AWS Certified Solutions Architect – Associate

HOL

Version 24.06

Ahmed Abdelwahed
ahmed@abdelwahed.me
www.abdelwahed.me
LinkedIn
GitHub

Amazon Web Services (AWS) Essentials

Creating an AWS Account

Free Cloud Computing Services - AWS (amazon.com)

AWS Global infrastructure

Global Infrastructure (amazon.com)

- A Region is a geographic area that contains multiple data centers (availability zones). Each region has at least two availability zones.
- Points of Presence (PoPs) are data centers that help AWS maintain services like high availability (HA) and are not available for public use. Another example is caching services, which provide fast access to your data. PoPs satisfy specific business requirements.
- AWS offers over 200 fully featured services.

AWS Documentation

AWS Documentation (amazon.com)

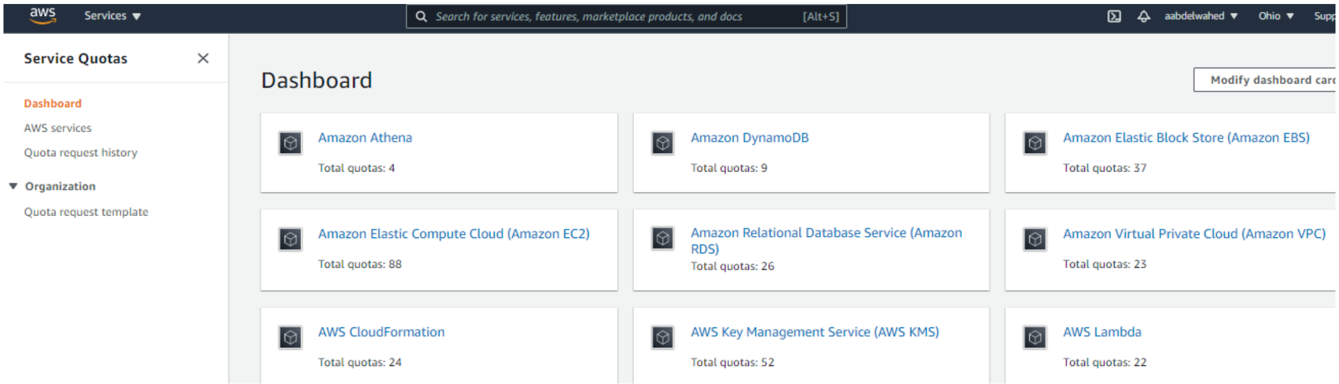
Amazon Web Services Service Status | CloudHarmony

AWS Artifact (amazon.com) Here you can download more reports about AWS regulations.

Global Infrastructure Regions & AZs (amazon.com)

Compliance Programs - Amazon Web Services (AWS), Here are AWS certifications

Dashboard | AWS Service Quotas (amazon.com)



Dashboard

Amazon Athena
Total quotas: 4

Amazon DynamoDB
Total quotas: 9

Amazon Elastic Block Store (Amazon EBS)
Total quotas: 37

Amazon Elastic Compute Cloud (Amazon EC2)
Total quotas: 88

Amazon Relational Database Service (Amazon RDS)
Total quotas: 26

Amazon Virtual Private Cloud (Amazon VPC)
Total quotas: 23

AWS CloudFormation
Total quotas: 24

AWS Key Management Service (AWS KMS)
Total quotas: 52

AWS Lambda
Total quotas: 22

Access more CloudFormation templates online at https://aws.amazon.com/quickstart/

Shared Responsibility Model

Customer Responsibilities

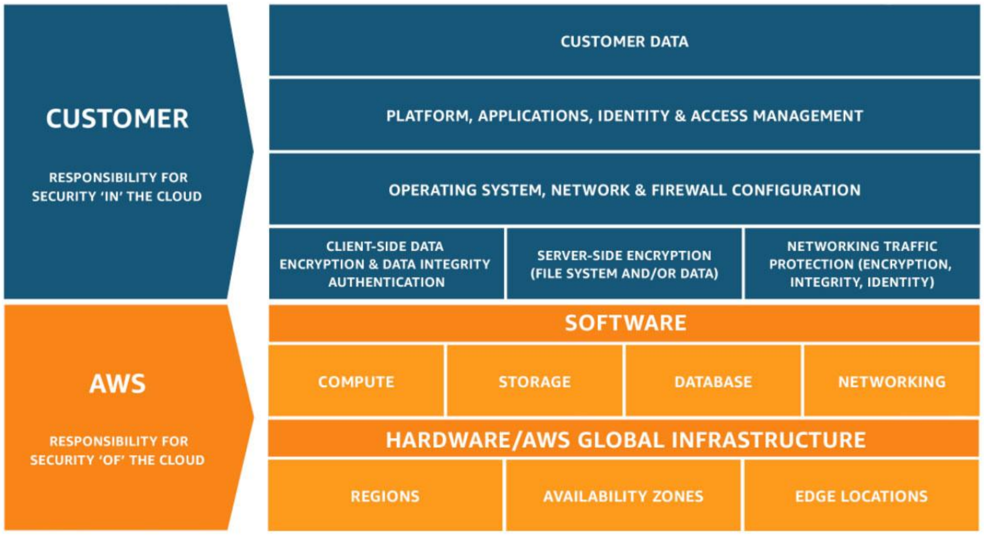
- **Customer Data:** Securing the data that they store and process in the AWS cloud.
- **Platform, Applications, Identity & Access Management:** Managing their applications, platform, and IAM configurations.
- **Operating System, Network & Firewall Configuration:** Configuring and securing their operating systems, network settings, and firewalls.
- **Client-Side Data Encryption & Data Integrity Authentication:** Encrypting data on the client side and ensuring data integrity and authentication.
- **Server-Side Encryption (File System and/or Data):** Implementing server-side encryption for file systems and data.
- **Networking Traffic Protection (Encryption, Integrity, Identity):** Ensuring encryption, integrity, and identity of network traffic.

AWS Responsibilities

- **Security of the Cloud:** AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud.
- **Hardware/AWS Global Infrastructure:**
  - **Regions:** Managing the physical locations where data is stored.
  - **Availability Zones:** Ensuring the availability and redundancy of data centers.
  - **Edge Locations:** Managing points of presence for content delivery and other services.

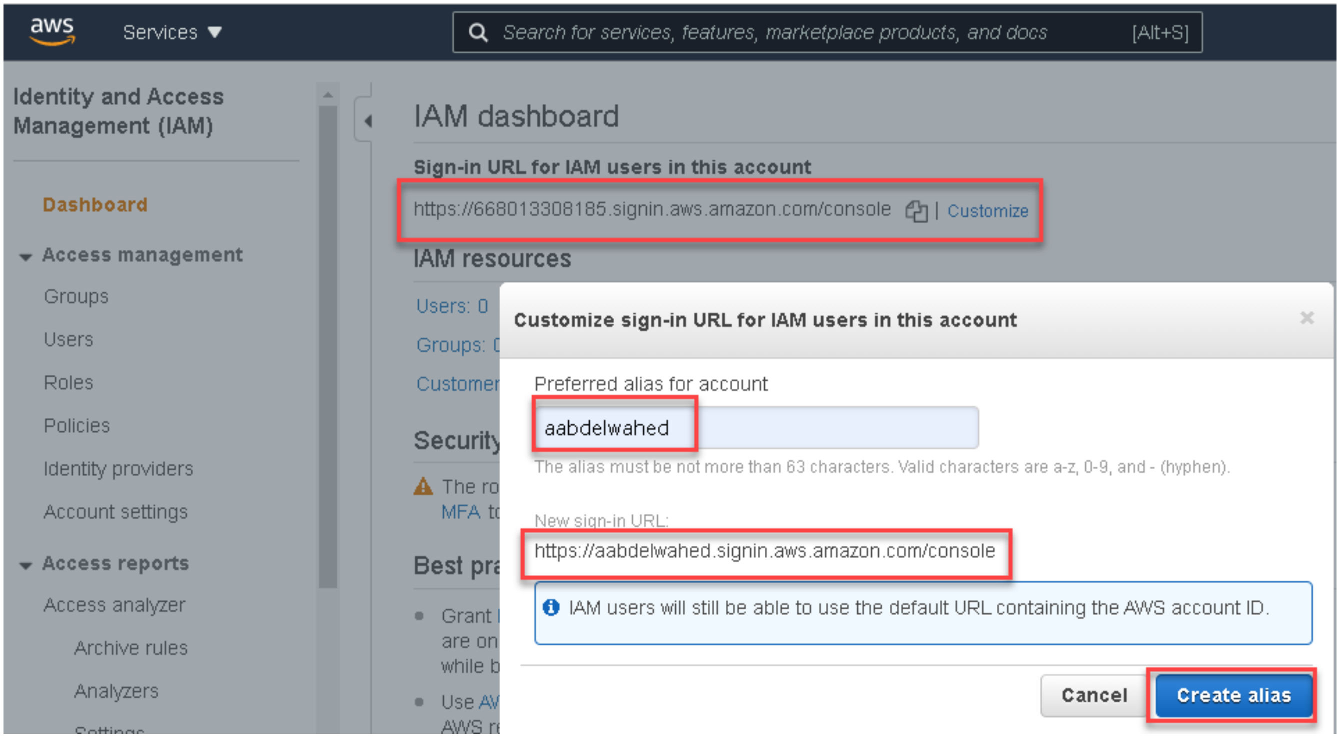
AWS Managed Services

- **Software:**
  - **Compute:** Securing compute resources.
  - **Storage:** Managing and securing storage solutions.
  - **Database:** Ensuring the security of managed database services.
  - **Networking:** Securing networking components.


CUSTOMER
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD
AWS
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

Identity Management

Utilize IAM for root and additional account management & Personalize sign-in link for IAM user access



Sign-in URL for IAM users in this account

https://668013308185.signin.aws.amazon.com/console | Customize

Customize sign-in URL for IAM users in this account

Preferred alias for account

aabdelwahed

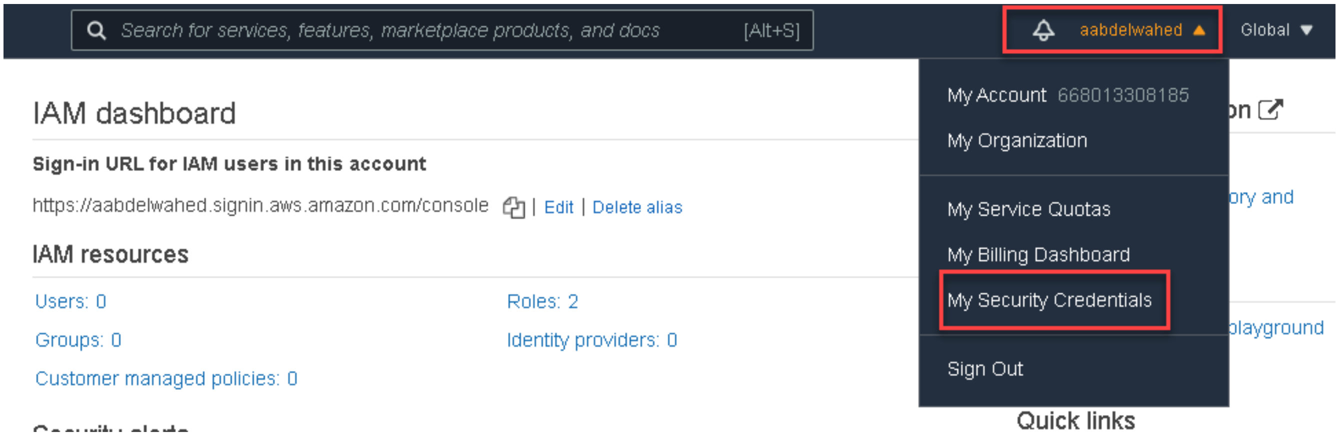
The alias must be not more than 63 characters. Valid characters are a-z, 0-9, and - (hyphen).

New sign-in URL:

https://aabdelwahed.signin.aws.amazon.com/console

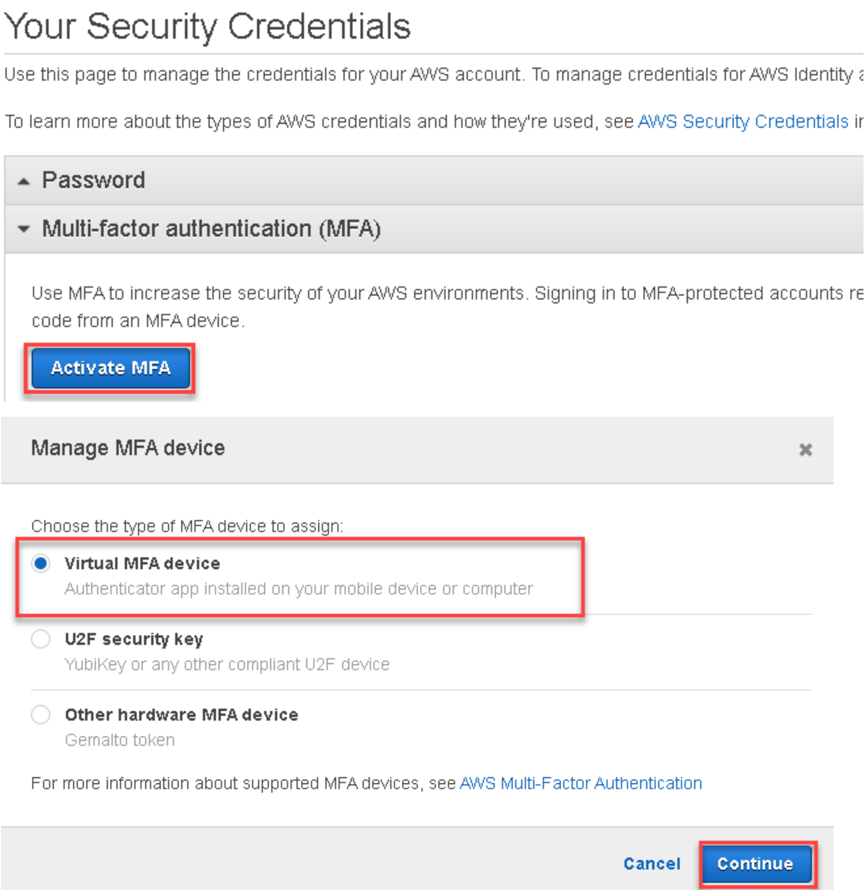
IAM users will still be able to use the default URL containing the AWS account ID.

Enable MFA for root account



Sign-in URL for IAM users in this account

https://aabdelwahed.signin.aws.amazon.com/console | Edit | Delete alias



Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity a

To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials ir

Use MFA to increase the security of your AWS environments. Signing in to MFA-protected accounts re code from an MFA device.

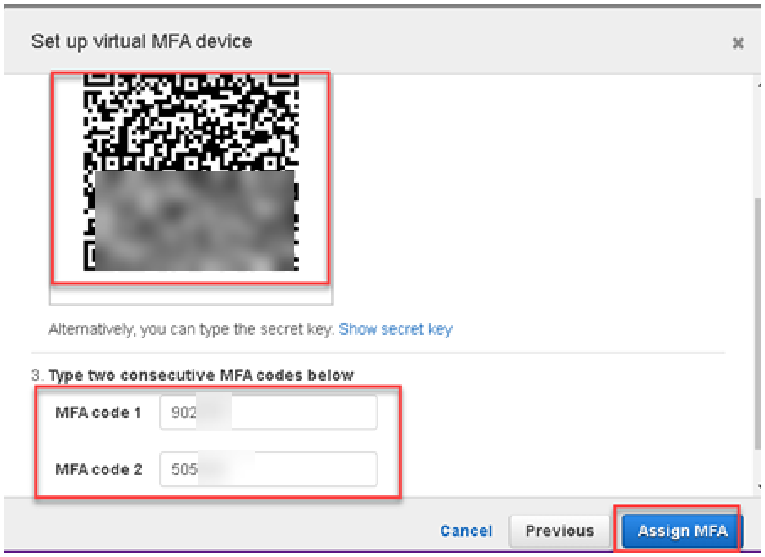
Choose the type of MFA device to assign:

● **Virtual MFA device**
Authenticator app installed on your mobile device or computer

○ **U2F security key**
YubiKey or any other compliant U2F device

○ **Other hardware MFA device**
Gemalto token

For more information about supported MFA devices, see AWS Multi-Factor Authentication



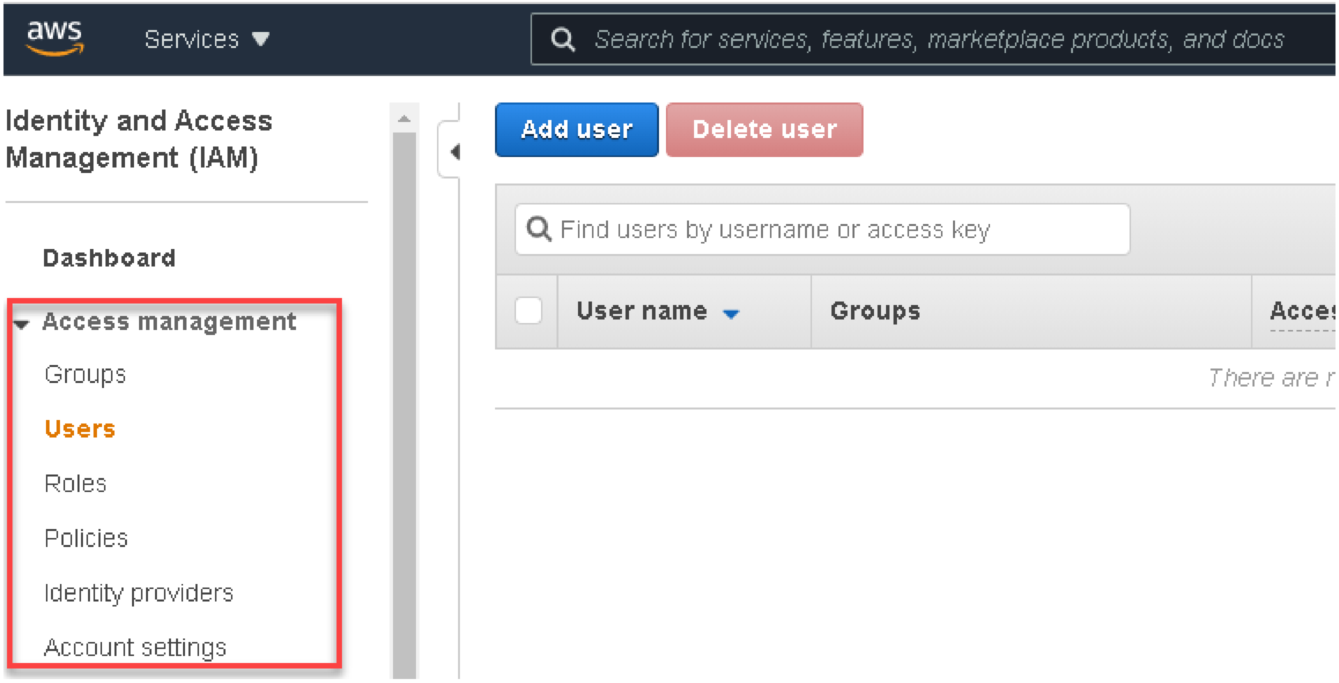
Alternatively, you can type the secret key. Show secret key

3. **Type two consecutive MFA codes below**

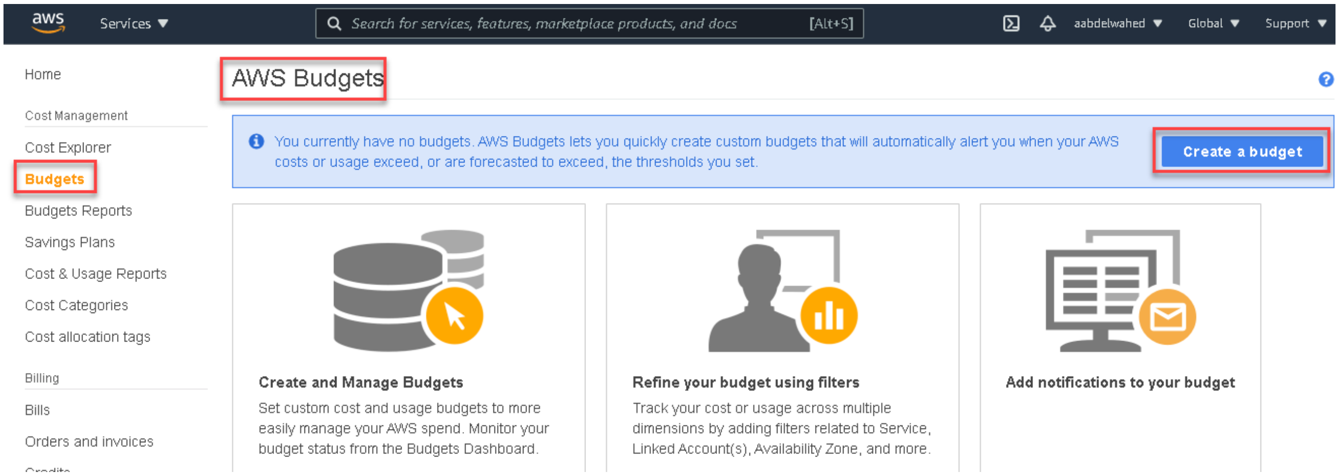
MFA code 1: 902[redacted]

MFA code 2: 505[redacted]

Create Users and Groups



Cost Alerts



You currently have no budgets. AWS Budgets lets you quickly create custom budgets that will automatically alert you when your AWS costs or usage exceed, or are forecasted to exceed, the thresholds you set.

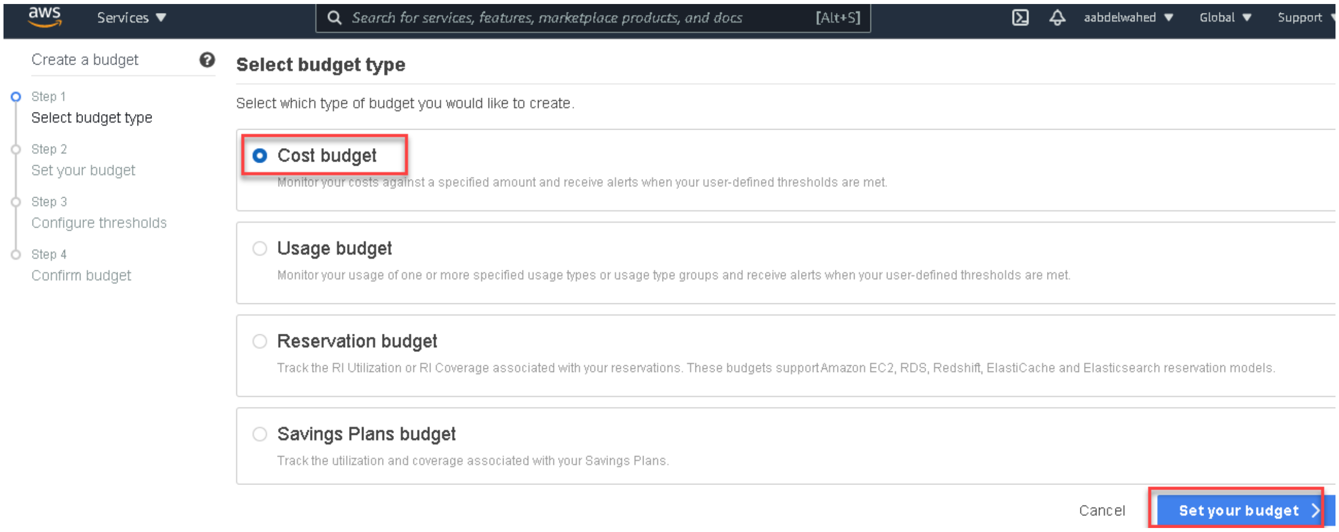
Create and Manage Budgets

Set custom cost and usage budgets to more easily manage your AWS spend. Monitor your budget status from the Budgets Dashboard.

Refine your budget using filters

Track your cost or usage across multiple dimensions by adding filters related to Service, Linked Account(s), Availability Zone, and more.

Add notifications to your budget


aws
Services ▼
Search for services, features, marketplace products, and docs [Alt+S]
aabdelwahed ▼
Global ▼
Support ▼

Create a budget

Step 1
Select budget type

Step 2
Set your budget

Step 3
Configure thresholds

Step 4
Confirm budget

Select budget type

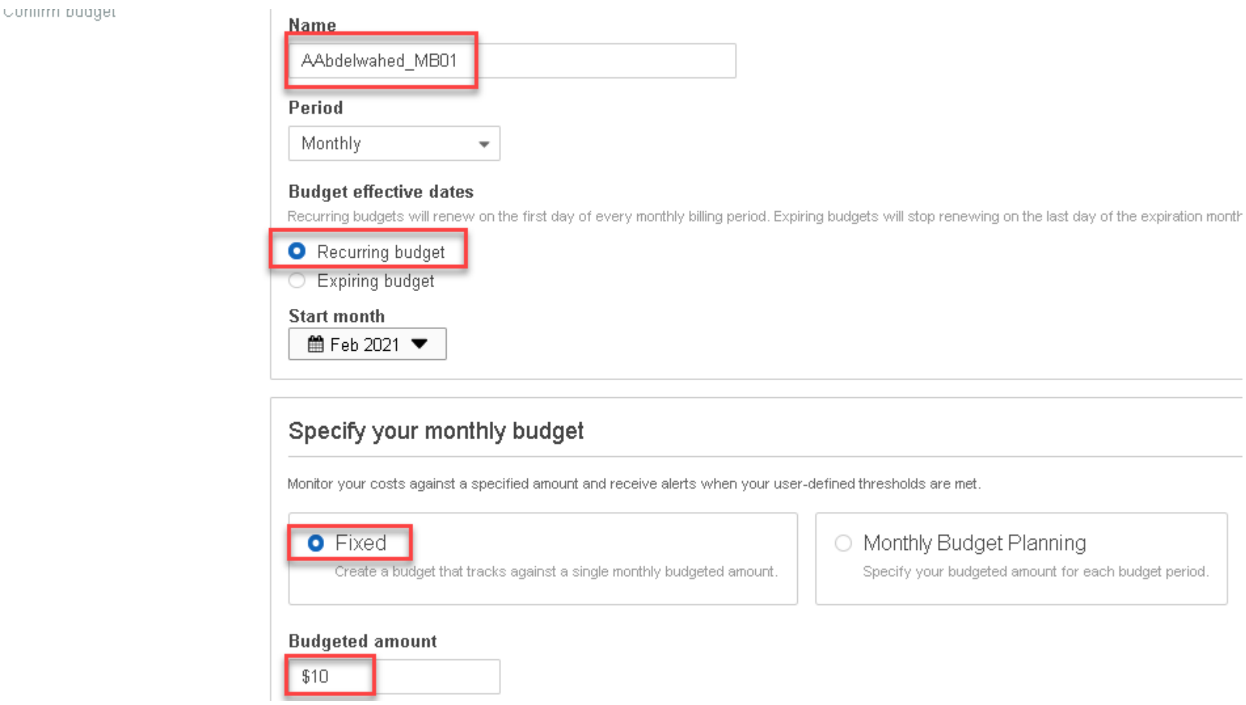
Select which type of budget you would like to create.

● Cost budget
Monitor your costs against a specified amount and receive alerts when your user-defined thresholds are met.

○ Usage budget
Monitor your usage of one or more specified usage types or usage type groups and receive alerts when your user-defined thresholds are met.

○ Reservation budget
Track the RI Utilization or RI Coverage associated with your reservations. These budgets support Amazon EC2, RDS, Redshift, ElastiCache and Elasticsearch reservation models.

○ Savings Plans budget
Track the utilization and coverage associated with your Savings Plans.



Name
AAbdelwahed_MB01

Period
Monthly

Budget effective dates
Recurring budgets will renew on the first day of every monthly billing period. Expiring budgets will stop renewing on the last day of the expiration month

● Recurring budget
○ Expiring budget

Start month
Feb 2021

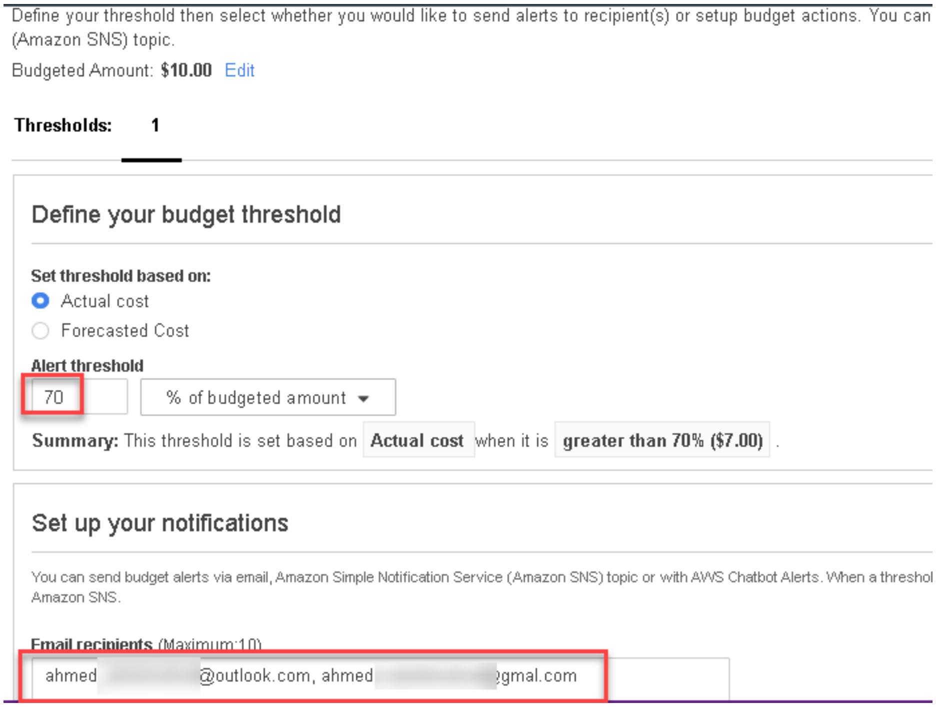
Specify your monthly budget

Monitor your costs against a specified amount and receive alerts when your user-defined thresholds are met.

● Fixed
Create a budget that tracks against a single monthly budgeted amount.

○ Monthly Budget Planning
Specify your budgeted amount for each budget period.

Budgeted amount
$10



Define your threshold then select whether you would like to send alerts to recipient(s) or setup budget actions. You can (Amazon SNS) topic.

Budgeted Amount: **$10.00** Edit

Thresholds: **1**

Define your budget threshold

Set threshold based on:

● Actual cost

○ Forecasted Cost

Alert threshold

70 | % of budgeted amount ▾

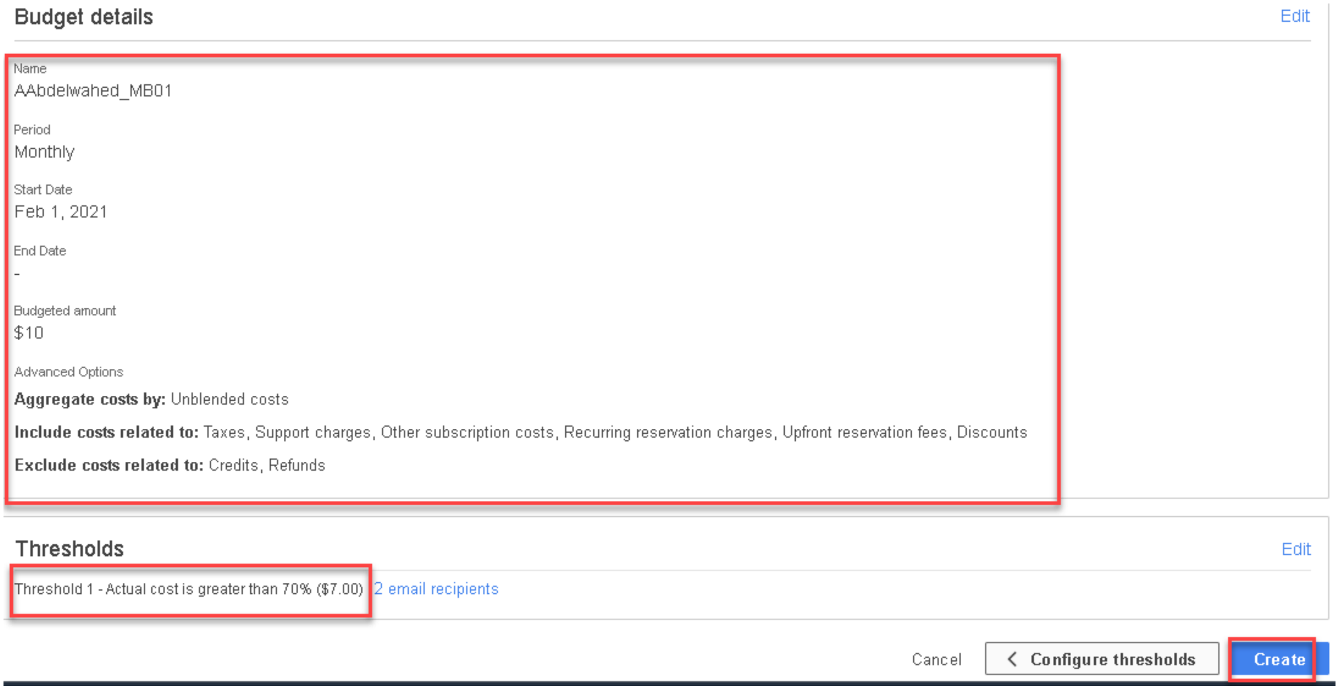
Summary: This threshold is set based on **Actual cost** when it is **greater than 70% ($7.00)** .

Set up your notifications

You can send budget alerts via email, Amazon Simple Notification Service (Amazon SNS) topic or with AWS Chatbot Alerts. When a threshol Amazon SNS.

Email recipients (Maximum:10)

ahmed [redacted]@outlook.com, ahmed [redacted]gmal.com



Budget details

Name
AAbdelwahed_MB01

Period
Monthly

Start Date
Feb 1, 2021

End Date
-

Budgeted amount
$10

Advanced Options

Aggregate costs by: Unblended costs

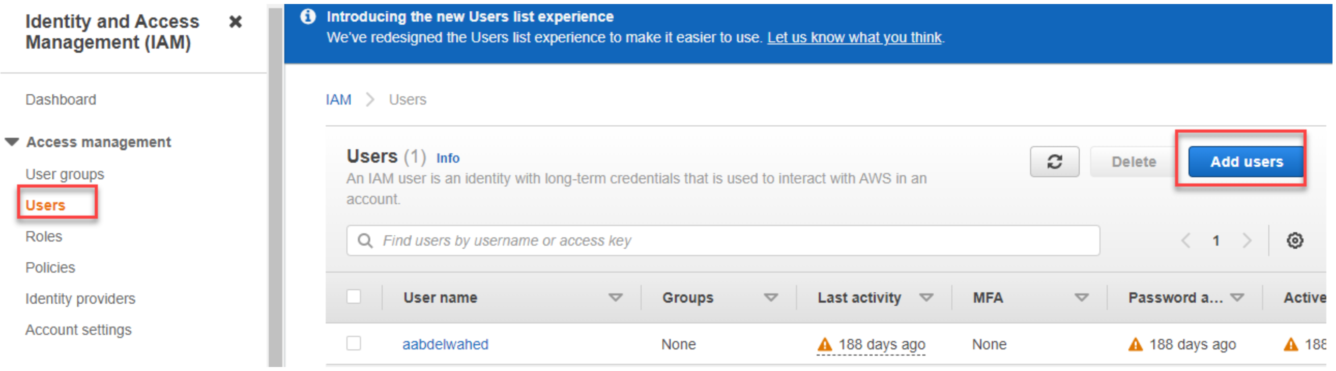
Include costs related to: Taxes, Support charges, Other subscription costs, Recurring reservation charges, Upfront reservation fees, Discounts

Exclude costs related to: Credits, Refunds

Thresholds

Threshold 1 - Actual cost is greater than 70% ($7.00) 2 email recipients

Set up a New Account and allocate a role to him.



Introducing the new Users list experience
We've redesigned the Users list experience to make it easier to use. Let us know what you think.

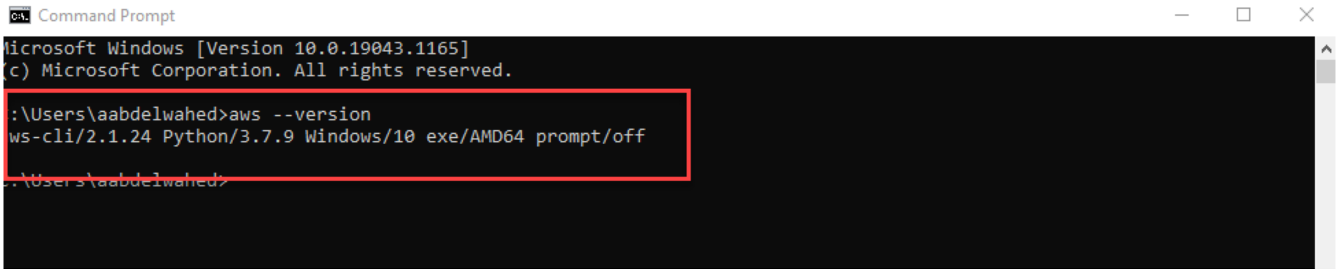
Users (1) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

□	User name	Groups	Last activity	MFA	Password a...	Active
□	aabdelwahed	None	⚠ 188 days ago	None	⚠ 188 days ago	⚠ 188

Please proceed by taking a few straightforward actions to establish a password and allocate specific permissions via the policy tab.

AWS access using console or CLI

To install the AWS CLI on Windows, simply search for "install AWS CLI on Windows" and follow the installation instructions. Once installed, open the command prompt to confirm the installation was successful.



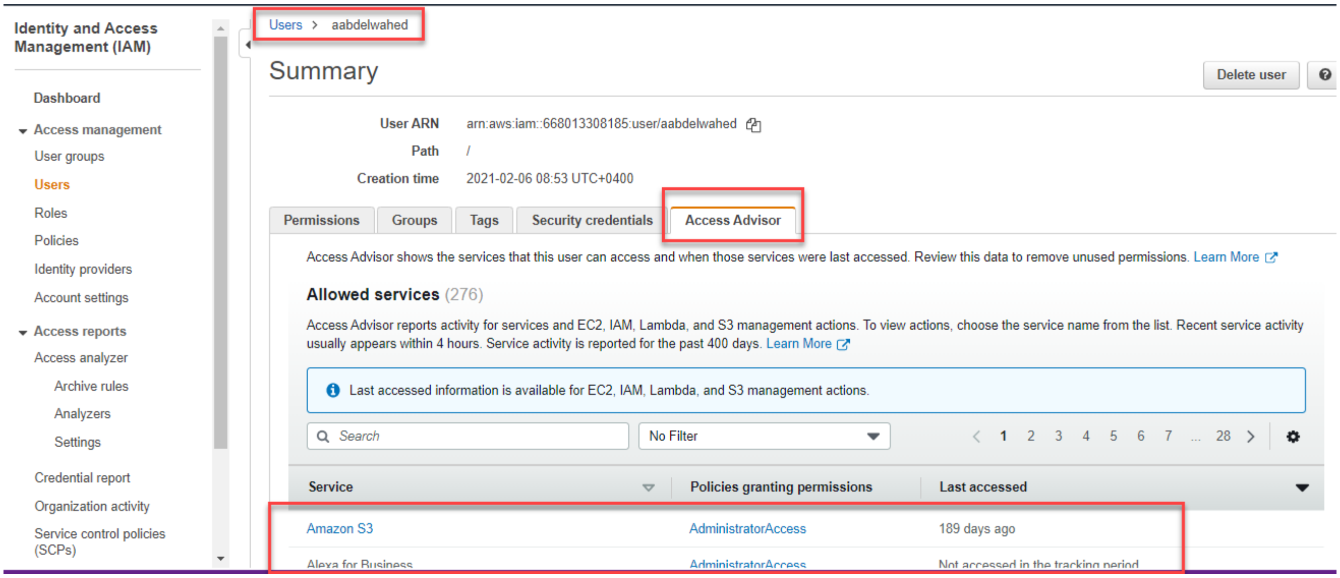
```
icrosoft Windows [Version 10.0.19043.1165]
c) Microsoft Corporation. All rights reserved.

:\Users\aabdelwahed>aws --version
ws-cli/2.1.24 Python/3.7.9 Windows/10 exe/AMD64 prompt/off

:\Users\aabdelwahed>
```

Monitor user actions

1- Choosing that user



Summary

User ARN arn:aws:iam::668013308185:user/aabdelwahed

Path /

Creation time 2021-02-06 08:53 UTC+0400

Access Advisor shows the services that this user can access and when those services were last accessed. Review this data to remove unused permissions. Learn More

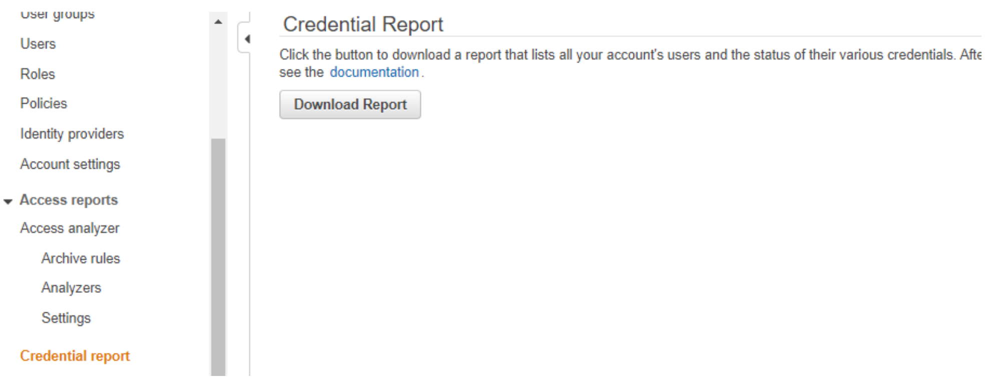
Allowed services (276)

Access Advisor reports activity for services and EC2, IAM, Lambda, and S3 management actions. To view actions, choose the service name from the list. Recent service activity usually appears within 4 hours. Service activity is reported for the past 400 days. Learn More

Last accessed information is available for EC2, IAM, Lambda, and S3 management actions.

Service	Policies granting permissions	Last accessed
Amazon S3	AdministratorAccess	189 days ago
Alexa for Business	AdministratorAccess	Not accessed in the tracking period

2- Credential Summary



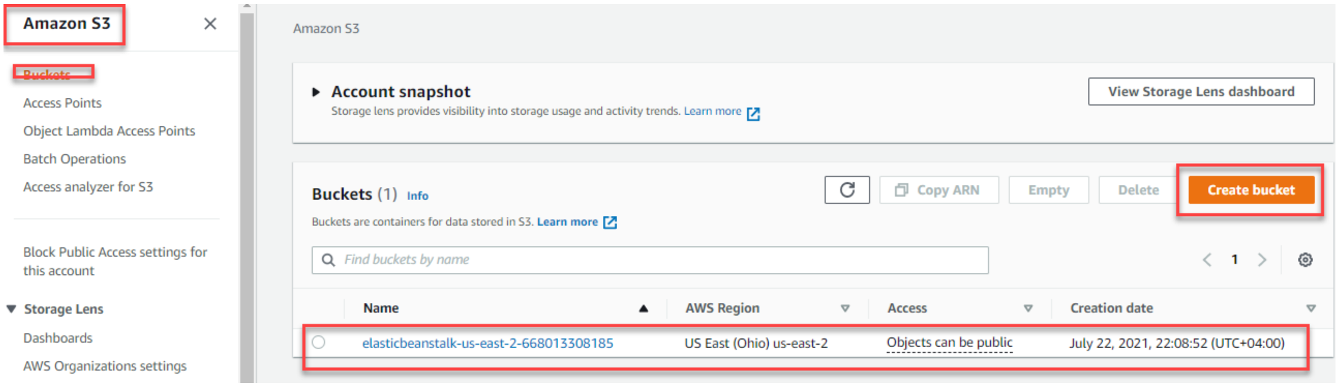
Credential Report

Click the button to download a report that lists all your account's users and the status of their various credentials. Afte see the documentation.

Working with Storage

S3 Buckets and Objects - Hands On

Navigate to S3 for bucket viewing or creation.



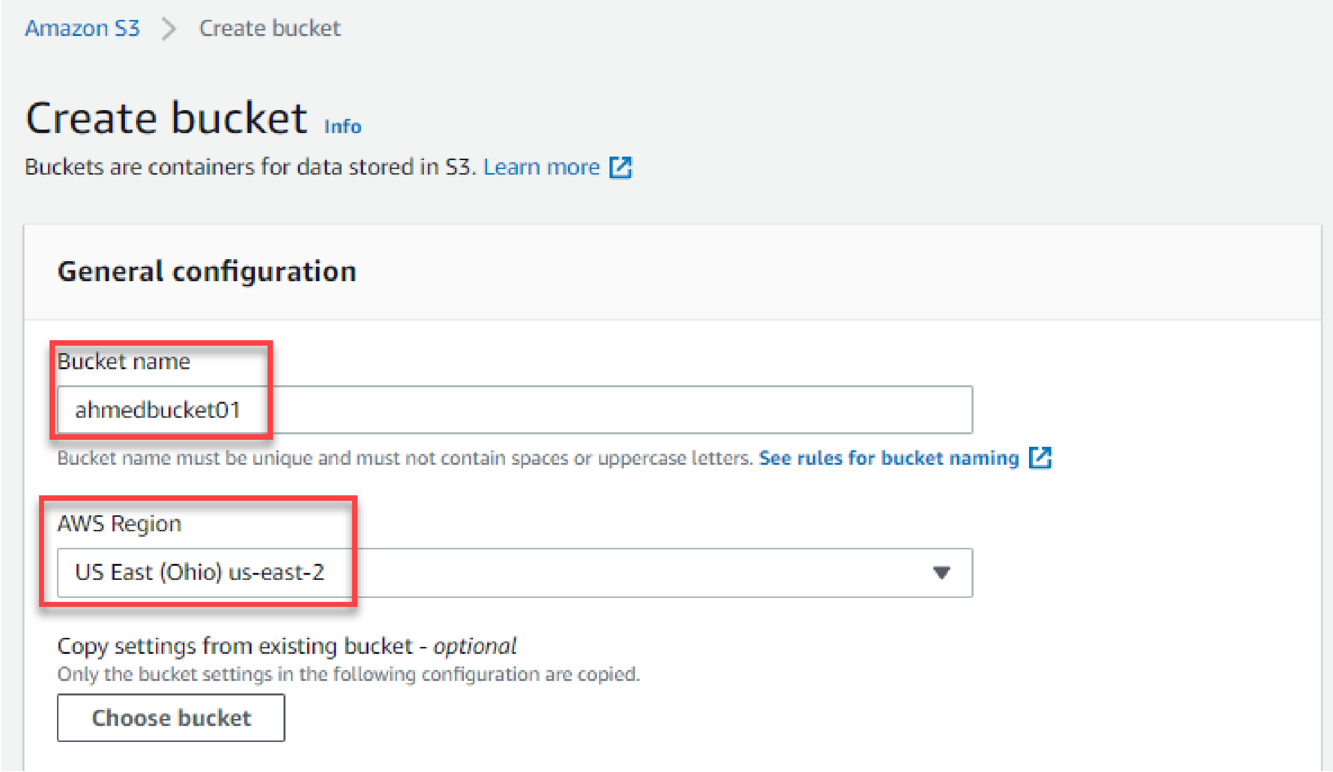
Storage lens provides visibility into storage usage and activity trends. Learn more

Buckets (1)

Buckets are containers for data stored in S3. Learn more

Name	AWS Region	Access	Creation date
elasticbeanstalk-us-east-2-668013308185	US East (Ohio) us-east-2	Objects can be public	July 22, 2021, 22:08:52 (UTC+04:00)

The bucket name needs to be distinctive and should not contain any uppercase letters.



Create bucket

Buckets are containers for data stored in S3. Learn more

General configuration

Bucket name

ahmedbucket01

Bucket name must be unique and must not contain spaces or uppercase letters. See rules for bucket naming

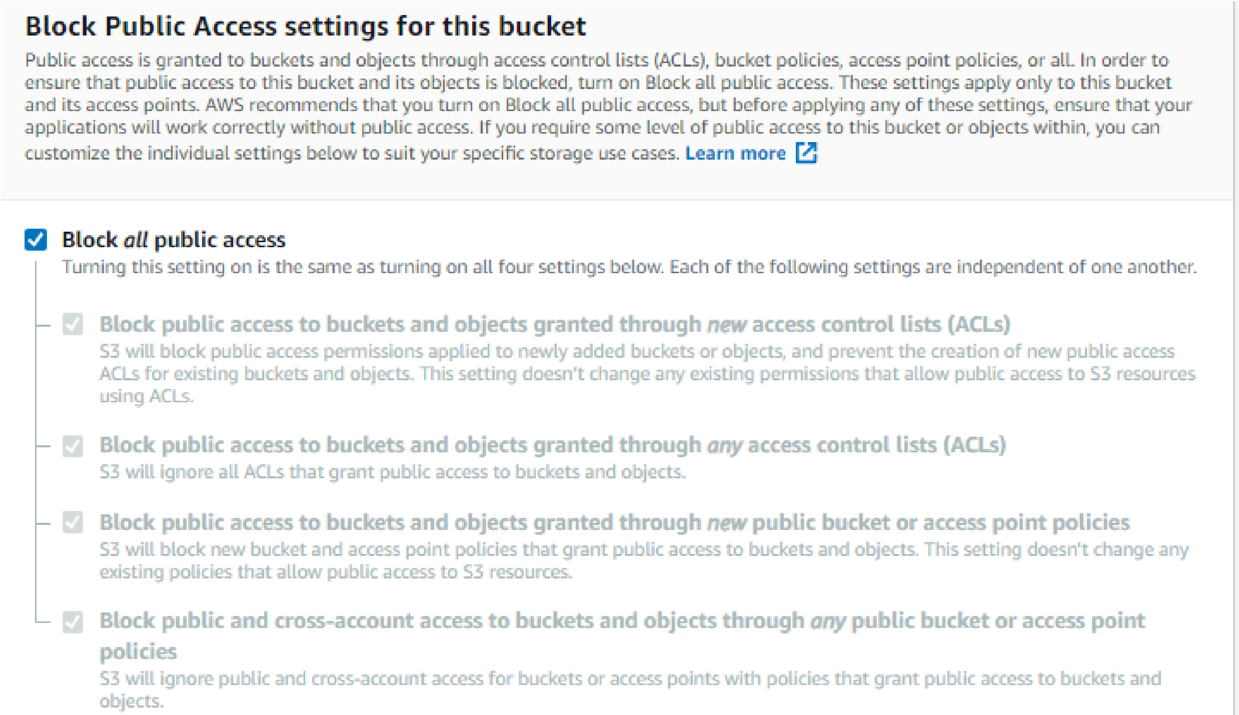
AWS Region

US East (Ohio) us-east-2

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

I'll keep the other options unchanged.

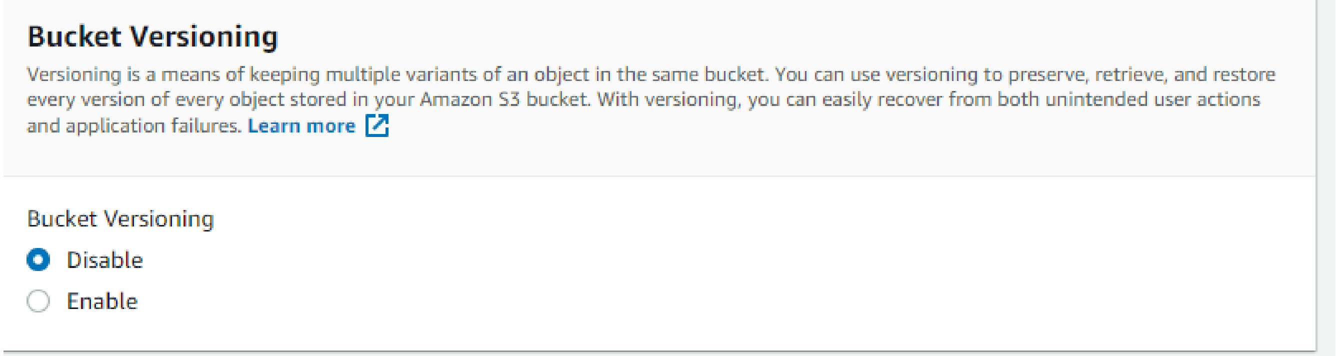


Block Public Access settings for this bucket

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



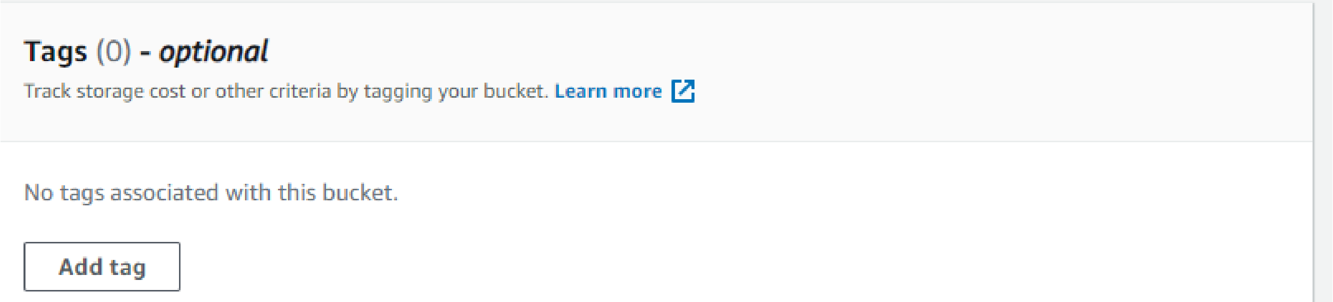
Bucket Versioning

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

Bucket Versioning

● Disable

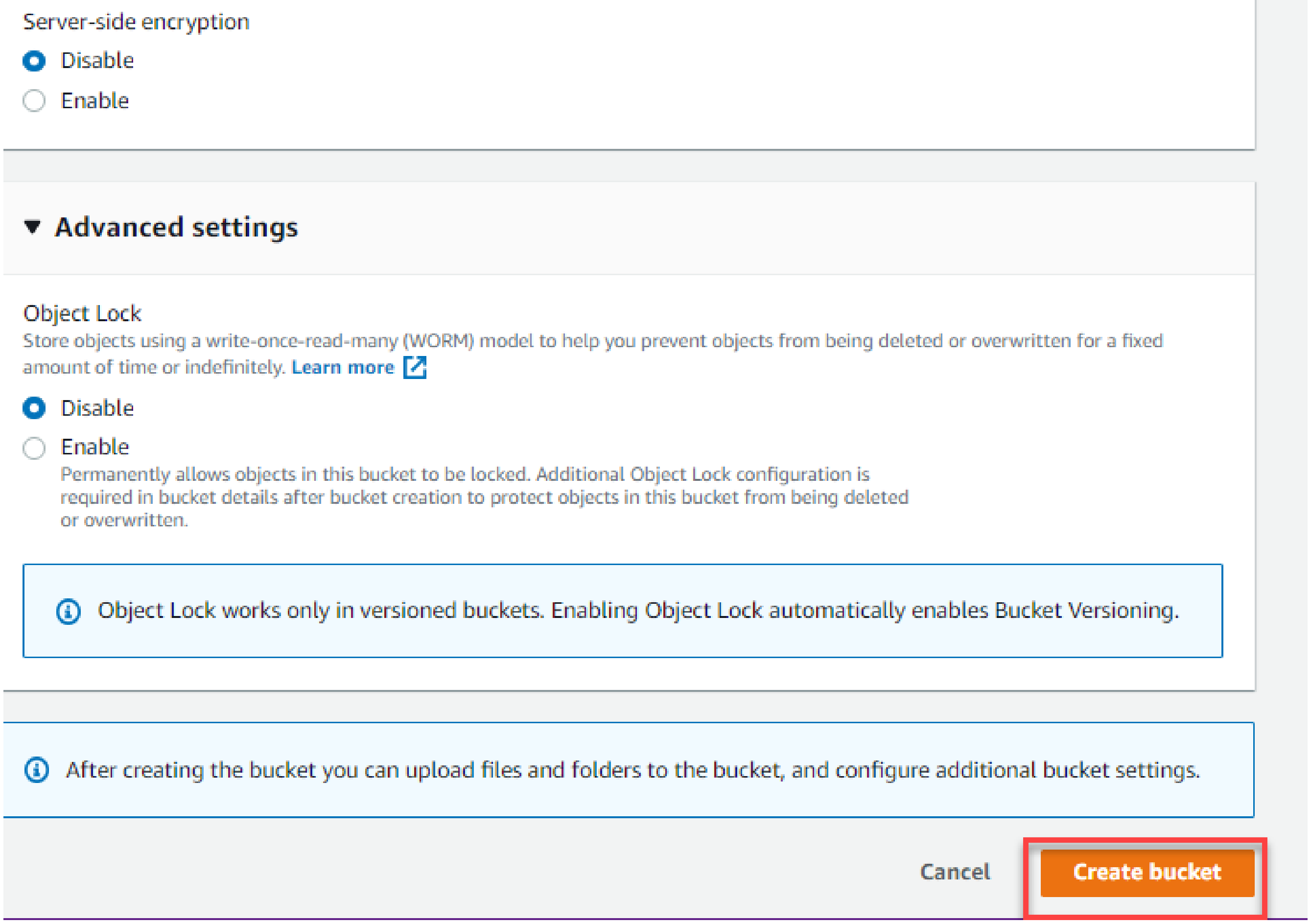
○ Enable



Tags (0) - *optional*

Track storage cost or other criteria by tagging your bucket. Learn more

No tags associated with this bucket.



Server-side encryption

● Disable

○ Enable

▼ Advanced settings

Object Lock

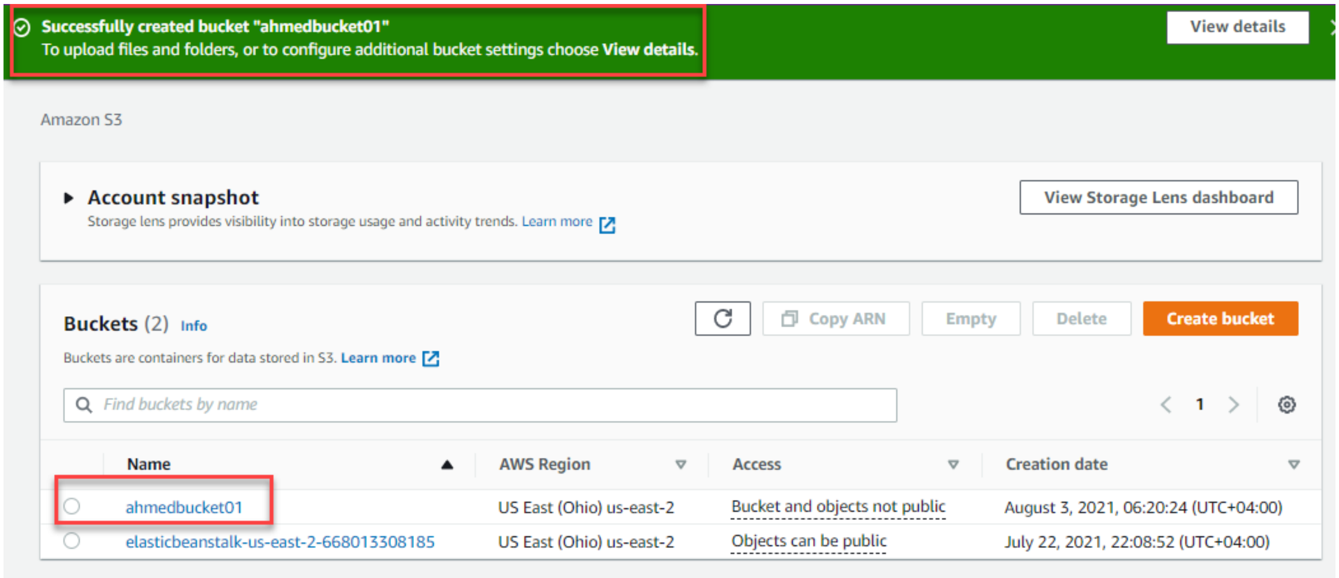
Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Learn more

● Disable

○ Enable
Permanently allows objects in this bucket to be locked. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten.

Object Lock works only in versioned buckets. Enabling Object Lock automatically enables Bucket Versioning.

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



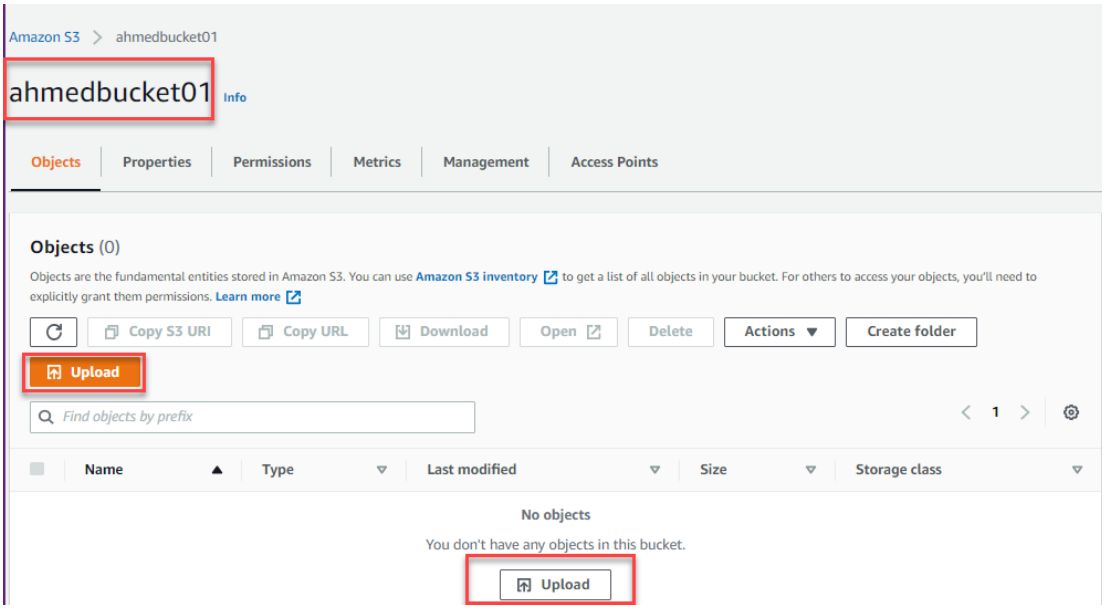
Successfully created bucket "ahmedbucket01"
To upload files and folders, or to configure additional bucket settings choose **View details**.

▶ Account snapshot
Storage lens provides visibility into storage usage and activity trends. Learn more

Buckets (2) Info
Buckets are containers for data stored in S3. Learn more

	Name	AWS Region	Access	Creation date
○	ahmedbucket01	US East (Ohio) us-east-2	Bucket and objects not public	August 3, 2021, 06:20:24 (UTC+04:00)
○	elasticbeanstalk-us-east-2-668013308185	US East (Ohio) us-east-2	Objects can be public	July 22, 2021, 22:08:52 (UTC+04:00)

Please proceed to upload your initial file into the bucket.



Amazon S3 > ahmedbucket01

ahmedbucket01 Info

Objects (0)

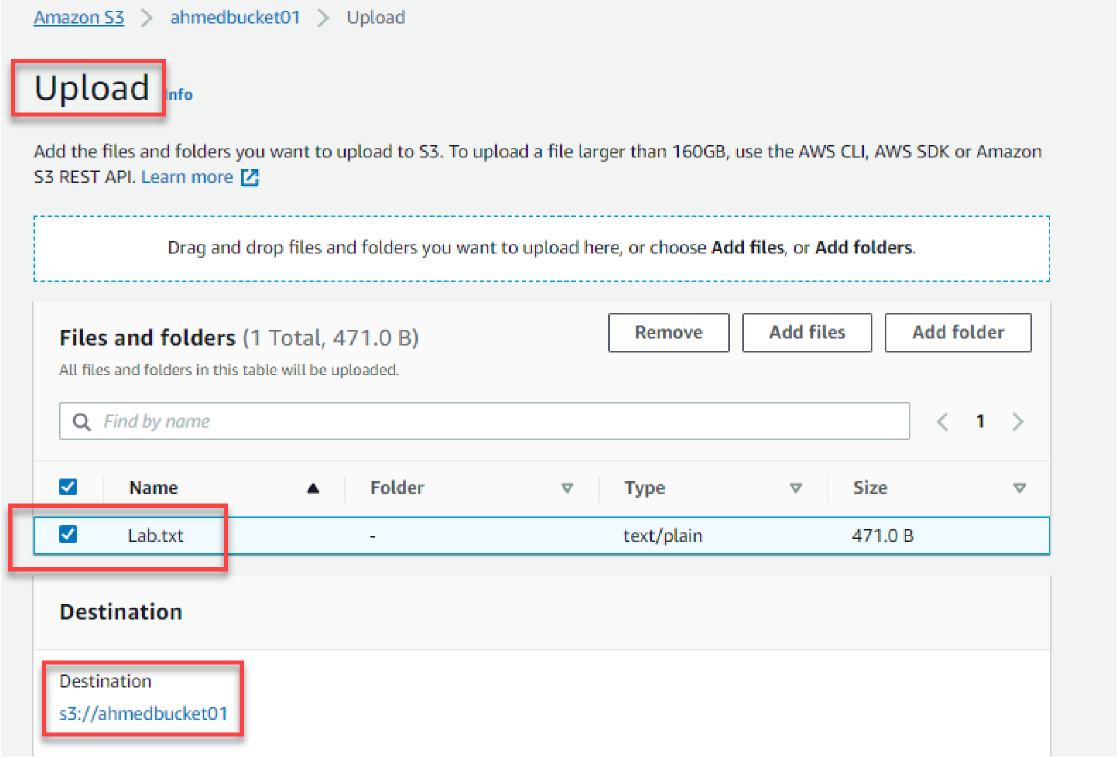
Objects are the fundamental entities stored in Amazon S3. You can use **Amazon S3 inventory** to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. **Learn more**

Name ▲	Type	Last modified	Size	Storage class

No objects

You don't have any objects in this bucket.

Select the standard settings when uploading the file.



Amazon S3 > ahmedbucket01 > Upload

Upload Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more

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

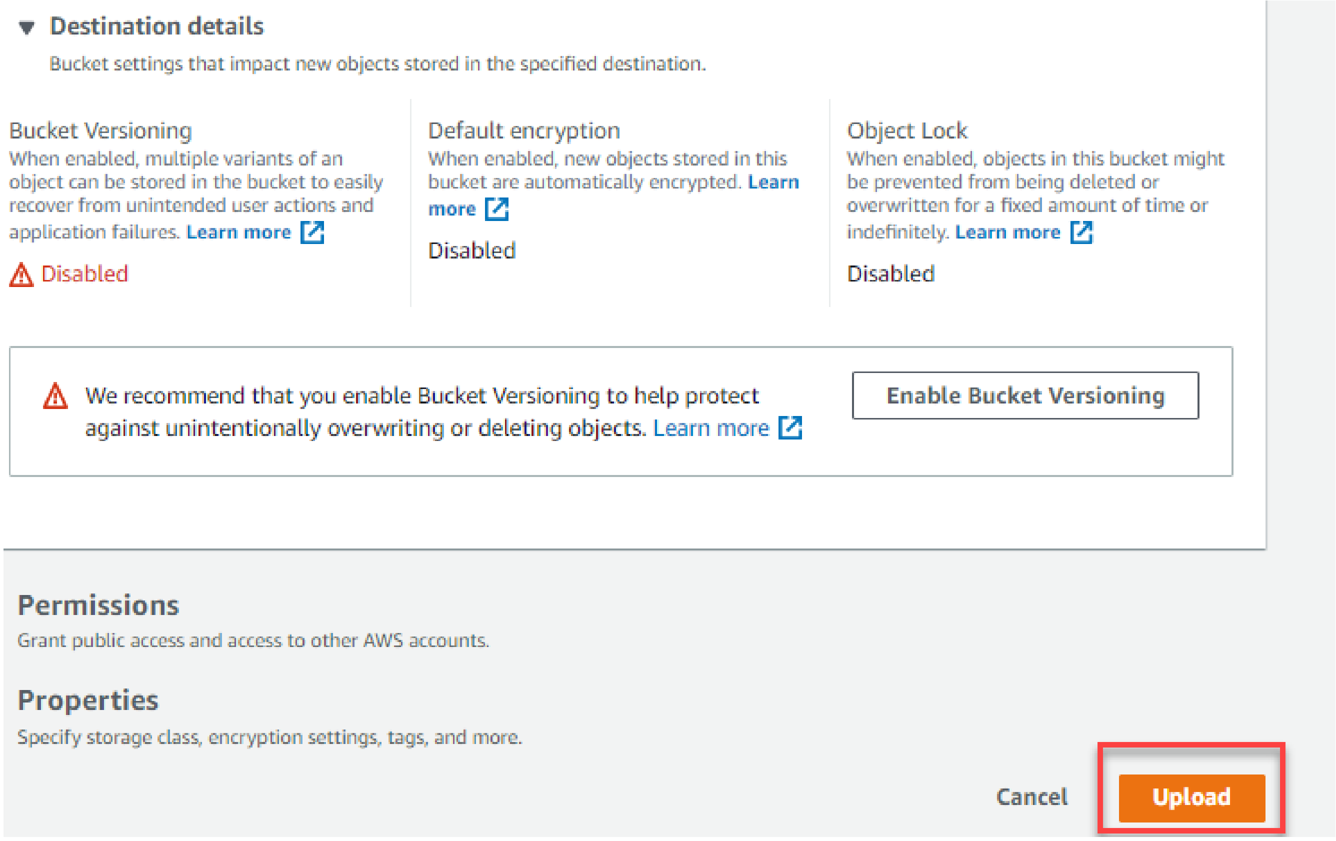
Files and folders (1 Total, 471.0 B)

All files and folders in this table will be uploaded.

☑	Name ▲	Folder	Type	Size
☑	Lab.txt	-	text/plain	471.0 B

Destination

Destination
s3://ahmedbucket01



▼ Destination details

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

Bucket Versioning

When enabled, multiple variants of an object can be stored in the bucket to easily recover from unintended user actions and application failures. Learn more

⚠ Disabled

Default encryption

When enabled, new objects stored in this bucket are automatically encrypted. Learn more

Disabled

Object Lock

When enabled, objects in this bucket might be prevented from being deleted or overwritten for a fixed amount of time or indefinitely. Learn more

Disabled

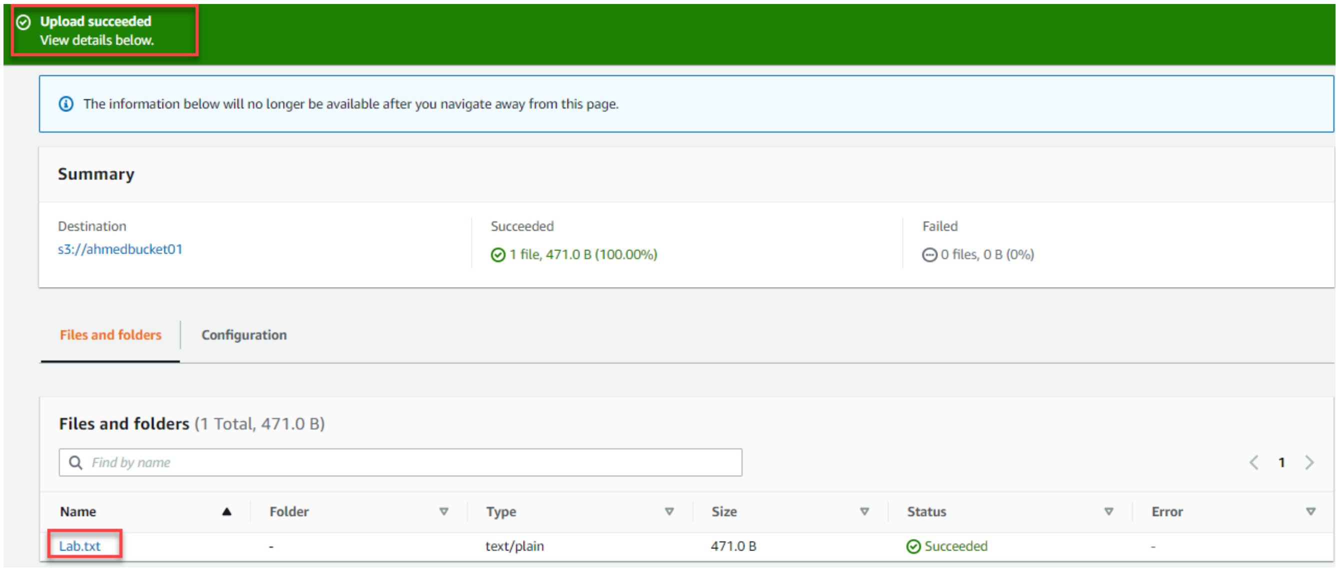
⚠ We recommend that you enable Bucket Versioning to help protect against unintentionally overwriting or deleting objects. Learn more

Permissions

Grant public access and access to other AWS accounts.

Properties

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



Upload succeeded
View details below.

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

Summary

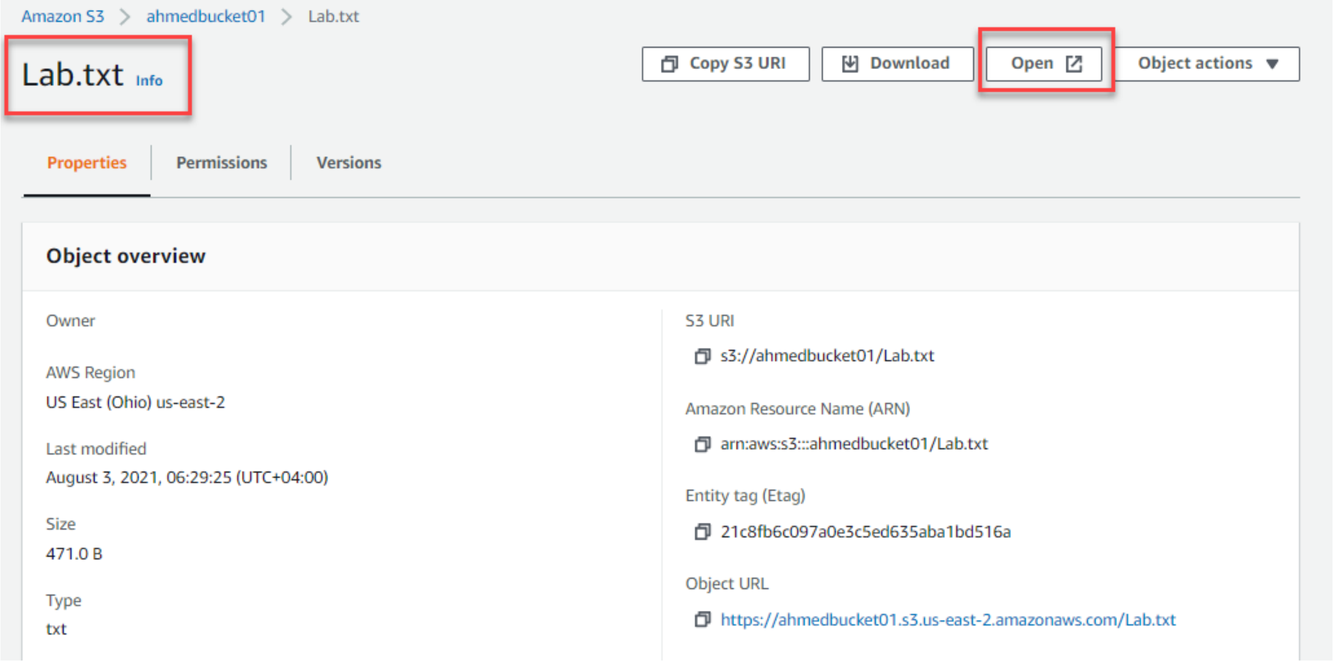
Destination	Succeeded	Failed
s3://ahmedbucket01	1 file, 471.0 B (100.00%)	0 files, 0 B (0%)

Files and folders (1 Total, 471.0 B)

Name	Folder	Type	Size	Status	Error
Lab.txt	-	text/plain	471.0 B	Succeeded	-

There are two methods to open this file.

1st



Object overview

Owner

AWS Region
US East (Ohio) us-east-2

Last modified
August 3, 2021, 06:29:25 (UTC+04:00)

Size
471.0 B

Type
txt

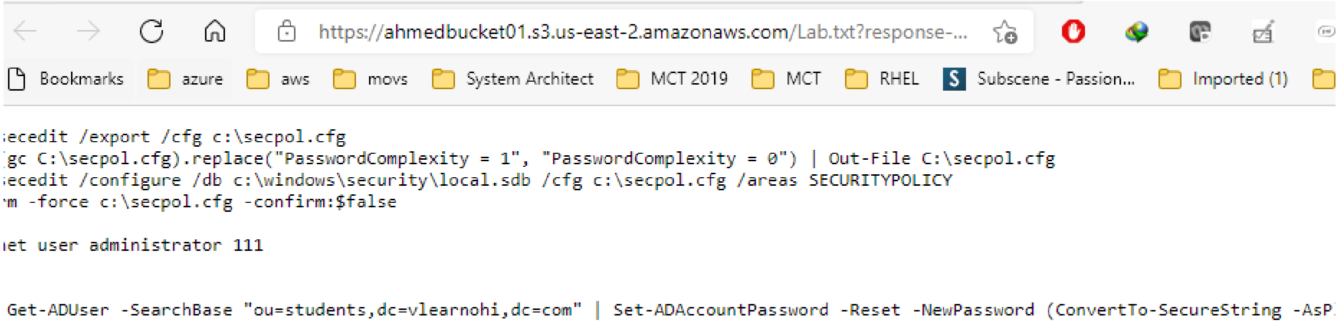
S3 URI
s3://ahmedbucket01/Lab.txt

Amazon Resource Name (ARN)
arn:aws:s3:::ahmedbucket01/Lab.txt

Entity tag (Etag)
21c8fb6c097a0e3c5ed635aba1bd516a

Object URL
https://ahmedbucket01.s3.us-east-2.amazonaws.com/Lab.txt

The URL mentioned is referred to as a pre-signed URL.

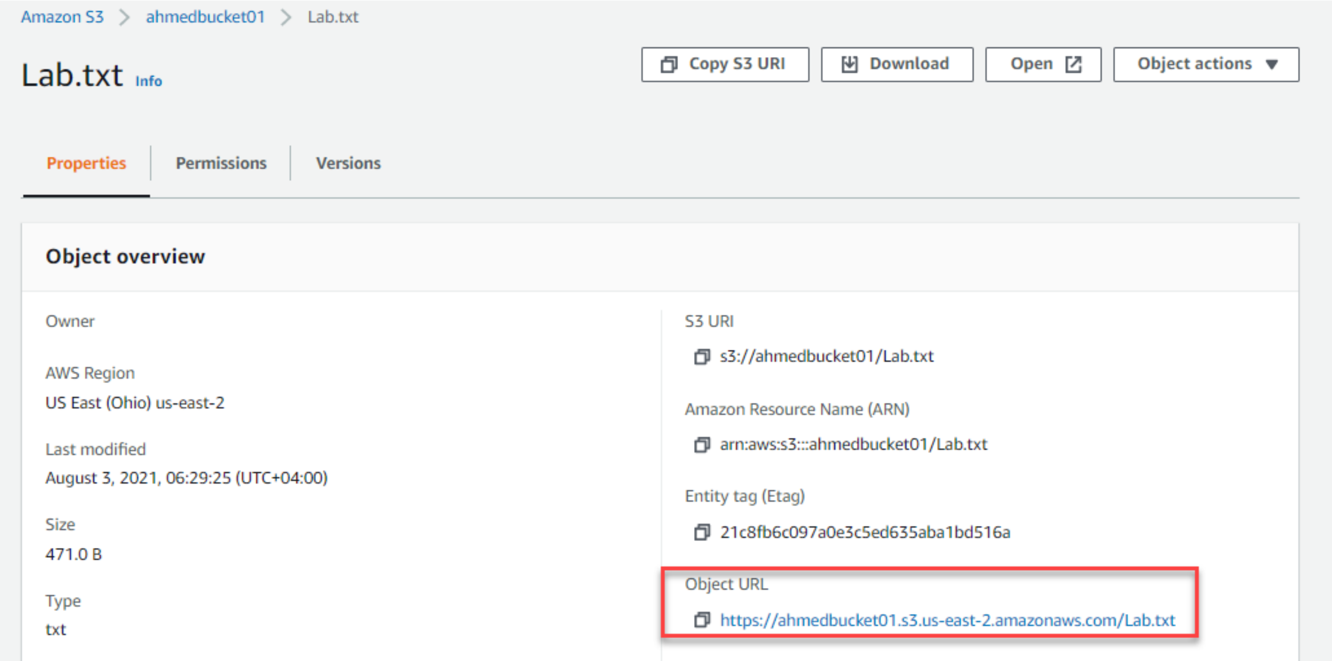


```
ecedit /export /cfg c:\secpol.cfg
gc C:\secpol.cfg).replace("PasswordComplexity = 1", "PasswordComplexity = 0") | Out-File C:\secpol.cfg
ecedit /configure /db c:\windows\security\local.sdb /cfg c:\secpol.cfg /areas SECURITYPOLICY
m -force c:\secpol.cfg -confirm:$false

et user administrator 111


Get-ADUser -SearchBase "ou=students,dc=vlearnohi,dc=com" | Set-ADAccountPassword -Reset -NewPassword (ConvertTo-SecureString -AsP
```

2nd



Object overview

Owner

AWS Region
US East (Ohio) us-east-2

Last modified
August 3, 2021, 06:29:25 (UTC+04:00)

Size
471.0 B

Type
txt

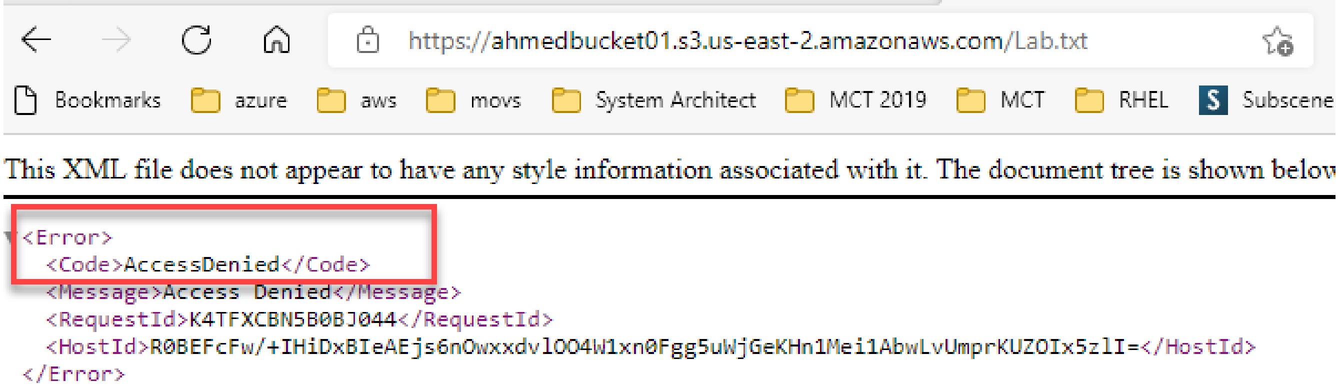
S3 URI
s3://ahmedbucket01/Lab.txt

Amazon Resource Name (ARN)
arn:aws:s3:::ahmedbucket01/Lab.txt

Entity tag (Etag)
21c8fb6c097a0e3c5ed635aba1bd516a

Object URL
https://ahmedbucket01.s3.us-east-2.amazonaws.com/Lab.txt

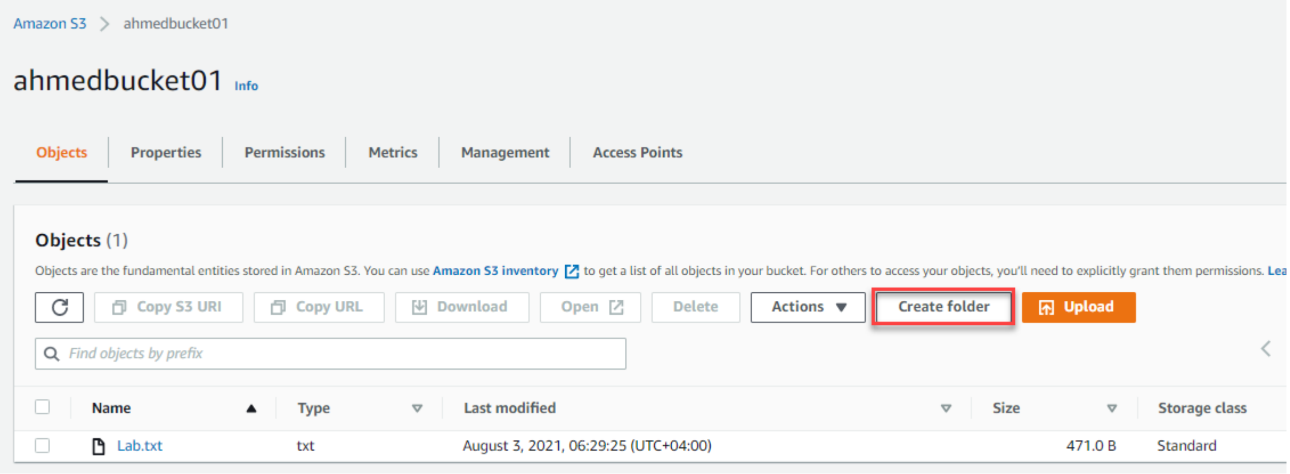
As we restrict all public access to the bucket during setup, the subsequent error occurs.



This XML file does not appear to have any style information associated with it. The document tree is shown below

```
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>K4TFXCBN5B0BJ044</RequestId>
  <HostId>R0BEFcFw/+IHiDxBIeAEjs6nOwxxdvlOO4W1xn0Fgg5uWjGeKHn1Mei1AbwLvUmprKUZOIx5zlI=</HostId>
</Error>
```

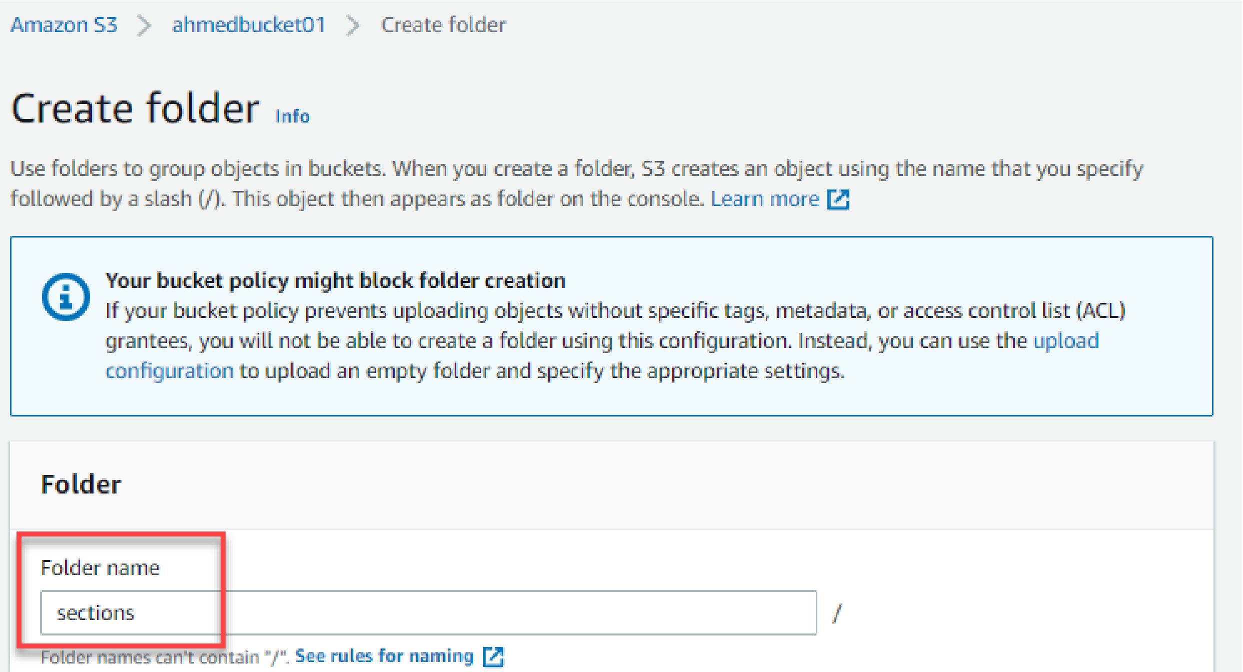
Create a subfolder in your bucket and upload the file into it.



Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use **Amazon S3 inventory** to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Lea

□	Name ▲	Type	Last modified	Size	Storage class
□	Lab.txt	txt	August 3, 2021, 06:29:25 (UTC+04:00)	471.0 B	Standard



Create folder Info

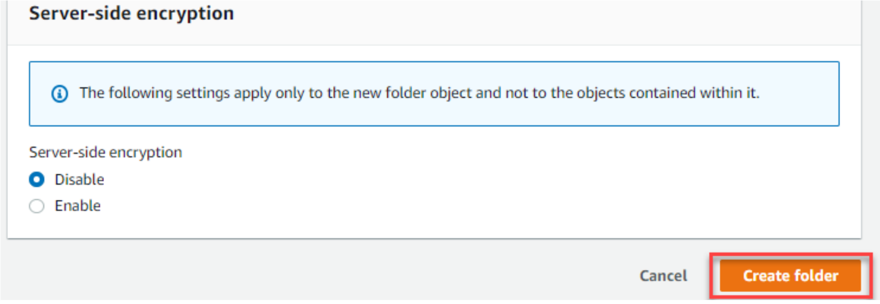
Use folders to group objects in buckets. When you create a folder, S3 creates an object using the name that you specify followed by a slash (/). This object then appears as folder on the console. Learn more

Your bucket policy might block folder creation
If your bucket policy prevents uploading objects without specific tags, metadata, or access control list (ACL) grantees, you will not be able to create a folder using this configuration. Instead, you can use the upload configuration to upload an empty folder and specify the appropriate settings.

Folder

Folder name: sections /

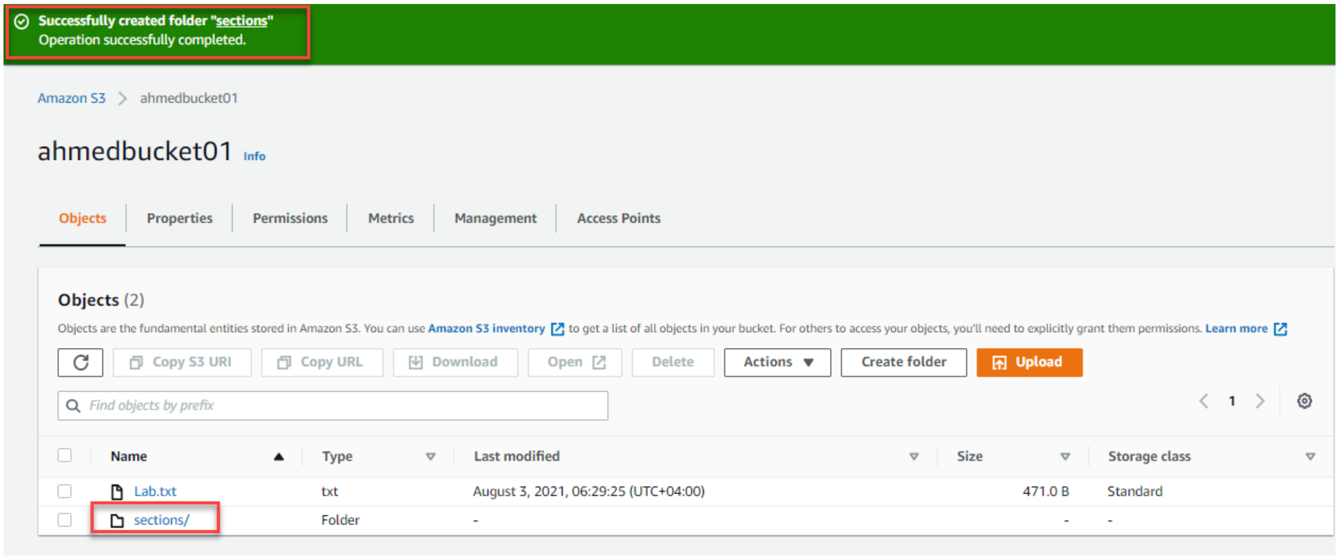
Folder names can't contain "/". See rules for naming



Server-side encryption

The following settings apply only to the new folder object and not to the objects contained within it.

Server-side encryption
● Disable
○ Enable



Successfully created folder "sections"
Operation successfully completed.

Amazon S3 > ahmedbucket01

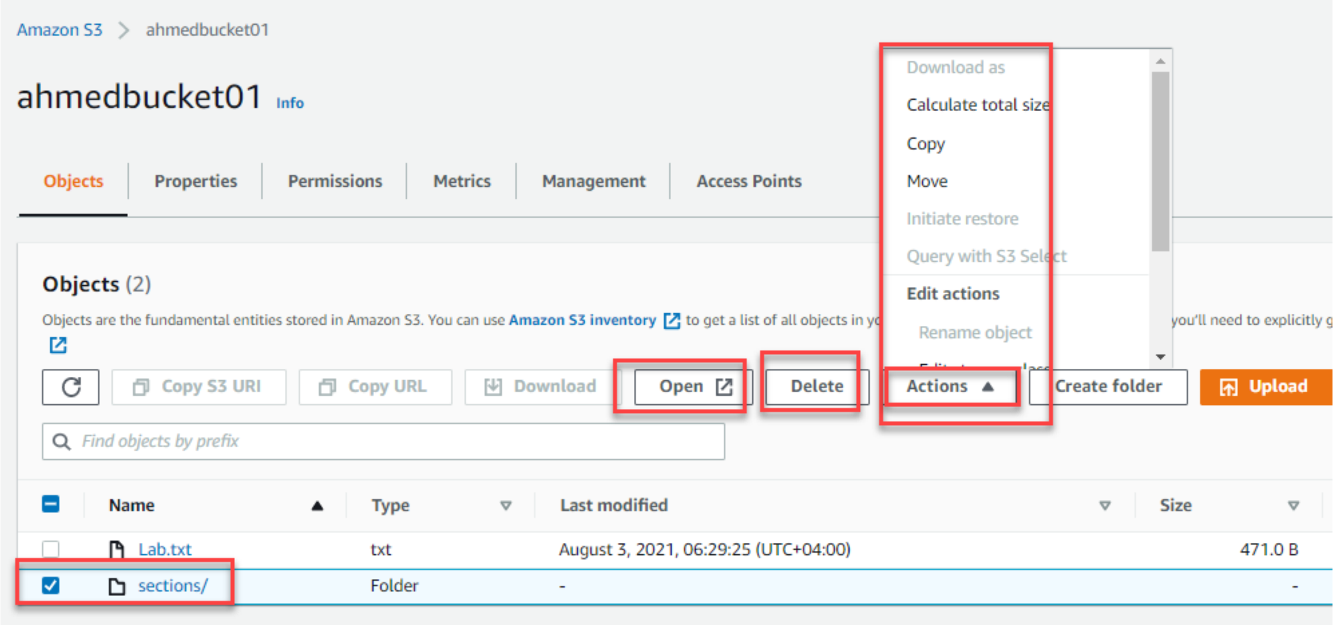
ahmedbucket01 Info

Objects (2)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

□	Name ▲	Type	Last modified	Size	Storage class
□	Lab.txt	txt	August 3, 2021, 06:29:25 (UTC+04:00)	471.0 B	Standard
□	sections/	Folder	-	-	-

you can take some action within you bucket objects



Amazon S3 > ahmedbucket01

ahmedbucket01 Info

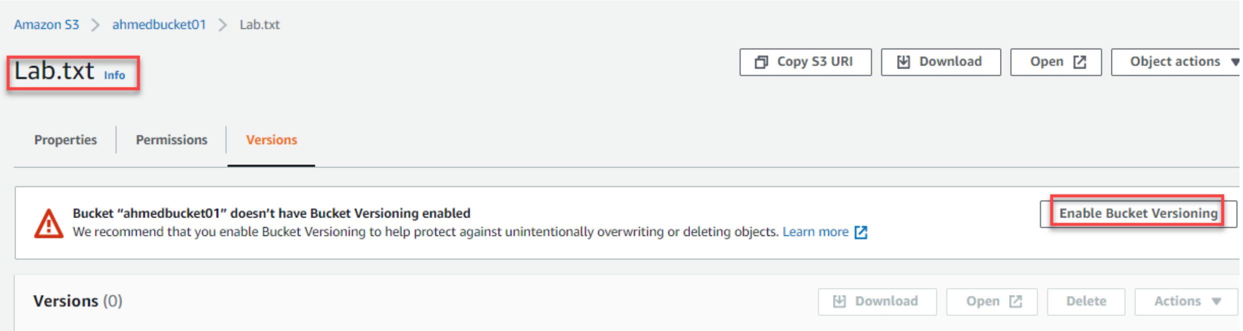
Objects (2)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in y… you'll need to explicitly g

☐	Name ▲	Type	Last modified	Size
□	Lab.txt	txt	August 3, 2021, 06:29:25 (UTC+04:00)	471.0 B
☑	sections/	Folder	-	-

S3 Versioning

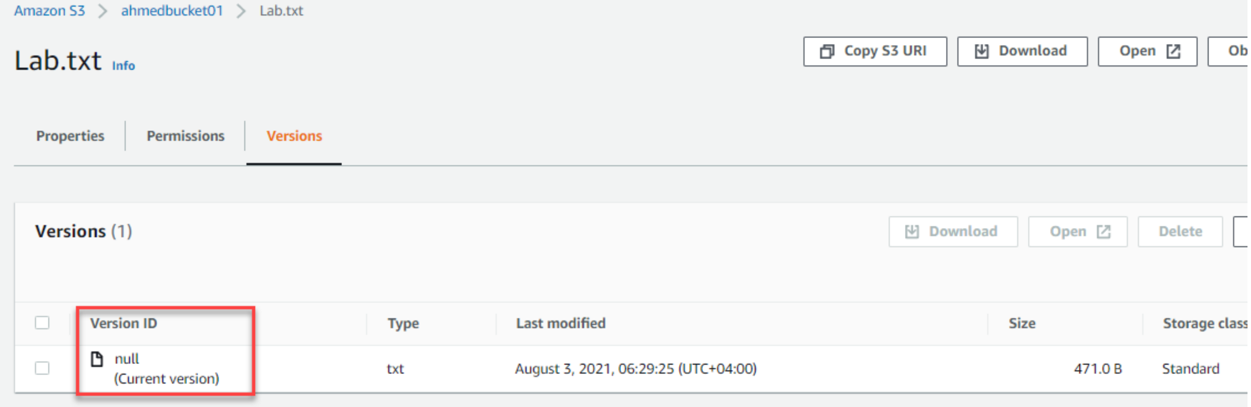
Activating Bucket Versioning safeguards against accidental overwrites or deletions of objects.



Bucket “ahmedbucket01” doesn't have Bucket Versioning enabled
We recommend that you enable Bucket Versioning to help protect against unintentionally overwriting or deleting objects. Learn more

Versions (0)

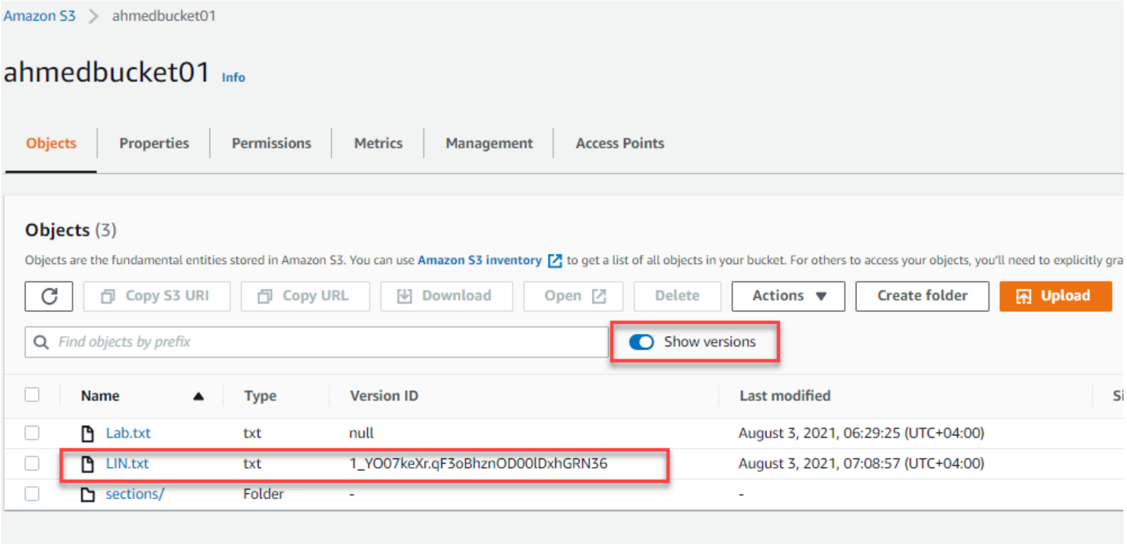
Version ID is null because we upload this object before we enable versioning



Versions (1)

□	Version ID	Type	Last modified	Size	Storage class
□	null (Current version)	txt	August 3, 2021, 06:29:25 (UTC+04:00)	471.0 B	Standard

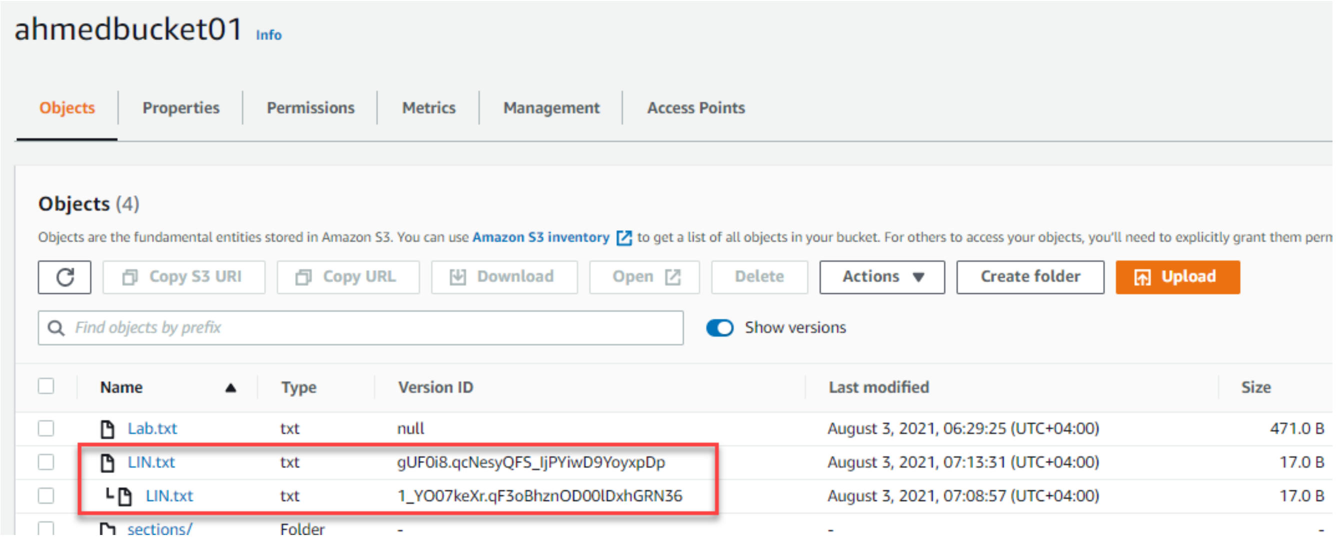
Proceed to upload an additional object; the system will automatically assign a version number.



Objects (3)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly gra

□	Name ▲	Type	Version ID	Last modified	Si
□	Lab.txt	txt	null	August 3, 2021, 06:29:25 (UTC+04:00)	
□	LIN.txt	txt	1_YO07keXr.qF3oBhznOD00lDxhGRN36	August 3, 2021, 07:08:57 (UTC+04:00)	
□	sections/	Folder	-	-	



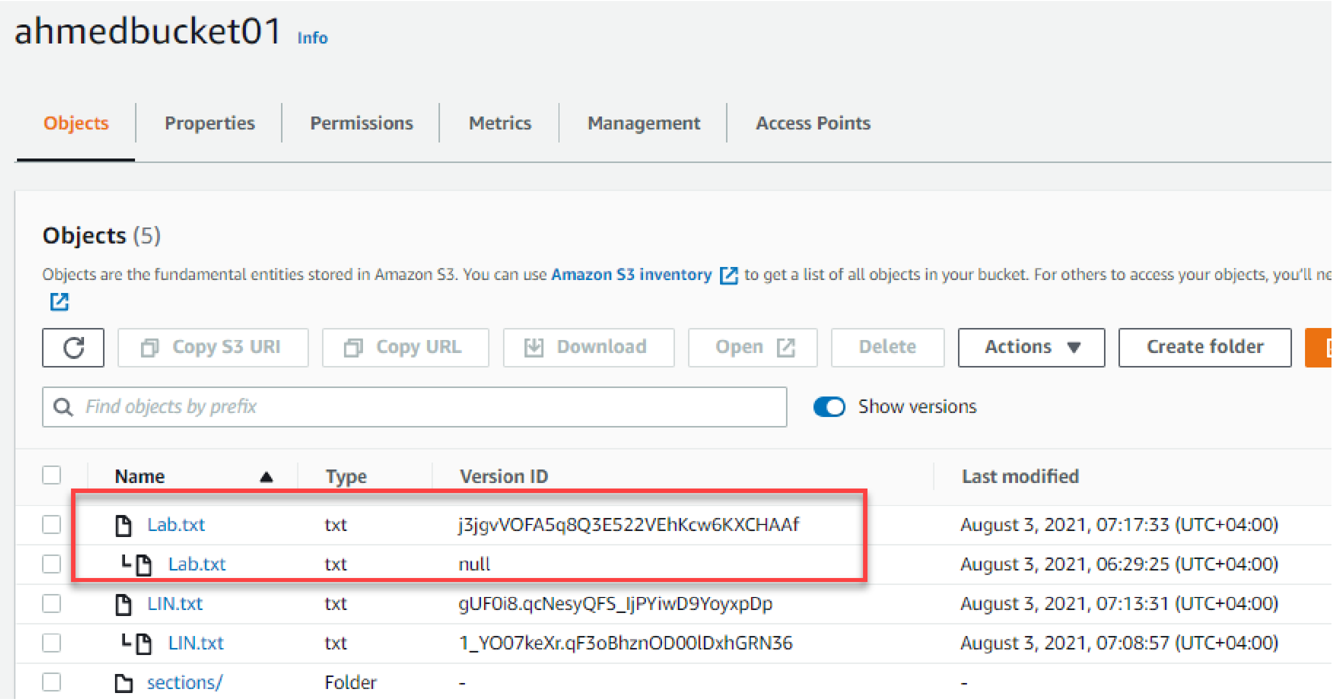
ahmedbucket01 Info

Objects (4)

Objects are the fundamental entities stored in Amazon S3. You can use **Amazon S3 inventory** to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them pern

□	Name ▲	Type	Version ID	Last modified	Size
□	Lab.txt	txt	null	August 3, 2021, 06:29:25 (UTC+04:00)	471.0 B
□	LIN.txt	txt	gUF0i8.qcNesyQFS_IjPYiwD9YoyxpDp	August 3, 2021, 07:13:31 (UTC+04:00)	17.0 B
□	└ LIN.txt	txt	1_YO07keXr.qF3oBhznOD00lDxhGRN36	August 3, 2021, 07:08:57 (UTC+04:00)	17.0 B
□	sections/	Folder	-	-	-

When another file is uploaded that contains a null version, the new file will be assigned a version number.



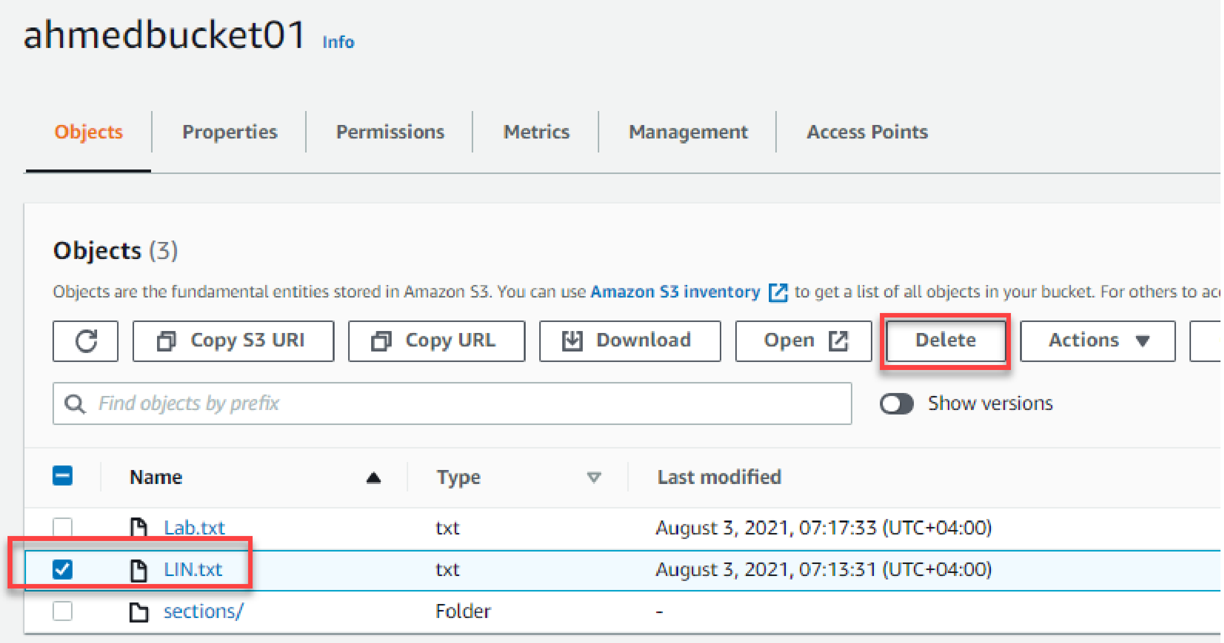
ahmedbucket01 Info

Objects (5)

Objects are the fundamental entities stored in Amazon S3. You can use **Amazon S3 inventory** to get a list of all objects in your bucket. For others to access your objects, you'll ne

□	Name ▲	Type	Version ID	Last modified
□	Lab.txt	txt	j3jgvVOFA5q8Q3E522VEhKcw6KXCHAAf	August 3, 2021, 07:17:33 (UTC+04:00)
□	└ Lab.txt	txt	null	August 3, 2021, 06:29:25 (UTC+04:00)
□	LIN.txt	txt	gUF0i8.qcNesyQFS_IjPYiwD9YoyxpDp	August 3, 2021, 07:13:31 (UTC+04:00)
□	└ LIN.txt	txt	1_YO07keXr.qF3oBhznOD00lDxhGRN36	August 3, 2021, 07:08:57 (UTC+04:00)
□	sections/	Folder	-	-

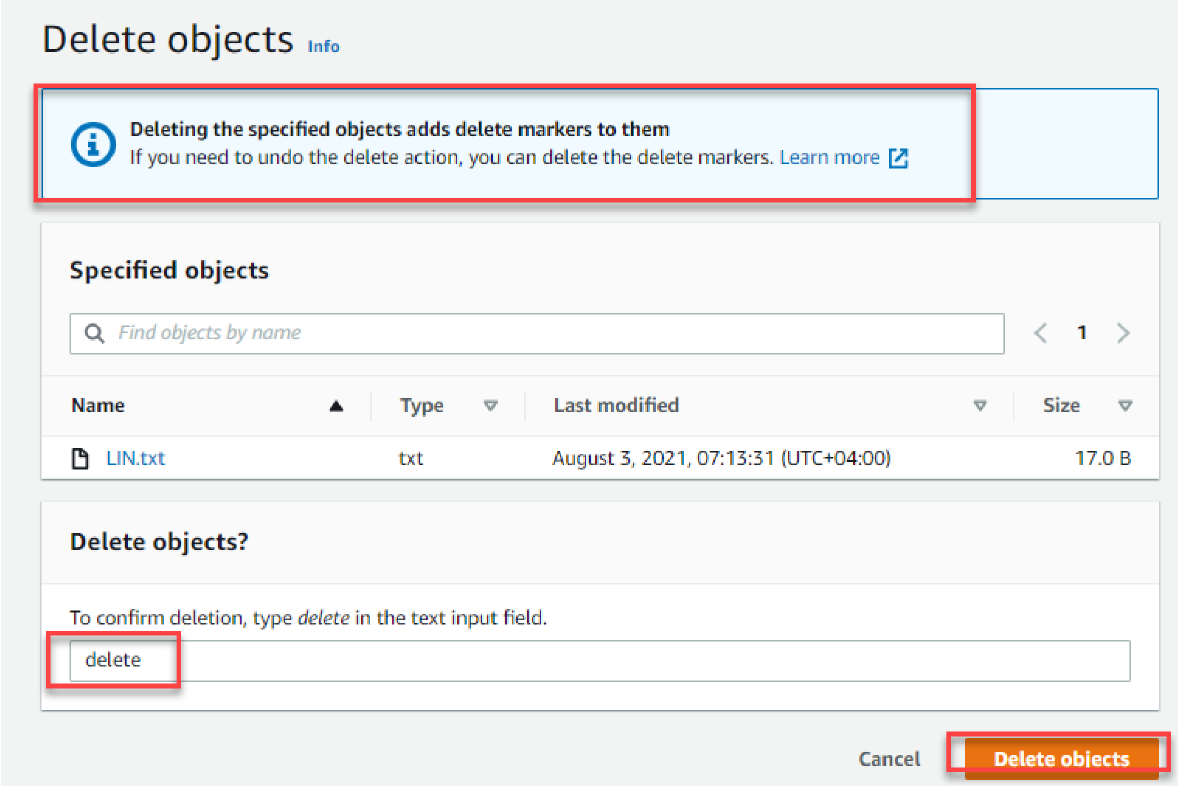
An attempt was made to delete a file holding a version, but instead of being erased, a mark indicating deletion was added.



Objects (3)

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

	Name	Type	Last modified
□	Lab.txt	txt	August 3, 2021, 07:17:33 (UTC+04:00)
☑	LIN.txt	txt	August 3, 2021, 07:13:31 (UTC+04:00)
□	sections/	Folder	-



Deleting the specified objects adds delete markers to them
If you need to undo the delete action, you can delete the delete markers. Learn more

Specified objects

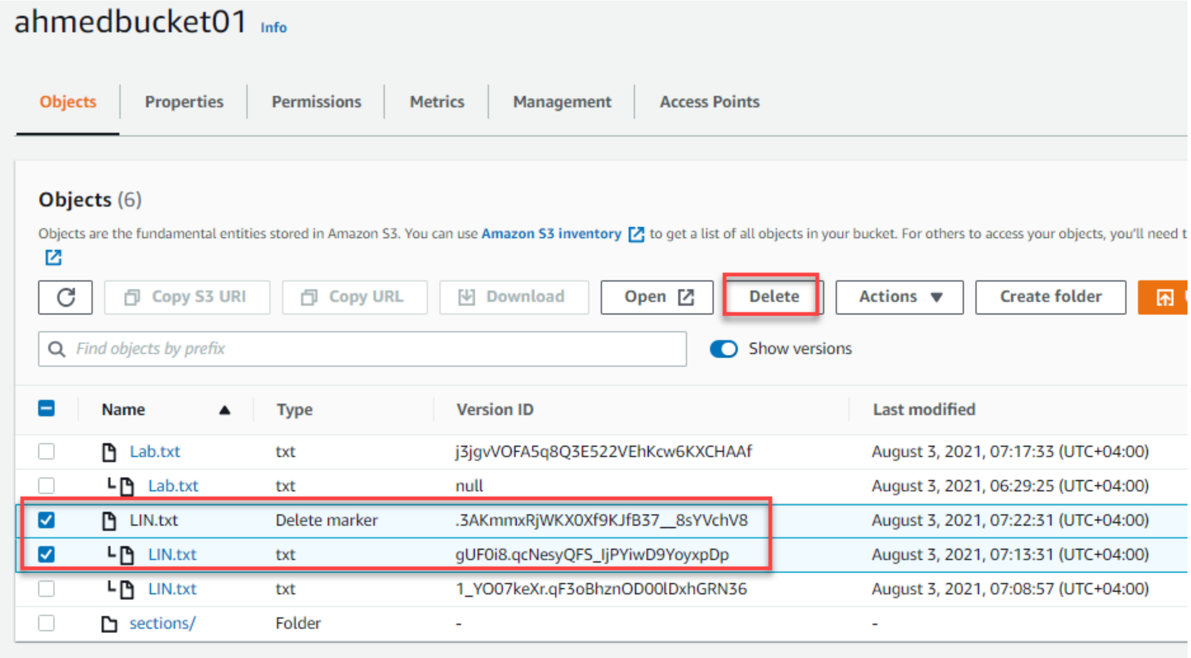
Name	Type	Last modified	Size
LIN.txt	txt	August 3, 2021, 07:13:31 (UTC+04:00)	17.0 B

Delete objects?

To confirm deletion, type *delete* in the text input field.

delete

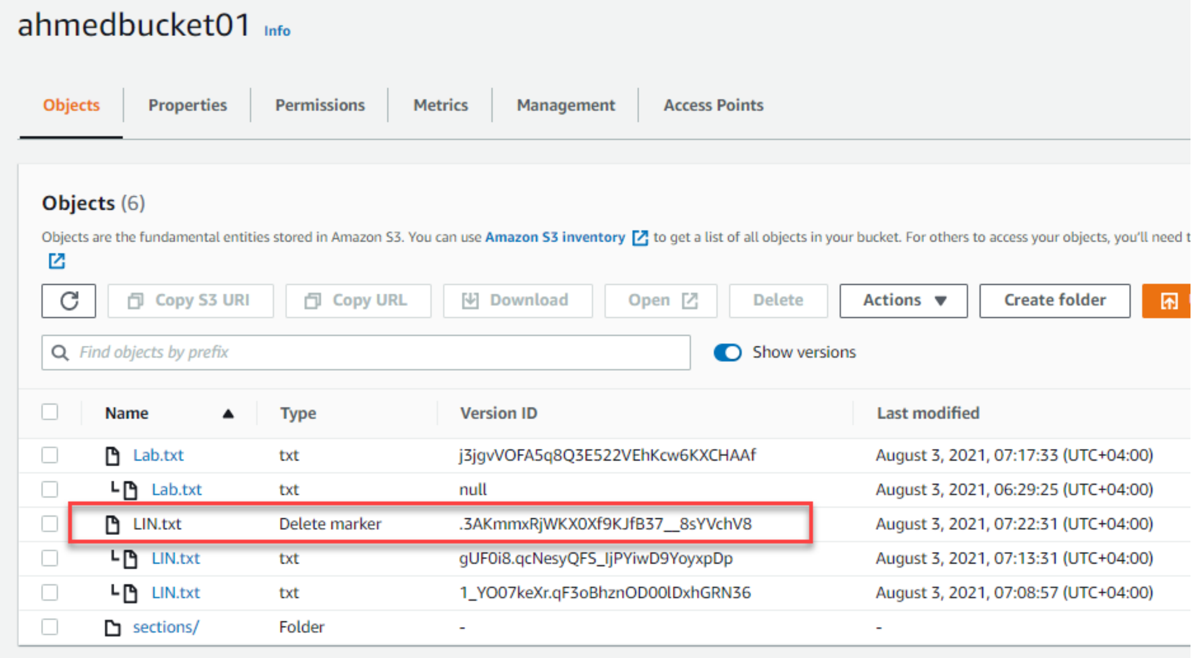
Attempt to remove once more.



Objects (6)

Objects are the fundamental entities stored in Amazon S3. You can use **Amazon S3 inventory** to get a list of all objects in your bucket. For others to access your objects, you'll need t

	Name ▲	Type	Version ID	Last modified
□	Lab.txt	txt	j3jgvVOFA5q8Q3E522VEhKcw6KXCHAAf	August 3, 2021, 07:17:33 (UTC+04:00)
□	└ Lab.txt	txt	null	August 3, 2021, 06:29:25 (UTC+04:00)
☑	LIN.txt	Delete marker	.3AKmmxRjWKX0Xf9KJfB37__8sYVchV8	August 3, 2021, 07:22:31 (UTC+04:00)
☑	└ LIN.txt	txt	gUF0i8.qcNesyQFS_IjPYiwD9YoyxpDp	August 3, 2021, 07:13:31 (UTC+04:00)
□	└ LIN.txt	txt	1_YO07keXr.qF3oBhznOD00lDxhGRN36	August 3, 2021, 07:08:57 (UTC+04:00)
□	sections/	Folder	-	-

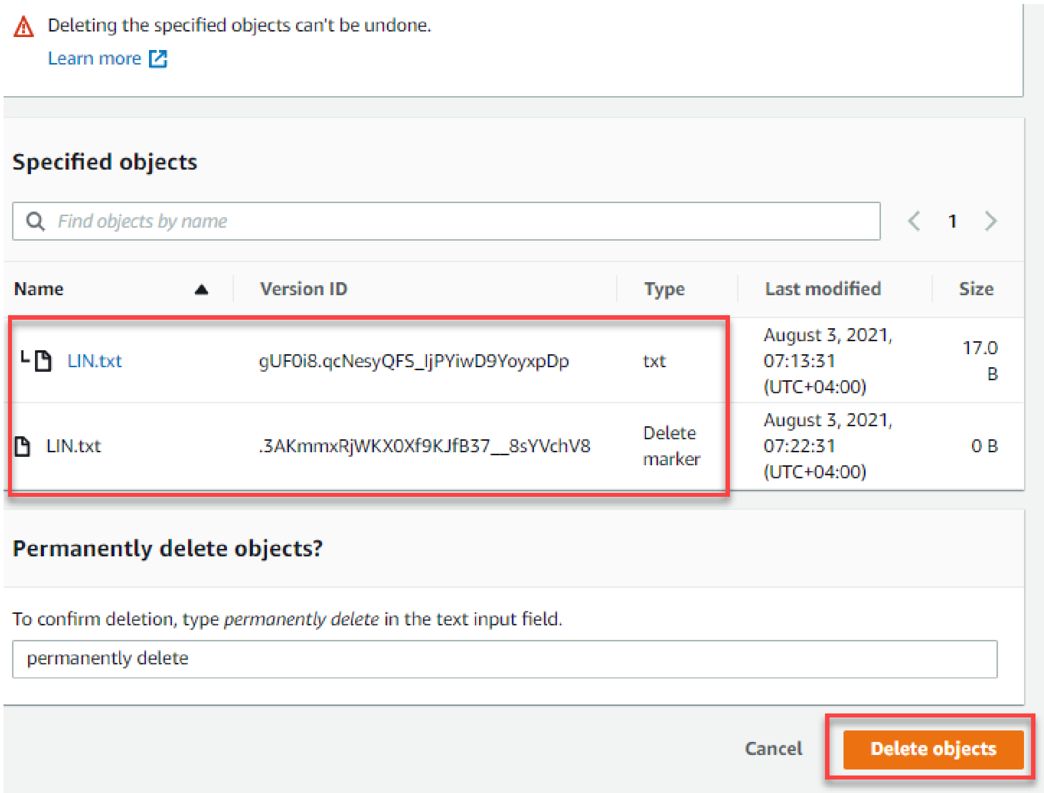


Objects (6)

Objects are the fundamental entities stored in Amazon S3. You can use **Amazon S3 inventory** to get a list of all objects in your bucket. For others to access your objects, you'll need t

□	Name ▲	Type	Version ID	Last modified
□	Lab.txt	txt	j3jgvVOFA5q8Q3E522VEhKcw6KXCHAAf	August 3, 2021, 07:17:33 (UTC+04:00)
□	└ Lab.txt	txt	null	August 3, 2021, 06:29:25 (UTC+04:00)
□	LIN.txt	Delete marker	.3AKmmxRjWKX0Xf9KJfB37__8sYVchV8	August 3, 2021, 07:22:31 (UTC+04:00)
□	└ LIN.txt	txt	gUF0i8.qcNesyQFS_IjPYiwD9YoyxpDp	August 3, 2021, 07:13:31 (UTC+04:00)
□	└ LIN.txt	txt	1_YO07keXr.qF3oBhznOD00lDxhGRN36	August 3, 2021, 07:08:57 (UTC+04:00)
□	sections/	Folder	-	-

Please permanently delete the file as it will be removed this time.



Deleting the specified objects can't be undone.
Learn more

Specified objects

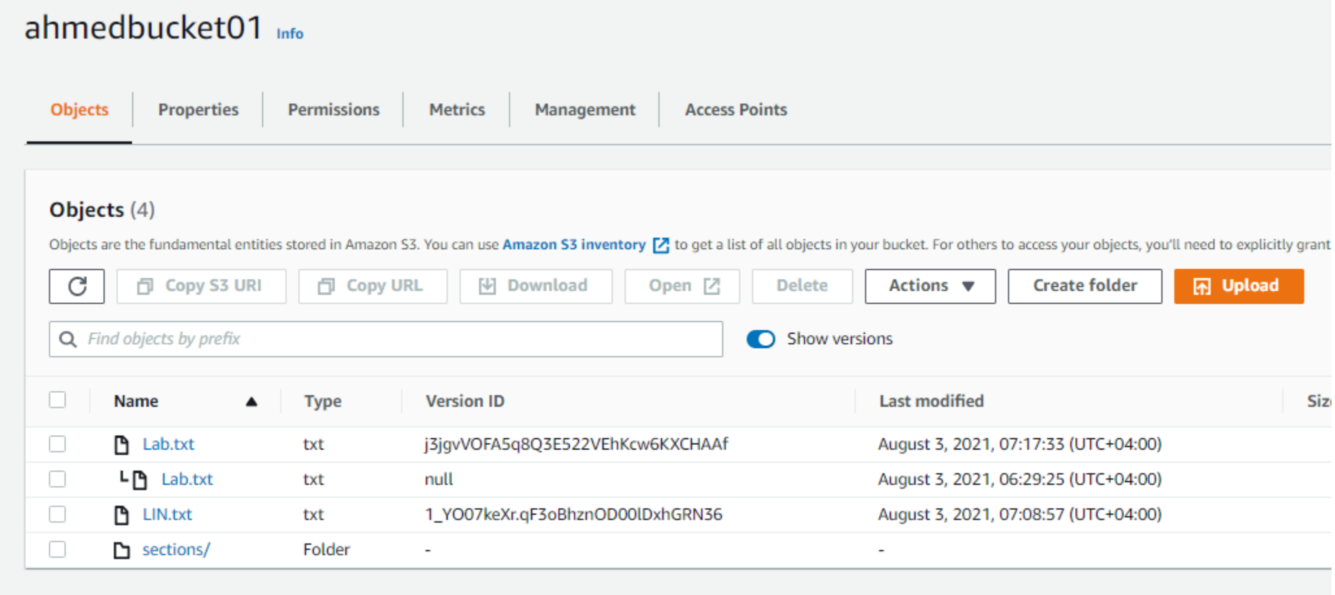
Name	Version ID	Type	Last modified	Size
LIN.txt	gUF0i8.qcNesyQFS_IjPYiwD9YoyxpDp	txt	August 3, 2021, 07:13:31 (UTC+04:00)	17.0 B
LIN.txt	.3AKmmxRjWKX0Xf9KJfB37__8sYVchV8	Delete marker	August 3, 2021, 07:22:31 (UTC+04:00)	0 B

Permanently delete objects?

To confirm deletion, type *permanently delete* in the text input field.

permanently delete

A copy of that file has been deleted.



ahmedbucket01 Info

Objects (4)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant

Show versions

Name	Type	Version ID	Last modified	Siz
Lab.txt	txt	j3jgvVOFA5q8Q3E522VEhKcw6KXCHAAf	August 3, 2021, 07:17:33 (UTC+04:00)	
Lab.txt	txt	null	August 3, 2021, 06:29:25 (UTC+04:00)	
LIN.txt	txt	1_YO07keXr.qF3oBhznOD00lDxhGRN36	August 3, 2021, 07:08:57 (UTC+04:00)	
sections/	Folder	-	-	

Turning off versioning will prevent new versions of files from being created, but existing versions will be retained.

Data Encryption Options in AWS

Client-Side Encryption:

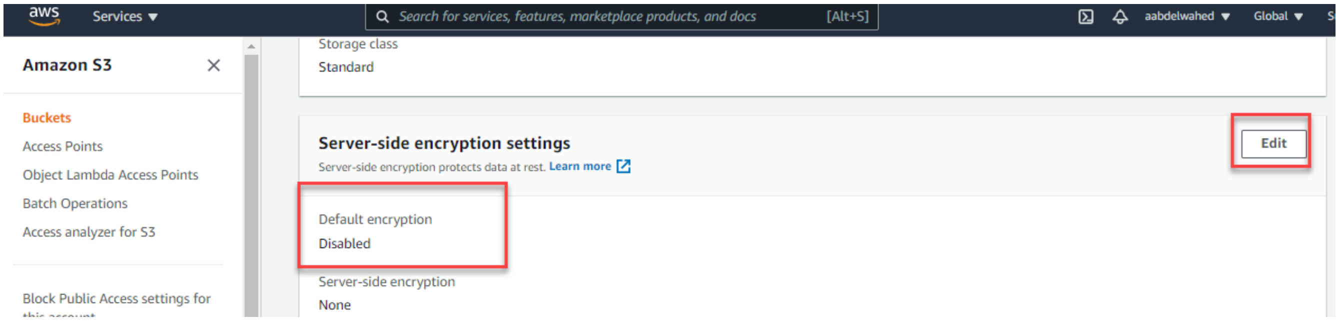
- You can encrypt your data before uploading it to AWS, ensuring you retain the decryption keys.

Server-Side Encryption:

- **S3-Managed Keys (SSE-S3):**
  - AWS manages the encryption key for you. AWS holds the master key, and you operate with that.
- **AWS KMS-Managed Keys (SSE-KMS):**
  - You have more control with your own encryption keys, which you can upload to AWS and utilize.
- **Customer-Provided Keys (SSE-C):**
  - You send encrypted data and separately request an encryption key from Amazon to access your information.

Applying Encryption to Buckets:

- You have the flexibility to apply encryption to a bucket either during its creation or afterwards.
- To apply encryption afterwards, select the bucket and navigate to the encryption options section.


aws
Services ▼
Search for services, features, marketplace products, and docs [Alt+S]
aabdelwahed ▼
Global ▼
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Edit

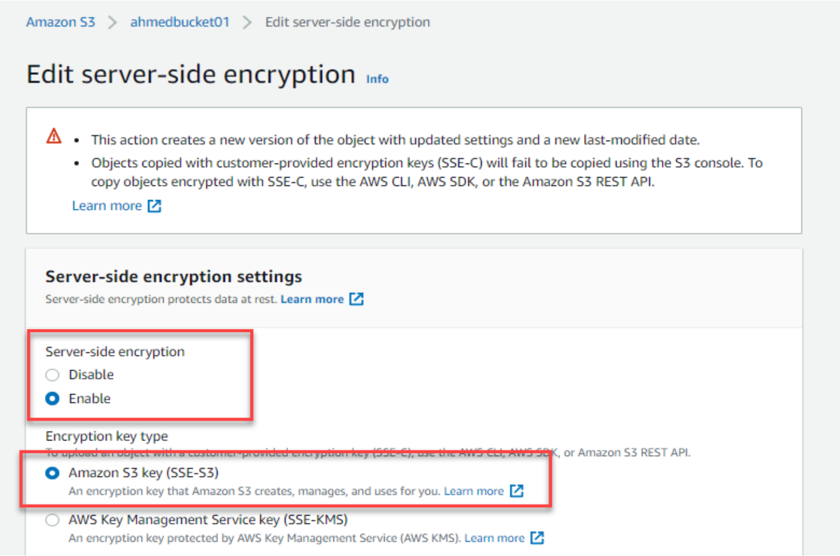
Storage class
Standard

Server-side encryption settings

Server-side encryption protects data at rest. Learn more

Default encryption
Disabled

Server-side encryption
None



Edit server-side encryption

- This action creates a new version of the object with updated settings and a new last-modified date.
- Objects copied with customer-provided encryption keys (SSE-C) will fail to be copied using the S3 console. To copy objects encrypted with SSE-C, use the AWS CLI, AWS SDK, or the Amazon S3 REST API.

Learn more

Server-side encryption settings

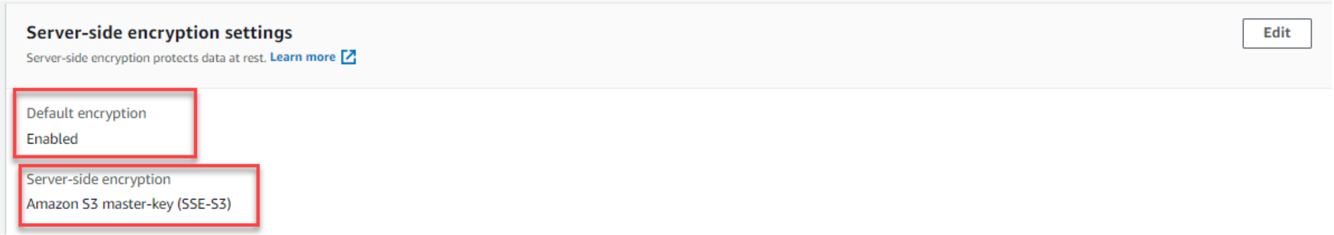
Server-side encryption protects data at rest. Learn more

Server-side encryption
○ Disable
● Enable

Encryption key type
To upload an object with a customer-provided encryption key (SSE-C), use the AWS CLI, AWS SDK, or Amazon S3 REST API.

● Amazon S3 key (SSE-S3)
An encryption key that Amazon S3 creates, manages, and uses for you. Learn more

○ AWS Key Management Service key (SSE-KMS)
An encryption key protected by AWS Key Management Service (AWS KMS). Learn more



Server-side encryption settings

Server-side encryption protects data at rest. Learn more

Edit

Default encryption
Enabled

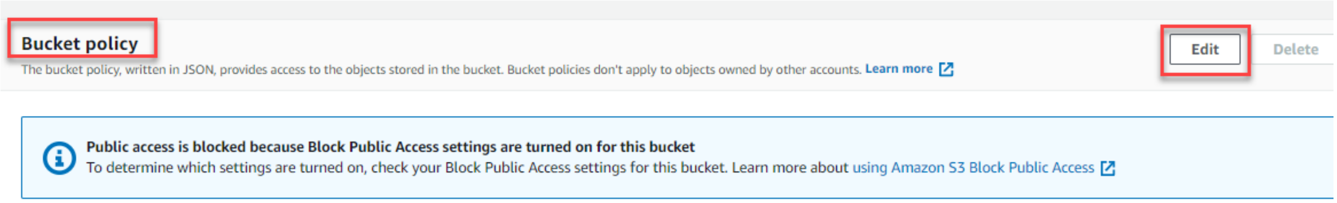
Server-side encryption
Amazon S3 master-key (SSE-S3)

S3 Bucket Policies

You can enforce S3 policies that only permit encrypted object uploads to your bucket. To implement an S3 policy, you can either follow the steps to create it or directly input JSON code; numerous examples are available at the provided link.

Bucket policy examples - Amazon Simple Storage Service

To set up a policy, choose your bucket and then look for the policy option below.

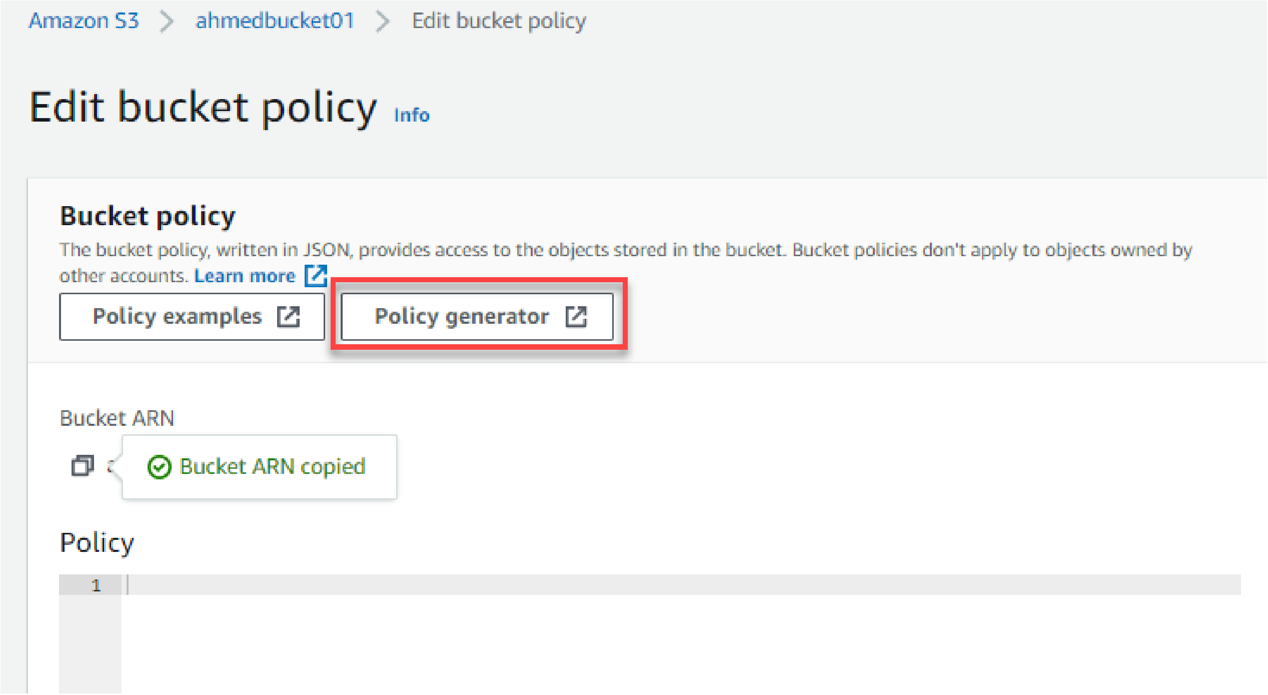


Bucket policy

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

Edit Delete

Public access is blocked because Block Public Access settings are turned on for this bucket
To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about using Amazon S3 Block Public Access



Amazon S3 > ahmedbucket01 > Edit bucket policy

Edit bucket policy Info

Bucket policy

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

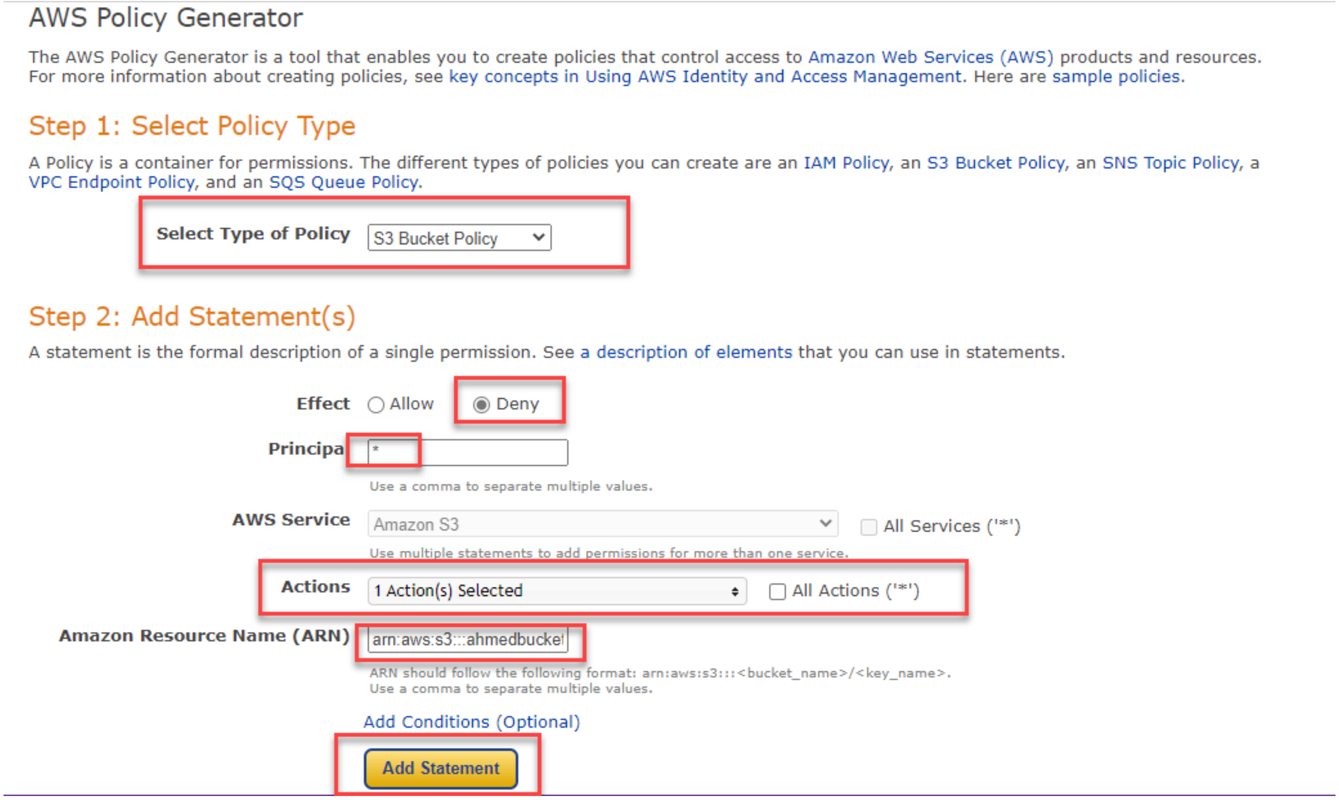
Policy examples | Policy generator

Bucket ARN

Bucket ARN copied

Policy

To deny the delete object action, select "Delete Object" from the list of actions. If you want to apply a policy for uploading objects, select "Put Object." Additionally, at the end of the bucket ARN, you need to add /*.



AWS Policy Generator

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

Step 1: Select Policy Type

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

Select Type of Policy S3 Bucket Policy

Step 2: Add Statement(s)

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

Effect ○ Allow ● Deny

Principa *

Use a comma to separate multiple values.

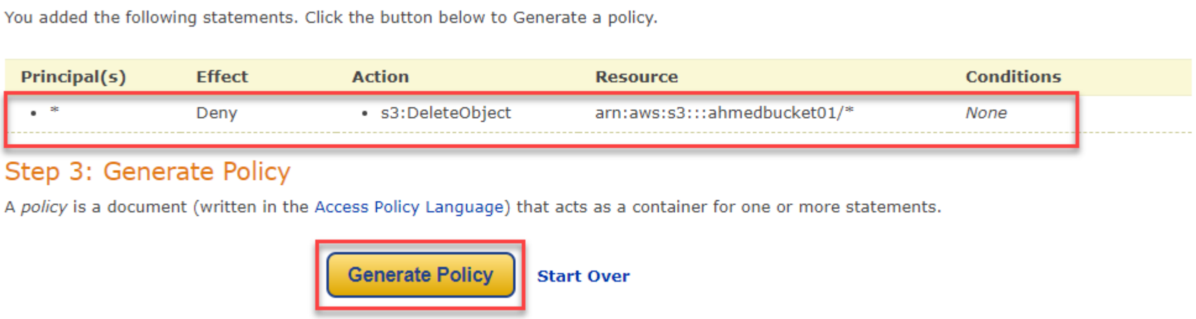
AWS Service Amazon S3 □ All Services ('*')

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

Actions 1 Action(s) Selected □ All Actions ('*')

Amazon Resource Name (ARN) arn:aws:s3:::ahmedbucke

ARN should follow the following format: arn:aws:s3:::<bucket_name>/<key_name>.
Use a comma to separate multiple values.



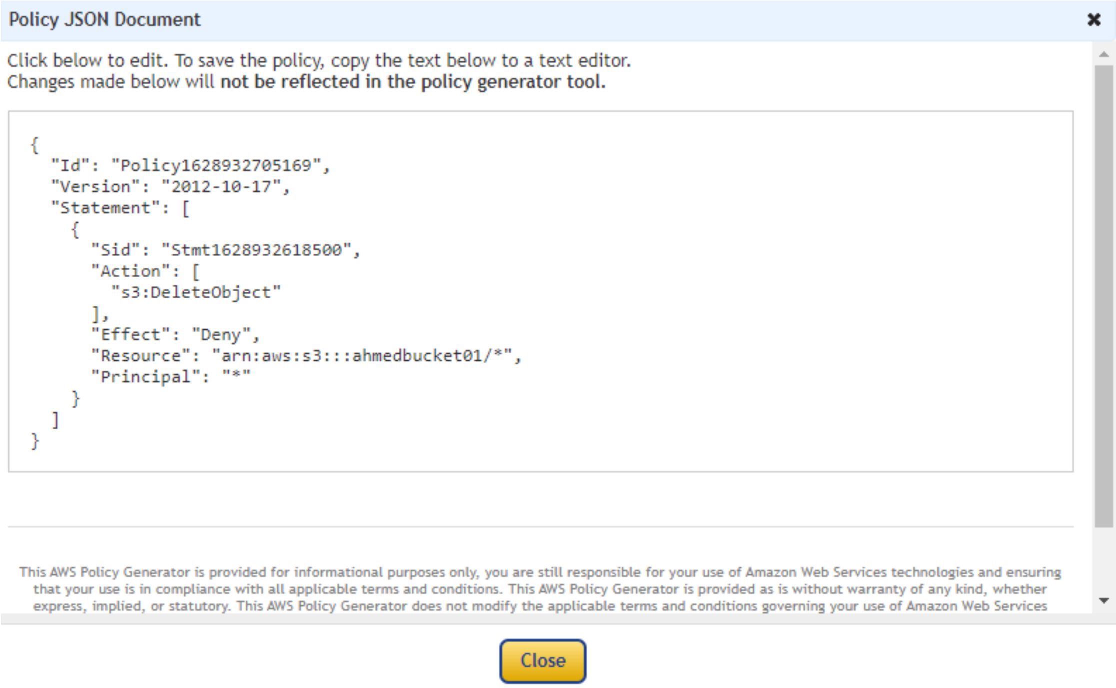
You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource	Conditions
• *	Deny	• s3:DeleteObject	arn:aws:s3:::ahmedbucket01/*	*None*

Step 3: Generate Policy

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

The JSON code will be generated initially, at which point you should copy it and paste it into the S3 console.

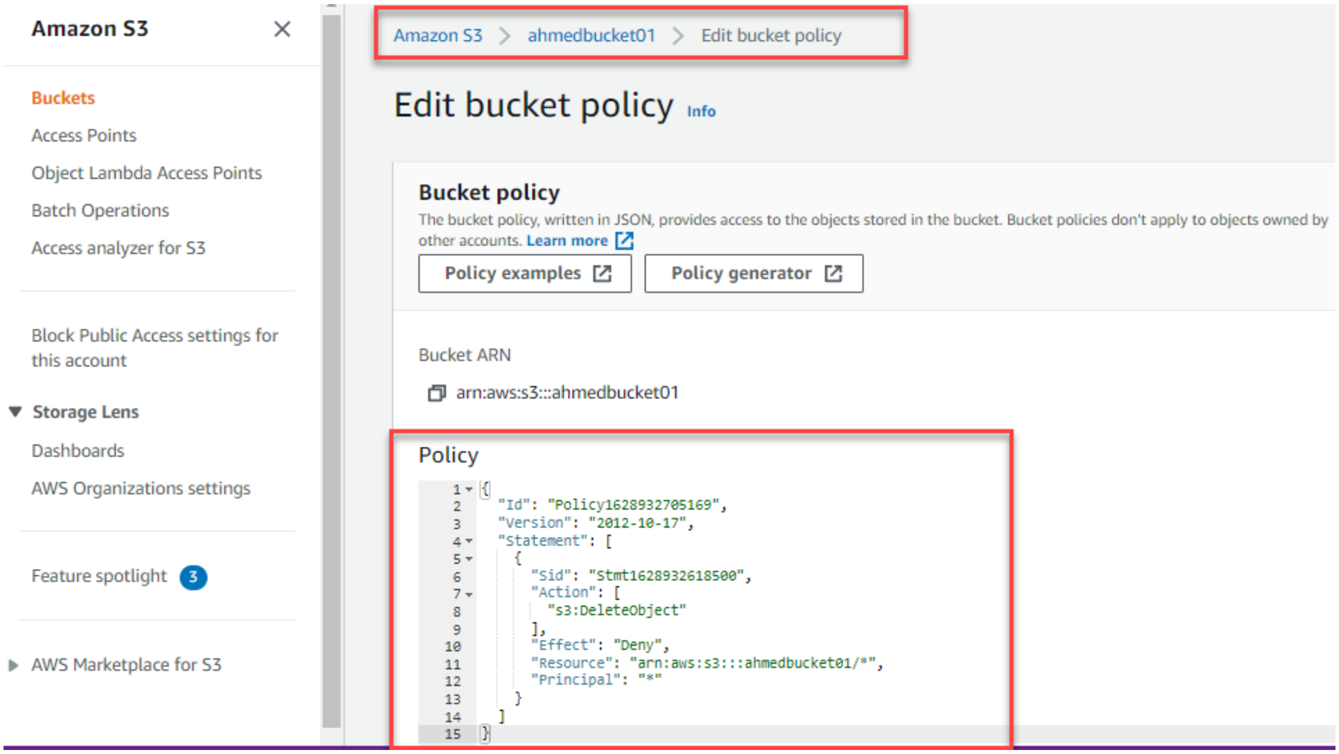


Policy JSON Document

Click below to edit. To save the policy, copy the text below to a text editor.
Changes made below will **not be reflected in the policy generator tool.**

```
{
  "Id": "Policy1628932705169",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1628932618500",
      "Action": [
        "s3:DeleteObject"
      ],
      "Effect": "Deny",
      "Resource": "arn:aws:s3:::ahmedbucket01/*",
      "Principal": "*"
    }
  ]
}
```

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided as is without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services



Amazon S3
Buckets
Access Points
Object Lambda Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
Amazon S3 > ahmedbucket01 > Edit bucket policy

Edit bucket policy Info

Bucket policy

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

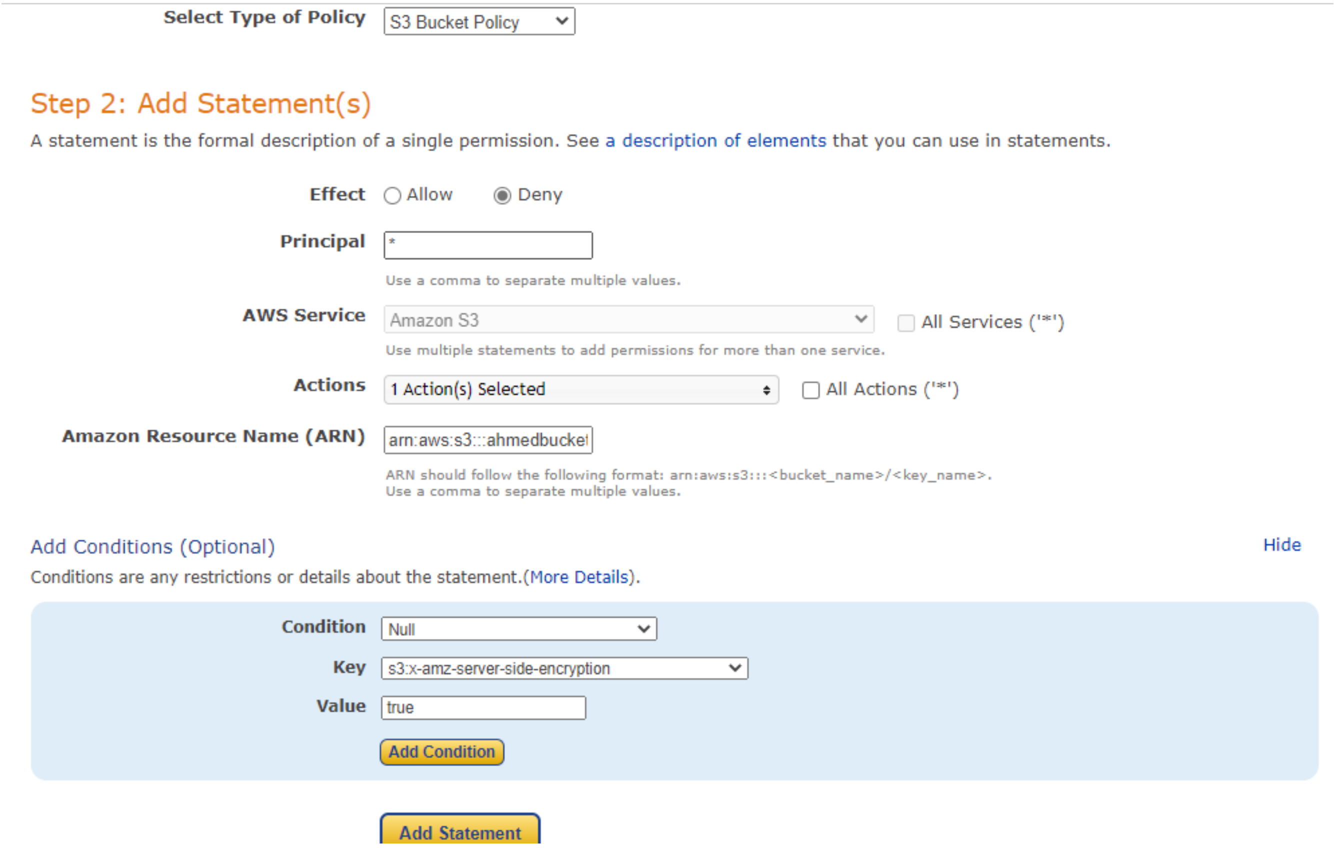
Bucket ARN

arn:aws:s3:::ahmedbucket01

Policy

```
{
  "Id": "Policy1628932705169",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1628932618500",
      "Action": [
        "s3:DeleteObject"
      ],
      "Effect": "Deny",
      "Resource": "arn:aws:s3:::ahmedbucket01/*",
      "Principal": "*"
    }
  ]
}
```

An additional policy is to block the upload of unencrypted objects into our bucket. Therefore, in the action settings, select 'put object'.



Select Type of Policy: S3 Bucket Policy

Step 2: Add Statement(s)

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

Effect ○ Allow ● Deny

Principal: *

Use a comma to separate multiple values.

AWS Service: Amazon S3 □ All Services ('*')

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

Actions: 1 Action(s) Selected □ All Actions ('*')

Amazon Resource Name (ARN): arn:aws:s3:::ahmedbucket

ARN should follow the following format: arn:aws:s3:::<bucket_name>/<key_name>.
Use a comma to separate multiple values.

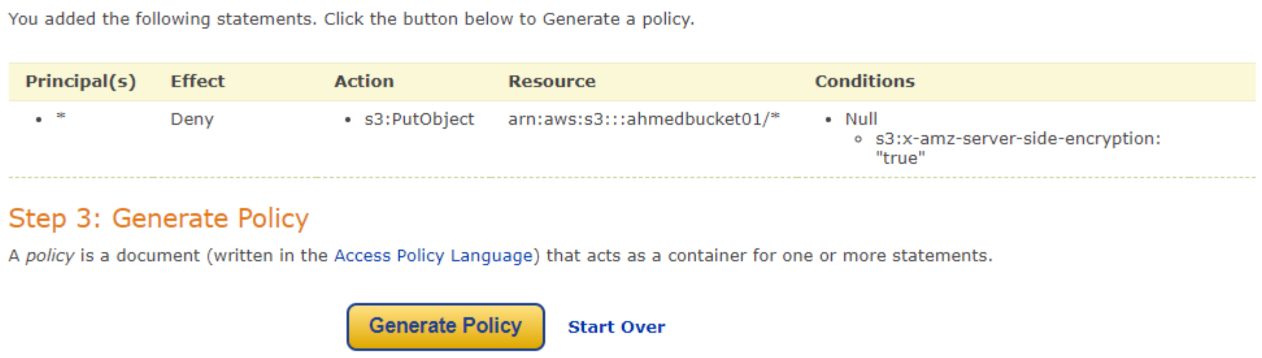
Add Conditions (Optional) Hide

Conditions are any restrictions or details about the statement.(More Details).

Condition: Null

Key: s3:x-amz-server-side-encryption

Value: true



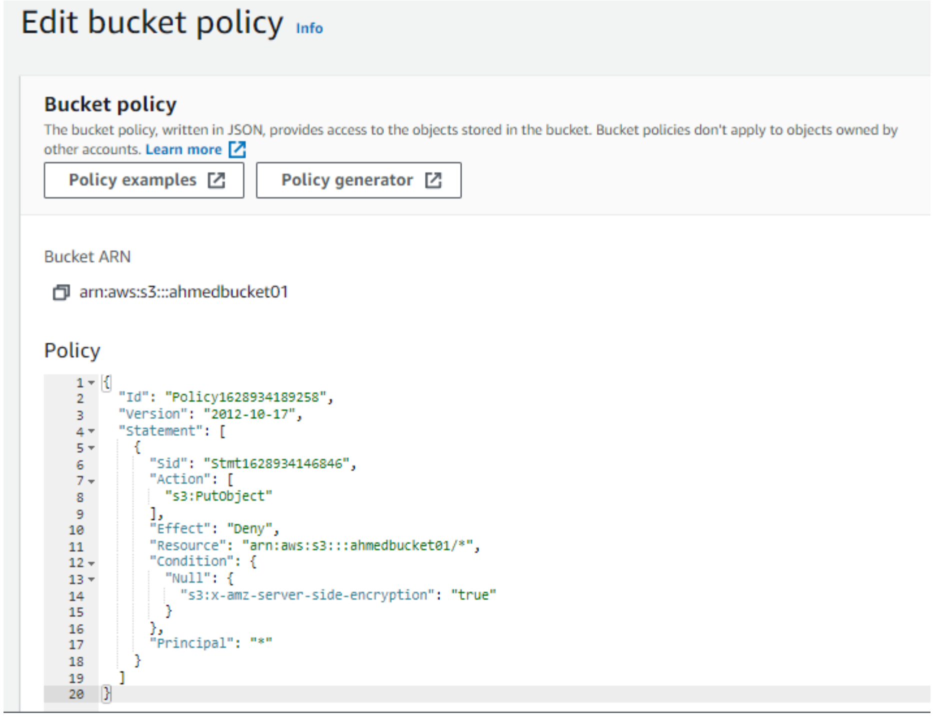
You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource	Conditions
• *	Deny	• s3:PutObject	arn:aws:s3:::ahmedbucket01/*	• Null ∘ s3:x-amz-server-side-encryption: "true"

Step 3: Generate Policy

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

Paste the produced code into the policy.



Edit bucket policy

Bucket policy

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

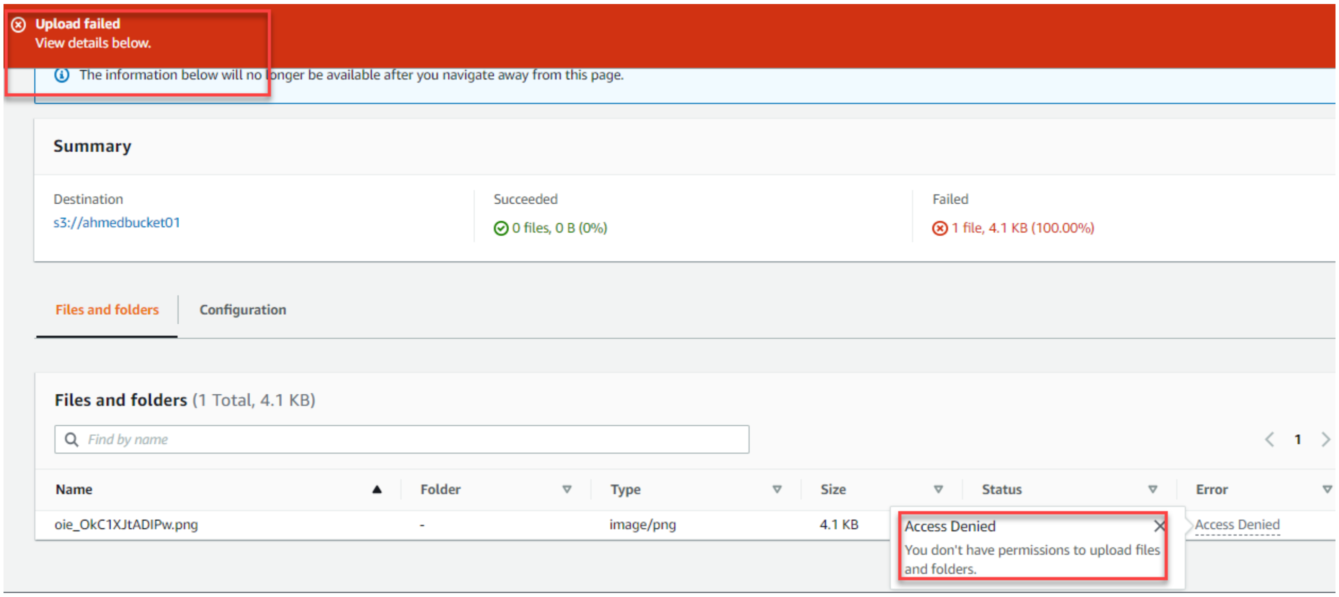
Bucket ARN

arn:aws:s3:::ahmedbucket01

Policy

```
{
  "Id": "Policy1628934189258",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1628934146846",
      "Action": [
        "s3:PutObject"
      ],
      "Effect": "Deny",
      "Resource": "arn:aws:s3:::ahmedbucket01/*",
      "Condition": {
        "Null": {
          "s3:x-amz-server-side-encryption": "true"
        }
      },
      "Principal": "*"
    }
  ]
}
```

Attempting to upload an object without encryption will result in an error.



Upload failed
View details below.

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

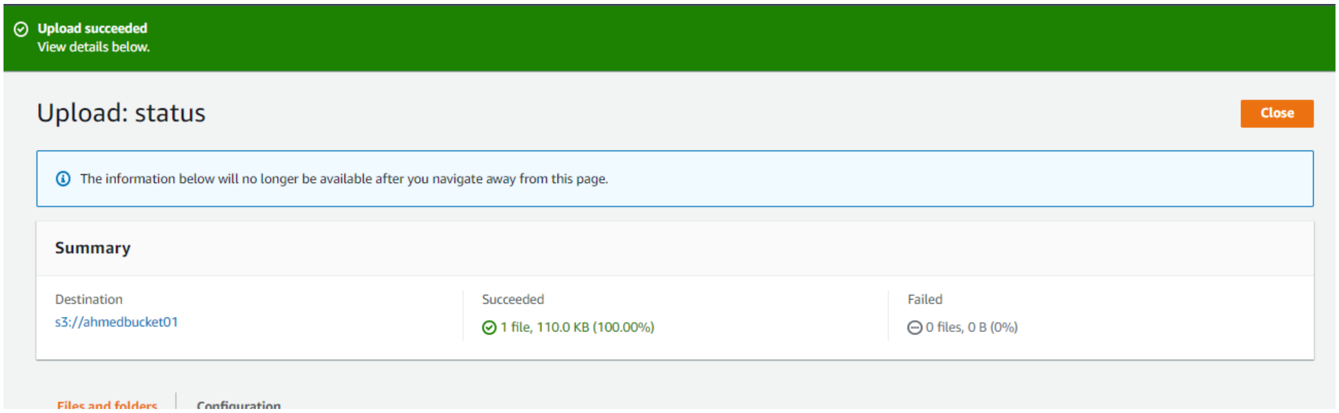
Summary

Destination	Succeeded	Failed
s3://ahmedbucket01	0 files, 0 B (0%)	1 file, 4.1 KB (100.00%)

Files and folders (1 Total, 4.1 KB)

Name	Folder	Type	Size	Status	Error
oie_OkC1XJtADIPw.png	-	image/png	4.1 KB	Access Denied You don't have permissions to upload files and folders.	Access Denied

Try one more time with encryption option



Upload succeeded
View details below.

Upload: status

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

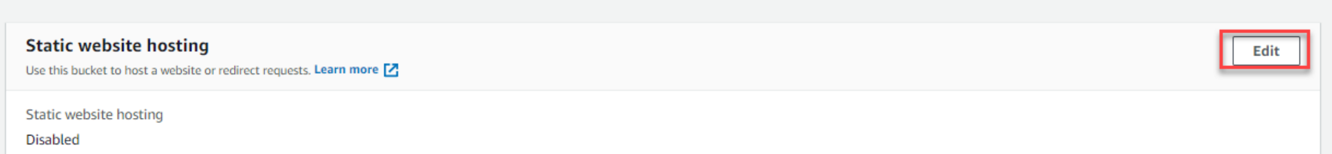
Summary

Destination	Succeeded	Failed
s3://ahmedbucket01	1 file, 110.0 KB (100.00%)	0 files, 0 B (0%)

Static Website

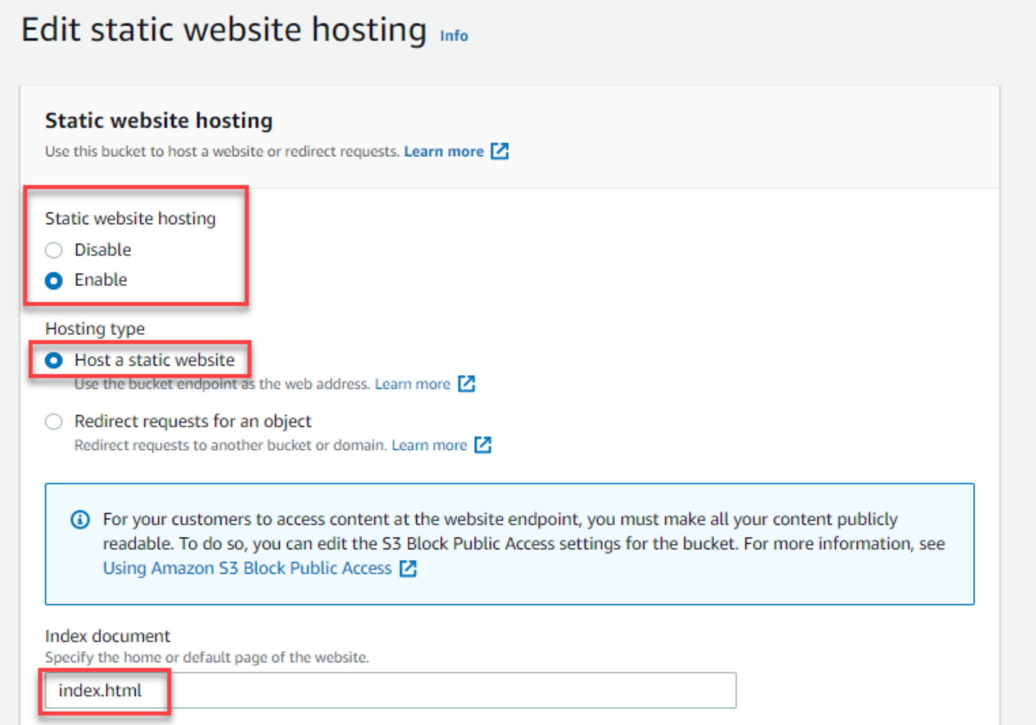
Begin by creating a page called index.html, then navigate to your bucket to upload the index file. After that, activate the static website feature and set the bucket permissions to public access.

Bucket properties



Static website hosting
Use this bucket to host a website or redirect requests. Learn more

Static website hosting
Disabled



Edit static website hosting Info

Static website hosting
Use this bucket to host a website or redirect requests. Learn more

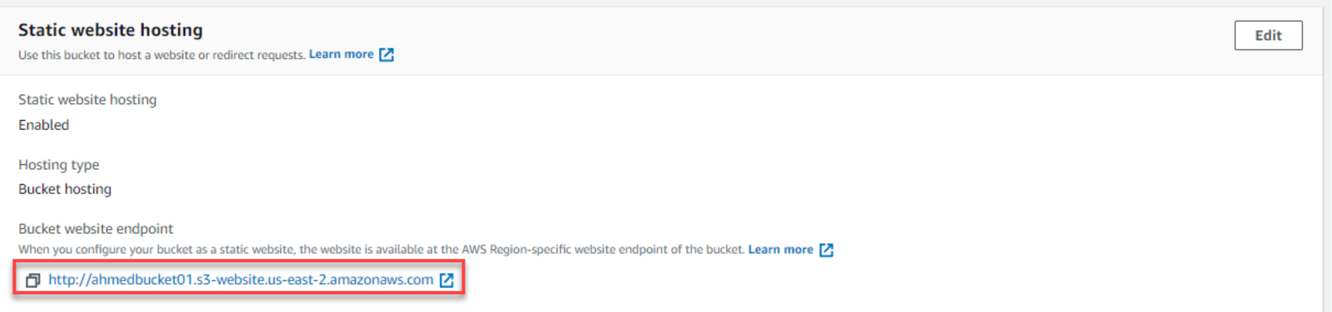
Static website hosting
○ Disable
● Enable

Hosting type
● Host a static website
Use the bucket endpoint as the web address. Learn more
○ Redirect requests for an object
Redirect requests to another bucket or domain. Learn more

For your customers to access content at the website endpoint, you must make all your content publicly 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.
index.html

You now possess the website link.



Static website hosting

Use this bucket to host a website or redirect requests. Learn more

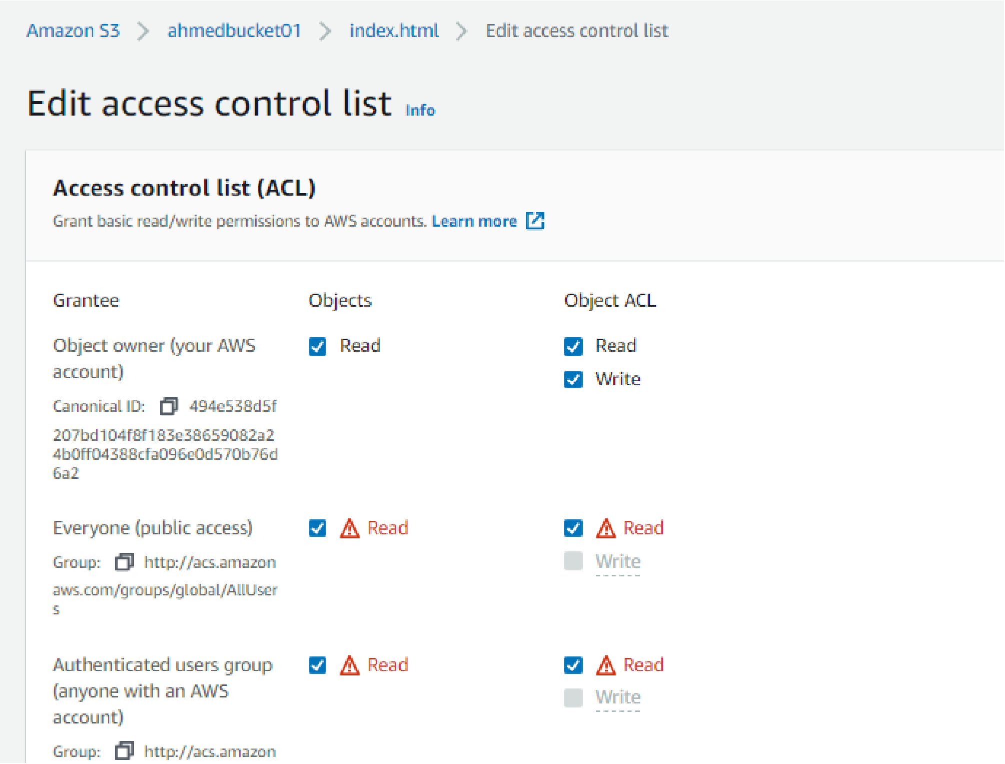
Static website hosting
Enabled

Hosting type
Bucket hosting

Bucket website endpoint
When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. Learn more

http://ahmedbucket01.s3-website.us-east-2.amazonaws.com

Grant public access to index.html.



Amazon S3 > ahmedbucket01 > index.html > Edit access control list

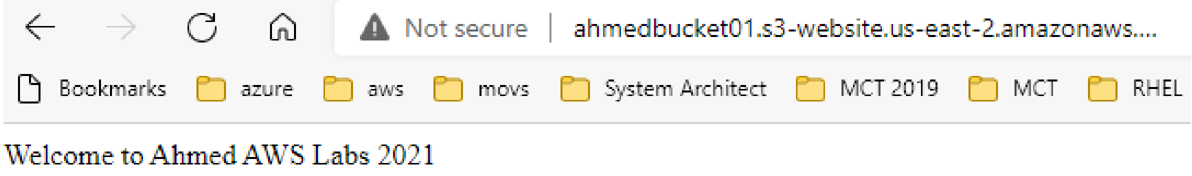
Edit access control list Info

Access control list (ACL)

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

Grantee	Objects	Object ACL
Object owner (your AWS account) Canonical ID: 494e538d5f207bd104f8f183e38659082a24b0ff04388cfa096e0d570b76d6a2	☑ Read	☑ Read ☑ Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	☑ ⚠ Read	☑ ⚠ Read □ Write
Authenticated users group (anyone with an AWS account) Group: http://acs.amazon	☑ ⚠ Read	☑ ⚠ Read □ Write

The website is now operational.



⚠ Not secure | ahmedbucket01.s3-website.us-east-2.amazonaws....

Welcome to Ahmed AWS Labs 2021

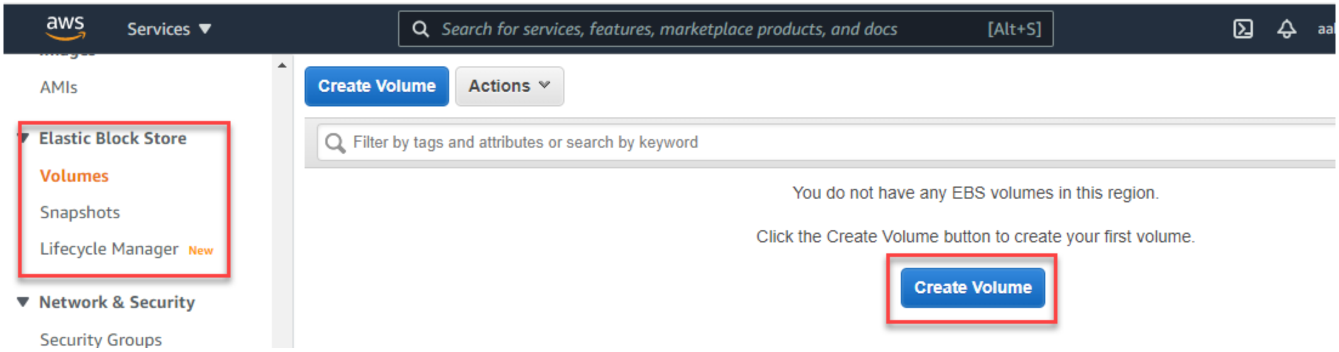
Elastic Block Storage (EBS)

is a block storage service that provides persistent storage for Amazon EC2 instances. It is accessible only across the private AWS network, ensuring secure and reliable connectivity. Each EBS volume functions like a virtual hard disk, acting as an independent storage resource that can be attached to an EC2 instance. Features of EBS:

1. **Redundancy and Durability:**
   - Once you create an EBS volume, it automatically replicates within its Availability Zone (AZ) to ensure high availability and fault tolerance.
   - EBS volumes are designed to offer durability from 99.8% to 99.999%, depending on the type of volume chosen. This means your data is safeguarded against hardware failures and other potential issues.
2. **Types of EBS Volumes:**
   - **General Purpose SSD (gp3 and gp2):** Balances price and performance for a wide variety of workloads.
   - **Provisioned IOPS SSD (io2 and io1):** Designed for I/O-intensive applications requiring high performance.
   - **Throughput Optimized HDD (st1):** Ideal for frequently accessed, throughput-intensive workloads.
   - **Cold HDD (sc1):** Suitable for less frequently accessed data.
3. **Performance:**
   - EBS volumes offer consistent and low-latency performance, making them ideal for applications requiring reliable storage.
   - You can increase the performance of your EBS volumes by using provisioned IOPS and optimizing the volume type based on your workload.
4. **Snapshots:**
   - EBS provides the ability to take point-in-time snapshots of volumes, which are stored in Amazon S3. These snapshots can be used for backup, restore, and replication purposes.
5. **Encryption:**
   - EBS supports encryption of data at rest, in transit, and during snapshots, providing a robust security model to protect your data.

How EBS Works:

- **Creating an EBS Volume:**
  - You can create an EBS volume from the AWS Management Console, AWS CLI, or AWS SDKs. During creation, you specify the volume type, size, and other parameters.
- **Attaching EBS Volumes:**
  - Once created, an EBS volume can be attached to any EC2 instance within the same Availability Zone. An instance can have multiple EBS volumes attached, allowing for flexible and scalable storage configurations.
- **Data Persistence:**
  - Data on an EBS volume persists independently of the life of an EC2 instance. You can detach a volume from one instance and attach it to another without losing data.

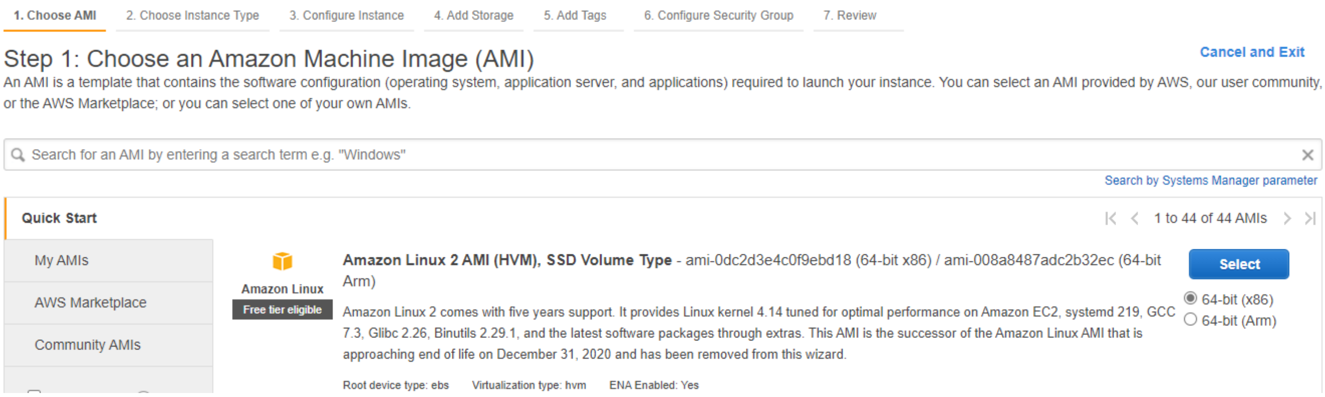


You do not have any EBS volumes in this region.

Click the Create Volume button to create your first volume.

Include a data disk while creating an EC2 instance.

1. Choose an AMI



Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

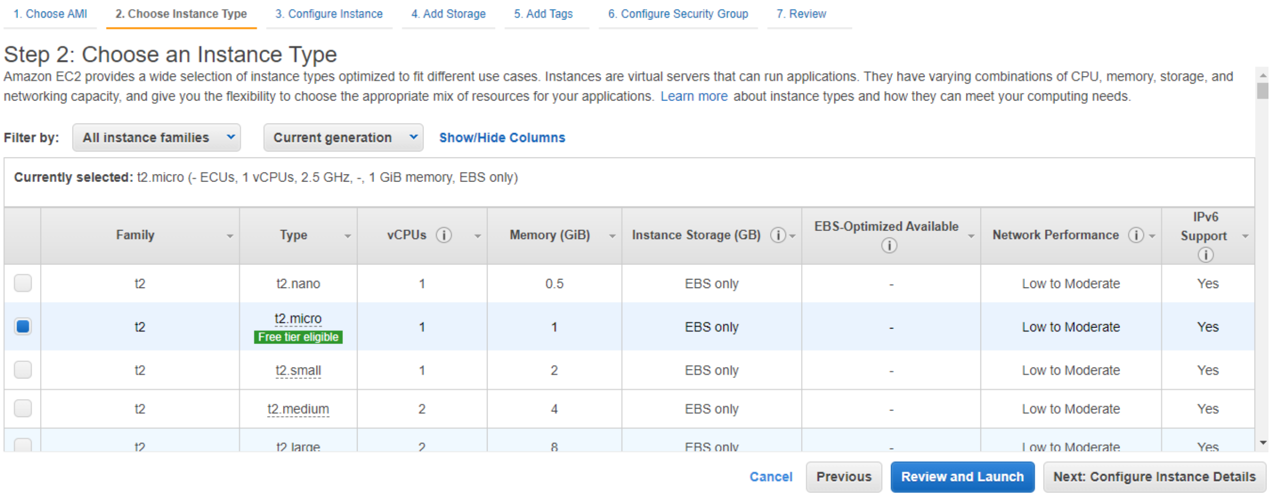
Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-0dc2d3e4c0f9ebd18 (64-bit x86) / ami-008a8487adc2b32ec (64-bit Arm)

Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is approaching end of life on December 31, 2020 and has been removed from this wizard.

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

● 64-bit (x86)
○ 64-bit (Arm)

2. Choose an Instance Type



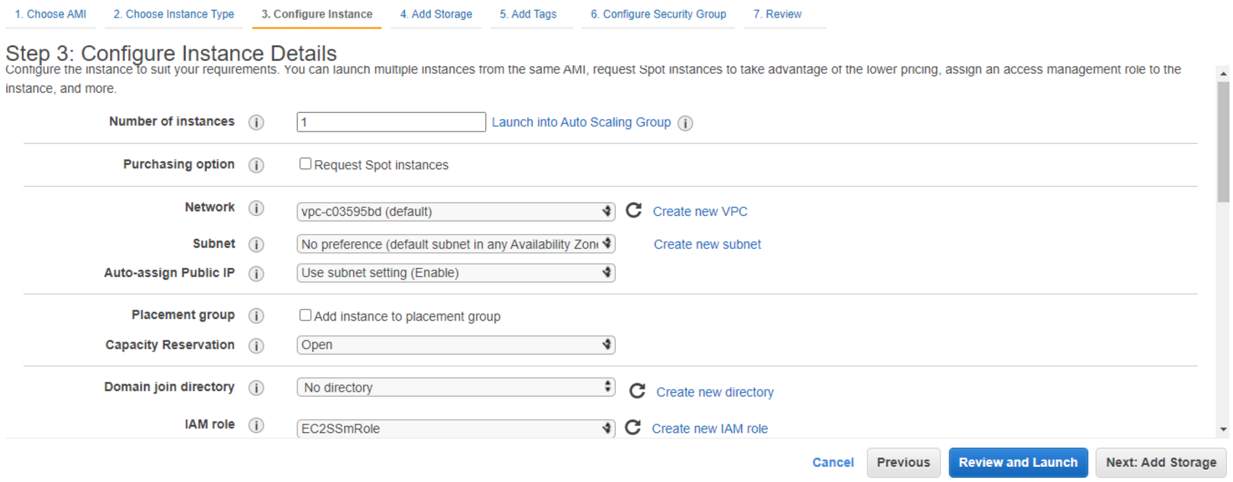
Step 2: Choose an Instance Type

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

Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
□	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
☑	t2	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
□	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
□	t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
□	t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes

3. Configure Instance

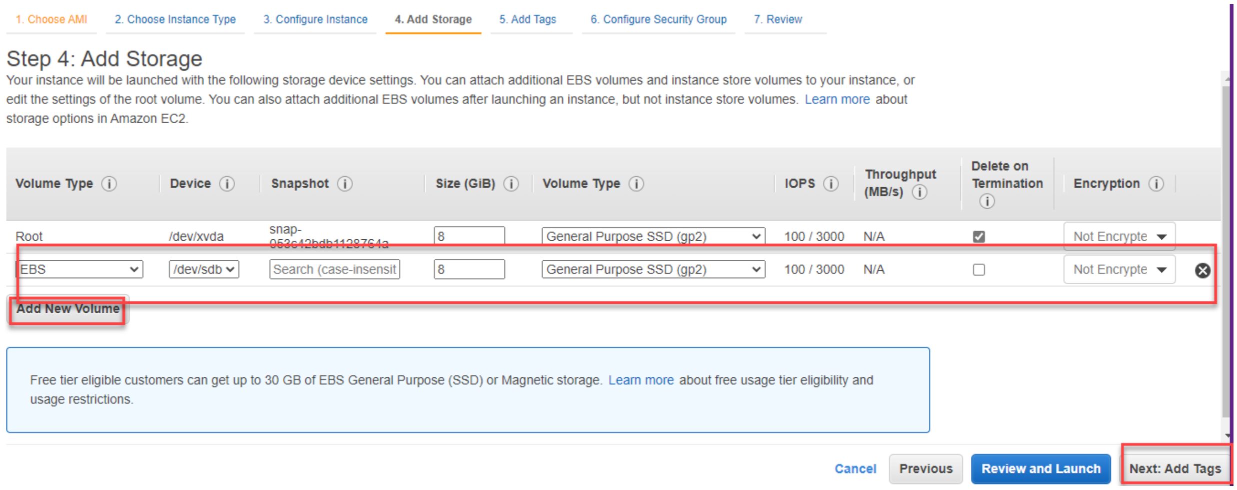


Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances	1 Launch into Auto Scaling Group
Purchasing option	□ Request Spot instances
Network	vpc-c03595bd (default) Create new VPC
Subnet	No preference (default subnet in any Availability Zon Create new subnet
Auto-assign Public IP	Use subnet setting (Enable)
Placement group	□ Add instance to placement group
Capacity Reservation	Open
Domain join directory	No directory Create new directory
IAM role	EC2SSmRole Create new IAM role

4. Add Storage



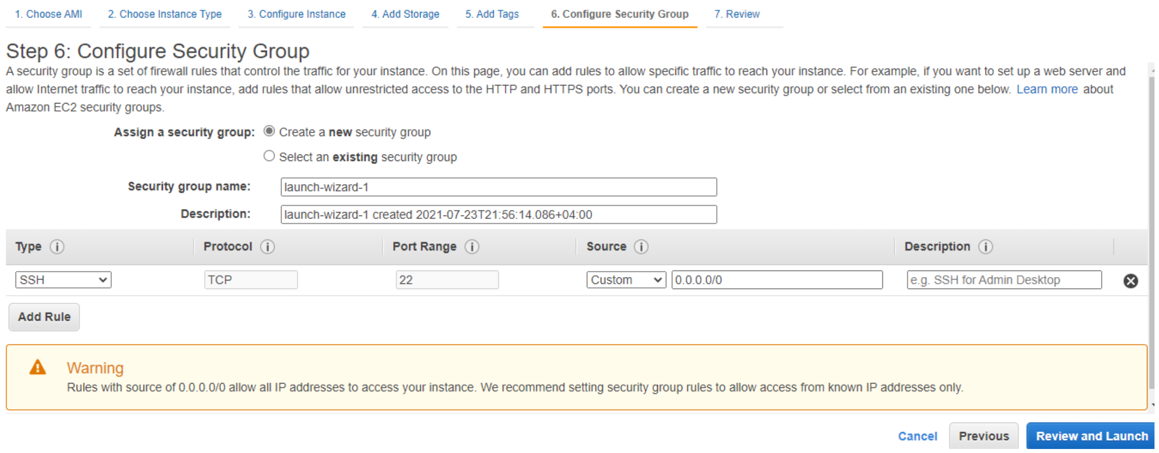
Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-053c42bdb1128764a	8	General Purpose SSD (gp2)	100 / 3000	N/A	☑	Not Encrypte
EBS	/dev/sdb	Search (case-insensit	8	General Purpose SSD (gp2)	100 / 3000	N/A	□	Not Encrypte

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.

5. Configure Security Group



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ● Create a **new** security group
○ Select an **existing** security group

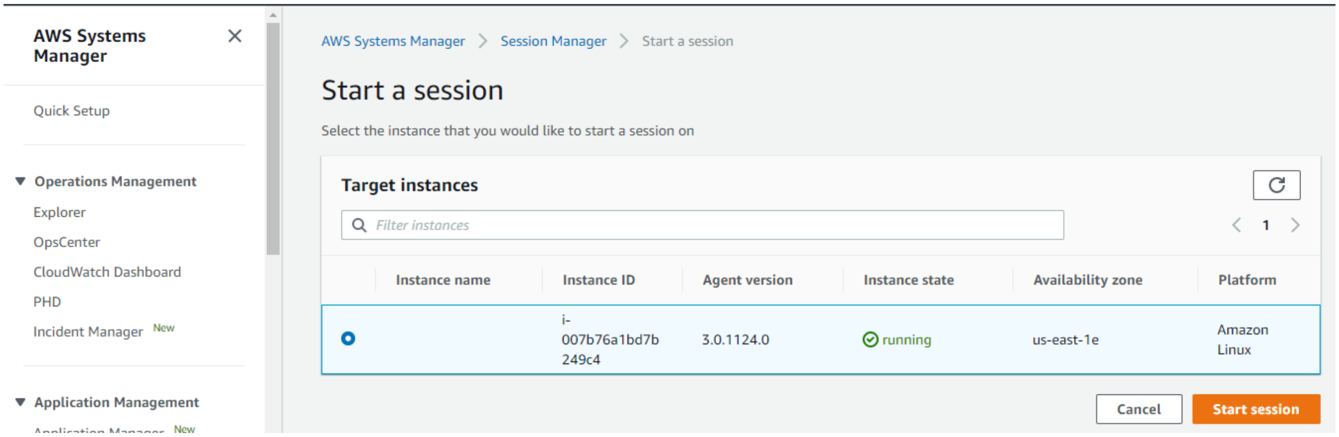
Security group name: launch-wizard-1

Description: launch-wizard-1 created 2021-07-23T21:56:14.086+04:00

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

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

Begin an SSM session with the EC2 instance. Once the disk is attached, proceed to format and mount it for use.



AWS Systems Manager > Session Manager > Start a session

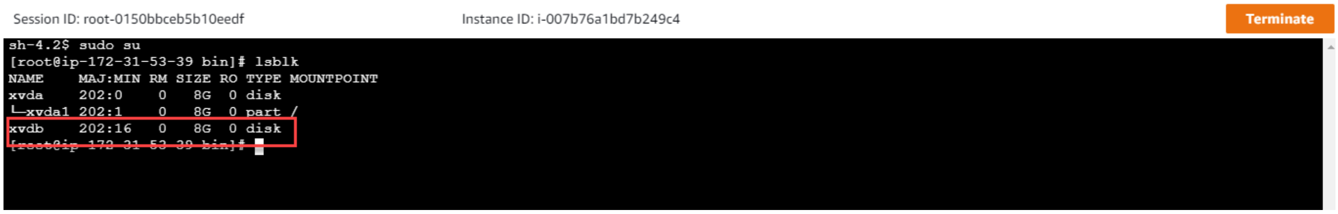
Start a session

Select the instance that you would like to start a session on

Target instances

Filter instances

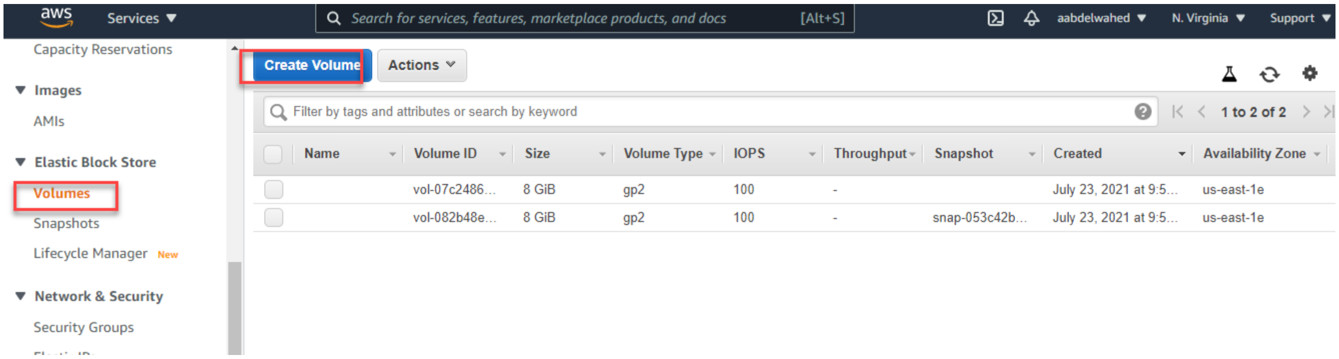
	Instance name	Instance ID	Agent version	Instance state	Availability zone	Platform
●		i-007b76a1bd7b249c4	3.0.1124.0	✓ running	us-east-1e	Amazon Linux



Session ID: root-0150bbceb5b10eedf   Instance ID: i-007b76a1bd7b249c4

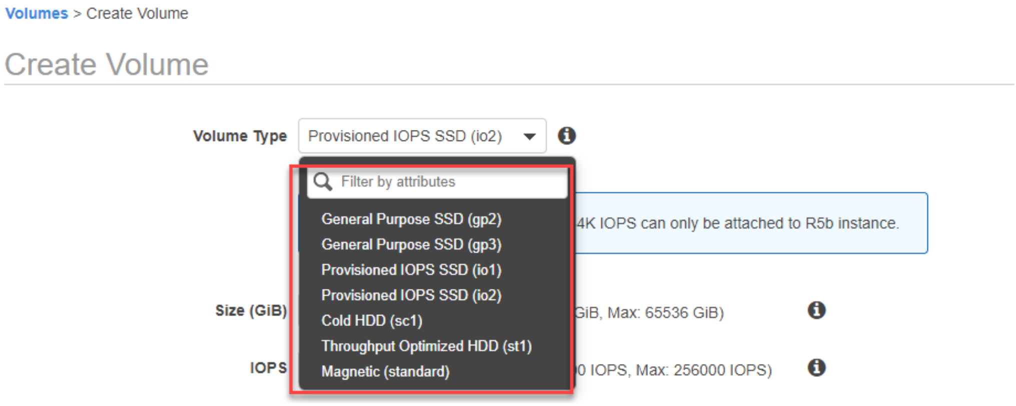
```
sh-4.2$ sudo su
[root@ip-172-31-53-39 bin]# lsblk
NAME    MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
xvda    202:0    0   8G  0 disk
└─xvda1 202:1    0   8G  0 part /
xvdb    202:16   0   8G  0 disk
[root@ip-172-31-53-39 bin]#
```

Creating and Configuring an Amazon EBS Volume



□	Name	Volume ID	Size	Volume Type	IOPS	Throughput	Snapshot	Created	Availability Zone
□		vol-07c2486…	8 GiB	gp2	100	-		July 23, 2021 at 9:5…	us-east-1e
□		vol-082b48e…	8 GiB	gp2	100	-	snap-053c42b…	July 23, 2021 at 9:5…	us-east-1e

Selecting Volume Type and Specifications:


Volumes > Create Volume
Create Volume
Filter by attributes
General Purpose SSD (gp2)
General Purpose SSD (gp3)
Provisioned IOPS SSD (io1)
Provisioned IOPS SSD (io2)
Cold HDD (sc1)
Throughput Optimized HDD (st1)
Magnetic (standard)

Volume Type: Provisioned IOPS SSD (io2)

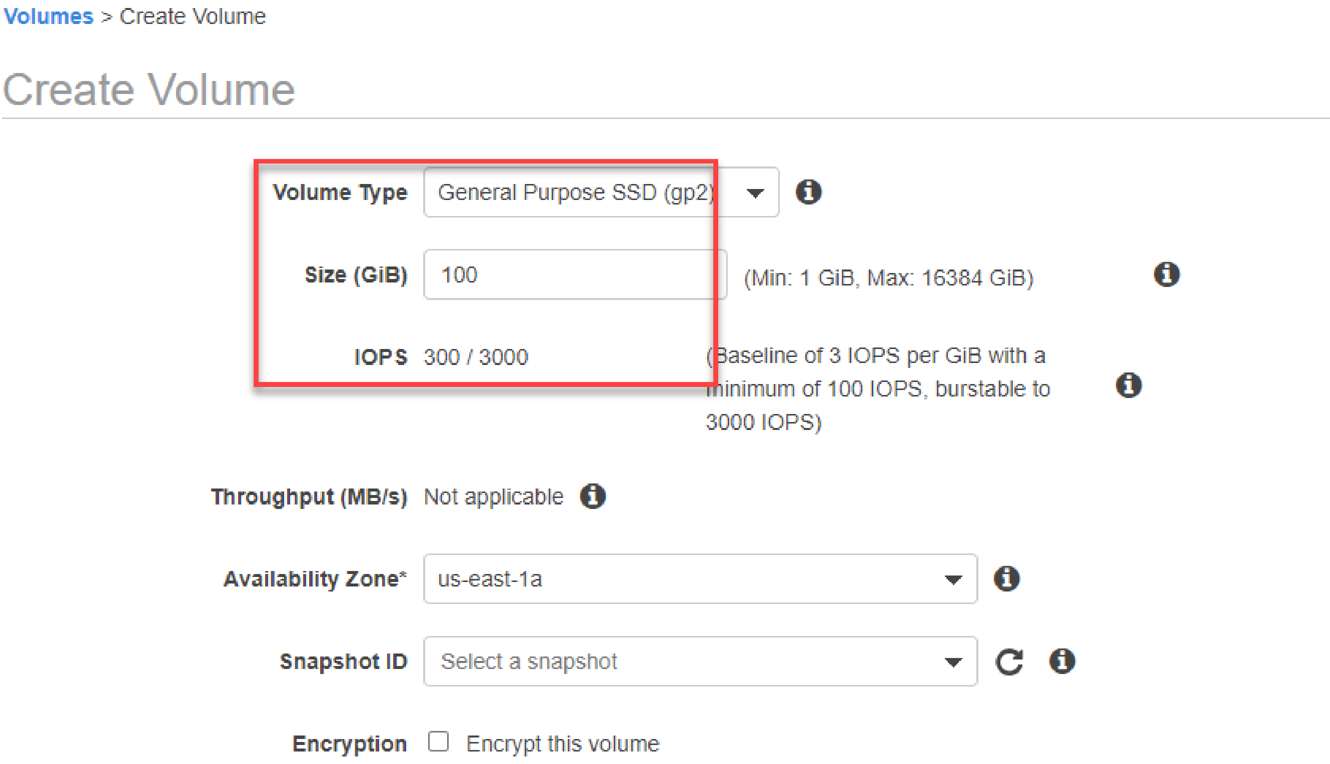
4K IOPS can only be attached to R5b instance.

Size (GiB) GiB, Max: 65536 GiB)

IOPS 0 IOPS, Max: 256000 IOPS)

Types of EBS Storage in AWS

1. **General Purpose SSD (gp2):** Balanced performance and cost, up to 3000 IOPS.
2. **General Purpose SSD (gp3):** Customizable performance, up to 16,000 IOPS and 1000 MB/s.
3. **Provisioned IOPS SSD (io1):** High-performance SSD, up to 64,000 IOPS.
4. **Provisioned IOPS SSD (io2):** Enhanced performance and durability, up to 256,000 IOPS.
5. **Cold HDD (sc1):** Low-cost storage for infrequently accessed data.
6. **Throughput Optimized HDD (st1):** High-throughput HDD for large sequential workloads.
7. **Magnetic (standard):** Cost-effective storage with lower performance.



Volumes > Create Volume

Create Volume

Volume Type: General Purpose SSD (gp2)

Size (GiB): 100 (Min: 1 GiB, Max: 16384 GiB)

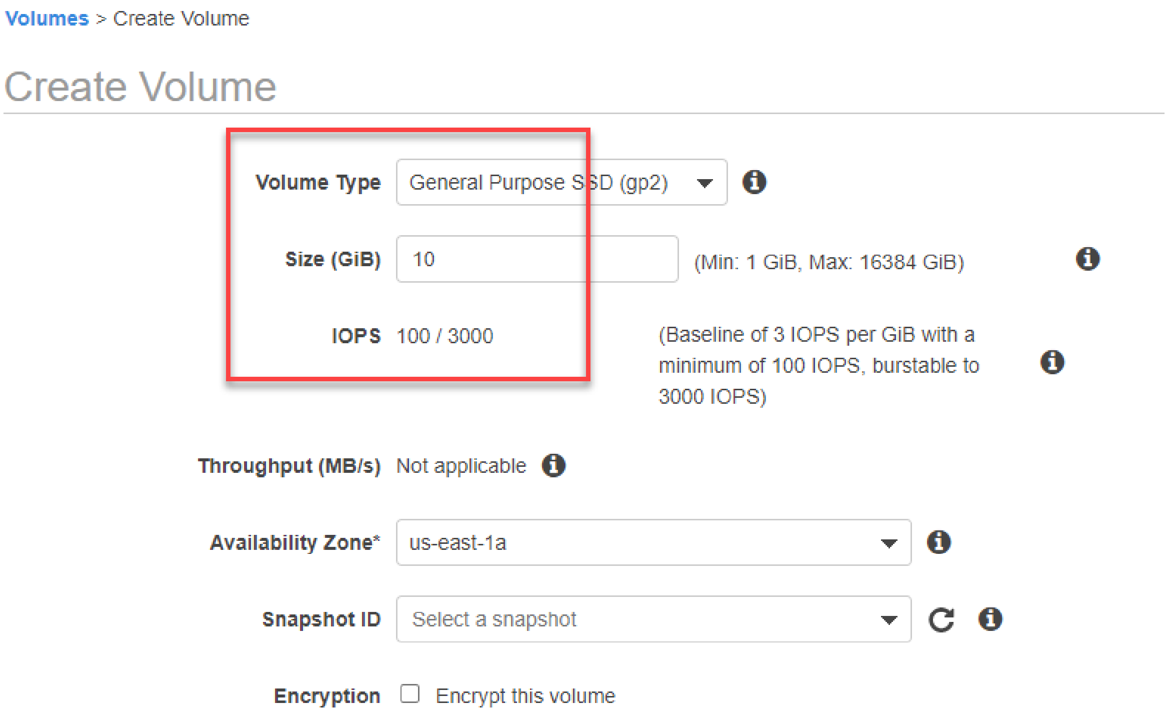
IOPS: 300 / 3000 (Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS)

Throughput (MB/s): Not applicable

Availability Zone*: us-east-1a

Snapshot ID: Select a snapshot

Encryption: □ Encrypt this volume



Volumes > Create Volume

Create Volume

Volume Type: General Purpose SSD (gp2)

Size (GiB): 10 (Min: 1 GiB, Max: 16384 GiB)

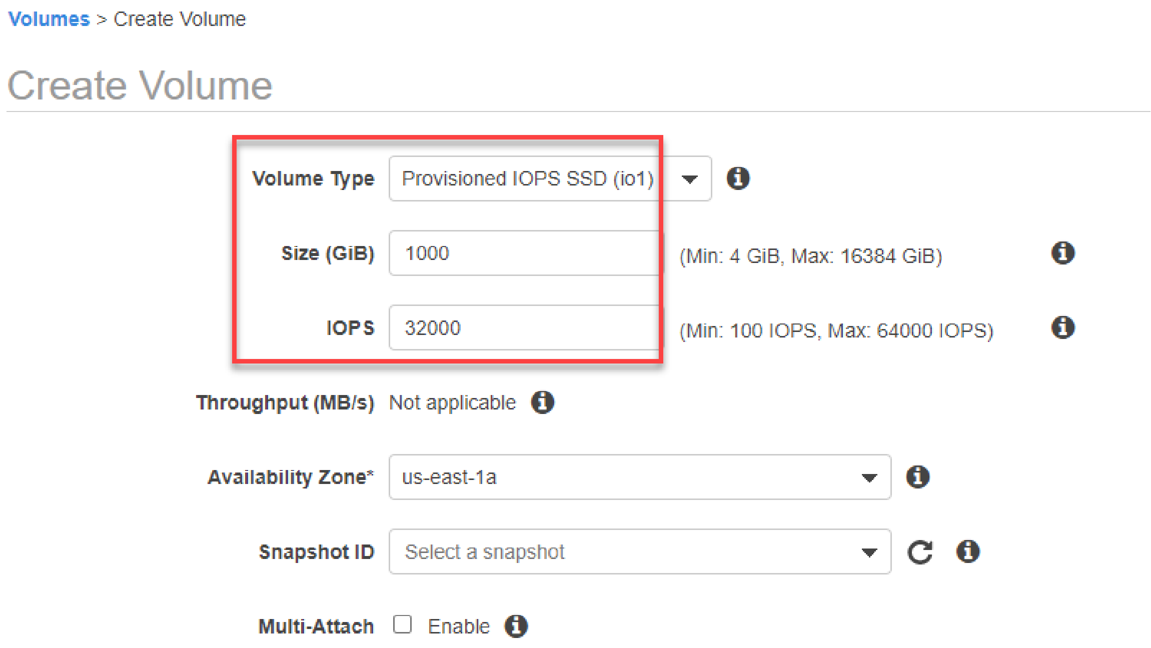
IOPS: 100 / 3000 (Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS)

Throughput (MB/s): Not applicable

Availability Zone*: us-east-1a

Snapshot ID: Select a snapshot

Encryption: □ Encrypt this volume



Volumes > Create Volume

Create Volume

Volume Type: Provisioned IOPS SSD (io1)

Size (GiB): 1000 (Min: 4 GiB, Max: 16384 GiB)

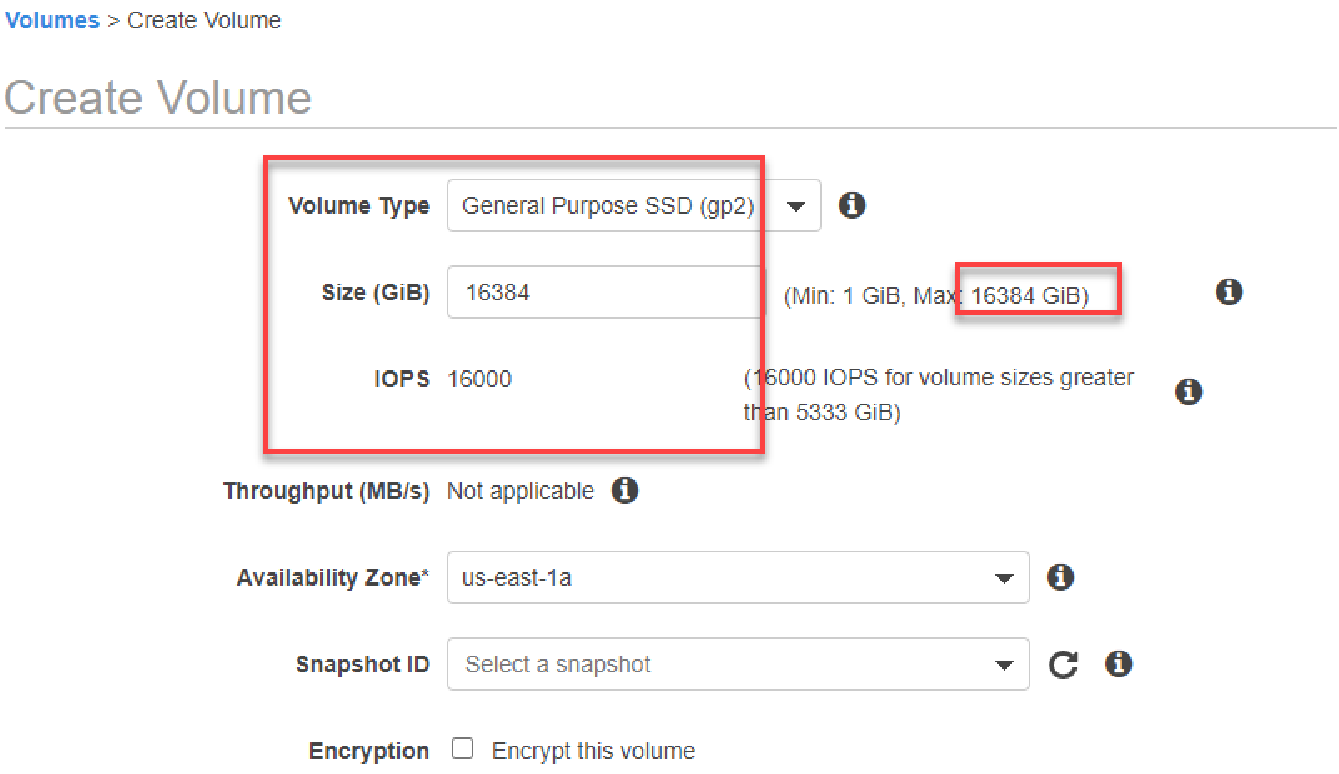
IOPS: 32000 (Min: 100 IOPS, Max: 64000 IOPS)

Throughput (MB/s): Not applicable

Availability Zone*: us-east-1a

Snapshot ID: Select a snapshot

Multi-Attach: □ Enable



Volumes > Create Volume

Create Volume

Volume Type: General Purpose SSD (gp2)

Size (GiB): 16384 (Min: 1 GiB, Max: 16384 GiB)

IOPS: 16000 (16000 IOPS for volume sizes greater than 5333 GiB)

Throughput (MB/s): Not applicable

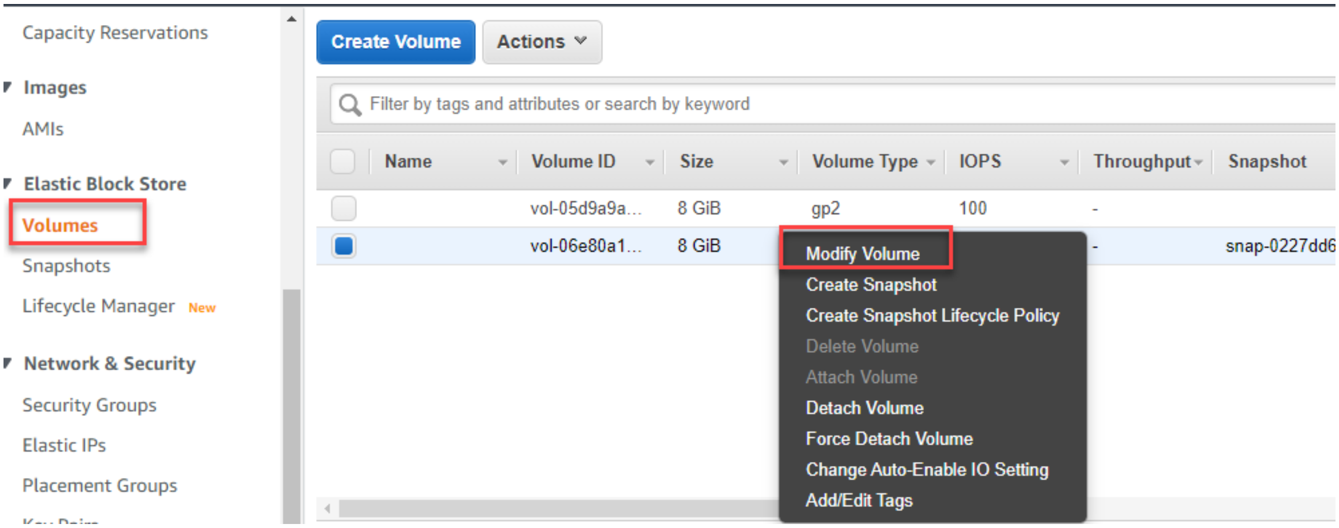
Availability Zone*: us-east-1a

Snapshot ID: Select a snapshot

Encryption: □ Encrypt this volume

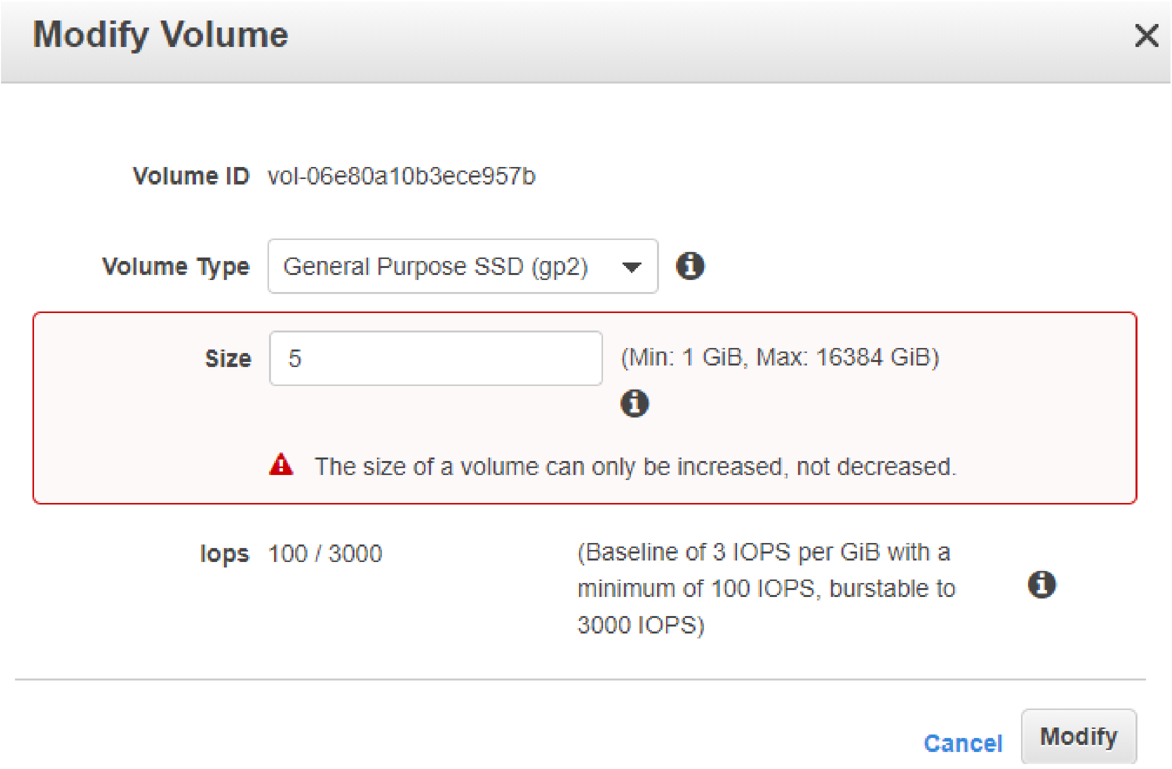
The IOPS settings can be adjusted manually. Proceed to the volume, modify the Volume type, and observe the alterations in disk capacity and IOPS.

EBS Operation: Volume Resizing



□	Name	Volume ID	Size	Volume Type	IOPS	Throughput	Snapshot
□		vol-05d9a9a...	8 GiB	gp2	100	-	
■		vol-06e80a1...	8 GiB			-	snap-0227dd6

It is impossible to reduce.



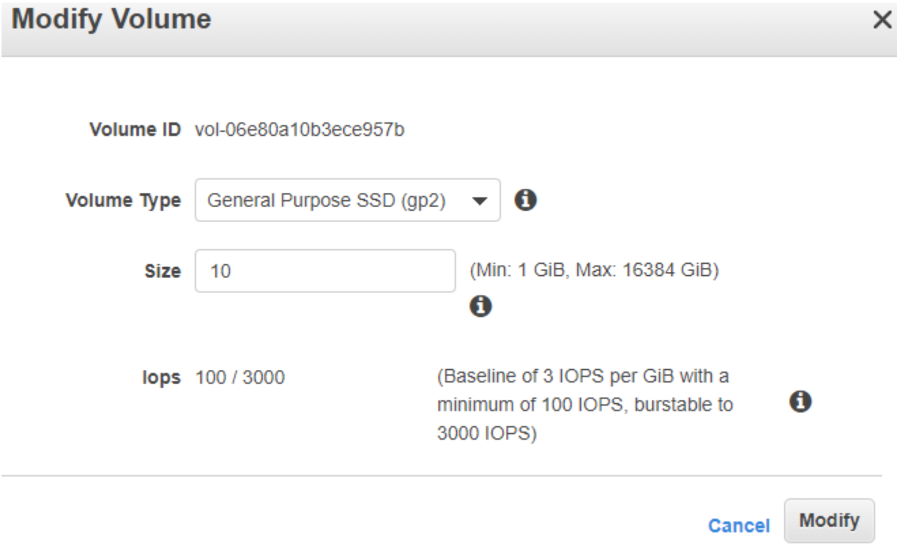
Volume ID vol-06e80a10b3ece957b

Volume Type General Purpose SSD (gp2)

Size 5 (Min: 1 GiB, Max: 16384 GiB)

The size of a volume can only be increased, not decreased.

Iops 100 / 3000 (Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS) only you can raise



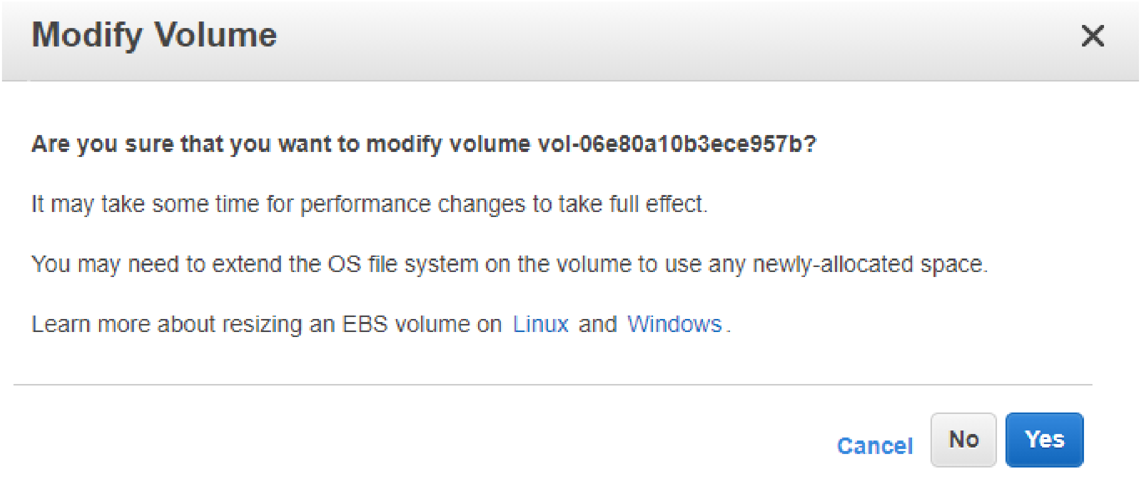
Modify Volume

Volume ID vol-06e80a10b3ece957b

Volume Type General Purpose SSD (gp2)

Size 10 (Min: 1 GiB, Max: 16384 GiB)

Iops 100 / 3000 (Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS)



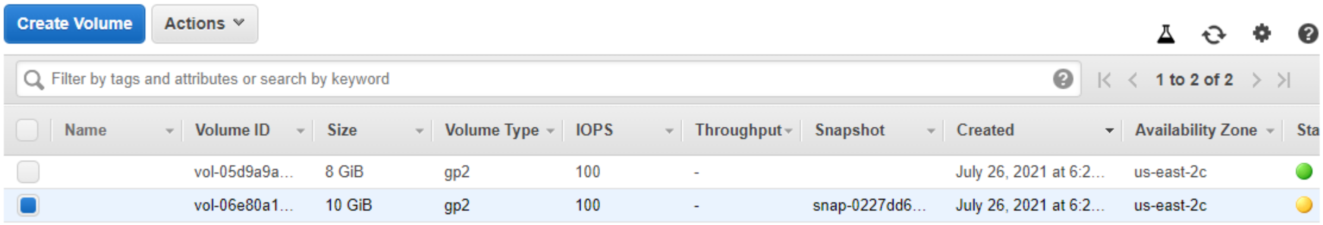
Modify Volume

Are you sure that you want to modify volume vol-06e80a10b3ece957b?

It may take some time for performance changes to take full effect.

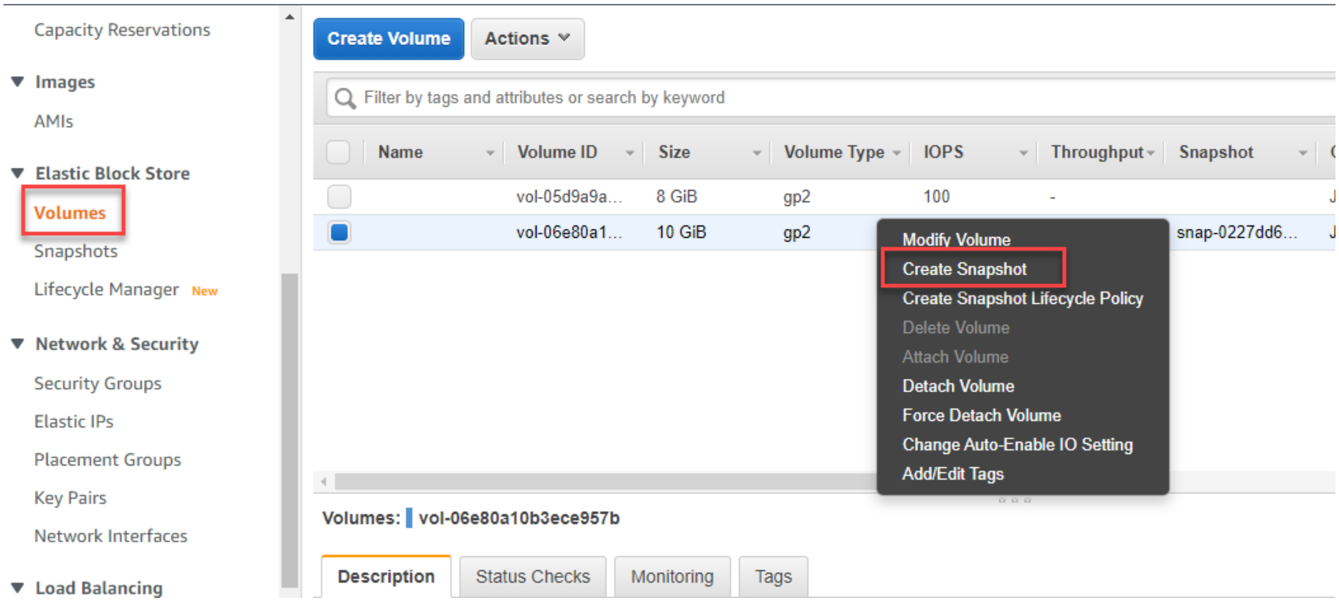
You may need to extend the OS file system on the volume to use any newly-allocated space.

Learn more about resizing an EBS volume on Linux and Windows.



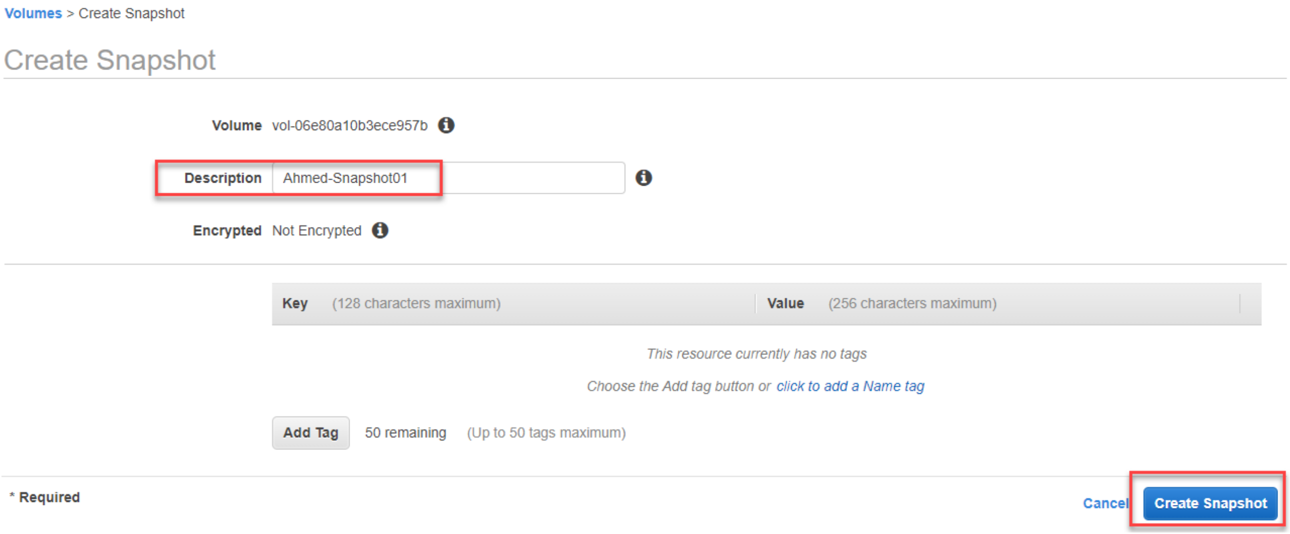
	Name	Volume ID	Size	Volume Type	IOPS	Throughput	Snapshot	Created	Availability Zone	Sta
□		vol-05d9a9a...	8 GiB	gp2	100	-		July 26, 2021 at 6:2...	us-east-2c	●
■		vol-06e80a1...	10 GiB	gp2	100	-	snap-0227dd6...	July 26, 2021 at 6:2...	us-east-2c	●

EBS Operation: Snapshots



	Name	Volume ID	Size	Volume Type	IOPS	Throughput	Snapshot
□		vol-05d9a9a...	8 GiB	gp2	100	-	
☑		vol-06e80a1...	10 GiB	gp2			snap-0227dd6...

Volumes: vol-06e80a10b3ece957b



Volume vol-06e80a10b3ece957b

Description Ahmed-Snapshot01

Encrypted Not Encrypted

Key (128 characters maximum) Value (256 characters maximum)

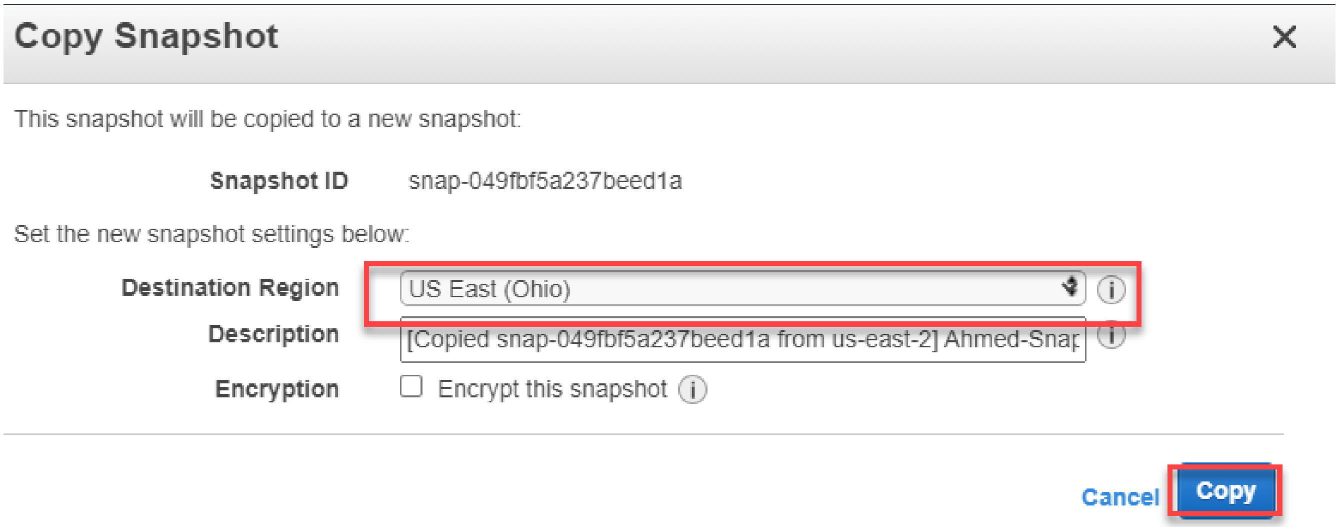
This resource currently has no tags

Choose the Add tag button or click to add a Name tag

50 remaining (Up to 50 tags maximum)

* Required

Additionally, you replicate the snapshot to a different region.



Copy Snapshot

This snapshot will be copied to a new snapshot:

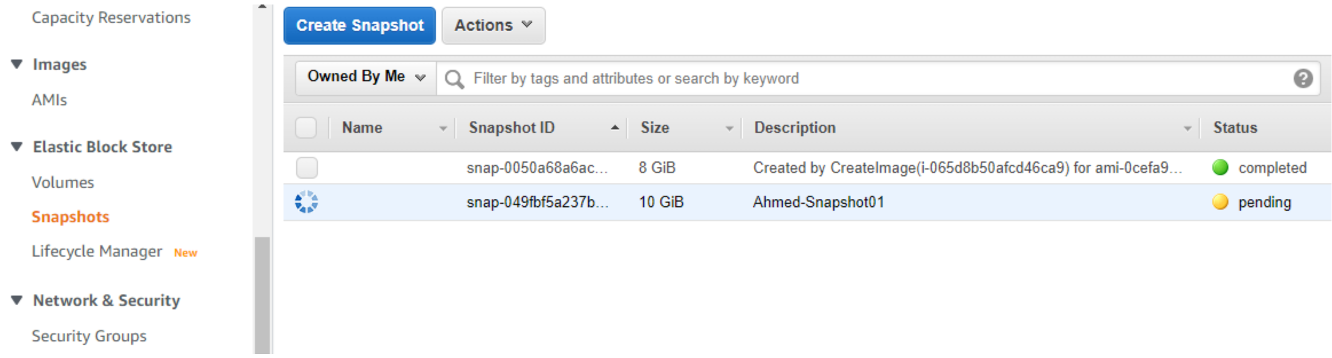
Snapshot ID snap-049fbf5a237beed1a

Set the new snapshot settings below:

Destination Region US East (Ohio)

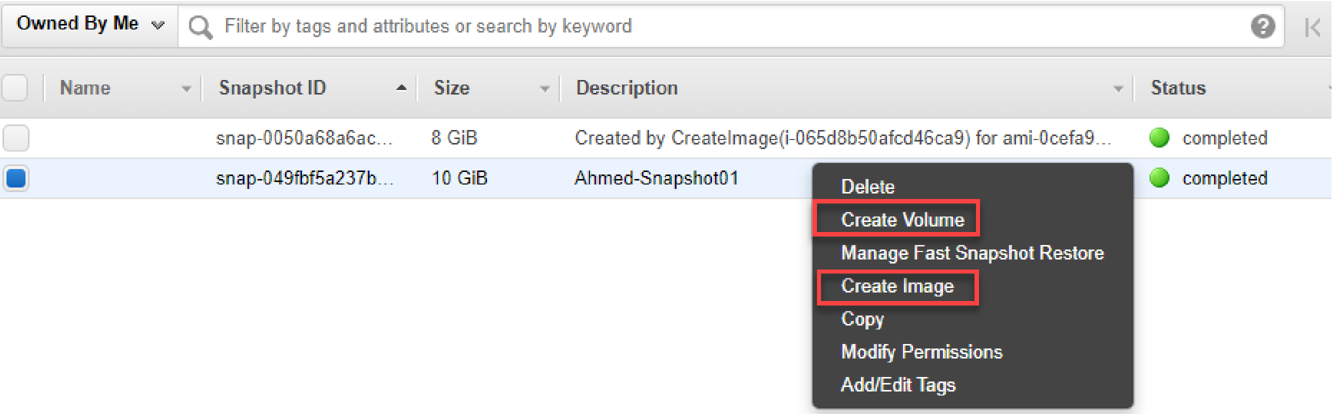
Description [Copied snap-049fbf5a237beed1a from us-east-2] Ahmed-Snap

Encryption □ Encrypt this snapshot



	Name	Snapshot ID	Size	Description	Status
□		snap-0050a68a6ac...	8 GiB	Created by CreateImage(i-065d8b50afcd46ca9) for ami-0cefa9...	completed
		snap-049fbf5a237b...	10 GiB	Ahmed-Snapshot01	pending

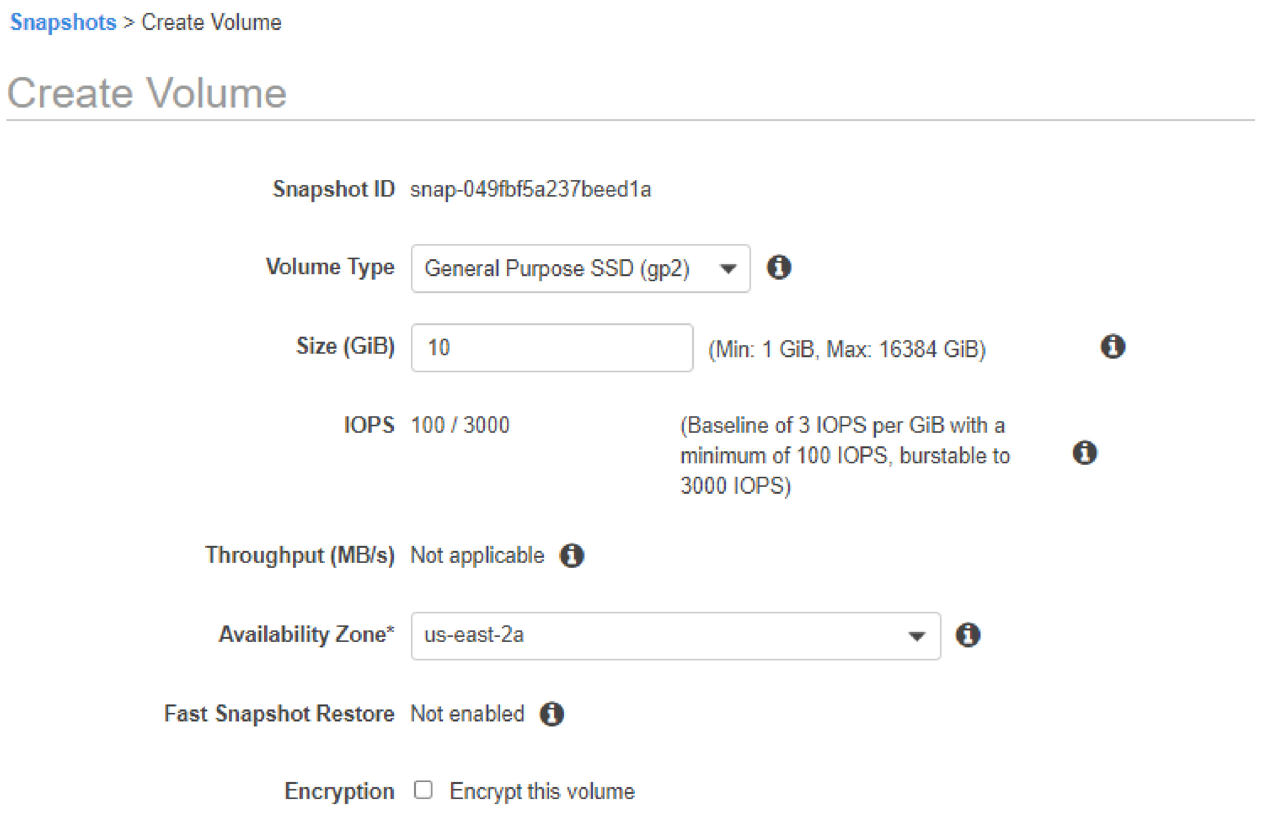
Additionally, you have the option to generate a volume or an image from the snapshot.



Owned By Me
Filter by tags and attributes or search by keyword

	Name	Snapshot ID	Size	Description	Status
□		snap-0050a68a6ac...	8 GiB	Created by CreateImage(i-065d8b50afcd46ca9) for ami-0cefa9...	completed
☑		snap-049fbf5a237b...	10 GiB	Ahmed-Snapshot01	completed

Delete
Create Volume
Manage Fast Snapshot Restore
Create Image
Copy
Modify Permissions
Add/Edit Tags



Snapshots > Create Volume

Create Volume

Snapshot ID snap-049fbf5a237beed1a

Volume Type General Purpose SSD (gp2)

Size (GiB) 10 (Min: 1 GiB, Max: 16384 GiB)

IOPS 100 / 3000 (Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS)

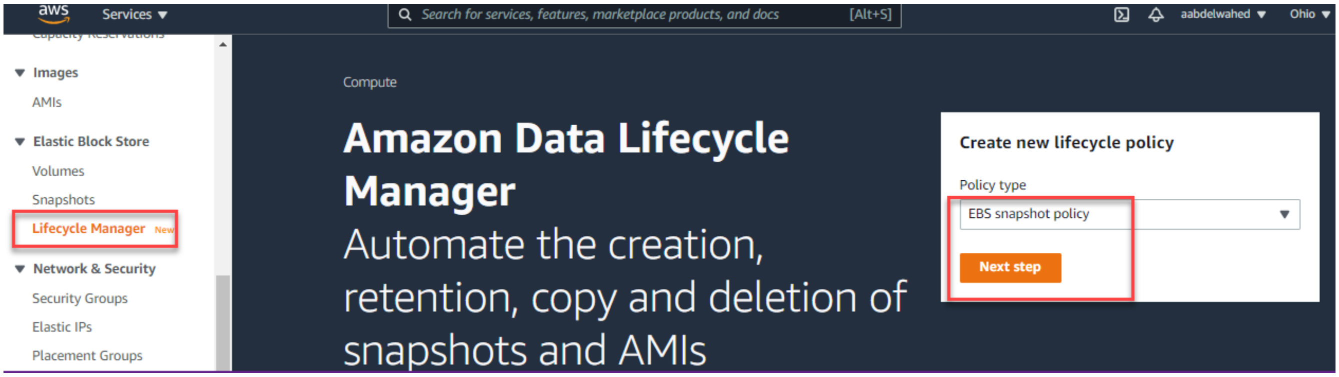
Throughput (MB/s) Not applicable

Availability Zone* us-east-2a

Fast Snapshot Restore Not enabled

Encryption ☐ Encrypt this volume

Automatic snapshot



Compute

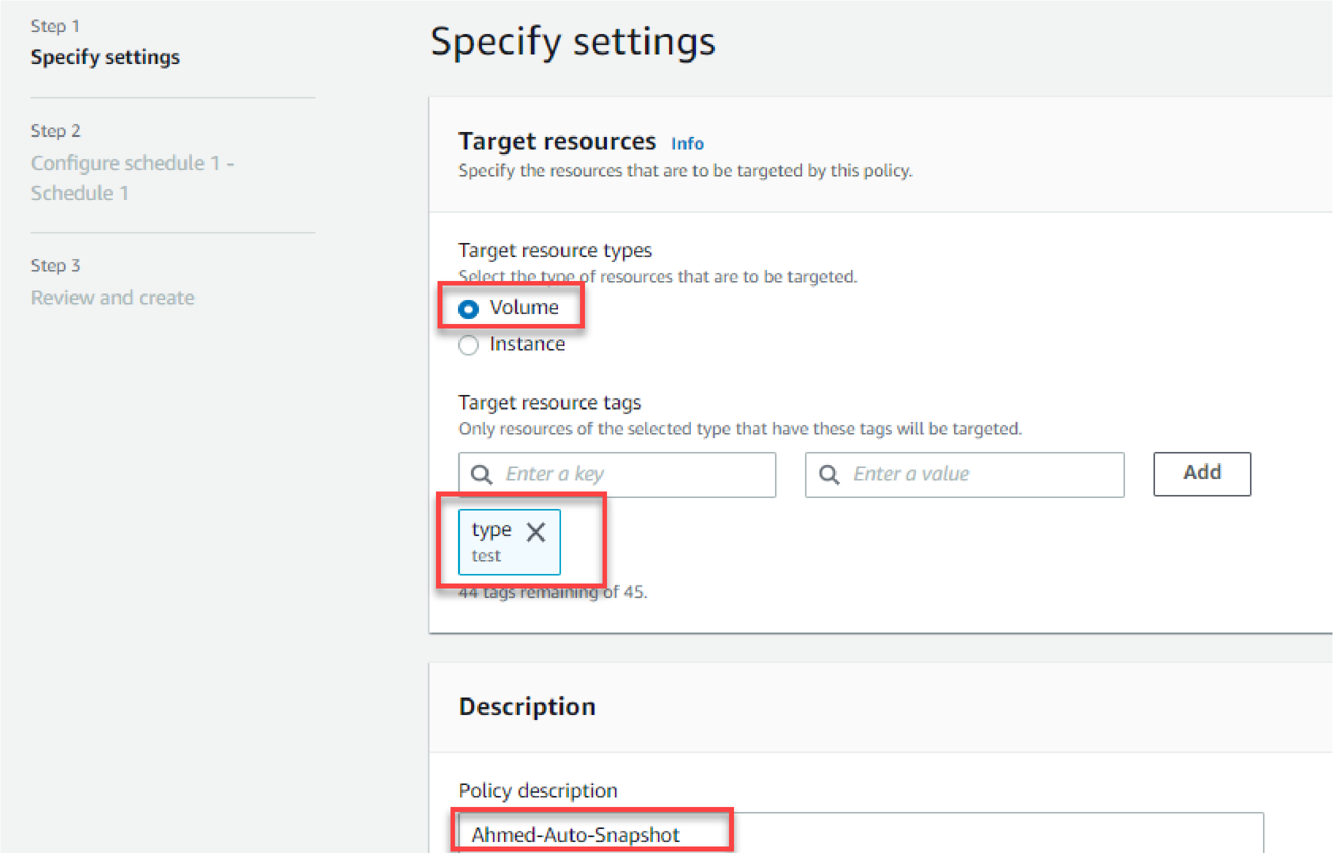
Amazon Data Lifecycle Manager

Automate the creation, retention, copy and deletion of snapshots and AMIs

Create new lifecycle policy

Policy type: EBS snapshot policy

Next step



Step 1
Specify settings

Step 2
Configure schedule 1 - Schedule 1

Step 3
Review and create

Specify settings

Target resources Info
Specify the resources that are to be targeted by this policy.

Target resource types
Select the type of resources that are to be targeted.

● Volume
○ Instance

Target resource tags
Only resources of the selected type that have these tags will be targeted.

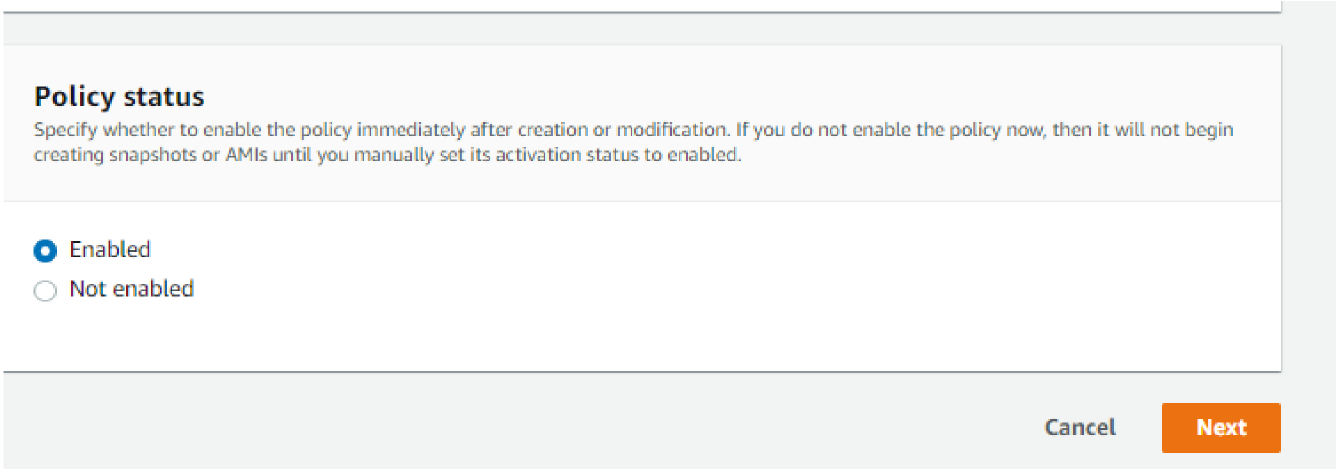
Enter a key | Enter a value | Add

type ✕
test

44 tags remaining of 45.

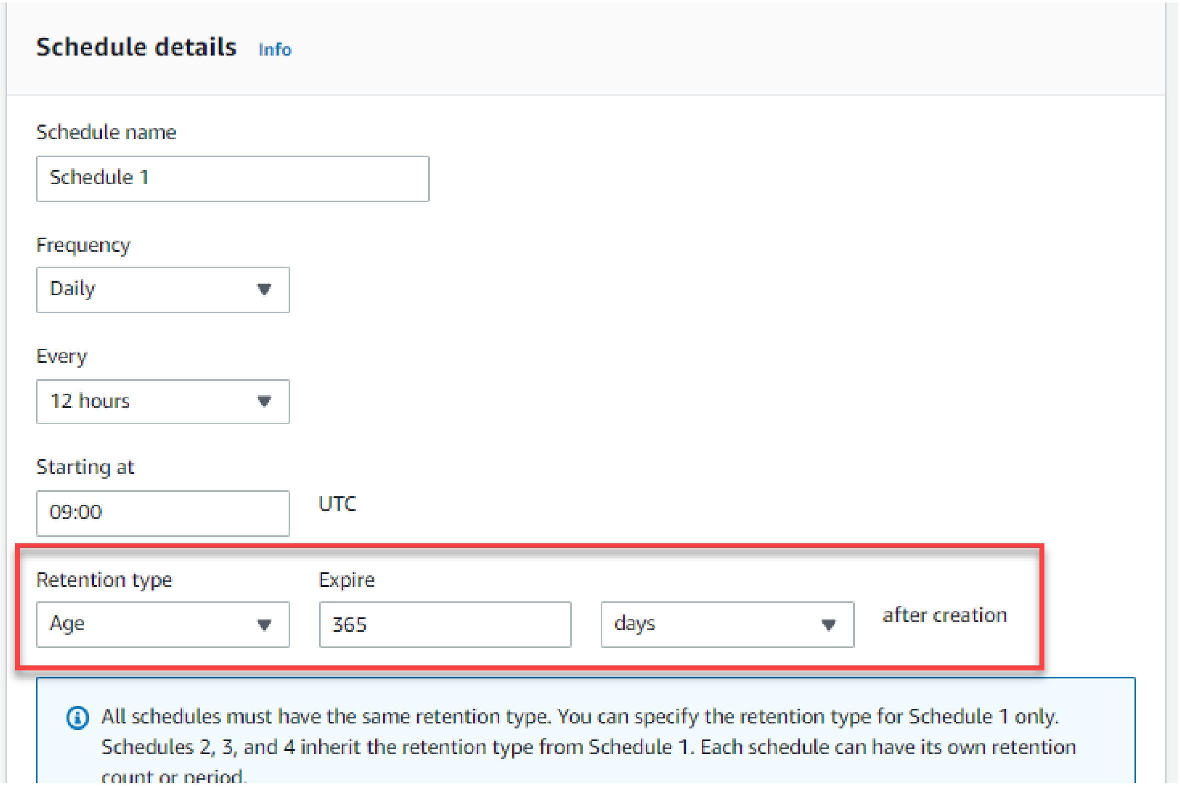
Description

Policy description
Ahmed-Auto-Snapshot



Policy status
Specify whether to enable the policy immediately after creation or modification. If you do not enable the policy now, then it will not begin creating snapshots or AMIs until you manually set its activation status to enabled.

● Enabled
○ Not enabled



Schedule details Info

Schedule name: Schedule 1

Frequency: Daily

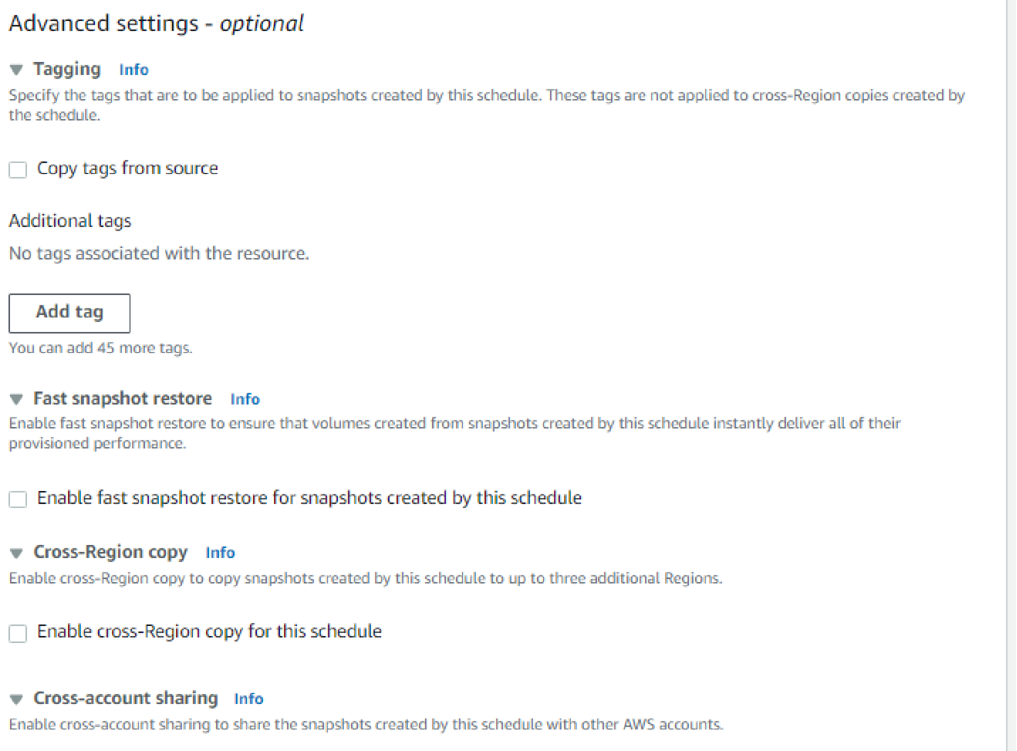
Every: 12 hours

Starting at: 09:00 UTC

Retention type: Age

Expire: 365 days after creation

ⓘ All schedules must have the same retention type. You can specify the retention type for Schedule 1 only. Schedules 2, 3, and 4 inherit the retention type from Schedule 1. Each schedule can have its own retention count or period.



Advanced settings - *optional*

▼ **Tagging** Info

Specify the tags that are to be applied to snapshots created by this schedule. These tags are not applied to cross-Region copies created by the schedule.

□ Copy tags from source

Additional tags

No tags associated with the resource.

You can add 45 more tags.

▼ **Fast snapshot restore** Info

Enable fast snapshot restore to ensure that volumes created from snapshots created by this schedule instantly deliver all of their provisioned performance.

□ Enable fast snapshot restore for snapshots created by this schedule

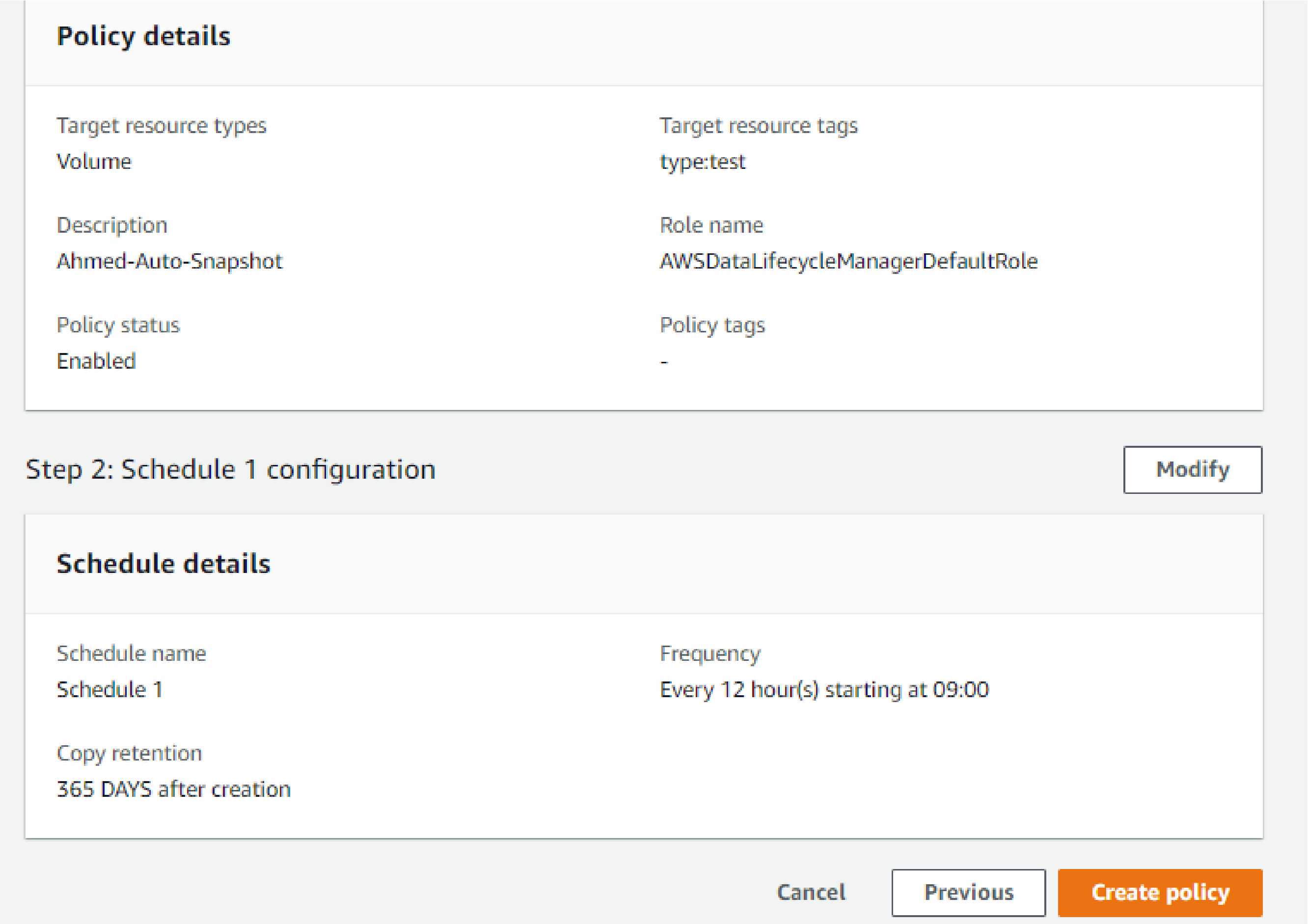
▼ **Cross-Region copy** Info

Enable cross-Region copy to copy snapshots created by this schedule to up to three additional Regions.

□ Enable cross-Region copy for this schedule

▼ **Cross-account sharing** Info

Enable cross-account sharing to share the snapshots created by this schedule with other AWS accounts.



Policy details

Target resource types
Volume

Target resource tags
type:test

Description
Ahmed-Auto-Snapshot

Role name
AWSDataLifecycleManagerDefaultRole

Policy status
Enabled

Policy tags
-

Step 2: Schedule 1 configuration

Schedule details

Schedule name
Schedule 1

Frequency
Every 12 hour(s) starting at 09:00

Copy retention
365 DAYS after creation

Amazon EC2

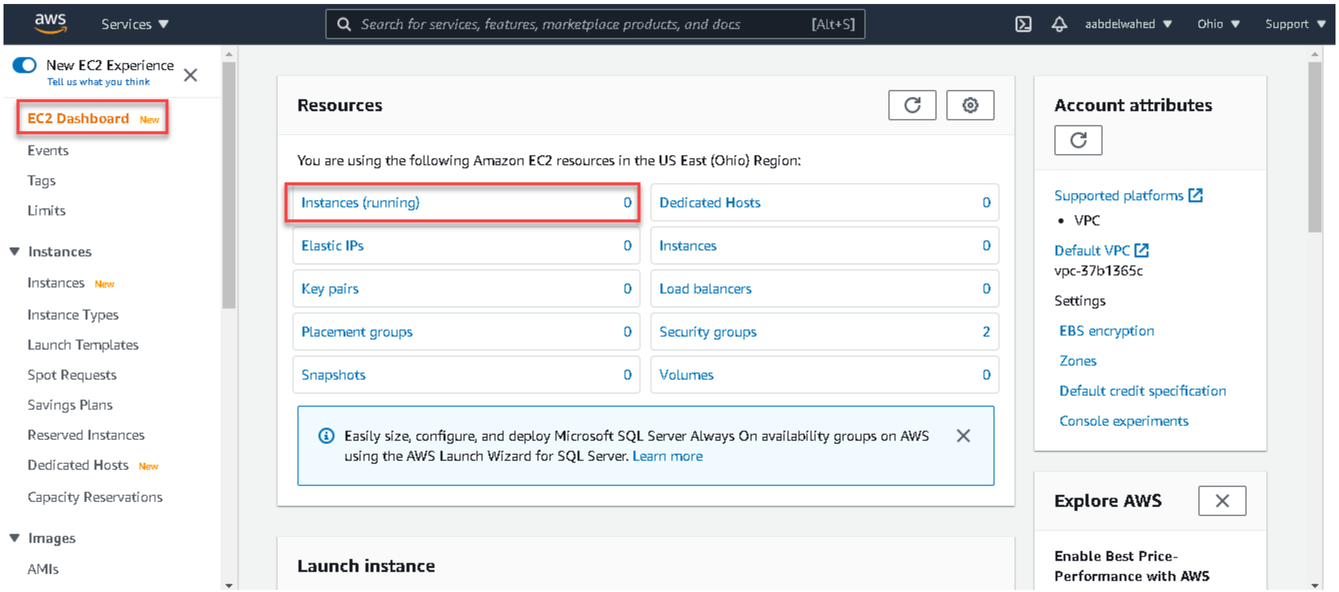
EC2 Types:

1. **On Demand:** Default, pay-as-you-go, most expensive for long term, ideal for unpredictable workloads.
2. **Reserved:** Long-term usage, up to 75% discount, available in 1-year or 3-year terms.
3. **Spot:** Low cost, terminates if spot price exceeds bid, suitable for flexible start and end times.
4. **Dedicated Host:** Physical server dedicated to you, required by some vendors, provides visibility and control over socket, core, and host ID.
5. **Dedicated Instance:** Dedicated hardware in a dedicated VPC, suitable for isolated workloads.

Security Group:

- Instance-level firewall that allows or denies traffic based on protocol and port, stateful, meaning return traffic is automatically allowed, operates at the instance level, not at the subnet level.

Set Up Linux EC2 Instance

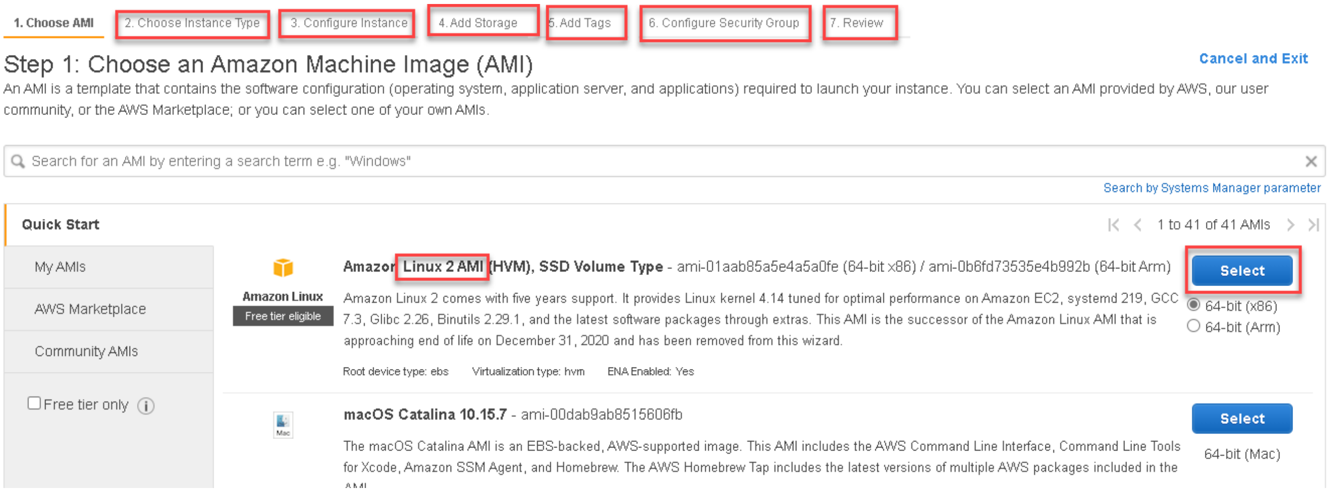


You are using the following Amazon EC2 resources in the US East (Ohio) Region:

Instances (running)	0	Dedicated Hosts	0
Elastic IPs	0	Instances	0
Key pairs	0	Load balancers	0
Placement groups	0	Security groups	2
Snapshots	0	Volumes	0

Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. Learn more

Choose a Linux distribution



Step 1: Choose an Amazon Machine Image (AMI)

Cancel and Exit

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

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

Search by Systems Manager parameter

Amazon Linux
Free tier eligible

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-01aab85a5e4a5a0fe (64-bit x86) / ami-0b6fd73535e4b992b (64-bit Arm)

Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is approaching end of life on December 31, 2020 and has been removed from this wizard.

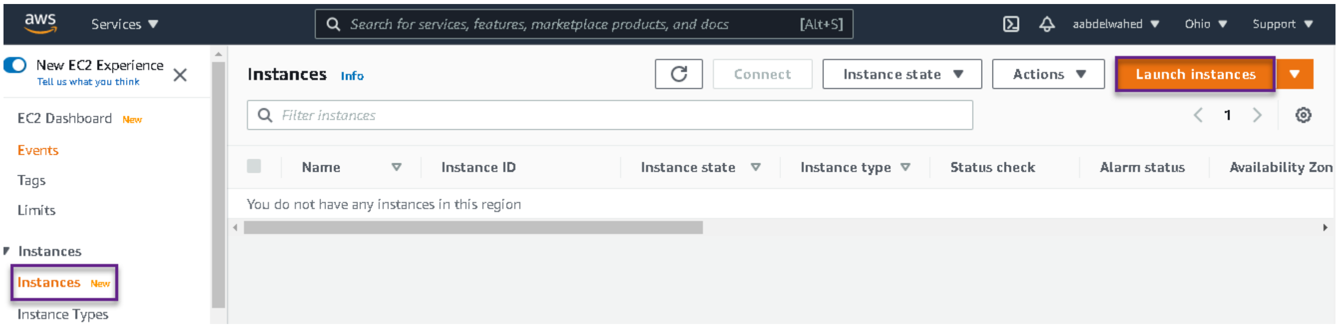
Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Select
● 64-bit (x86)
○ 64-bit (Arm)

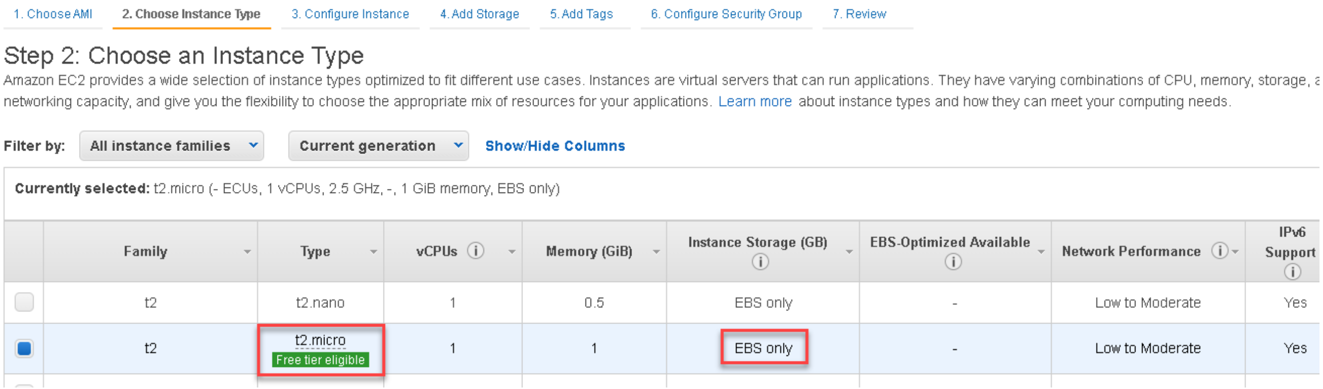
macOS Catalina 10.15.7 - ami-00dab9ab8515606fb

The macOS Catalina AMI is an EBS-backed, AWS-supported image. This AMI includes the AWS Command Line Interface, Command Line Tools for Xcode, Amazon SSM Agent, and Homebrew. The AWS Homebrew Tap includes the latest versions of multiple AWS packages included in the

Select
64-bit (Mac)



You do not have any instances in this region



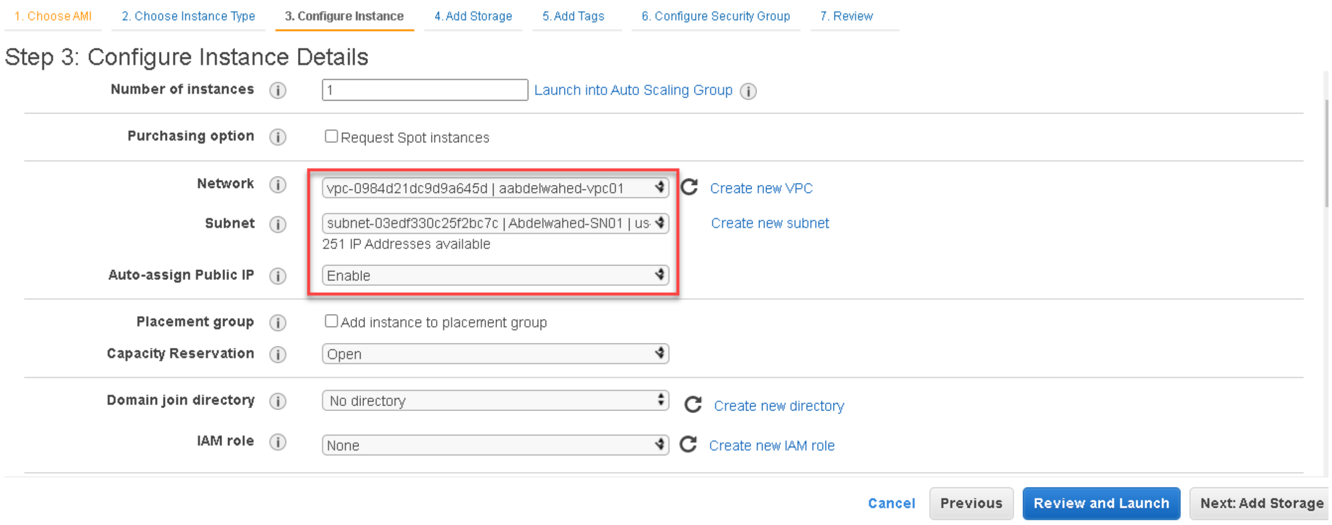
Step 2: Choose an Instance Type

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

Filter by: All instance families Current generation **Show/Hide Columns**

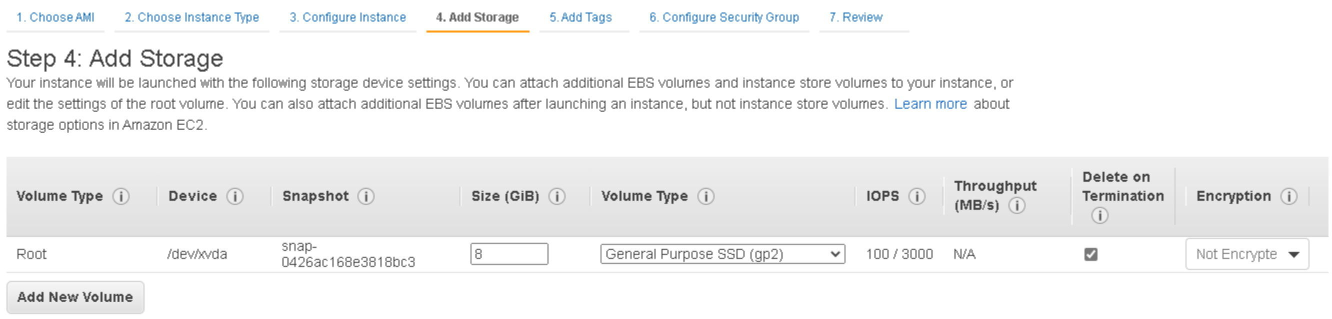
Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
□	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
☑	t2	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes



Step 3: Configure Instance Details

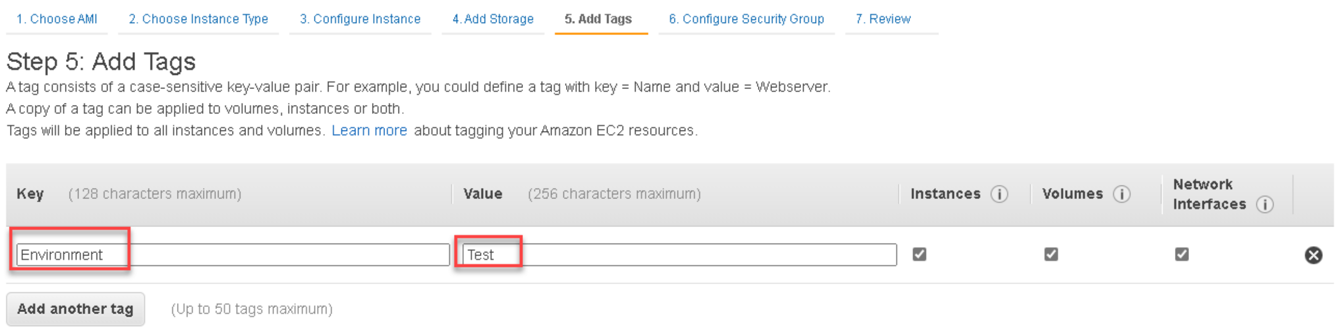
Number of instances	1 — Launch into Auto Scaling Group
Purchasing option	□ Request Spot instances
Network	vpc-0984d21dc9d9a645d | aabdelwahed-vpc01 — Create new VPC
Subnet	subnet-03edf330c25f2bc7c | Abdelwahed-SN01 | us- — Create new subnet 251 IP Addresses available
Auto-assign Public IP	Enable
Placement group	□ Add instance to placement group
Capacity Reservation	Open
Domain join directory	No directory — Create new directory
IAM role	None — Create new IAM role



Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

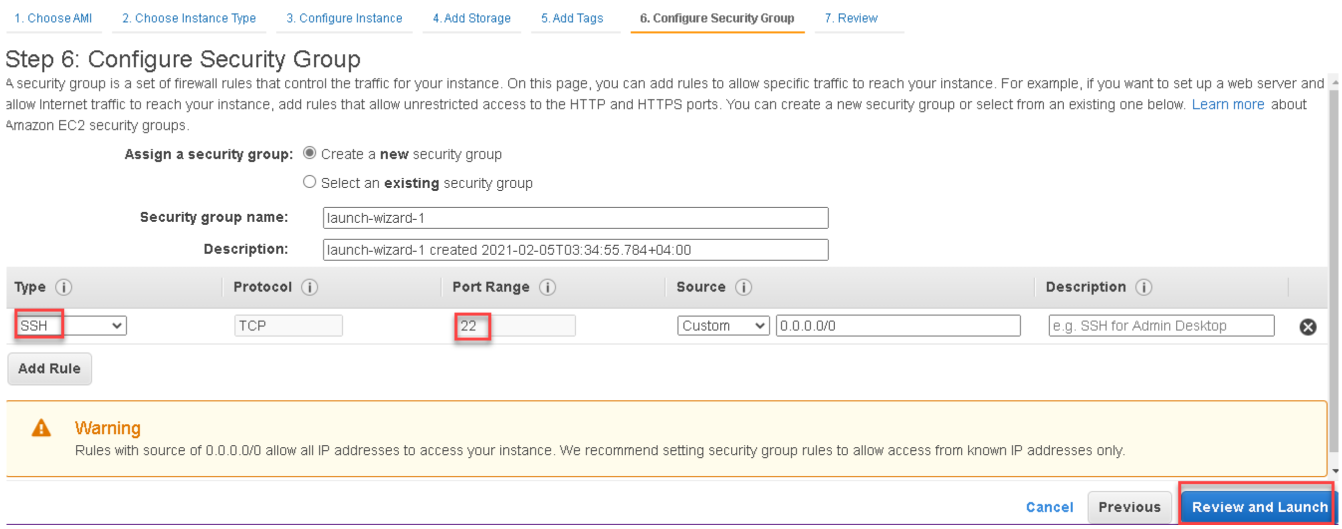
Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-0426ac168e3818bc3	8	General Purpose SSD (gp2)	100 / 3000	N/A	☑	Not Encrypte



Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes	Network Interfaces
Environment	Test	☑	☑	☑



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ● Create a **new** security group

○ Select an **existing** security group

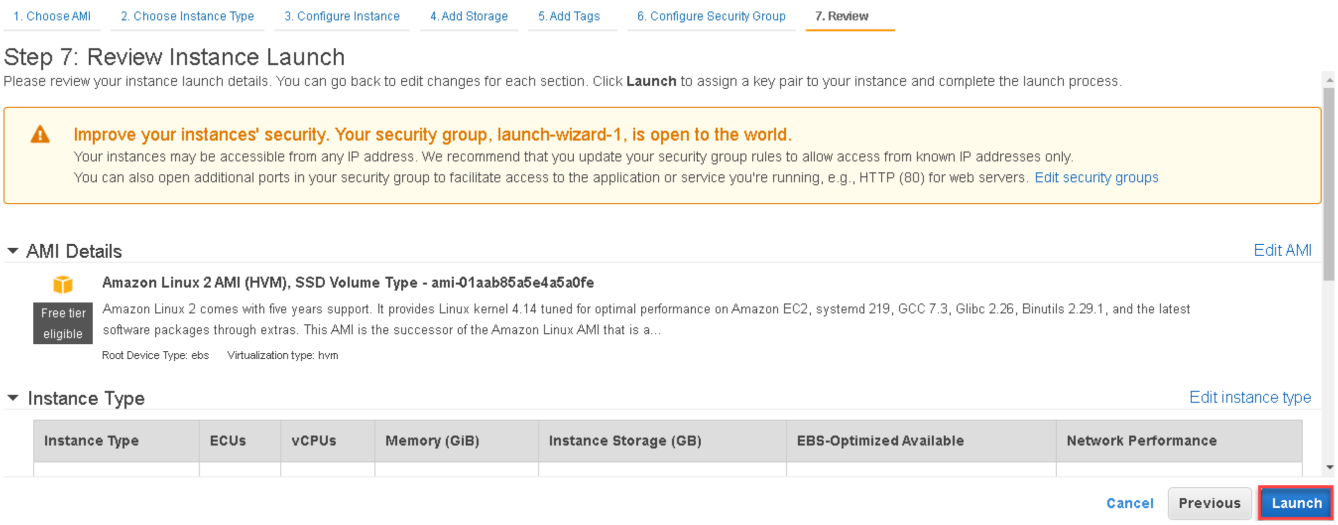
Security group name: launch-wizard-1

Description: launch-wizard-1 created 2021-02-05T03:34:55.784+04:00

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

Warning

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



Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

Improve your instances' security. Your security group, launch-wizard-1, is open to the world.

Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only.
You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. Edit security groups

AMI Details — Edit AMI

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-01aab85a5e4a5a0fe

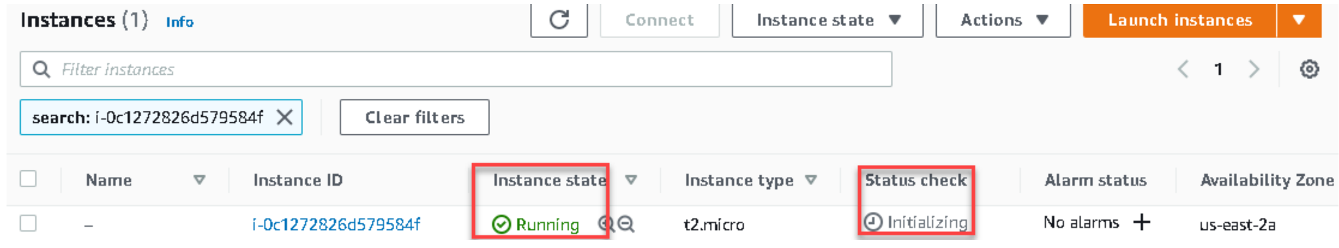
Free tier eligible

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

Root Device Type: ebs Virtualization type: hvm

Instance Type — Edit instance type

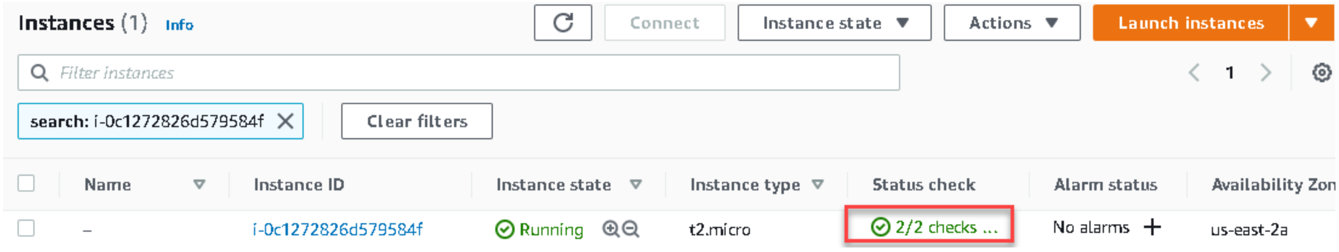
Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance



Instances (1) Info

search: i-0c1272826d579584f ✕ Clear filters

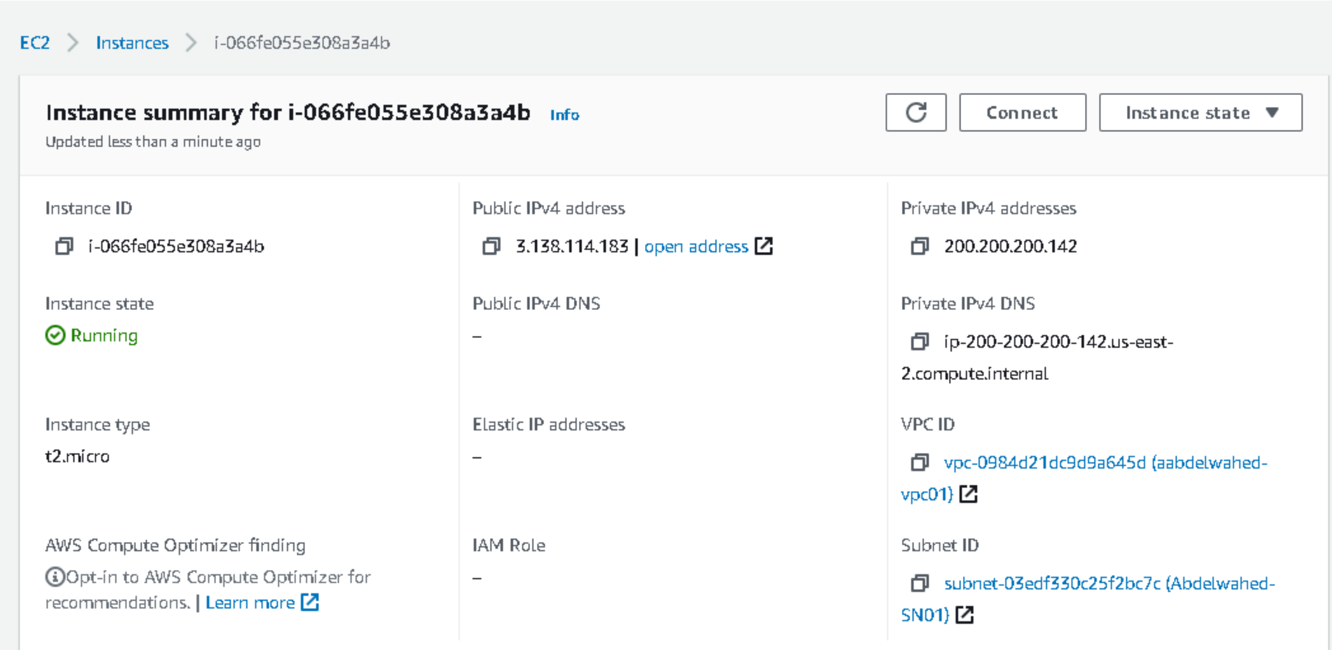
	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
□	–	i-0c1272826d579584f	Running	t2.micro	Initializing	No alarms +	us-east-2a



Instances (1) Info

search: i-0c1272826d579584f ✕ Clear filters

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zon
□	–	i-0c1272826d579584f	Running	t2.micro	2/2 checks ...	No alarms +	us-east-2a



EC2 > Instances > i-066fe055e308a3a4b

Instance summary for i-066fe055e308a3a4b Info

Updated less than a minute ago

Instance ID: i-066fe055e308a3a4b

Public IPv4 address: 3.138.114.183 | open address

Private IPv4 addresses: 200.200.200.142

Instance state: Running

Public IPv4 DNS: –

Private IPv4 DNS: ip-200-200-200-142.us-east-2.compute.internal

Instance type: t2.micro

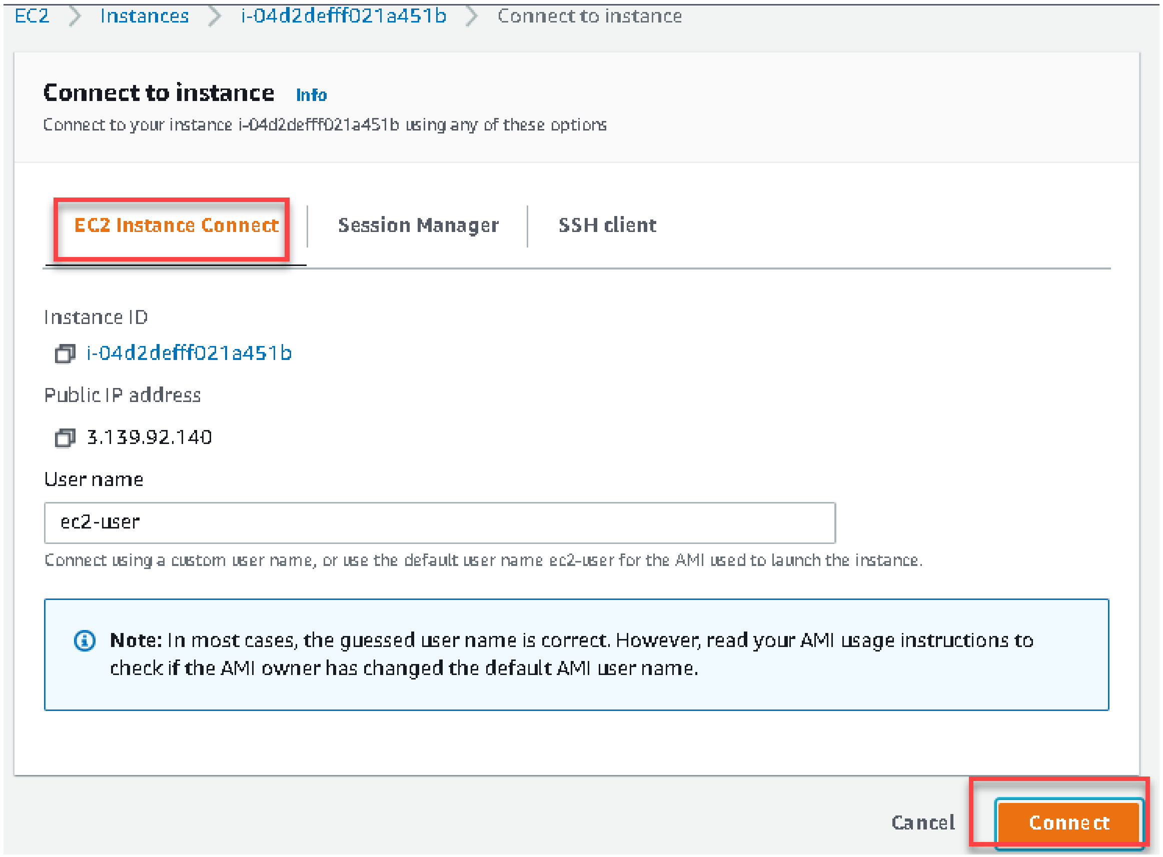
Elastic IP addresses: –

VPC ID: vpc-0984d21dc9d9a645d (aabdelwahed-vpc01)

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

IAM Role: –

Subnet ID: subnet-03edf330c25f2bc7c (Abdelwahed-SN01)



EC2 > Instances > i-04d2defff021a451b > Connect to instance

Connect to instance Info

Connect to your instance i-04d2defff021a451b using any of these options

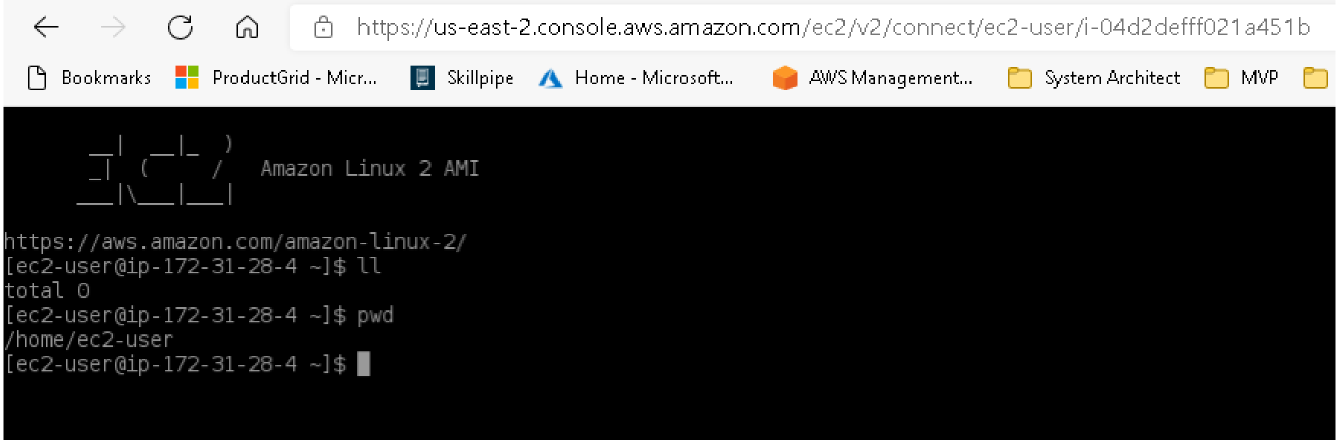
Instance ID: i-04d2defff021a451b

Public IP address: 3.139.92.140

User name: ec2-user

Connect using a custom user name, or use the default user name ec2-user for the AMI used to launch the instance.

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



```
       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-28-4 ~]$ ll
total 0
[ec2-user@ip-172-31-28-4 ~]$ pwd
/home/ec2-user
[ec2-user@ip-172-31-28-4 ~]$ 
```

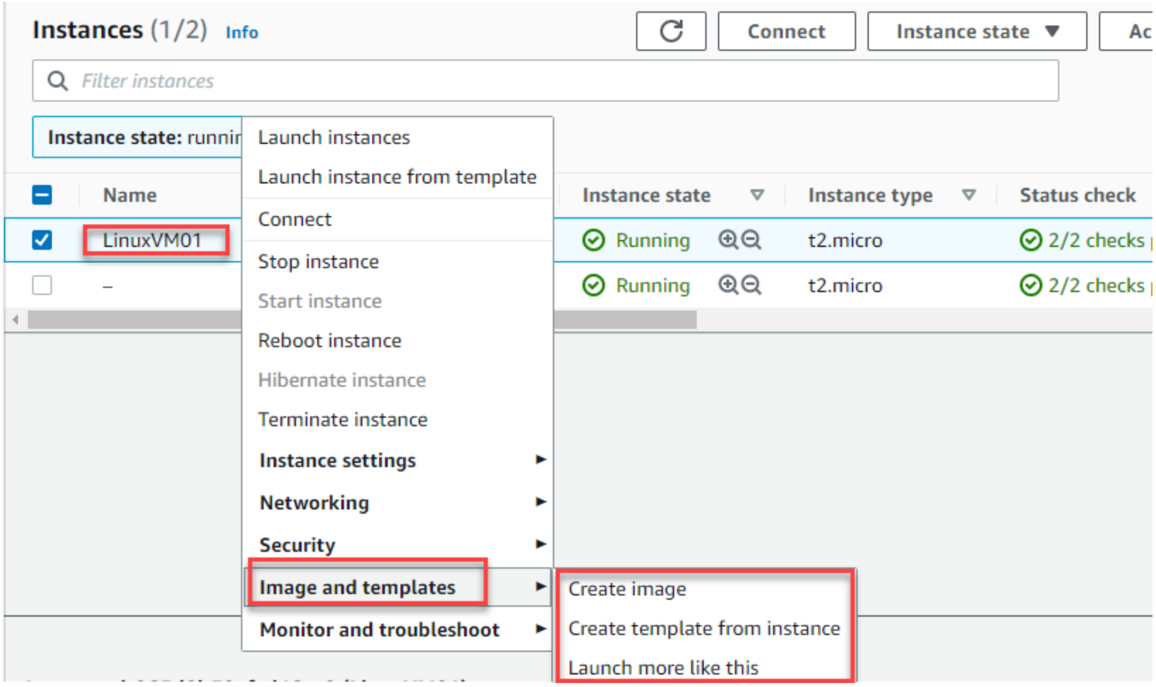
Use the command line to access your EC2 instance:

```
ssh -i "C:\Downloads/AbdelwahedKey01.pem" ec2-user@ec2-3-139-92-140.us-east-2.compute.amazonaws.com
```

Amazon Machine Images (AMI)

You can create your own images; for example, you can configure one EC2 machine and then use it as your own custom AMI, allowing you to use it as a pre-configured machine.

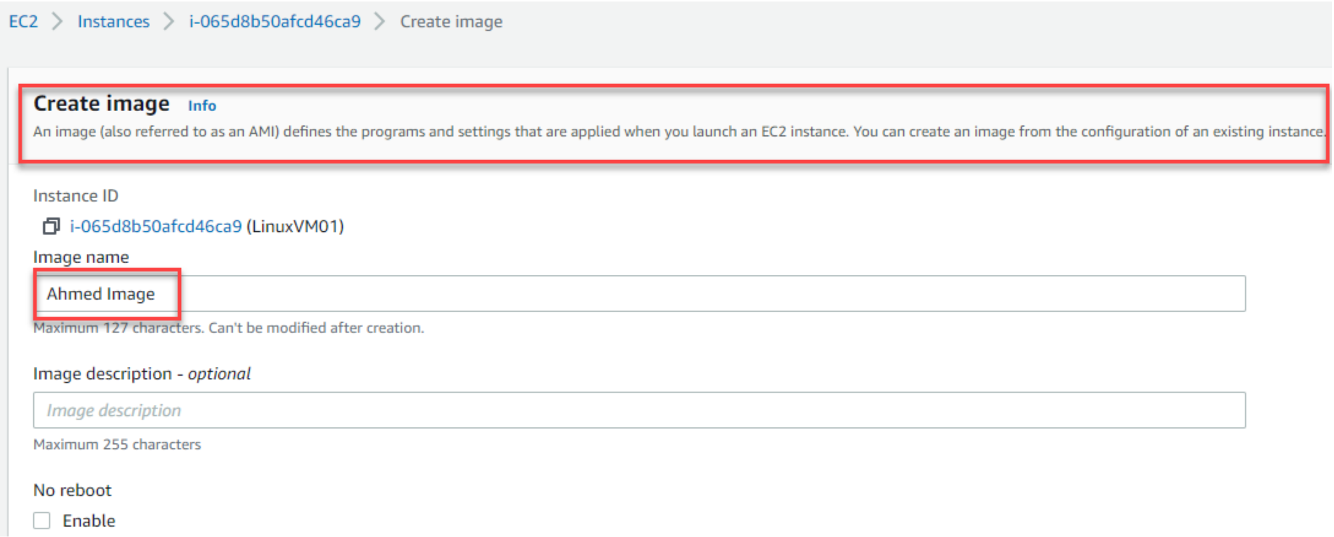
In this example, I have one EC2 Linux instance where I will install and configure the httpd service with a custom default page, then allow port 80 so it can be accessed from the internet using the public IP. Here are the steps to use it as a custom AMI:



Instances (1/2) Info

Instance state: runnir

☐	Name	Instance state	Instance type	Status check
☑	LinuxVM01	Running	t2.micro	2/2 checks
☐	–	Running	t2.micro	2/2 checks



EC2 > Instances > i-065d8b50afcd46ca9 > Create image

Create image Info

An image (also referred to as an AMI) defines the programs and settings that are applied when you launch an EC2 instance. You can create an image from the configuration of an existing instance.

Instance ID

i-065d8b50afcd46ca9 (LinuxVM01)

Image name

Ahmed Image

Maximum 127 characters. Can't be modified after creation.

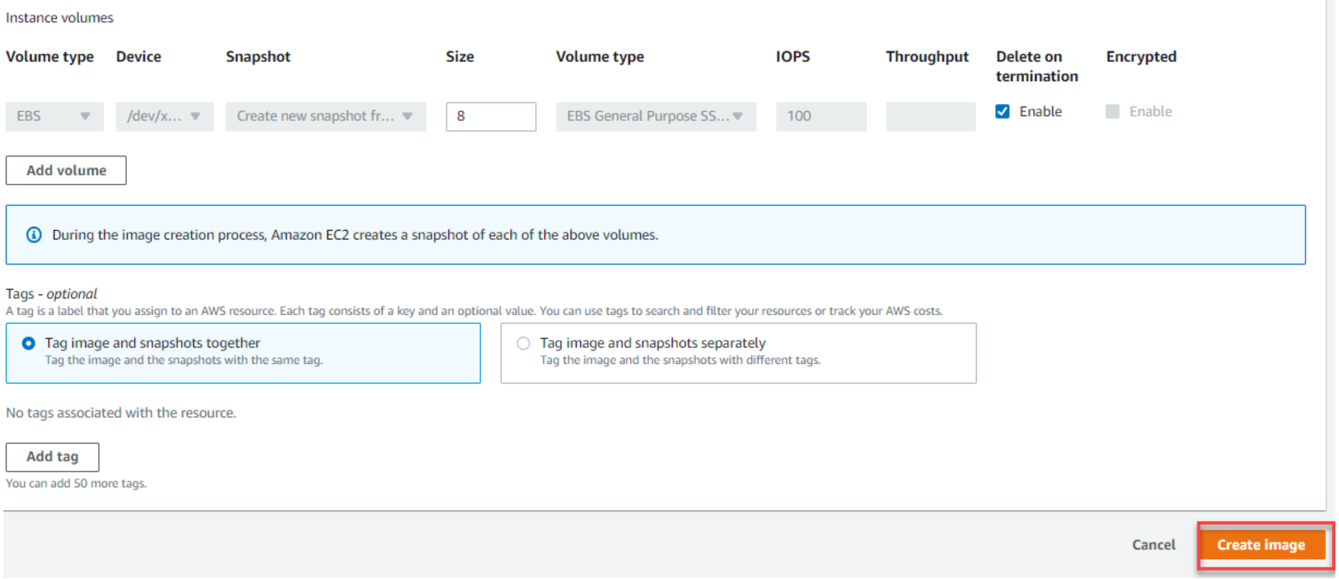
Image description - *optional*

Image description

Maximum 255 characters

No reboot

☐ Enable



Instance volumes

Volume type	Device	Snapshot	Size	Volume type	IOPS	Throughput	Delete on termination	Encrypted
EBS	/dev/x...	Create new snapshot fr...	8	EBS General Purpose SS...	100		☑ Enable	□ Enable

Add volume

ⓘ During the image creation process, Amazon EC2 creates a snapshot of each of the above volumes.

Tags - *optional*

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

● Tag image and snapshots together
Tag the image and the snapshots with the same tag.

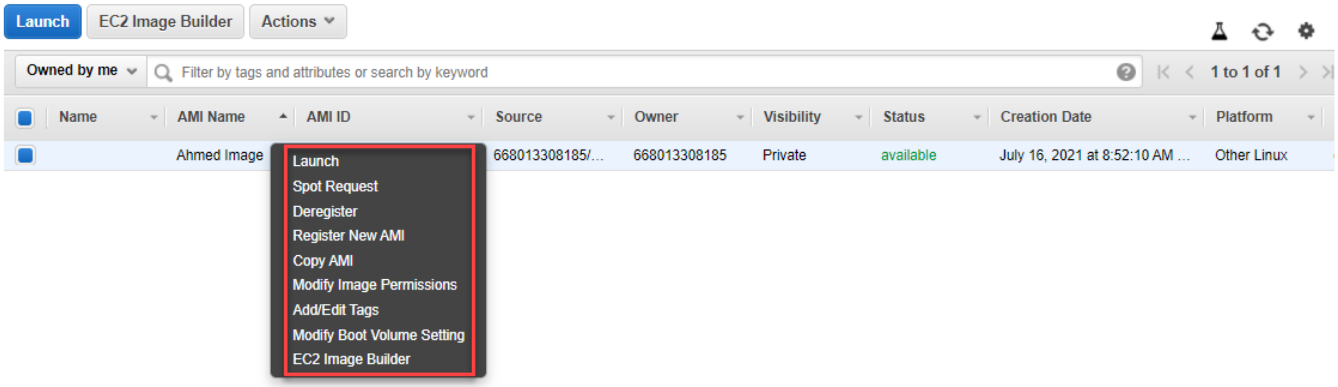
○ Tag image and snapshots separately
Tag the image and the snapshots with different tags.

No tags associated with the resource.

Add tag

You can add 50 more tags.

Cancel | Create image

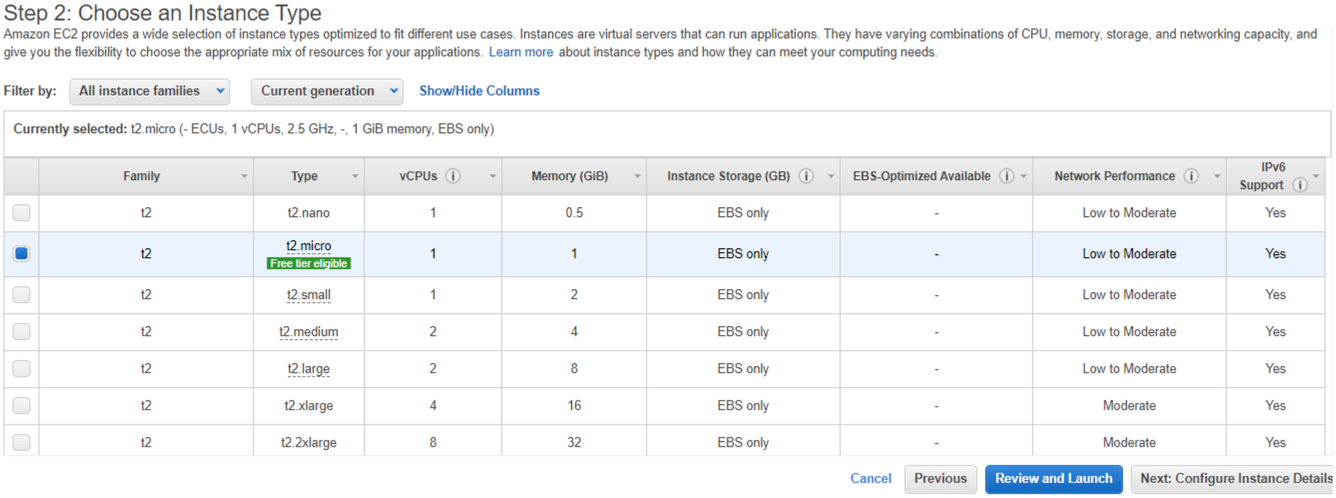


Launch | EC2 Image Builder | Actions ▾

Owned by me ▾ | Filter by tags and attributes or search by keyword | 1 to 1 of 1

	Name	AMI Name	AMI ID	Source	Owner	Visibility	Status	Creation Date	Platform
☑		Ahmed Image		668013308185/...	668013308185	Private	available	July 16, 2021 at 8:52:10 AM ...	Other Linux

I will initiate another EC2 instance using this by choosing the launch option.



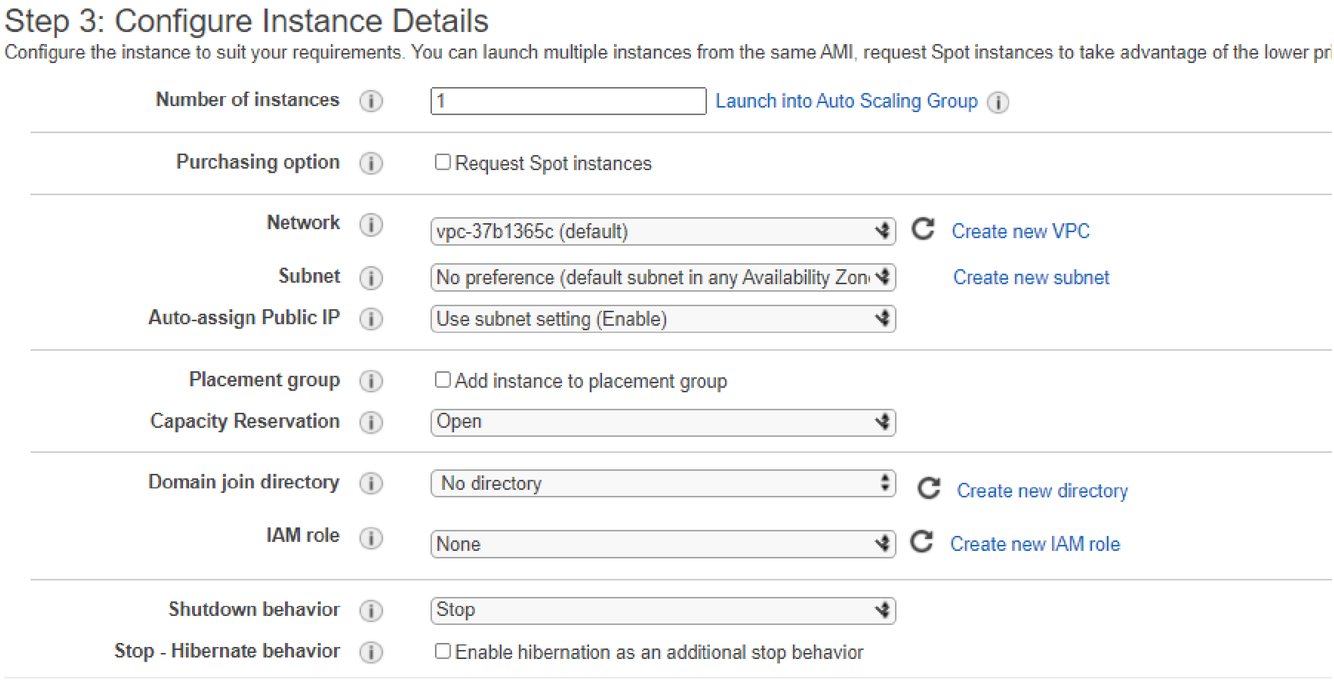
Step 2: Choose an Instance Type

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

Filter by: All instance families · Current generation · Show/Hide Columns

Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)

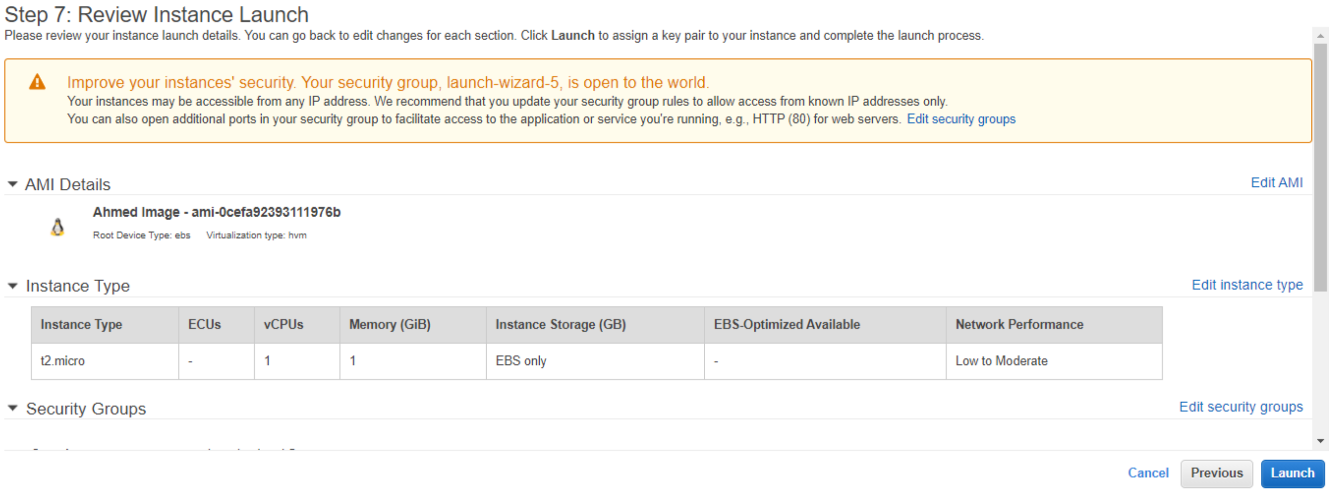
	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
☐	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
☑	t2	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
☐	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
☐	t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
☐	t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes
☐	t2	t2.xlarge	4	16	EBS only	-	Moderate	Yes
☐	t2	t2.2xlarge	8	32	EBS only	-	Moderate	Yes



Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pri

Number of instances	1 Launch into Auto Scaling Group
Purchasing option	☐ Request Spot instances
Network	vpc-37b1365c (default) Create new VPC
Subnet	No preference (default subnet in any Availability Zon Create new subnet
Auto-assign Public IP	Use subnet setting (Enable)
Placement group	☐ Add instance to placement group
Capacity Reservation	Open
Domain join directory	No directory Create new directory
IAM role	None Create new IAM role
Shutdown behavior	Stop
Stop - Hibernate behavior	☐ Enable hibernation as an additional stop behavior



Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

Improve your instances' security. Your security group, launch-wizard-5, is open to the world.
Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only.
You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. Edit security groups

▾ AMI Details — Edit AMI

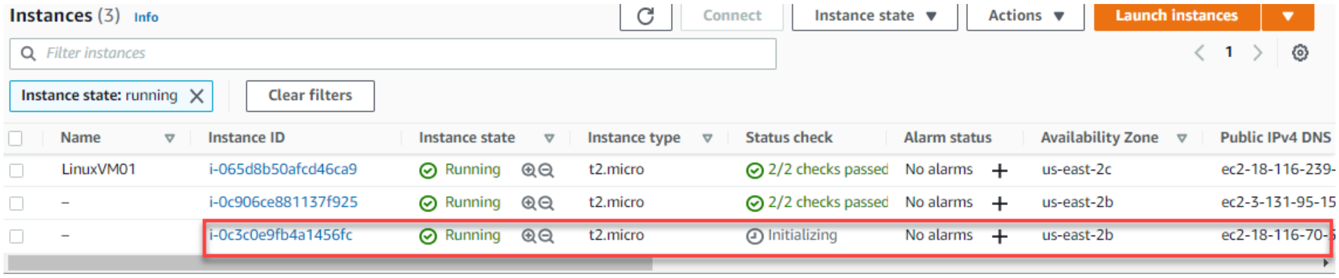
Ahmed Image - ami-0cefa92393111976b
Root Device Type: ebs   Virtualization type: hvm

▾ Instance Type — Edit instance type

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

▾ Security Groups — Edit security groups

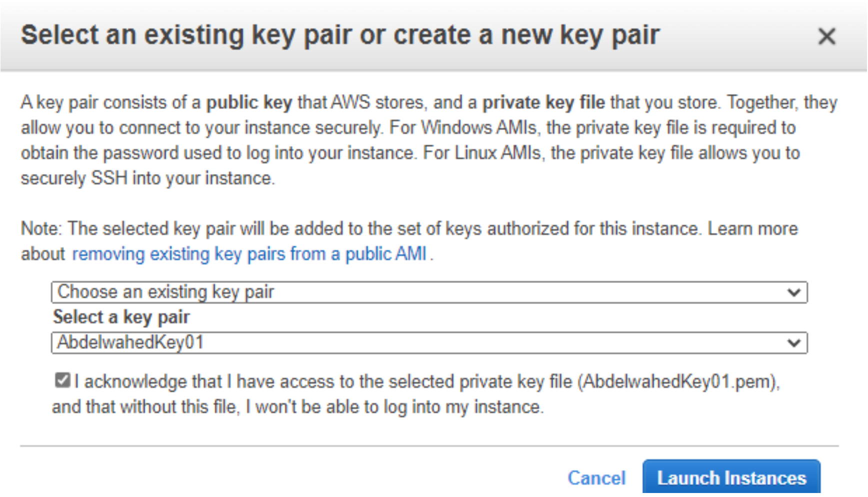
Once operational, you should verify that the web service functions over the internet in the same manner as it did with the previous EC2 configurations.



Instances (3) Info

Instance state: running

□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
□	LinuxVM01	i-065d8b50afcd46ca9	Running	t2.micro	2/2 checks passed	No alarms	us-east-2c	ec2-18-116-239-
□	–	i-0c906ce881137f925	Running	t2.micro	2/2 checks passed	No alarms	us-east-2b	ec2-3-131-95-15
□	–	i-0c3c0e9fb4a1456fc	Running	t2.micro	Initializing	No alarms	us-east-2b	ec2-18-116-70-



Select an existing key pair or create a new key pair

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

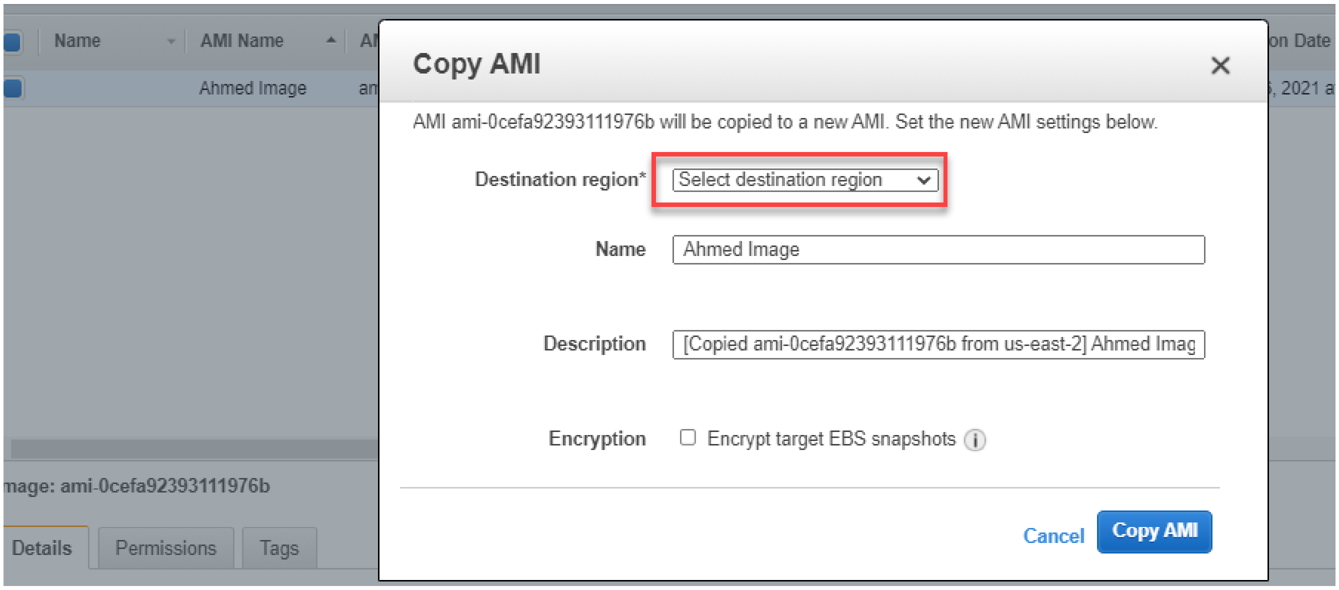
Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI .

Choose an existing key pair

Select a key pair
AbdelwahedKey01

☑ I acknowledge that I have access to the selected private key file (AbdelwahedKey01.pem), and that without this file, I won't be able to log into my instance.

Additionally, AMI can be replicated to a different region or account.



AMI ami-0cefa92393111976b will be copied to a new AMI. Set the new AMI settings below.

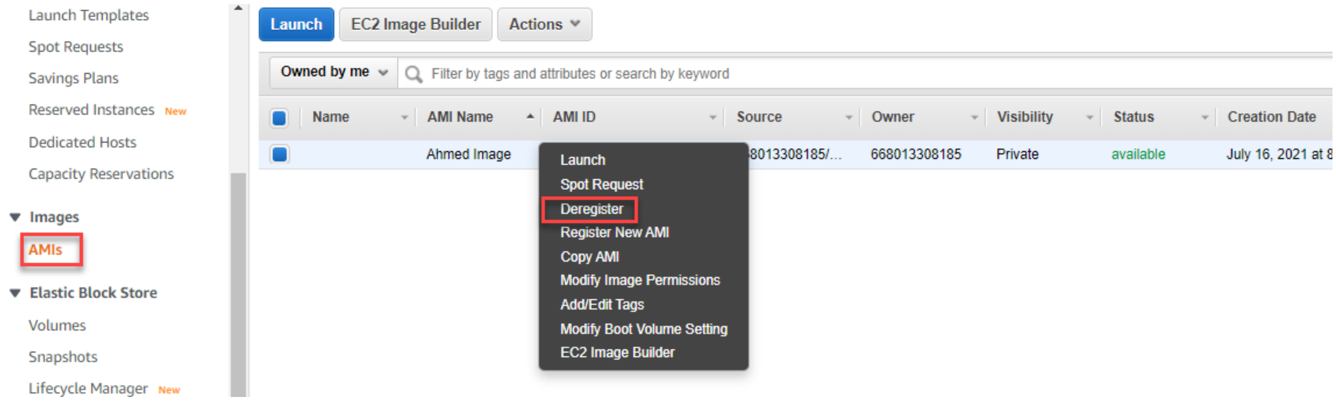
Destination region* Select destination region

Name Ahmed Image

Description [Copied ami-0cefa92393111976b from us-east-2] Ahmed Imag

Encryption □ Encrypt target EBS snapshots

Delete AMI

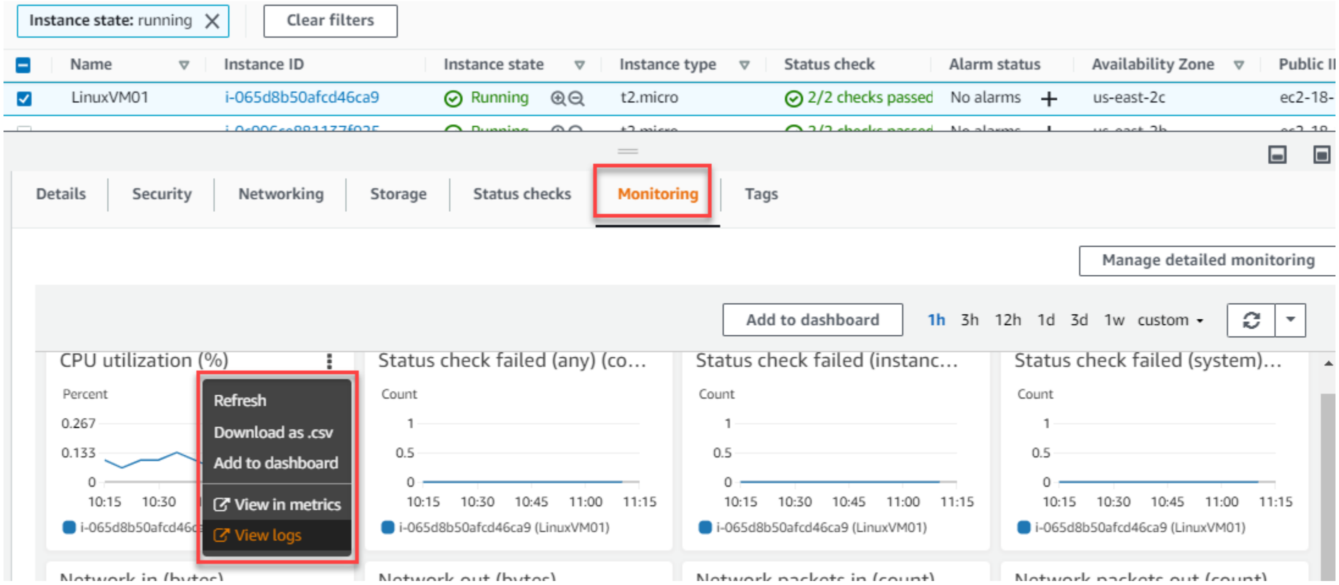


Name	AMI Name	AMI ID	Source	Owner	Visibility	Status	Creation Date
	Ahmed Image		8013308185/...	668013308185	Private	available	July 16, 2021 at 8

CloudWatch Metrics for EC2

Amazon CloudWatch provides monitoring for Amazon EC2 instances, allowing you to track performance and operational data in real-time.

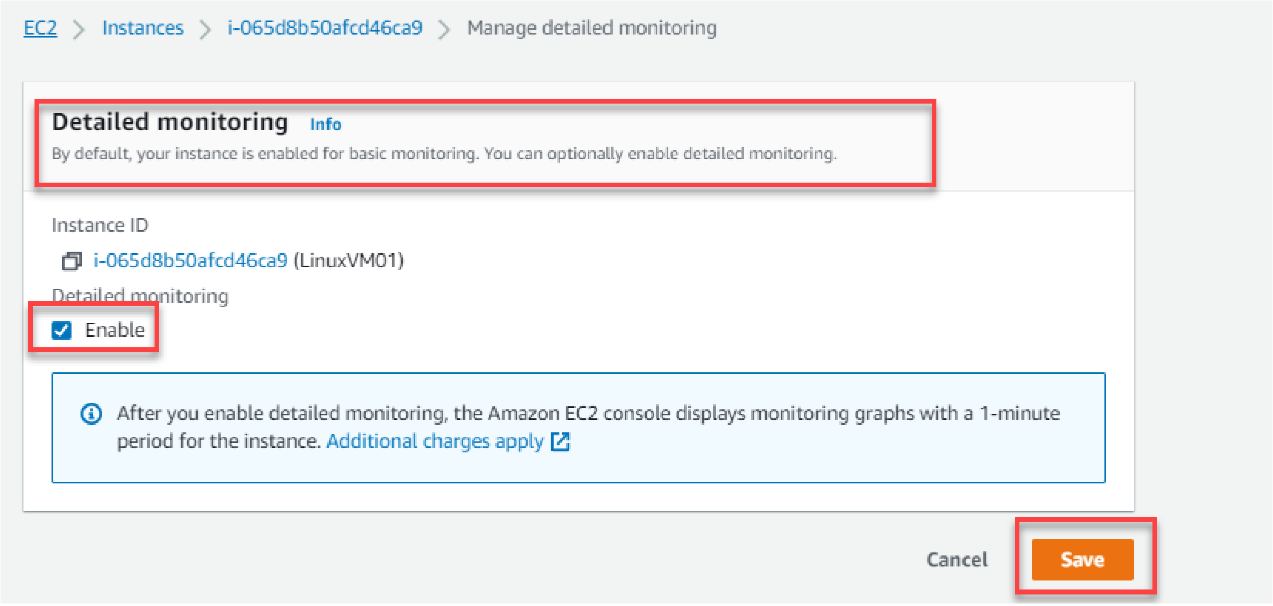
After choosing the instance, you can view all the associated metrics in the monitoring tab that update every 5 minutes.



Instance state: running

☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public II
☑	LinuxVM01	i-065d8b50afcd46ca9	Running	t2.micro	2/2 checks passed	No alarms	us-east-2c	ec2-18-

You can also activate more frequent monitoring that updates every minute for an additional fee.



EC2 > Instances > i-065d8b50afcd46ca9 > Manage detailed monitoring

Detailed monitoring Info

By default, your instance is enabled for basic monitoring. You can optionally enable detailed monitoring.

Instance ID

i-065d8b50afcd46ca9 (LinuxVM01)

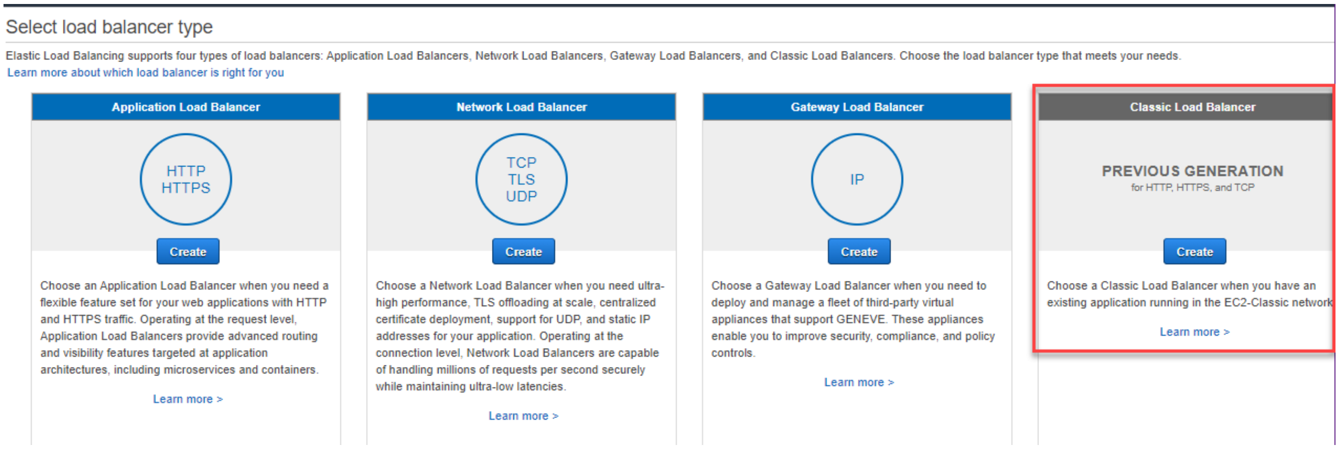
Detailed monitoring

☑ Enable

After you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period for the instance. Additional charges apply

Classic Load Balancer (CLB) with Hands On

Set up 3 EC2 instances allowing HTTP from the Security Group and enable SSM, then tag those instances. Next, create a Document to install Apache, execute the command to apply your newly created Document, and finally, test the HTTP connectivity.



Select load balancer type

Elastic Load Balancing supports four types of load balancers: Application Load Balancers, Network Load Balancers, Gateway Load Balancers, and Classic Load Balancers. Choose the load balancer type that meets your needs.

Learn more about which load balancer is right for you

Application Load Balancer

HTTP
HTTPS

Create

Choose an Application Load Balancer when you need a flexible feature set for your web applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers.

Learn more >

Network Load Balancer

TCP
TLS
UDP

Create

Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your application. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.

Learn more >

Gateway Load Balancer

IP

Create

Choose a Gateway Load Balancer when you need to deploy and manage a fleet of third-party virtual appliances that support GENEVE. These appliances enable you to improve security, compliance, and policy controls.

Learn more >

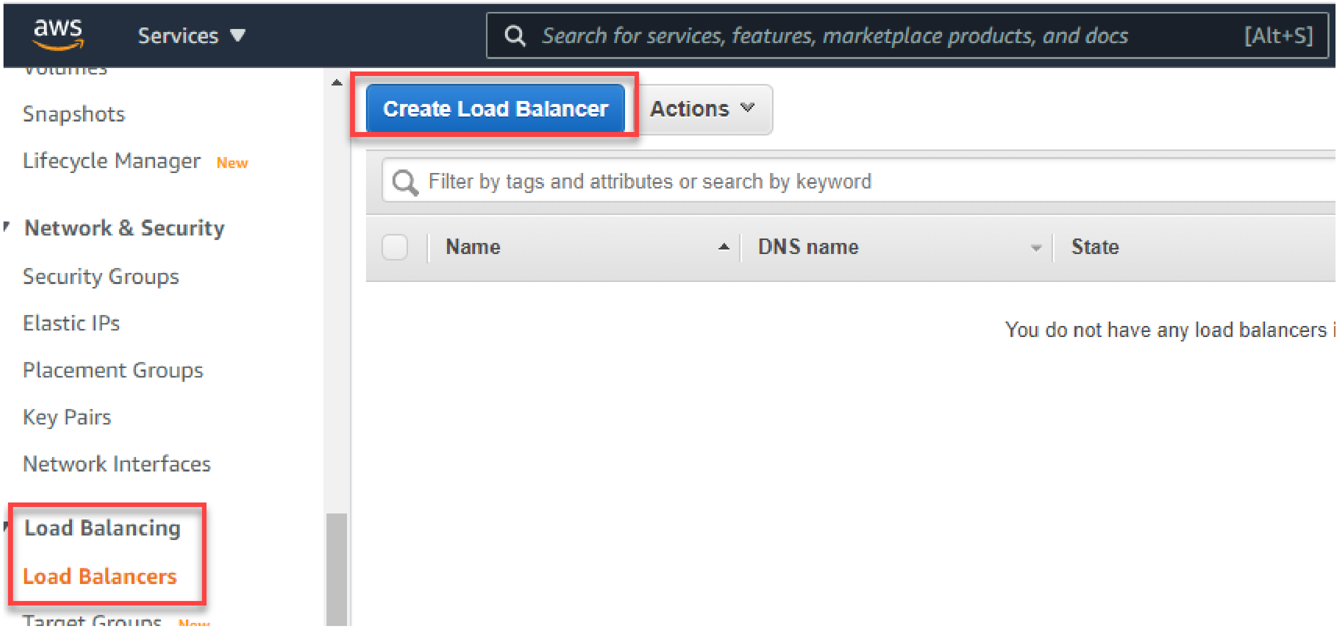
Classic Load Balancer

PREVIOUS GENERATION
for HTTP, HTTPS, and TCP

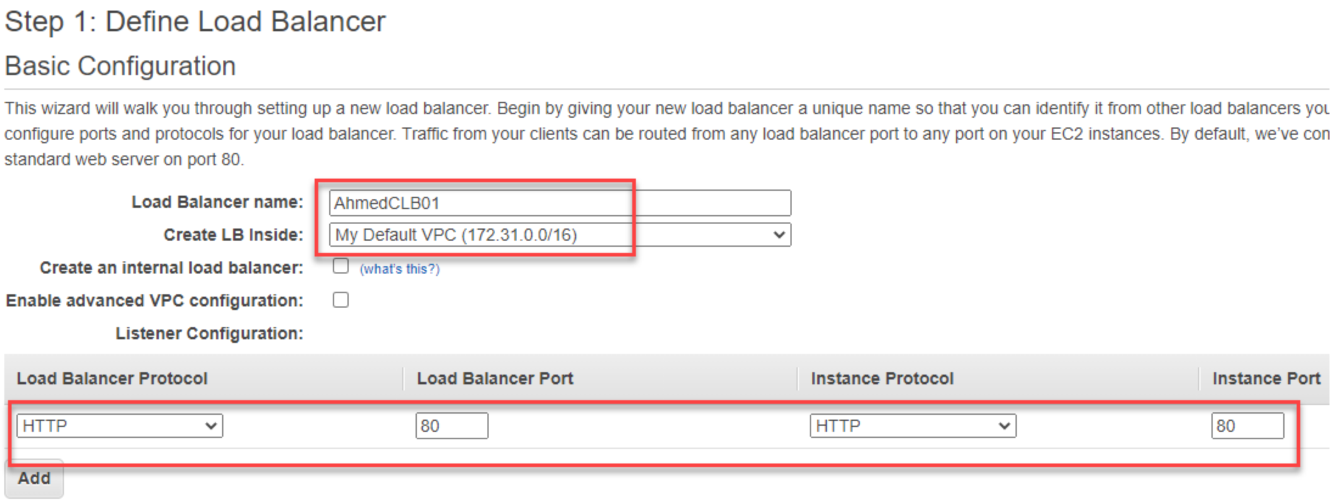
Create

Choose a Classic Load Balancer when you have an existing application running in the EC2-Classic network

Learn more >



You do not have any load balancers i



Step 1: Define Load Balancer

Basic Configuration

This wizard will walk you through setting up a new load balancer. Begin by giving your new load balancer a unique name so that you can identify it from other load balancers you configure ports and protocols for your load balancer. Traffic from your clients can be routed from any load balancer port to any port on your EC2 instances. By default, we've con standard web server on port 80.

Load Balancer name: AhmedCLB01

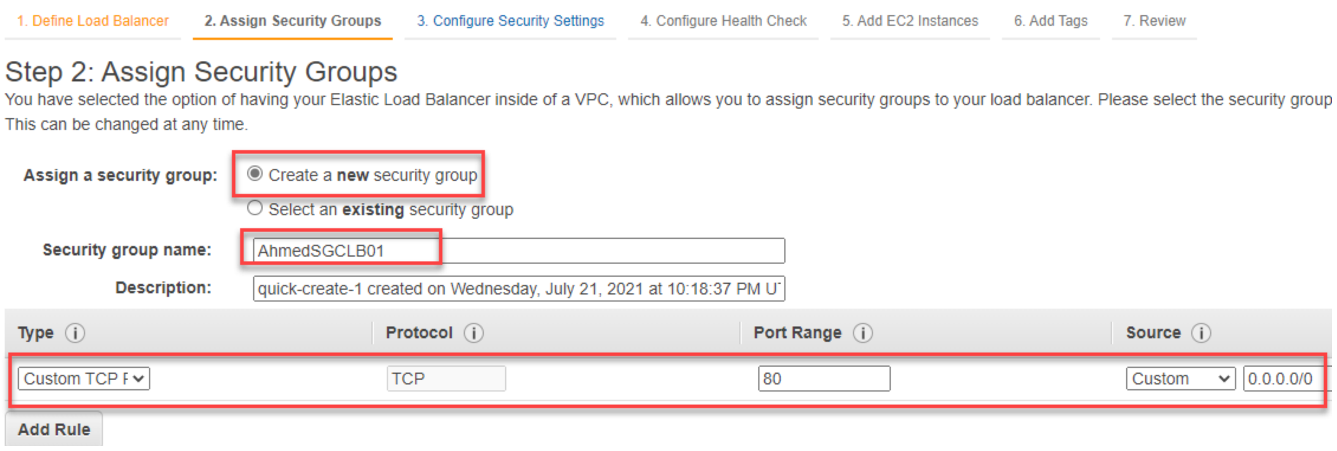
Create LB Inside: My Default VPC (172.31.0.0/16)

Create an internal load balancer: □ (what's this?)

Enable advanced VPC configuration: □

Listener Configuration:

Load Balancer Protocol	Load Balancer Port	Instance Protocol	Instance Port
HTTP	80	HTTP	80



1. Define Load Balancer
2. Assign Security Groups
3. Configure Security Settings
4. Configure Health Check
5. Add EC2 Instances
6. Add Tags
7. Review

Step 2: Assign Security Groups

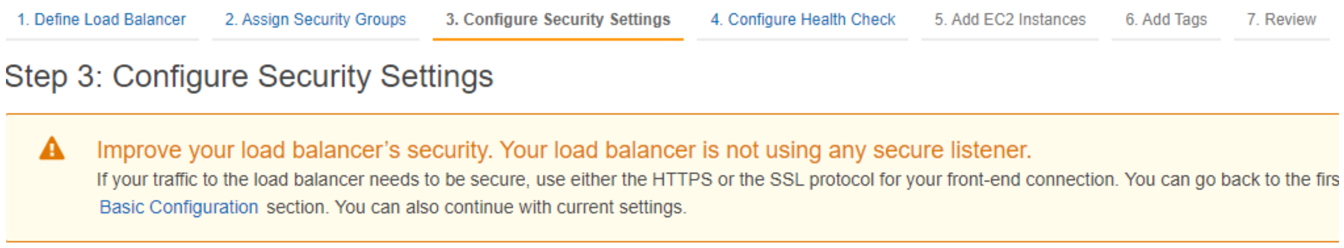
You have selected the option of having your Elastic Load Balancer inside of a VPC, which allows you to assign security groups to your load balancer. Please select the security group This can be changed at any time.

Assign a security group: ● Create a **new** security group
○ Select an **existing** security group

Security group name: AhmedSGCLB01

Description: quick-create-1 created on Wednesday, July 21, 2021 at 10:18:37 PM U

Type	Protocol	Port Range	Source
Custom TCP F	TCP	80	Custom 0.0.0.0/0

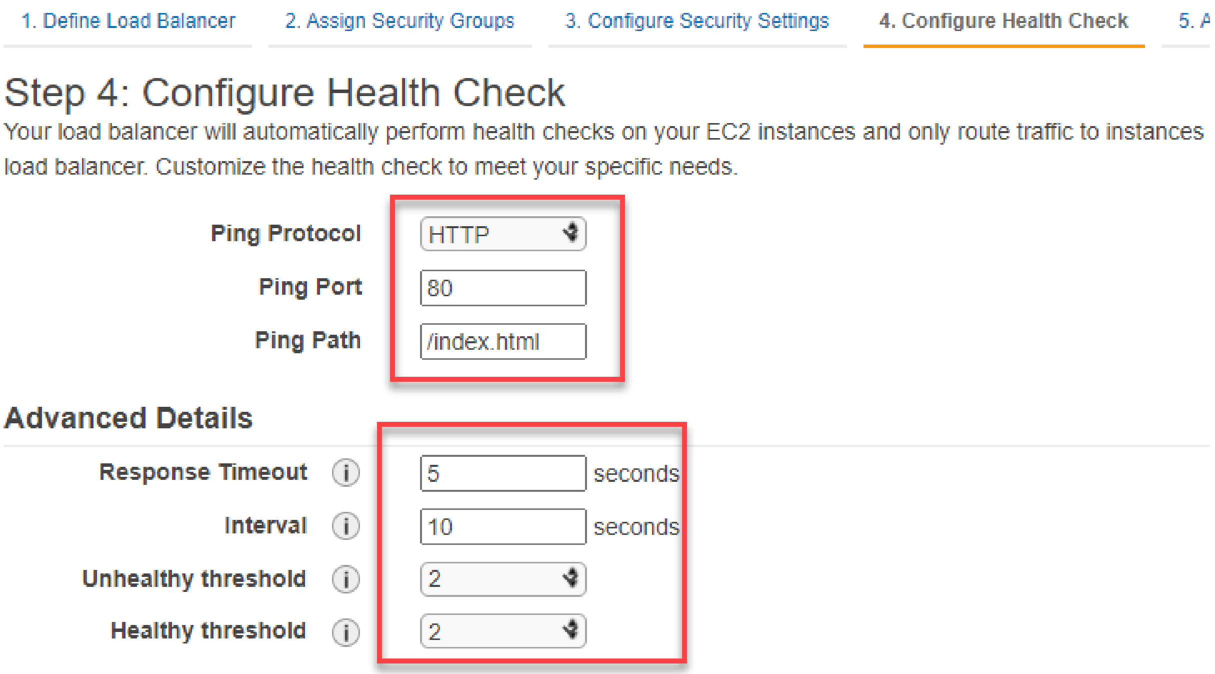


1. Define Load Balancer
2. Assign Security Groups
3. Configure Security Settings
4. Configure Health Check
5. Add EC2 Instances
6. Add Tags
7. Review

Step 3: Configure Security Settings

Improve your load balancer's security. Your load balancer is not using any secure listener.

If your traffic to the load balancer needs to be secure, use either the HTTPS or the SSL protocol for your front-end connection. You can go back to the firs Basic Configuration section. You can also continue with current settings.



1. Define Load Balancer | 2. Assign Security Groups | 3. Configure Security Settings | **4. Configure Health Check** | 5. A

Step 4: Configure Health Check

Your load balancer will automatically perform health checks on your EC2 instances and only route traffic to instances load balancer. Customize the health check to meet your specific needs.

Ping Protocol HTTP

Ping Port 80

Ping Path /index.html

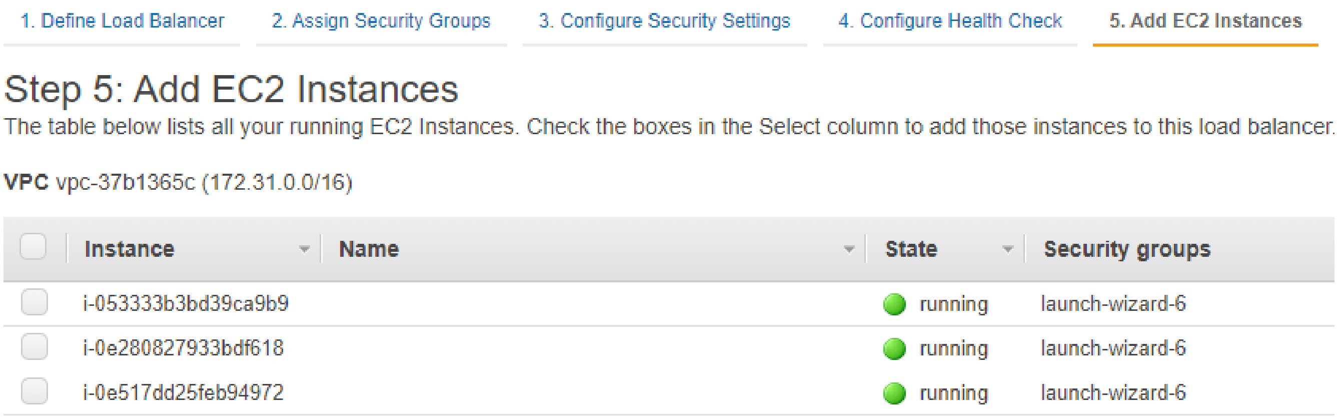
Advanced Details

Response Timeout 5 seconds

Interval 10 seconds

Unhealthy threshold 2

Healthy threshold 2



1. Define Load Balancer | 2. Assign Security Groups | 3. Configure Security Settings | 4. Configure Health Check | **5. Add EC2 Instances**

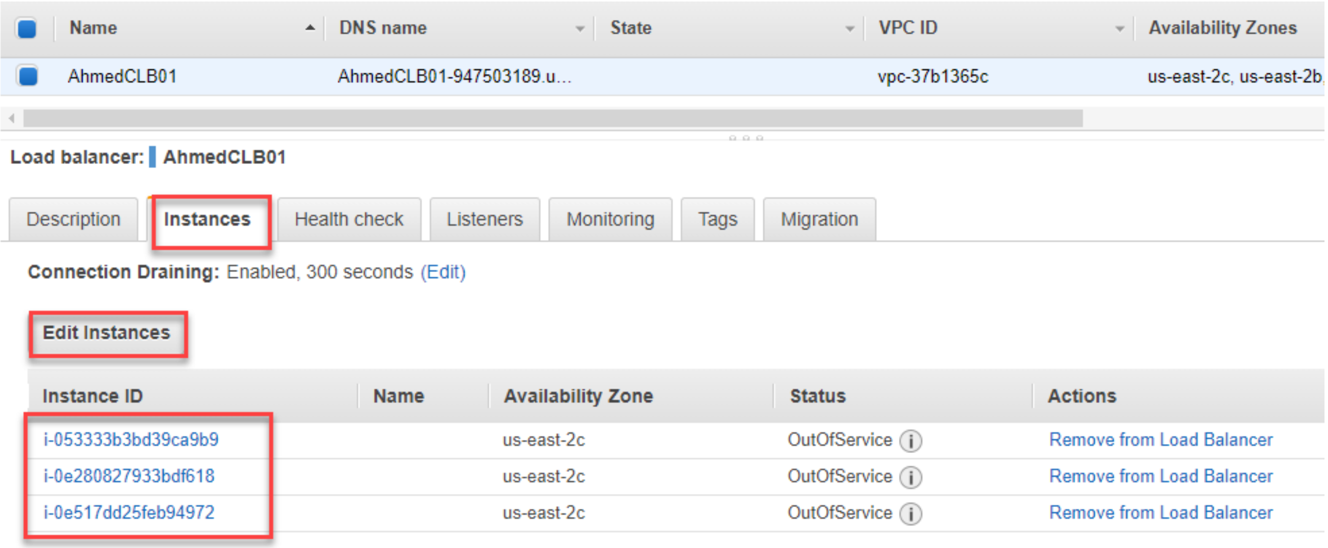
Step 5: Add EC2 Instances

The table below lists all your running EC2 Instances. Check the boxes in the Select column to add those instances to this load balancer.

VPC vpc-37b1365c (172.31.0.0/16)

□	Instance	Name	State	Security groups
□	i-053333b3bd39ca9b9		● running	launch-wizard-6
□	i-0e280827933bdf618		● running	launch-wizard-6
□	i-0e517dd25feb94972		● running	launch-wizard-6

Instances that contain HTTP service are included.

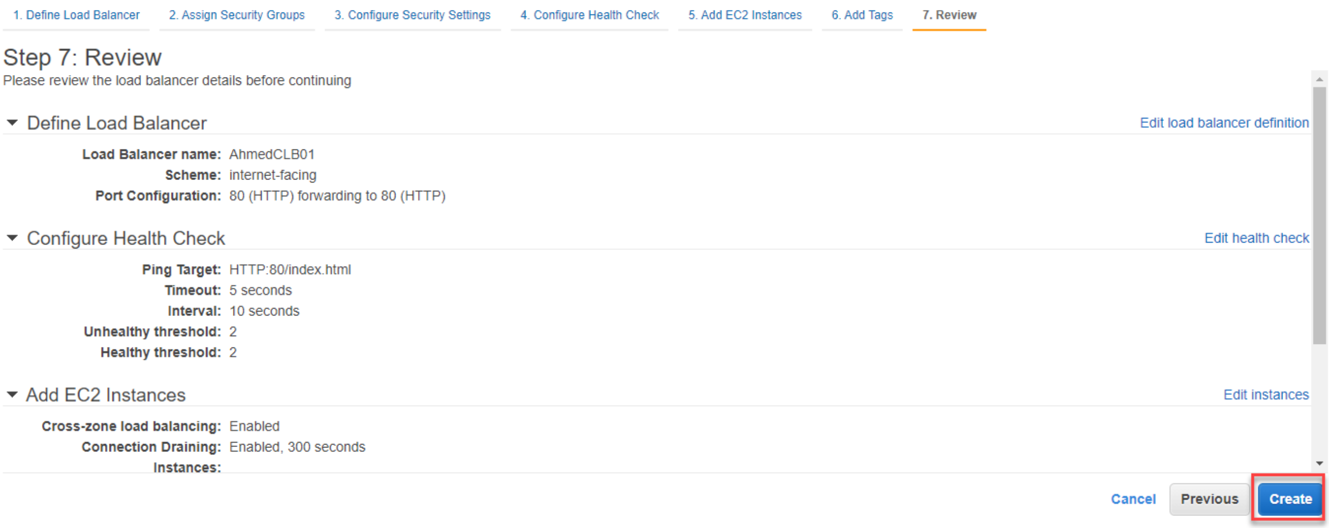


Name	DNS name	State	VPC ID	Availability Zones
AhmedCLB01	AhmedCLB01-947503189.u...		vpc-37b1365c	us-east-2c, us-east-2b,

Load balancer: AhmedCLB01

Connection Draining: Enabled, 300 seconds (Edit)

Instance ID	Name	Availability Zone	Status	Actions
i-053333b3bd39ca9b9		us-east-2c	OutOfService	Remove from Load Balancer
i-0e280827933bdf618		us-east-2c	OutOfService	Remove from Load Balancer
i-0e517dd25feb94972		us-east-2c	OutOfService	Remove from Load Balancer



1. Define Load Balancer
2. Assign Security Groups
3. Configure Security Settings
4. Configure Health Check
5. Add EC2 Instances
6. Add Tags
7. Review

Step 7: Review

Please review the load balancer details before continuing

Define Load Balancer

Edit load balancer definition

Load Balancer name: AhmedCLB01
Scheme: internet-facing
Port Configuration: 80 (HTTP) forwarding to 80 (HTTP)

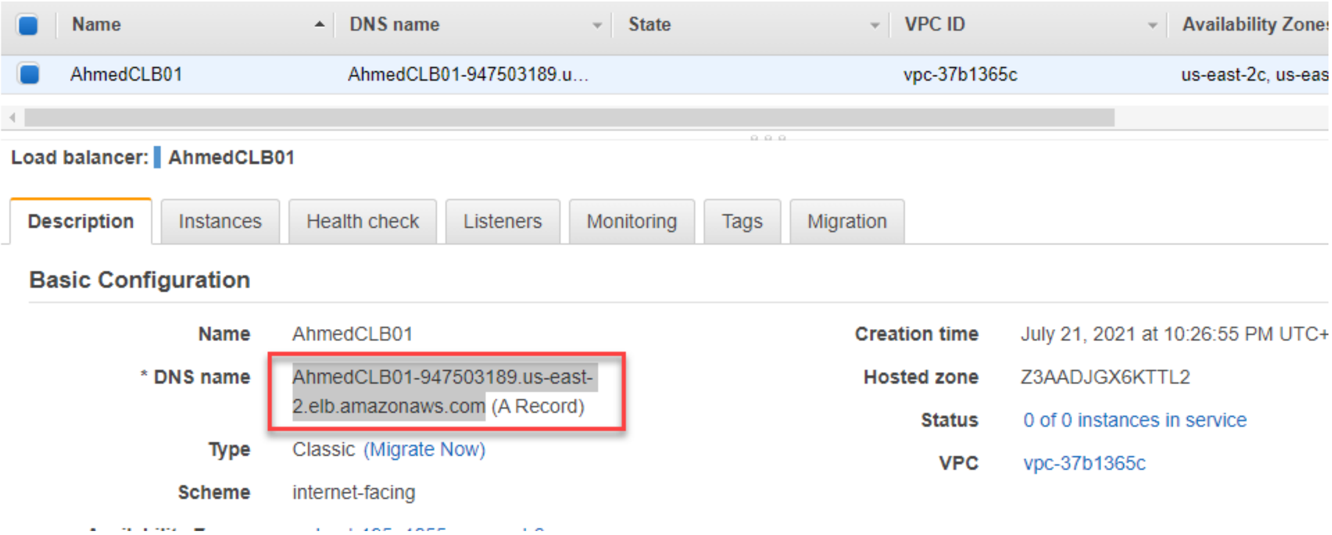
Configure Health Check

Ping Target: HTTP:80/index.html
Timeout: 5 seconds
Interval: 10 seconds
Unhealthy threshold: 2
Healthy threshold: 2

Add EC2 Instances

Cross-zone load balancing: Enabled
Connection Draining: Enabled, 300 seconds
Instances:

Copy the DNS address to connect to the CLB.



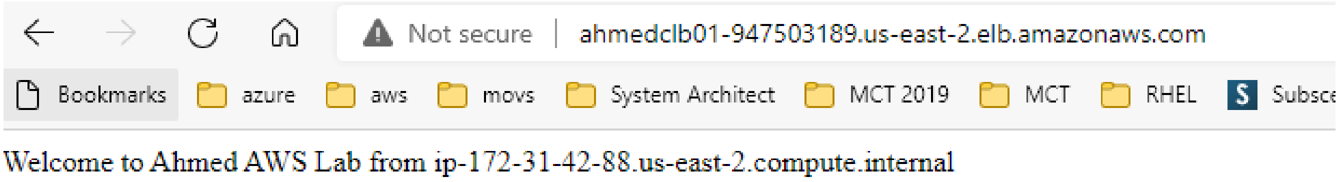
Name	DNS name	State	VPC ID	Availability Zone
AhmedCLB01	AhmedCLB01-947503189.u...		vpc-37b1365c	us-east-2c, us-eas

Load balancer: AhmedCLB01

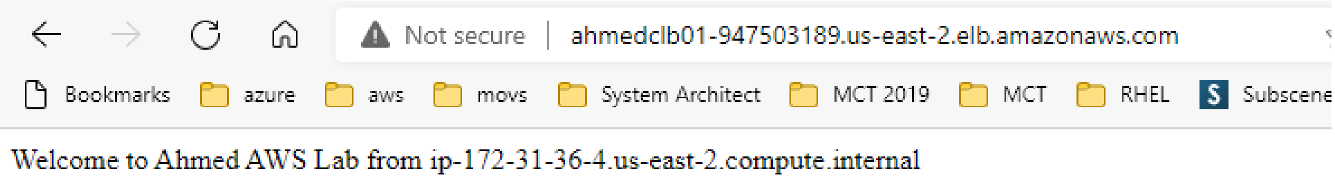
Basic Configuration

Name: AhmedCLB01
* DNS name: AhmedCLB01-947503189.us-east-2.elb.amazonaws.com (A Record)
Type: Classic (Migrate Now)
Scheme: internet-facing
Creation time: July 21, 2021 at 10:26:55 PM UTC+
Hosted zone: Z3AADJGX6KTTL2
Status: 0 of 0 instances in service
VPC: vpc-37b1365c

Refreshing the page will result in a server address change, indicating that the load balancer is functioning.

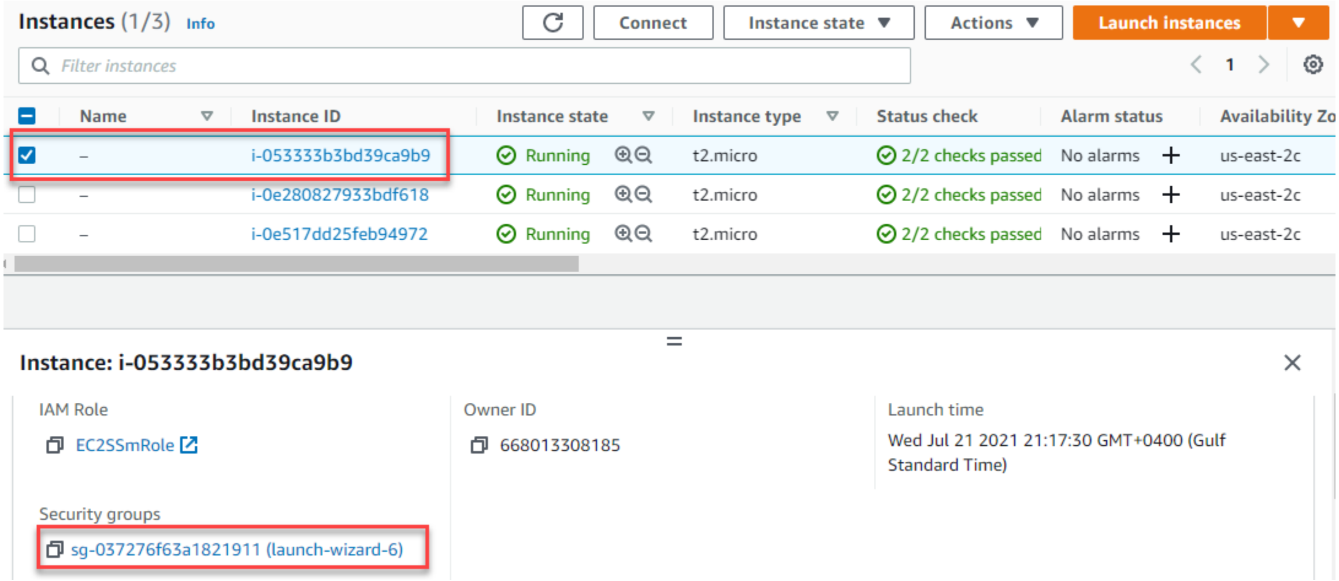


Welcome to Ahmed AWS Lab from ip-172-31-42-88.us-east-2.compute.internal



Welcome to Ahmed AWS Lab from ip-172-31-36-4.us-east-2.compute.internal

Additionally, you have the option to block direct traffic to the instances and instead permit access solely through the load balancer by appropriately configuring your security group. To choose the correct security group, follow the subsequent step.



☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zo
☑	–	i-053333b3bd39ca9b9	Running	t2.micro	2/2 checks passed	No alarms	us-east-2c
☐	–	i-0e280827933bdf618	Running	t2.micro	2/2 checks passed	No alarms	us-east-2c
☐	–	i-0e517dd25feb94972	Running	t2.micro	2/2 checks passed	No alarms	us-east-2c

Instance: i-053333b3bd39ca9b9

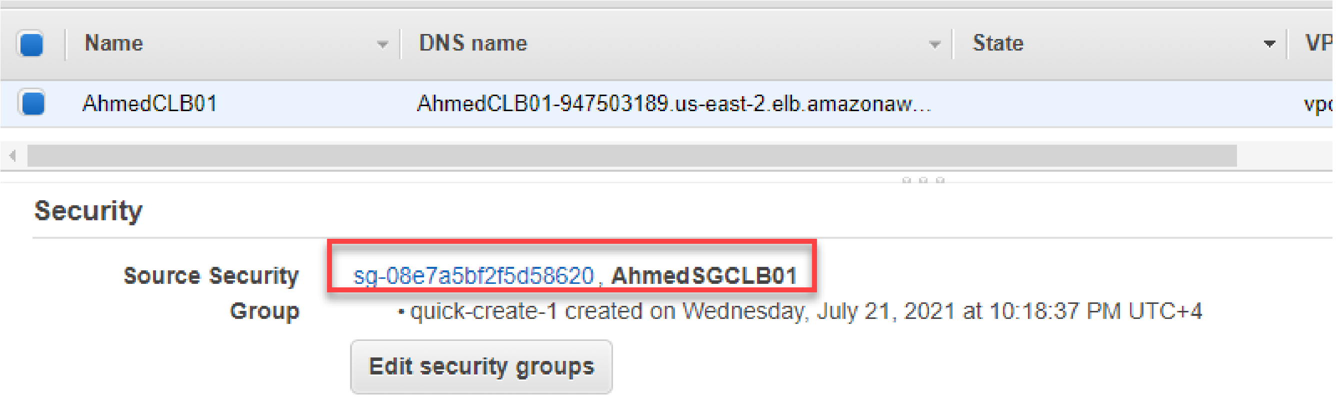
IAM Role: EC2SSmRole

Owner ID: 668013308185

Launch time: Wed Jul 21 2021 21:17:30 GMT+0400 (Gulf Standard Time)

Security groups: sg-037276f63a1821911 (launch-wizard-6)

I'll permit traffic exclusively through the specified security group associated with the load balancer.

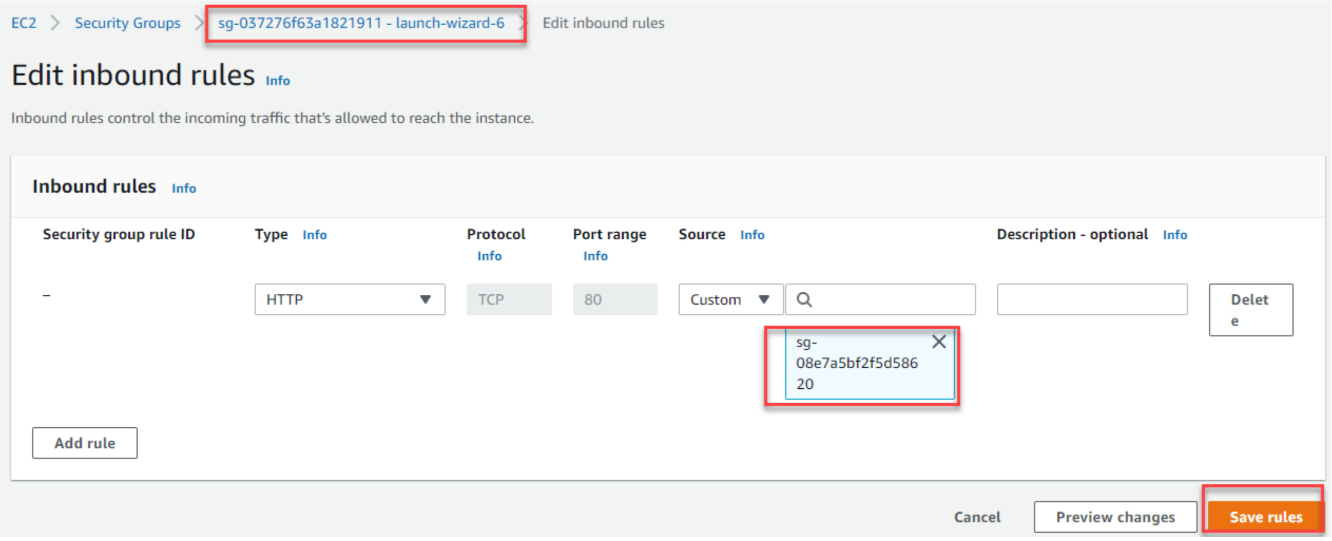


☐	Name	DNS name	State	VP
☐	AhmedCLB01	AhmedCLB01-947503189.us-east-2.elb.amazonaw...		vpc

Security

Source Security Group: sg-08e7a5bf2f5d58620 , AhmedSGCLB01
• quick-create-1 created on Wednesday, July 21, 2021 at 10:18:37 PM UTC+4

Now update the security groups for all instances under the load balancer to permit traffic exclusively through the LB.



EC2 > Security Groups > sg-037276f63a1821911 - launch-wizard-6 > Edit inbound rules

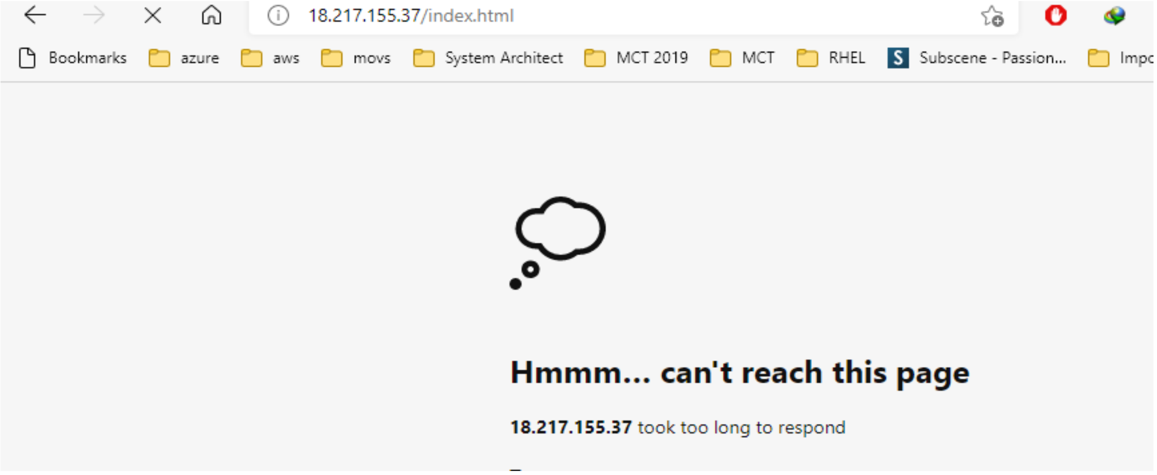
Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type	Protocol	Port range	Source		Description - optional
–	HTTP	TCP	80	Custom	sg-08e7a5bf2f5d58620	

Public IP addresses no longer grant direct access to servers.

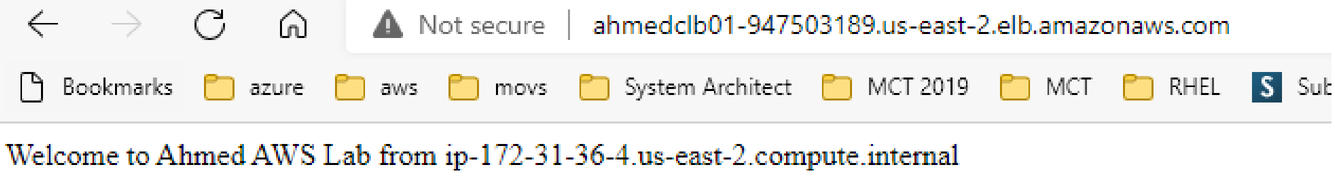


18.217.155.37/index.html

Hmmm... can't reach this page

18.217.155.37 took too long to respond

Access is still available via LB



Not secure | ahmedclb01-947503189.us-east-2.elb.amazonaws.com

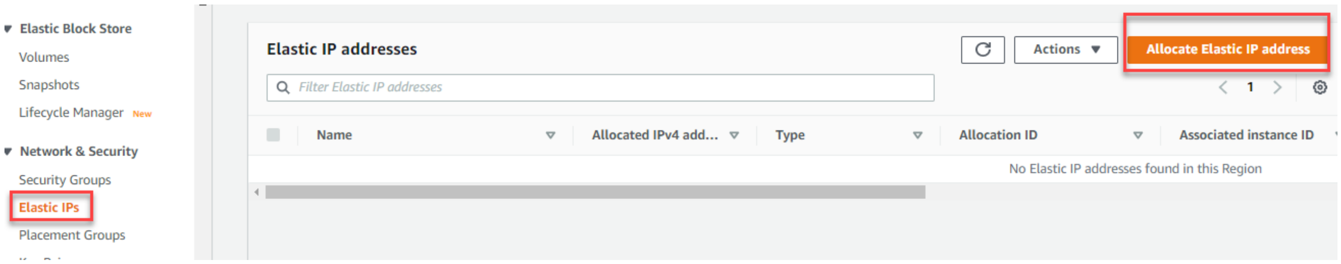
Welcome to Ahmed AWS Lab from ip-172-31-36-4.us-east-2.compute.internal

Elastic IP addresses

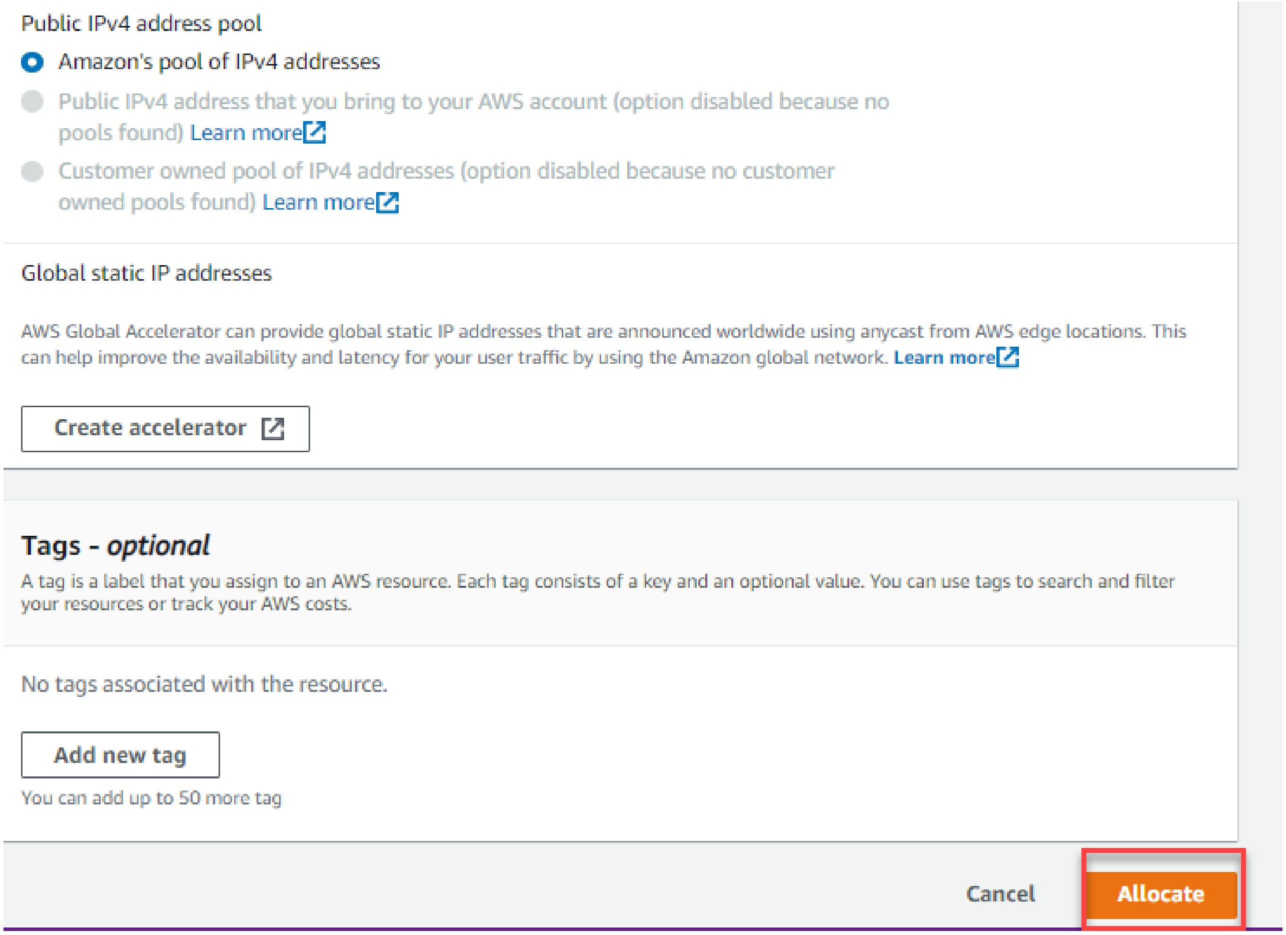
An Elastic IP address is a static IPv4 address designed for dynamic cloud computing. It is allocated to your AWS account and remains yours until you release it.

Key Points:

1. **Reassociation:**
   - You can reassign your Elastic IP address to any instance within your account, allowing you to quickly recover or move your applications.
2. **Failover:**
   - Elastic IP addresses can be used to mask the failure of an instance or software by quickly remapping the address to another instance in your account.
3. **Costs:**
   - Elastic IP addresses are free of charge as long as they are associated with a running instance. AWS charges you for idle Elastic IP addresses that are not associated with a running instance to encourage efficient use.
4. **Scalability:**
   - You can scale your applications by associating Elastic IP addresses with instances that need to handle additional traffic.
5. **Elastic Load Balancer Integration:**
   - Elastic IP addresses can be associated with Elastic Load Balancers to distribute incoming traffic across multiple instances, enhancing availability and fault tolerance.
6. **Public IP Replacement:**
   - An Elastic IP address is a great replacement for a public IP address, giving you more control over your IP addresses and improving the reliability of your applications.



No Elastic IP addresses found in this Region


Public IPv4 address pool

● Amazon's pool of IPv4 addresses

○ Public IPv4 address that you bring to your AWS account (option disabled because no pools found) Learn more

○ Customer owned pool of IPv4 addresses (option disabled because no customer owned pools found) Learn more

Global static IP addresses

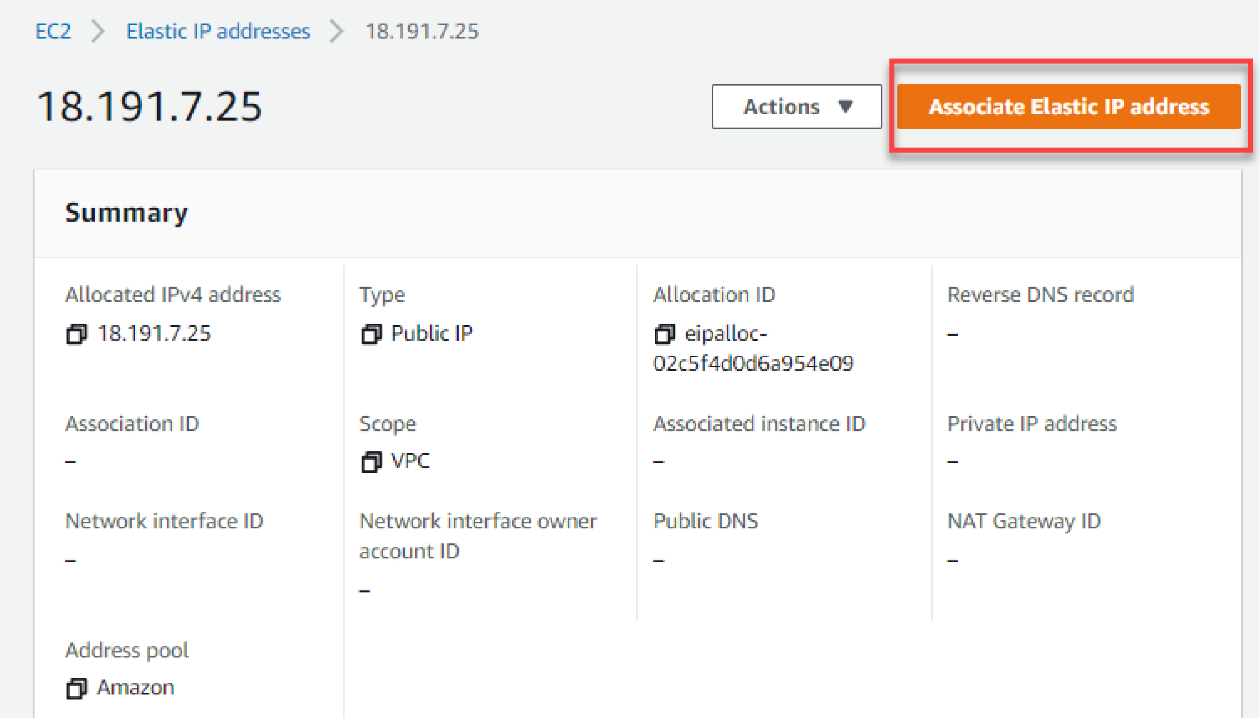
AWS Global Accelerator can provide global static IP addresses that are announced worldwide using anycast from AWS edge locations. This can help improve the availability and latency for your user traffic by using the Amazon global network. Learn more

Tags - *optional*

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

No tags associated with the resource.

You can add up to 50 more tag


EC2 > Elastic IP addresses > 18.191.7.25
Actions ▼
Associate Elastic IP address

18.191.7.25

Summary

Allocated IPv4 address
18.191.7.25

Type
Public IP

Allocation ID
eipalloc-02c5f4d0d6a954e09

Reverse DNS record
–

Association ID
–

Scope
VPC

Associated instance ID
–

Private IP address
–

Network interface ID
–

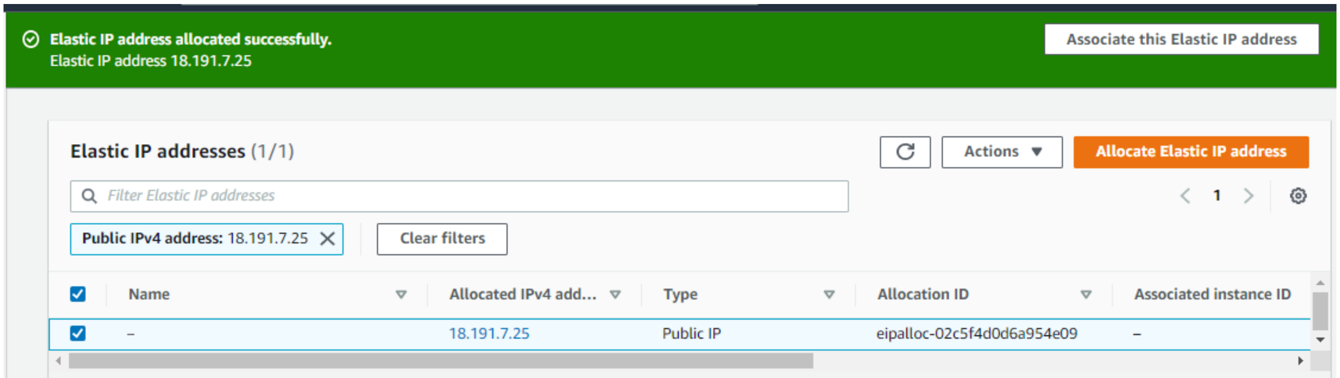
Network interface owner account ID
–

Public DNS
–

NAT Gateway ID
–

Address pool
Amazon

Select the instance to allocate this IP to.

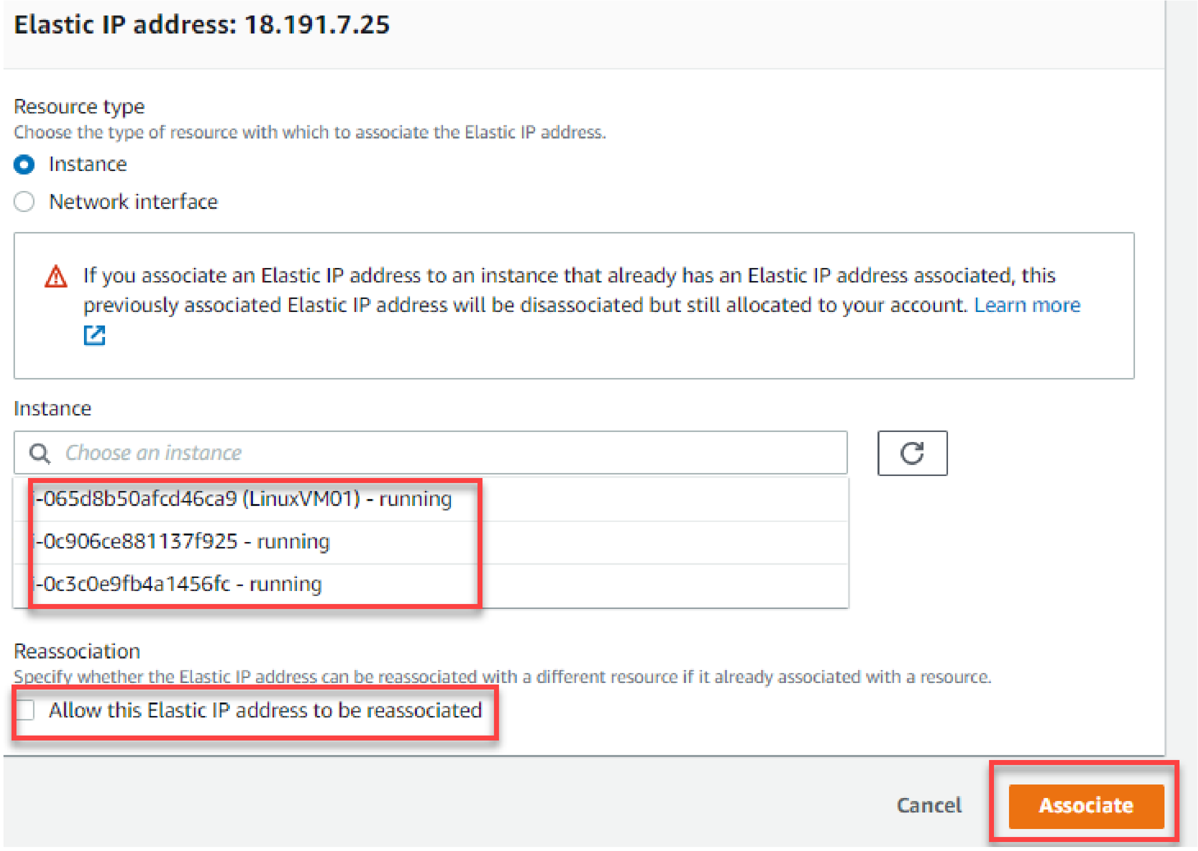

Associate this Elastic IP address
Actions ▼
Allocate Elastic IP address
Filter Elastic IP addresses
Clear filters
1

Elastic IP address allocated successfully.
Elastic IP address 18.191.7.25

Elastic IP addresses (1/1)

Public IPv4 address: 18.191.7.25

☑	Name	Allocated IPv4 add...	Type	Allocation ID	Associated instance ID
☑	–	18.191.7.25	Public IP	eipalloc-02c5f4d0d6a954e09	–



Elastic IP address: 18.191.7.25

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

● Instance
○ Network interface

⚠ If you associate an Elastic IP address to an instance that already has an Elastic IP address associated, this previously associated Elastic IP address will be disassociated but still allocated to your account. Learn more

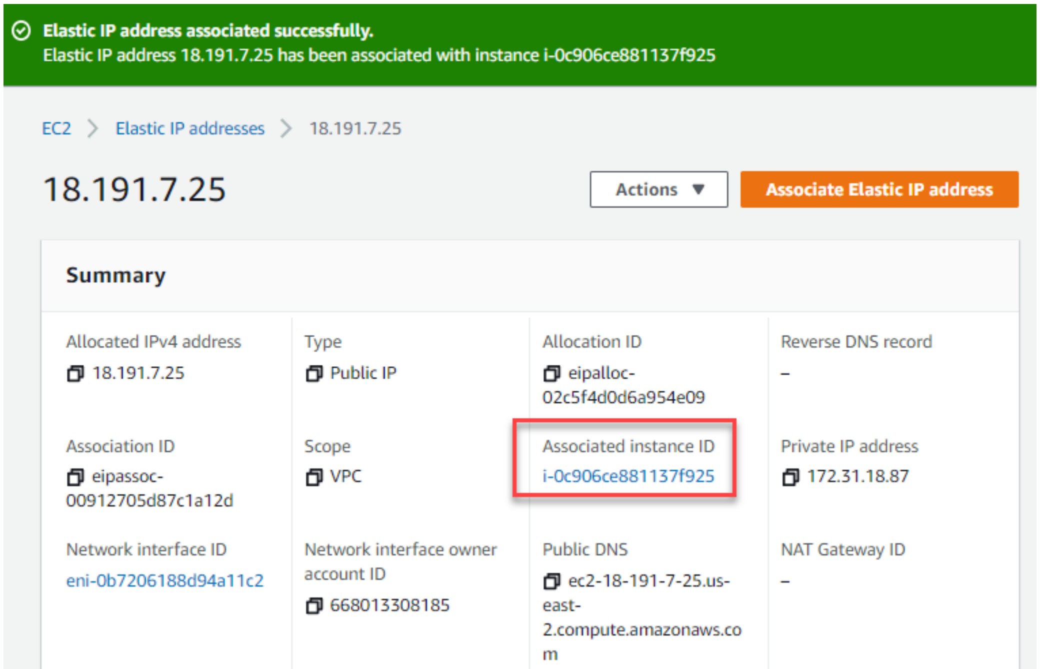
Instance

Choose an instance

-065d8b50afcd46ca9 (LinuxVM01) - running
i-0c906ce881137f925 - running
i-0c3c0e9fb4a1456fc - running

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

□ Allow this Elastic IP address to be reassociated



Elastic IP address associated successfully.
Elastic IP address 18.191.7.25 has been associated with instance i-0c906ce881137f925

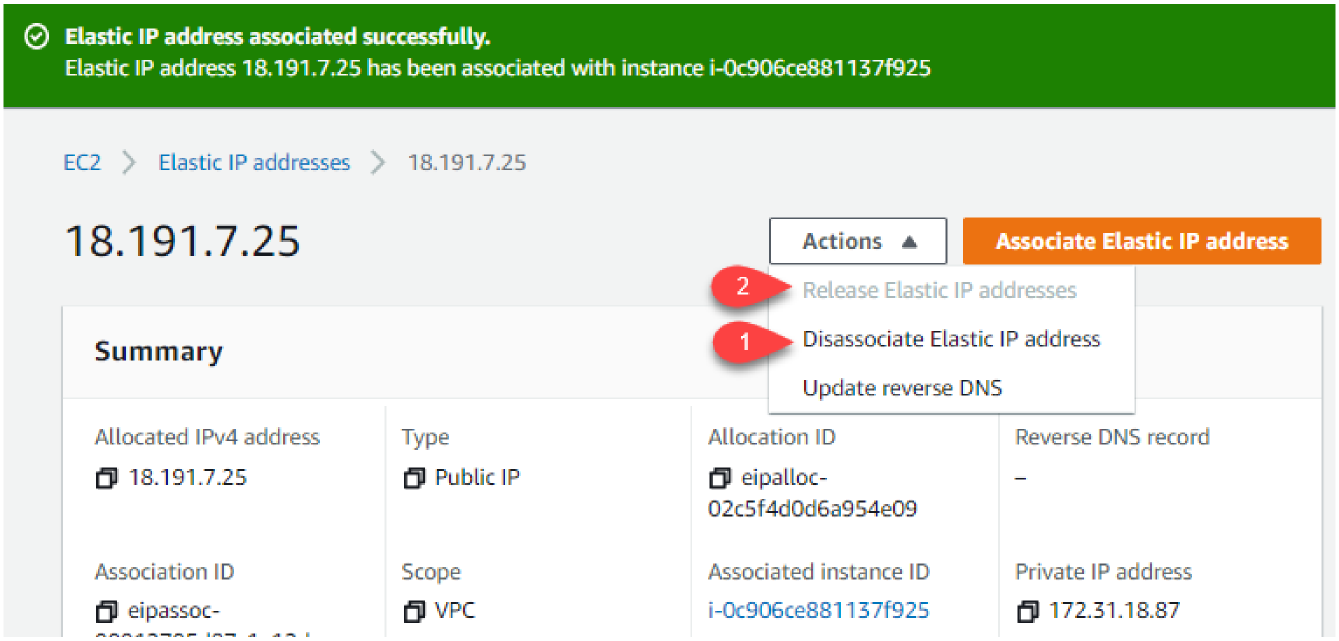
EC2 > Elastic IP addresses > 18.191.7.25

18.191.7.25

Summary

Allocated IPv4 address 18.191.7.25	Type Public IP	Allocation ID eipalloc-02c5f4d0d6a954e09	Reverse DNS record –
Association ID eipassoc-00912705d87c1a12d	Scope VPC	Associated instance ID i-0c906ce881137f925	Private IP address 172.31.18.87
Network interface ID eni-0b7206188d94a11c2	Network interface owner account ID 668013308185	Public DNS ec2-18-191-7-25.us-east-2.compute.amazonaws.com	NAT Gateway ID –

You can detach from the instance to free up that address.



Elastic IP address associated successfully.
Elastic IP address 18.191.7.25 has been associated with instance i-0c906ce881137f925

EC2 > Elastic IP addresses > 18.191.7.25

18.191.7.25

Summary

Allocated IPv4 address: 18.191.7.25

Type: Public IP

Allocation ID: eipalloc-02c5f4d0d6a954e09

Reverse DNS record: –

Association ID: eipassoc-

Scope: VPC

Associated instance ID: i-0c906ce881137f925

Private IP address: 172.31.18.87

Actions ▲
Associate Elastic IP address
2
Release Elastic IP addresses
1
Disassociate Elastic IP address
Update reverse DNS

Virtual Private Cloud (VPC)

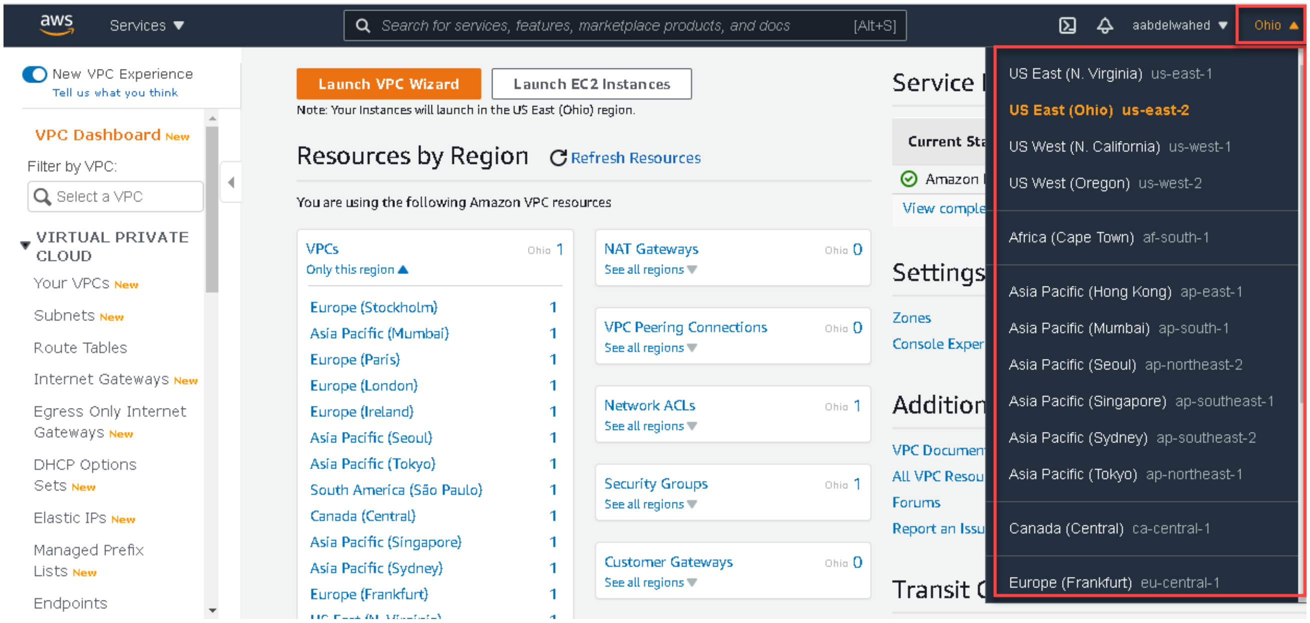
A Virtual Private Cloud (VPC) is a logically isolated section of the AWS cloud where you can launch AWS resources in a virtual network that you define. It gives you full control over your virtual networking environment, including selection of your IP address range, creation of subnets, and configuration of route tables and network gateways.

Key Features:

1. **Isolation:**
   - Each VPC is logically isolated from other VPCs in the AWS cloud, ensuring a secure environment for your resources.
2. **Subnets:** Divide your VPC into subnets, which can be designated as public, private, or VPN-only.
3. **Route Tables:** Configure route tables to control the routing of traffic within your VPC.
4. **Internet Gateway:** Attach an internet gateway to enable communication between your VPC and the internet.
5. **NAT Gateway:** Use a NAT gateway to allow instances in a private subnet to connect to the internet or other AWS services, while preventing the internet from initiating connections with those instances.
6. **Security Groups:** Act as a virtual firewall for your instances to control inbound and outbound traffic.
7. **Network ACLs:** Provide an additional layer of security by controlling traffic to and from subnets.
8. **Peering Connections:** Establish peering connections between your VPCs to enable traffic routing between them using private IP addresses.
9. **VPN Connection:** Set up a VPN connection between your VPC and your own data center for a secure and encrypted connection.
10. **Elastic IP Addresses:** Allocate Elastic IP addresses for instances in your VPC to maintain a static IP address.
11. **VPC Flow Logs:** Capture and monitor the traffic that flows in and out of your network interfaces within your VPC.
12. **Enhanced Network Performance:** Benefit from advanced network features such as high throughput, low latency, and consistent performance for your applications.

Benefits:

1. **Security:**
   - Enhanced security features, such as security groups and network ACLs, provide robust protection for your resources.
2. **Customization:**
   - Full control over IP address ranges, subnets, and network configurations allows for highly customized network setups.
3. **Scalability:**
   - Easily scale your network infrastructure and resources as your business needs grow.
4. **Cost-Effectiveness:**
   - Efficiently manage your resources and optimize costs by choosing the right VPC configuration for your applications.

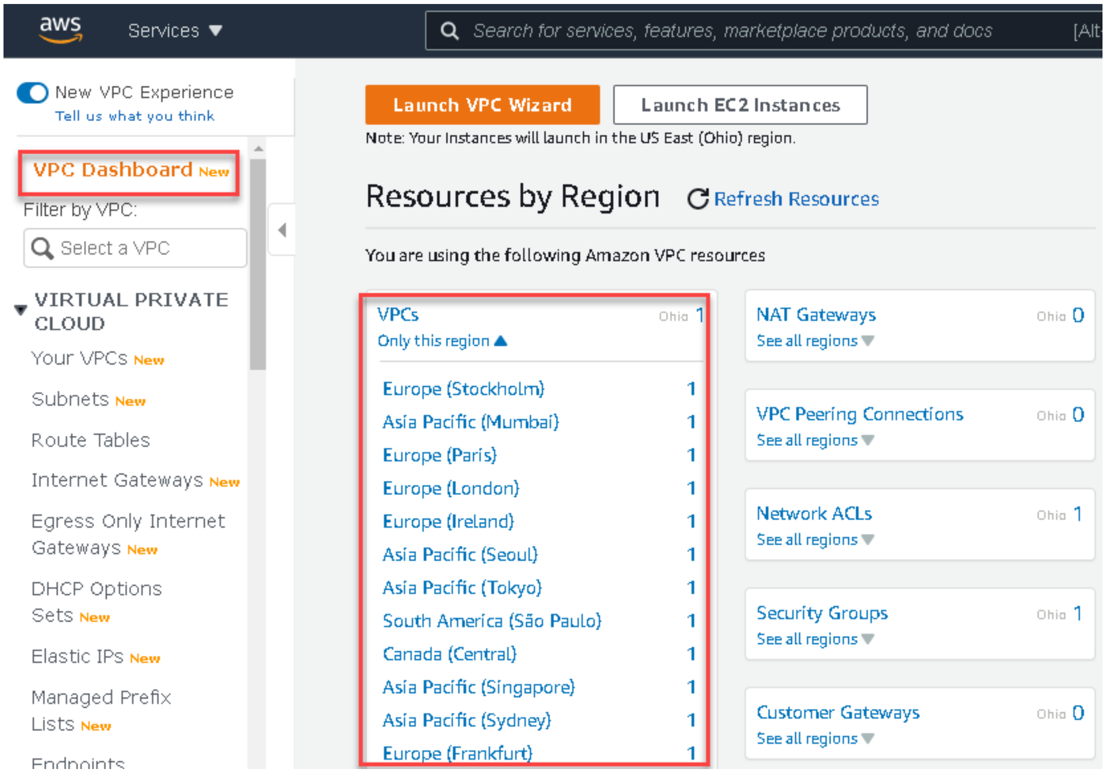

aws
Services ▼
Search for services, features, marketplace products, and docs [Alt+S]
aabdelwahed ▼
Ohio ▲
New VPC Experience
Tell us what you think
VPC Dashboard New
Filter by VPC:
Select a VPC
VIRTUAL PRIVATE CLOUD
Your VPCs New
Subnets New
Route Tables
Internet Gateways New
Egress Only Internet Gateways New
DHCP Options Sets New
Elastic IPs New
Managed Prefix Lists New
Endpoints
Launch VPC Wizard
Launch EC2 Instances
Resources by Region
Refresh Resources
NAT Gateways Ohio 0 See all regions
VPC Peering Connections Ohio 0 See all regions
Network ACLs Ohio 1 See all regions
Security Groups Ohio 1 See all regions
Customer Gateways Ohio 0 See all regions
Service
Current Sta
Amazon
View comple
Settings
Zones
Console Exper
Addition
VPC Documen
All VPC Resou
Forums
Report an Issu
Transit
US East (N. Virginia) us-east-1
US East (Ohio) us-east-2
US West (N. California) us-west-1
US West (Oregon) us-west-2
Africa (Cape Town) af-south-1
Asia Pacific (Hong Kong) ap-east-1
Asia Pacific (Mumbai) ap-south-1
Asia Pacific (Seoul) ap-northeast-2
Asia Pacific (Singapore) ap-southeast-1
Asia Pacific (Sydney) ap-southeast-2
Asia Pacific (Tokyo) ap-northeast-1
Canada (Central) ca-central-1
Europe (Frankfurt) eu-central-1

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

You are using the following Amazon VPC resources

VPCs Only this region ▲	Ohio 1
Europe (Stockholm)	1
Asia Pacific (Mumbai)	1
Europe (Paris)	1
Europe (London)	1
Europe (Ireland)	1
Asia Pacific (Seoul)	1
Asia Pacific (Tokyo)	1
South America (São Paulo)	1
Canada (Central)	1
Asia Pacific (Singapore)	1
Asia Pacific (Sydney)	1
Europe (Frankfurt)	1

Switching to a different region

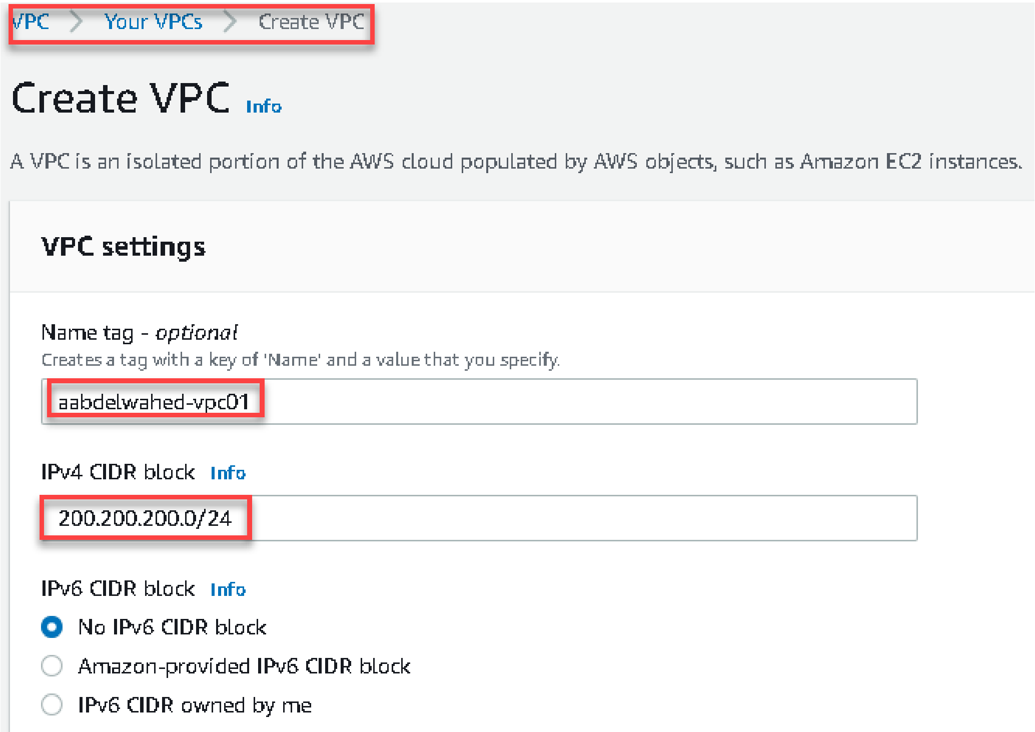


Note: Your Instances will launch in the US East (Ohio) region.

You are using the following Amazon VPC resources

VPCs Only this region ▲	Ohio 1
Europe (Stockholm)	1
Asia Pacific (Mumbai)	1
Europe (Paris)	1
Europe (London)	1
Europe (Ireland)	1
Asia Pacific (Seoul)	1
Asia Pacific (Tokyo)	1
South America (São Paulo)	1
Canada (Central)	1
Asia Pacific (Singapore)	1
Asia Pacific (Sydney)	1
Europe (Frankfurt)	1

Establish a New Virtual Private Cloud



VPC > Your VPCs > Create VPC

Create VPC Info

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

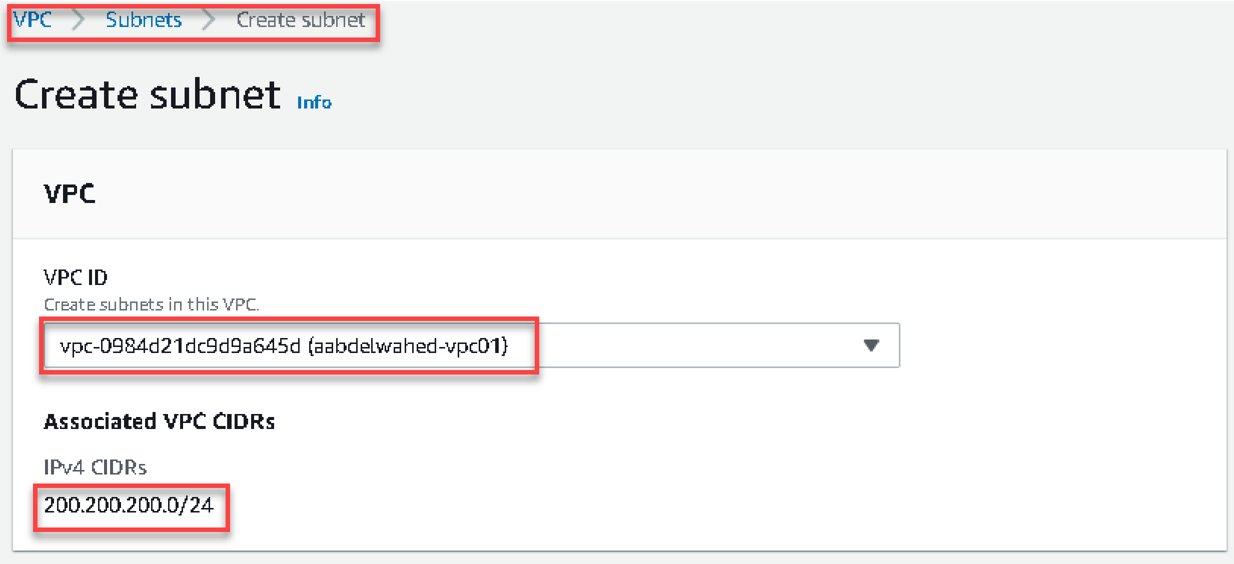
VPC settings

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.
aabdelwahed-vpc01

IPv4 CIDR block Info
200.200.200.0/24

IPv6 CIDR block Info
● No IPv6 CIDR block
○ Amazon-provided IPv6 CIDR block
○ IPv6 CIDR owned by me

Include and connect a subnet within the CIDR block.



VPC > Subnets > Create subnet

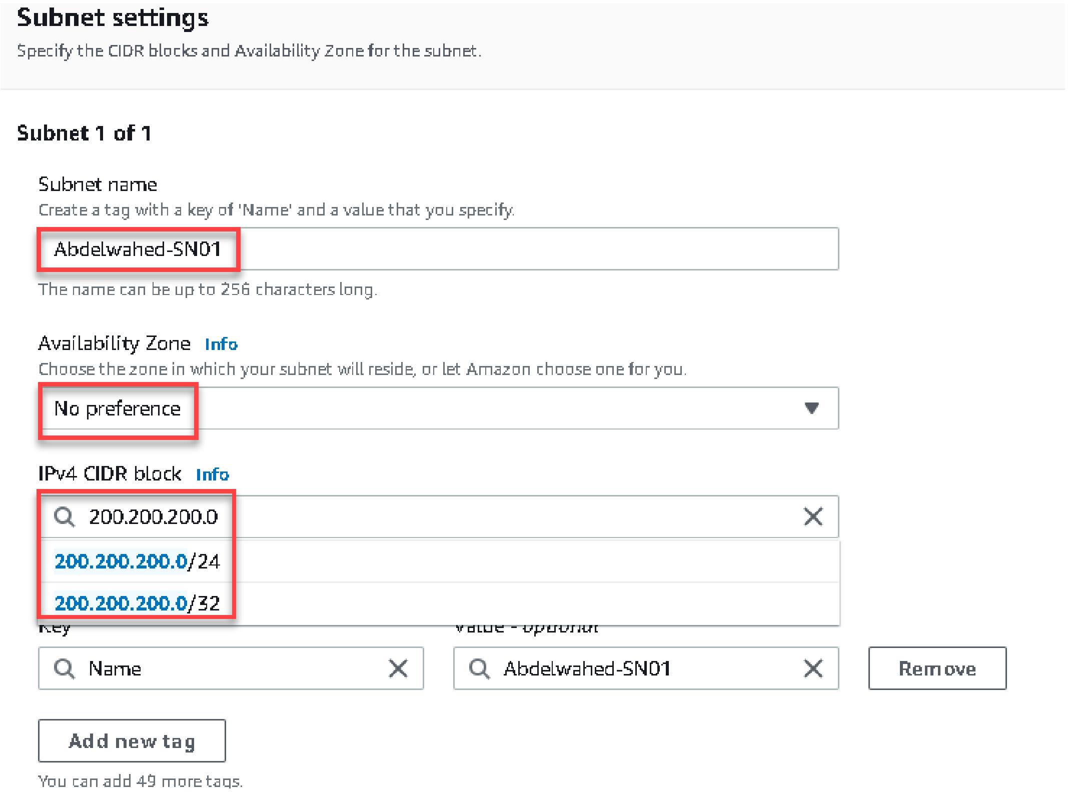
Create subnet Info

VPC

VPC ID
Create subnets in this VPC.
vpc-0984d21dc9d9a645d (aabdelwahed-vpc01)

Associated VPC CIDRs

IPv4 CIDRs
200.200.200.0/24



Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

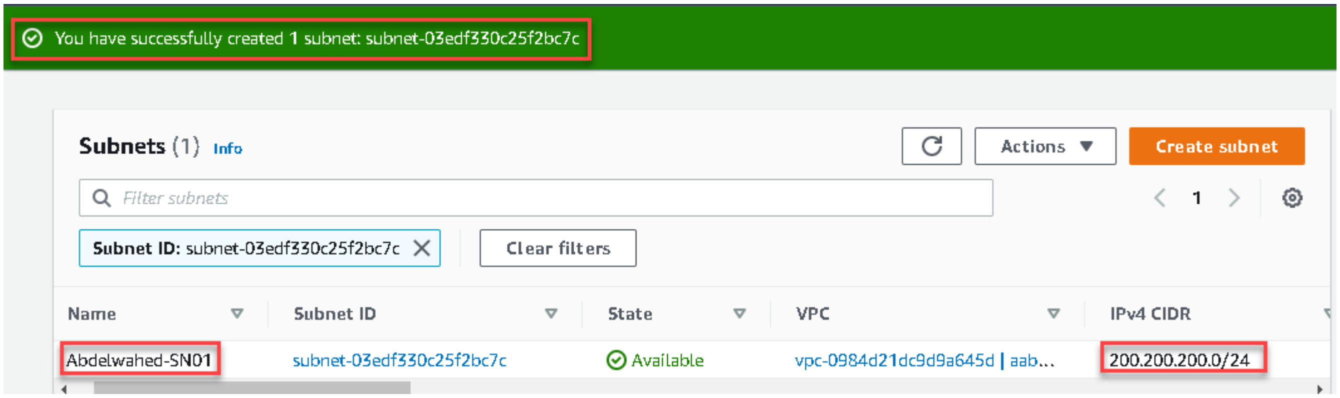
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
Abdelwahed-SN01
The name can be up to 256 characters long.

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

IPv4 CIDR block Info
200.200.200.0
200.200.200.0/24
200.200.200.0/32

Key	Value - optional
Name	Abdelwahed-SN01

You can add 49 more tags.

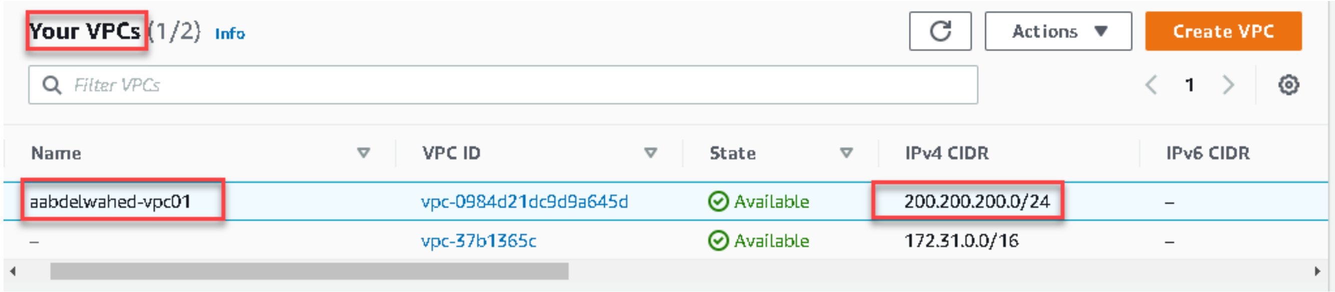


You have successfully created 1 subnet: subnet-03edf330c25f2bc7c

Subnets (1) Info

Subnet ID: subnet-03edf330c25f2bc7c

Name	Subnet ID	State	VPC	IPv4 CIDR
Abdelwahed-SN01	subnet-03edf330c25f2bc7c	Available	vpc-0984d21dc9d9a645d | aab...	200.200.200.0/24



Your VPCs (1/2) Info

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR
aabdelwahed-vpc01	vpc-0984d21dc9d9a645d	Available	200.200.200.0/24	–
–	vpc-37b1365c	Available	172.31.0.0/16	–