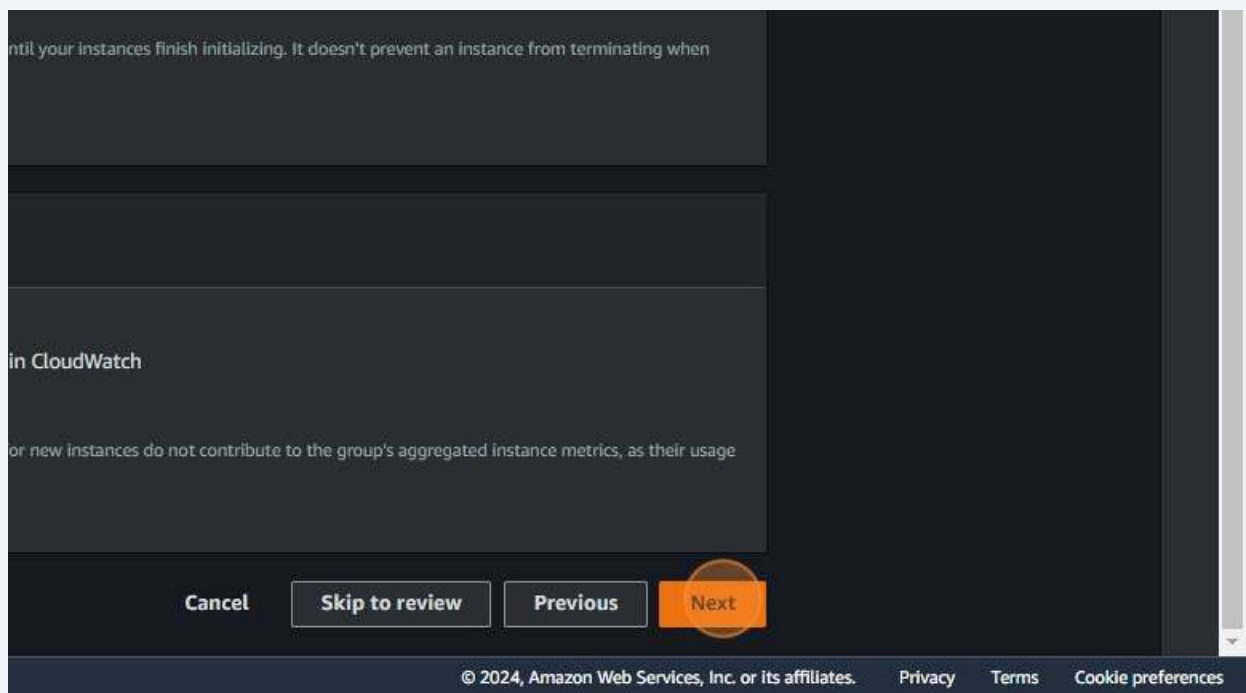
☒ No VPC Lattice service

☐ Attach to VPC Lattice

102 Click here.



103 Click "Next"



104 Click the "Max desired capacity" field.

The screenshot shows the AWS Auto Scaling console interface. The 'Scaling' tab is selected, and the 'Scaling limits' section is visible. The 'Max desired capacity' field is highlighted with a red circle. The 'Automatic scaling - optional' section is also visible, showing two options: 'No scaling policies' (selected) and 'Target tracking scaling policy'.

Scaling [Info](#)
You can resize your Auto Scaling group manually or automatically to meet changes in demand.

Scaling limits
Set limits on how much your desired capacity can be increased or decreased.

Min desired capacity
1
Equal or less than desired capacity

Max desired capacity
1
Equal or greater than desired capacity

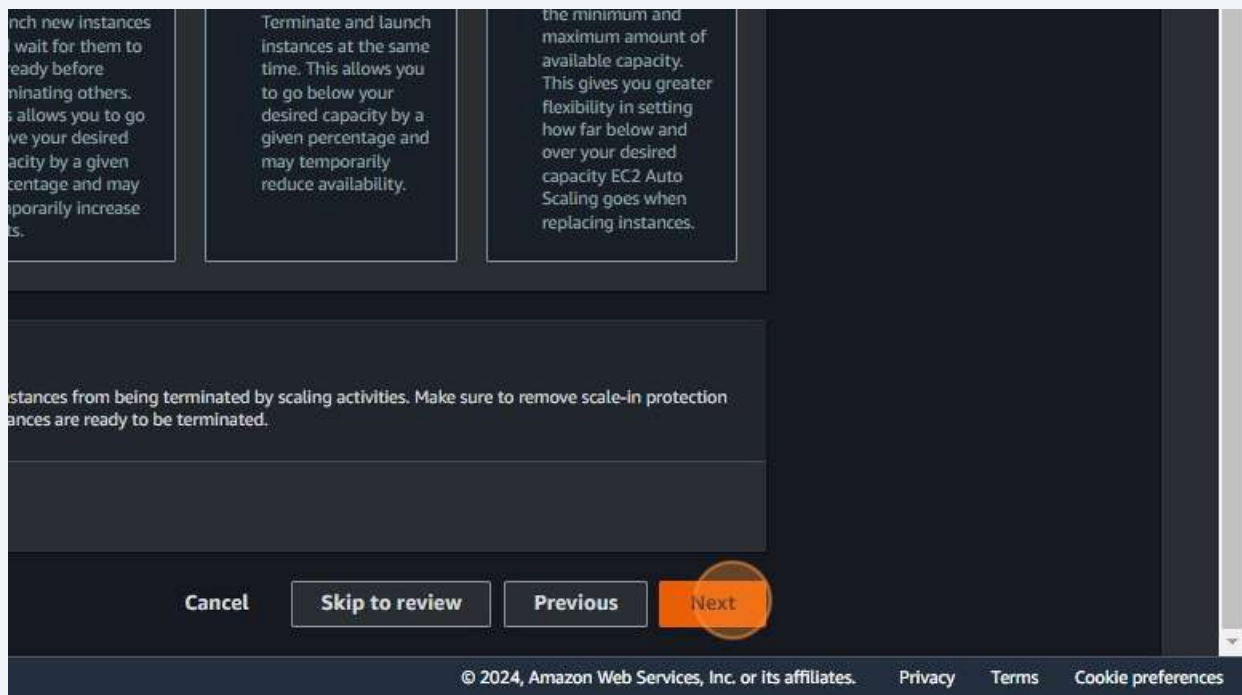
Automatic scaling - optional
Choose whether to use a target tracking policy [Info](#)
You can set up other metric-based scaling policies and scheduled scaling after creating your Auto Scaling group.

☒ **No scaling policies**
Your Auto Scaling group will remain at its initial size and will not dynamically resize to meet demand.

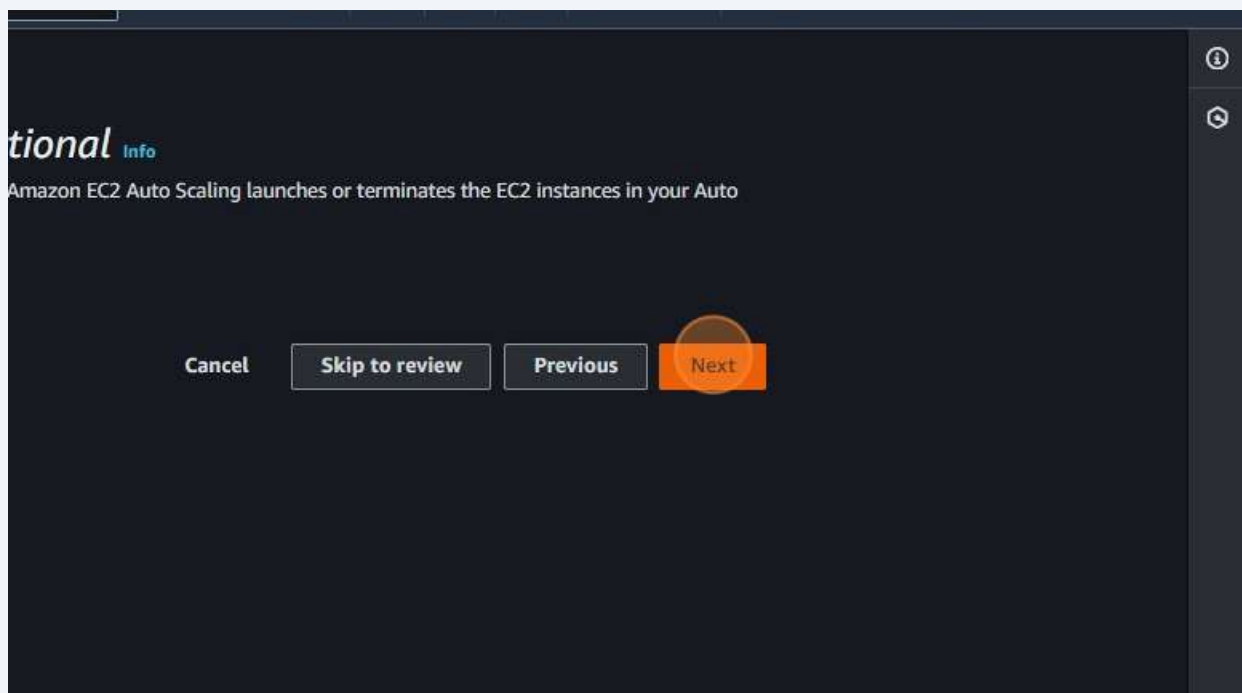
☐ **Target tracking scaling policy**
Choose a CloudWatch metric and target scaling policy adjust the desired capacity the metric's value.

105 Type " **Backspace 4**"

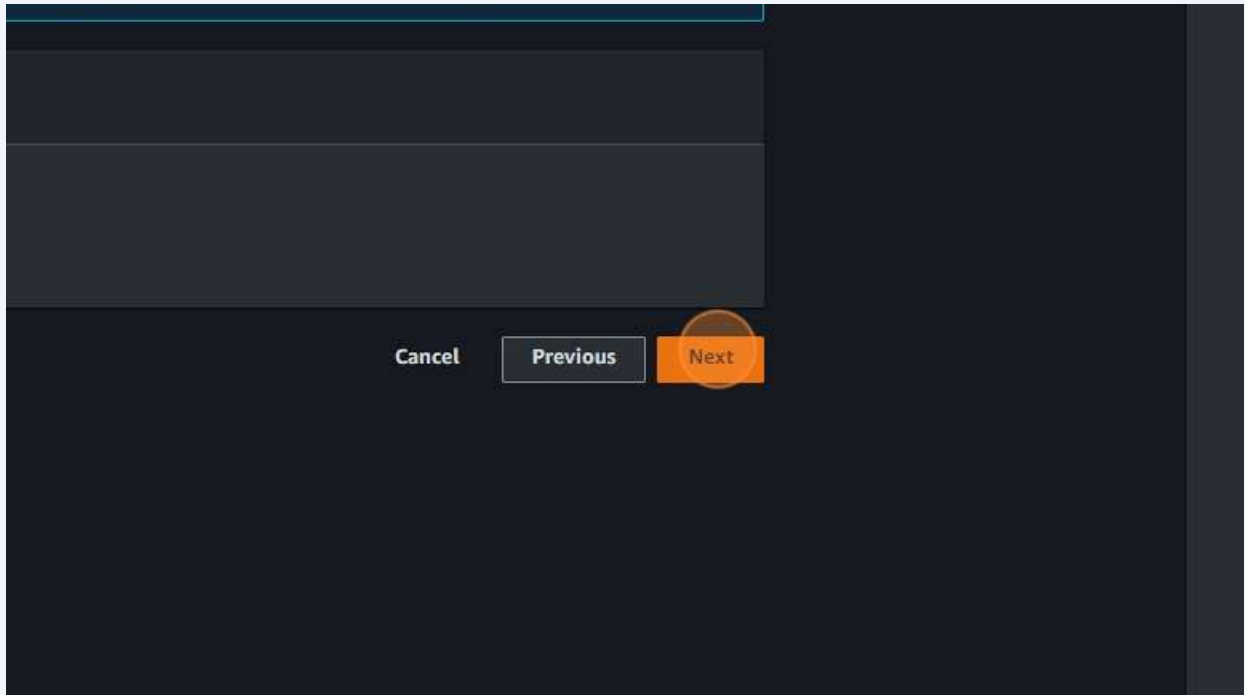
106 Click "Next"



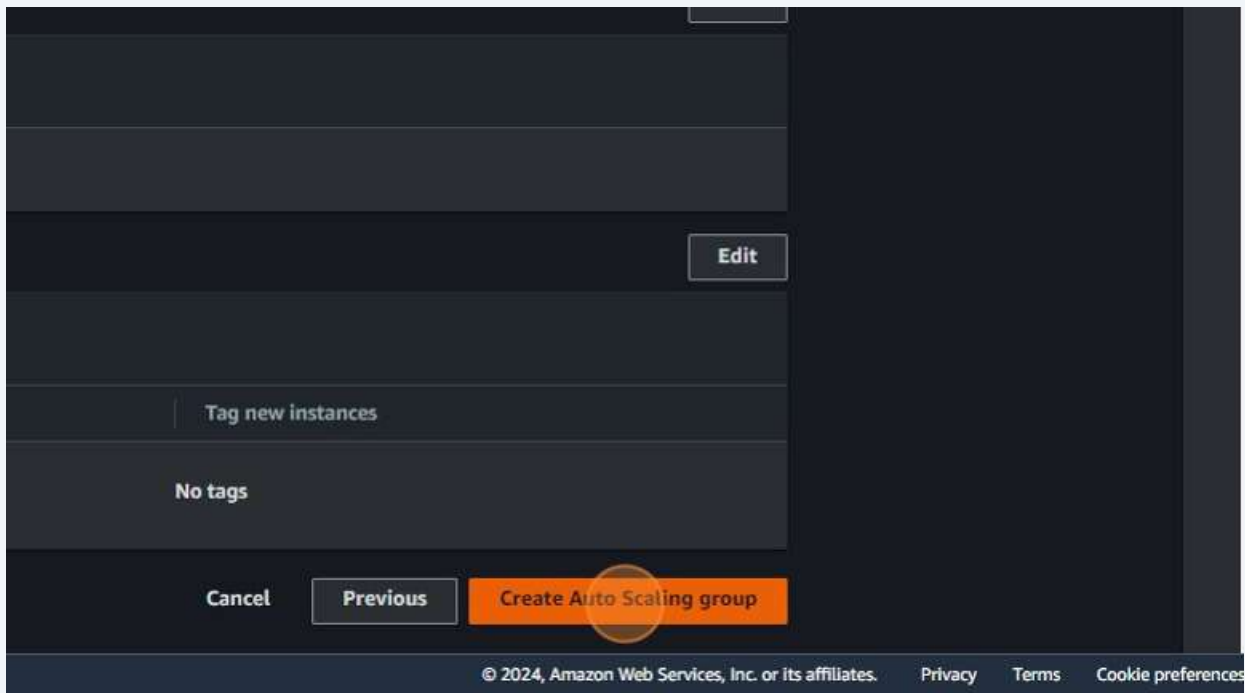
107 Click "Next"



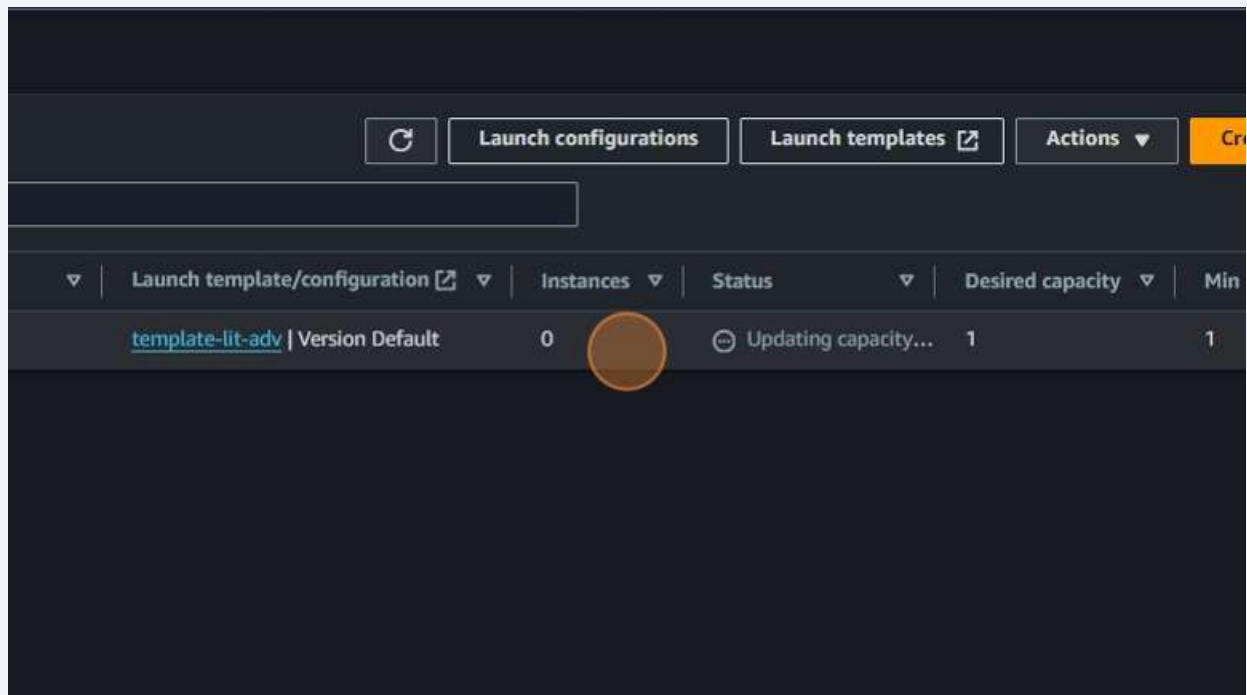
108 Click "Next"



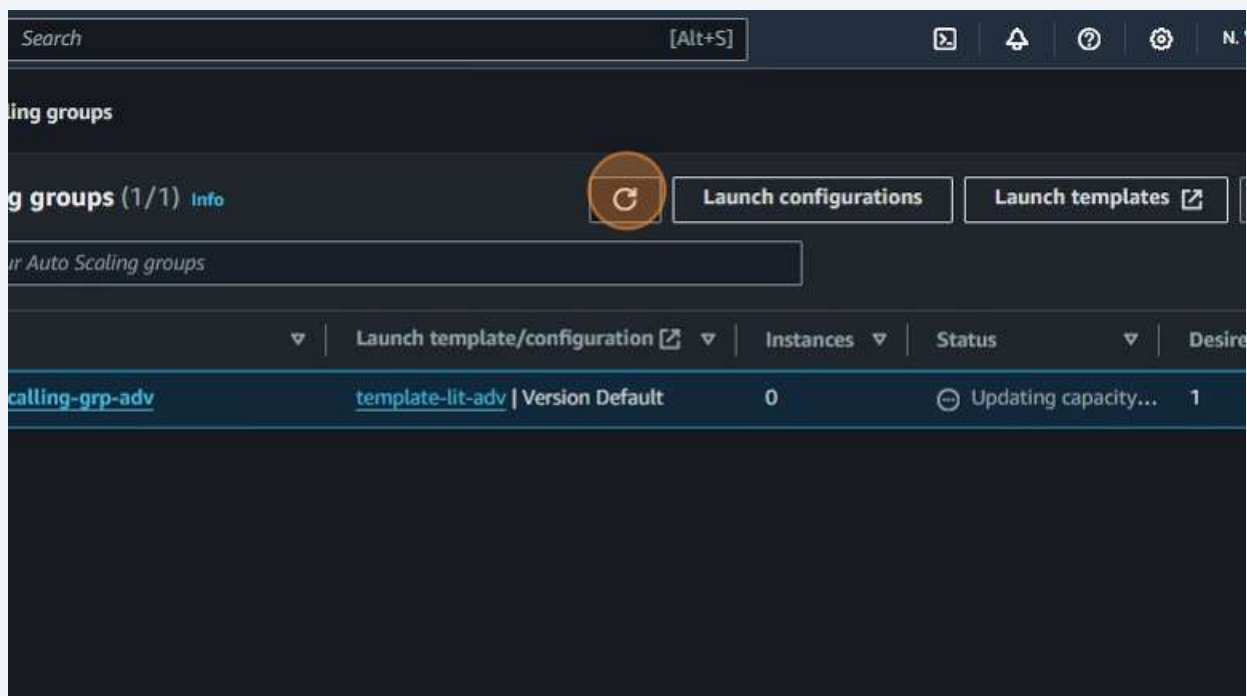
109 Click "Create Auto Scaling group"



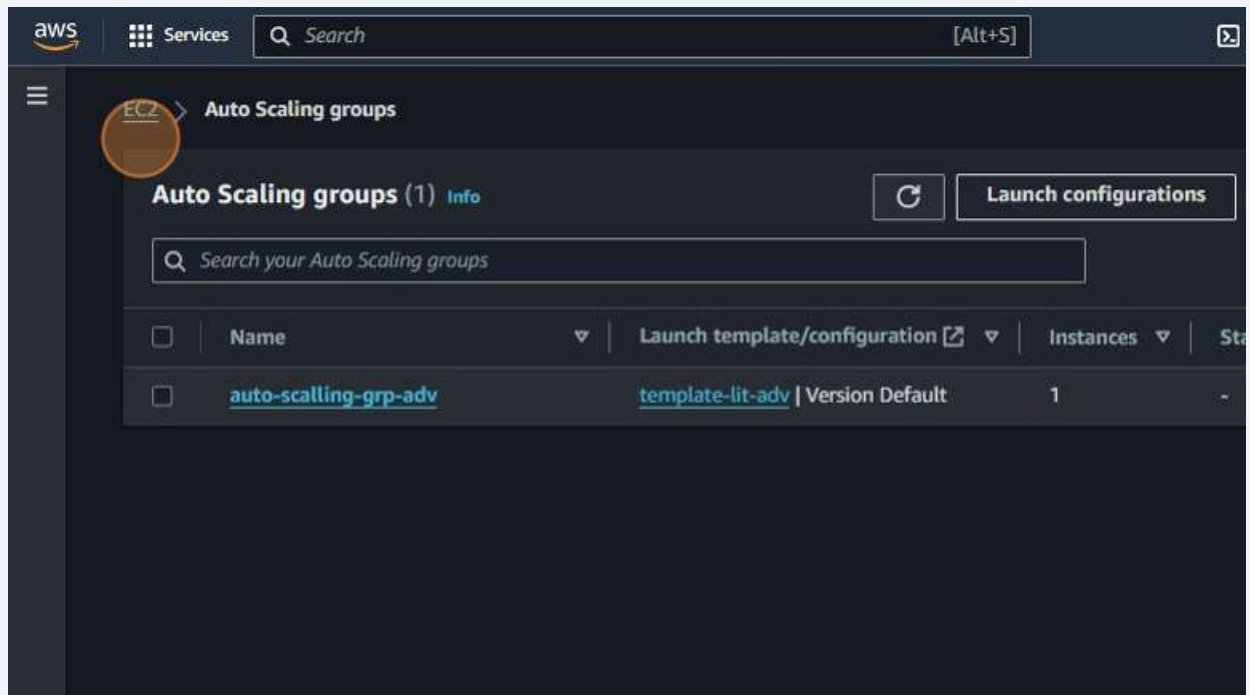
110 Click "0"



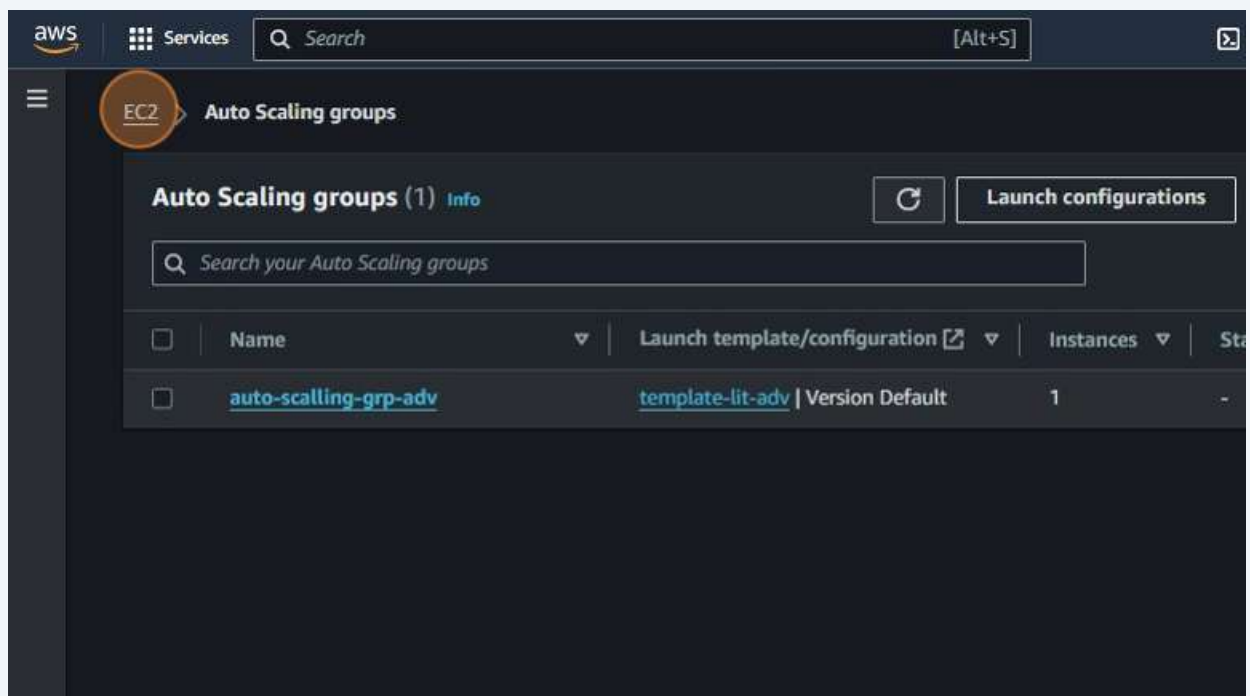
111 Click here.



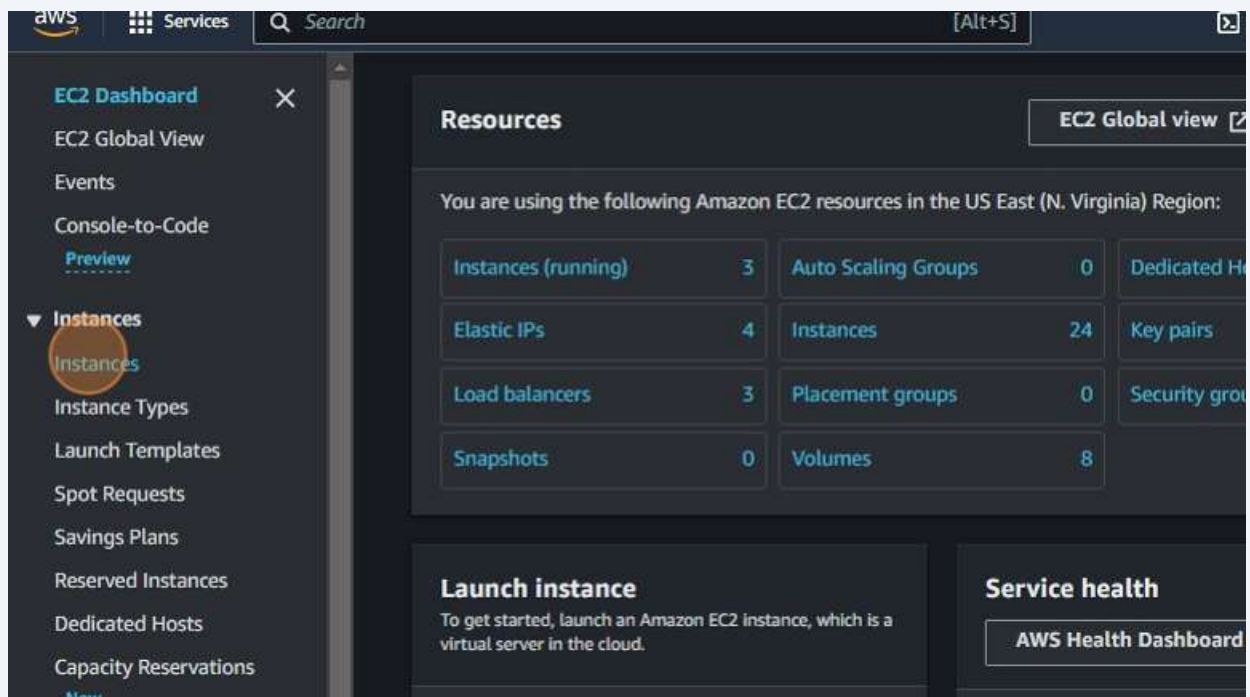
112 Click here.



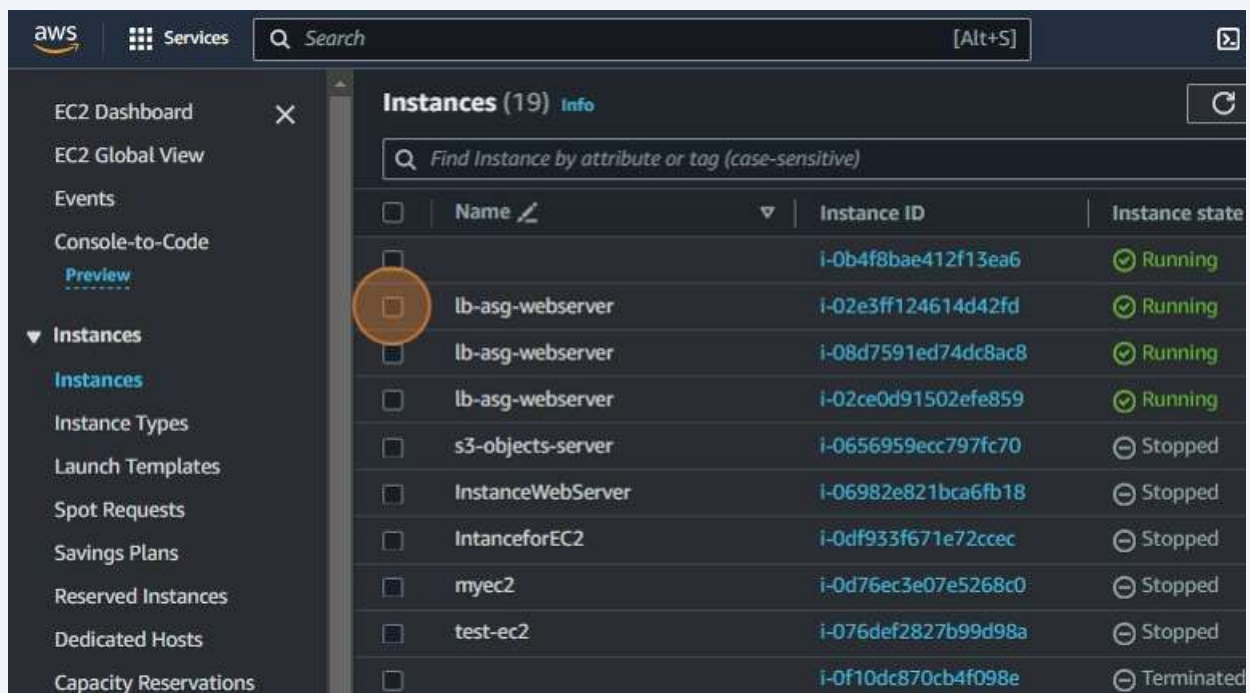
113 Click "EC2"



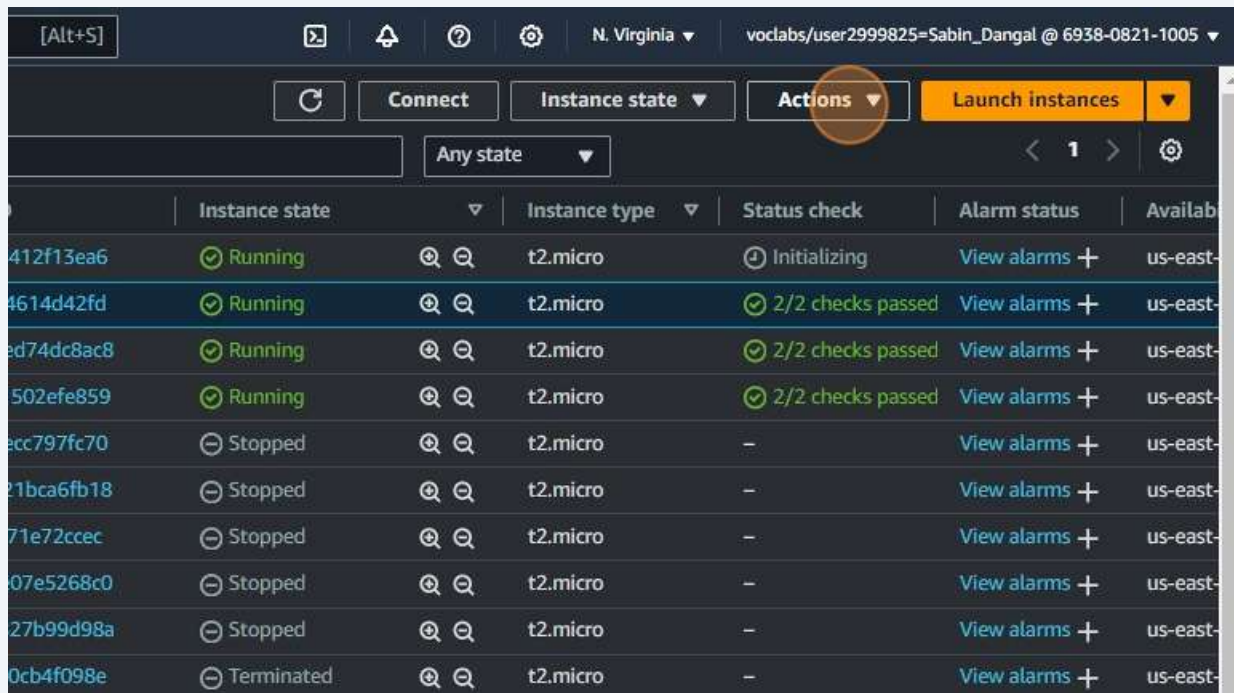
114 Click "Instances"



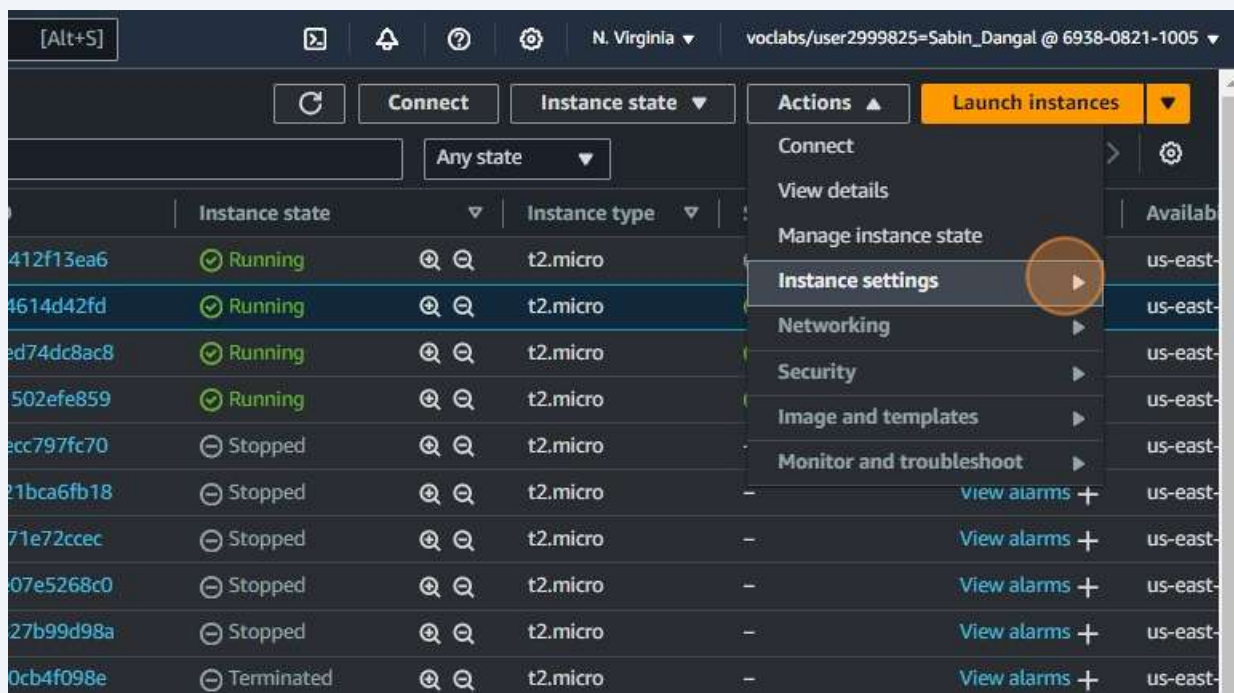
115 Click this checkbox.



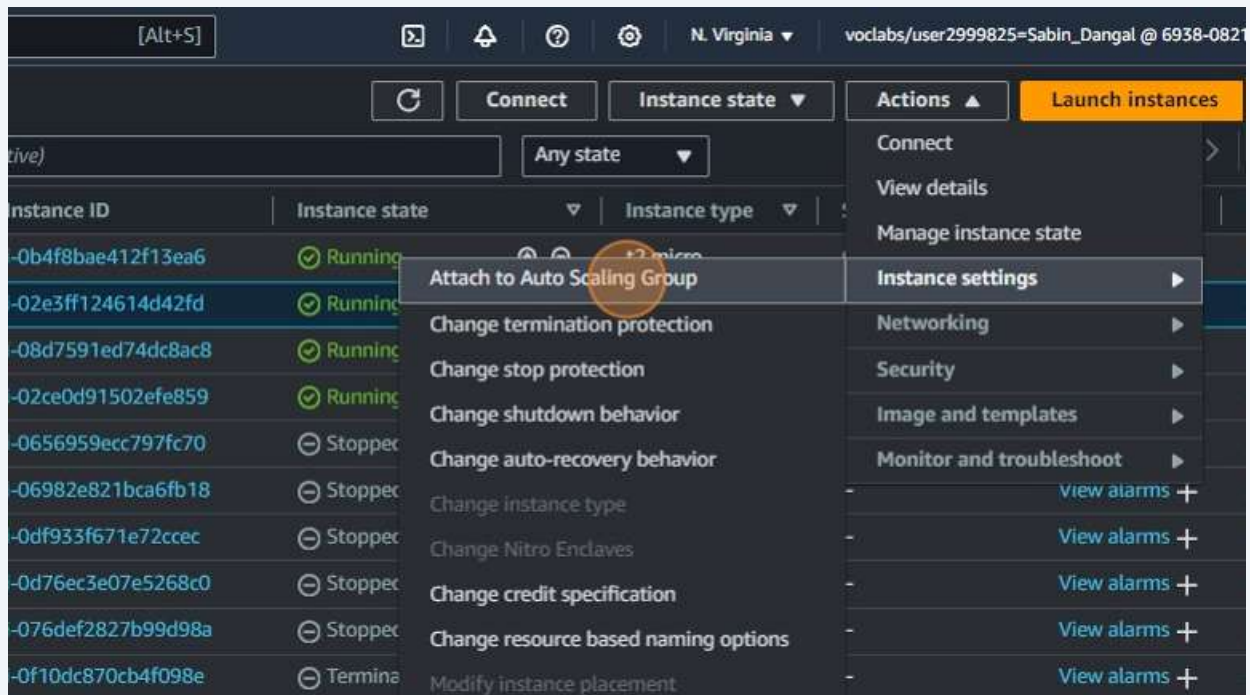
116 Click "Actions"



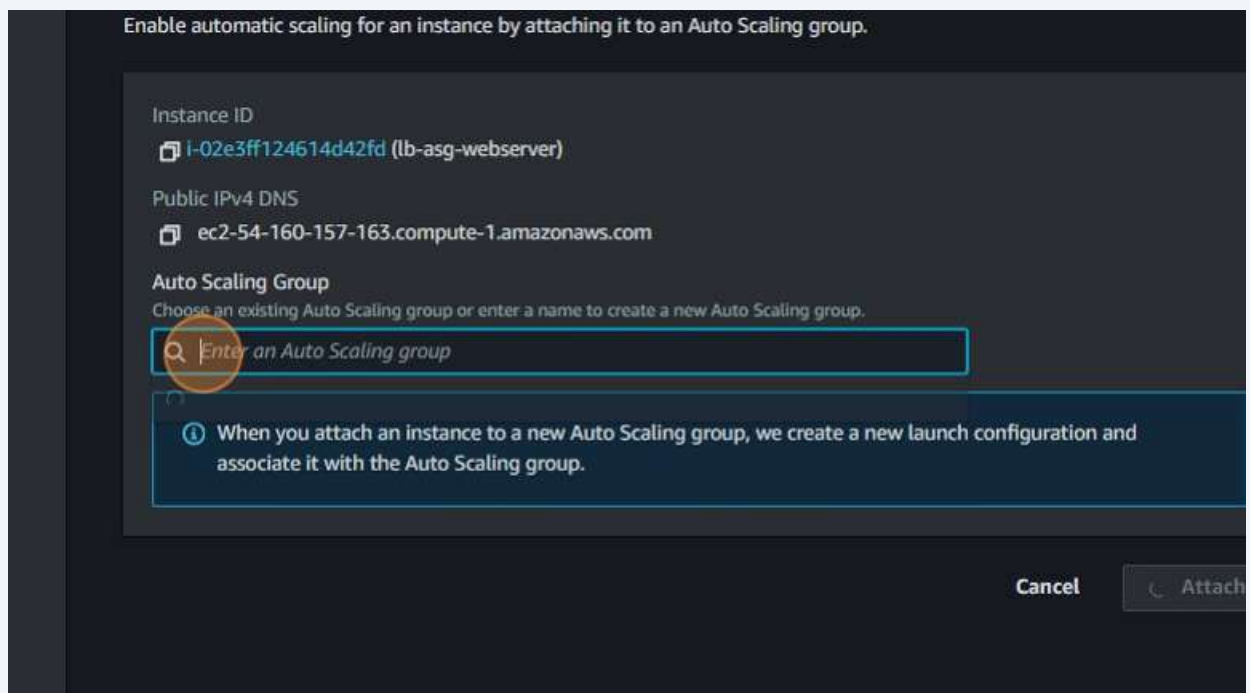
117 Click here.



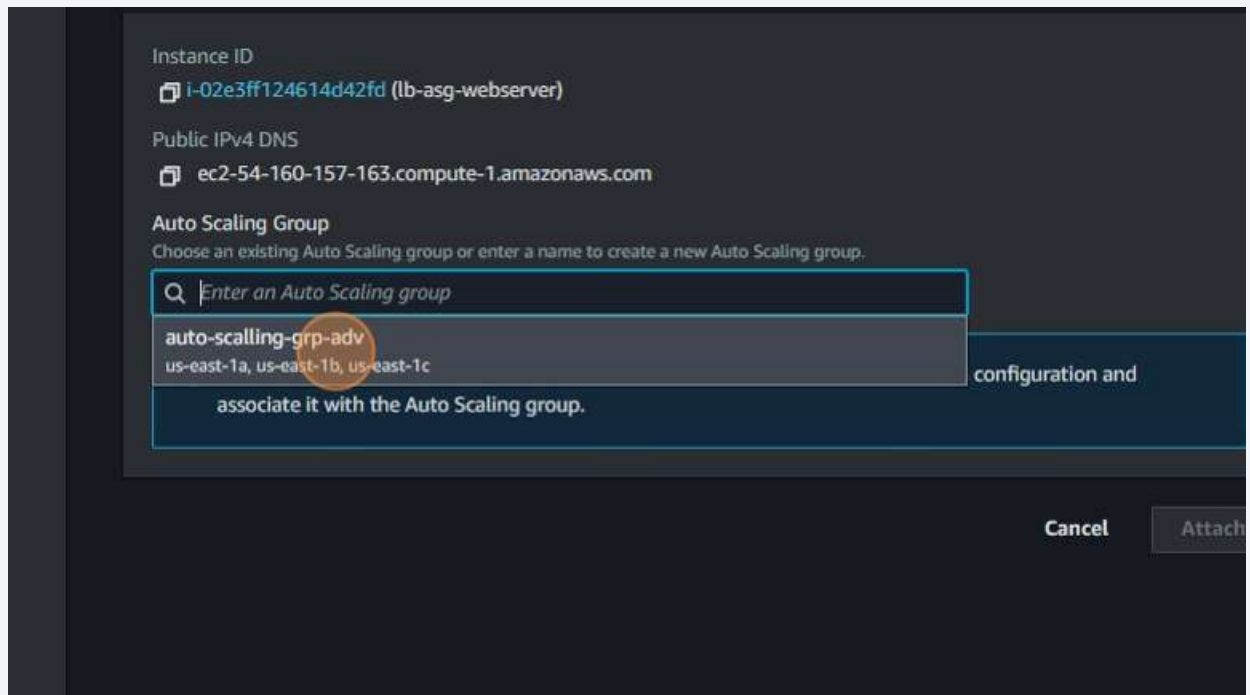
118 Click "Attach to Auto Scaling Group"



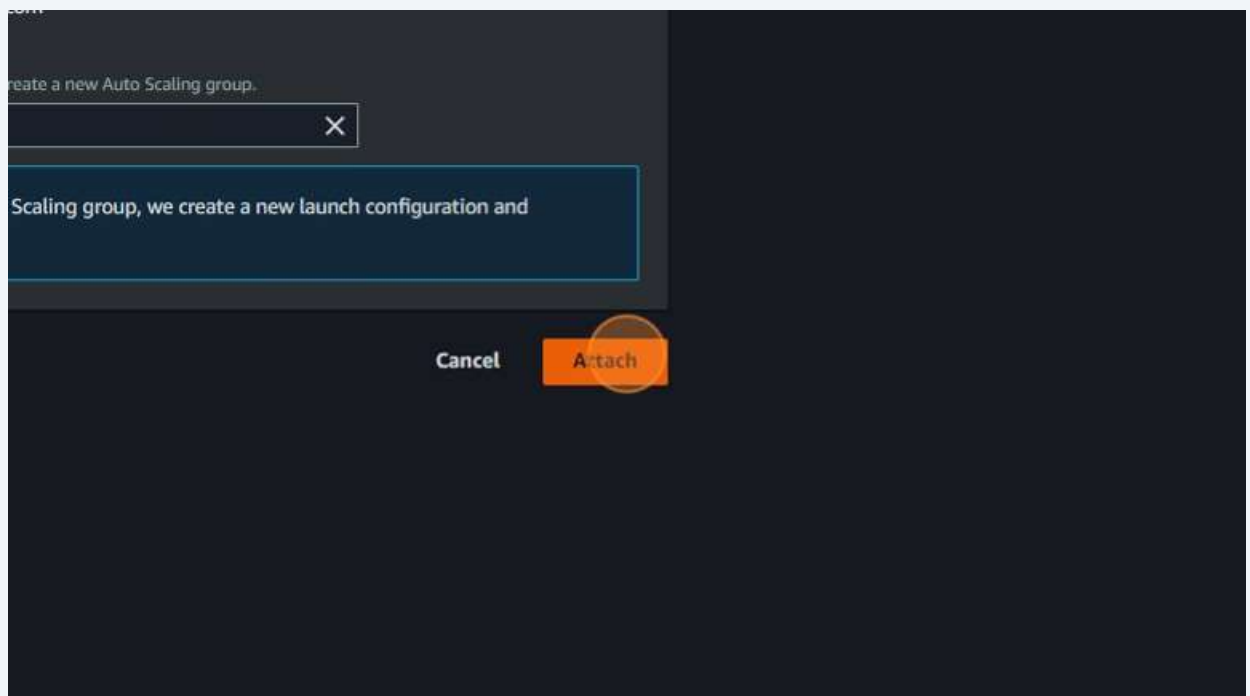
119 Click the "Auto Scaling Group" field.



120 Click "us-east-1a, us-east-1b, us-east-1c"



121 Click "Attach"



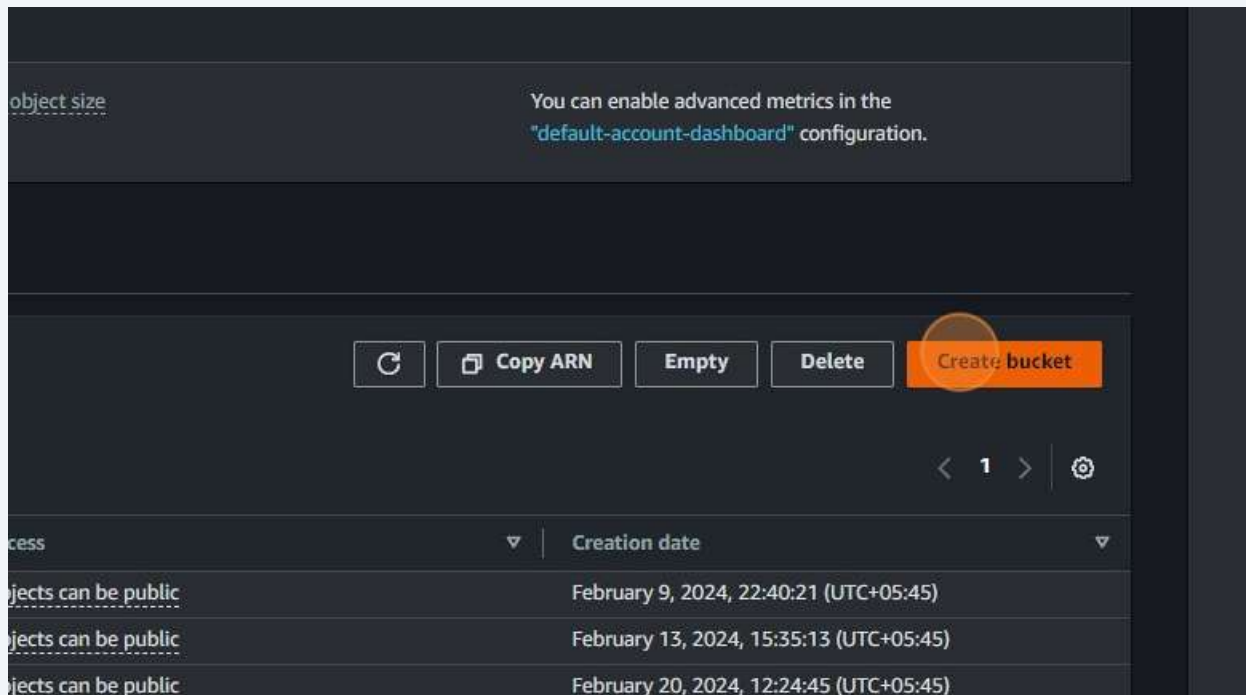
Hosting a Static Portfolio Website on S3

122

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

123

Click "Create bucket"



124 Click the "Bucket name" field.

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

Bucket type [Info](#)

- ☒ **General purpose**
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.
- ☐ **Directory - New**
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name [Info](#)

myawsbucket

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

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

Choose bucket

Format: s3://bucket/prefix

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

125 Type "static-website-s3-bucket-global"

126 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.

127 Click this checkbox.

Bucket owner: Full control. Enforced 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](#)

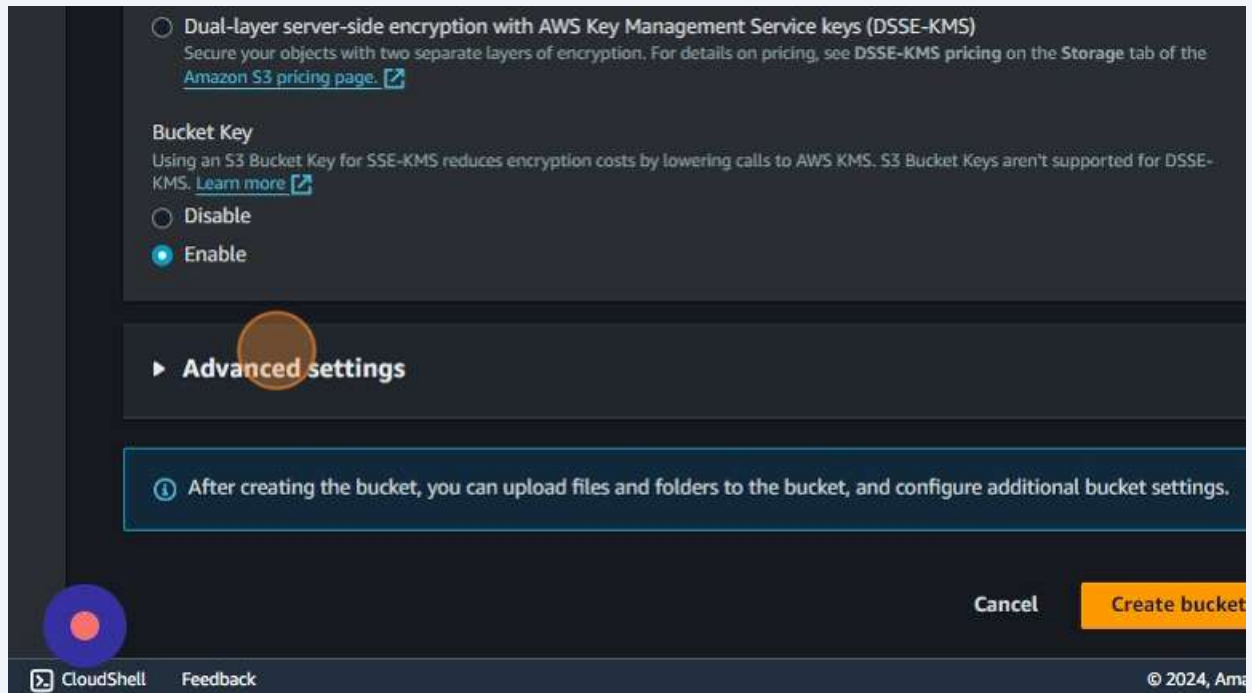
☒ **Block all public access**

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

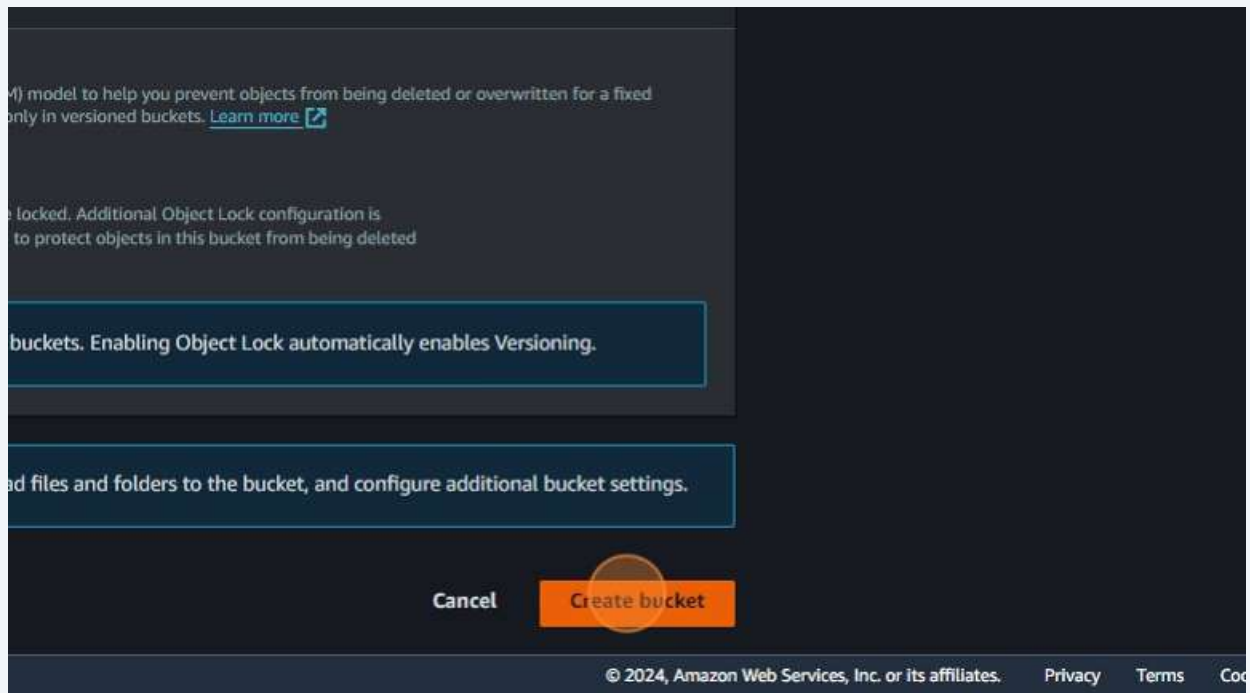
- ☒ **Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing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

128 Switch to tab "How to host static website on S3 [Step-by-Step] | GoLinuxCloud"

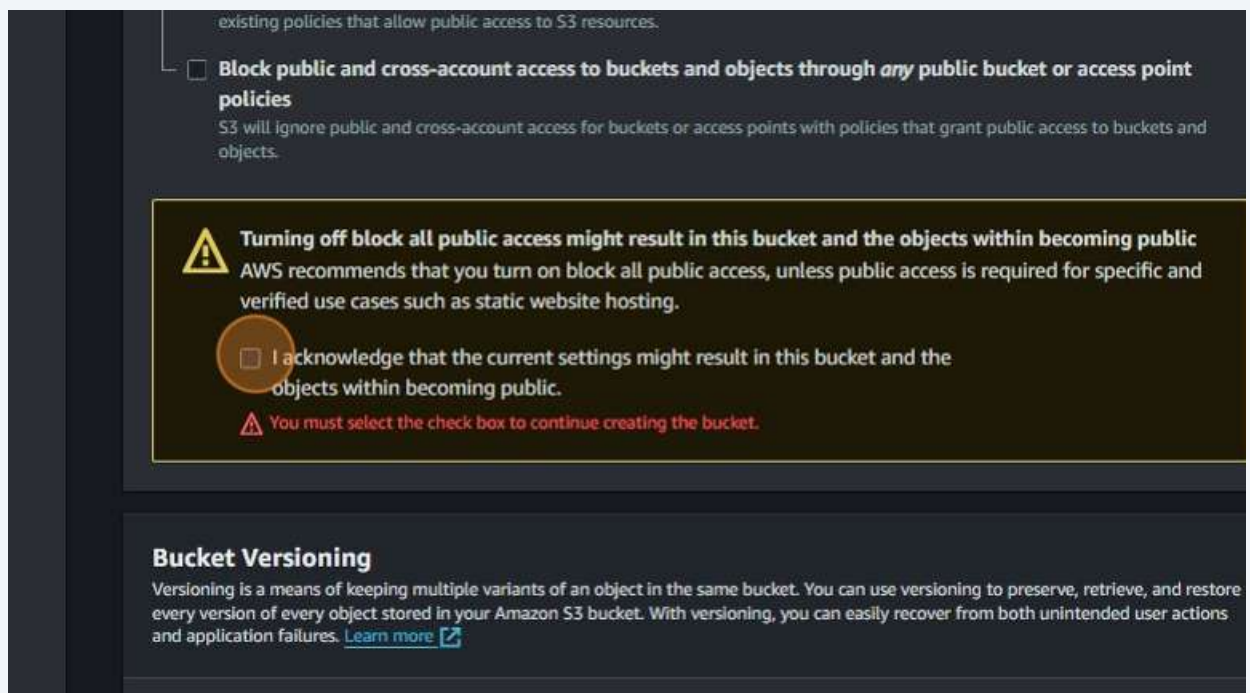
129 Click "Advanced settings"



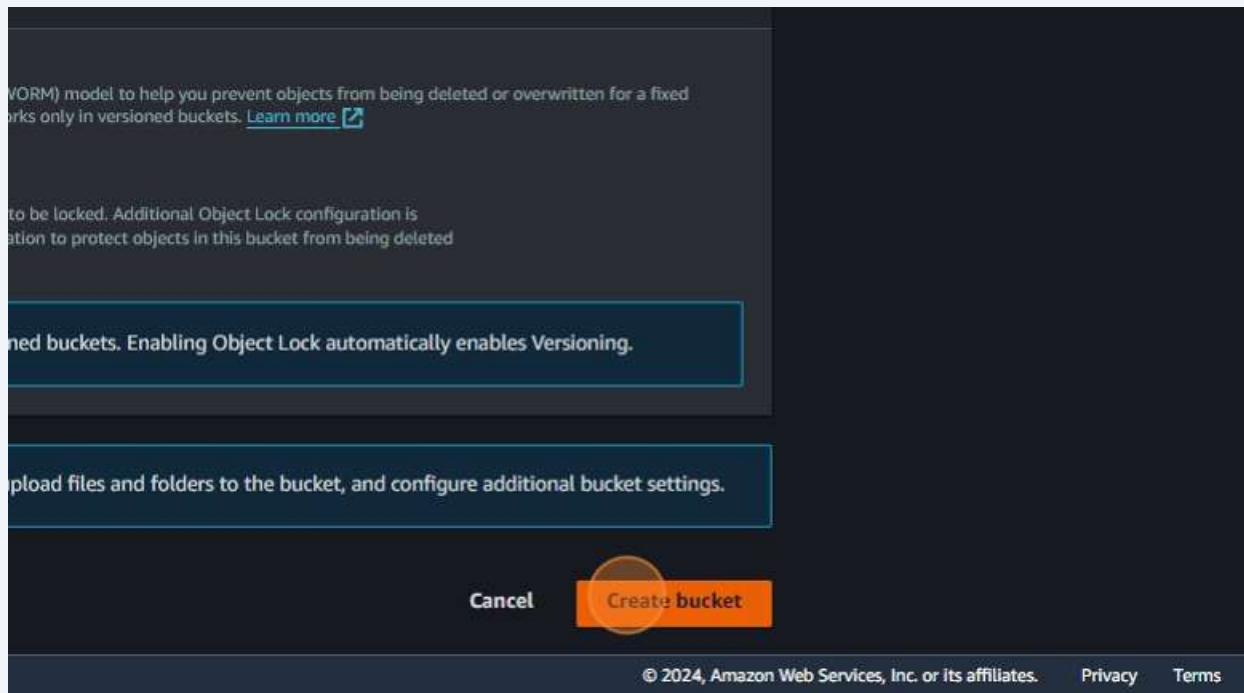
130 Click "Create bucket"



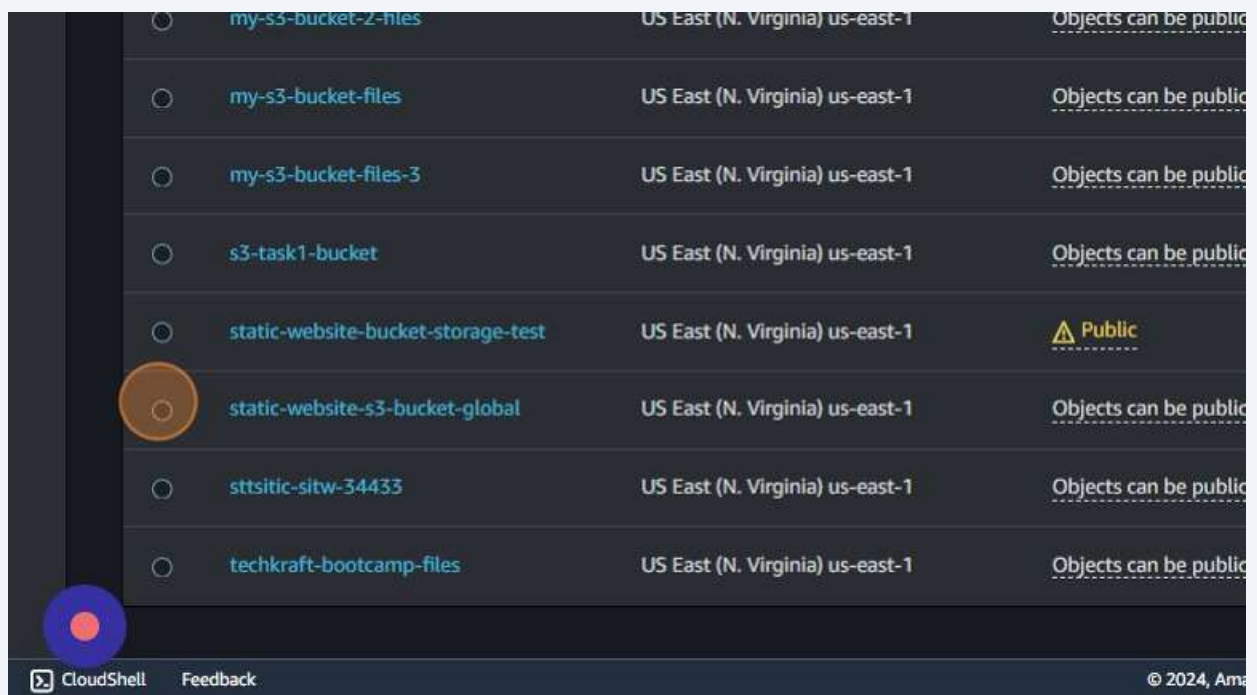
131 Click this checkbox.



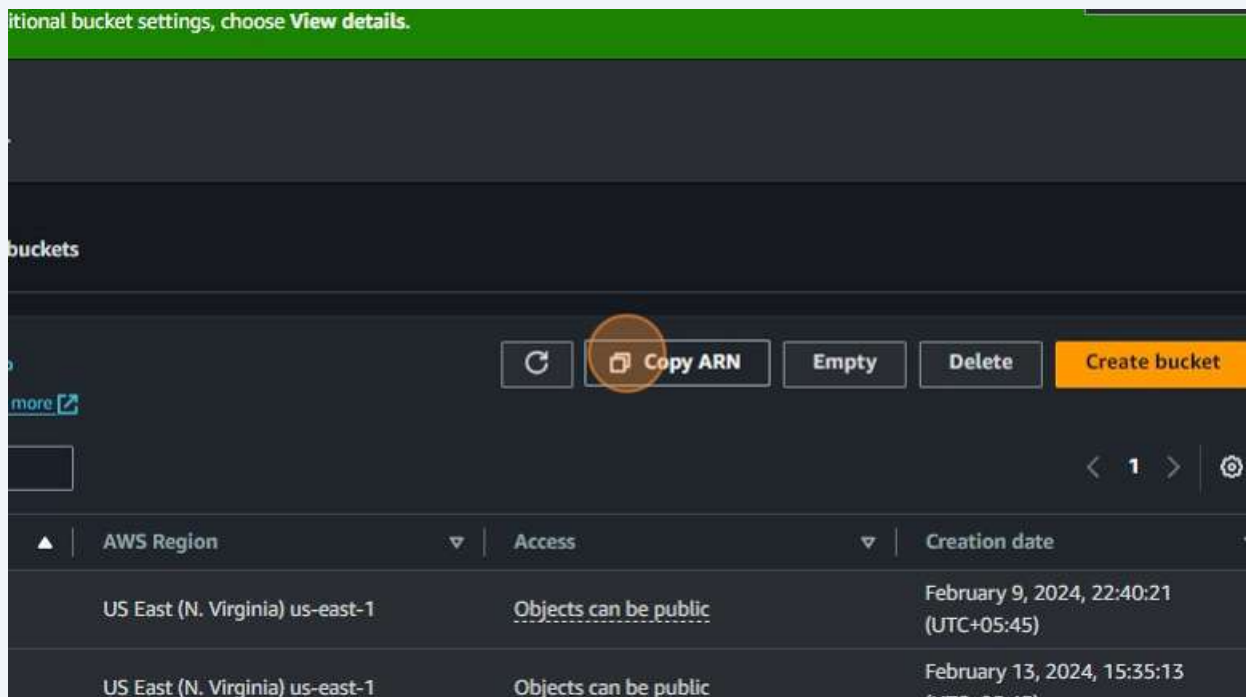
132 Click "Create bucket"



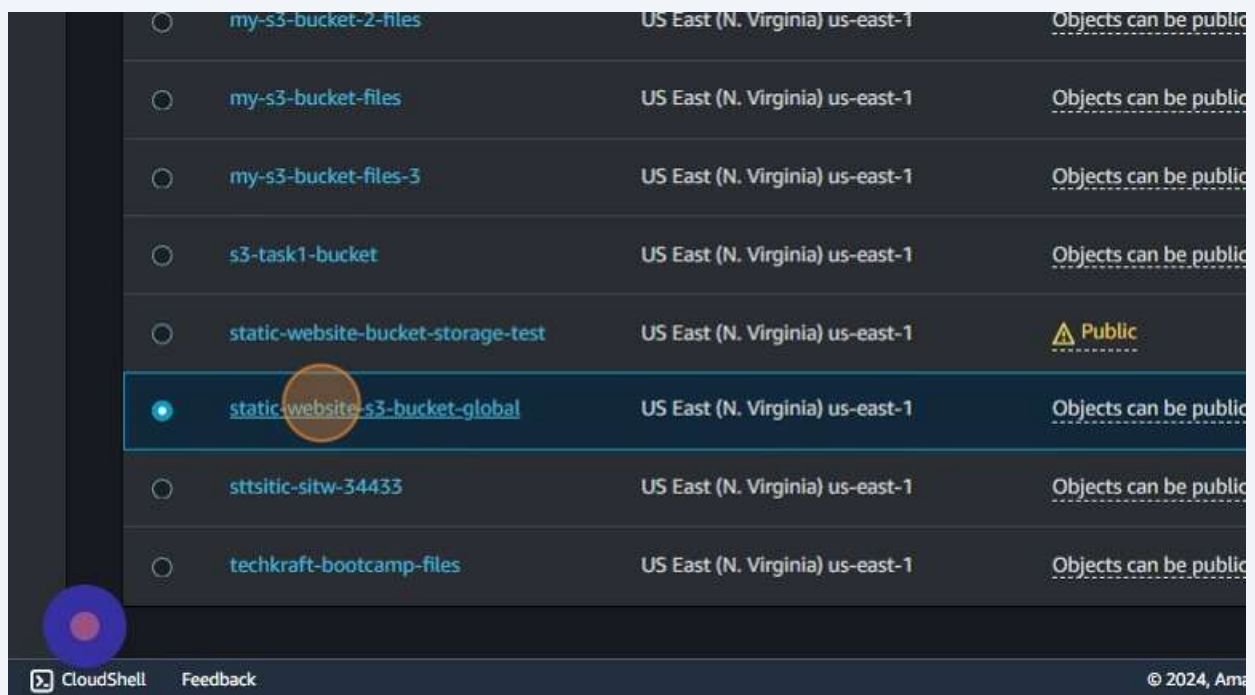
133 Click this radio button.



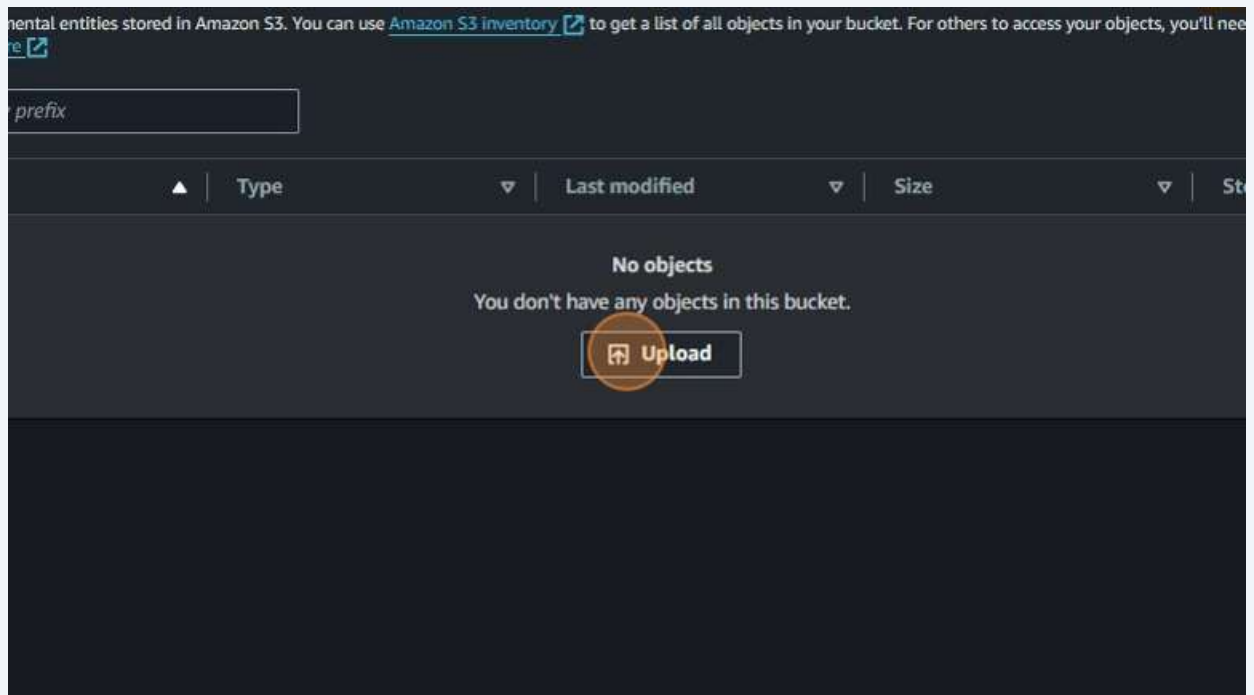
134 Click here.



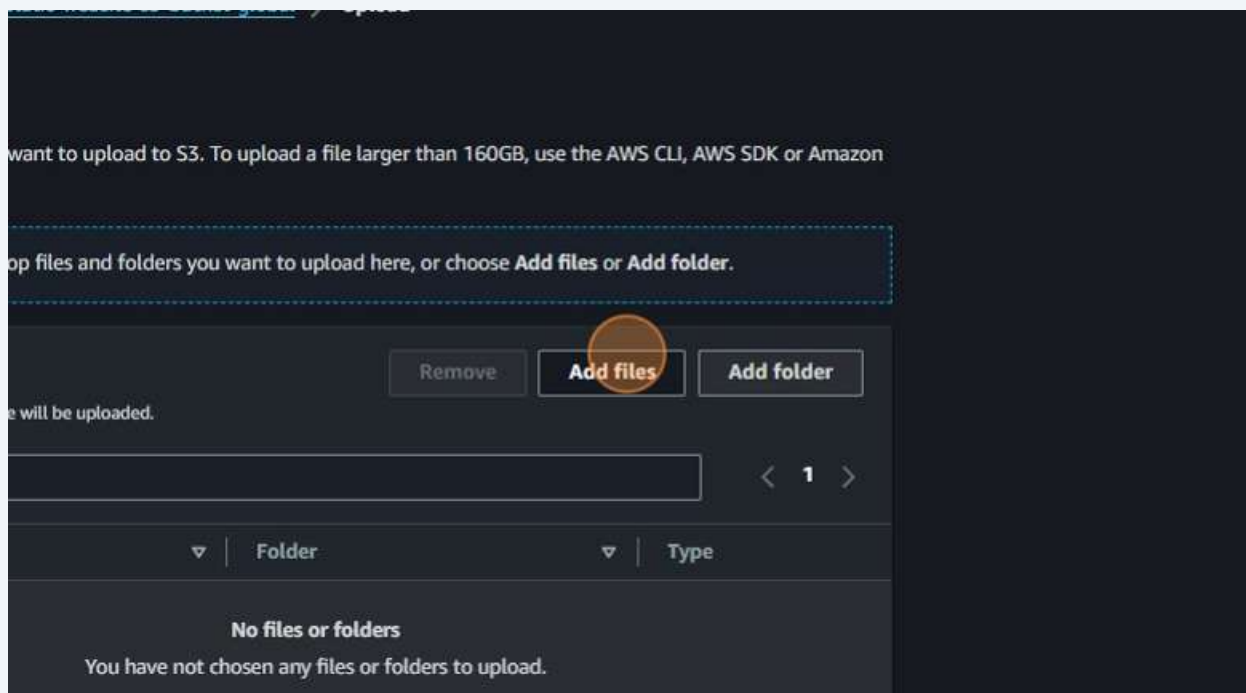
135 Click "static-website-s3-bucket-global"



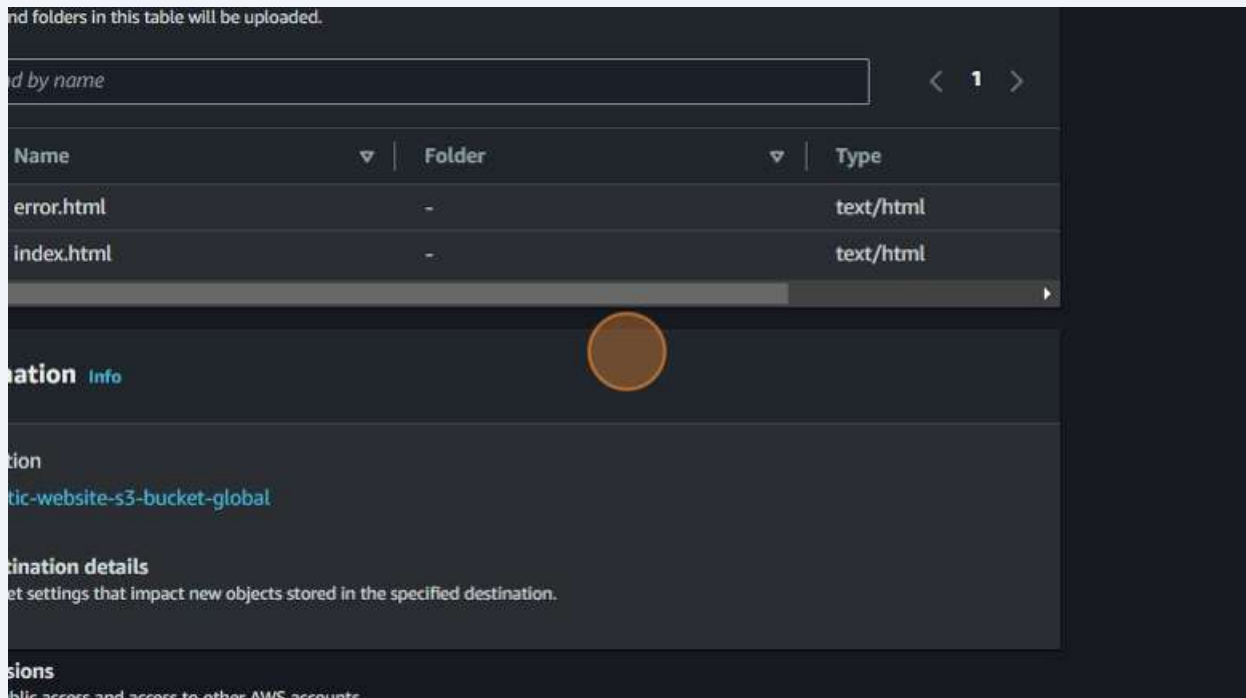
136 Click "Upload"



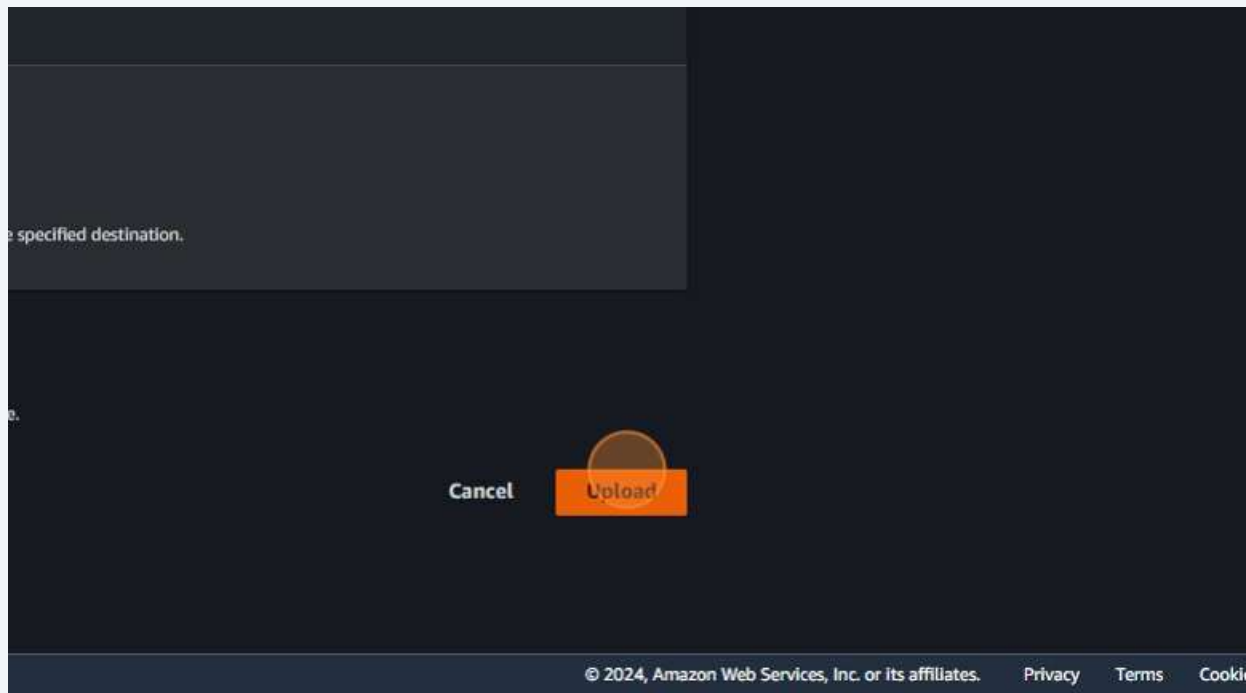
137 Click "Add files"



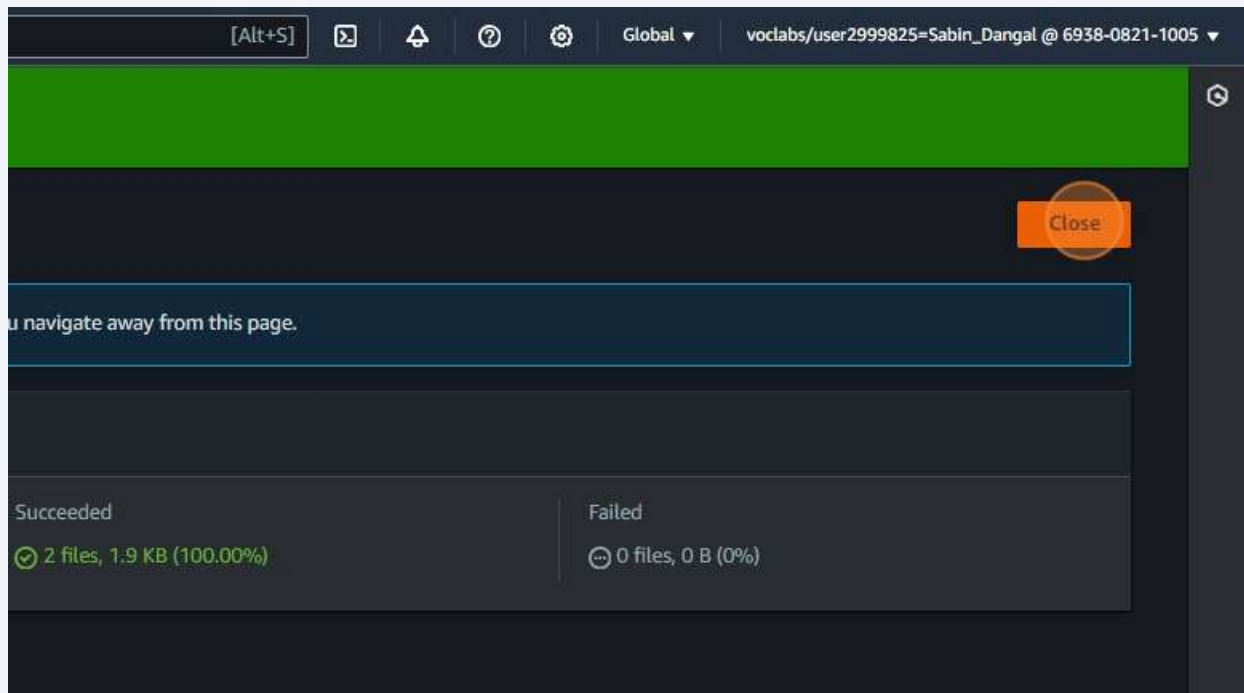
138 Click here.



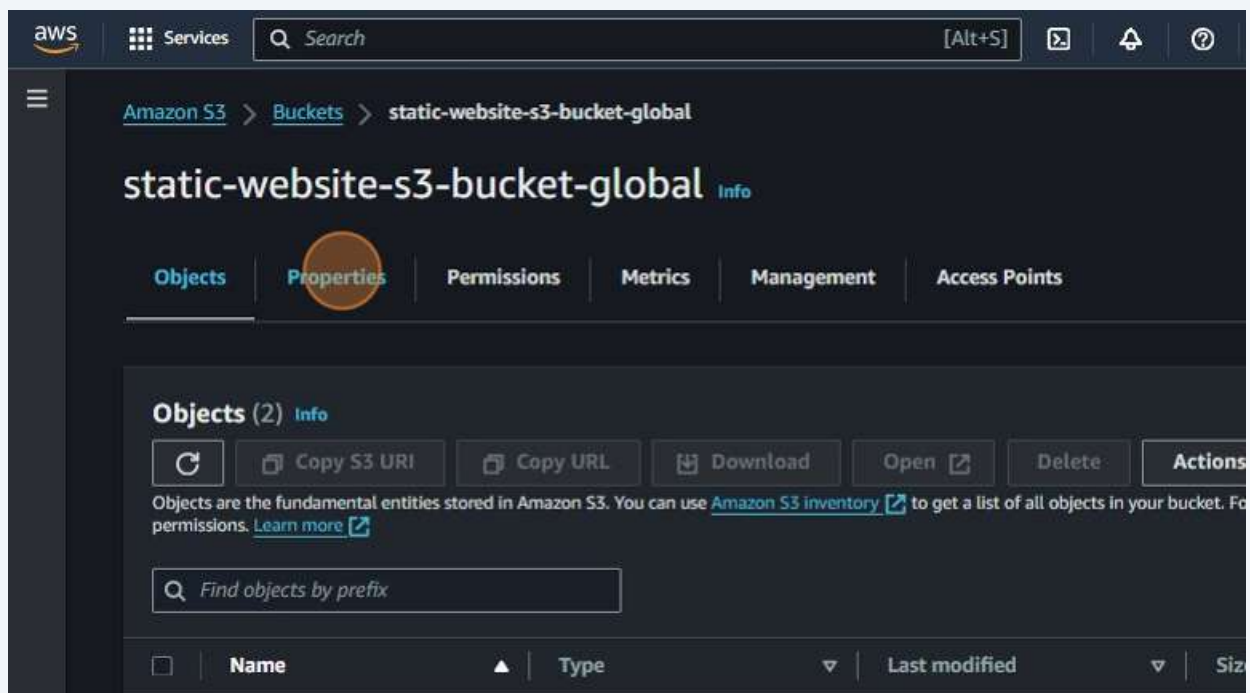
139 Click "Upload"



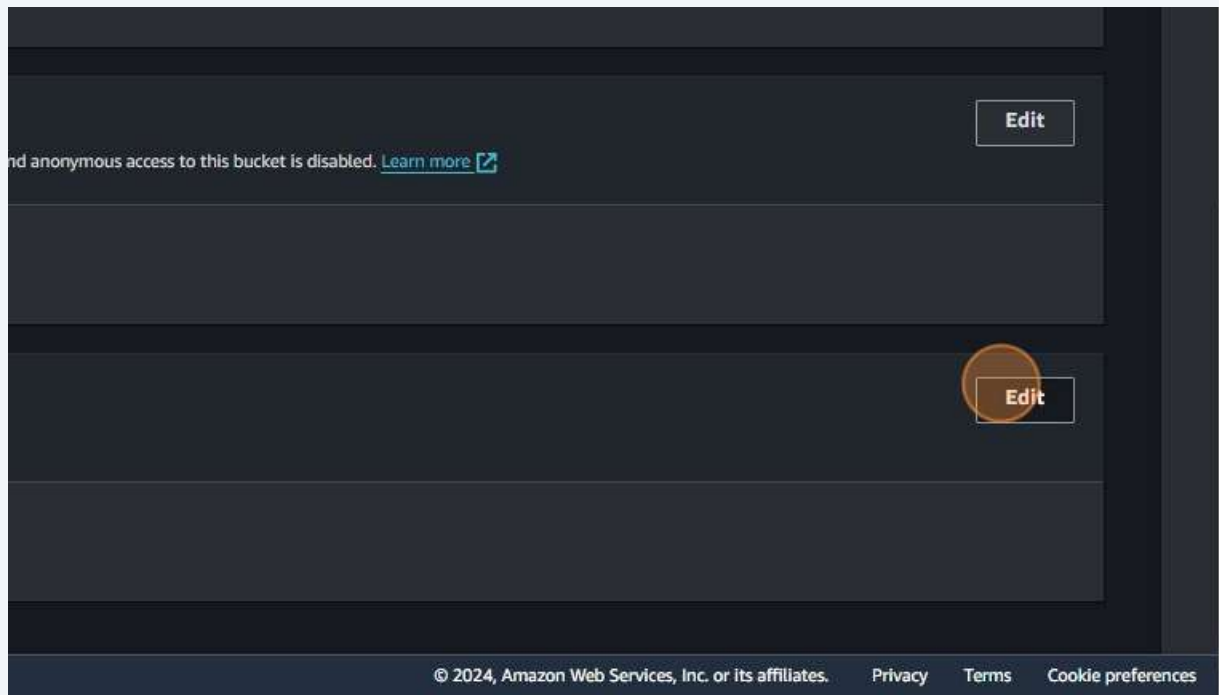
140 Click "Close"



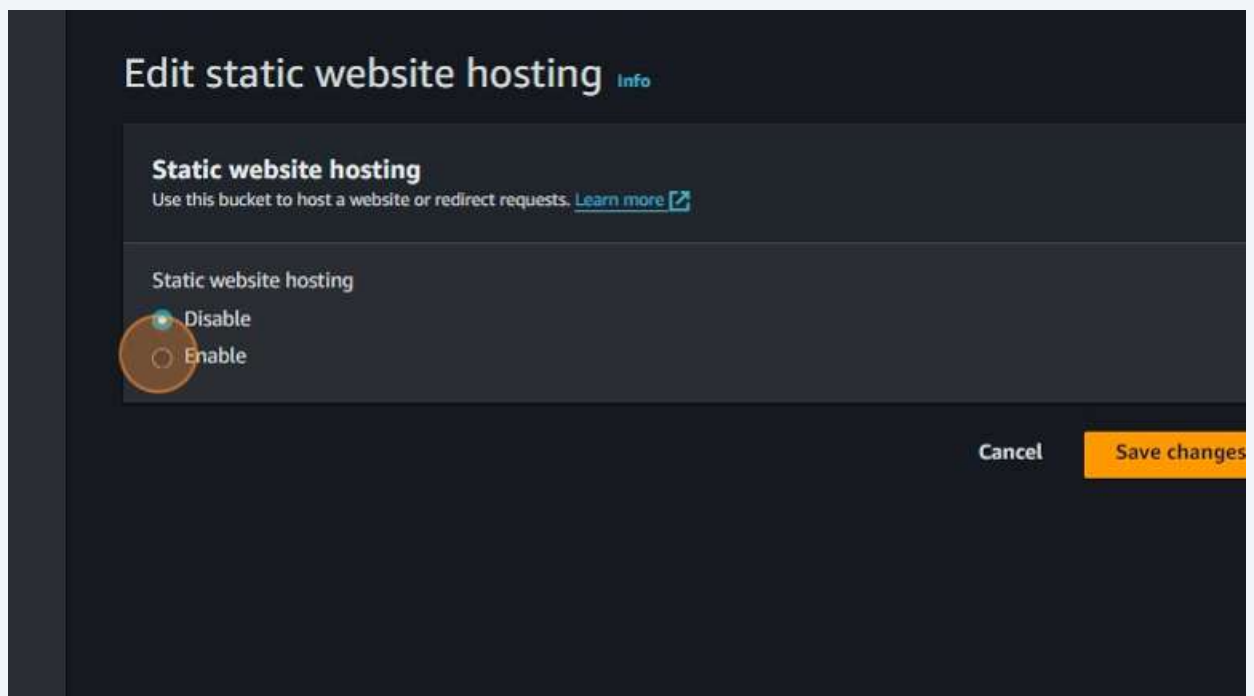
141 Click "Properties"



142 Click "Edit"



143 Click this radio button.



144 Click the "Index document" field.

☐ Redirect requests for an object
Redirect requests to another bucket or domain. [Learn more](#)

Index document
Specify the home or default page of the website.


Error document - optional
This is returned when an error occurs.

Redirection rules - optional
Redirection rules, written in JSON, automatically redirect webpage requests for specific content. [Learn more](#)

| 1 | |
|---|--|
| | |


145 Type "index.html"

146 Click the "Error document - optional" field.

readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see [Using Amazon S3 Block Public Access](#) 

Index document
Specify the home or default page of the website.

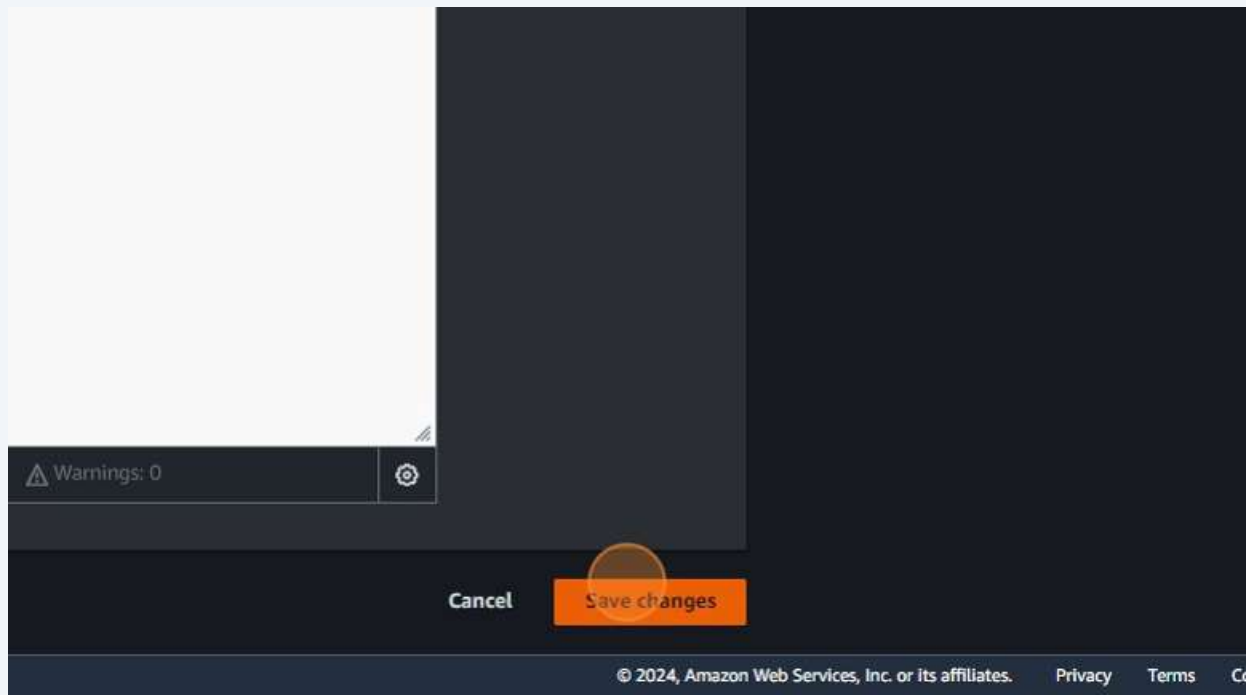
Error document - optional
This is returned when an error occurs.

Redirection rules - optional
Redirection rules, written in JSON, automatically redirect webpage requests for specific content. [Learn more](#) 

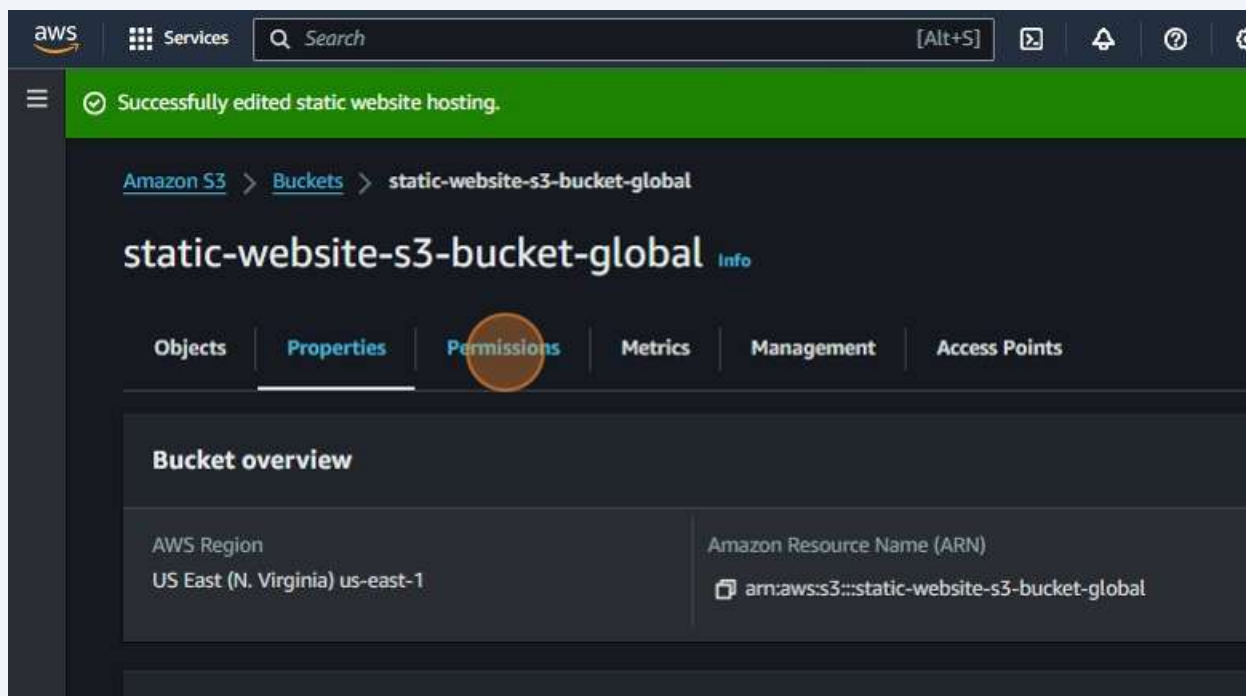
| 1 | |
|---|--|
| | |

147 Type "error.html"

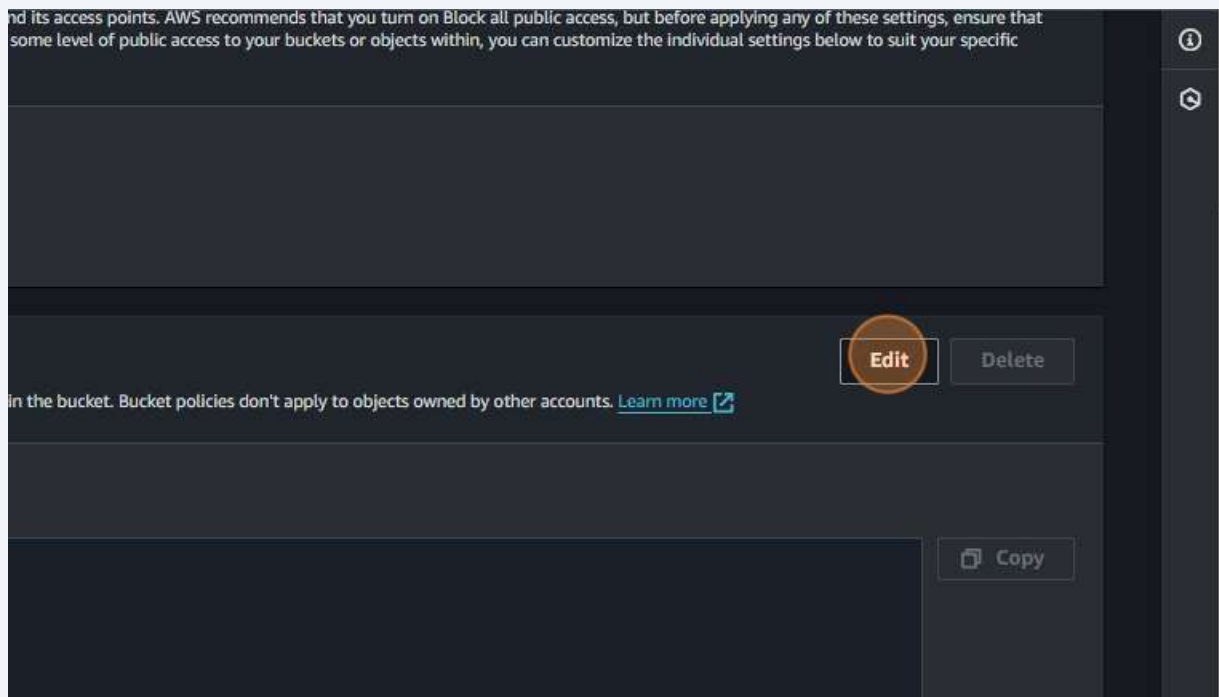
148 Click "Save changes"



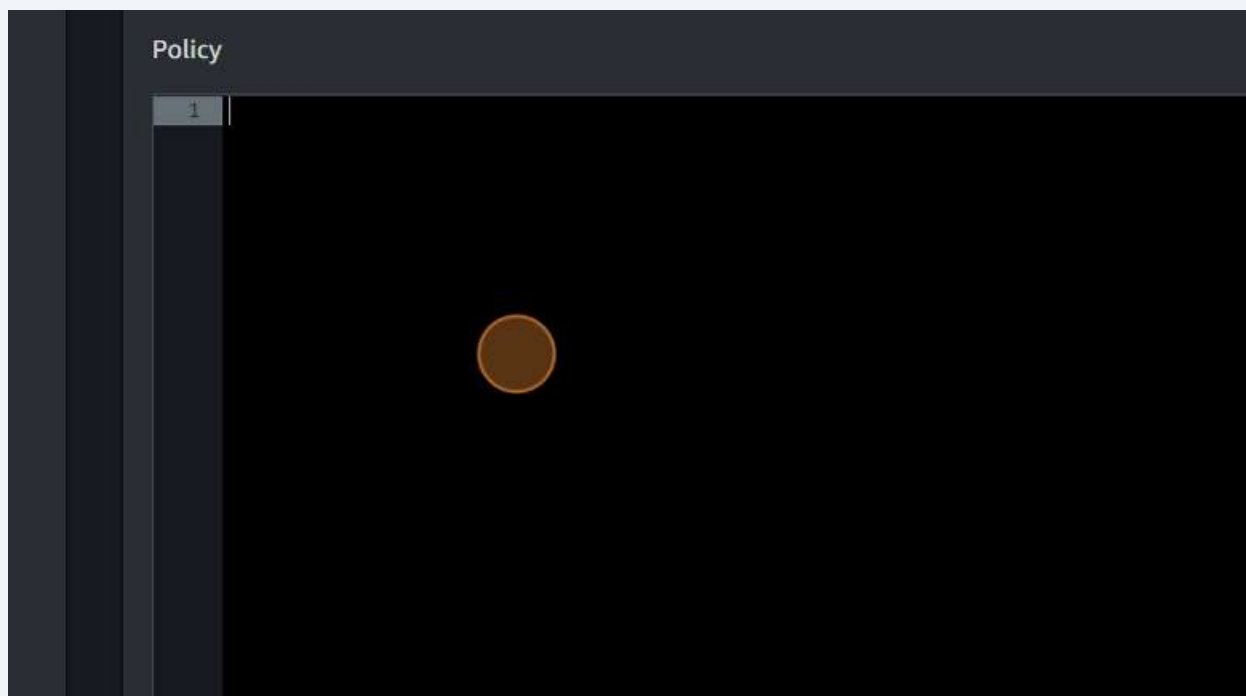
149 Click "Permissions"



150 Click "Edit"

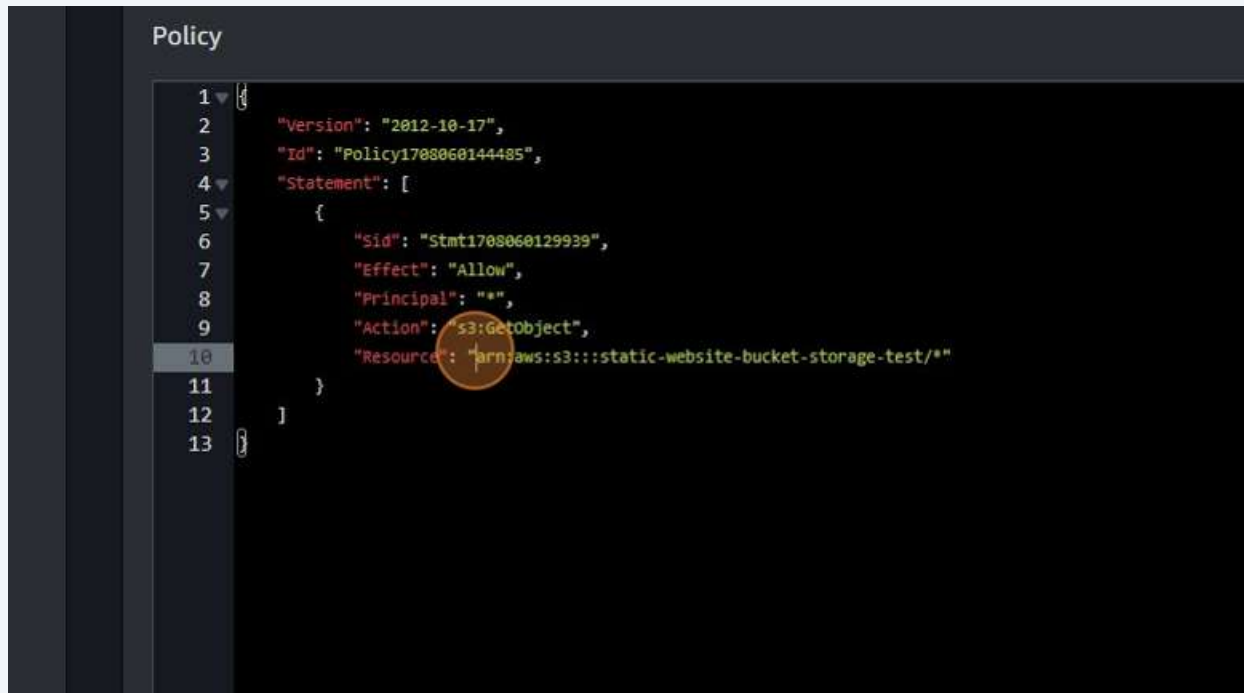


151 Click here.



152 Press **ctrl + v**

153 Click here.



The screenshot shows a code editor with a dark theme. The title bar of the editor is labeled "Policy". The code is a JSON document with the following structure:

```
1 {  
2   "Version": "2012-10-17",  
3   "Id": "Policy1708060144485",  
4   "Statement": [  
5     {  
6       "Sid": "Stmnt1708060129939",  
7       "Effect": "Allow",  
8       "Principal": "*",  
9       "Action": "s3:GetObject",  
10      "Resource": "arn:aws:s3:::static-website-bucket-storage-test/*"  
11    }  
12  ]  
13 }
```

A red circle is drawn around the "Resource" field on line 10, specifically around the value "arn:aws:s3:::static-website-bucket-storage-test/*". The line number 10 is highlighted in the left margin.

154 Double-click here.

```
version": "2012-10-17",
"policy": "Policy1708060144485",
"statement": [
  {
    "sid": "Stmt1708060129939",
    "effect": "Allow",
    "principal": "*",
    "action": "s3:GetObject",
    "resource": "arn:aws:s3:::static-website-bucket-storage-test/*"
  }
]
```

Edit statement
Stmt1708060129939

Add actions
Choose a service
Filter services

Included
S3

Available
AMP
API Gateway
API Gateway V2
ASC
Access Analyzer

155 Click "Save changes"

ASC
Access Analyzer
Account
Activate
Alexa for Business

Add a resource Add

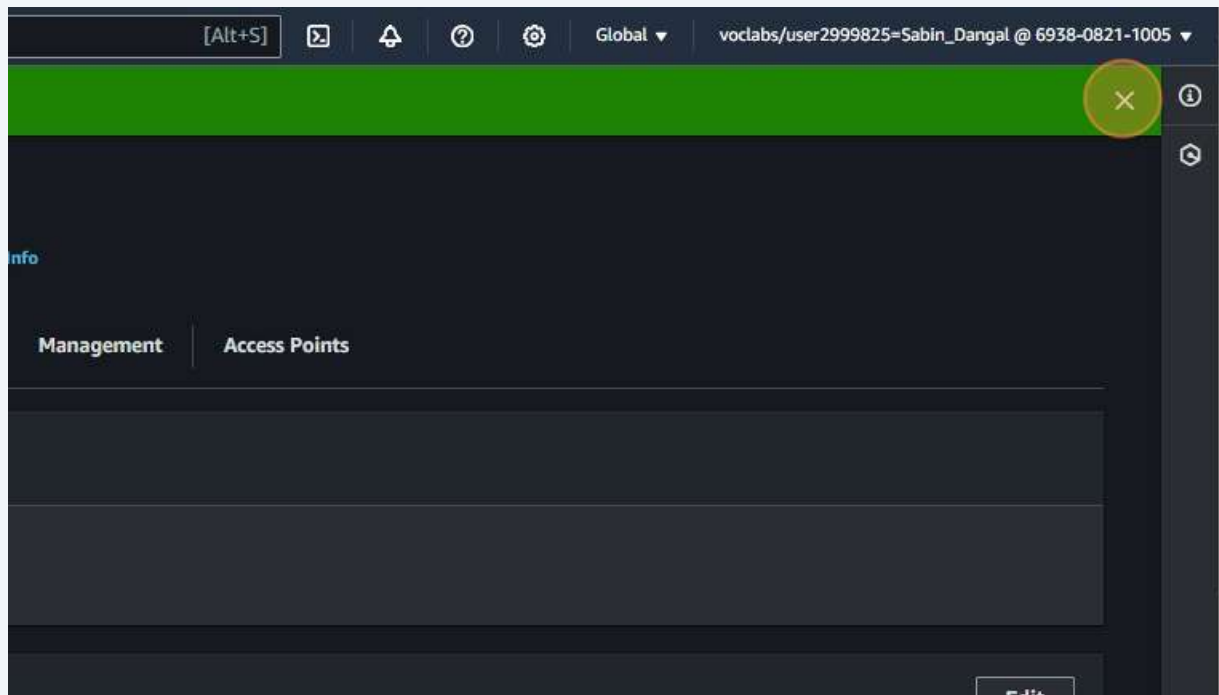
Add a condition (optional) Add

Preview external access

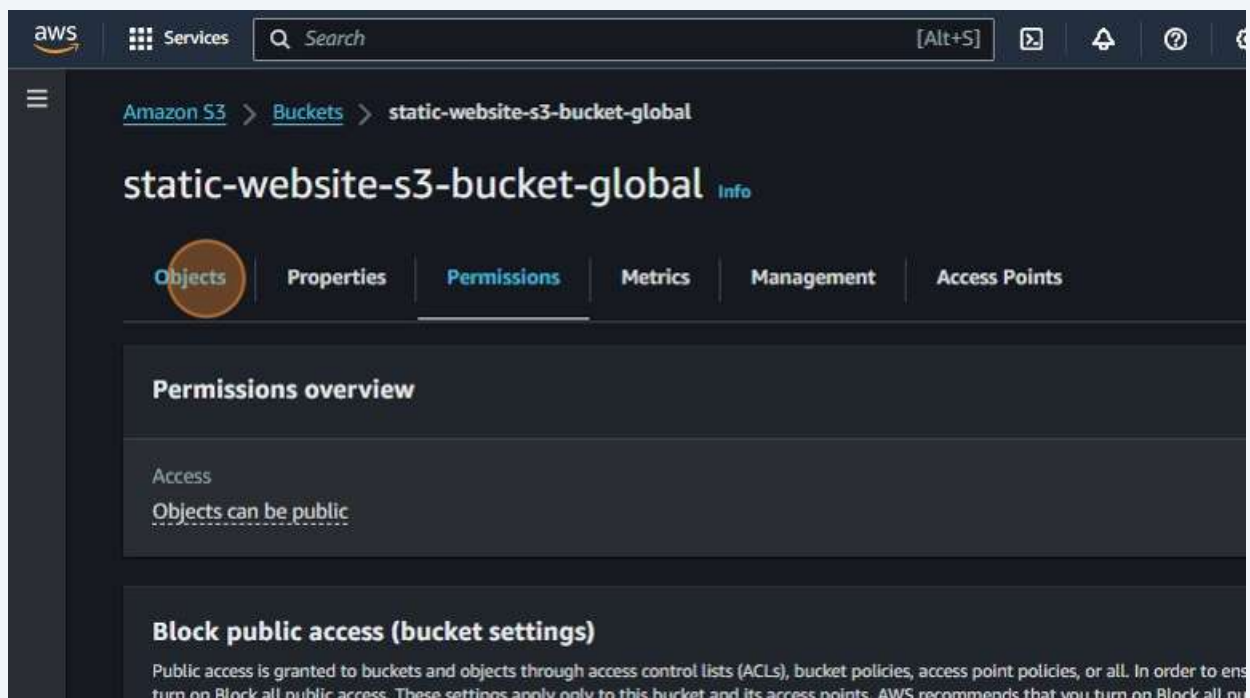
Cancel Save changes

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

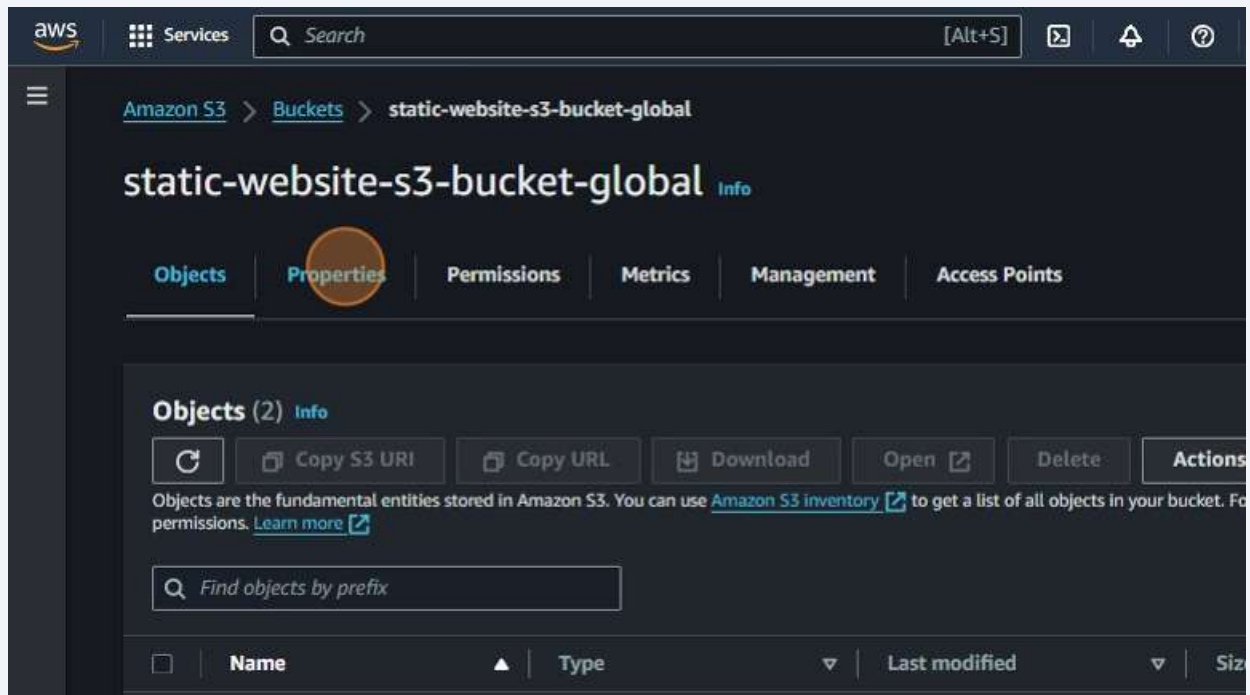
156 Click here.



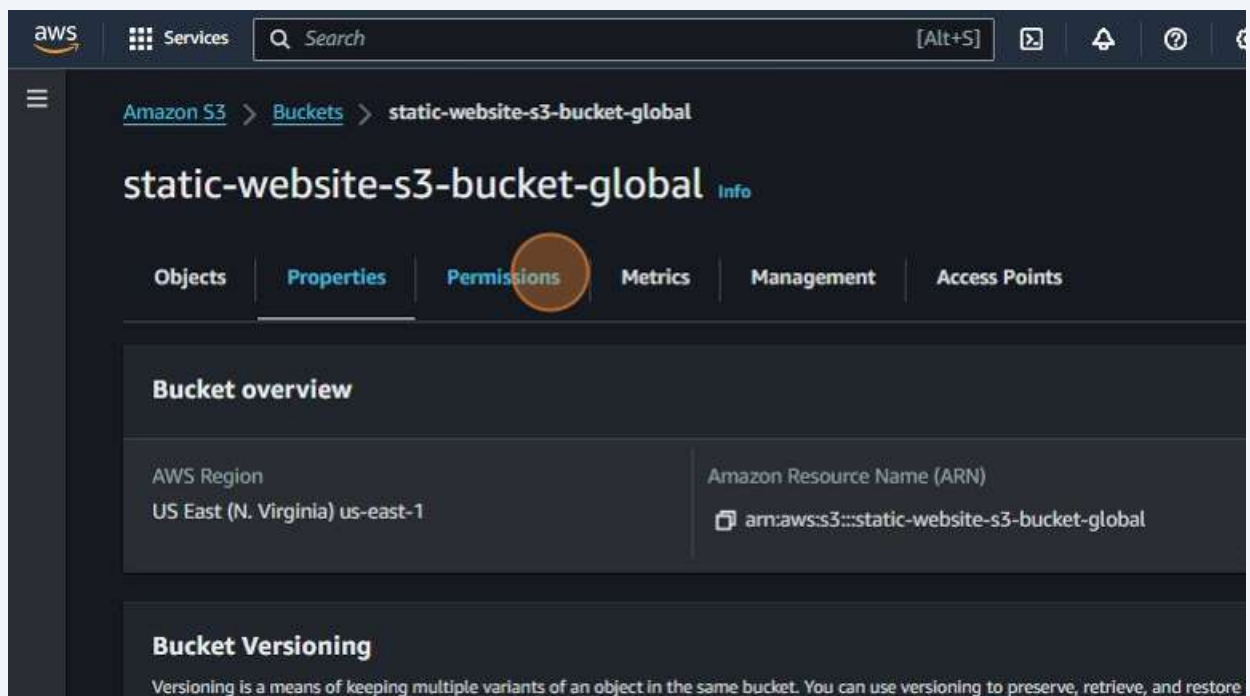
157 Click "Objects"



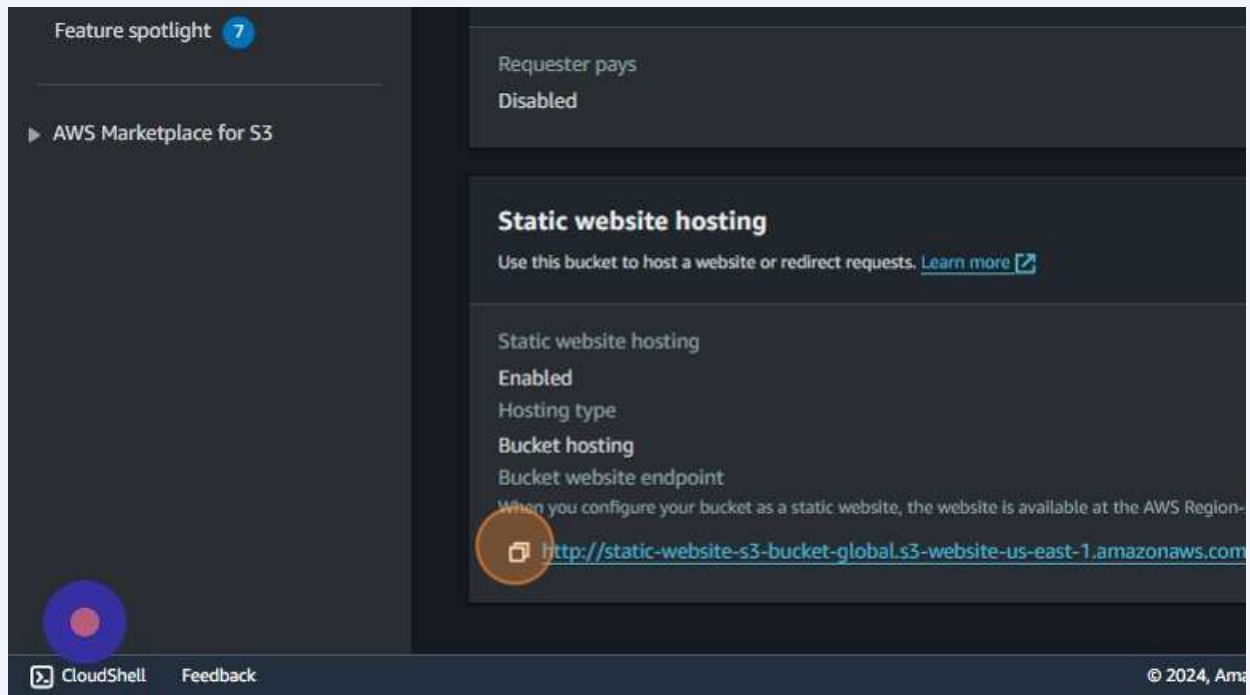
158 Click "Properties"



159 Click "Permissions"



160 Click here.



161 In a new tab, navigate to <http://static-website-s3-bucket-global.s3-website-us-east-1.amazonaws.com/>

Submit Form

ID:

Name:

