

Securing Data in AWS S3 Buckets



Hello!

I am Bryce Cox

My passion lies at the intersection
of cybersecurity and cloud
computing.

You can find me at:

<https://github.com/brycecox11>



The Objective

Securely configure AWS S3 buckets by applying encryption, access controls, and policy best practices.



Roadmap

Create an S3 Bucket

1

Enable Server-Side
Encryption

3

Configure S3 Access
Logs

5

Enable Bucket
Versioning

2

Set Bucket Policies

4

Step 1: Create an S3 Bucket

- ⬡ We are going to create an S3 bucket for our future information to be stored and encrypted.
- ⬡ This bucket will be named bryce-secure-bucket.
- ⬡ S3 is versatile works with Lambda, CloudTrail, Athena, Redshift, and more.

Create bucket Info

Buckets are containers for data stored in S3.

General configuration

AWS Region

US East (N. Virginia) us-east-1

Bucket type Info

☒ General purpose

Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

☐ Directory

Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name Info

bryce-secure-bucket

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). [Learn More](#)

Copy settings from existing bucket - optional

Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Format: s3://bucket/prefix

► Account snapshot - *updated every 24 hours* All AWS Regions

[View Storage Lens dashboard](#)

Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. [Learn more](#)

General purpose buckets

Directory buckets

General purpose buckets (1/1) Info All AWS Regions



[Copy ARN](#)

[Empty](#)

[Delete](#)

[Create bucket](#)

Buckets are containers for data stored in S3.

< 1 >

Name	AWS Region	IAM Access Analyzer	Creation date
bryce-secure-bucket	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 11, 2025, 15:53:57 (UTC-04:00)

Step 2: Enable Bucket Versioning

- ⬡ We are going to enable bucket version in the “Properties” tab.
- ⬡ Enabling bucket versioning in Amazon S3 helps you protect and preserve your data.
- ⬡ Every time you upload a file with the same name, S3 saves a new version, instead of overwriting it.

Edit Bucket Versioning Info

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

Cancel

Save changes

Step 3: Enable Server-Side Encryption

- ⬡ We are going to enable encryption in the “Properties” tab.
- ⬡ We are going to change the default encryption to server-side encryption with AWS KMS.
- ⬡ We are also going to create a symmetric key for this bucket.

Step 1

● Configure key

Step 2

● Add labels

Step 3 - optional

● Define key administrative permissions

Step 4 - optional

● Define key usage permissions

Step 5 - optional

● Edit key policy

Step 6

● Review

Review

Key configuration

Key type
Symmetric

Key spec
SYMMETRIC_DEFAULT

Key usage
Encrypt and decrypt

Origin
AWS KMS

Regionality
Single-Region key

Edit

ⓘ You cannot change the key configuration after the key is created.

Alias and description

Alias
s3-secure-bucket-key

Description
Key for secure bucket.


Edit

Step 4: Set Bucket Policies


- ⬡ We are going to set a bucket policies in the “Permissions” tab.
- ⬡ Bucket policies are used to control access to an entire S3 bucket and its objects. They're written in JSON and define who can access what, and how.

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:::bryce-secure-bucket`

Policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Principal": {  
7         "AWS": "arn:aws:iam::123456789012:user/bucket-user"  
8       },  
9       "Action": "s3:GetObject",  
10      "Resource": "arn:aws:s3:::bryce-secure-bucket/*"  
11    }  
12  ]  
13 }
```

Step 5: Configure S3 Access Logs

- ⬡ We are going to configure our S3 access logs to go to our “my-log-bucket” by going to the “Properties” tab.
- ⬡ Storing server access logs in Amazon S3 is a best practice for security, monitoring, and compliance.

Edit server access logging [Info](#)

Server access logging

Log requests for access to your bucket. [Learn more](#)

Server access logging

- ☐ Disable
- ☒ 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 US East (N. Virginia) us-east-1 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://my-log-bucket

[Browse S3](#)

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

Destination Region

US East (N. Virginia) us-east-1

Destination bucket name

my-log-bucket

Destination prefix

-

Log object key format

- ☒ [DestinationPrefix][YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
- ☐ [DestinationPrefix][SourceAccountId]/[SourceRegion]/[SourceBucket]/[YYYY]/[MM]/[DD]/[YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
- To speed up analytics and query applications, use this format.

Log object key example

2025-07-01-10-12-56-[UniqueString]

[Cancel](#)

[Save changes](#)

Mission Complete!

We were able to securely configure AWS S3 buckets by applying encryption, access controls, and policy best practices.



Thanks!

Any questions?

You can find me at:

Github:

<https://github.com/brycecox11>

LinkedIn:

<https://www.linkedin.com/in/brycecox-559616219/>

Email: bcox8898@gmail.com



Credits

Special thanks to Rajneesh Gupta, who designed this project.

- Rajneesh Gupta Github:
<https://github.com/0xrajneesh>
- Project:
<https://github.com/0xrajneesh/Cloud-Security-Projects-For-Beginners/blob/main/Project-4-Securing-Data-In-AWS-S3-Bucket.md>