Configuring Amazon S3 security settings and access controls

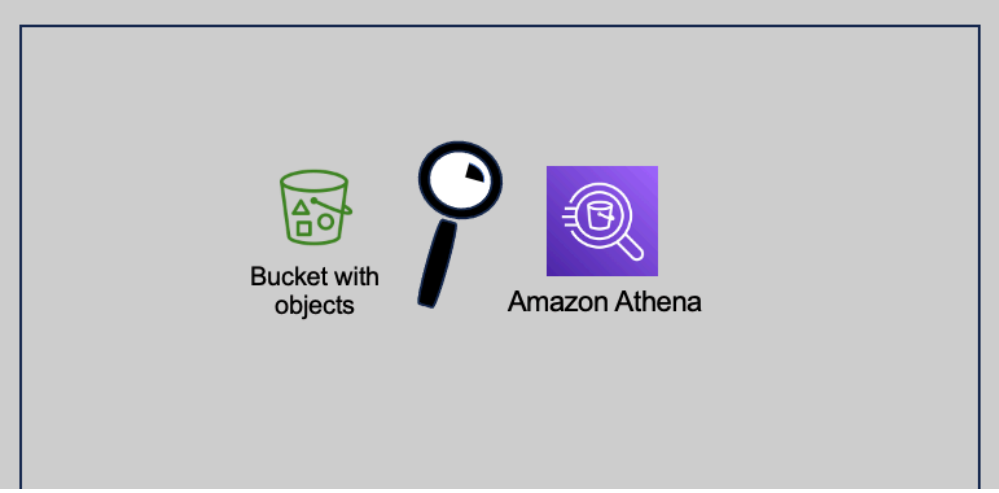
- Getting started at an AWS hosted workshop
- S3 Security Best Practices
  - Prepare Your Lab
    - Attach IAM Role to EC2 Instance
    - Connect to the EC2 Instance
    - Bucket Name
  - Lab 1 - S3 Security Exercises
    - Require HTTPS
    - Require SSE-KMS Encryption
    - Restrict Access to an S3 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
  - 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

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

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.

Access control lists (ACLs) define user access and the operations users can take on specific resources. Amazon Simple Storage Service (Amazon S3) was launched in 2006 with ACLs as its first authorization mechanism. Since 2011, Amazon S3 has also supported AWS Identity and Access Management (IAM) policies for managing access to S3 buckets, and it recommends using policies instead of ACLs. Although ACLs continue to be supported in Amazon S3, most use cases no longer require them.

In this lab we will configure CloudTrail with data events and use Amazon Athena to query the CloudTrail logs for objects actively being used with ACLs.



© 2008 - 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy policy Terms of use Cookie preferences

Previous Next