# 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

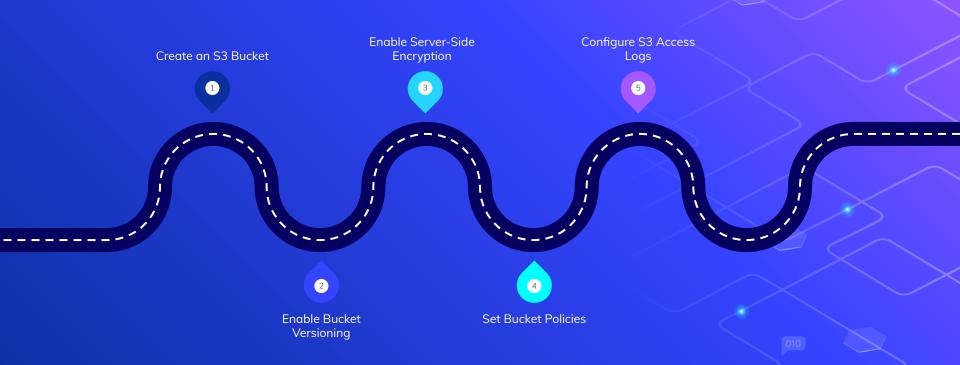


## The Objective

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

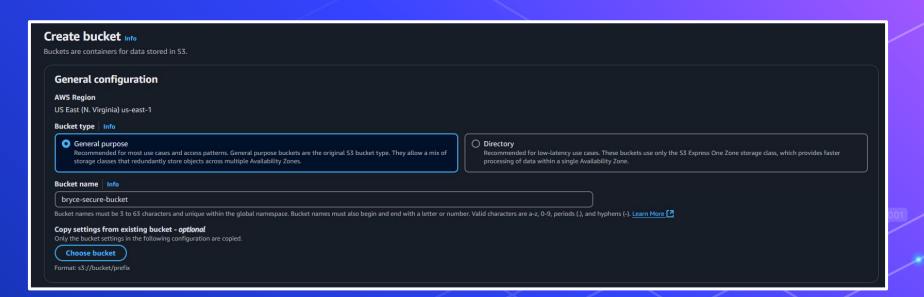


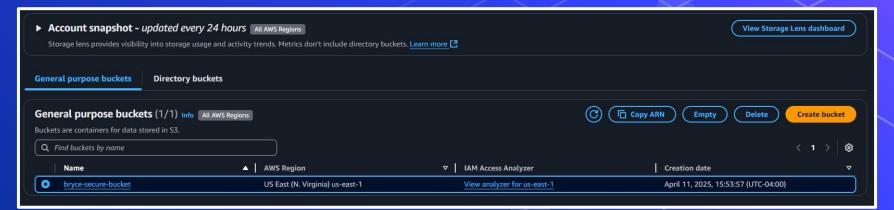
## Roadmap



## 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.





## 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

① 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 2

Disabled

Cancel

Save changes

100

## 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 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 🔀

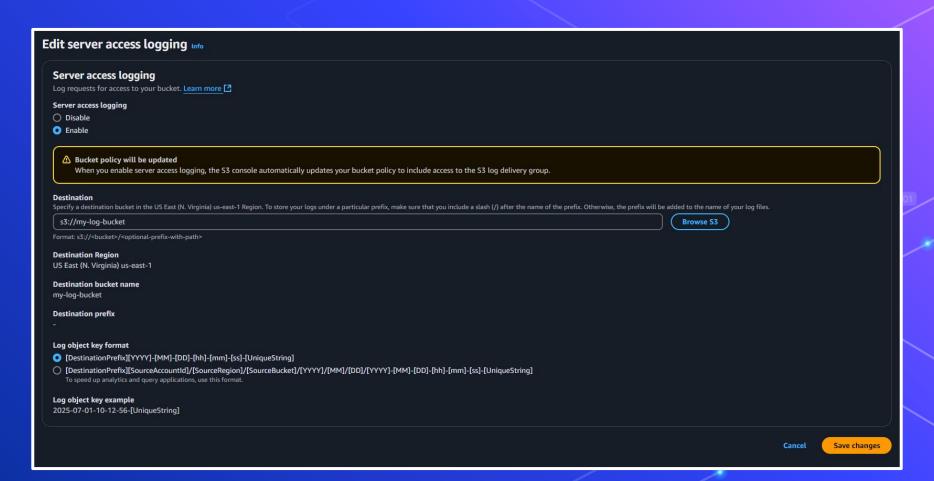
#### **Bucket ARN**

arn:aws:s3:::bryce-secure-bucket

#### **Policy**

## **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.



## 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/bryce

cox-559616219/

Email: bcox8898@gmail.com



### **Credits**

Special thanks to Rajneesh Gupta, who designed this project.

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