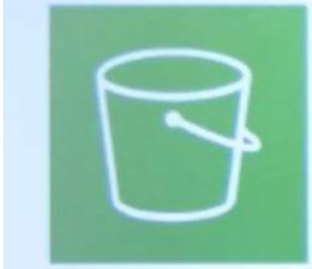


Controlling Access to AWS S3 Buckets

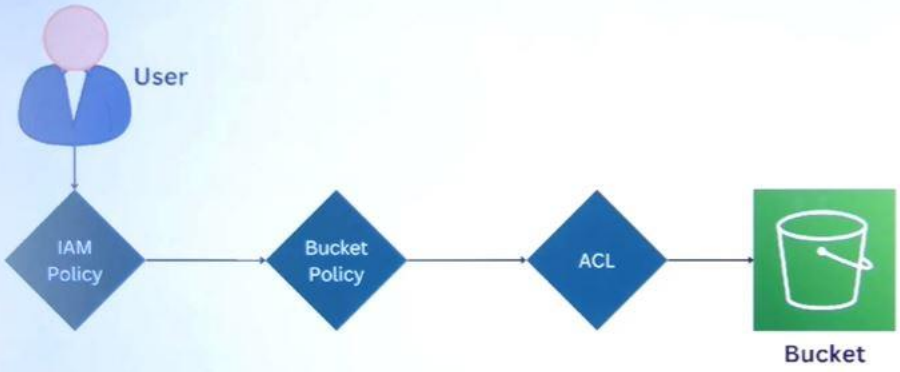
Controlling Access

The process of managing who can view, change, or delete the objects stored within your AWS S3 Bucket.

Controlling Access -Tools

- IAM Policies
- Bucket Policies
- ACLs

How It Works ?



Controlling Access

IAM Policy	Bucket Policy	ACL	Outcome
Not Attached	Not Attached	Not Attached	Access Denied
Not Attached	Not Attached	Allows Access	Access Granted
Not Attached	Allows Access	Not Attached	Access Granted
Not Attached	Allows Access	Allows Access	Access Granted
Allows Access	Not Attached	Not Attached	Access Granted
Allows Access	Not Attached	Allows Access	Access Granted
Allows Access	Allows Access	Not Attached	Access Granted
Allows Access	Allows Access	Allows Access	Access Granted

Note: A single deny rule in the IAM policy, bucket policy, or ACL (if present) will result in total denial of access.

IAM Policy Vs Bucket Policy

Feature	IAM Policy	Bucket Policy
Management	Managed via the IAM dashboard	Managed via the S3 dashboard
Format	JSON	JSON
Scope	Applies to AWS services/Identity-based	Applies S3 buckets/Resource-based
Use Cases	Broad AWS permissions	Specific S3 permissions
Attached To	IAM users, groups, roles	S3 buckets
Best for	Multiple AWS services	Specific S3 access
Cross-Account	Complex configuration	Ideal for S3 cross-account
Public Access	Not Applicable	Explicit public access control