AMAZON SIMPLE STORAGE SERVICE (S3)

# Configure and enforce granular access controls

At creation, all S3 buckets are private by default, with S3 Block Public Access enabled, access control lists (ACLs) disabled, and all new objects automatically encrypted. With S3 access management tools, you can grant access and define user and resource-based policies based on your needs.

## Amazon S3 default access management settings

### S3 Block Public Access

- Enabled by default for new buckets
- Block access to specific buckets or an entire AWS account
- Overrides all public access policies

### S3 Object Ownership

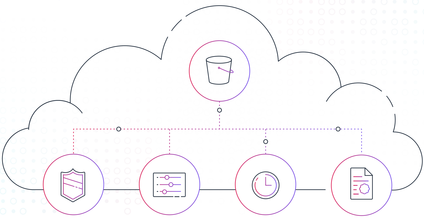
- ACLs disabled by default for new buckets
- Simplify cross-account workflows
- Access control is based only on policies

### Encryption in Amazon S3

- Base level of encryption (SSE-S3) automatically applied to all new objects
- Four options for server-side encryption: SSE-S3, SSE-KMS, SSE-C, DSSE-KMS
- Encrypt data server-side, client-side, and in transit to ensure strict access control

## Create access policies for your S3 resources

### Resource-based policies



**Bucket Policies**
Enforce access policies for objects in an S3 bucket.

**Query String Authentication**
Grant time-limited access to third parties with temporary URLs.

**Access Control Lists (ACLs)**
ACLs are disabled by default for new buckets, with IAM policies now recommended, but when enabled can allow you to define what users and accounts have read and/or write permissions at the object or bucket levels.

**S3 Access Points**
Manage access to your shared data sets on S3. Create Access Points with permissions for each application or groups of applications, or limit access to a Virtual Private Cloud (VPC).

Use S3 Object Ownership to disable ACLs and manage access only through policies.

## Define and grant user access

### User-based policies

#### AWS Identity and Access Management (IAM)

- Create users, groups, and roles within your AWS account
- Set and manage guardrails and fine-grained access controls
- Use AWS CloudTrail to monitor account activities

#### Virtual private cloud (VPC) endpoints

- Allow any users in your virtual network to access your S3 resources
- Provide specific access and permissions to groups of users based on the network the user is connected to
- Use VPC endpoints to deny bucket access if the request doesn't originate from the specified endpoint

## Track who is accessing what data, from where, and when

**Access Analyzer for S3**

- Reviews and alerts you to all buckets that allow access to anyone on the internet or other AWS customers
- Receive a report showing the source and level of public or shared access of your buckets, at no cost
- With one click, block all unintended public access to your bucket or drill down for granular levels of access

**S3 server access logging**

- Receive detailed records of requests made to a bucket (and store them in S3)
- See requester, bucket name, request time, request action, and error codes
- Access log information can be used to trigger S3 Event Notifications or in access audits

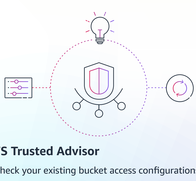
**AWS CloudTrail**

- Enable continuous delivery of events or view most recent events on demand
- Learn details about an S3 access request, including requester, IP address, time, and error codes
- Reports on actions taken by users, roles, and AWS services

Includes calls from the S3 console and S3 APIs

**S3 Inventory**

- Report on objects by prefix or bucket
- Audit object metadata, including encryption status
- Configure delivery of daily or weekly reports



**AWS Trusted Advisor**

- Check your existing bucket access configurations
- Fault tolerance checks for Amazon S3 buckets that don't have versioning enabled, or have versioning suspended
- Recommendations to help address security gaps

**Amazon GuardDuty and Amazon Macie**

- Discover, classify, and protect sensitive stored data
- Protect your AWS accounts with intelligent threat detection
- Evaluate bucket-level preventative controls and receive actionable security findings

## Discover how to secure your data using Amazon S3

Learn more

© 2023, Amazon Web Services, Inc. or its affiliates.