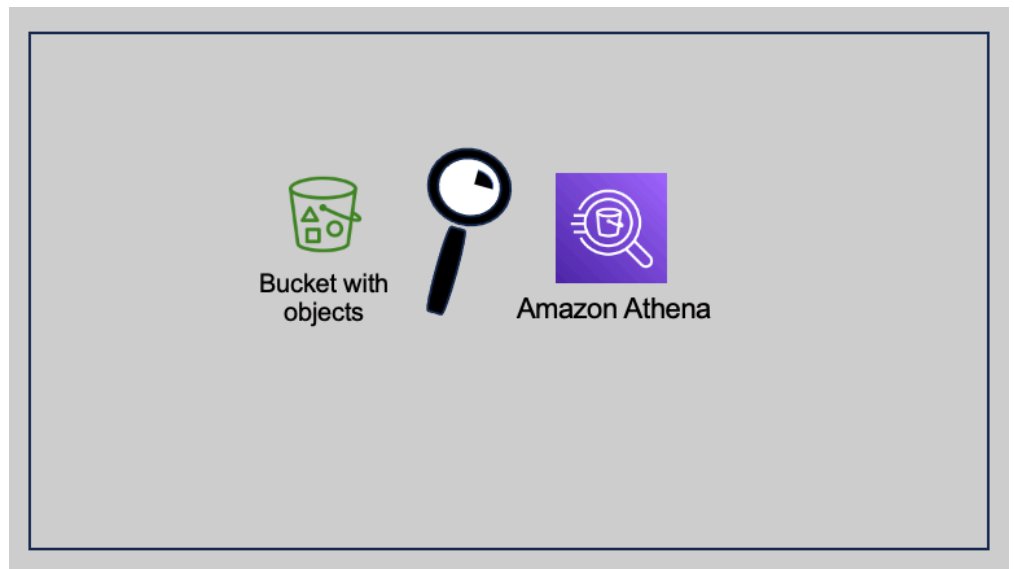Configuring Amazon S3 security settings and access controls › S3 Security Best Practices › Lab 4 - S3 Access Control

Finding S3 access control lists with S3 Inventory

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 S3 Inventory and use Amazon Athena to find existing objects with ACLs.

Previous   Next