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.

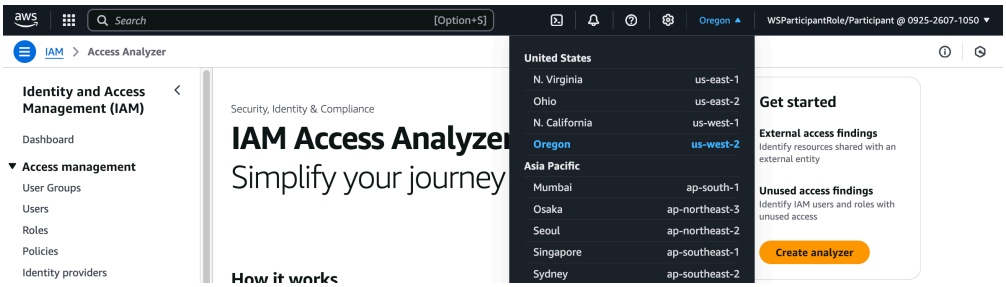
Earlier in this lab, we showed how to use AWS config to detect a public S3 bucket by selecting a specific rule to review when a configuration change has occurred.

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`.

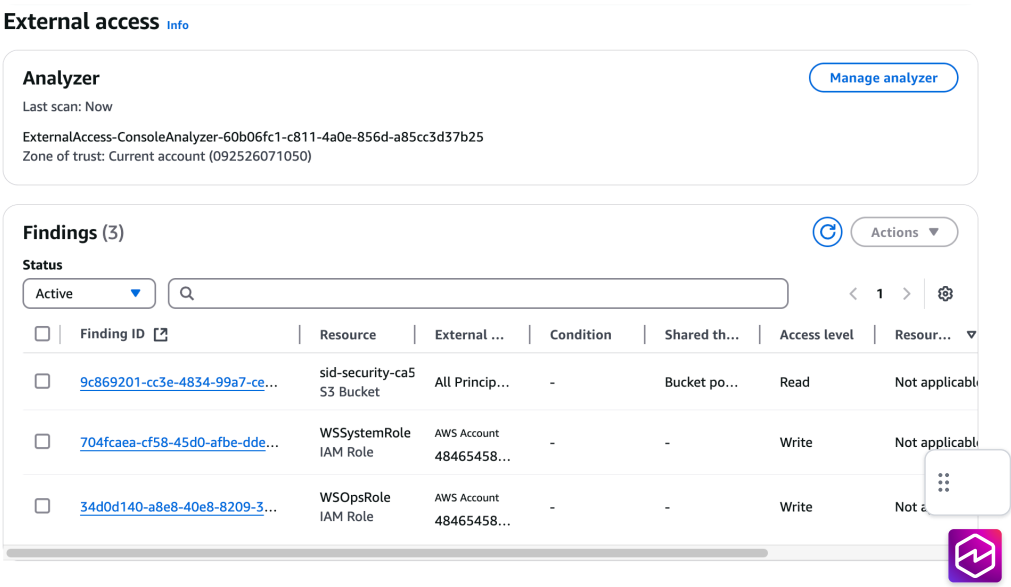
Click `Access Analyzer`.

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`.

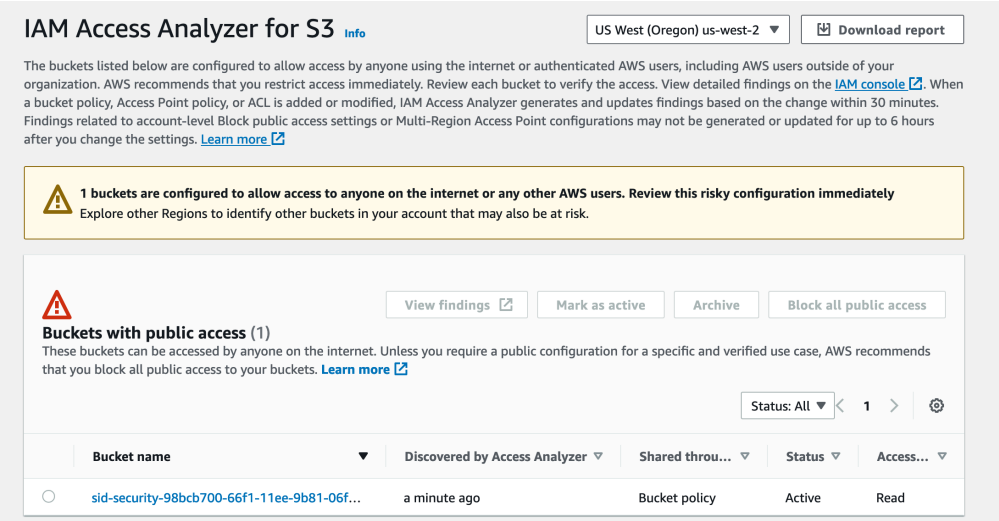


Notice All Principals have Access Level Read. This is because in the prior AWS Config exercise we modified the S3 bucket policy to allow public read to a the text01 object.

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.



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-xxxxxxxx`.
- Click `Permissions`.
- Under `Bucket Policy` click `Delete`
- Type `delete` and click `Delete` to confirm.

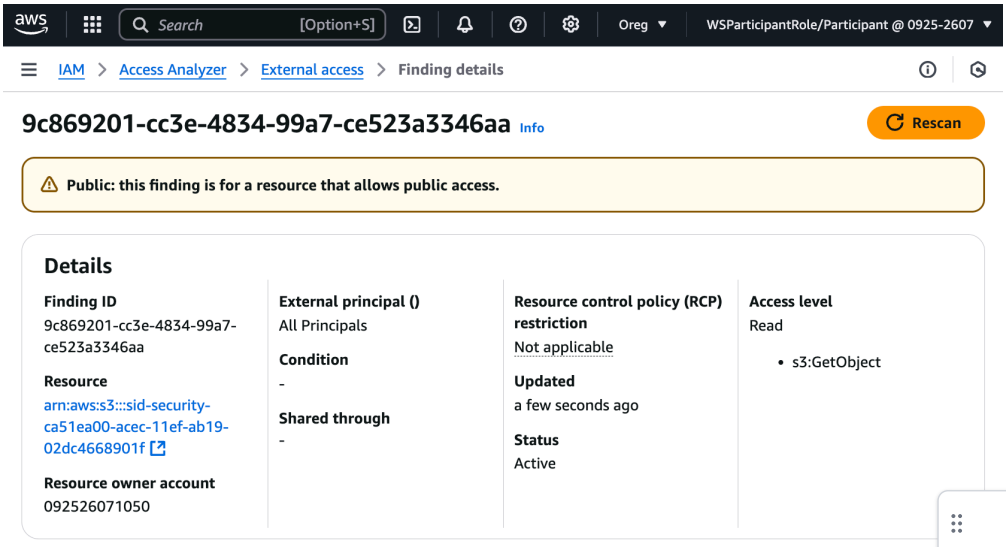
This will remove the bucket policy that is allowing public access to objects within our bucket.

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

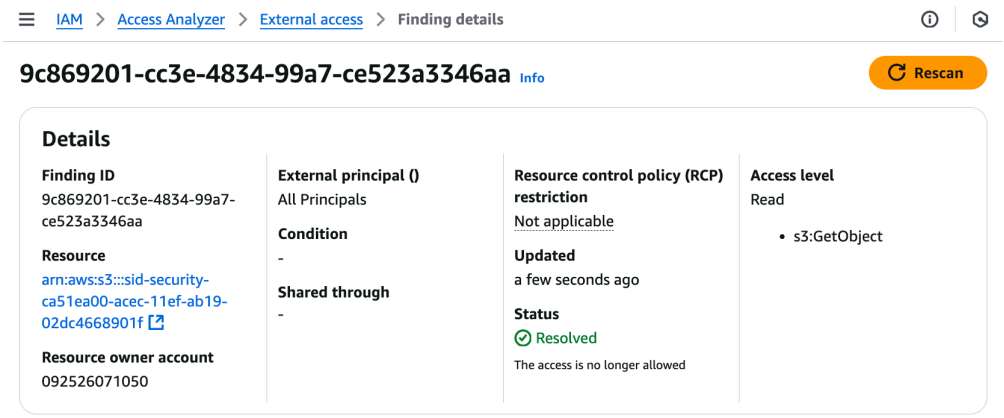
Click `Access Analyzer` > `External Access`.

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.



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.



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