AWS S3

Amazon S3 (Simple Storage Service) is a scalable object storage service offered by AWS (Amazon Web Services).

Object Storage: S3 stores data as objects within buckets. Each object consists of data, metadata, and a unique identifier.

Scalability: S3 scales automatically as your data grows, so you don't need to worry about running out of space.

Access Control: You can control who has access to your data using AWS Identity and Access Management (IAM) policies, bucket policies, and access control lists (ACLs).

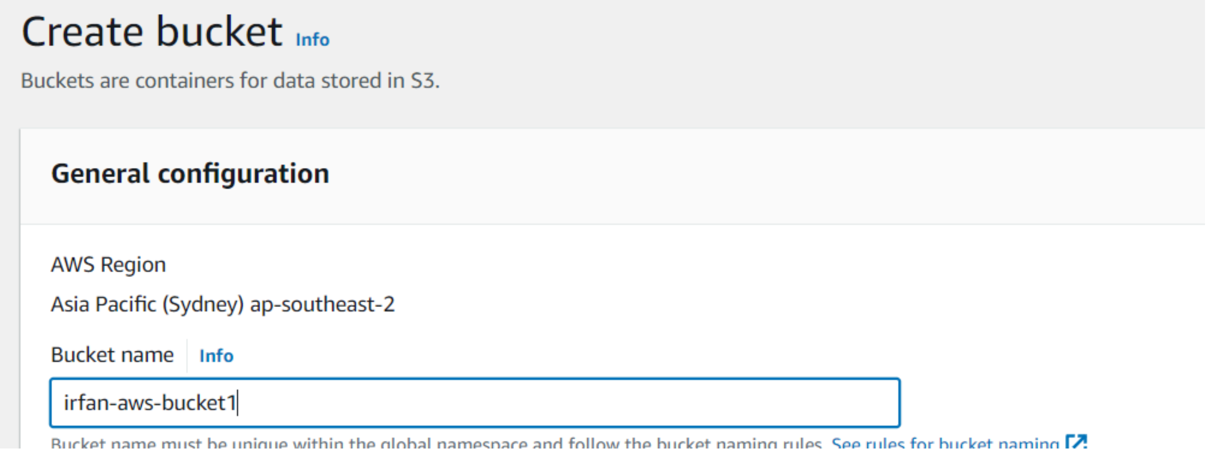
Security: S3 supports encryption both in transit and at rest, and integrates with AWS Key Management Service (KMS) for key management.

Versioning: S3 provides versioning, which allows you to keep multiple versions of an object in the same bucket.

Storage Classes: S3 offers various storage classes like S3 Standard, S3 Intelligent-Tiering, S3 Glacier (for archival), and more, optimised for different use cases based on cost and performance.

Use Cases: S3 is widely used for backup and restore, data archiving, big data analytics, and serving static website content.

How to Create Bucket in AWS



Create bucket Info

Buckets are containers for data stored in S3.

General configuration

AWS Region

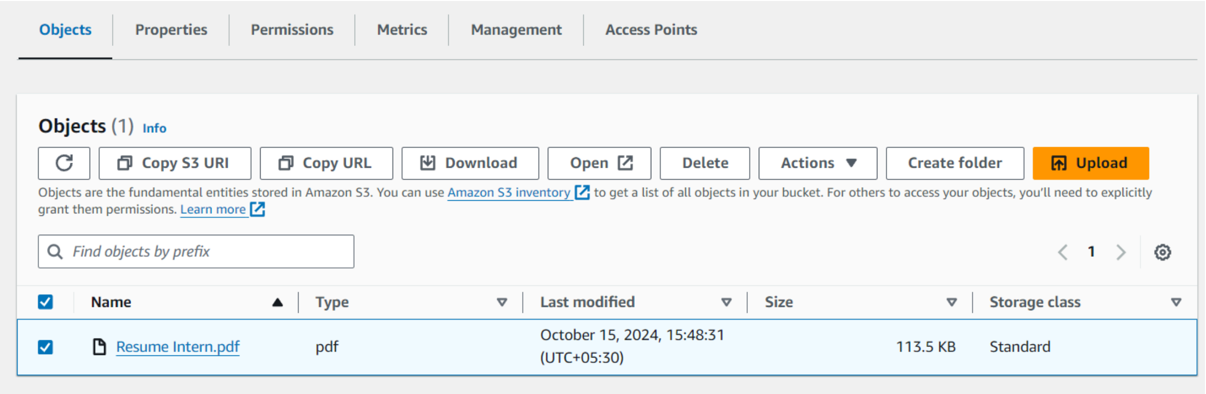
Asia Pacific (Sydney) ap-southeast-2

Bucket name Info

irfan-aws-bucket1

Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

Note: Bucket name should be unique World-wide.



Objects (1) Info

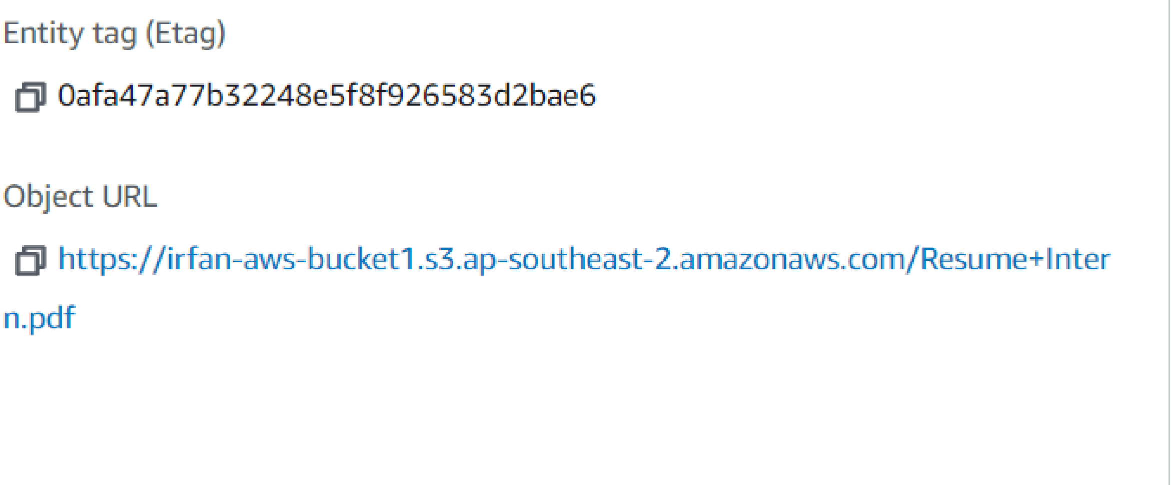
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Find objects by prefix

☑	Name	Type	Last modified	Size	Storage class
☑	Resume Intern.pdf	pdf	October 15, 2024, 15:48:31 (UTC+05:30)	113.5 KB	Standard

Click Open to open up the file.

URL:-

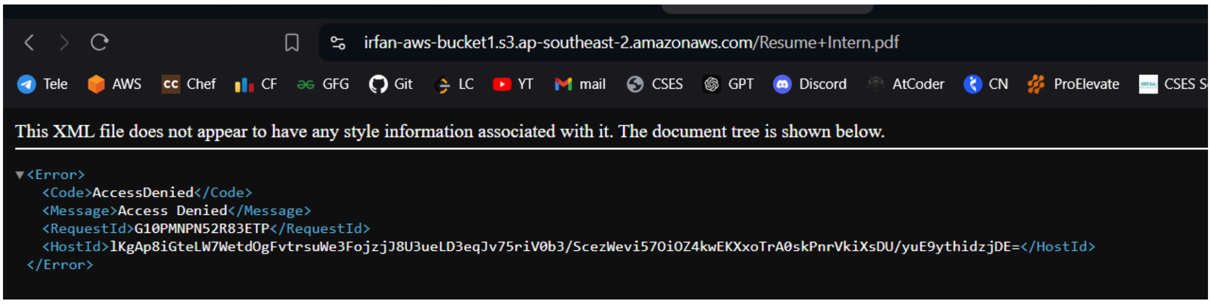


Entity tag (Etag)

0afa47a77b32248e5f8f926583d2bae6

Object URL

https://irfan-aws-bucket1.s3.ap-southeast-2.amazonaws.com/Resume+Intern.pdf

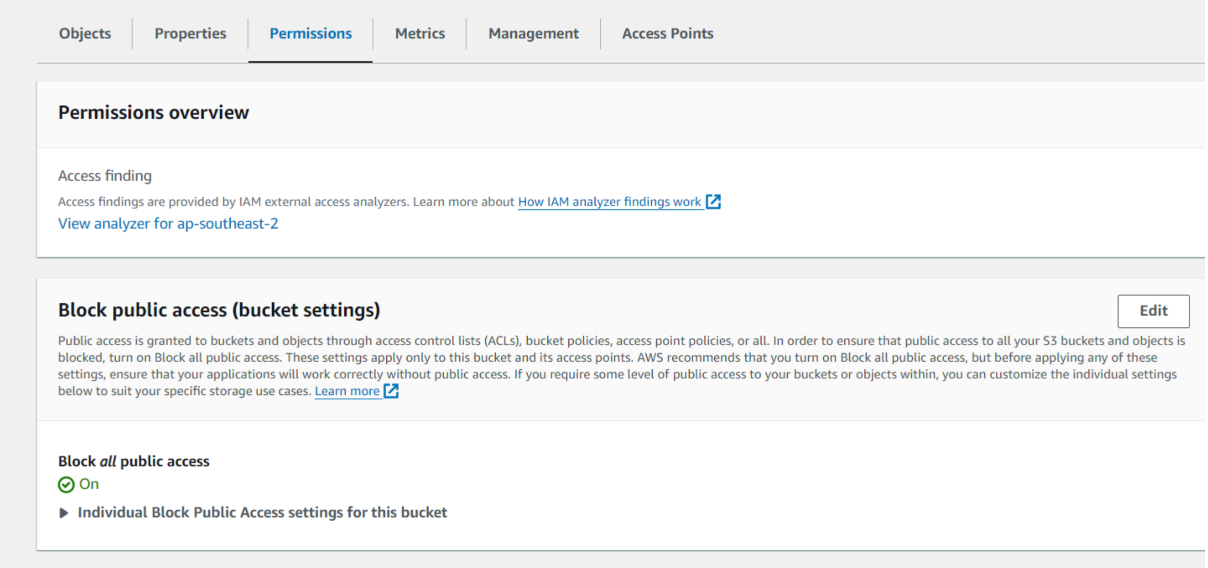


irfan-aws-bucket1.s3.ap-southeast-2.amazonaws.com/Resume+Intern.pdf

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>G10PMNPN52R83ETP</RequestId>
   <HostId>lKgAp8iGteLW7WetdOgFvtrsuWe3FojzjJ8U3ueLD3eqJv75riV0b3/ScezWevi57OiOZ4kwEKXxoTrA0skPnrVkiXsDU/yuE9ythidzjDE=</HostId>
 </Error>
```

Not accessible.



Permissions overview

Access finding

Access findings are provided by IAM external access analyzers. Learn more about How IAM analyzer findings work

View analyzer for ap-southeast-2

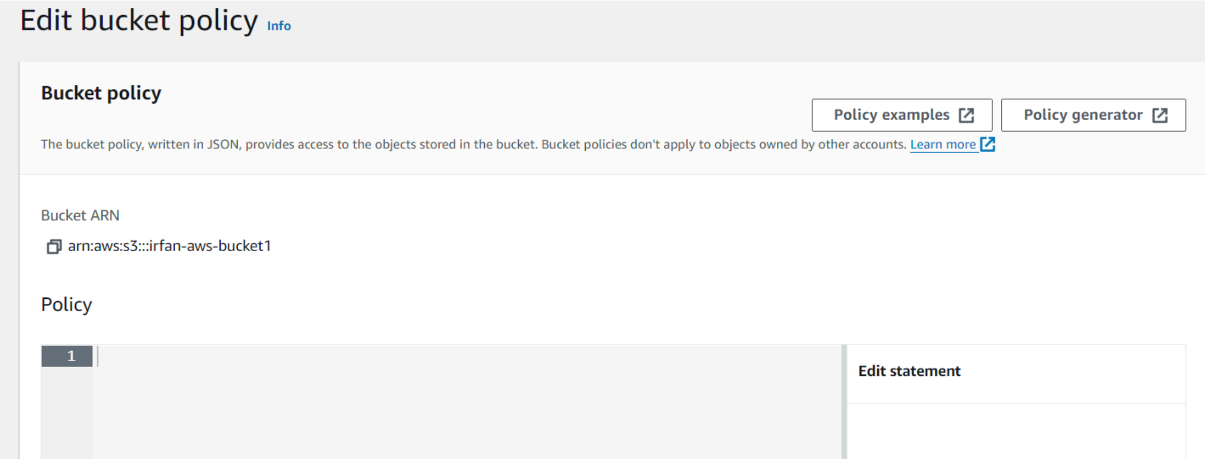
Block public access (bucket settings)

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

✓ On

▶ Individual Block Public Access settings for this bucket



Edit bucket policy Info

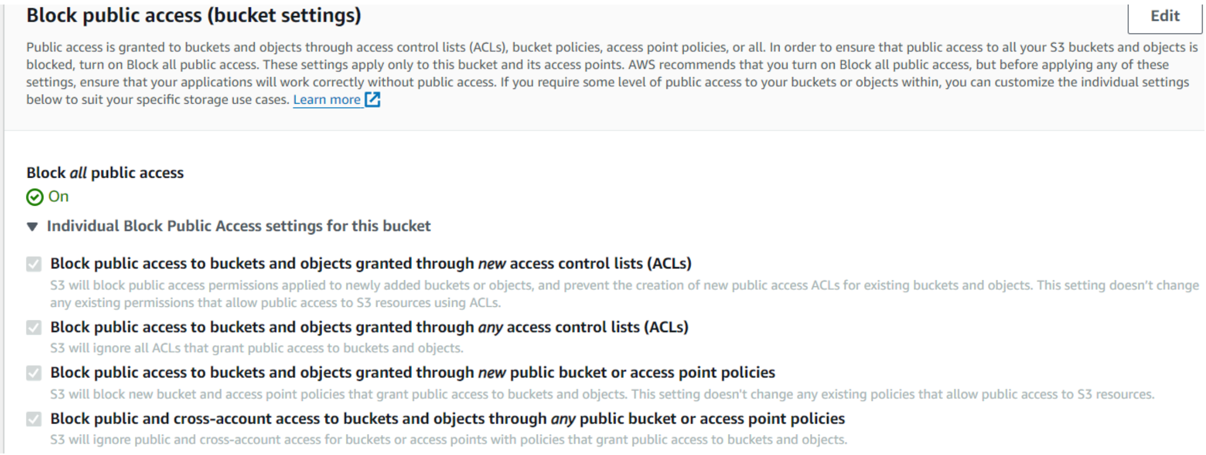
Bucket policy

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:::irfan-aws-bucket1

Policy



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
✓ On

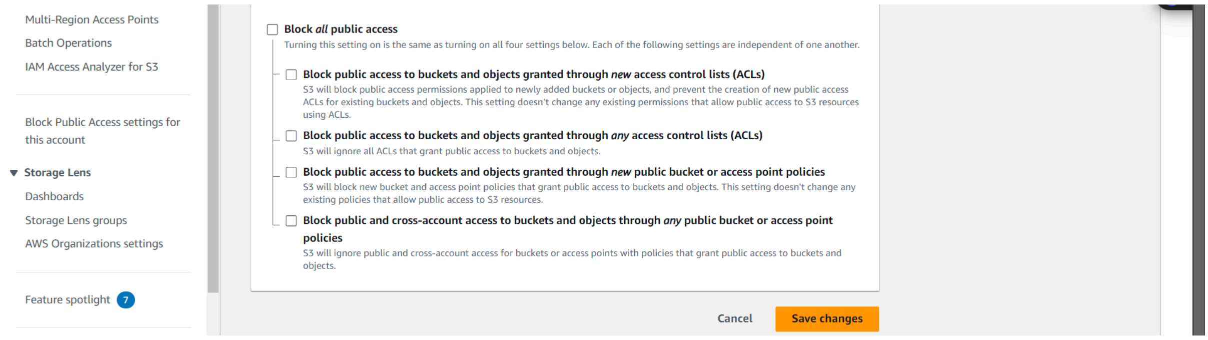
▼ Individual Block Public Access settings for this bucket

☑ 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.



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

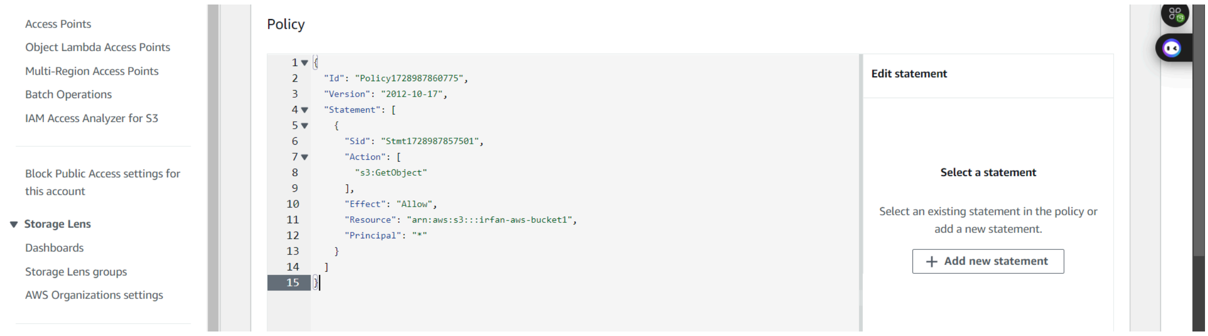
□ Block *all* public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

□ 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.



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

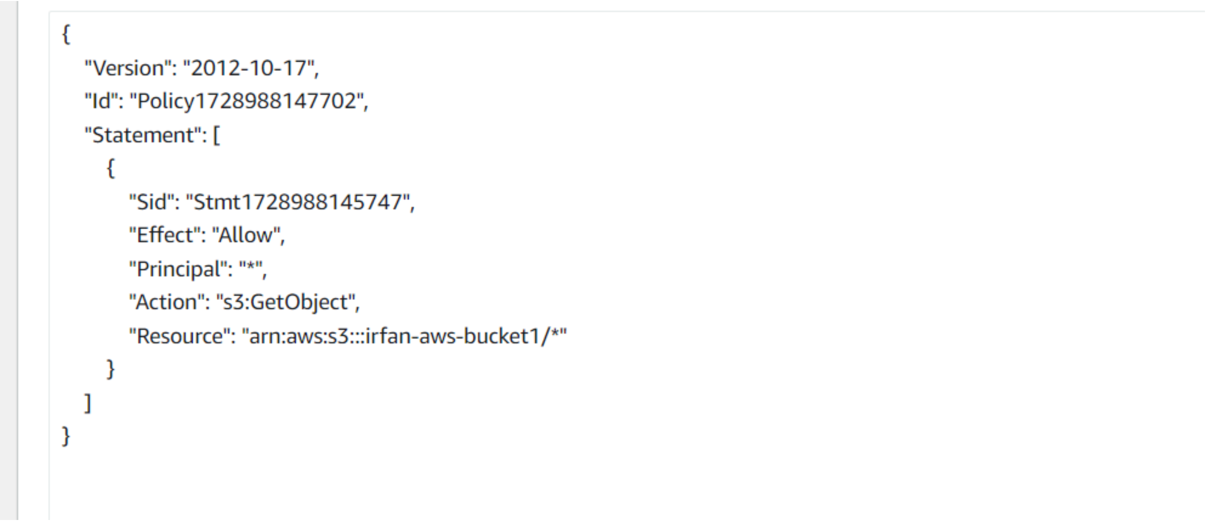
Policy

```
{
  "Id": "Policy1728987860775",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1728987857501",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::irfan-aws-bucket1",
      "Principal": "*"
    }
  ]
}
```

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.



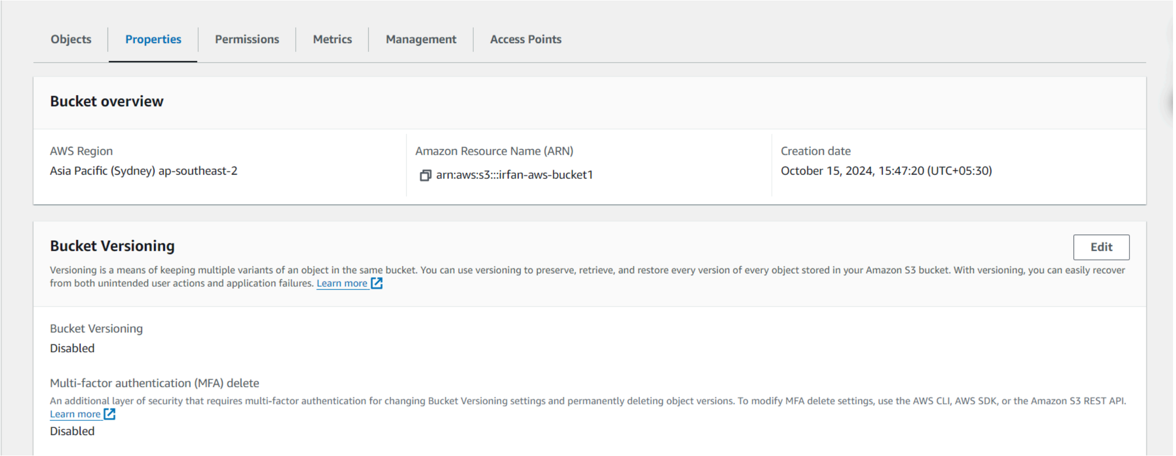
```
{
  "Version": "2012-10-17",
  "Id": "Policy1728988147702",
  "Statement": [
    {
      "Sid": "Stmt1728988145747",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::irfan-aws-bucket1/*"
    }
  ]
}
```

Added */ at end of ARN.

https://irfan-aws-bucket1.s3.ap-southeast-2.amazonaws.com/Resume+Intern.pdf
Public URL created:

We have made the Bucket Public. Any other object uploaded will also be public.

S3 Versioning - What is Versioning - Prevent a Object from Deletion



Bucket overview

AWS Region
Asia Pacific (Sydney) ap-southeast-2

Amazon Resource Name (ARN)
arn:aws:s3:::irfan-aws-bucket1

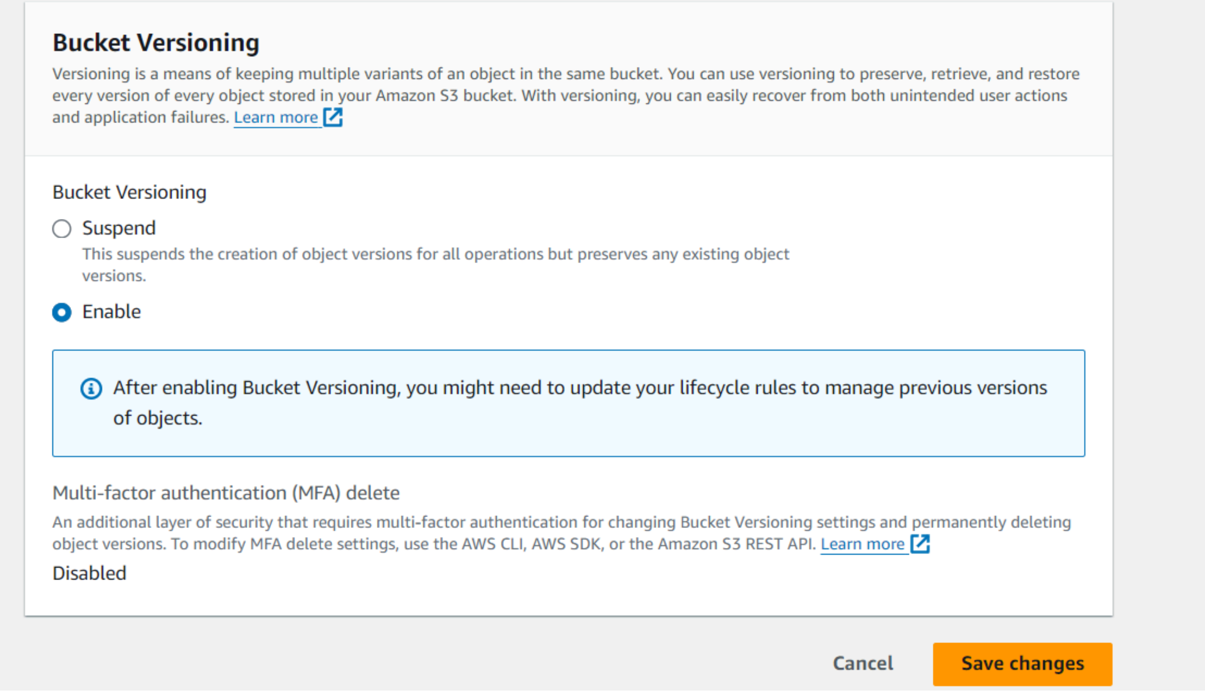
Creation date
October 15, 2024, 15:47:20 (UTC+05:30)

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
Disabled

Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more
Disabled



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

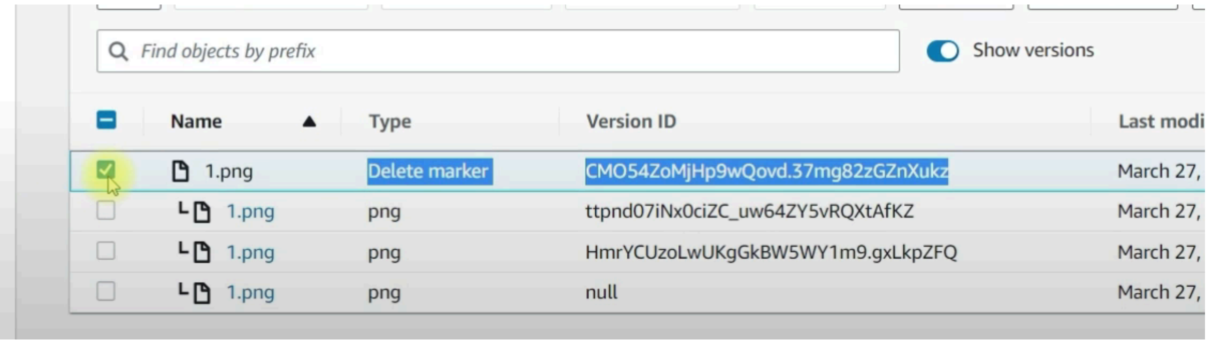
Bucket Versioning

○ Suspend
This suspends the creation of object versions for all operations but preserves any existing object versions.

● Enable

After enabling Bucket Versioning, you might need to update your lifecycle rules to manage previous versions of objects.

Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more
Disabled



	Name	Type	Version ID	Last modi
☑	1.png	Delete marker	CMO54ZoMjHp9wQovd.37mg82zGZnXukz	March 27,
□	└ 1.png	png	ttpnd07iNx0ciZC_uw64ZY5vRQXtAfKZ	March 27,
□	└ 1.png	png	HmrYCUzoLwUKgGkBW5WY1m9.gxLkpZFQ	March 27,
□	└ 1.png	png	null	March 27,

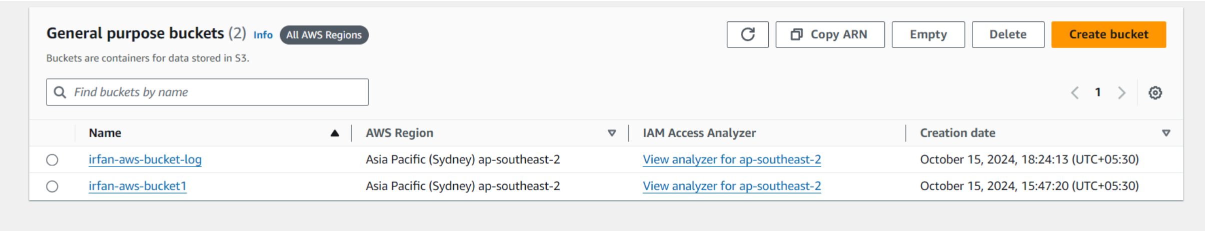
Same/Cross Region Replication - What is SRR/CRR - Use of SRR/CRR?

Same-Region Replication (SRR) replicates objects between S3 buckets within the same AWS region, while **Cross-Region Replication (CRR)** replicates objects across different AWS regions.

Use of SRR: SRR is primarily used for data redundancy within the same region, compliance requirements, and backup in case of data corruption.

Use of CRR: CRR provides disaster recovery, geographic data distribution for reduced latency, and compliance with regulations requiring data storage in specific regions.

AWS S3 - Configure Logging in S3 Bucket - How to Enable S3 Logging



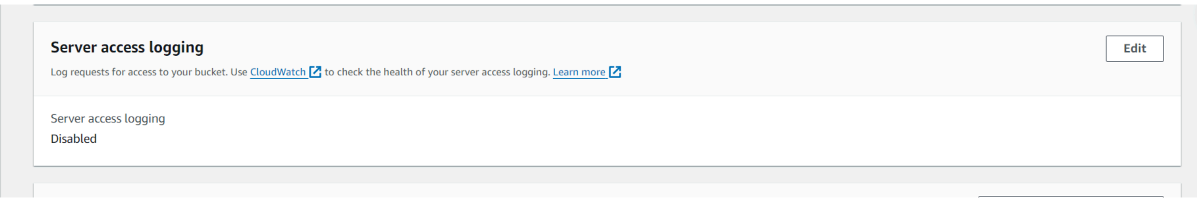
General purpose buckets (2) Info All AWS Regions

Buckets are containers for data stored in S3.

	Name	AWS Region	IAM Access Analyzer	Creation date
○	irfan-aws-bucket-log	Asia Pacific (Sydney) ap-southeast-2	View analyzer for ap-southeast-2	October 15, 2024, 18:24:13 (UTC+05:30)
○	irfan-aws-bucket1	Asia Pacific (Sydney) ap-southeast-2	View analyzer for ap-southeast-2	October 15, 2024, 15:47:20 (UTC+05:30)

Log files should be made in different bucket .
If done in same bucket it will be stuck in a loop. File added to Bucket. It gets logged. This logging also triggers the log..which triggers another log.

Both bucket in same region.

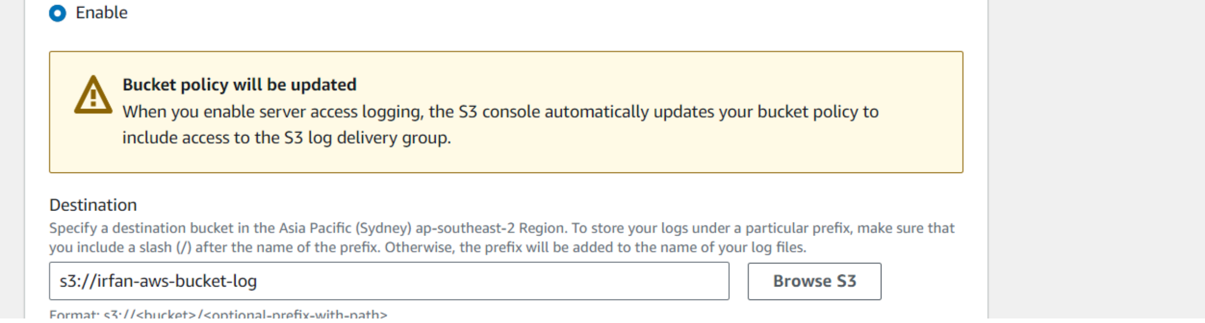


Server access logging

Log requests for access to your bucket. Use CloudWatch to check the health of your server access logging. Learn more

Server access logging
Disabled

Enable.
Choose the log-bucket.



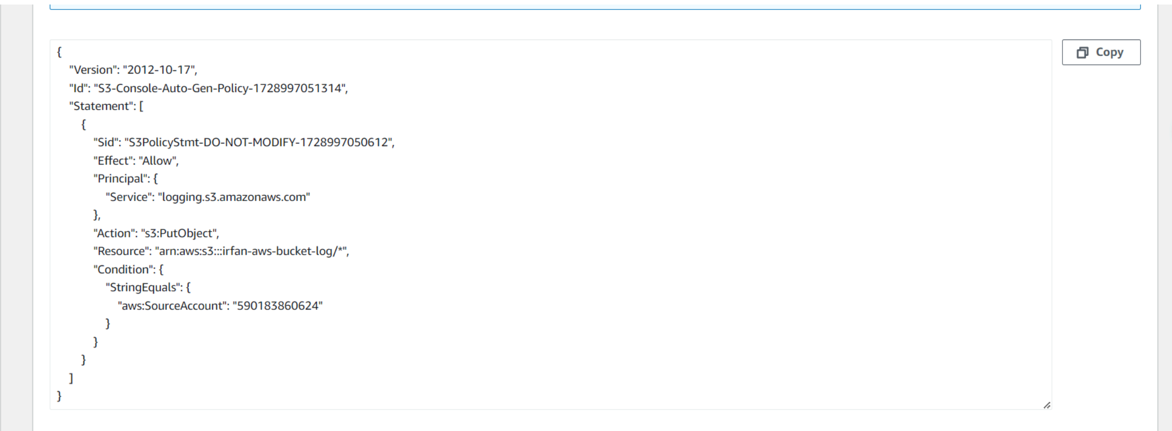
● Enable

Bucket policy will be updated
When you enable server access logging, the S3 console automatically updates your bucket policy to include access to the S3 log delivery group.

Destination
Specify a destination bucket in the Asia Pacific (Sydney) ap-southeast-2 Region. To store your logs under a particular prefix, make sure that you include a slash (/) after the name of the prefix. Otherwise, the prefix will be added to the name of your log files.

s3://irfan-aws-bucket-log

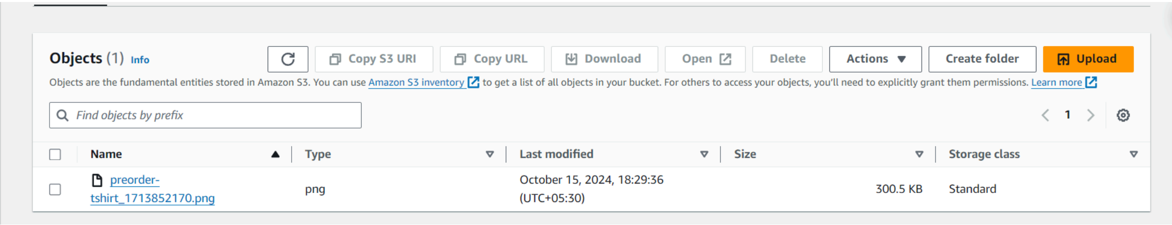
Format: s3://<bucket>/<optional-prefix-with-path>



```
{
  "Version": "2012-10-17",
  "Id": "S3-Console-Auto-Gen-Policy-1728997051314",
  "Statement": [
    {
      "Sid": "S3PolicyStmt-DO-NOT-MODIFY-1728997050612",
      "Effect": "Allow",
      "Principal": {
        "Service": "logging.s3.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::irfan-aws-bucket-log/*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "590183860624"
        }
      }
    }
  ]
}
```

Permissions added automatically in log bucket.

Uploaded a file.

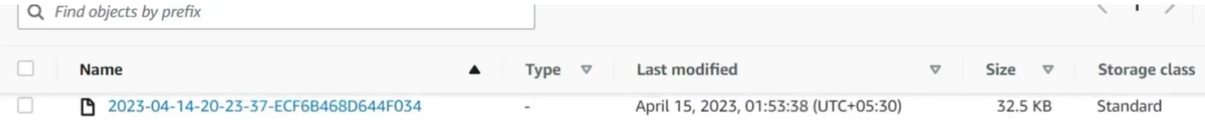


Objects (1) Info

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

Find objects by prefix

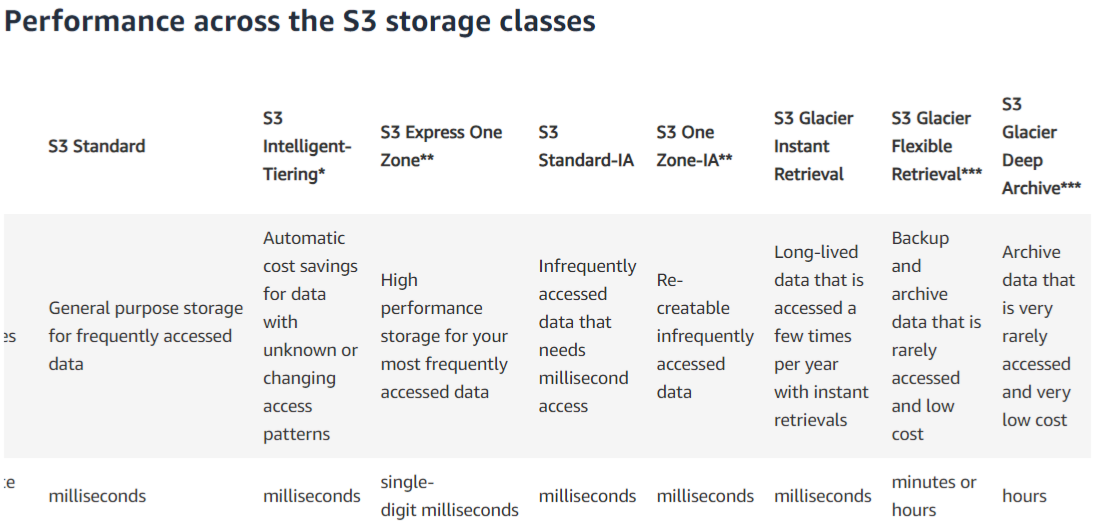
□	Name	Type	Last modified	Size	Storage class
□	preorder-tshirt_1713852170.png	png	October 15, 2024, 18:29:36 (UTC+05:30)	300.5 KB	Standard



Find objects by prefix

□	Name	Type	Last modified	Size	Storage class
□	2023-04-14-20-23-37-ECF6B468D644F034	-	April 15, 2023, 01:53:38 (UTC+05:30)	32.5 KB	Standard

Logs added.



Performance across the S3 storage classes

	S3 Standard	S3 Intelligent-Tiering*	S3 Express One Zone**	S3 Standard-IA	S3 One Zone-IA**	S3 Glacier Instant Retrieval	S3 Glacier Flexible Retrieval***	S3 Glacier Deep Archive***
es	General purpose storage for frequently accessed data	Automatic cost savings for data with unknown or changing access patterns	High performance storage for your most frequently accessed data	Infrequently accessed data that needs millisecond access	Re-creatable infrequently accessed data	Long-lived data that is accessed a few times per year with instant retrievals	Backup and archive data that is rarely accessed and low cost	Archive data that is very rarely accessed and very low cost
:e	milliseconds	milliseconds	single-digit milliseconds	milliseconds	milliseconds	milliseconds	minutes or hours	hours

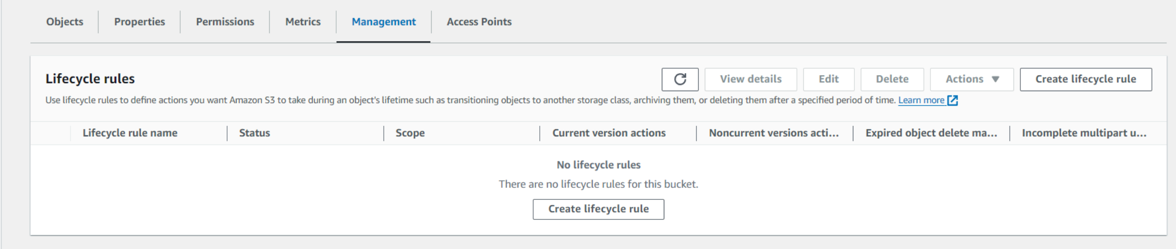
Amazon S3 offers a variety of **storage classes** tailored to different use cases, balancing cost, performance, and durability:

1. **S3 Standard**: General-purpose storage for frequently accessed data with low latency and high throughput.
2. **S3 Intelligent-Tiering**: Automatically moves data between two access tiers (frequent and infrequent) based on usage patterns to optimize costs.
3. **S3 Standard-IA (Infrequent Access)**: For data that is accessed less frequently but requires rapid access when needed, at a lower cost than Standard.
4. **S3 One Zone-IA**: Like Standard-IA but stored in a single availability zone, offering lower cost but reduced redundancy.
5. **S3 Glacier**: Low-cost storage for archival data that is infrequently accessed, with retrieval times ranging from minutes to hours.
6. **S3 Glacier Deep Archive**: The lowest-cost storage for data that is rarely accessed, with retrieval times of up to 12 hours.
7. **S3 Outposts**: For data that needs to be stored locally on-premises, using S3 APIs, and ensuring data residency.

Data Lifecycle Management

If a movie is released ..in initial days it requires frequent access and then the number of requests decreases.

We have to move from a faster access storage to slow to save costs.



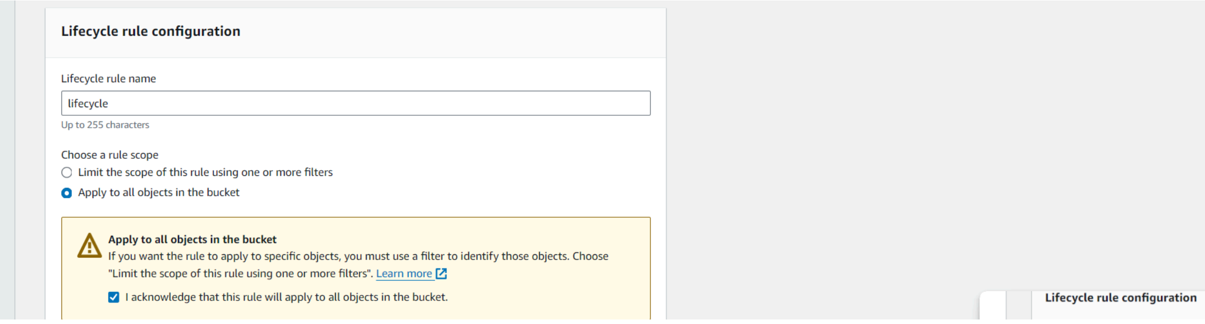
Lifecycle rules

Use lifecycle rules to define actions you want Amazon S3 to take during an object's lifetime such as transitioning objects to another storage class, archiving them, or deleting them after a specified period of time. Learn more

Lifecycle rule name	Status	Scope	Current version actions	Noncurrent versions acti...	Expired object delete ma...	Incomplete multipart u...

No lifecycle rules

There are no lifecycle rules for this bucket.


Lifecycle rule configuration

Lifecycle rule name

lifecycle

Up to 255 characters

Choose a rule scope

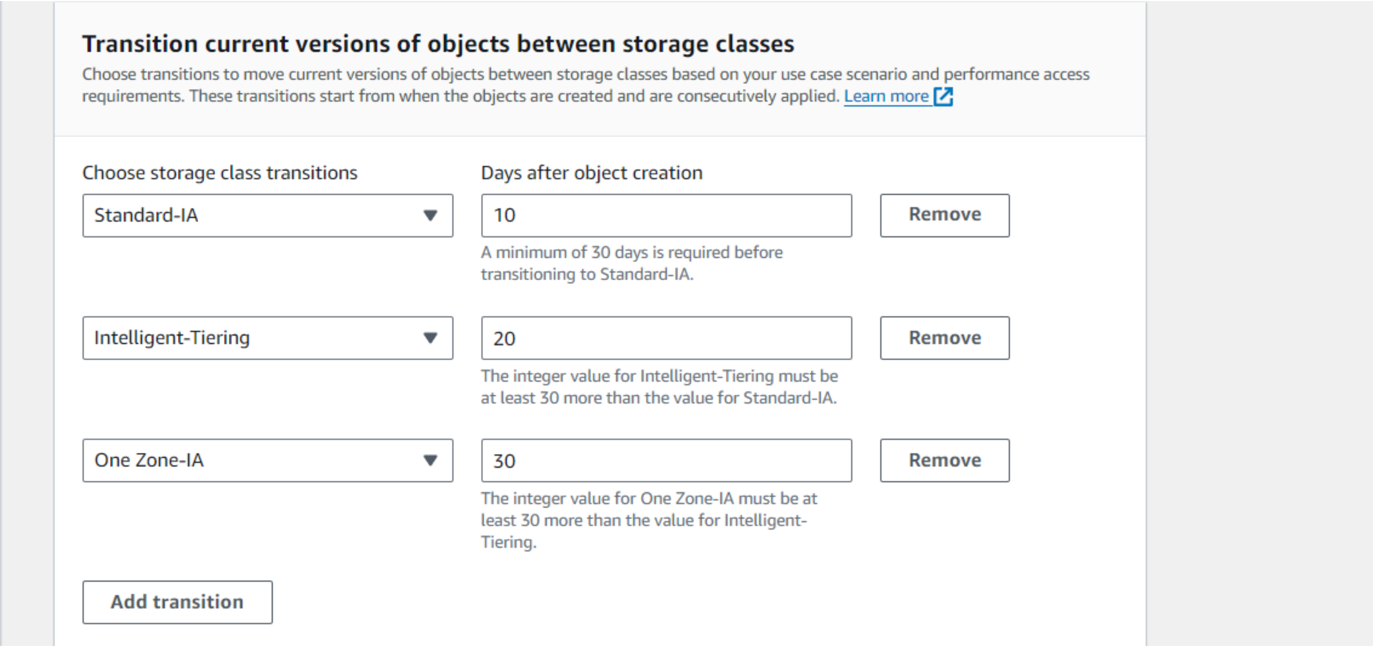
○ Limit the scope of this rule using one or more filters

● Apply to all objects in the bucket

Apply to all objects in the bucket

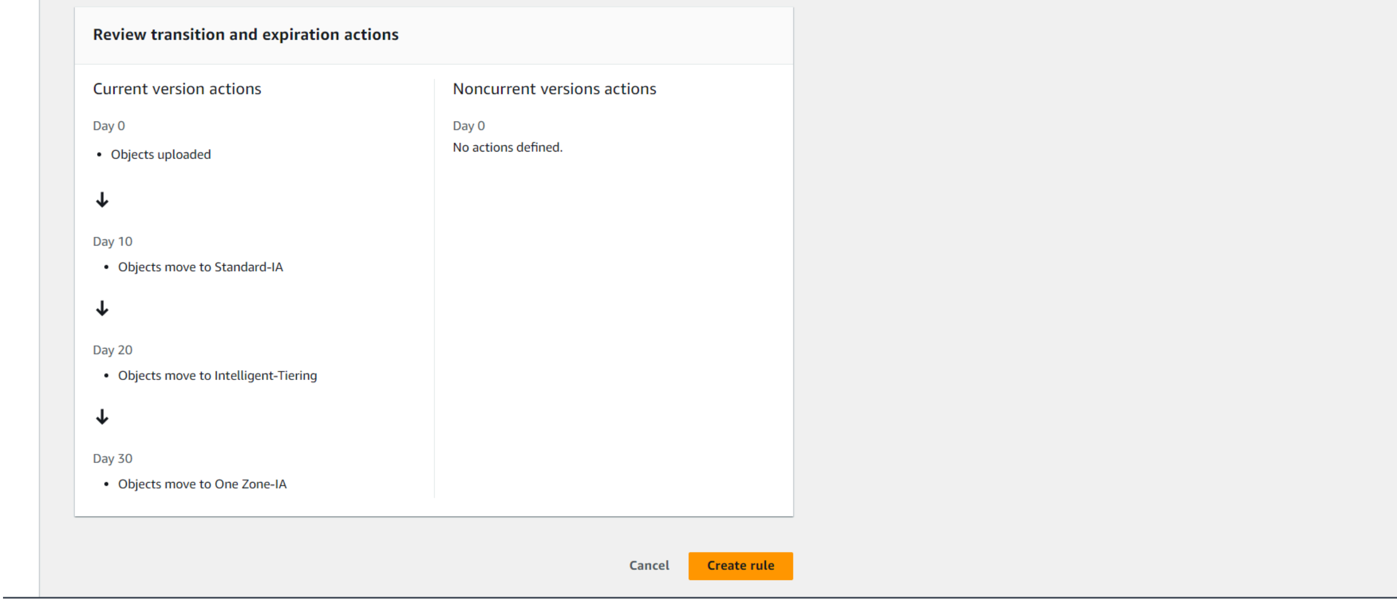
If you want the rule to apply to specific objects, you must use a filter to identify those objects. Choose "Limit the scope of this rule using one or more filters". Learn more

☑ I acknowledge that this rule will apply to all objects in the bucket.


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 ▼	10 A minimum of 30 days is required before transitioning to Standard-IA.	Remove
Intelligent-Tiering ▼	20 The integer value for Intelligent-Tiering must be at least 30 more than the value for Standard-IA.	Remove
One Zone-IA ▼	30 The integer value for One Zone-IA must be at least 30 more than the value for Intelligent-Tiering.	Remove



Review transition and expiration actions

Current version actions

Day 0

- Objects uploaded

↓

Day 10

- Objects move to Standard-IA

↓

Day 20

- Objects move to Intelligent-Tiering

↓

Day 30

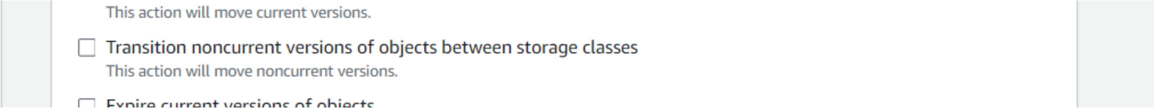
- Objects move to One Zone-IA

Noncurrent versions actions

Day 0

No actions defined.

For versions:



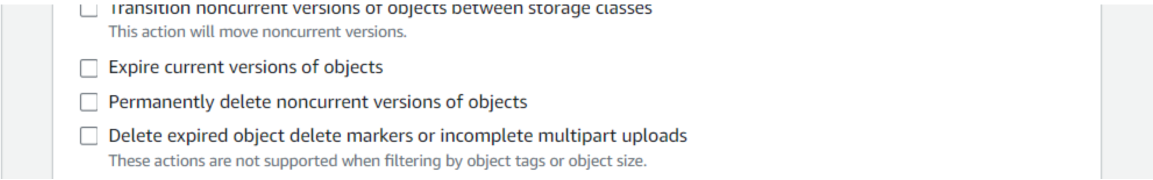
This action will move current versions.

☐ Transition noncurrent versions of objects between storage classes

This action will move noncurrent versions.

☐ Expire current versions of objects

For expiration:



☐ Transition noncurrent versions of objects between storage classes

This action will move noncurrent versions.

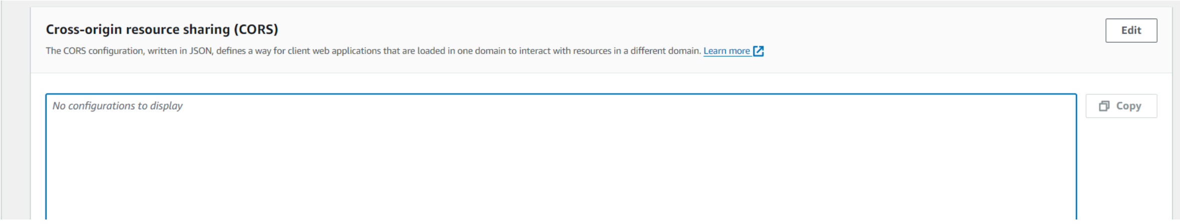
☐ Expire current versions of objects

☐ 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.

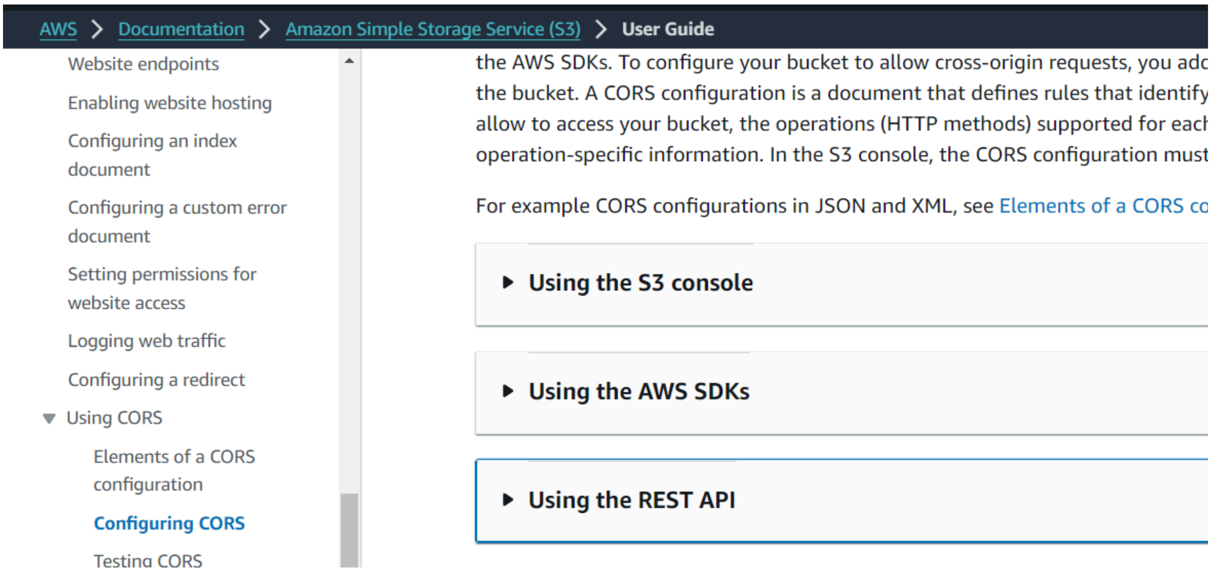
What is CORS and How To Enable IT in S3



Cross-origin resource sharing (CORS)

The CORS configuration, written in JSON, defines a way for client web applications that are loaded in one domain to interact with resources in a different domain. Learn more

No configurations to display



AWS > Documentation > Amazon Simple Storage Service (S3) > User Guide
Website endpoints
Enabling website hosting
Configuring an index document
Configuring a custom error document
Setting permissions for website access
Logging web traffic
Configuring a redirect
Using CORS
Elements of a CORS configuration
Configuring CORS
Testing CORS

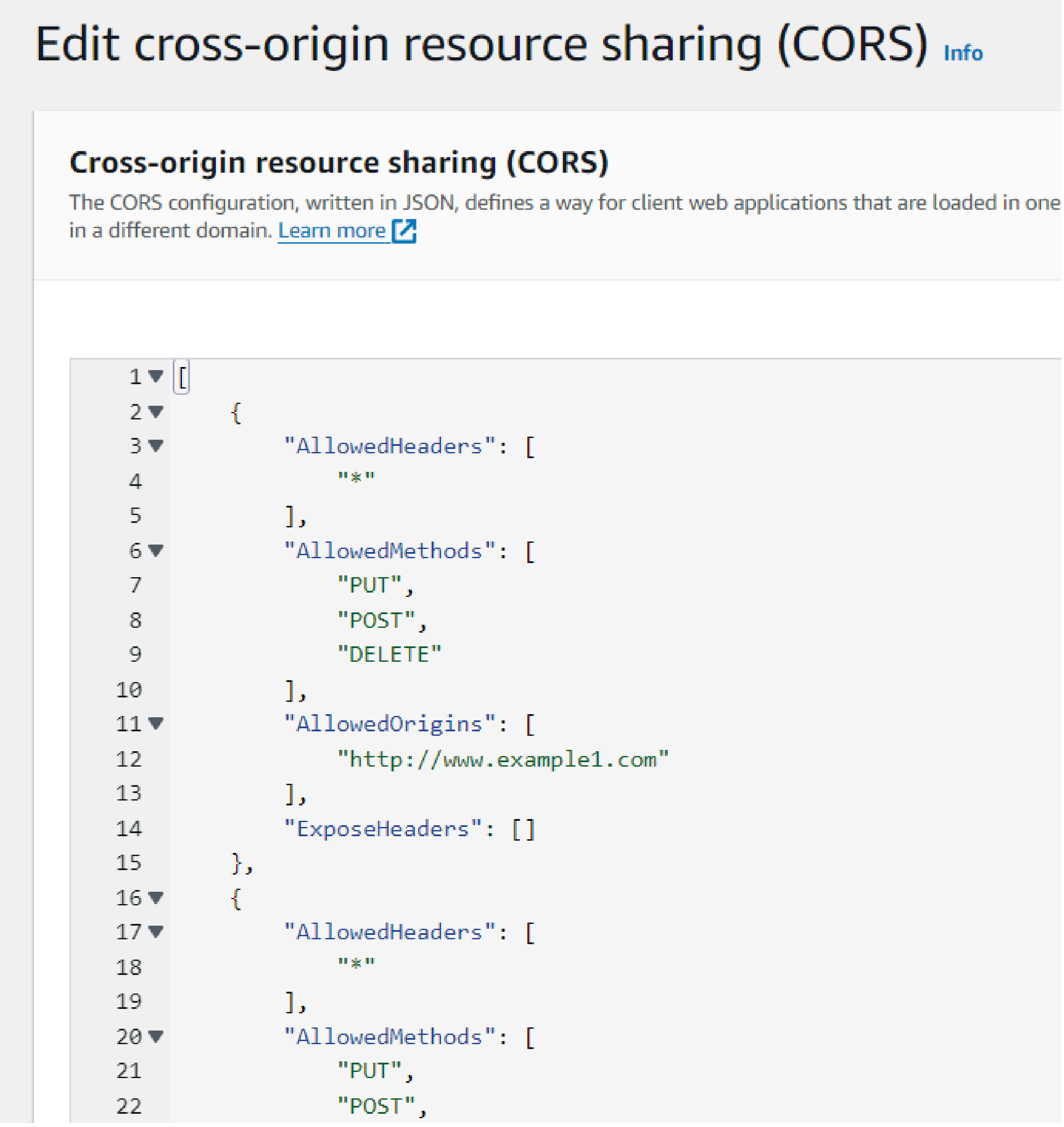
the AWS SDKs. To configure your bucket to allow cross-origin requests, you adc the bucket. A CORS configuration is a document that defines rules that identify allow to access your bucket, the operations (HTTP methods) supported for each operation-specific information. In the S3 console, the CORS configuration must

For example CORS configurations in JSON and XML, see Elements of a CORS co

▶ **Using the S3 console**

▶ **Using the AWS SDKs**

▶ **Using the REST API**



Edit cross-origin resource sharing (CORS)

Cross-origin resource sharing (CORS)

The CORS configuration, written in JSON, defines a way for client web applications that are loaded in one in a different domain. Learn more

```
[
    {
        "AllowedHeaders": [
            "*"
        ],
        "AllowedMethods": [
            "PUT",
            "POST",
            "DELETE"
        ],
        "AllowedOrigins": [
            "http://www.example1.com"
        ],
        "ExposeHeaders": []
    },
    {
        "AllowedHeaders": [
            "*"
        ],
        "AllowedMethods": [
            "PUT",
            "POST",
```

Encryption:
AWS Key Management Service (KMS) is a managed service that allows you to create, manage, and control encryption keys (KMS keys) to protect your data. KMS keys are used to encrypt data across various AWS services, including S3, RDS, and EBS.