



Configuring Amazon S3 security settings and access controls

Getting started at an AWS hosted workshop

▼ S3 Security Best Practices

▼ Prepare Your Lab

- Attach IAM Role to EC2 Instance
- Connect to the EC2 Instance
- Bucket Name

▼ Lab 1 - S3 Security Exercises

- Require HTTPS
- Require SSE-KMS Encryption
- Restrict Access to an S3 VPC Endpoint
- Use AWS Config Rules to Detect a Public Bucket
- Use Amazon Access Analyzer for S3

▼ Lab 2 - S3 Access Grants

- S3 Access Grants Lab - Initial Setup
- Configure S3 Access Grants for IAM user

▼ Lab 3 - Enabling Malware Protection for S3 by using GuardDuty

- Enabling Malware Protection for S3 for your bucket
- Testing GuardDuty Malware with an object.

▼ Lab 4 - S3 Access Control Lists

- Block Public ACLs
- Configure S3 Block Public Access
- Disable S3 ACLs

▼ Finding S3 access control lists with S3 Inventory

Enabling Amazon S3 Inventory

- Setting up Amazon Athena
- Use Amazon Athena to query Amazon S3 Inventory and identify objects with ACL elements

► Use Amazon Athena to query CloudTrail logs and identify S3 requests that depend on ACLs

Lab Summary

[Configuring Amazon S3 security settings and access controls](#) > ... > [Lab 4 - S3 Access Control Lists](#) > [Finding S3 acc](#)

Enabling Amazon S3 Inventory

In this exercise, we will enable Amazon S3 Inventory and walk through the format of the S3 Inventory report.

From the AWS console in the top search bar, search and select S3.

- Click the bucket name starting with `sid-security-xxxxxxx`.
- Click on the **Management** tab.
- Scroll down to **Create inventory configuration**
- Type `"test"` as the Inventory configuration name
- Under **Report details** click **"Browse S3"** and click on the radio button to the left of the S3 bucket starting with `sid-security-xxxxxxx`.
- Keep all the defaults until you get to **Inventory report encryption**
- Click **Specify an encryption key** and **Server-side encryption with Amazon S3 managed keys (SSE-S3)** under **Encryption type**
- Select **Object ACL** and **Object owner** under **Permissions**.

Your screen should look like the following:

Inventory report encryption [Info](#)

Server-side encryption protects data at rest.

Server-side encryption

☐ Do not specify an encryption key
The bucket settings for default encryption are used to encrypt objects when storing them in Amazon S3.

☒ Specify an encryption key
The specified encryption key is used to encrypt objects before storing them in Amazon S3.

Encryption type [Info](#)

☒ Server-side encryption with Amazon S3 managed keys (SSE-S3)

☐ Server-side encryption with AWS Key Management Service keys (SSE-KMS)

Additional metadata fields - optional

Choose the metadata that should be included for each listed object in the report. [Learn more](#)

Object

☐ Size

☐ Last modified

☐ Multipart upload

☐ Replication status

☐ Encryption

☐ Bucket key status

Permissions

☒ Object ACL

☒ Object owner

Storage class

☐ Storage class

Click **Create**

There will be two dialog boxes at the top, they should look similar to:



Amazon S3

Buckets

sid-security-ca51ea00-acec-11ef-ab19-02dc4668901f

Management

Inventory configurations

Inventory test successfully created.

It may take up to 48 hours to deliver the first report.

Bucket policy successfully created

Amazon S3 created a policy on the destination bucket to allow it to place data in that bucket. [Learn more](#)

View policy

Inventory configurations (1)

Info

View details

Edit

Delete

Create job from manifest

Create inventory configuration

You can create inventory configurations on a bucket to generate a flat file list of your objects and metadata. These scheduled reports can include all objects in the bucket or be limited to a shared prefix. [Learn more](#)

< 1 >

	Name	Status	Scope	Destination	Frequency	Last export	Format
<input type="radio"/>	test	Enabled	Entire bucket	s3://sid-security-c...	Daily	-	CSV

Since the first report can take up to 48 hours to deliver as mentioned we have pre-populated the bucket `sid-security-xxxxxxx` with a prefix called "inventory" and a S3 Inventory report named `s3inventoryreportfordemo.csv`. We still ran through the creation of setting up S3 Inventory so you have a working knowledge of how to do so.

Now before we go any further we need to setup Amazon Athena to query the S3 Inventory report.

Previous

Next

