



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 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
- 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](#) > [S3 Security Best Practices](#) > Lab 4 - S3 Access C...

Lab 4 - S3 Access Control Lists

As of April 2023, Amazon S3 now automatically enables S3 Block Public Access and disables S3 access control lists (ACLs) for all new S3 buckets in all AWS Regions.

To help customers simplify their security management, it is best practice for all Amazon S3 customers to consider disabling Access Control Lists (ACLs) and migrate to S3 bucket policies with IAM policies.

We recognize that there will be existing customers who wish to dive deeper into ACLs.

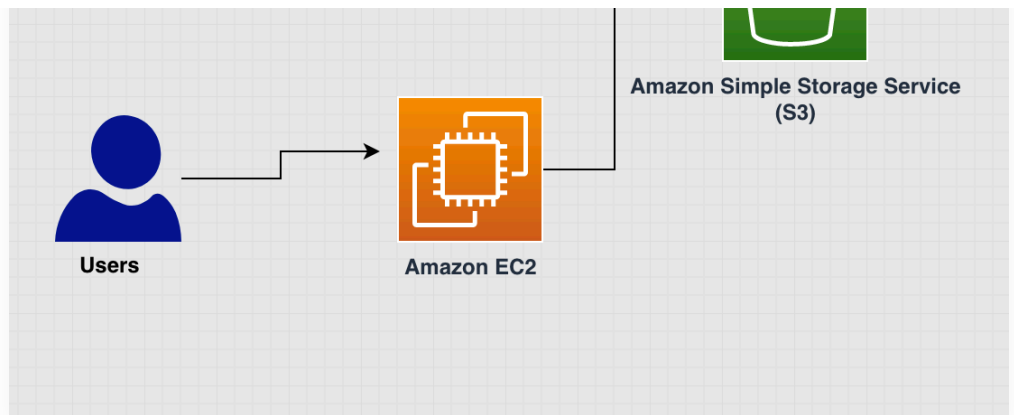
The following labs will guide you around how to secure S3 environments where ACLs are in use and how to migrate your buckets from using ACLs so you can use policy based security access controls.

© 2008 - 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

[Privacy policy](#)

[Terms of use](#)

[Cookie preferences](#)



[Previous](#)

[Next](#)

