OpenSecOps SOAR S3 Buckets

Standard Operating Procedure

Table of Contents

1 Introduction

The purpose of this document is to specify baseline settings for AWS S3 Buckets so that teams can provision S3 Buckets in a safe, conformant way.

2 Scope of SOP

This document covers AWS S3 Buckets and how they are to be set up in the CloudSecOps AWS organisation.

Document Versions

Version	Date	Changes	Author
1.0	2022-09-12	First version	Peter Bengtson
1.1	2025-04-07	Replaced “Delegat” with “OpenSecOps” throughout	Peter Bengtson

Please add new entries *above* already existing rows.

3 Make your S3 Bucket Non-Public

Always explicitly set your bucket to be non-public, unless it needs to be publicly accessible (for which see next section). Failing to make it inaccessible to the world is a `CRITICAL` security issue that immediately will be detected by our automated security monitoring. A security incident will be created which your team will have to fix as a show-stopping silver bullet, i.e. with immediate priority over all ongoing work in the team as a whole.

3.1 CloudFormation

```
ExampleBucket:
    Type: AWS::S3::Bucket
    Properties:
      PublicAccessBlockConfiguration:
        BlockPublicAcls: true
        BlockPublicPolicy: true
        IgnorePublicAcls: true
        RestrictPublicBuckets: true
```

3.2 Terraform

```
resource "aws_s3_bucket" "example" {
  bucket = "example"
}

resource "aws_s3_bucket_public_access_block" "example" {
  bucket = aws_s3_bucket.example.id

  block_public_acls   = true
  block_public_policy = true
}
```

4 Public S3 Buckets

If you need an S3 bucket to be publicly readable and/or writable – which should be very rare – you must set one or both of the following tags on your S3 bucket:

```
soar:s3:request-publicly-readable
soar:s3:request-publicly-writable
```

The tags are case-sensitive. The value of the tags should be empty (“”). (NB: `publicly` is the correct spelling; “-ally” would be incorrect.)

When one or both of the above tags are present, the S3 bucket will be left open.

SOC will be notified of your request via a Jira incident. You will be contacted about the reasons for wanting to create a storage volume open to the world. Should SOC deny the request, you will also be contacted prior to the removal of the tag.

If the S3 bucket already has been closed by the Moonstone SOAR, adding the tags after the fact will *not* open the bucket again. You must add the tag(s), then open the bucket for read and/or write again either manually in the console, using the CLI, the API, or in code.

5 Enabling S3 Bucket Server-Side Encryption

All AWS S3 buckets created in Moonstone **MUST** have server-side encryption enabled. This applies to S3 buckets created manually, by using Terraform, or by using CloudFormation. It also applies to all S3 buckets created by or for third-party software such as Jenkins and Curity, as well as to buckets created by, and for, such things as CodePipeline.

Remediating this is very easy. Use the following tips to enable AES-256 encryption for existing buckets. Also, incorporate the code snippets in all your future infrastructure-as-code-created S3 buckets, so they are compliant right from the start, in all environments.

NB: Encryption can be enabled at any time. It doesn't matter whether the S3 bucket is empty or not. Encryption is completely transparent.

5.1 CloudFormation

```
ExampleBucket:
  Type: 'AWS::S3::Bucket'
  Properties:
    BucketEncryption:
      ServerSideEncryptionConfiguration:
        - ServerSideEncryptionByDefault:
            SSEAlgorithm: AES256
```

5.2 Terraform

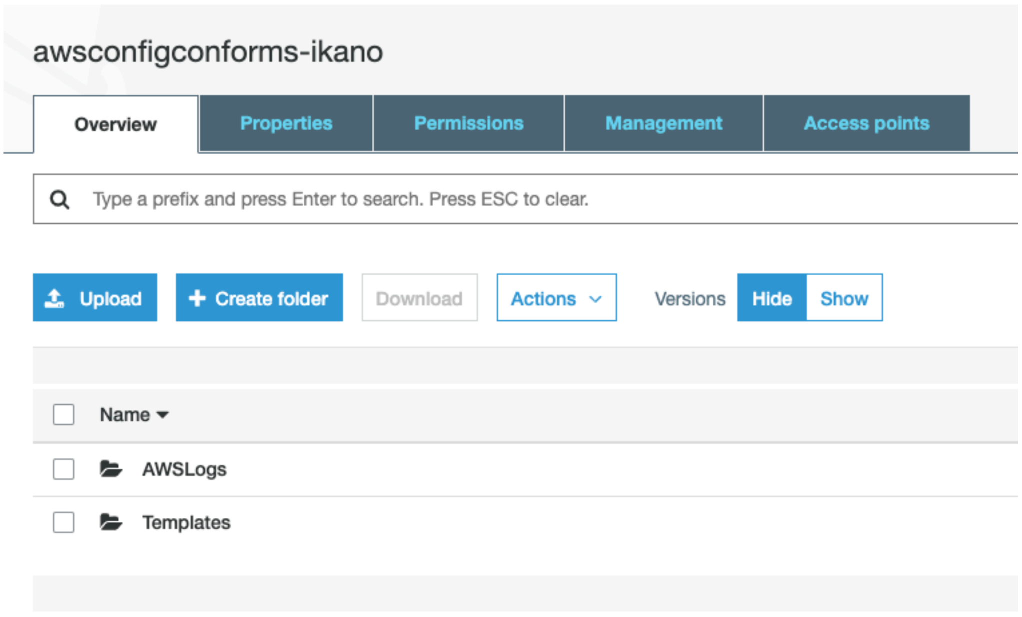
NB: The following example will encrypt the bucket and all its contents. If you have copied the S3 boilerplate example code from the Terraform documentation, you might have copied the example which encrypts all items in the bucket but not the bucket itself. That kind of setup will not satisfy the security control. The following, on the other hand, will:

```
resource "aws_s3_bucket" "mybucket" {
  bucket = "mybucket"

  server_side_encryption_configuration {
    rule {
      apply_server_side_encryption_by_default {
        sse_algorithm = "AES256"
      }
    }
  }
}
```

5.3 Buckets created manually

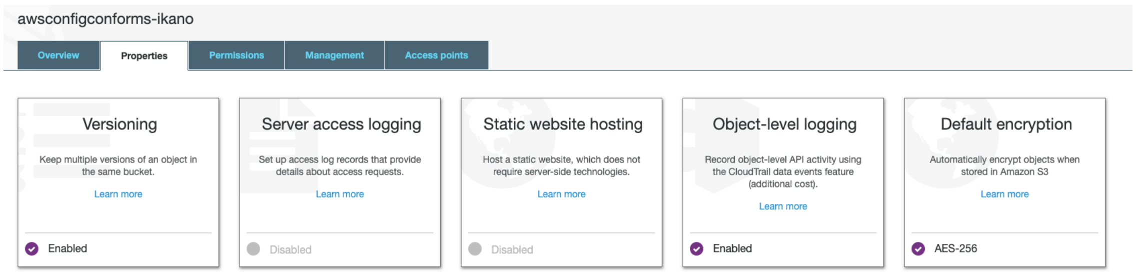
Use the console to navigate to the bucket, e.g.:


awsconfigconforms-ikano

AWSLogs

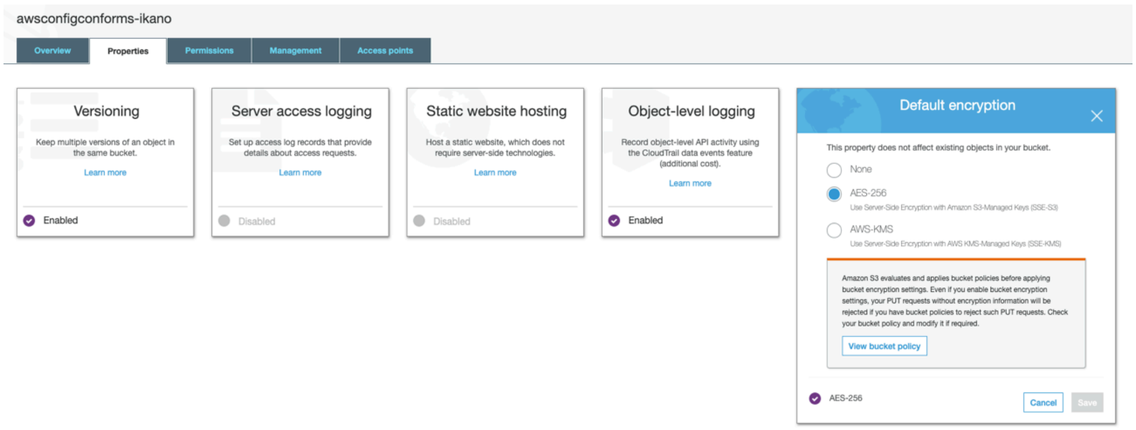
Templates

Click on Properties:


awsconfigconforms-ikano

Versioning	Server access logging	Static website hosting	Object-level logging	Default encryption
Keep multiple versions of an object in the same bucket.	Set up access log records that provide details about access requests.	Host a static website, which does not require server-side technologies.	Record object-level API activity using the CloudTrail data events feature (additional cost).	Automatically encrypt objects when stored in Amazon S3
Learn more	Learn more	Learn more	Learn more	Learn more
Enabled	Disabled	Disabled	Enabled	AES-256

Then click on Default encryption and choose AES-256:


awsconfigconforms-ikano

Versioning	Server access logging	Static website hosting	Object-level logging
Keep multiple versions of an object in the same bucket.	Set up access log records that provide details about access requests.	Host a static website, which does not require server-side technologies.	Record object-level API activity using the CloudTrail data events feature (additional cost).
Learn more	Learn more	Learn more	Learn more
Enabled	Disabled	Disabled	Enabled

Default encryption

This property does not affect existing objects in your bucket.

None [✓ AES-256] AWS-KMS

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.

AES-256

6 Other Considerations

6.1 Versioning

Consider enabling versioning for S3 buckets containing data which must not be lost or where changes to data must be trackable at all times. If you enable versioning, you should also enable one or more life-cycle rules for the data in the bucket.

6.2 Life-Cycle Rules

If your bucket contains logs or any continuously incoming high-volume data, consider enabling life-cycle rules to delete data after a suitable period of time, or storage costs might become an issue.

6.3 Glacier Considerations

If you write life-cycle rules to transition S3 bucket data to Glacier, make sure the items in your bucket aren’t too small. There is a lower limit to what can be transferred to Glacier; also, retrieving small items from Glacier can become expensive. Therefore: do not store items smaller than 200 KB in Glacier.

7 Security Hub Controls for S3 Buckets

Below are the enabled controls in AWS Security Hub pertaining to S3 buckets. Your buckets must comply with all of them. Be proactive. It is easiest to make them compliant from the beginning, rather than when the automated security checks have created tickets for your team to fix misconfigurations which constitute security risks.

In the following list, all CIS.n.n required controls are satisfied by the enterprise infrastructural layer; you should never have to consider yourself with these.

However, the four S3.n rules (S3.2, S3.3, S3.4, and S3.6) are your responsibility at all times, no matter how you create your infrastructure.

7.1 CRITICAL

■ Critical	S3.2	S3 buckets should prohibit public read access
■ Critical	S3.3	S3 buckets should prohibit public write access
■ Critical	CIS.2.3	Ensure the S3 bucket used to store CloudTrail logs is not publicly accessible

7.2 HIGH

■ High	S3.6	S3 permissions granted to other AWS accounts in bucket policies should be restricted

7.3 MEDIUM

■ Medium	S3.4	S3 buckets should have server-side encryption enabled

7.4 LOW

■ Low	CIS.2.2	Ensure CloudTrail log file validation is enabled
■ Low	CIS.2.4	Ensure CloudTrail trails are integrated with CloudWatch Logs
■ Low	CIS.2.6	Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket
■ Low	CIS.3.8	Ensure a log metric filter and alarm exist for S3 bucket policy changes