



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

Enabling Cloudtrail data events

Setting up Amazon Athena

Lab Summary

[Configuring Amazon S3 security settings and access controls](#) > [S3 Security Best Practices](#) >

Lab Summary

To recap what we have learned:

- **Lab 1 - Security exercises:** Grant and restrict permissions to your S3 buckets with S3 bucket policies. Use AWS Config and Access Analyzer to detect buckets within your account and organization that have public access, and remediate public access where unintended.
- **Lab 2 - S3 Access Grants:** S3 Access Grants complement the existing S3 security management tools to manage permissions for IAM roles/users, AWS services, as well as corporate identities. We encourage exploring S3 Access Grants where you want to scale your fine-grained access control with a simplified model for defining access permissions.
- **Lab 3 - Enabling Malware Protection for S3 by using GuardDuty:** Automatically scan for the potential presence of malware within your S3 buckets to protect your users and applications.
- **Lab 4 - S3 Access Control Lists:** To align with S3's best practices for managing security permissions, we encourage all customers to consider disabling ACLs within their environments. This lab demonstrates how to manage your S3 ACL permissions, detect where they may still be present in your AWS accounts, and disable ACLs on your buckets.



Workshop complete

Congratulations you have completed the the Amazon S3 security workshop.

[Previous](#)

