

Amazon Simple Storage Service (S3)

Configure, automate, and enforce granular access controls



At creation and by default, all S3 resources are private and only accessible to the resource owner and account administrator. With S3 access management tools, you can enable access to an S3 bucket or object, define user policies, and block all public access requests.

Create access policies to your S3 resources

Resource-based policies



Bucket Policies

Enforce access policies to all objects in an S3 bucket

Query String Authentication

Grant time-limited access to third parties with temporary URLs

Access Control Lists (ACLs)

Define what users and accounts have read and/or write permissions

Configure at the object and bucket levels

Use S3 Batch Operations to manage ACLs for hundreds to billions of objects — in minutes

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).

Define and grant user access within an AWS account

User policies

AWS Identity and Access Management (IAM)



Create users, groups, and roles within your AWS account

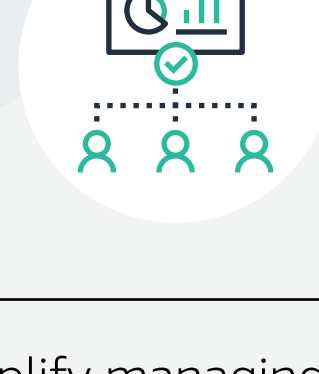


Define permissions to S3 and AWS resources

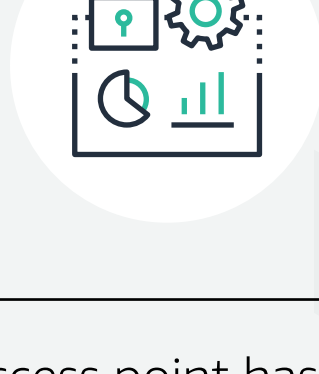


Use AWS CloudTrail to monitor account activities

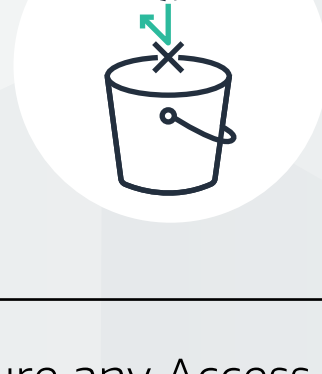
Managing data access with S3 Access Points



Simplify managing data access at scale for shared data sets in S3



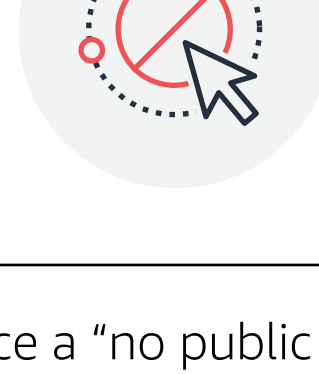
Each access point has distinct permissions and network controls to your data



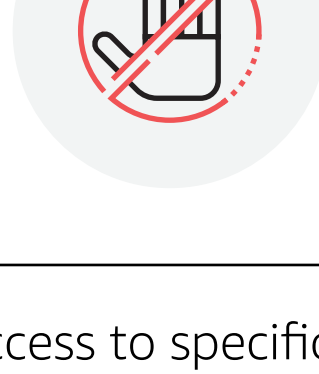
Configure any Access Point to restrict access from a VPC to firewall your data or block all public access to your bucket

Block all public access requests

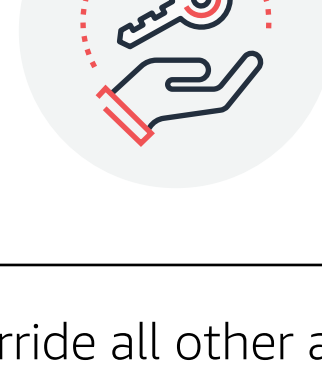
S3 Block Public Access



Enforce a "no public access" policy with a few clicks



Block access to specific buckets or an entire AWS account



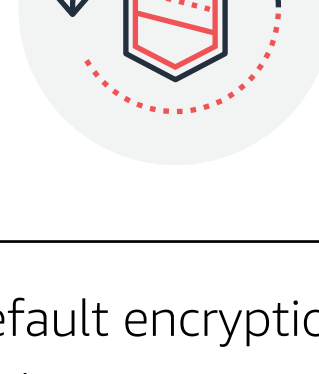
Override all other access policies



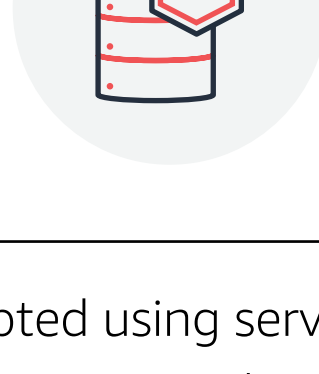
Discover publicly accessible buckets with

Trusted Advisor bucket permission check
S3 Management Console's access indicator

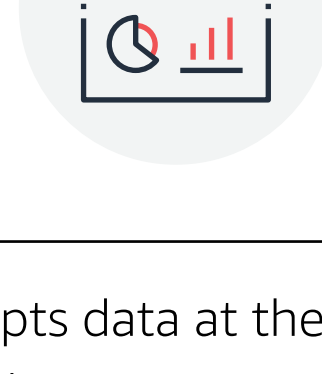
Default encryption for S3 buckets



Set default encryption so all new objects are encrypted



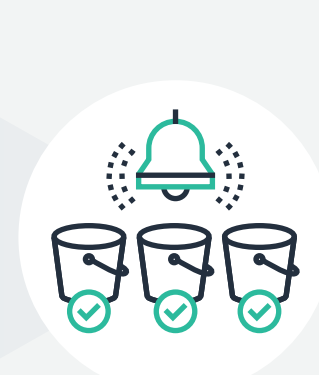
Encrypted using server-side encryption with either S3-managed or customer master keys



Encrypts data at the object level as it is written and decrypts when you access it

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

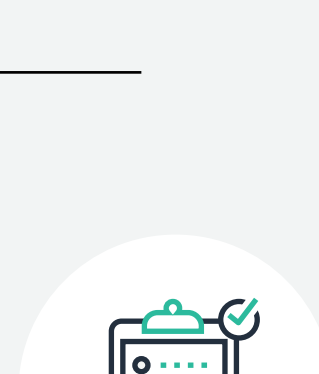


Receive a report showing the source and level of public or shared access of your buckets

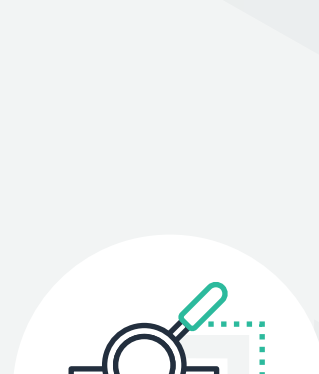


With one click, block all unintended public access to your bucket or drill down for granular levels of access

S3 Inventory



Report on objects by prefix or bucket

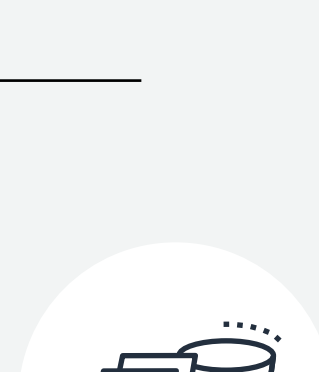


Audit object metadata, including encryption status

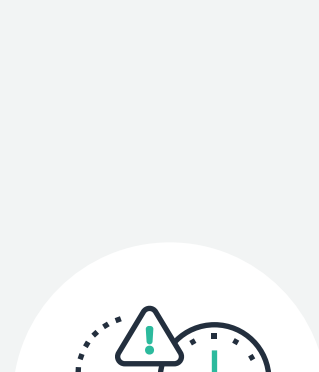


Configure delivery of daily or weekly reports

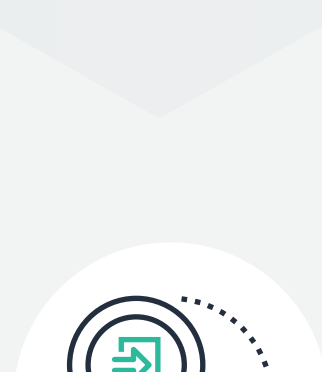
S3 Server Access Logging



Receive detailed records of requests made to a bucket (and store them in S3)

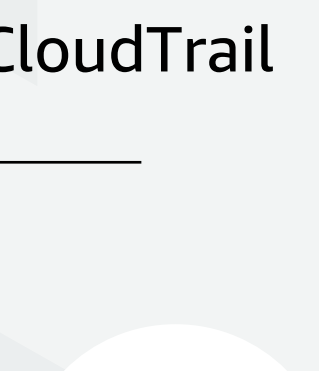


See requester, bucket name, request time, request action, and error code

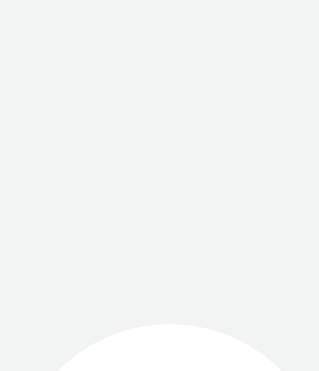


Access log information can be useful in security and access audits

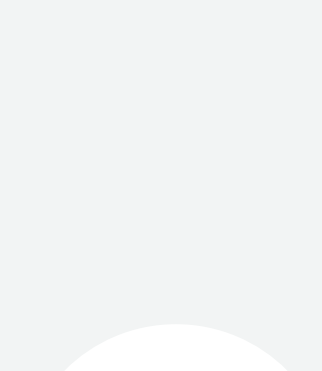
AWS CloudTrail



Reports on actions taken by users, roles, and AWS services



Enable continuous delivery of events or view most recent events on demand

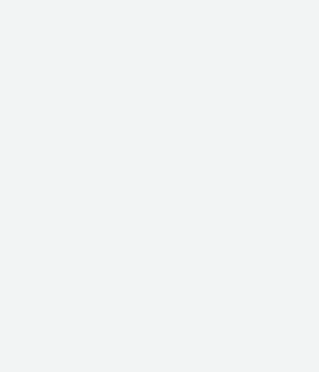


Learn details about an S3 access request, including requester, IP address, time, and error code

S3 Event Notifications



Configure events to occur when changes are made to S3 resources

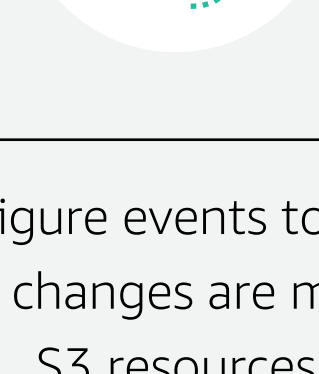


Trigger workflows and alerts, and invoke AWS Lambda

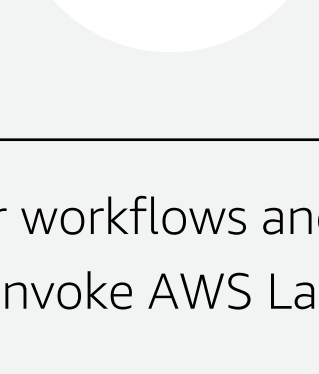


Use with Replication Time Control to get notifications for replication performance

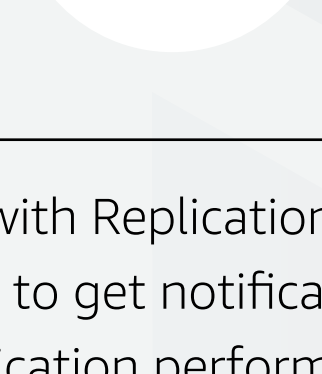
Amazon Macie



Discover, classify, and protect sensitive stored data



Monitor data access patterns for anomalies



Receive alerts when unauthorized access or inadvertent data leaks are detected

Learn more about Amazon S3 security features

https://aws.amazon.com/s3/features/#Access_management_and_security