06

S3 Security

6.1
Access Controls

Bucket Policies

1)

JSON-based policies that define access permissions for the entire bucket.

2)

Allow or deny permissions to users, groups, or AWS accounts.

3)

Useful for granting cross-account access.

IAM Policies

1)

Managed via AWS Identity and Access Management (IAM).

2)

Control access to S3 buckets and objects at the user or group level.

3)

Define granular permissions for specific actions

Access Control Lists (ACLs)

1)

Legacy method for managing access to individual objects and buckets.

2)

Grant read/write permissions to AWS accounts or predefined groups

Block Public Access

1)

Centralized settings to prevent public access to S3 buckets and objects.

2)

Override bucket policies and ACLs that grant public access.

6.2
Data Encryption

Server-side Encryption

SSE-S3

Amazon-managed keys for encryption (AES-256).

SSE-KMS

AWS Key Management Service (KMS) managed keys for additional control and auditing.

SSE-C

Customer-provided keys for encryption.

Client-side Encryption

1)

Data is encrypted by the client before it is uploaded to S3.

2)

Client is responsible for managing encryption keys.

6.3

Logging & Monitoring

S3 Server Access Logging

- Logs requests made against your S3 bucket.
- Useful for security auditing and access monitoring.

AWS CloudTrail

- Records API calls made on your AWS account.
- Provides detailed logs for S3 operations, including object-level actions.

AWS Config

- Tracks configuration changes to your S3 buckets.
- Ensures compliance with internal policies and standards.

6.4
Data integrity

Data Integrity

Maintains multiple versions of an object in a bucket.
Protects against accidental deletion or overwriting.

Bucket Versioning

MFA Delete

Requires multi-factor authentication for delete operations on versioned objects.
Adds an extra layer of protection against accidental or malicious deletions.

07

S3 CORS

CORS

A mechanism that allows web applications running at a different origin (domain) to access resources in your S3 bucket.
A Security feature for the Web browser

08

Pre Signed URLS

Pre Signed URL

Pre-Signed URLs allow you to grant temporary access to your S3 objects to users without requiring them to have AWS credentials.

Use Case

Temporary Access

Share files with users temporarily without exposing your AWS credentials

Upload to S3

Allow users to upload files directly to S3 without needing IAM permissions.

Controlled Distribution

Share downloadable links for media files, software packages, etc., with controlled access.

09

Object Locks

S3 Object Lock

Helps you store objects using a write-once-read-many (WORM) model, which prevents objects from being deleted or overwritten for a specified period or indefinitely.

Key Points

Retention Modes:

- Governance Mode: Most people can't change or delete the data, but those with special permissions can override the lock.

- Compliance Mode: No one, not even the root user, can change or delete the data until the lock expires.

Key Points

Retention Period:

You can set a time period during which the data is protected and can't be altered.

Legal Holds:

A legal hold is like a freeze that prevents data from being deleted. It stays in place until you manually remove **it.**

Regulatory Compliance: If the law says you need to keep certain records unchanged for a number of years, Object Lock ensures that these records can't be tampered with.

Data Protection: Protects your backup files or important documents from being accidentally deleted or changed.

Legal Requirements: Ensures data involved in legal cases remains intact and unaltered.

Use Cases

Thanks!

Do you have any questions?

mayamnaiel2013@gmail.com

The Tech Stuff