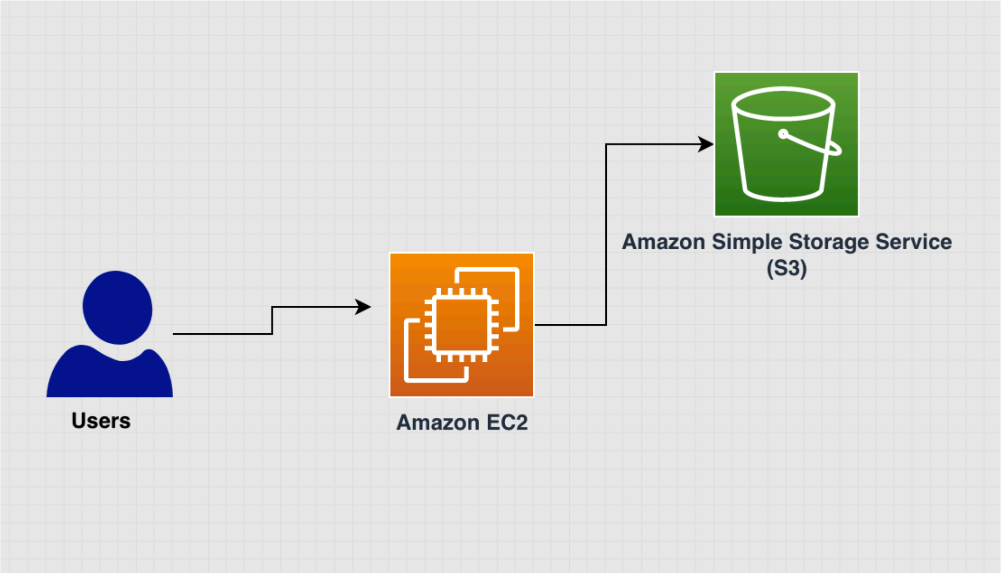
Configuring Amazon S3 security settings and access controls

- 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
  - Lab 3 - Enabling Malware Protection for S3 by using GuardDuty
  - Lab 4 - S3 Access Control Lists
  - Lab Summary

Configuring Amazon S3 security settings and access controls > S3 Security Best Practices > Lab 1 - S3 Security...

Lab 1 - S3 Security Exercises

The following exercises will show you how to use bucket policies, encryption, and VPC endpoints to secure your S3 buckets. We will also explore using AWS Config and IAM Access Analyzer to review your S3 security posture.



Previous Next