Cheat Sheet

Advanced Amazon S3 Security

Security guides are often rather basic and superficial. Knowing the least privilege principle is crucial and forms the foundation of security best practices, but following it in practice isn't always straightforward. S3, for example, comes with many different methods to define permissions for buckets and objects. If you define permissions only via IAM roles, you might still have more privileges than required. There are also ACLs and bucket policies, which allow more fine granular access control. Using the right tool for each job is as vital as following the right principles. With this cheat sheet, you have all the options at hand, together with reasons when to use them.

Table of Contents

Access control

In this category, you find S3 features you can use to manage permissions for your buckets and objects.

1 Bucket policies

Bucket policies are one way to set the permissions you want to grant for your S3 buckets. With bucket policies, you specify permissions on the bucket side instead of the account side, as you would do with IAM.

When should you use a bucket policy?

- **Public or cross-account access**
  In cases where you need to define public or cross-account access for a bucket, you might be unable to create an IAM role, and then have to use a bucket policy.
- **Controlling specific actions**
  When you need to control specific actions, such as explicitly denying actions that an IAM role grants. Using bucket policies, you can get away with fewer IAM roles or define more fine-grained access.
- **Bucket-centric access control**
  When you follow a data-centric approach and want to control permissions at the place of usage.

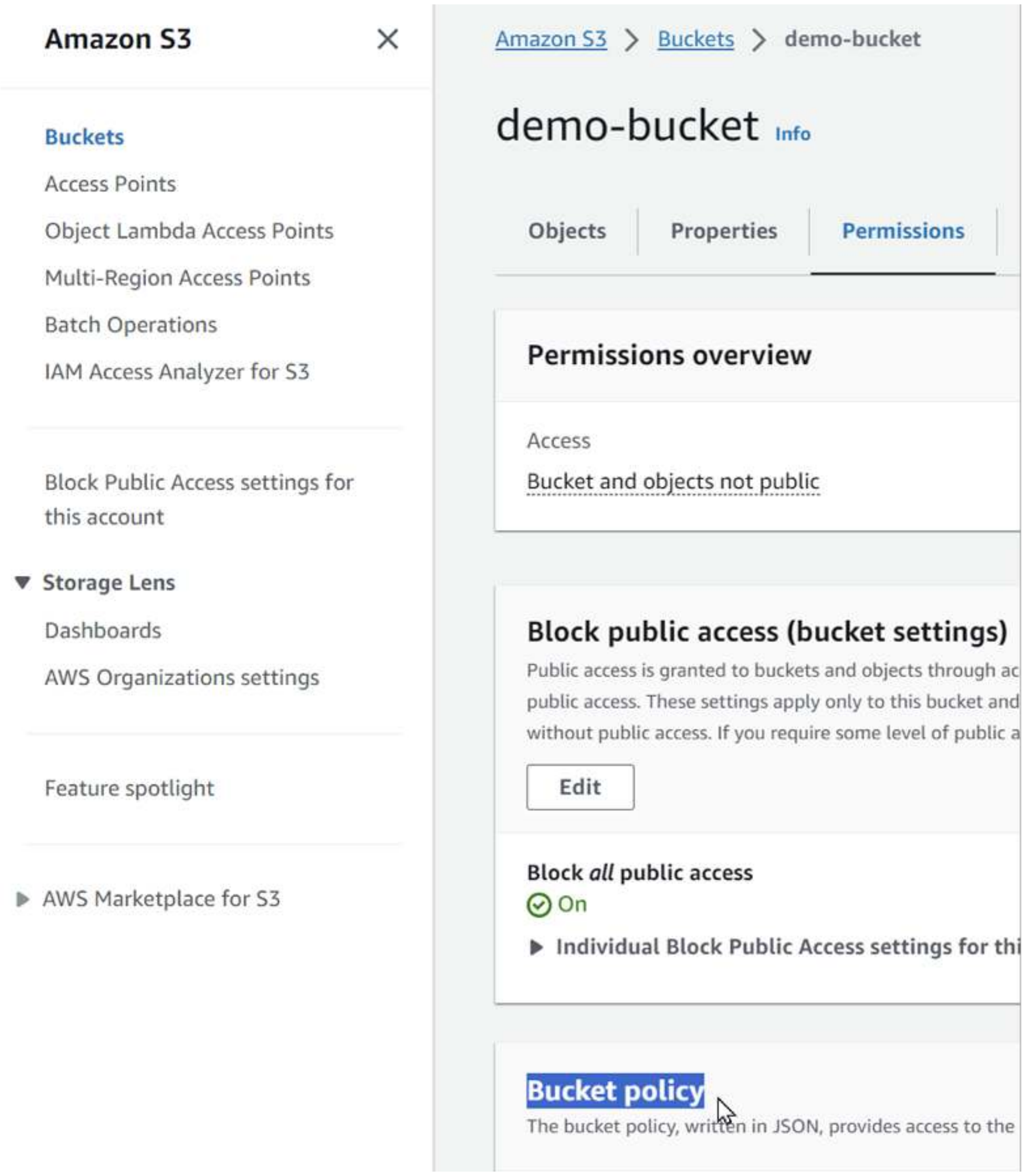
Where do you find bucket policies?

Here are the steps on where you can find the bucket policy of a S3 bucket:

- Go to the AWS console and find “S3 / Buckets.”
- Select the bucket whose permissions you want to adjust.
- Click the “Permissions” tab.
- Now scroll down the page to where you can find the “Bucket Policy” section.

Figure 1 shows the section in the AWS console.

Next page →


Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Amazon S3 > Buckets > demo-bucket
demo-bucket Info
Objects
Properties
Permissions
Edit

Permissions overview

Access
Bucket and objects not public

Block public access (bucket settings)

Public access is granted to buckets and objects through ac
public access. These settings apply only to this bucket and
without public access. If you require some level of public a

Block *all* public access
✓ On

▶ Individual Block Public Access settings for thi

Bucket policy

The bucket policy, written in JSON, provides access to the

Figure 1: Finding the bucket policy of an S3 bucket

Resources

Check out these examples of bucket policies.

2 Access control lists

Access control lists (ACLs) provide you with a way to define your S3 buckets' permissions. With ACLs, you can define fine granular permissions either for the bucket or for individual objects.

When should you use an ACL?

- **Object level access control**
  When you need to define permissions for specific objects, using an ACL is the right choice.

- **Transferring objects with permission between buckets**
  ACL permissions for objects are transferred alongside objects when moved between buckets.

- **Keeping permissions simple**
  ACLs come with simple read/write/list permissions, which makes them easier to define than the complex JSON files required for bucket policies and IAM permissions.

- **Public or cross-account access**
  When you need to define public or cross-account access for a bucket, you might not be able to define an IAM role.

- **Controlling specific actions**
  ACLs come in handy when you need to control specific actions, such as explicitly denying actions that an IAM role granted. ACLs can let you get away with using fewer IAM roles and let you define more fine-grained access.

- **Bucket-centric access control**
  ACLs are preferable if you're following a data-centric approach and want to control permissions at the place of usage.

Where do you find ACLs?

Here are the steps to how to find the ACL for your S3 buckets:

- In the AWS console, look for "S3 / Buckets."
- Select the bucket whose permissions you want to adjust.
- Now go down to the "Permissions" tab and select that.
- Once you're in the permissions menu, scroll down to where you can find the "Access control list (ACL)" section.

Figure 2 shows the section in the AWS console.

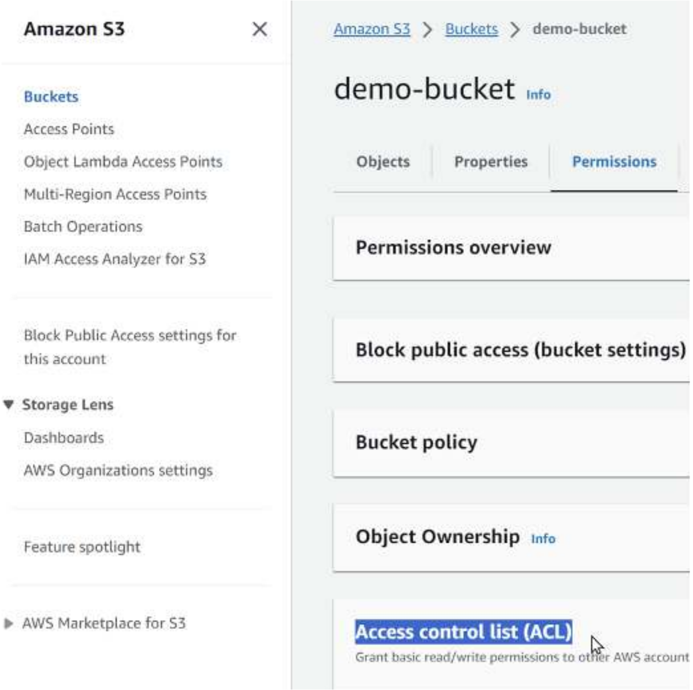

Amazon S3
×
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
▼ Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
▶ AWS Marketplace for S3
Amazon S3 > Buckets > demo-bucket
demo-bucket Info
Objects
Properties
Permissions
Permissions overview
Block public access (bucket settings)
Bucket policy
Object Ownership Info
Access control list (ACL)
Grant basic read/write permissions to other AWS account

Figure 2: Finding the ACL of an S3 bucket

Resources

You can find more details on S3 ACLs here.

3 S3 Access Points

With S3 Access Points, you can define your access rules via a proxy. When you use S3 Access Points, all S3 queries go through a central service that checks permissions.

When should you use an S3 Access Point?

- **Access control for data shared externally**
  When you need to share S3 data outside of your AWS accounts when you don't want to handle ACLs for every potential user.

- **Centralized access management**
  When you need central access management independently of your buckets or IAM roles.

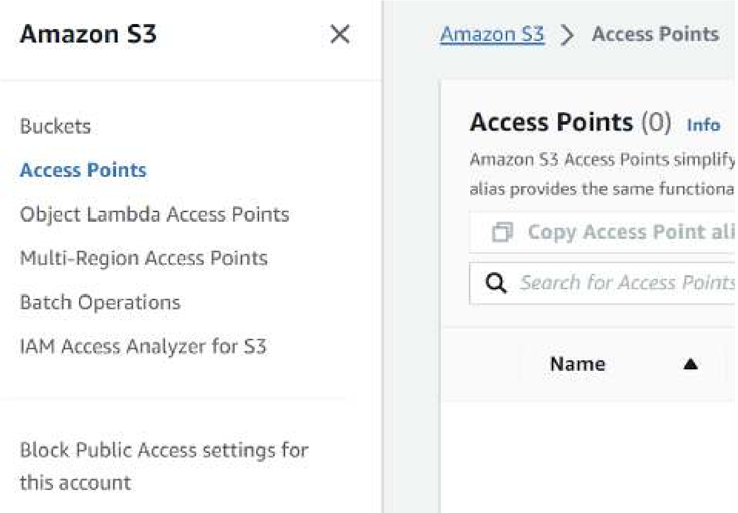
- **Simplified permissions**
  When you don't want to handle complex JSON files that come with bucket policies and IAM roles.

- **Improving usability for external developers**
  When you want an external developer with a single endpoint access to S3 data in multiple buckets or from various regions.

- **Custom functionality**
  When you want to execute Lambda functions where someone is granted specific access to an S3 bucket.

Where do you find S3 Access Points?

You can find S3 Access Points in the AWS console under "S3 / Access Points." Figure 3 shows the section in the AWS console.


Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Amazon S3 > Access Points
Access Points (0) Info
Copy Access Point ali
Search for Access Points
Name ▲

Amazon S3 Access Points simplify
alias provides the same functiona

Figure 3: Finding S3 Access Points

4 VPC endpoints for S3

VPC endpoints can give your Amazon EC2 instances access to S3 buckets without exposing those instances to the public internet.

When should you use VPC endpoints for S3?

- **Private EC2 instances**
  When your private EC2 instances inside a VPC need access to S3 buckets.

Where do you find VPC endpoints for S3?

You can find VPC endpoints in the AWS console under "VPC". When you click "Endpoints," you can create an endpoint for AWS services.

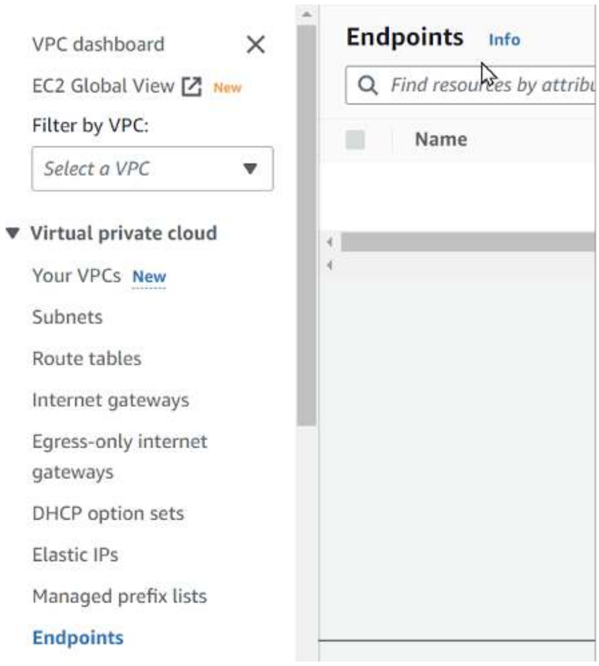


Figure 4: Finding VPC Endpoints

Data durability

In this category, you find S3 features that help you prevent data from being deleted, whether that's caused by simple human error or malicious actors.

1 S3 Object Lock

Object Lock blocks the delete action for a specific object for all users. You can enable it in a particular period after upload or until you explicitly unlock an object again.

When should you use Object Lock?

- **Protecting specific objects**
  When you want to protect your data from deletion at the object level.

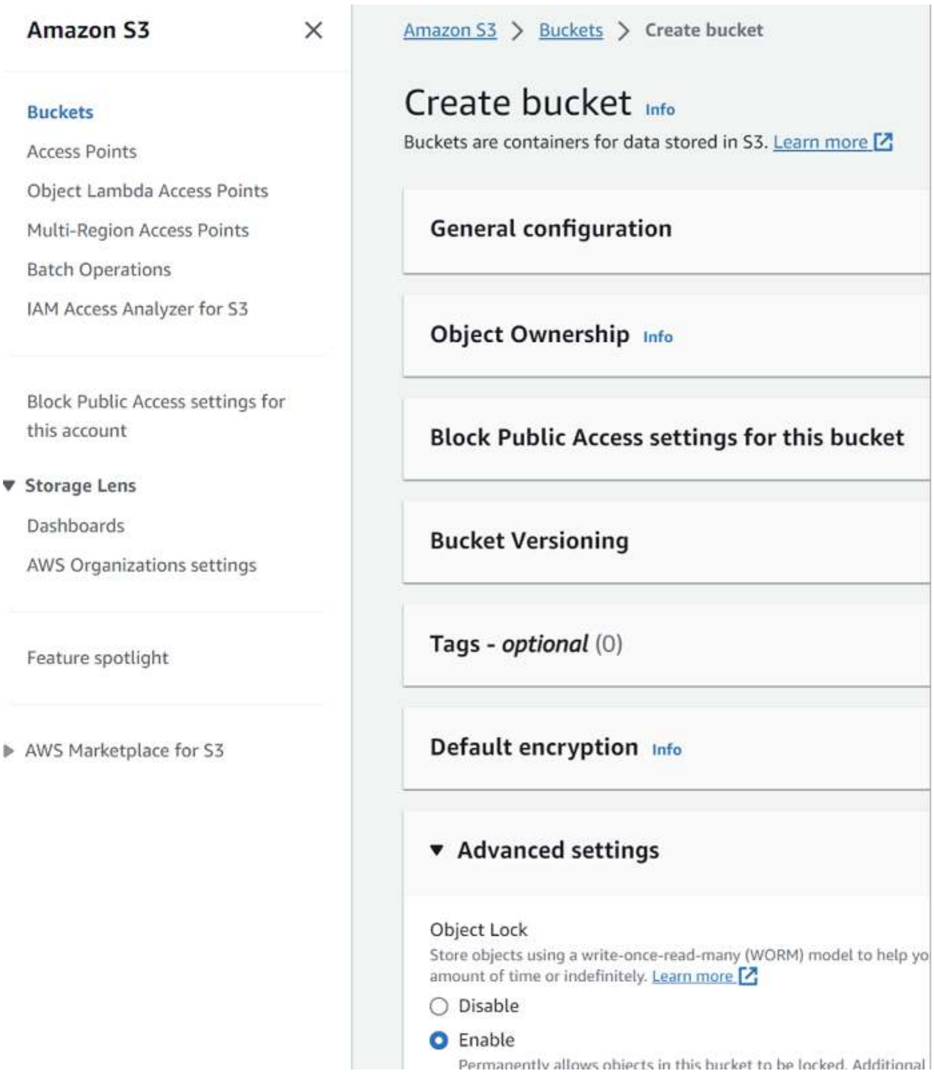
- **Retention for compliance**
  When you must keep data around to comply with particular laws or standards. This will help prevent data from being accidentally deleted, leading to fines.

- **Simple protection**
  When you don't need the whole feature set provided by ACLs and just want to manage who has the item's delete access.

Where do you find Object Lock?

You find Object Lock in the AWS console under "S3 / Buckets" when you create a new bucket. It will be at the bottom of the form under the "Advanced Settings" section. Note that enabling Object Lock for an existing bucket is only possible by contacting AWS support.

Figure 5 shows the location of Object Locking in the AWS console.



Amazon S3 ✕

Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3

Block Public Access settings for this account

▼ Storage Lens
Dashboards
AWS Organizations settings

Feature spotlight

▶ AWS Marketplace for S3

Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3. Learn more

General configuration

Object Ownership Info

Block Public Access settings for this bucket

Bucket Versioning

Tags - *optional* (0)

Default encryption Info

▼ Advanced settings

Object Lock
Store objects using a write-once-read-many (WORM) model to help yo
amount of time or indefinitely. Learn more

○ Disable
● Enable
Permanently allows objects in this bucket to be locked. Additional

Figure 5: Finding S3 Object Locking

2 S3 MFA delete

Another way to prevent accidental data deletion is with multi-factor authentication (MFA) deletion. Using MFA deletion, every user with write access can delete an object, but that action has to be confirmed via MFA first.

When should you use MFA delete?

- **Prevent accidental deletion**
  When the creation of objects is expensive, or the data required to create the object isn't easy to come by, MFA delete can highlight the importance of the object before a user deletes it.

- **Preventing outside attackers from deleting data**
  There is always a chance that a hacker will get access to the AWS credentials. Enabling MFA deletion requirements will prevent the hacker from doing more damage.

Where do you find MFA delete?

Enabling MFA delete is not possible via the AWS console. You must use the AWS CLI from the root user account. To do that you'll also need the bucket name and number from the root account's MFA device.

The following command enables versioning and MFA Delete for an existing bucket:

```
$ aws s3api put-bucket-versioning \
--bucket <BUCKET_NAME> \
--versioning-configuration Status=Enabled,MFADelete=Enabled \
--mfa "SERIAL <MFA_SERIAL_NUMBER>"
```

3 S3 cross-region replication

Cross-region replication can help to prevent data destruction from a region-wide outtake.

When should you use cross-region replication?

- **Disaster recovery**
  When you need to ensure that you can restore replicated objects after they are lost in a primary region.

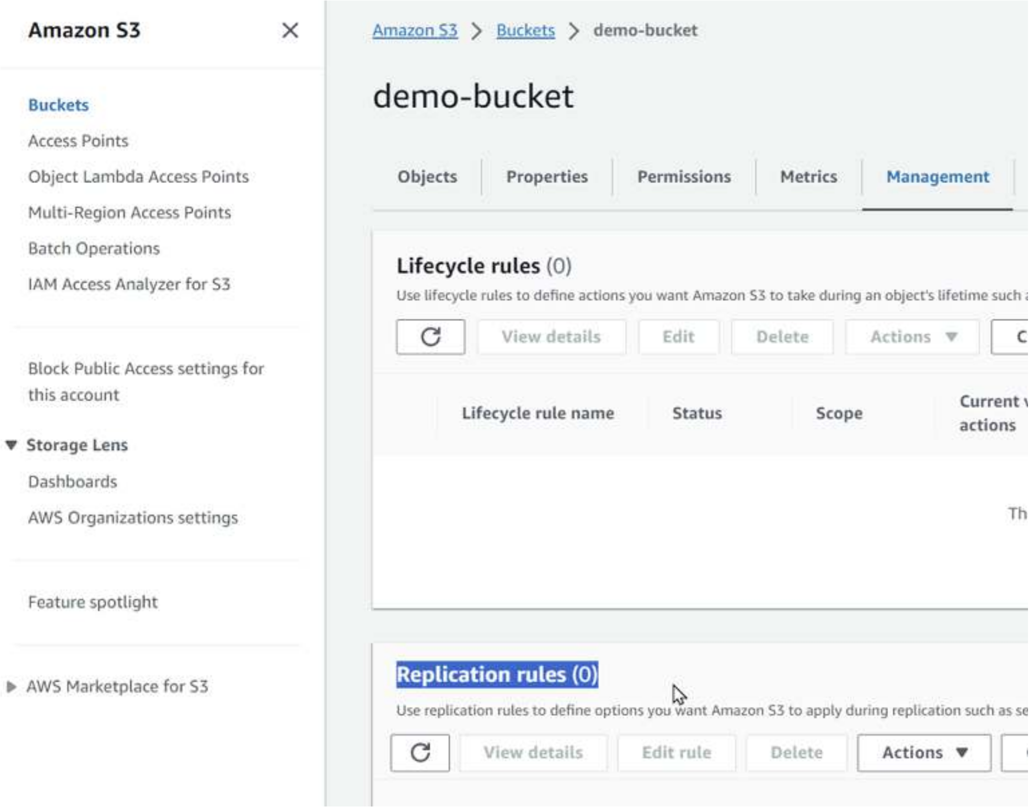
- **Compliance**
  When a law or standard requires you to store data in multiple, disparate locations.

Where do you find cross-region replication?

Here are the steps on how to find cross-region replication:

- Go to the AWS console and find “S3 / Buckets.”
- Select the bucket that you want to replicate across regions.
- Click the “Management” tab for that bucket.
- Go to the “Replication rules” section.
- Go to the “Replication rules” section.
- Here, select cross-region replication.

Figure 6 shows the section in the AWS console.



Use lifecycle rules to define actions you want Amazon S3 to take during an object's lifetime such a

Use replication rules to define options you want Amazon S3 to apply during replication such as se

Figure 6: Finding S3 Cross-Replication

Storage visibility

In this category, you'll find AWS services and S3 features that can provide insights into the data you store.

1 S3 Storage Lens

S3 Storage Lens is an easy way to view your S3 storage usage and activity. Even if you already follow best practices, you need to know what's happening with your data.

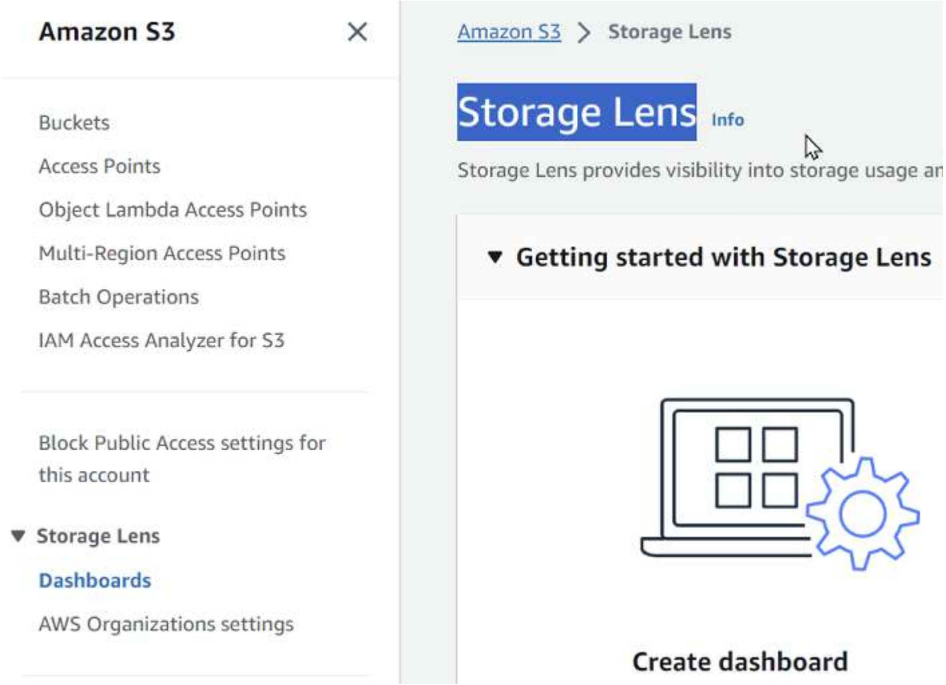
When should you use the Storage Lens?

- **Organization-wide storage visibility**
  When you need a complete view of storage usage and activity over all accounts in your organization.

- **Recommendations**
  When you want automatic recommendations for best practices, you might have missed when creating your buckets.

Where do you find Storage Lens?

Storage Lense is in the AWS console under "S3 / Storage Lense" under "Dashboards". You can see it in Figure 7.


Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
▼ Storage Lens
Dashboards
AWS Organizations settings
Amazon S3 > Storage Lens
Storage Lens
Info
▼ Getting started with Storage Lens
Create dashboard

Storage Lens provides visibility into storage usage an

Figure 7: Finding the S3 Storage Lense

2 S3 event logging

It's possible to log all your S3-related API events with Amazon CloudTrail to know exactly when each action was executed and by whom.

When should you use event logging?

- **Access logging for compliance**
  When a law or standard requires you to know who accessed objects and when exactly that access took place.

- **Finding suspicious access patterns**
  When you want to keep your access controls up-to-date and need constant insight if they still reflect your intentions.

Where do you find event logging?

You can find CloudTrail in the AWS console under "CloudTrail," as it's a service that works with many AWS services, not just S3. In Figure 8, you see the location of CloudTrail in the AWS console.

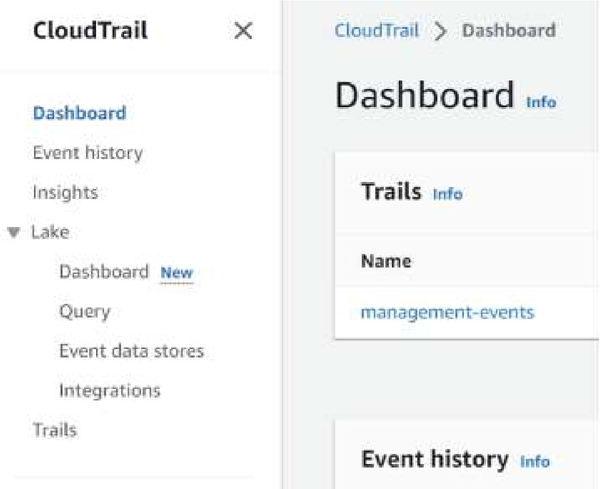


Figure 8: Finding CloudTrail in the AWS console

3 AWS Config

AWS Config scans the configuration of your AWS resources and checks them for issues. This way, you can locate potential security risks in existing resources.

When should you use AWS Config?

- **Compliance**
  When you need to keep your configurations compliant with particular laws or standards.
- **Configuration history**
  When you need to keep a history of all past resource configurations.
- **Automatic remediation**
  When you don't have the personnel to fix all configuration issues manually.

Where do you find AWS Config?

You find AWS Config in the AWS console under "Config."

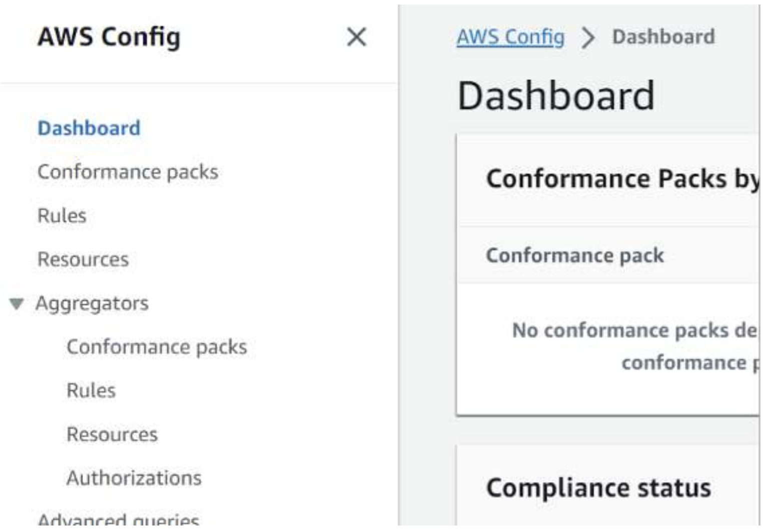


Figure 9: Finding AWS Config

Data loss prevention

In this category, you find S3 features that prevent data leaks by minimizing the sensitive data you keep or show to users.

1 Data masking with Amazon Macie

Amazon Macie is a service that can scan data in AWS for sensitive information. It can trigger Lambda functions that remove or replace fields in S3 objects, effectively masking them so that specific users won't be exposed to that data.

When should you use data masking?

- **Compliance audits**

  When you need to give access to an auditor and you don't want to expose them to all of your data, but object-level access isn't fine-grained enough.

- **Demo data**

  When you need realistic datasets for product demos but don't want them to include sensitive information.

- **Third-party data sharing**

  When you need to share data with customers or business partners but want to filter out confidential information.

Where do you find data masking?

Data masking isn't a feature that S3 or other AWS services provide out of the box, but one way to implement it is with AWS Macie, a Lambda function, and Amazon EventBridge. You can find Amazon Macie in the AWS console under "Macie", AWS Lambda under "Lambda," and Amazon EventBridge under "EventBridge."

Using EventBridge is required since Macie can't trigger Lambda functions directly. Check out this guide on how to set up EventBridge with Macie.

2 S3 lifecycle rules

Lifecycle rules are automated data modification rules for S3 buckets. They move objects into cheaper storage tiers, add delete markers, or delete them permanently.

When should you use lifecycle rules?

- **Automatic pruning**

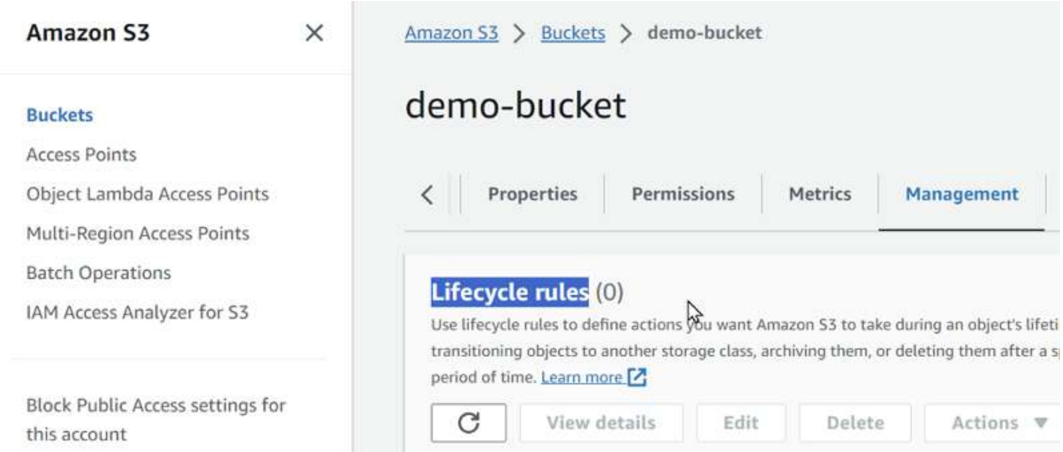
  When you need sensitive data for a short period but want to ensure it gets deleted later.

- **Compliance**

  When you must keep data for a long time, but it doesn't need to be accessible immediately.

Where do you find lifecycle rules?

Find the lifecycle rules in the AWS console under "S3 / Buckets." Select one of your buckets, and click the "Management" tab.


Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Amazon S3 > Buckets > demo-bucket
demo-bucket
Properties
Permissions
Metrics
Management
Lifecycle rules (0)
View details
Edit
Delete
Actions

Use lifecycle rules to define actions you want Amazon S3 to take during an object's lifeti transitioning objects to another storage class, archiving them, or deleting them after a s period of time. Learn more

Figure 10: Finding S3 Lifecycle Rules

Get more security for AWS S3 deployments with Wiz

If managing the minutiae of your S3 deployment seems like a lot of work, there is a way to make it easier and faster to narrow down the security vulnerabilities in your system with the help of Wiz.