

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

Lab 2 - S3 Access Grants

Lab 3 - Enabling Malware Protection for S3 by using GuardDuty

Lab Summary

Configuring Amazon S3 security settings and access controls

S3 Security Best Practices

Prepare Your Lab

Bucket Name

From the AWS console in the top search bar, search and select S3.

Click on the sid-security-xxxxxxx bucket.

Amazon S3

Buckets

Access Points

Batch Operations

Access analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight

Amazon S3

Buckets (1)

Find buckets by name

Name	AWS Region	Access	Creation date
sid-security-8353b790-868b-11eb-9bd4-0a342d0461c3	US West (Oregon) us-west-2	Objects can be public	March 16, 2021, 15:12:30 (UTC-04:00)

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

Privacy policy

Terms of use

Cookie preferences

Copy your unique bucket name on top and paste it into your text editor. We will use this later.

Amazon S3

Buckets

Access Points

Batch Operations

Access analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight

Amazon S3

sid-security-8353b790-868b-11eb-9bd4-0a342d0461c3

sid-security-8353b790-868b-11eb-9bd4-0a342d0461c3

Objects

Properties

Permissions

Metrics

Management

Access Points

Objects (2)

Find objects by prefix

Name	Type	Last modified	Size	Storage class
app1/	Folder	-	-	-
app2/	Folder	-	-	-

Previous

Next

1/1