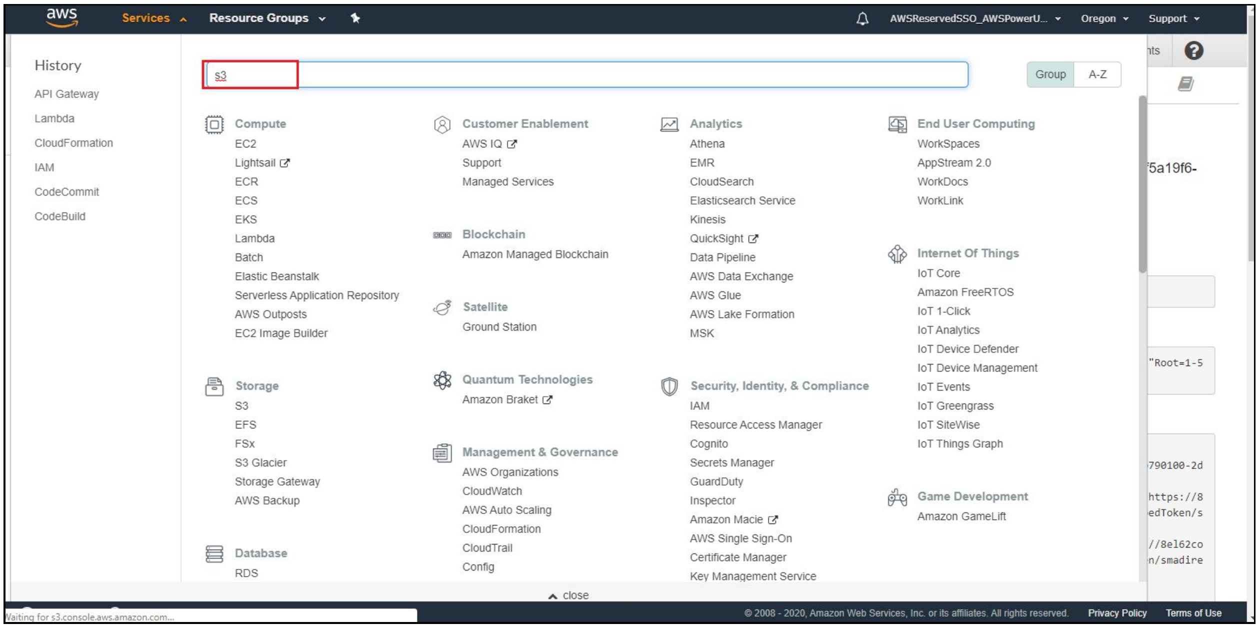
Simple Storage Service (S3)

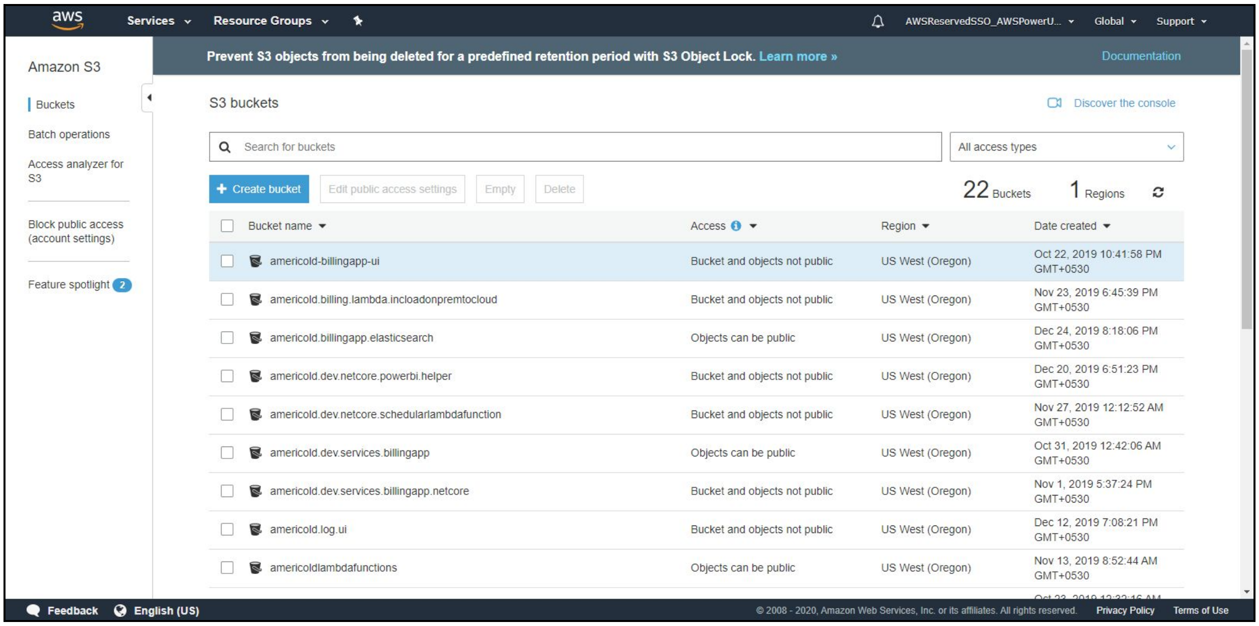
Objective:

The objective of this document is to provide an overview of creation and configuration of an S3 bucket.

In order to create an S3 bucket first we need to login into the AWS console and search for **S3** service.

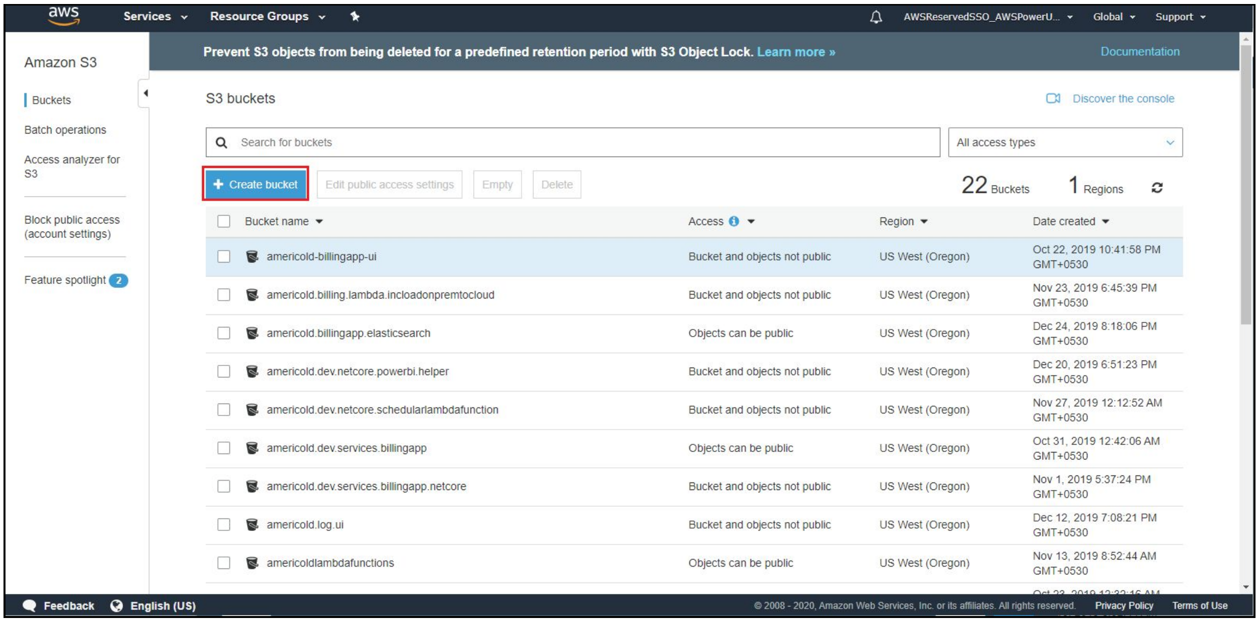


Now the dashboard of the S3 bucket will be as shown below.



Bucket name	Access	Region	Date created
americold-billingapp-ui	Bucket and objects not public	US West (Oregon)	Oct 22, 2019 10:41:58 PM GMT+0530
americold.billing.lambda.incloadonpremtocloud	Bucket and objects not public	US West (Oregon)	Nov 23, 2019 6:45:39 PM GMT+0530
americold.billingapp.elasticsearch	Objects can be public	US West (Oregon)	Dec 24, 2019 8:18:06 PM GMT+0530
americold.dev.netcore.powerbi.helper	Bucket and objects not public	US West (Oregon)	Dec 20, 2019 6:51:23 PM GMT+0530
americold.dev.netcore.schedularlambdafunction	Bucket and objects not public	US West (Oregon)	Nov 27, 2019 12:12:52 AM GMT+0530
americold.dev.services.billingapp	Objects can be public	US West (Oregon)	Oct 31, 2019 12:42:06 AM GMT+0530
americold.dev.services.billingapp.netcore	Bucket and objects not public	US West (Oregon)	Nov 1, 2019 5:37:24 PM GMT+0530
americold.log.ui	Bucket and objects not public	US West (Oregon)	Dec 12, 2019 7:08:21 PM GMT+0530
americoldlambdafunctions	Objects can be public	US West (Oregon)	Nov 13, 2019 8:52:44 AM GMT+0530

Now Click on **create bucke**t to create a new bucket.



Prevent S3 objects from being deleted for a predefined retention period with S3 Object Lock. Learn more »

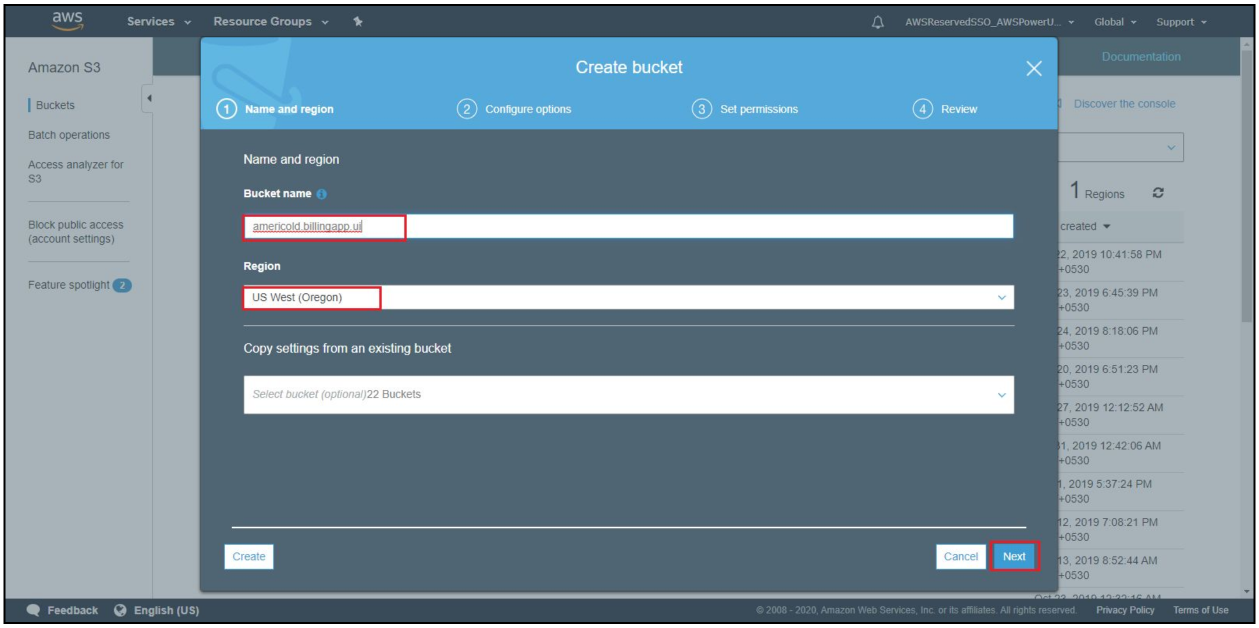
S3 buckets

Search for buckets

22 Buckets 1 Regions

Bucket name	Access	Region	Date created
americold-billingapp-ui	Bucket and objects not public	US West (Oregon)	Oct 22, 2019 10:41:58 PM GMT+0530
americold.billing.lambda.incloadonpremtocloud	Bucket and objects not public	US West (Oregon)	Nov 23, 2019 6:45:39 PM GMT+0530
americold.billingapp.elasticsearch	Objects can be public	US West (Oregon)	Dec 24, 2019 8:18:06 PM GMT+0530
americold.dev.netcore.powerbi.helper	Bucket and objects not public	US West (Oregon)	Dec 20, 2019 6:51:23 PM GMT+0530
americold.dev.netcore.schedularlambdafunction	Bucket and objects not public	US West (Oregon)	Nov 27, 2019 12:12:52 AM GMT+0530
americold.dev.services.billingapp	Objects can be public	US West (Oregon)	Oct 31, 2019 12:42:06 AM GMT+0530
americold.dev.services.billingapp.netcore	Bucket and objects not public	US West (Oregon)	Nov 1, 2019 5:37:24 PM GMT+0530
americold.log.ui	Bucket and objects not public	US West (Oregon)	Dec 12, 2019 7:08:21 PM GMT+0530
americoldlambdafunctions	Objects can be public	US West (Oregon)	Nov 13, 2019 8:52:44 AM GMT+0530

Now give a name to S3 bucket that should be unique for all S3 buckets in AWS, select a region to create S3 bucket in that specified region and click on next to setup the configuration for S3 bucket. Here we have given the name as **americold-billingapp-ui** and selected region as US West - 2 (Oregon)



Name and region

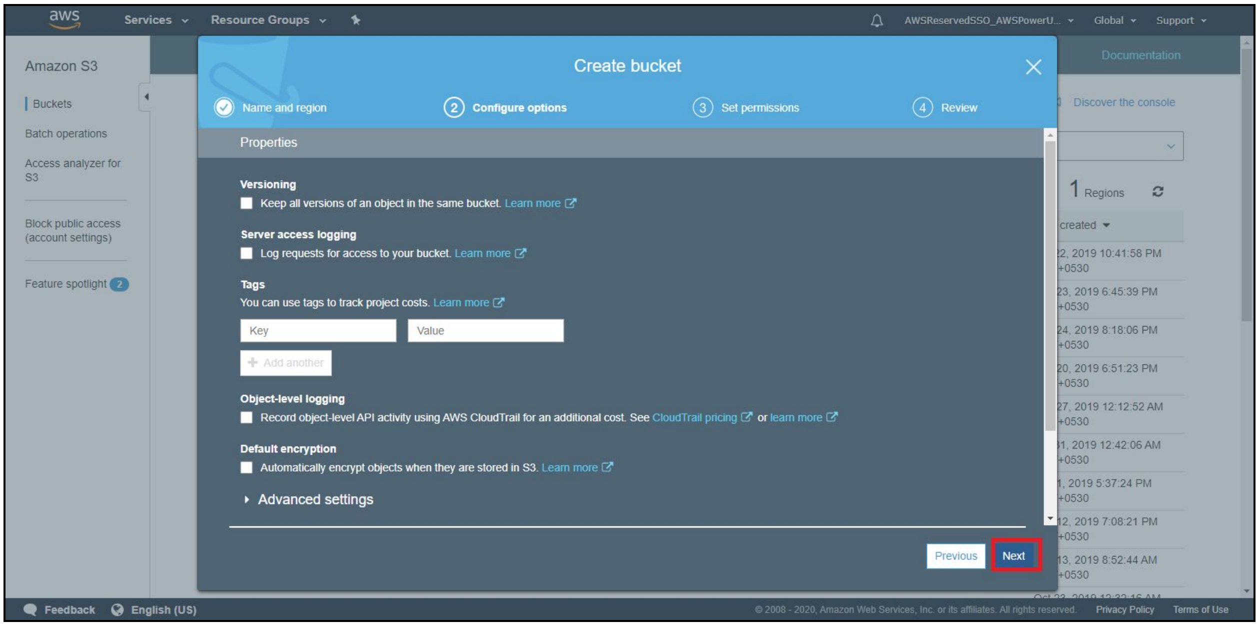
Bucket name: americold.billingapp.ui

Region: US West (Oregon)

Copy settings from an existing bucket

Select bucket (optional)22 Buckets

Here we have given the default configuration and click on **next** to set the permissions.



Create bucket

✓ Name and region ② Configure options ③ Set permissions ④ Review

Properties

Versioning

□ Keep all versions of an object in the same bucket. Learn more

Server access logging

□ Log requests for access to your bucket. Learn more

Tags

You can use tags to track project costs. Learn more

Key | Value

+ Add another

Object-level logging

□ Record object-level API activity using AWS CloudTrail for an additional cost. See CloudTrail pricing or learn more

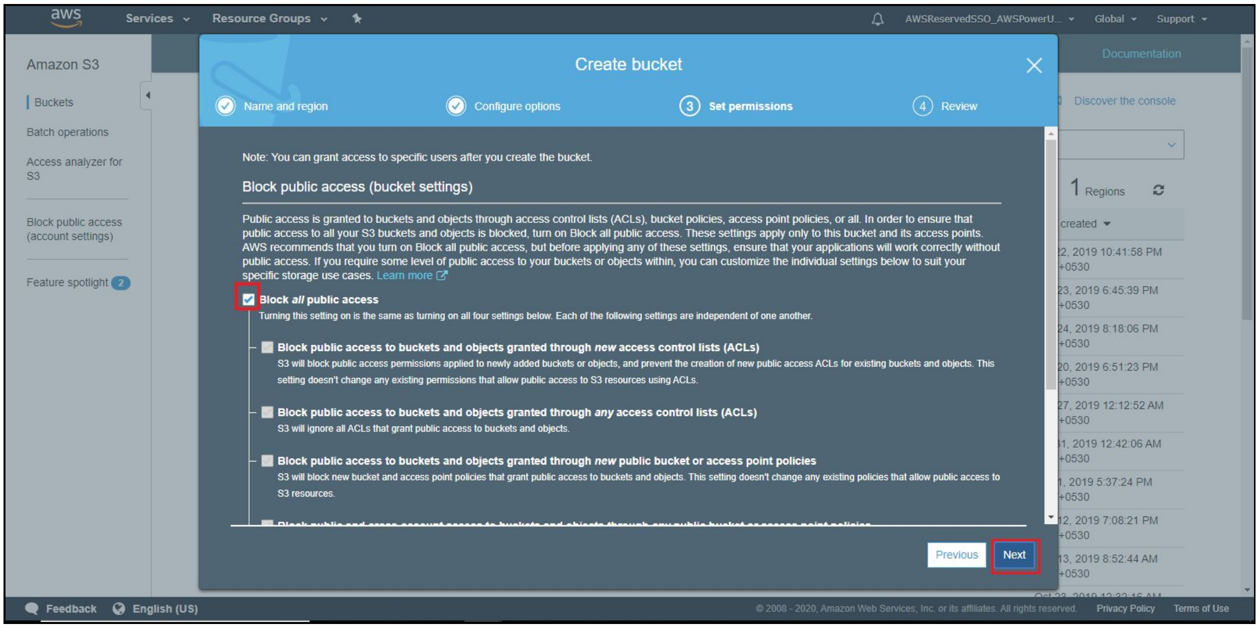
Default encryption

□ Automatically encrypt objects when they are stored in S3. Learn more

▸ Advanced settings

Previous Next

Now select the Block all public access check box to restrict the bucket access with in the AWS account and click on next.



Create bucket

✓ Name and region ✓ Configure options ③ Set permissions ④ Review

Note: You can grant access to specific users after you create the bucket.

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

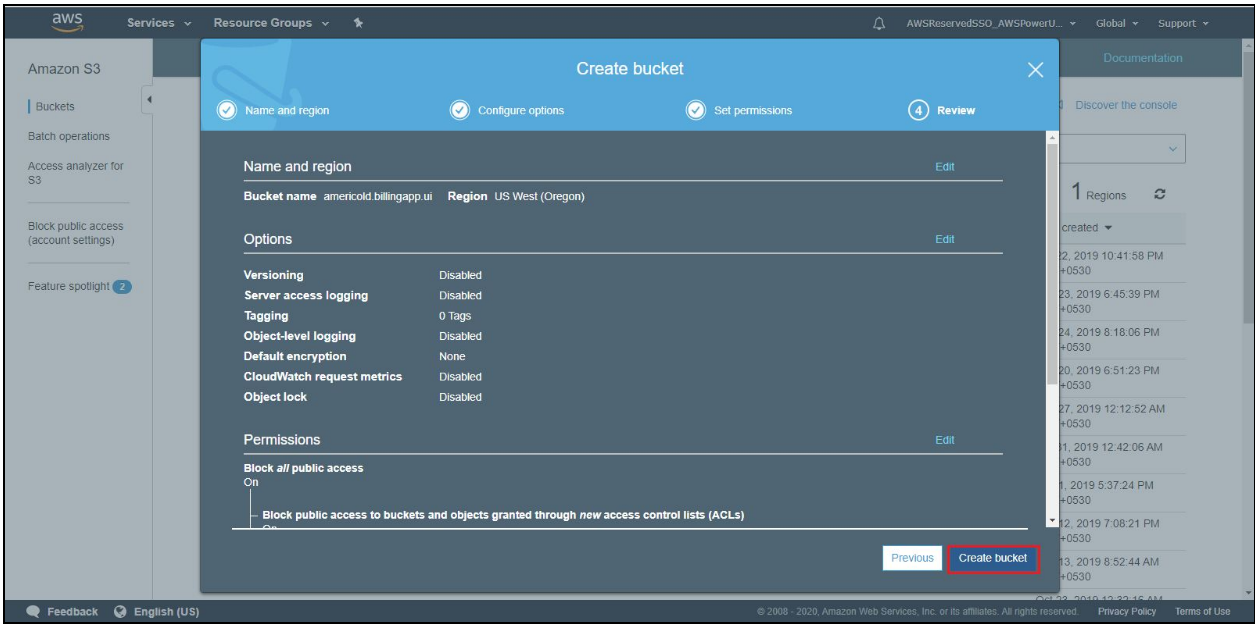
☑ **Block *all* public access**

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.

Previous Next

Now review the bucket configuration and click on **create bucket**.



Name and region

Bucket name americold.billingapp.ui **Region** US West (Oregon)

Options

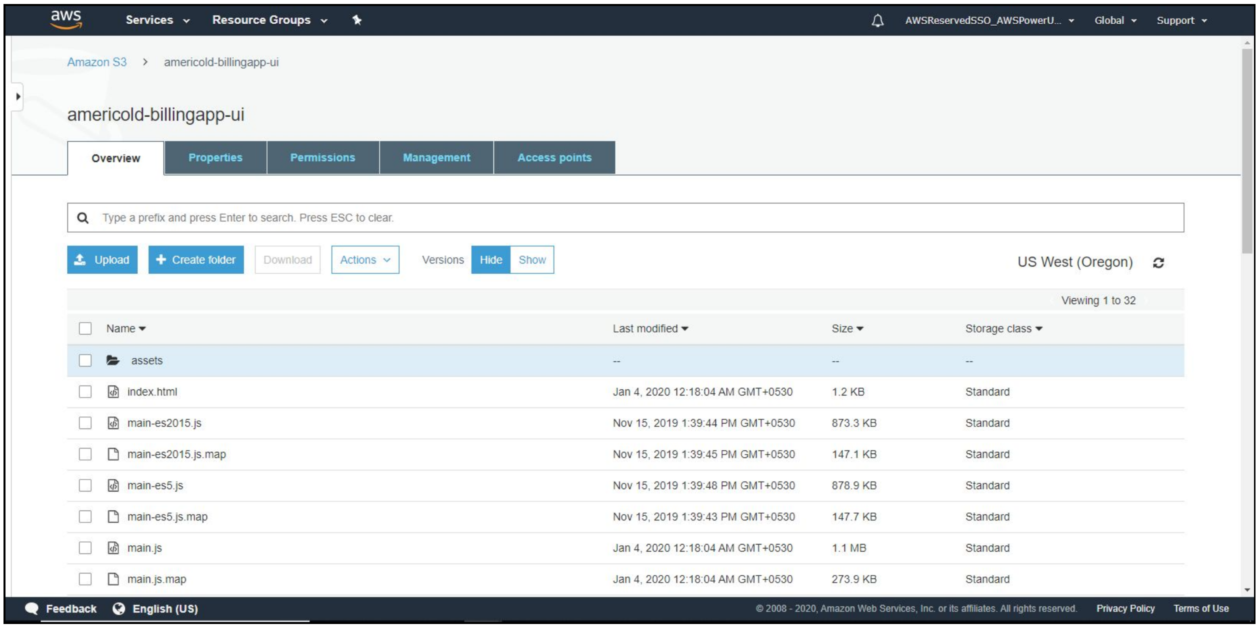
Versioning	Disabled
Server access logging	Disabled
Tagging	0 Tags
Object-level logging	Disabled
Default encryption	None
CloudWatch request metrics	Disabled
Object lock	Disabled

Permissions

Block *all* public access
On

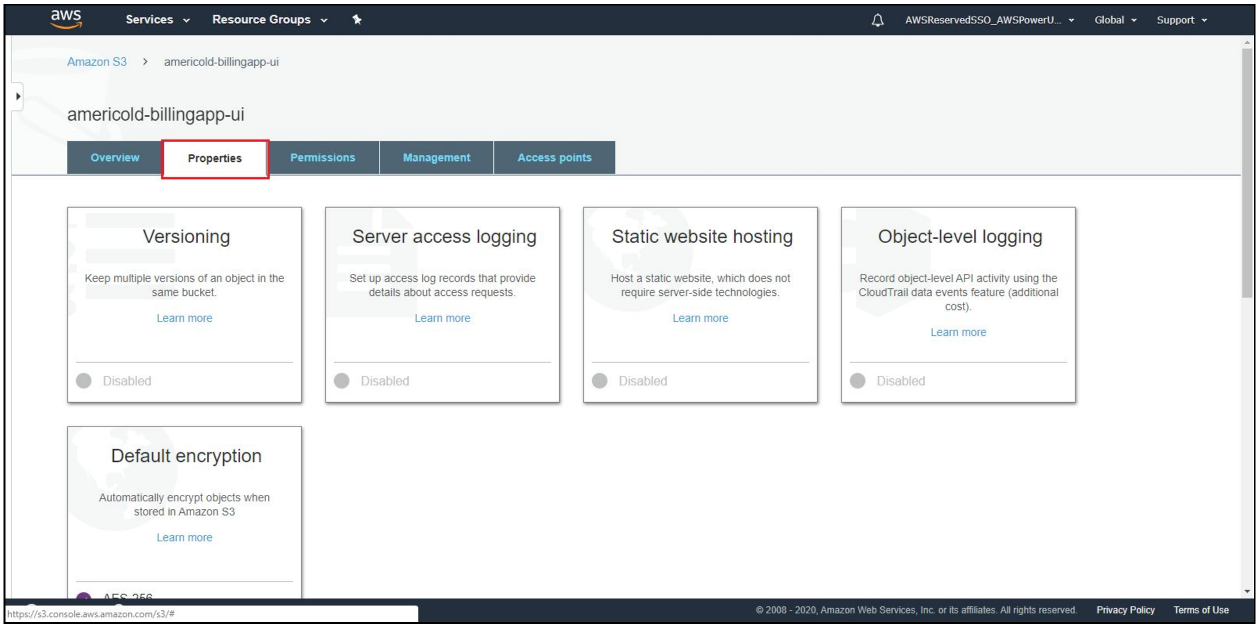
Block public access to buckets and objects granted through *new* access control lists (ACLs)

Now the bucket is created and the artifacts stored in the bucket as follows.



Name	Last modified	Size	Storage class
assets	--	--	--
index.html	Jan 4, 2020 12:18:04 AM GMT+0530	1.2 KB	Standard
main-es2015.js	Nov 15, 2019 1:39:44 PM GMT+0530	873.3 KB	Standard
main-es2015.js.map	Nov 15, 2019 1:39:45 PM GMT+0530	147.1 KB	Standard
main-es5.js	Nov 15, 2019 1:39:48 PM GMT+0530	878.9 KB	Standard
main-es5.js.map	Nov 15, 2019 1:39:43 PM GMT+0530	147.7 KB	Standard
main.js	Jan 4, 2020 12:18:04 AM GMT+0530	1.1 MB	Standard
main.js.map	Jan 4, 2020 12:18:04 AM GMT+0530	273.9 KB	Standard

Now click on the **Properties** of the bucket.



Versioning: Keep multiple versions of an object in the same bucket. — Disabled

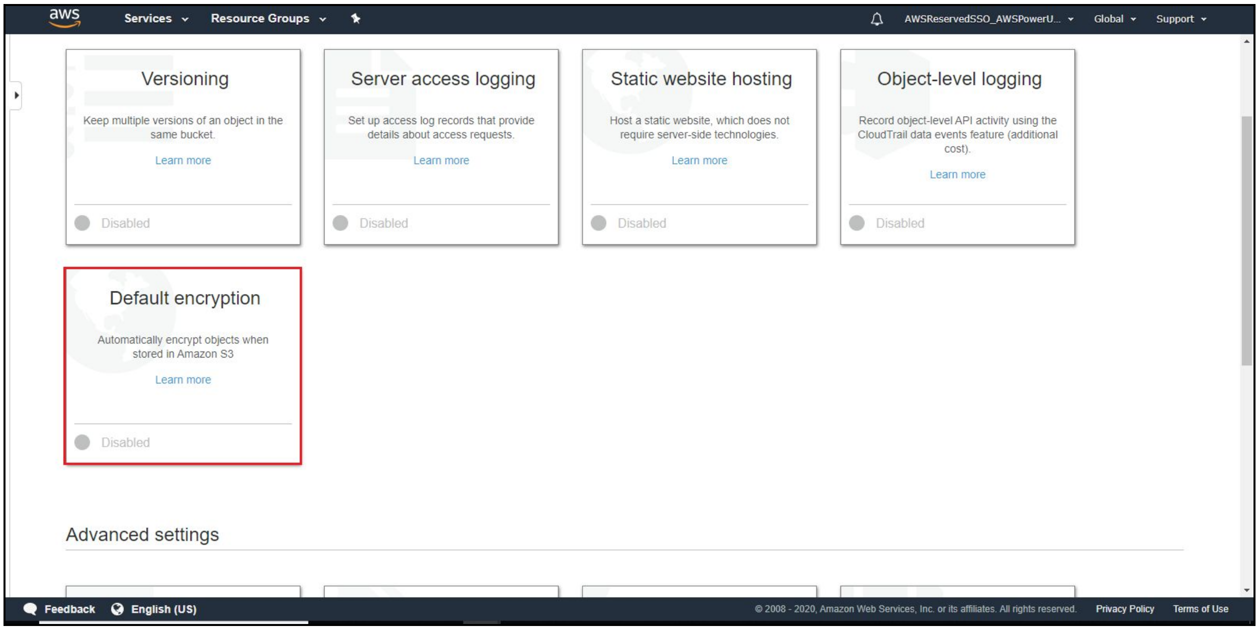
Server access logging: Set up access log records that provide details about access requests. — Disabled

Static website hosting: Host a static website, which does not require server-side technologies. — Disabled

Object-level logging: Record object-level API activity using the CloudTrail data events feature (additional cost). — Disabled

Default encryption: Automatically encrypt objects when stored in Amazon S3

Now click on **default encryption** to enable the encryption for the data in S3 bucket.



Versioning: Keep multiple versions of an object in the same bucket. — Disabled

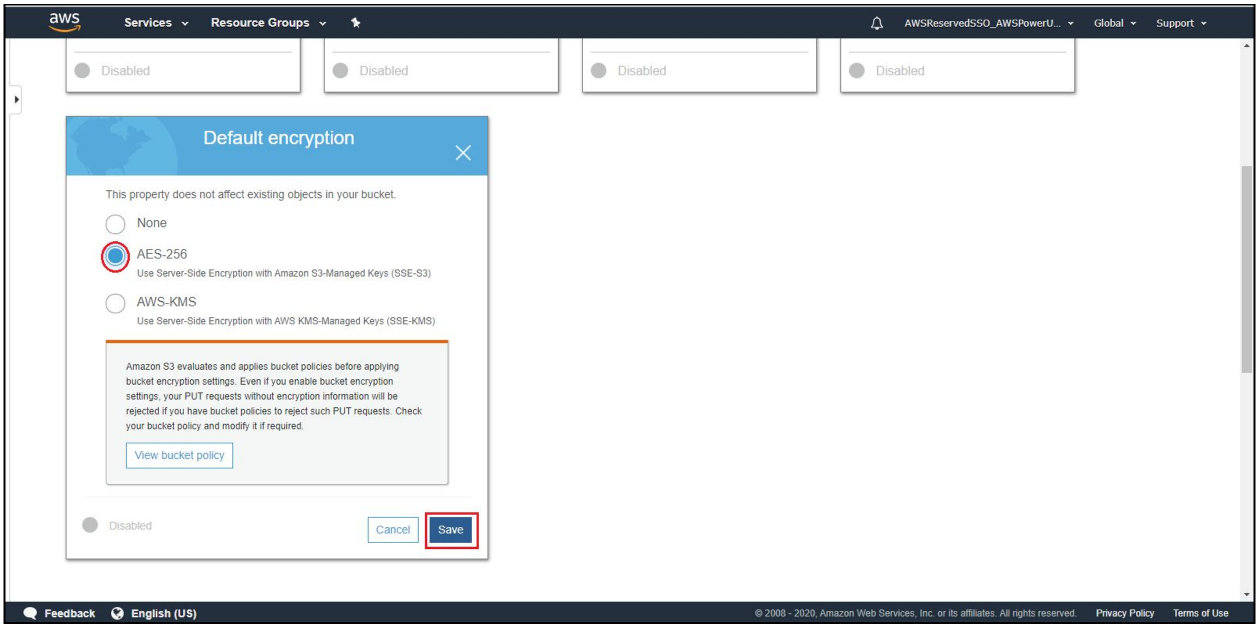
Server access logging: Set up access log records that provide details about access requests. — Disabled

Static website hosting: Host a static website, which does not require server-side technologies. — Disabled

Object-level logging: Record object-level API activity using the CloudTrail data events feature (additional cost). — Disabled

Default encryption: Automatically encrypt objects when stored in Amazon S3 — Disabled

By default the encryption of the bucket will be disabled. Here we are encrypting the S3 bucket data using **AES-256** method for side encryption. Now select the AES-256 button and click on save.



Default encryption

This property does not affect existing objects in your bucket.

○ None

● AES-256
Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)

○ AWS-KMS
Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

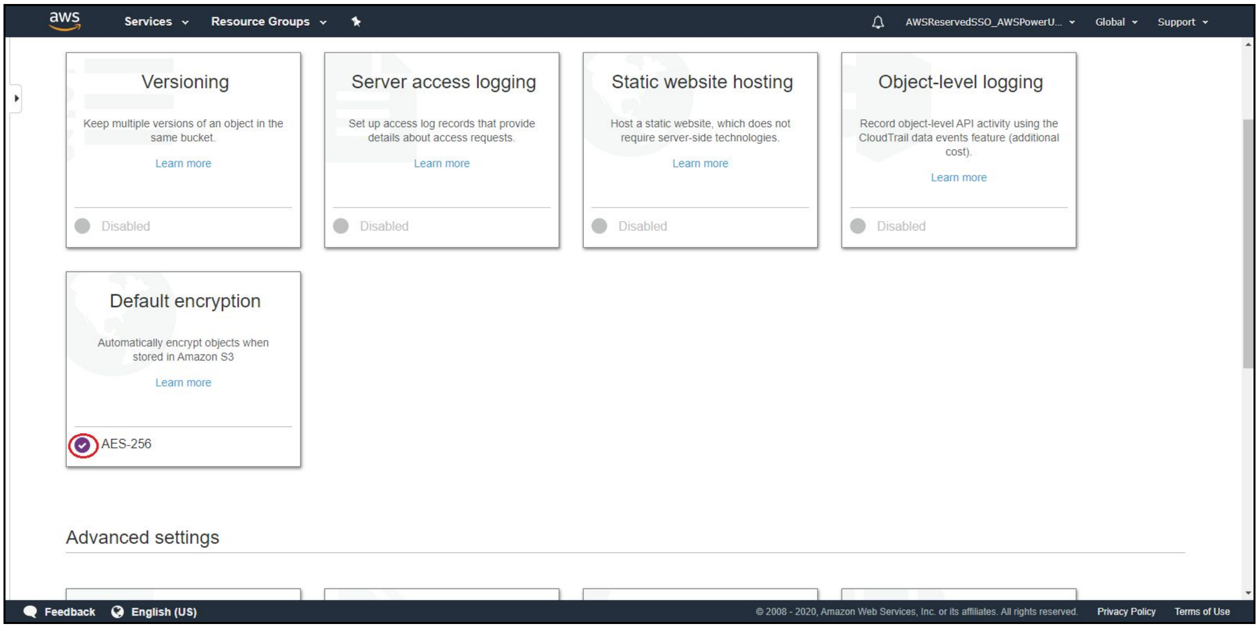
Amazon S3 evaluates and applies bucket policies before applying bucket encryption settings. Even if you enable bucket encryption settings, your PUT requests without encryption information will be rejected if you have bucket policies to reject such PUT requests. Check your bucket policy and modify it if required.

View bucket policy

Disabled

Cancel | Save

Now the data in S3 bucket will be encrypted.


aws
Services
Resource Groups
AWSReservedSSO_AWSPowerU...
Global
Support
Feedback
English (US)
© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

Versioning
Keep multiple versions of an object in the same bucket.
Learn more
Disabled

Server access logging
Set up access log records that provide details about access requests.
Learn more
Disabled

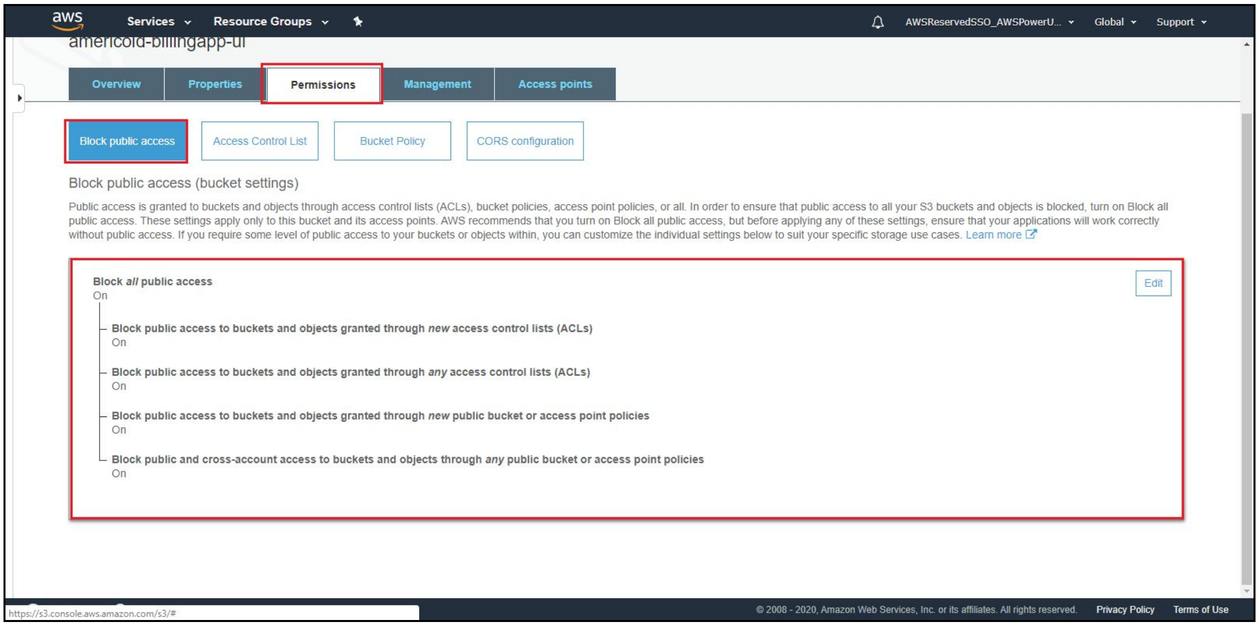
Static website hosting
Host a static website, which does not require server-side technologies.
Learn more
Disabled

Object-level logging
Record object-level API activity using the CloudTrail data events feature (additional cost).
Learn more
Disabled

Default encryption
Automatically encrypt objects when stored in Amazon S3
Learn more
✓ AES-256

Advanced settings

Now click on the **Permissions** tab to add or restrict the data in S3 bucket. Here we have restricted all the public access for the bucket.



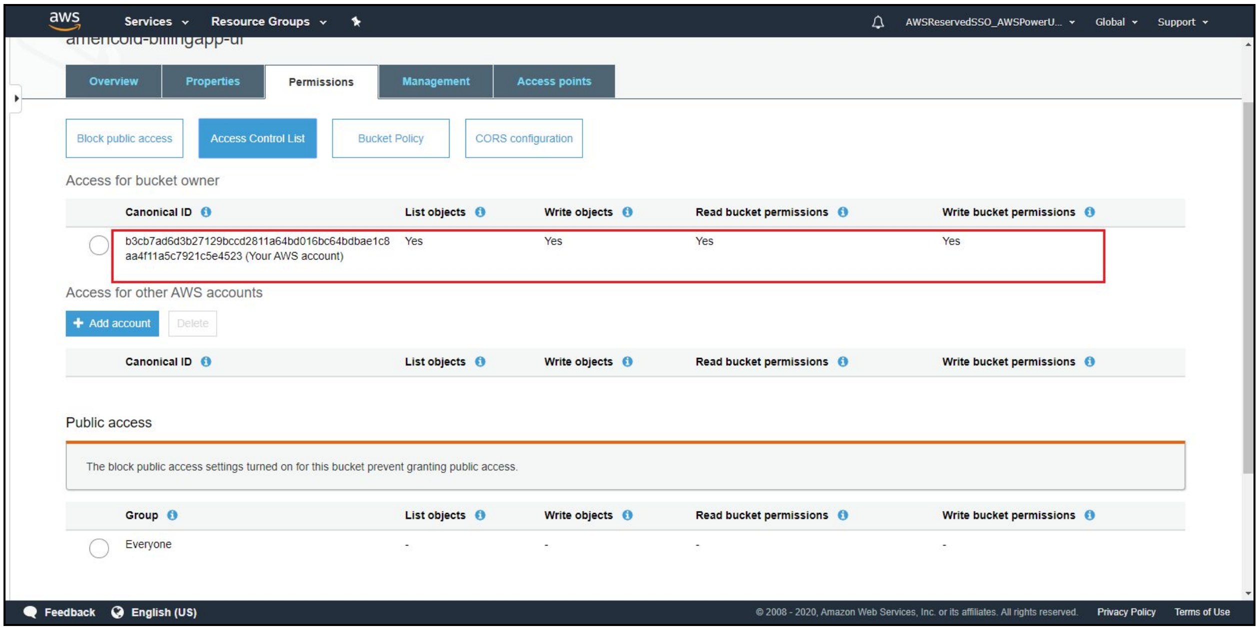
Block public access (bucket settings)

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

- Block public access to buckets and objects granted through *new* access control lists (ACLs)
  On
- Block public access to buckets and objects granted through *any* access control lists (ACLs)
  On
- Block public access to buckets and objects granted through *new* public bucket or access point policies
  On
- Block public and cross-account access to buckets and objects through *any* public bucket or access point policies
  On

In Access Control List to check who are currently accessing the S3 bucket. Here **Canonical ID** is a **unique id** for an **AWS** account. You can't use this to give a single IAM user permissions on a bucket. If needed we can add the other AWS accounts to access the bucket data (cross account access).



Access for bucket owner

	Canonical ID	List objects	Write objects	Read bucket permissions	Write bucket permissions
○	b3cb7ad6d3b27129bccd2811a64bd016bc64bdbae1c8 aa4f11a5c7921c5e4523 (Your AWS account)	Yes	Yes	Yes	Yes

Access for other AWS accounts

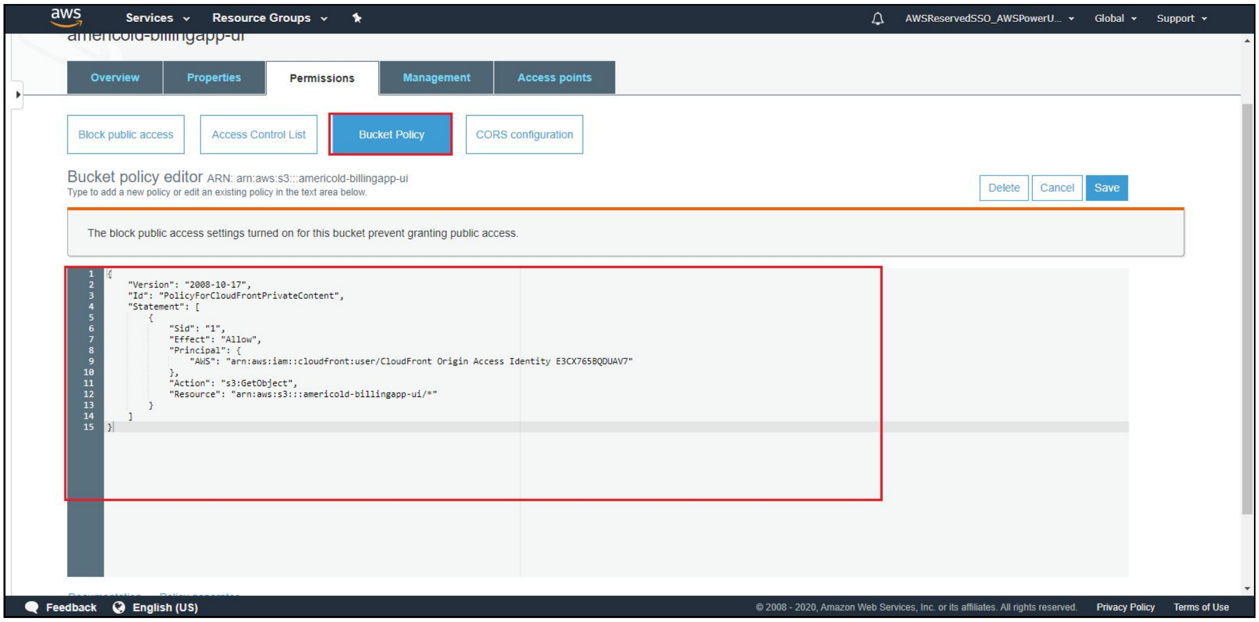
	Canonical ID	List objects	Write objects	Read bucket permissions	Write bucket permissions

Public access

The block public access settings turned on for this bucket prevent granting public access.

	Group	List objects	Write objects	Read bucket permissions	Write bucket permissions
○	Everyone	-	-	-	-

Now goto the **Bucket Policy** tab to check how we are accessing the data in the S3 bucket. Here we have updated the bucket policy from cloudfront service to access the data only through the respective cloudfront distribution.

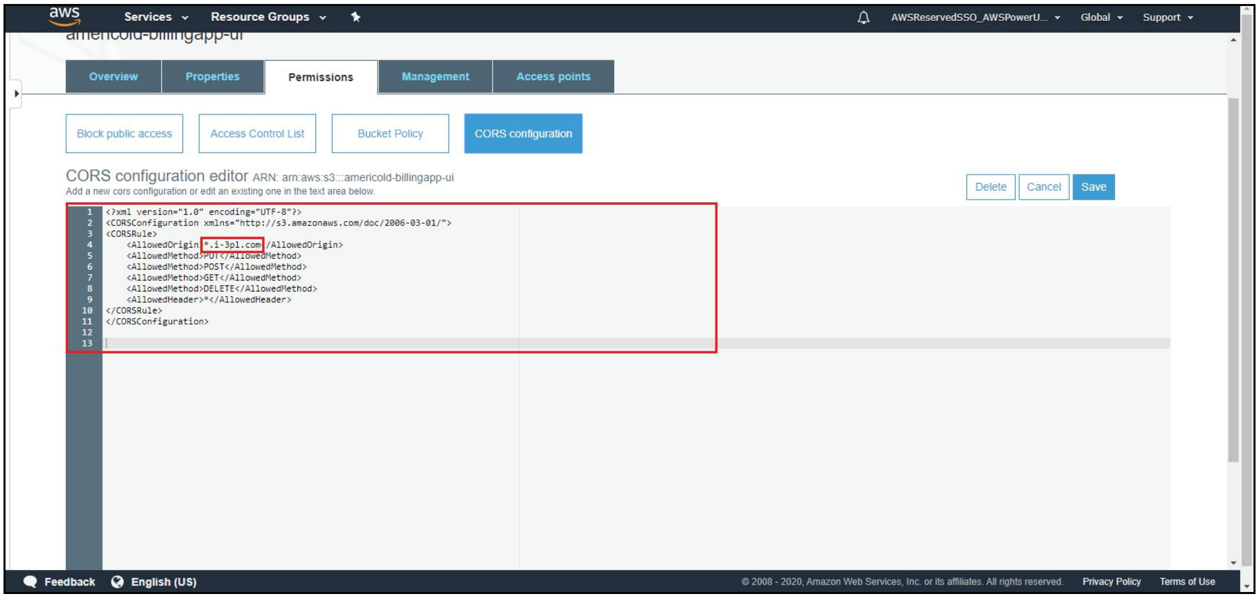


Bucket policy editor ARN: arn:aws:s3:::americold-billingapp-ui
Type to add a new policy or edit an existing policy in the text area below.

The block public access settings turned on for this bucket prevent granting public access.

```
{
    "Version": "2008-10-17",
    "Id": "PolicyForCloudFrontPrivateContent",
    "Statement": [
        {
            "Sid": "1",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access Identity E3CX765BQDUAV7"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::americold-billingapp-ui/*"
        }
    ]
}
```

Now goto **CORS configuration** tab to check the policies of the S3 bucket for CORS. Here we have added the allowed methods to the bucket, it will define the operations that can allowed by an origin. In the below configuration we have added the allowed origin as ***.i-3pl.com** defines that the operation will be done only if the requests to bucket coming to the specified domain. It allows us to restrict the cross origin access.



CORS configuration editor ARN: arn:aws:s3:::americold-billingapp-ui
Add a new cors configuration or edit an existing one in the text area below.

```
<?xml version="1.0" encoding="UTF-8"?>
<CORSConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
<CORSRule>
    <AllowedOrigin>*.i-3pl.com</AllowedOrigin>
    <AllowedMethod>PUT</AllowedMethod>
    <AllowedMethod>POST</AllowedMethod>
    <AllowedMethod>GET</AllowedMethod>
    <AllowedMethod>DELETE</AllowedMethod>
    <AllowedHeader>*</AllowedHeader>
</CORSRule>
</CORSConfiguration>
```