AWS S3 and Cross-Account Access – Complete Guide

1. What is Amazon S3?

Amazon Simple Storage Service (S3) is a scalable object storage service used for storing and retrieving any amount of data from anywhere. It is widely used for backup, data archiving, hosting static websites, big data analytics, and cloud-native applications.

Key Features:

1   Object-based storage for files, images, videos, and backups.

2   Highly durable (99.999999999% durability) and available.

3   Supports versioning, encryption, and lifecycle management.

4   Integrates with AWS services like Lambda, CloudFront, and Athena.

2. Common Use Cases of S3

1   Data backups and disaster recovery.

2   Static website hosting.

3   Big data storage and analytics input.

4   Application data storage for mobile/web apps.

5   Media storage for streaming and content distribution.

3. Cross-Account S3 Access Setup

This section demonstrates how to allow one AWS account (Account B) to access an S3 bucket located in another AWS account (Account A). This setup is often required when multiple teams or environments need to share data securely.

Step-by-Step Setup:

1   **Account A (Owner):** Create an S3 bucket (e.g., cross-account-demo-111111111111).

2   Add a bucket policy allowing Account B access:

3   { "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Principal": {"AWS": "arn:aws:iam:::root"}, "Action": ["s3:GetObject", "s3:ListBucket"], "Resource": ["arn:aws:s3:::cross-account-demo-", "arn:aws:s3:::cross-account-demo-/*"] }] }

4   **Account B (Consumer):** Create an IAM user or role with permissions to access Account A's bucket.

5   Attach IAM policy to allow S3 list and get access.

6   Use AWS CLI to test access:

7   aws sts get-caller-identity aws s3 ls s3://cross-account-demo- aws s3 cp s3://cross-account-demo-/test.txt .

8   Optionally, copy the file into your own bucket in Account B.

4. Security Best Practices for S3

1 Enable S3 Block Public Access.

2 Use IAM roles and least privilege principle.

3 Enable versioning and MFA delete.

4 Use encryption (SSE-S3 or SSE-KMS).

5 Enable access logging and CloudTrail auditing.

5. Conclusion

Amazon S3 provides a robust and secure storage solution that integrates seamlessly with other AWS services. Cross-account access enables efficient and secure collaboration between AWS accounts, ensuring controlled data sharing while maintaining strong security practices.