

AWS S3

- How to Make Private object URL to Public URL and Give Permission
- Storage Classes

1. Create Bucket and put some file or images or code and go to the properties of this object and Copy this Object URL and Paste In other page and when we try to access it then it Gives Error.

The screenshot shows the AWS S3 Object Properties page for an object named '9c15477d25ff2fb3781cb35208d31f87.jpeg'. The 'Properties' tab is selected. The 'Object overview' section displays the following details:

Attribute	Value
Owner	23mapot019
AWS Region	Asia Pacific (Sydney) ap-southeast-2
Last modified	August 2, 2024, 18:18:25 (UTC+05:30)
Size	913.9 KB
Type	jpeg
Key	9c15477d25ff2fb3781cb35208d31f87.jpeg
S3 URI	s3://ip-my-bucket-03/9c15477d25ff2fb3781cb35208d31f87.jpeg
Amazon Resource Name (ARN)	arn:aws:s3:::ip-my-bucket-03/9c15477d25ff2fb3781cb35208d31f87.jpeg
Entity tag (Etag)	bdd7b0332e4617daa1ee4a74dd0e4b36
Object URL	https://ip-my-bucket-03.s3.ap-southeast-2.amazonaws.com/9c15477d25ff2fb3781cb35208d31f87.jpeg

The 'Management configurations' section includes:

- Bucket properties
- Bucket Versioning
- Management configurations
- Replication status

At the bottom of the page, there are links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

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>F86J7933CR24HVB2</RequestId>
<HostId>j3/h7nQ11IwckGyZ7MZYHhWavXLjhHPcdGeX/DtFq4XWih+qXEPke8qm4bNbUriBEB2nPnnxtSqvmvitpkBmVH14P/PxWT3J82+dk1fqfY=</HostId>
</Error>
```

2. Go to the permission of the bucket and edit the Block Public Access.

The screenshot shows the AWS S3 console with the 'Permissions' tab selected for the 'ip-my-bucket-03' bucket. The 'Block public access (bucket settings)' section is open, showing that 'Block all public access' is set to 'On'. The 'Edit' button is visible next to the setting. Below it, the 'Bucket policy' section is partially visible.

3. Untick the Block all Public Access and Save changes and check Block All public Changes Will Off.

Sydney BansarUjani

Amazon S3

Buckets Access Grants Access Points Object Lambda Access Points Multi-Region Access Points Batch Operations IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens Dashboards Storage Lens groups AWS Organizations settings

Feature spotlight 7

AWS Marketplace for S3

Amazon S3 > Buckets > ip-my-bucket-03 > Edit Block public access (bucket settings)

Edit Block public access (bucket settings) Info

Block public access (bucket settings)

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

Cancel **Save changes**

CloudShell Feedback

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

Amazon S3

Buckets Access Grants Access Points Object Lambda Access Points Multi-Region Access Points Batch Operations IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens Dashboards Storage Lens groups AWS Organizations settings

Feature spotlight 7

AWS Marketplace for S3

Amazon S3 > Buckets > ip-my-bucket-03 > Edit Block public access (bucket settings)

Edit Block public access (bucket settings) Info

Block public access (bucket settings)

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

Cancel **Save changes**

The screenshot shows the AWS S3 console with the 'Buckets' section selected. In the center, a modal dialog titled 'Edit Block public access (bucket settings)' is open. The dialog contains a warning message: 'Updating the Block Public Access settings for this bucket will affect this bucket and all objects within. This may result in some objects becoming public.' Below this is a text input field with the word 'confirm' typed into it. At the bottom right of the dialog are 'Cancel' and 'Confirm' buttons. The main S3 interface shows a breadcrumb path: Amazon S3 > Buckets > ip-my-bucket-03 > Edit Block public access (bucket settings). The top navigation bar includes the AWS logo, services menu, search bar, and account information for Sydney and BansarUjani.

The screenshot shows the AWS S3 console with the 'Buckets' section selected. The main area displays the 'Block all public access' settings, which are currently set to 'Off'. A note indicates that turning 'On' would block public access to the bucket and its objects. Below this, there is a 'Bucket policy' section which is currently empty. The top navigation bar includes the AWS logo, services menu, search bar, and account information for Sydney and BansarUjani.

4. Go to the Bucket Policy And edit it.

The screenshot shows the AWS S3 'Edit bucket policy' interface. The left sidebar includes links for Buckets, Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Block Public Access settings, Storage Lens (expanded), Dashboards, Storage Lens groups, AWS Organizations settings, Feature spotlight (7 notifications), and AWS Marketplace for S3. The main content area has tabs for 'Bucket policy' (selected) and 'Info'. It displays the JSON policy:

```
arn:aws:s3:::ip-my-bucket-03
```

. Buttons for 'Policy examples' and 'Policy generator' are available. The 'Policy' section shows a single statement numbered 1. A 'Select a statement' dropdown and an 'Add new statement' button are present. The bottom navigation bar includes CloudShell, Feedback, © 2024, Amazon Web Services, Inc. or its affiliates., Privacy, Terms, and Cookie preferences.

5. Go to the policy Generator. and Select the S3 bucket in select type of policy.

In Effect select allow

In principal Write * (* means all of can access this object)

In Action Select GetObject

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

SQS Queue Policy
SQS Queue Policy
S3 Bucket Policy
VPC Endpoint Policy
IAM Policy
SNS Topic 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 SQS

All Services ('*')

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

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

Cloudy 29°C Search ENG IN 4:05 PM 8/4/2024

Step 3: Generate Policy

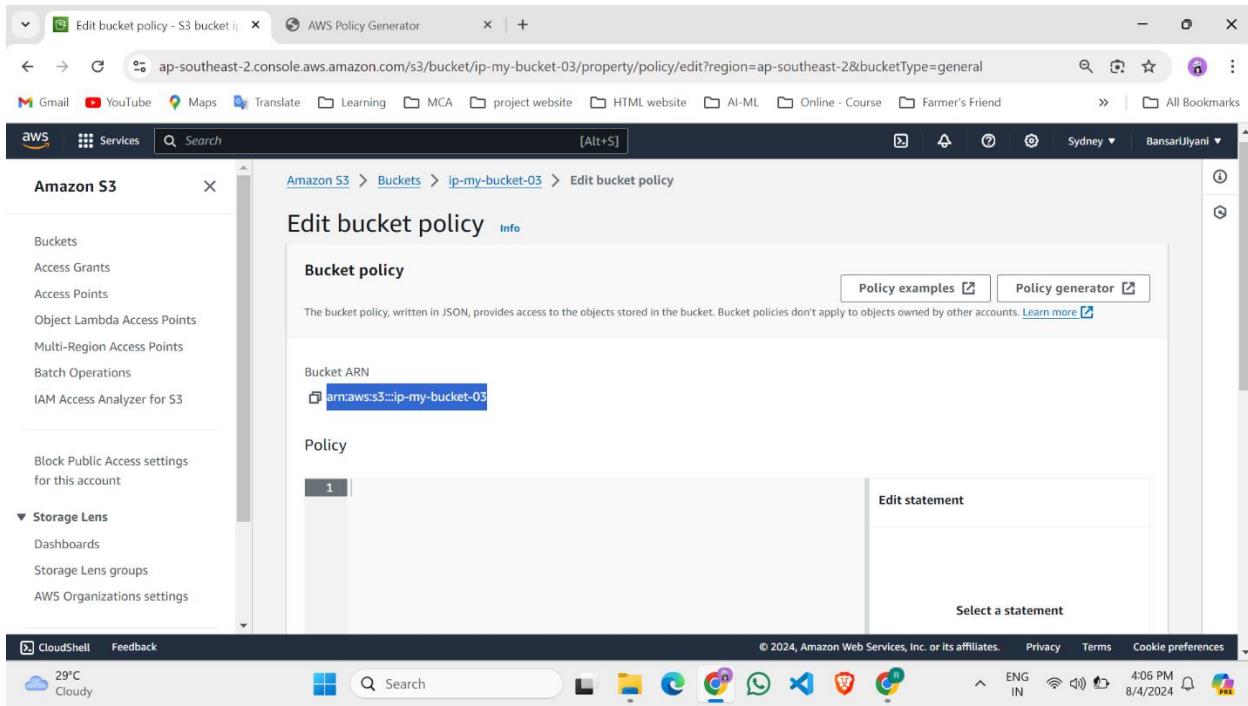
A policy is a document (written in the [Access Policy Language](#)) that acts as a container for one or more statements.

Add one or more statements above to generate a policy.

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 technologies.

Cloudy 29°C Search ENG IN 4:06 PM 8/4/2024

6. Generate policy and Get ARN of bucket from the bucket policy and paste it in ARN and put /* after this ARN.



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

1 Action(s) Selected

I) `arn:aws:s3:::ip-my-bucket-03/*`

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

Add Conditions (Optional)

Add Statement

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 ('*')

Actions All Actions ('*')

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

Add Conditions (Optional)

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.

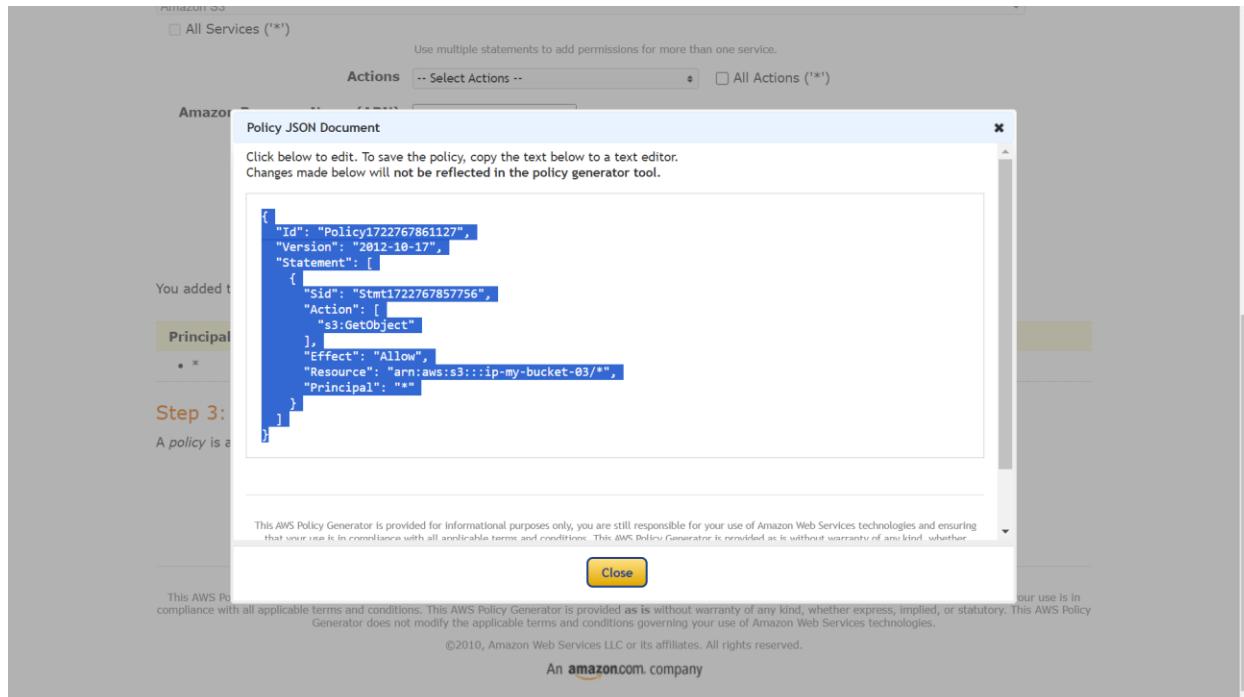
Add one or more statements above to generate a policy.

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 technologies.

©2010, Amazon Web Services LLC or its affiliates. All rights reserved.

An [amazon.com](#) company

7. Click on Add statement and Get this code . Copy it and paste it in Bucket Policy and Save Changes.



The screenshot shows the AWS Policy Generator interface. The URL is ap-southeast-2.console.aws.amazon.com/s3/bucket/ip-my-bucket-03/property/policy/edit?region=ap-southeast-2&bucketType=general. The policy document is displayed:

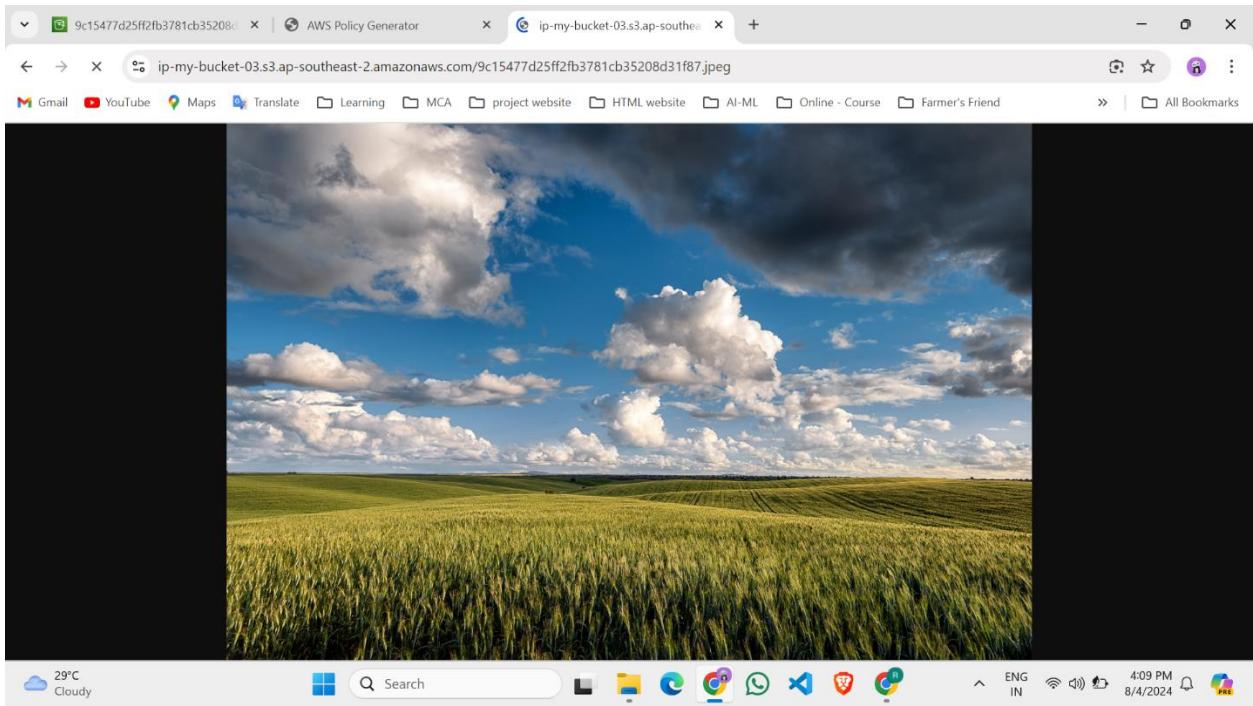
```
1 {  
2   "Id": "Policy1722767861127",  
3   "Version": "2012-10-17",  
4   "Statement": [  
5     {  
6       "Sid": "Stmt1722767857756",  
7       "Action": [  
8         "s3:GetObject"  
9       ],  
10      "Effect": "Allow",  
11      "Resource": "arn:aws:s3:::ip-my-bucket-03/*",  
12      "Principal": "*"  
13    }  
14  ]  
15 }
```

The right panel shows the 'Edit statement' section with a 'Select a statement' dropdown and a 'Add new statement' button.

The screenshot shows the Amazon S3 bucket 'ip-my-bucket-03'. The URL is Amazon.S3.ap-southeast-2.amazonaws.com/Buckets/ip-my-bucket-03. The bucket contains one object:

Name	Type	Last modified	Size	Storage class
9c15477d25ff2fb3781cb35208d31f87.jpeg	jpeg	August 2, 2024, 18:18:25 (UTC+05:30)	913.9 KB	Standard

8. Now Copy the object URL and Paste it in other Page And now You can See the object



Storage Classes

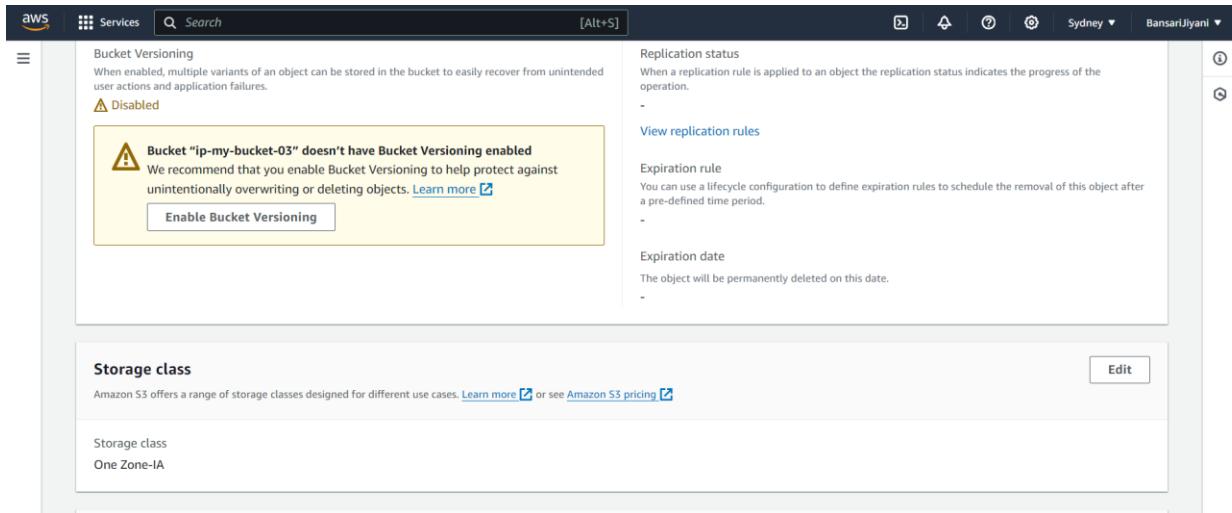
1. Create One bucket And Upload Any file and got the object Properties.and Go to the Storage class

The screenshot shows the AWS S3 Bucket Properties page for a bucket named "ip-my-bucket-03". A yellow warning box at the top left states: "Bucket 'ip-my-bucket-03' doesn't have Bucket Versioning enabled. We recommend that you enable Bucket Versioning to help protect against unintentionally overwriting or deleting objects. [Learn more](#)". Below this, there are sections for "Expiration rule" and "Expiration date". Under "Storage class", it says "Standard". There is also a section for "Server-side encryption settings" which shows "Encryption type: SSE-S3". At the bottom, there is a section for "Additional checksums".

The screenshot shows a comparison table for AWS Storage Classes. The columns are: Storage class, Designed for, Availability Zones, Min storage duration, and Cost. The rows include:

Storage class	Designed for	Availability Zones	Min storage duration	Cost
Standard	Frequently accessed data (more than once a month) with milliseconds access	≥ 3	-	-
Intelligent-Tiering	Data with changing or unknown access patterns	≥ 3	-	-
Standard-IA	Infrequently accessed data (once a month) with milliseconds access	≥ 3	30 days	1
One Zone-IA	Recreatable, infrequently accessed data (once a month) stored in a single Availability Zone with milliseconds access	1	30 days	1
Glacier Instant Retrieval	Long-lived archive data accessed once a quarter with instant retrieval in milliseconds	≥ 3	90 days	1
Glacier Flexible Retrieval (formerly Glacier)	Long-lived archive data accessed once a year with retrieval of minutes to hours	≥ 3	90 days	-
Glacier Deep	Long-lived archive data accessed less than once a year with retrieval of hours	≥ 3	180 days	-

2. Edit Standard With One-Zone-IA



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.
⚠️ Disabled

Bucket "ip-my-bucket-03" doesn't have Bucket Versioning enabled
We recommend that you enable Bucket Versioning to help protect against unintentionally overwriting or deleting objects. [Learn more](#)

[Enable Bucket Versioning](#)

Replication status
When a replication rule is applied to an object the replication status indicates the progress of the operation.

[View replication rules](#)

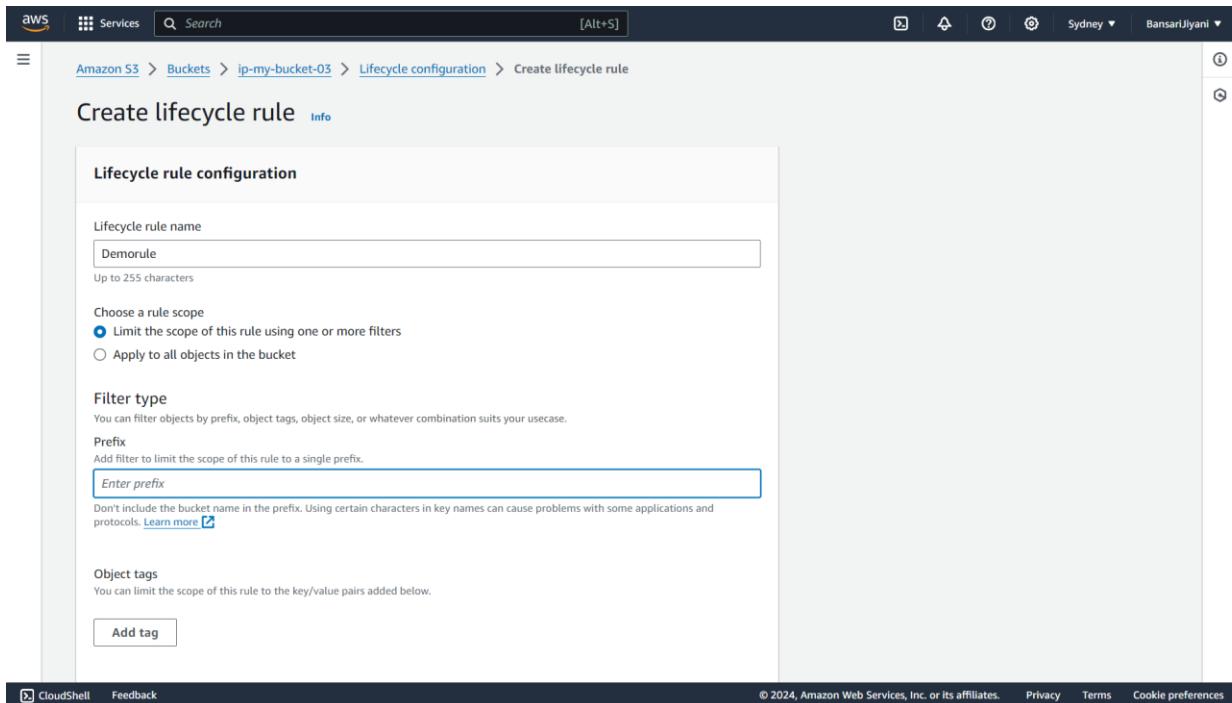
Expiration rule
You can use a lifecycle configuration to define expiration rules to schedule the removal of this object after a pre-defined time period.

Expiration date
The object will be permanently deleted on this date.

Storage class
Amazon S3 offers a range of storage classes designed for different use cases. [Learn more](#) or see [Amazon S3 pricing](#)

Storage class
One Zone-IA

3. Got to the Management of bucket and Create a Lifecycle as per your choice .



Amazon S3 > Buckets > ip-my-bucket-03 > Lifecycle configuration > Create lifecycle rule

Create lifecycle rule [Info](#)

Lifecycle rule configuration

Lifecycle rule name
Demorule
Up to 255 characters

Choose a rule scope
 Limit the scope of this rule using one or more filters
 Apply to all objects in the bucket

Filter type
You can filter objects by prefix, object tags, object size, or whatever combination suits your usecase.

Prefix
Add filter to limit the scope of this rule to a single prefix.
Enter prefix

Object tags
You can limit the scope of this rule to the key/value pairs added below.

[Add tag](#)

Also add the key for object

aws Services Search [Alt+S] Sydney BansarUjani

Up to 255 characters

Choose a rule scope

Limit the scope of this rule using one or more filters

Apply to all objects in the bucket

Filter type

You can filter objects by prefix, object tags, object size, or whatever combination suits your usecase.

Prefix

Add filter to limit the scope of this rule to a single prefix.

Enter prefix

Don't include the bucket name in the prefix. Using certain characters in key names can cause problems with some applications and protocols. [Learn more](#)

Object tags

You can limit the scope of this rule to the key/value pairs added below.

Key	Value - optional
key	value

Remove

Add tag

Object size

You can limit the scope of this rule to apply to objects based on their size. For example, you can filter out objects that might not be cost effective to transition to Glacier Flexible Retrieval (formerly Glacier) because of per-object fees.

Specify minimum object size

Specify maximum object size

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

Select a Lifecycle Rule actions

aws Services Search [Alt+S] Sydney BansarUjani

Lifecycle rule actions

Choose the actions you want this rule to perform. Per-request fees apply. [Learn more](#) or see [Amazon S3 pricing](#)

Move current versions of objects between storage classes

Move noncurrent versions of objects between storage classes

Expire current versions of objects

Permanently delete noncurrent versions of objects

Delete expired object delete markers or incomplete multipart uploads

These actions are not supported when filtering by object tags or object size.

Transition current versions of objects between storage classes

Choose transitions to move current versions of objects between storage classes based on your use case scenario and performance access requirements. These transitions start from when the objects are created and are consecutively applied. [Learn more](#)

Choose storage class transitions Days after object creation

Standard-IA Number of days Remove

A valid integer value is required.

Add transition

Review transition and expiration actions

Current version actions Noncurrent versions actions

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

Add the version of object between the Storage class like this and create a rule.

The screenshot shows the AWS S3 Storage Class Transition configuration page. At the top, there are several checkboxes for actions: Move noncurrent versions of objects between storage classes, Expire current versions of objects, Permanently delete noncurrent versions of objects, and Delete expired object delete markers or incomplete multipart uploads. A note states: "These actions are not supported when filtering by object tags or object size."

The main section is titled "Transition current versions of objects between storage classes". It lists four transitions:

- Standard-IA: Days after object creation: 90, Remove button
- One Zone-IA: Days after object creation: 60, Remove button. Note: "The integer value for One Zone-IA must be at least 30 more than the value for Standard-IA."
- Glacier Flexible Retrieval (formerly Glacier): Days after object creation: 30, Remove button. Note: "The integer value for Glacier Flexible Retrieval (formerly Glacier) must be at least 30 more than the value for One Zone-IA."
- Glacier Deep Archive: Days after object creation: Number of days, Remove button. Note: "A valid integer value is required."

An "Add transition" button is located below the list.

A yellow warning box contains the following text:
⚠️ Transitioning small objects to Glacier Flexible Retrieval (formerly Glacier) or Glacier Deep Archive will incur a per object cost
You will be charged for each object you transition to S3 Glacier Flexible Retrieval (formerly Glacier) or S3

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

Snow Family Service

- **Description :** AWS Snow Family is a service for customers who want to transport terabytes or petabytes of data to and from AWS, or who want to access the storage and compute power of the AWS Cloud locally and cost effectively in places where connecting to the internet might not be an option.
- **PRACTICAL :**

1. Search Snow Family Device and Order an AWS snow Family Device

The screenshot shows the AWS Snow Family service page. At the top, there's a navigation bar with the AWS logo, a search bar, and account information for 'Sydney' and 'BansariJiyani'. The main content area has a dark background with white text. It features the heading 'AWS Snow Family' and the subtext 'Process data at the edge and migrate data into and out of AWS'. Below this is a 'Ready to get started?' section with two buttons: 'Order an AWS Snow family device' (highlighted in orange) and 'Create your large data migration plan for migration greater than 500TB'. To the left, a sidebar titled 'Home' lists options like 'Large data migration plans', 'Create job', 'Jobs', and 'Prepaid jobs'. On the right, sections for 'Pricing' (listing 'AWS Snowcone', 'AWS Snowball', and 'AWS Snowmobile') and 'Getting started' (linking to the 'Snowball Edge data migration guide'). At the bottom, there's a footer with links for 'CloudShell', 'Feedback', and various AWS terms like '© 2024, Amazon Web Services, Inc. or its affiliates.', 'Privacy', 'Terms', and 'Cookie preferences'.

2. Give the Job name and Select option For a job type and go -> next

Snow family > Create new job

Step 1
Job type

Step 2
Compute and storage

Step 3
Features and options

Step 4
Security, shipping, and notification preferences

Step 5
Job summary

Job type Info

Job name Info
Your job will be created in the Asia Pacific (Sydney) region.

DemoJob1

Choose a job type

Import into Amazon S3 Info
AWS will ship an empty device to you for storage and compute workloads. You'll transfer your data onto it, and ship it back. After AWS gets it, your data will be moved.

Export from Amazon S3 Info
Choose what data you want to export from your S3 buckets for storage and compute workloads. AWS will load that data onto a device and ship it to you. When you're done ship the device back for erasing.

Local compute and storage only Info
Perform local compute and storage workloads without transferring data. You can order multiple devices in a cluster for increased durability and storage capacity.

Cancel **Next**

3. Select any snow device as per requirements

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

Step 2
Compute and storage

Step 3
Features and options

Step 4
Security, shipping, and notification preferences

Step 5
Job summary

Note:
Due to high demand for Snowball Edge Compute Optimized with GPU, your order will be sent to you as soon as a device is available.

Snow devices Info

Name	Compute	Memory	Storage (HDD)	Storage (SSD)
Snowcone	2 vCPUs	4 GB	8 TB	-
Snowcone SSD	2 vCPUs	4 GB	-	14 T
Snowball Edge Storage Optimized with 80TB	40 vCPUs	80 GB	80 TB	1 TB
Snowball Edge Storage Optimized with 210TB	104 vCPUs	416 GB	-	210 T
Snowball Edge Compute Optimized	52 vCPUs	208 GB	39.5 TB	7.68 T
<input checked="" type="radio"/> Snowball Edge Compute Optimized with GPU	52 vCPUs, GPU	208 GB	39.5 TB	7.68 T
Snowball Edge Compute Optimized	104 vCPUs	416 GB	-	28 T

Choose your pricing option Info
For Snowball Edge devices, you can choose to pay per day or to prepay for one or three years upfront at a discounted rate. For more information about pricing, see the [Snow pricing page](#).

Pricing Option
On-demand, per day pricing

4. Choose pricing Option and this pricing options are depends on your snow device which you choose

The screenshot shows the AWS Snowball Edge Compute Optimized with GPU configuration page. At the top, there is a table of device options with columns for name, vCPUs, memory, storage, and price. The 'Snowball Edge Compute Optimized with GPU' row is selected and highlighted. Below the table, a section titled 'Choose your pricing option' provides information about payment options: On-demand, per day pricing; 1 year commit upfront pricing; and 3 year commit upfront pricing. A dropdown menu shows 'On-demand, per day pricing' is currently selected. Other sections include 'Compute using EC2-compatible instances - optional' and a footer with standard AWS links.

5. Select EC2 compatible instance and that is also we change as per our personal machine.

- Select S3 bucket that where you want to put or load data

The screenshot shows the continuation of the AWS Snowball Edge Compute Optimized with GPU configuration page. It includes sections for selecting an EC2 AMI (Amazon-Linux-2 for Snow Family) and choosing an S3 bucket. The 'ip-my-bucket-03' bucket is selected. A 'Create a new S3 bucket' button is available. The bottom of the page features a search bar, a table of S3 buckets, and navigation buttons for 'Cancel', 'Previous', and 'Next'.

6. Got to the next and select Remote device Management and go -> next

Job type

Features and options [Info](#)

AWS Services for Snow
Select from the different tabs below to learn more and include additional AWS services for snow. These services will incur extra charges. [Pricing](#)

AWS IoT Greengrass

AWS IoT Greengrass for Snow
AWS Snow supports pre-installation of a Greengrass validated AMI on your Snow jobs to enable easy onboarding of IoT workloads for Snow devices. Once you receive the device, you can install AWS IoT Greengrass v2 on this AMI and run your IoT workloads. For more information on getting started with AWS IoT Greengrass for Snow, refer to [AWS IoT Greengrass documentation](#). This service will incur extra charges. [Pricing](#)

Install AWS IoT Greengrass validated AMI on my Snow device

0 service(s) selected

Remote device management [Info](#)
You can use OpsHub or Snowball Client to remotely unlock, reboot and monitor your device. [Learn more](#)

Manage the device remotely with OpsHub or Snowball Client

Cancel Previous Next

7. Select the encryption and service access type and also create a service role as per your needs and set the notification and create new SNS topic And Give SNS topic name and Email address.

Job type

Security, shipping, and notification preferences [Info](#)

Security preferences
Our IAM service role templates have changed recently.

Encryption [Info](#)
Select the AWS KMS key to encrypt your data.
Enter a key ARN

aws/importexport (default)

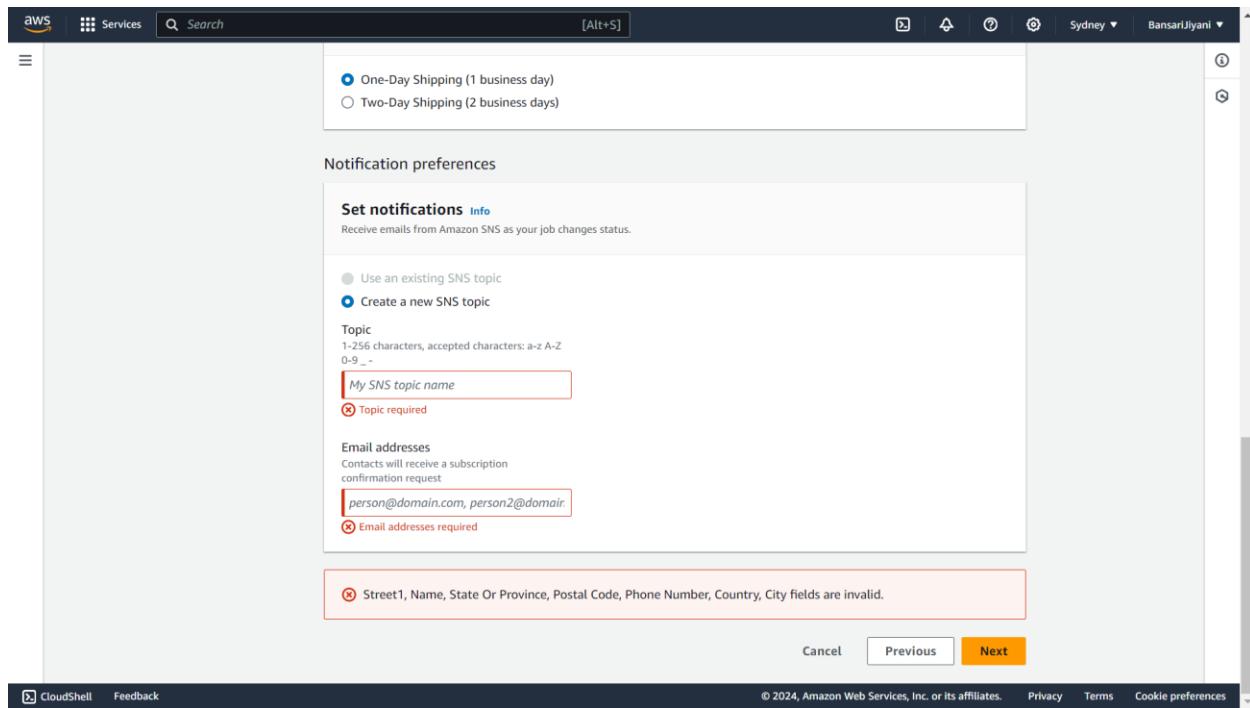
Choose service access type [Info](#)
Snow jobs require permissions to write to S3 and publish to SNS on your behalf.
By creating a Snow job, you grant Snow Family permissions to use S3 and SNS on your behalf. [Learn more](#)

Create service role

Shipping preferences
Shipping address [Info](#)

Use recent address
 Add a new address

Cancel Previous Next



- **What is Edge computing**

- Edge computing in AWS is a powerful approach to building and deploying applications that require low-latency access to data and resources. By utilizing AWS services like Outposts, Local Zones, Wavelength, and IoT Greengrass, businesses can optimize their infrastructure to deliver faster, more reliable, and cost-effective solutions. This makes edge computing an essential strategy for modern applications that demand high performance and real-time processing.

