



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

Lab Summary

[Configuring Amazon S3 security settings and access controls](#) > [S3 Security Best Practices](#) > [Lab 3 - Enabling Malware](#)

Enabling Malware Protection for S3 for your bucket

In this exercise, we will walk through how to enable GuardDuty Malware Protection for S3 independently. *Note* If you also want to use other dedicated protection plans in GuardDuty, you must get started with the Amazon GuardDuty service. For information about GuardDuty protection plans, see Features of GuardDuty.

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

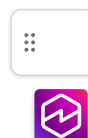
- Click "Get started".

You will be guided to the Malware Protection for S3 main page and click "Enable".

From here you will enter the wizard:

- Click "Browse S3".
- Select the bucket `sid-security-xxxxxxx`, there should only be one option.
- Keep the rest of the defaults.
- *Note* in the 'Tag scanned objects' section this will tag an object if a threat is found, we will explore this more later.

Your screen should look like the following:



GuardDuty > Malware Protection for S3 > Enable Malware Protection for S3

Enable Malware Protection for S3

info

Detects malware by scanning the newly uploaded files to your selected S3 buckets and object prefixes. [AWS Service Terms for GuardDuty Malware Protection](#) will apply.

Scanning cost will apply. [Learn more](#)

Enter S3 bucket details

S3 bucket

sid-security-d6ae2700-9c57-11ef-9d5d-025a5a8c72b7

X

View

Browse S3

The AWS Region of your S3 bucket must be US West (Oregon).

Prefix

Limit the scope of the malware scan by entering one or more prefixes.

All the objects in the S3 bucket

Objects beginning with a specific prefix

Tag scanned objects

Allow GuardDuty to add tags to your scanned objects. Use these tags to check the latest malware scan status for your S3 object and set up tag-based access control (TBAC). S3 Object Tagging cost will apply. [Learn more](#)

You can further update your S3 resource policy to setup tag-based access control (TBAC).

Tag objects

After each malware scan, GuardDuty tags your S3 object with a scan status - NO_THREATS_FOUND, THREATS_FOUND, UNSUPPORTED, ACCESS_DENIED, or FAILED.

Do not tag objects

If you do not use tags, objects can be accessed before the malware scan completes.

Service access

info

GuardDuty requires permissions to perform malware scan actions on your behalf.

Choose a method to authorize GuardDuty

Create and use a new service role

Use an existing service role

Role name

Enter a meaningful name to identify this role.

GuardDutyS3MalwareScanRole-0d21b91f-a748-44cc-8311-f556a1c89278

Role name must be 1-64 characters. Valid characters are a-z, A-Z, 0-9, and '+', '@', '-' characters.

Tag Malware Protection Plan ID - optional

A tag is a custom label that you assign to the Malware Protection Plan ID associated with your S3 bucket. Each tag consists of a key and an optional value.

Cancel

Enable

Now click "Enable"

Info

This will take a moment while the configurations are set.

Now you should be returned to the main screen again and we can move on to testing with an object in the next section.

GuardDuty > Malware Protection for S3

Malware Protection for S3

info

Detects malware by scanning the newly uploaded files to your selected S3 buckets and object prefixes. [AWS Service Terms for GuardDuty Malware Protection](#) will apply.

Scanning cost will apply. [Learn more](#)

Monitoring and access management

View CloudWatch metrics for your scanned S3 objects.

[Learn more](#)

Configure EventBridge alerts to get notified about recent scans.

[Learn more](#)

Enable tagging to add tags to the scanned objects. Using these tags, set up tag-based access control (TBAC) policy on your S3 bucket resource.

[Learn more](#)

Protected buckets (1)

Refresh

Disable

Edit

Enable

Enabled Malware Protection for S3 for the listed buckets and object prefixes.

S3 bucket

Prefix

Malware Protection plan ID

Status

Status details

Created

sid-security-fbd51d40-add2-11ef-aeef-0a5351ee2b45

-

72c9bca50f160b331f39

Active

-

a few seconds ago

https://catalog.us-east-1.prod.workshops.aws/workshops/8f6b34da-c21e-4094-8070-8d98e2e6ca08/en-US/s3-security-best-practices-lab/03-s3guardduty/01-g... 2/3

[Previous](#)

[Next](#)

