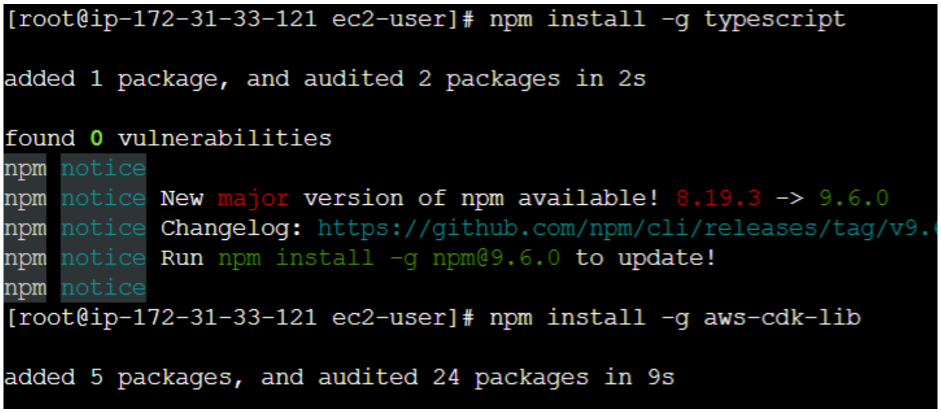
CDK

Statement

1. Setup the CDK environment on your machine and create a sample CDK Project.
2. Create a CDK code using TS to deploy an S3 Bucket with versioning, Encryption enabled (KMS) and Add Lifecycle rules for Infrequent Access transition after 30 days and Glacier after 90 Days.

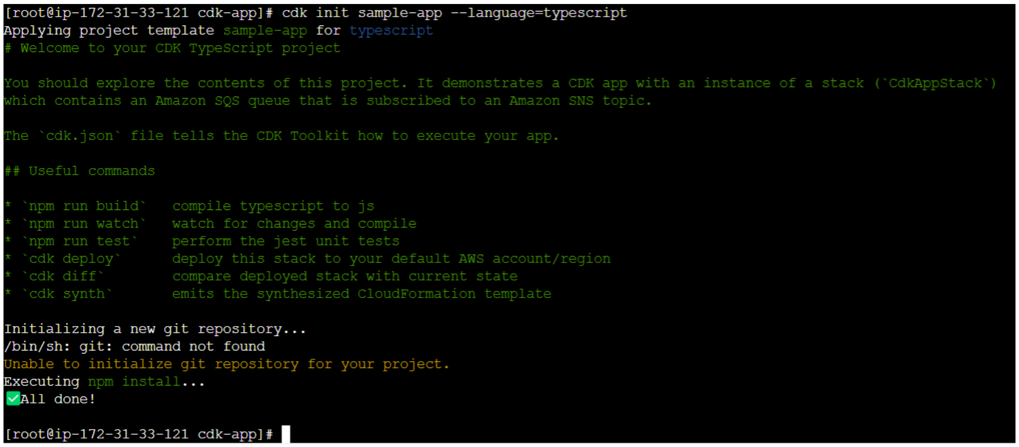
Solution

Configuring the typescript and CDK environment in my machine.



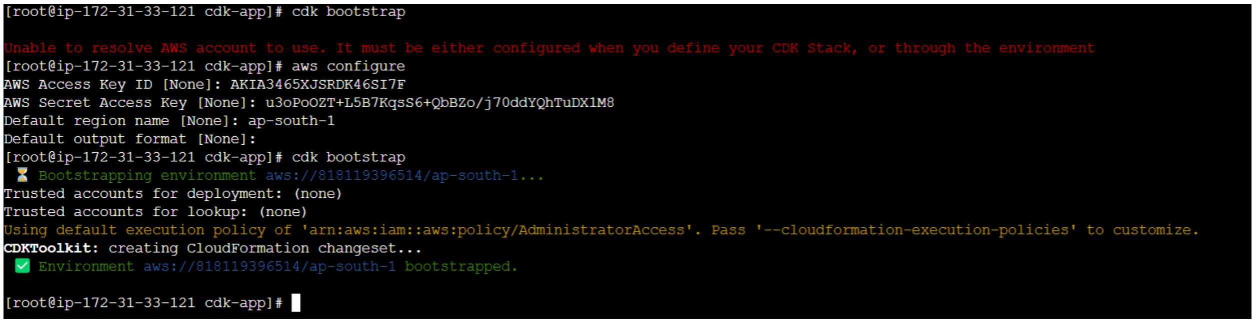
```
[root@ip-172-31-33-121 ec2-user]# npm install -g typescript

added 1 package, and audited 2 packages in 2s

found 0 vulnerabilities
npm notice
npm notice New major version of npm available! 8.19.3 -> 9.6.0
npm notice Changelog: https://github.com/npm/cli/releases/tag/v9.
npm notice Run npm install -g npm@9.6.0 to update!
npm notice
[root@ip-172-31-33-121 ec2-user]# npm install -g aws-cdk-lib

added 5 packages, and audited 24 packages in 9s
```

Initializing the a sample CDK application with the typescript language



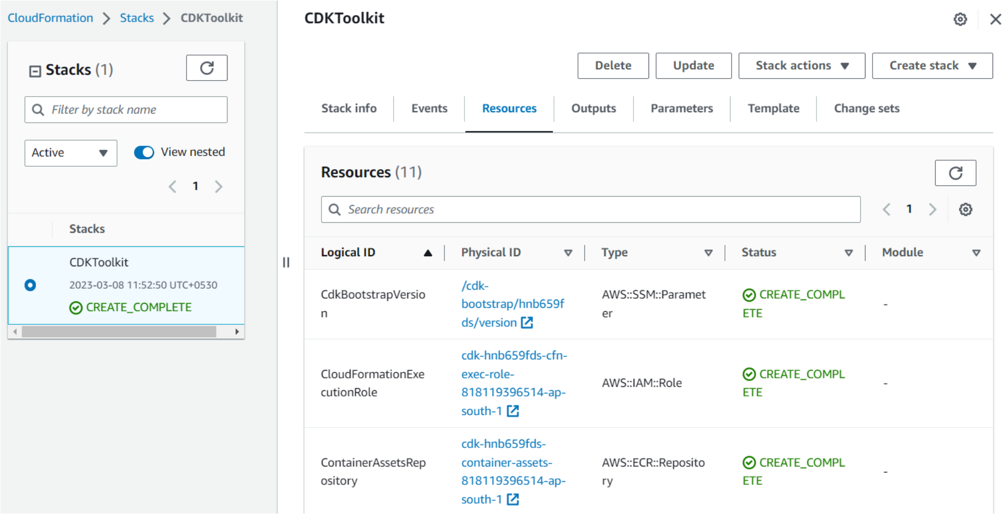
```
[root@ip-172-31-33-121 cdk-app]# cdk init sample-app --language=typescript
Applying project template sample-app for typescript
# Welcome to your CDK TypeScript project

You should explore the contents of this project. It demonstrates a CDK app with an instance of a stack (`CdkAppStack`)
which contains an Amazon SQS queue that is subscribed to an Amazon SNS topic.

The `cdk.json` file tells the CDK Toolkit how to execute your app.

## Useful commands

* `npm run build`   compile typescript to js
* `npm run watch`   watch for changes and compile
* `npm run test`    perform the jest unit tests
* `cdk deploy`      deploy this stack to your default AWS account/region
* `cdk diff`        compare deployed stack with current state
* `cdk synth`       emits the synthesized CloudFormation template

Initializing a new git repository...
/bin/sh: git: command not found
Unable to initialize git repository for your project.
Executing npm install...
✅All done!

[root@ip-172-31-33-121 cdk-app]# 
```

Running the bootstrap command to give the required permission to run the CDK in our account. It is one time setup per region.



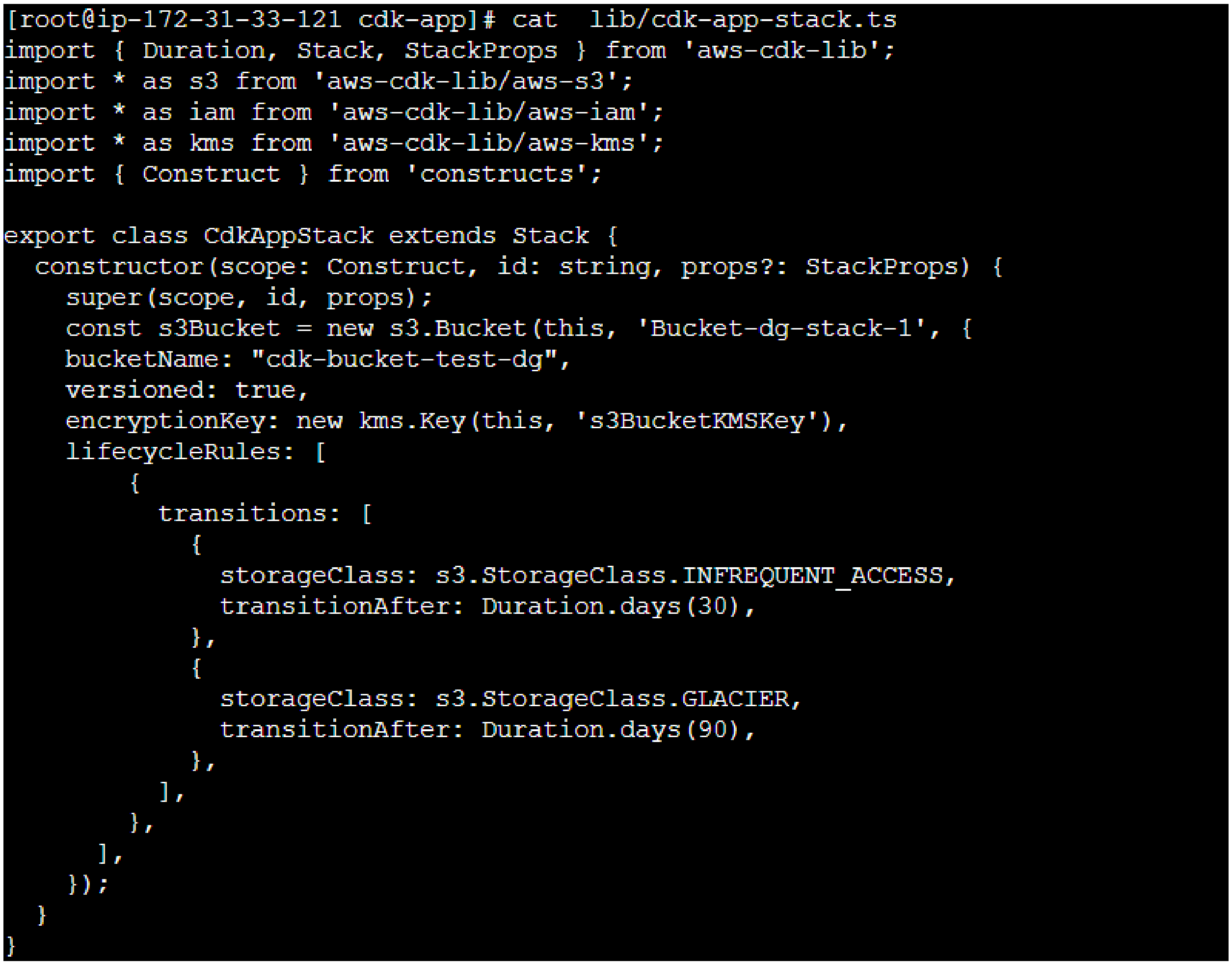
```
[root@ip-172-31-33-121 cdk-app]# cdk bootstrap

Unable to resolve AWS account to use. It must be either configured when you define your CDK Stack, or through the environment
[root@ip-172-31-33-121 cdk-app]# aws configure
AWS Access Key ID [None]: AKIA3465XJSRDK46SI7F
AWS Secret Access Key [None]: u3oPoOZT+L5B7KqsS6+QbBZo/j70ddYQhTuDX1M8
Default region name [None]: ap-south-1
Default output format [None]:
[root@ip-172-31-33-121 cdk-app]# cdk bootstrap
 ⏳ Bootstrapping environment aws://818119396514/ap-south-1...
Trusted accounts for deployment: (none)
Trusted accounts for lookup: (none)
Using default execution policy of 'arn:aws:iam::aws:policy/AdministratorAccess'. Pass '--cloudformation-execution-policies' to customize.
CDKToolkit: creating CloudFormation changeset...
 ✅ Environment aws://818119396514/ap-south-1 bootstrapped.

[root@ip-172-31-33-121 cdk-app]# 
```

That Bootstrap will create the required resources using the cloud formation stack.



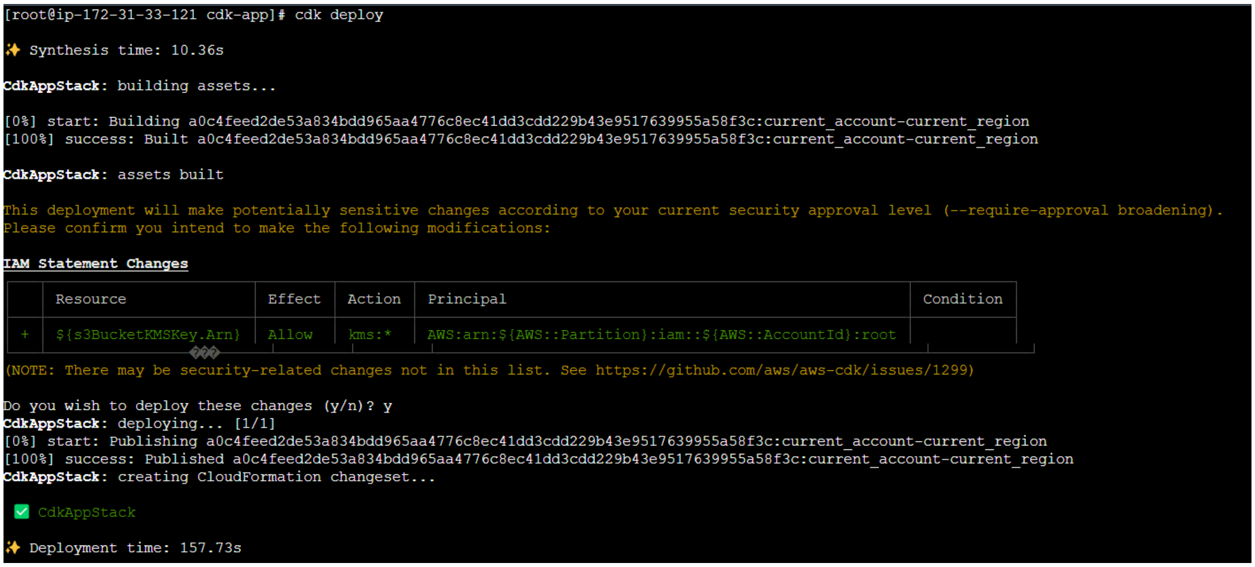
Logical ID	Physical ID	Type	Status	Module
CdkBootstrapVersion	/cdk-bootstrap/hnb659fds/version	AWS::SSM::Parameter	CREATE_COMPLETE	-
CloudFormationExecutionRole	cdk-hnb659fds-cfn-exec-role-818119396514-ap-south-1	AWS::IAM::Role	CREATE_COMPLETE	-
ContainerAssetsRepository	cdk-hnb659fds-container-assets-818119396514-ap-south-1	AWS::ECR::Repository	CREATE_COMPLETE	-

CDK code in typescript to create a bucket with the encryption, enabled the versioning and added a life cycle rule after uploading the object into the bucket after 30 days it will move to the Infrequent access and after 90 days it will move to the glacier.



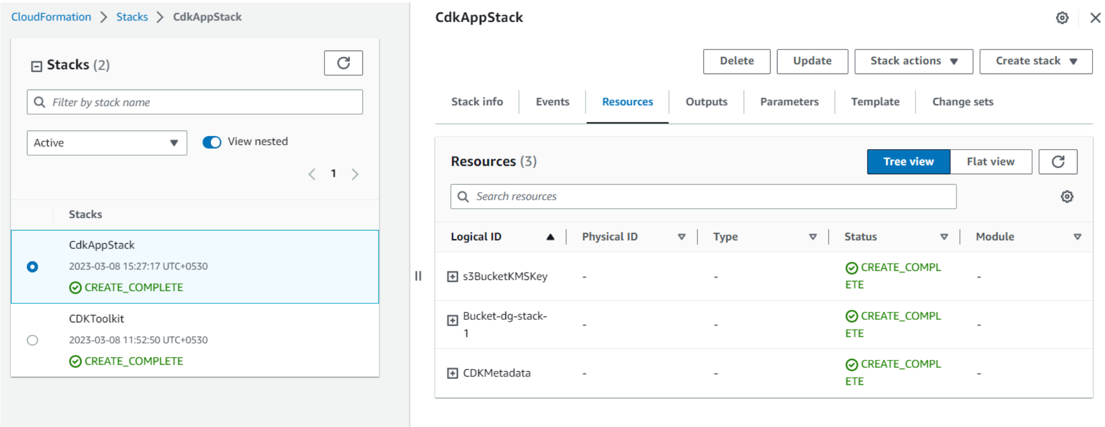
```
[root@ip-172-31-33-121 cdk-app]# cat  lib/cdk-app-stack.ts
import { Duration, Stack, StackProps } from 'aws-cdk-lib';
import * as s3 from 'aws-cdk-lib/aws-s3';
import * as iam from 'aws-cdk-lib/aws-iam';
import * as kms from 'aws-cdk-lib/aws-kms';
import { Construct } from 'constructs';

export class CdkAppStack extends Stack {
  constructor(scope: Construct, id: string, props?: StackProps) {
    super(scope, id, props);
    const s3Bucket = new s3.Bucket(this, 'Bucket-dg-stack-1', {
    bucketName: "cdk-bucket-test-dg",
    versioned: true,
    encryptionKey: new kms.Key(this, 's3BucketKMSKey'),
    lifecycleRules: [
        {
          transitions: [
            {
              storageClass: s3.StorageClass.INFREQUENT_ACCESS,
              transitionAfter: Duration.days(30),
            },
            {
              storageClass: s3.StorageClass.GLACIER,
              transitionAfter: Duration.days(90),
            },
          ],
        },
      ],
    });
  }
}
```

Deploying the stack



```
[root@ip-172-31-33-121 cdk-app]# cdk deploy

✨ Synthesis time: 10.36s

CdkAppStack: building assets...

[0%] start: Building a0c4feed2de53a834bdd965aa4776c8ec41dd3cdd229b43e9517639955a58f3c:current_account-current_region
[100%] success: Built a0c4feed2de53a834bdd965aa4776c8ec41dd3cdd229b43e9517639955a58f3c:current_account-current_region

CdkAppStack: assets built

This deployment will make potentially sensitive changes according to your current security approval level (--require-approval broadening).
Please confirm you intend to make the following modifications:

IAM Statement Changes
┌───┬────────────────────────┬────────┬────────┬──────────────────────────────────────────────────────┬───────────┐
│   │ Resource               │ Effect │ Action │ Principal                                            │ Condition │
├───┼────────────────────────┼────────┼────────┼──────────────────────────────────────────────────────┼───────────┤
│ + │ ${s3BucketKMSKey.Arn}  │ Allow  │ kms:*  │ AWS:arn:${AWS::Partition}:iam::${AWS::AccountId}:root │           │
└───┴────────────────────────┴────────┴────────┴──────────────────────────────────────────────────────┴───────────┘
(NOTE: There may be security-related changes not in this list. See https://github.com/aws/aws-cdk/issues/1299)

Do you wish to deploy these changes (y/n)? y
CdkAppStack: deploying... [1/1]
[0%] start: Publishing a0c4feed2de53a834bdd965aa4776c8ec41dd3cdd229b43e9517639955a58f3c:current_account-current_region
[100%] success: Published a0c4feed2de53a834bdd965aa4776c8ec41dd3cdd229b43e9517639955a58f3c:current_account-current_region
CdkAppStack: creating CloudFormation changeset...

 ✅ CdkAppStack

✨ Deployment time: 157.73s
```

Stack was created to provision the respective resources.



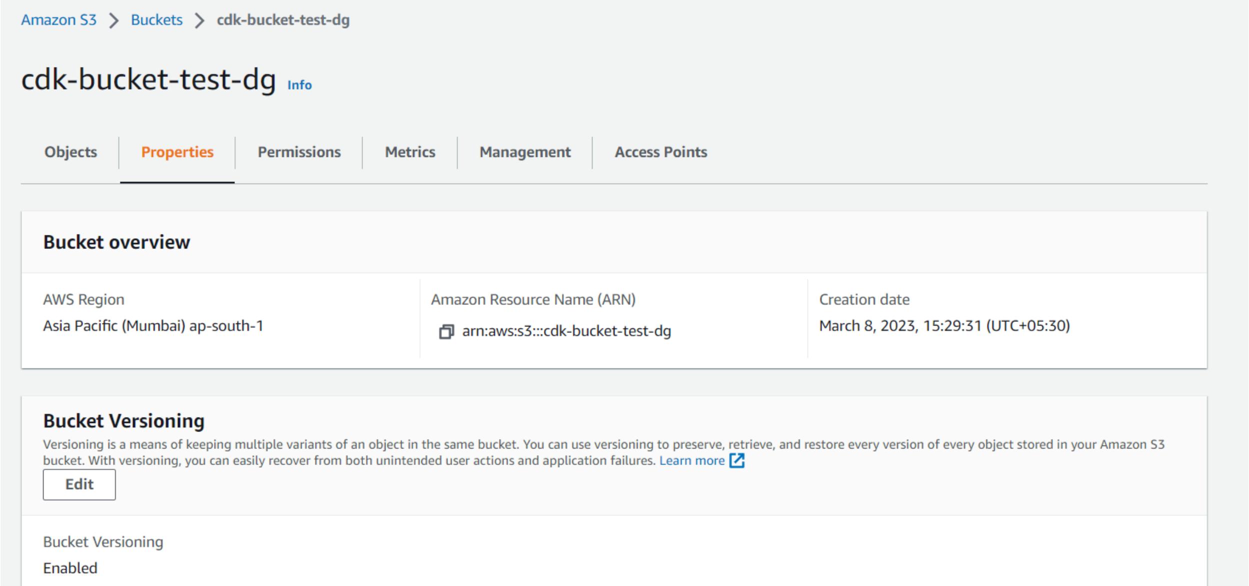
Stacks
● CdkAppStack 2023-03-08 15:27:17 UTC+0530 CREATE_COMPLETE
○ CDKToolkit 2023-03-08 11:52:50 UTC+0530 CREATE_COMPLETE

CdkAppStack

Resources (3)

Logical ID	Physical ID	Type	Status	Module
s3BucketKMSKey	-	-	CREATE_COMPLETE	-
Bucket-dg-stack-1	-	-	CREATE_COMPLETE	-
CDKMetadata	-	-	CREATE_COMPLETE	-

Following resources are provisioned with the CDK.



cdk-bucket-test-dg

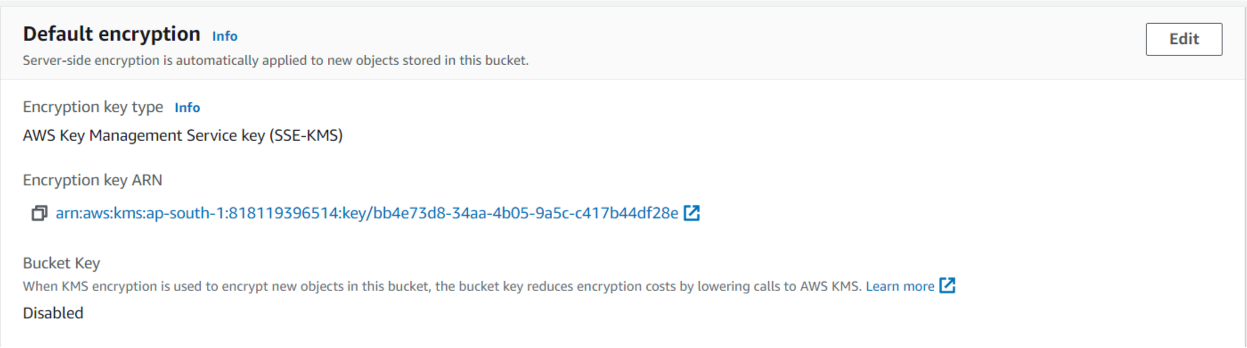
Bucket overview

AWS Region	Amazon Resource Name (ARN)	Creation date
Asia Pacific (Mumbai) ap-south-1	arn:aws:s3:::cdk-bucket-test-dg	March 8, 2023, 15:29:31 (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
Enabled



Default encryption

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption key type

AWS Key Management Service key (SSE-KMS)

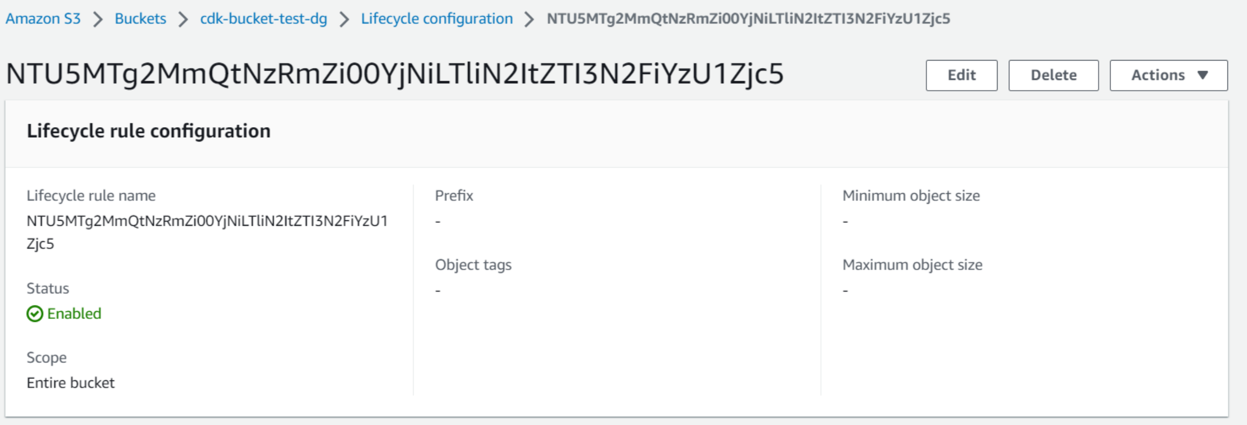
Encryption key ARN

arn:aws:kms:ap-south-1:818119396514:key/bb4e73d8-34aa-4b05-9a5c-c417b44df28e

Bucket Key

When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. Learn more

Disabled


Amazon S3 > Buckets > cdk-bucket-test-dg > Lifecycle configuration > NTU5MTg2MmQtNzRmZi00YjNiLTliN2ItZTI3N2FiYzU1Zjc5
Edit
Delete
Actions ▼

NTU5MTg2MmQtNzRmZi00YjNiLTliN2ItZTI3N2FiYzU1Zjc5

Lifecycle rule configuration

Lifecycle rule name

NTU5MTg2MmQtNzRmZi00YjNiLTliN2ItZTI3N2FiYzU1Zjc5

Status

✓ Enabled

Scope

Entire bucket

Prefix

-

Object tags

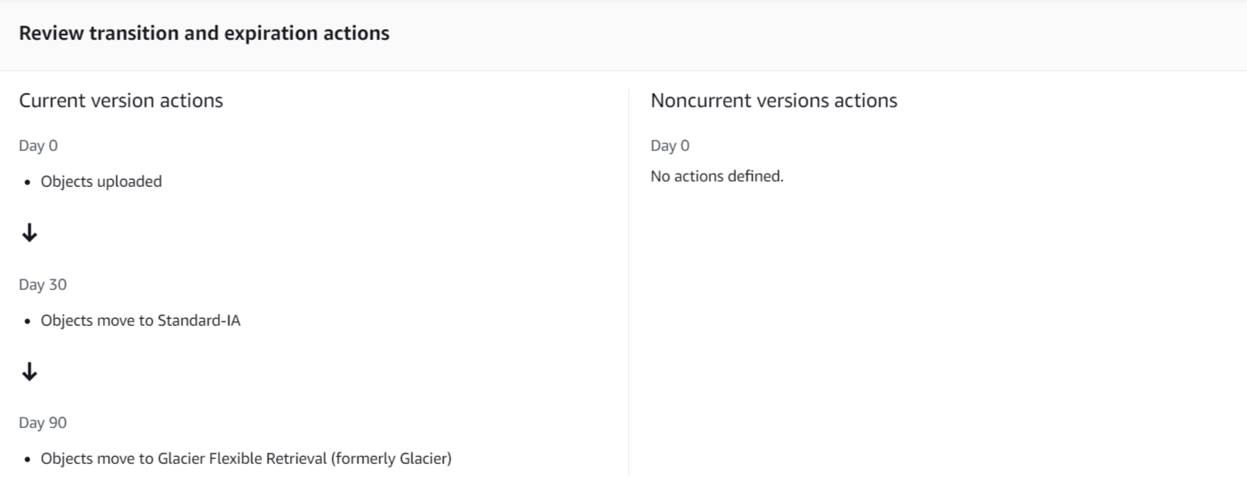
-

Minimum object size

-

Maximum object size

-



Review transition and expiration actions

Current version actions

Day 0

- Objects uploaded

↓

Day 30

- Objects move to Standard-IA

↓

Day 90

- Objects move to Glacier Flexible Retrieval (formerly Glacier)

Noncurrent versions actions

Day 0

No actions defined.