



Configuring Amazon S3 security settings and access controls

Getting started at an AWS hosted workshop

▼ S3 Security Best Practices

▼ Prepare Your Lab

Attach IAM Role to EC2 Instance

Connect to the EC2 Instance

Bucket Name

▼ Lab 1 - S3 Security Exercises

Require HTTPS

Require SSE-KMS Encryption

Restrict Access to an S3 VPC Endpoint

Use AWS Config Rules to Detect a Public Bucket

[Use Amazon Access Analyzer for S3](#)

► Lab 2 - S3 Access Grants

► Lab 3 - Enabling Malware Protection for S3 by using GuardDuty

► Lab 4 - S3 Access Control Lists

Lab Summary

[Configuring Amazon S3 security settings and access controls](#) > [S3 Security Best Practices](#) > [Lab 1 - S3 Security Exercises](#)

Use Amazon Access Analyzer for S3

It is best practice to secure your AWS account and resources with least-privilege permissions.

IAM Access Analyzer helps you identify the resources in your organization and accounts, such as Amazon S3 buckets, shared with an external entity including public access. This lets you identify unintended access to your resources and data, which is a security risk.

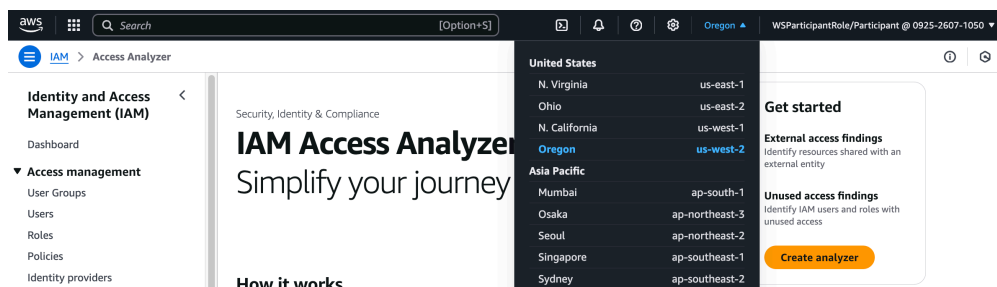
Earlier in this lab, we showed how to use AWS config to detect a public S3 bucket by selecting a specific rule to review when a configuration change has occurred.

In this exercise, we will show how IAM Access Analyzer and IAM Access Analyzer for S3 will help you identify a public bucket, evaluate and remediate to ensure you can follow best practices in achieving least privilege with your permissions management.

From the AWS console in the top search bar, search and select IAM.

Click Access Analyzer.

Ensure you are in **us-west-2 (Oregon)** region, then click Create analyzer



Leave the defaults and click Create analyzer at the bottom of the page. It may take around 2 to 3 minutes until you should see the Active Findings begin to populate.

Select Access Analyzer > External Access look for the S3 Bucket sid-security-xxxxx. You can filter using the **Active findings** search bar by typing S3 and selecting the Resource Type: AWS:S3:Bucket in the popup and pressing enter.

External access [Info](#)

Analyzer [Manage analyzer](#)

Last scan: Now

ExternalAccess-ConsoleAnalyzer-60b06fc1-c811-4a0e-856d-a85cc3d37b25
Zone of trust: Current account (092526071050)

Findings (3) [Refresh](#) [Actions](#)

Status

Active

<input type="checkbox"/>	Finding ID	Resource	External ...	Condition	Shared th...	Access level	Resour...
<input type="checkbox"/>	9c869201-cc3e-4834-99a7-ce...	sid-security-ca5 S3 Bucket	All Princip...	-	Bucket po...	Read	Not applica...
<input type="checkbox"/>	704fcaea-cf58-45d0-afbe-dde...	WSSystemRole IAM Role	AWS Account 48465458...	-	-	Write	Not applica...
<input type="checkbox"/>	34d0d140-a8e8-40e8-8209-3...	WSOpsRole IAM Role	AWS Account 48465458...	-	-	Write	Not a...

Notice All Principals have Access Level Read. This is because in the prior AWS Config exercise we modified the S3 bucket policy to allow public read to a the text01 object.

From the AWS console in the top search bar, search and select S3.

Click IAM Access Analyzer for S3

Your screen should look similar to the following.

The screenshot shows the IAM Access Analyzer for S3 console. At the top, it says "IAM Access Analyzer for S3" with an "Info" link. Below this, there's a summary of findings: "1 buckets are configured to allow access to anyone on the internet or any other AWS users. Review this risky configuration immediately". A yellow banner contains a warning icon and the text: "1 buckets are configured to allow access to anyone on the internet or any other AWS users. Review this risky configuration immediately. Explore other Regions to identify other buckets in your account that may also be at risk." Below the banner, there's a section titled "Buckets with public access (1)" with a warning icon. It explains that these buckets can be accessed by anyone on the internet. To the right of this section are buttons: "View findings", "Mark as active", "Archive", and "Block all public access". Below this is a table with columns: "Bucket name", "Discovered by Access Analyzer", "Shared through", "Status", and "Access...". The table has one row with the bucket name "sid-security-98bcb700-66f1-11ee-9b81-06f...", discovered "a minute ago", with a "Bucket policy", status "Active", and access level "Read".

Notice there is 1 bucket that allows access to anyone on the internet. Let's fix that.

Select Buckets on the left hand side navigation

- Click the bucket name starting with sid-security-xxxxxxx.
- Click Permissions.
- Under Bucket Policy click Delete
- Type delete and click Delete to confirm.

This will remove the bucket policy that is allowing public access to objects within our bucket.

From the AWS console in the top search bar, search and select IAM.

Click Access Analyzer > External Access.

Ensure you are in us-west-2 (Oregon) region.

Under Active Findings look for the S3 Bucket sid-security-xxxxx. You may need to refresh the page. Click on the Finding ID for the S3 bucket.

The screenshot shows the IAM Access Analyzer console with the finding details for the bucket "sid-security-98bcb700-66f1-11ee-9b81-06f...". The finding ID is "9c869201-cc3e-4834-99a7-ce523a3346aa". A yellow banner contains a warning icon and the text: "Public: this finding is for a resource that allows public access." Below this is a table with columns: "Details", "External principal", "Resource control policy (RCP)", and "Access level". The "Details" column contains: "Finding ID: 9c869201-cc3e-4834-99a7-ce523a3346aa", "Resource: arn:aws:s3:::sid-security-ca51ea00-acec-11ef-ab19-02dc4668901f", and "Resource owner account: 092526071050". The "External principal" column contains: "All Principals", "Condition: -", and "Shared through: -". The "Resource control policy (RCP)" column contains: "restriction: Not applicable", "Updated: a few seconds ago", and "Status: Active". The "Access level" column contains: "Read" and "s3:GetObject".

Click Rescan on the right. You may need wait 2 to 3 minutes and refresh the page. The status will change to resolved. Your screen should look similar to the following.

IAM > Access Analyzer > External access > Finding details

9c869201-cc3e-4834-99a7-ce523a3346aa Info

Rescan

Details

Finding ID

9c869201-cc3e-4834-99a7-ce523a3346aa

Resource

arn:aws:s3:::sid-security-ca51ea00-acec-11ef-ab19-02dc4668901f

Resource owner account

092526071050

External principal ()

All Principals

Condition

-

Shared through

-

Resource control policy (RCP) restriction

Not applicable

Updated

a few seconds ago

Status

Resolved

The access is no longer allowed

Access level

Read

s3:GetObject

You have successfully used IAM Access Analyzer to identify a public S3 bucket, mitigate its public access by removing the bucket policy allowing bucket access and verified using Access Analyzer to confirm the bucket is no longer public.

Lab complete

Congratulations you have completed the S3 security exercises lab. In this lab, you learned how to grant and restrict permissions to your S3 buckets with S3 bucket policies. Use AWS Config and Access Analyzer to detect buckets within your account and organization that have public access, and remediate public access where unintended.

Previous

Next

https://catalog.us-east-1.prod.workshops.aws/workshops/8f6b34da-c21e-4094-8070-8d98e2e6ca08/en-US/s3-security-best-practices-lab/01-securityexercises/05-... 3/3