Planning for AWS S3 Data Security

Learn how to secure your Amazon S3 buckets and objects with this entry-level AWS training. Understand how to write IAM policies, define bucket access, limit public access, and monitor S3 resources. This course will help you sharpen your cloud skills and ensure your cloud storage is safe, and that permissions are properly managed for both individuals and teams transitioning to AWS S3.

CBT Nuggets course material →

STUDY PLAN

WEEK 1

Manage Access to AWS Resources — 96 min.

Overview	1
Supplemental File	1
Authorization and Authentication at AWS	7
Management Interfaces at AWS	8
Permissions Delegation with Roles	9
Evaluating Permissions at AWS	7
Security Policy Types and Elements	9
Amazon Resource Names	9
Using Dynamic Security Policy Conditions and Variables	9
Managing Permissions with the Management Console	8
Managing Permissions on the Command Line	9

Plan for S3 Confidentiality Data Security

Overview	1
Supplemental File	1
S3 Confidentiality	1
S3 Client-Side Encryption	1
S3 Server-Side Encryption: Client Key	1
S3 Server-Side Encryption: S3 Keys	1
S3 Server-Side Encryption: KMS Keys	1
S3 Public Access Account Restrictions	1

Plan for S3 Integrity and Availability Data Security

Overview	1
Supplemental File	1
S3 Integrity and Availability	1

S3 Lifecycle Policies	1
S3 Bucket Replication	1
S3 Replication: Destination Bucket	1
S3 Replication: Source Bucket	1
Glacier Vaults and Vault Lock Policies	1

Last updated 12.3.2024