

[illegible]

Name	IAM Access Analyzer
URL	https://attackdefense.com/challengedetails?cid=2471
Type	AWS Cloud Security : Defense

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

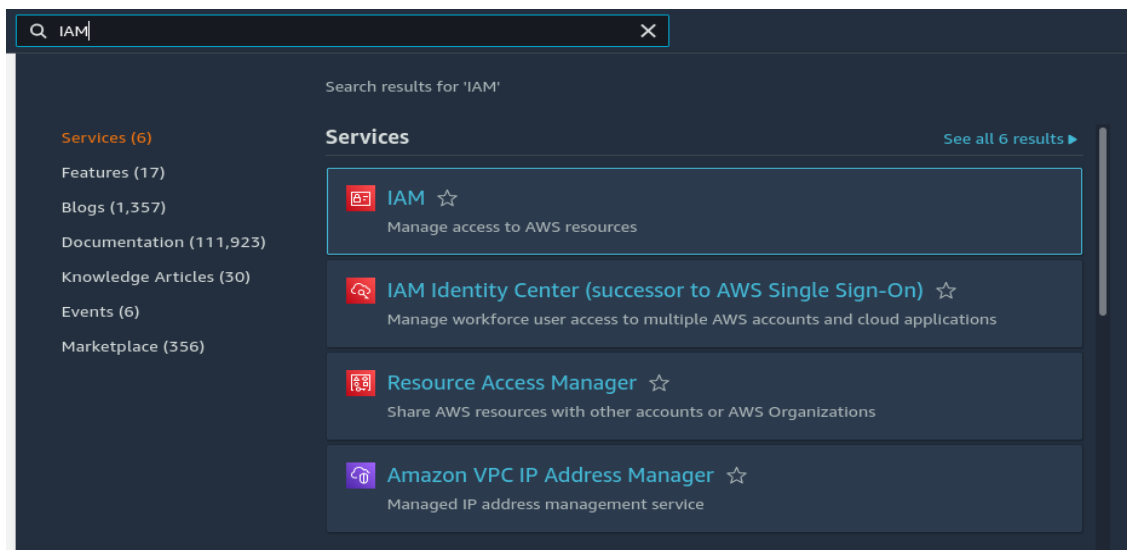
Solution:

Step 1: Click the lab link button to get access credentials. Login to the AWS account with these credentials.

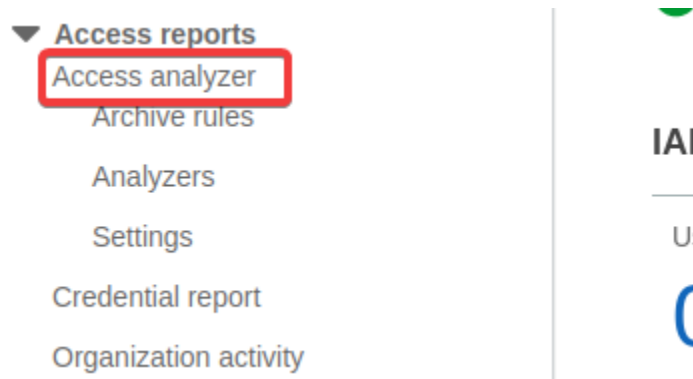
Access Credentials to your AWS lab Account

Login URL	https://210855491654.signin.aws.amazon.com/console
Region	US East (N. Virginia) us-east-1
Username	david
Password	Ad5OQyVG5mBCgbei

Step 2: Search for “IAM” and navigate to the IAM dashboard.



Step 3: Click on “Access analyzer” from the access reports.



Step 4: Click on “Create analyzer”.

Create analyzer

Step 5: Set everything as default and click on “Create analyzer”.

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

[IAM](#) > [Access Analyzer](#) > Create analyzer

Create analyzer [Info](#)

The analyzer scans the resources within the zone of trust.

Region

US East (N. Virginia)

You should enable Access Analyzer in each Region where you use AWS resources.

Name

ConsoleAnalyzer-978c9776-731a-4e3f-86c4-18a03d6704fc

Maximum 255 characters

Zone of trust [Info](#)

Policies for all supported resources within your zone of trust are analyzed to identify access allowed from outside the zone of trust.

Current account (210855491654)



Tags [Info](#)

Optionally, add tags to the analyzer. Tags are words or phrases that act as metadata for identifying and organizing your AWS resources. Each tag consists of a key and one optional value.

No tags associated with the resource.

Add tag

You can add up to 50 tags.

 When you enable Access Analyzer, a service-linked role is created in the current account. The service-linked role grants permission to Access Analyzer to interact with AWS resources on your behalf. [Learn more](#) 

Cancel

Create analyzer

After the successful creation of an access analyzer, it identifies resources shared with external principals by using logic-based reasoning to analyze the resource-based policies in your AWS environment and list them as findings in the active findings table.

Step 6: Click on “Finding ID” of the resource “Secret”. This will list details about the finding.

<input type="checkbox"/>	Finding ID	Resource	External principal	Condition	Shared through
<input type="checkbox"/>	32170698-9ae4-4aa...	Secret account-Uu6Tvt	AWS Account 002763723555	-	-
<input type="checkbox"/>	c673cc58-90f4-480c...	S3 Bucket lab-zone-21085549...	All Principals	-	Bucket policy
<input type="checkbox"/>	1fb7c1b2-33bc-4093...	S3 Bucket lab-bucket-ip-2108...	All Principals	Source IP 103.149.159.22/	Bucket policy
<input type="checkbox"/>	b5400d88-4d88-409...	IAM Role TheOracle	AWS Account 719592403832	-	-
<input type="checkbox"/>	3b306705-ce94-413...	IAM Role TheOracle	AWS Account 002763723555	-	-
<input type="checkbox"/>	ecf2469d-1c2f-4477-...	IAM Role ad_role	All Principals	-	-
<input type="checkbox"/>	077a5e86-278f-4abd...	KMS Key aa94d1bb-5f4e-48...	AWS Account 002763723555	-	-

This finding informs that the resource has been shared with an external AWS account having an id 002763723555.

32170698-9ae4-4aab-9eba-3abab927aa11 [Info](#)

Details

Finding ID 32170698-9ae4-4aab-9eba-3abab927aa11	Updated 2 minutes ago	Status Active
Resource arn:aws:secretsmanager:us-east-1:210855491654:secret:account-Uu6Tvt ↗	External principal (AWS Account) 002763723555	Condition -
Resource owner account 210855491654		

This page also includes information about the access and the external principal granted to it.

Access level

Write

- secretsmanager:CancelRotateSecret
- secretsmanager>DeleteSecret
- secretsmanager:RemoveRegionsFromReplication
- secretsmanager:ReplicateSecretToRegions
- secretsmanager:RestoreSecret
- secretsmanager:RotateSecret
- secretsmanager:StopReplicationToReplica
- secretsmanager:UpdateSecret
- secretsmanager:UpdateSecretVersionStage

Permissions

- secretsmanager>DeleteResourcePolicy
- secretsmanager:PutResourcePolicy
- secretsmanager:ValidateResourcePolicy

Read

- secretsmanager:DescribeSecret
- secretsmanager:GetResourcePolicy
- secretsmanager:ListSecretVersionIds
- secretsmanager:UntagResource

Tagging

- secretsmanager:TagResource

Step 7: Right click on the resource arn and open the link in the new tab. This will make it easier to switch back to the analyzer dashboard.

Resource

[arn:aws:secretsmanager:us-east-1:210855491654:secret:account-Uu6Tvt](#)

Resource owner account

210855491654

External principal (AWS Account)

002763723555

Step 8: Navigate to the “Resource permissions” and check out the resource policy.

In this resource-based policy, the IAM element Effect specifies whether the statement results in allow or an explicit deny. The IAM Action element defines the actions that are performed with

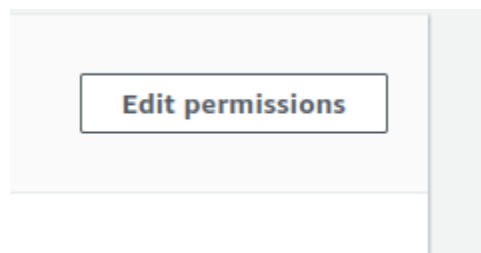
the secret. The IAM Resource element is the secret that the policy is attached to. The IAM Principal element specifies the user with access to perform actions with the secret.

This policy grants full access to the secret for the two AWS accounts. Remove the external AWS account arn and keep the one which having an arn of this account.

Resource permissions - optional [Info](#)
Add or edit a resource policy to access secrets across AWS accounts.

```
1 {  
2   "Version" : "2012-10-17",  
3   "Statement" : [ {  
4     "Sid" : "EnableAnotherAWSAccountToReadTheSecret",  
5     "Effect" : "Allow",  
6     "Principal" : {  
7       "AWS" : [ "arn:aws:iam::002763723555:root", "arn:aws:iam::210855491654:root" ]  
8     },  
9     "Action" : "secretsmanager:*",  
10    "Resource" : "*"   
11  } ]  
12 }
```

Click on “Edit permissions”.



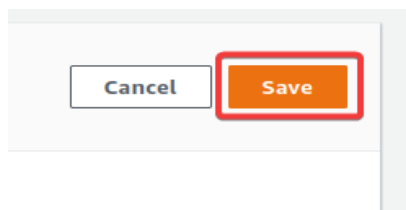
Remove the external AWS account arn from principal.

Resource permissions - optional [Info](#)

Add or edit a resource policy to access secrets across AWS accounts.

```
1 {  
2   "Version" : "2012-10-17",  
3   "Statement" : [ {  
4     "Sid" : "EnableAnotherAWSAccountToReadTheSecret",  
5     "Effect" : "Allow",  
6     "Principal" : {  
7       "AWS" : [ "arn:aws:iam::210855491654:root" ]  
8     },  
9     "Action" : "secretsmanager:*",  
10    "Resource" : "*"   
11  } ]  
12 }
```

Click on "Save".



Now the access to the secret is only allowed for the current account. Now switch back to the tab which has an access analyzer dashboard.

Step 9: On the finding page, Click on the "Rescan" button to run a scan again in this particular resource.





ured through

If the resource is no longer shared outside of your zone of trust, the status of the finding is changed to Resolved. The finding is no longer displayed in the Active findings table, and instead

is displayed in the Resolved findings table. Now , the access is removed, the status changed to Resolved.

32170698-9ae4-4aab-9eba-3abab927aa11 [Info](#)

Details

Finding ID 32170698-9ae4-4aab-9eba-3abab927aa11	Updated a few seconds ago	Status  Resolved The access is no longer allowed
Resource arn:aws:secretsmanager:us-east-1:210855491654:secret:account-Uu6Tvt 	External principal (AWS Account) 002763723555	Condition -
Resource owner account 210855491654		

Step 10: Click on “Finding ID” of the resource “S3 Bucket” which has a name that starts with “lab-zone”.


<input type="checkbox"/>	Finding ID	Resource	External principal	Condition	Shared through
<input type="checkbox"/>	c673cc58-90f4-480c...	S3 Bucket lab-zone-21085549...	All Principals	-	Bucket policy
<input type="checkbox"/>	1fb7c1b2-33bc-4093...	S3 Bucket lab-bucket-ip-2108...	All Principals	Source IP 103.149.159.22/...	Bucket policy
<input type="checkbox"/>	b5400d88-4d88-409...	IAM Role TheOracle	AWS Account 719592403832	-	-
<input type="checkbox"/>	3b306705-ce94-413...	IAM Role TheOracle	AWS Account 002763723555	-	-
<input type="checkbox"/>	ecf2469d-1c2f-4477-...	IAM Role ad_role	All Principals	-	-
<input type="checkbox"/>	077a5e86-278f-4abd...	KMS Key aa94d1bb-5f4e-48...	AWS Account 002763723555	-	-

Step 11: Right click on the resource arn and open the link in the new tab. This will navigate to the S3 dashboard.

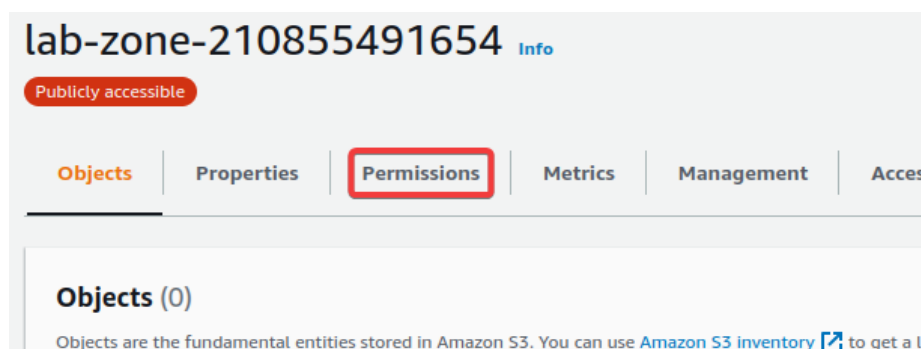
c673cc58-90f4-480c-823e-849d7c6fa20f [Info](#)

 Public: this finding is for a resource that allows public access.

Details

Finding ID c673cc58-90f4-480c-823e-849d7c6fa20f	Updated 9 minutes ago	Status Active
Resource arn:aws:s3:::lab-zone-210855491654 	External principal All Principals	Condition -
Resource owner account 210855491654		

Step 12: Click on Permissions.




lab-zone-210855491654 [Info](#)

Publicly accessible

[Objects](#) | [Properties](#) | **[Permissions](#)** | [Metrics](#) | [Management](#) | [Access](#)

Objects (0)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#)  to get a l

Notice the permissions overview section. The access of this bucket is public.

Permissions overview

Access

 Public

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or a this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Edit

Block all public access

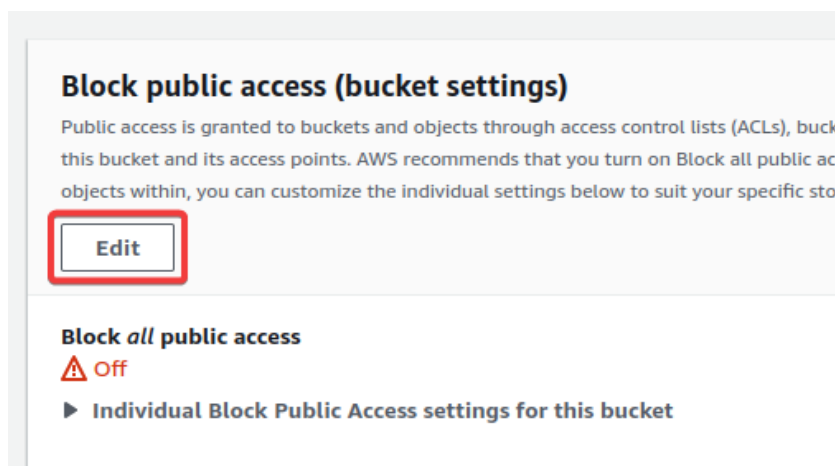
 Off

A bucket policy is a resource-based policy that you can use to grant access permissions to your bucket and the objects in it. Only the bucket owner can associate a policy with a bucket. The permissions attached to the bucket apply to all of the objects in the bucket that are owned by the bucket owner.

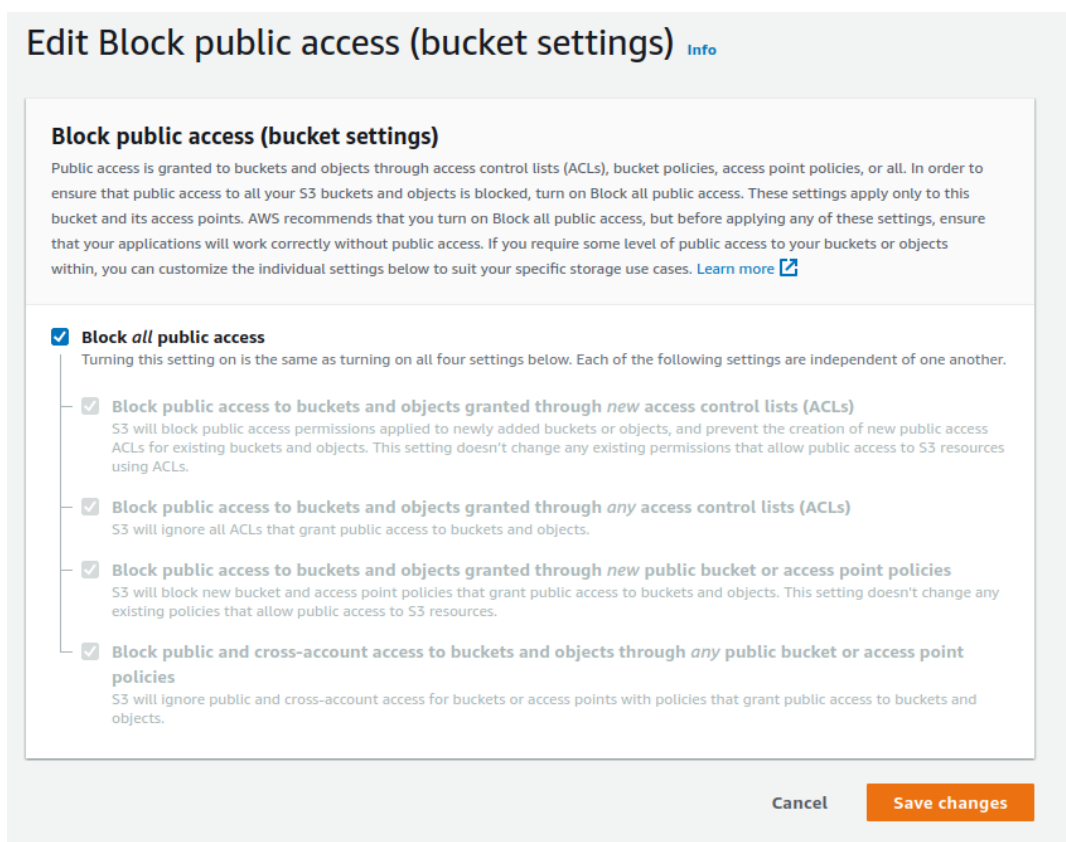
The following policy grants the Read, Write, List permission to any public anonymous users.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "s3:PutObject",
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::lab-zone-210855491654/*",
        "arn:aws:s3:::lab-zone-210855491654"
      ]
    }
  ]
}
```

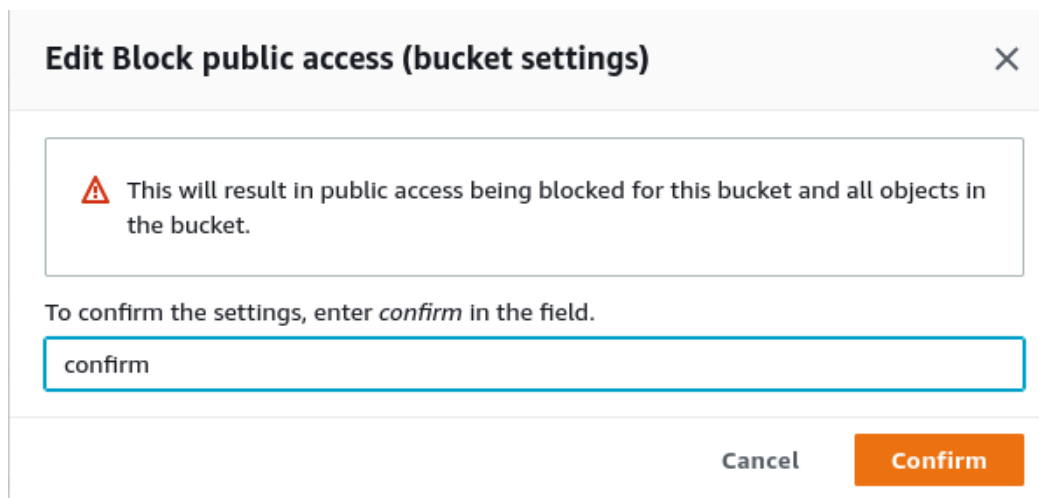
Step 13: Click on “Edit” under block public access.



Step 14: Block all public access by checking the box and click on “Save changes”.



Step 15: Enter “confirm” and save the settings.



Edit Block public access (bucket settings) ✕

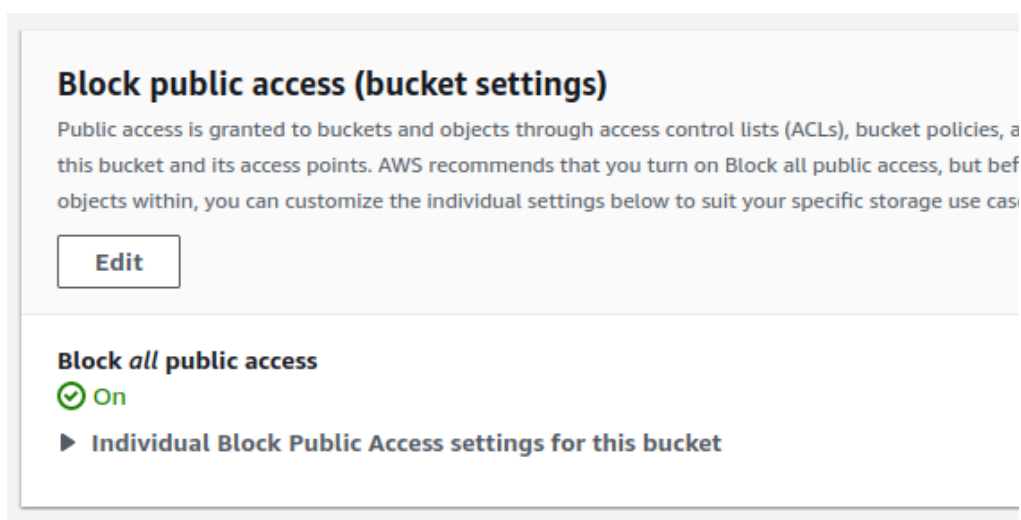
⚠ This will result in public access being blocked for this bucket and all objects in the bucket.

To confirm the settings, enter *confirm* in the field.

confirm

Cancel Confirm

All public access to the bucket is blocked.



Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, and access points. AWS recommends that you turn on Block all public access, but before you turn on Block all public access, you can customize the individual settings below to suit your specific storage use case.

Edit

Block all public access

✔ On

► Individual Block Public Access settings for this bucket

Switch to the tab which has an access analyzer dashboard.

Step 16: On the finding page, Click on the “Rescan” button to run a scan again in this particular resource.



 Feedback


 Rescan

shared through

bucket policy

The access is removed, the status changed to Resolved.

849d7c6fa20f [Info](#)

<p>Updated</p> <p>a few seconds ago</p>	<p>Status</p> <div data-bbox="1036 1129 1227 1192"> Resolved</div> <p>The access is no longer allowed</p>
<p>External principal</p> <p>All Principals</p>	<p>Condition</p> <p>-</p>

Step 17: Click on “Finding ID” of the resource “S3 Bucket” which has a name that starts with “lab-bucket-ip”.

<input type="checkbox"/>	Finding ID	Resource	External principal	Condition
<input type="checkbox"/>	1fb7c1b2-33bc-4093...	S3 Bucket lab-bucket-ip-2108...	All Principals	Source IP 103.14
<input type="checkbox"/>	b5400d88-4d88-409...	IAM Role TheOracle	AWS Account 719592403832	-
<input type="checkbox"/>	3b306705-ce94-413...	IAM Role TheOracle	AWS Account 002763723555	-
<input type="checkbox"/>	ecf2469d-1c2f-4477-...	IAM Role ad_role	All Principals	-
<input type="checkbox"/>	077a5e86-278f-4abd...	KMS Key aa94d1bb-5f4e-48...	AWS Account 002763723555	-

Step 18: Right click on the resource arn and open the link in the new tab. This will navigate to the S3 dashboard.

1fb7c1b2-33bc-4093-a08a-b604c78d70b2 [Info](#)

Details

Finding ID
1fb7c1b2-33bc-4093-a08a-b604c78d70b2

Updated
18 minutes ago

Status
Active

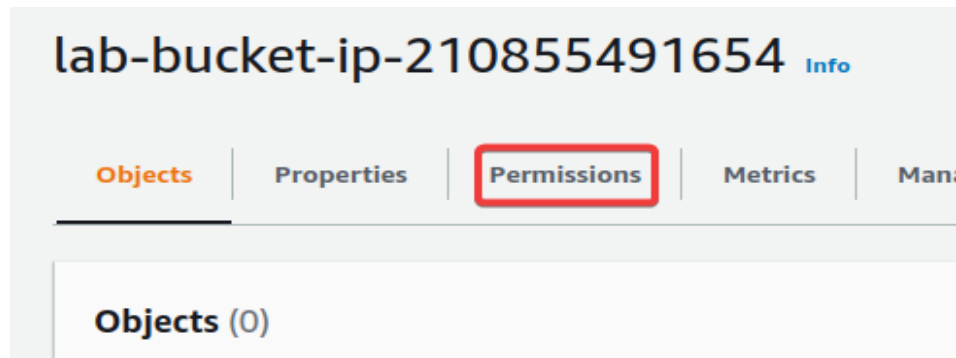
Resource
[arn:aws:s3:::lab-bucket-ip-210855491654](#) [🔗](#)

External principal
All Principals

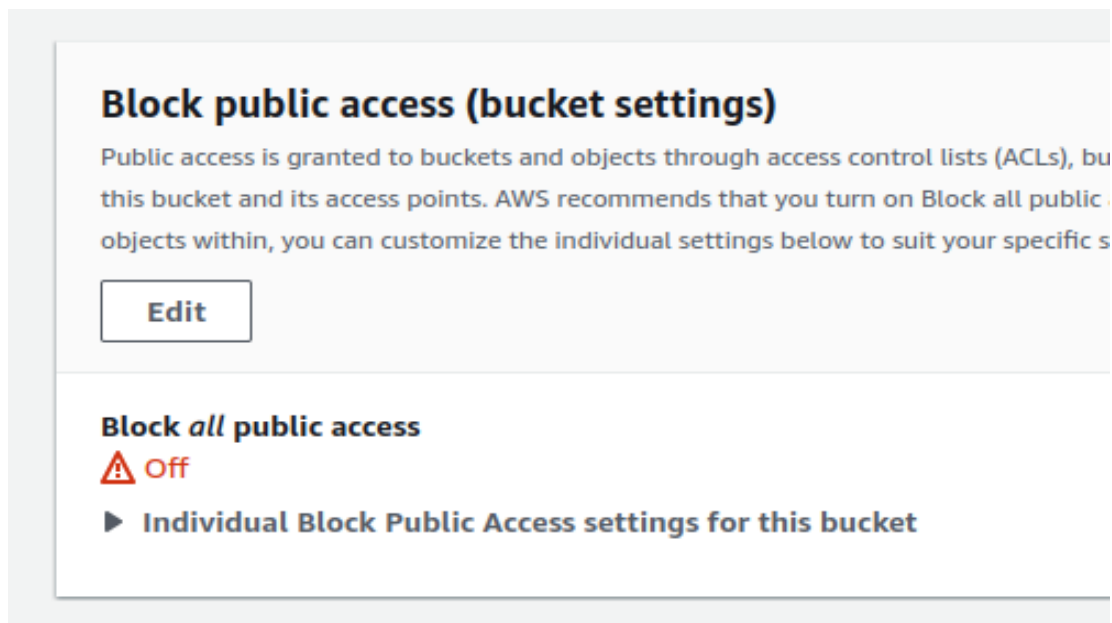
Condition
Source IP:
103.149.159.2

Resource owner account
210855491654

Step 19: Click on “Permissions”.



Step 20: Scroll down to the Block public access section and click on the “Edit” button.



Step 21: Block all public access by checking the box and click on Save changes.

Edit Block public access (bucket settings) [Info](#)

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☒ Block all public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☒ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- ☒ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
- ☒ **Block public access to buckets and objects granted through *new* public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- ☒ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Cancel

Save changes

Enter "confirm" and save the settings.

Edit Block public access (bucket settings) ×



This will result in public access being blocked for this bucket and all objects in the bucket.

To confirm the settings, enter *confirm* in the field.

Cancel

Confirm

All the public access has been blocked.

Public access is granted to buckets and objects through access control lists (ACLs), buckets, and this bucket and its access points. AWS recommends that you turn on Block all public access to objects within, you can customize the individual settings below to suit your specific storage

Block *all* public access

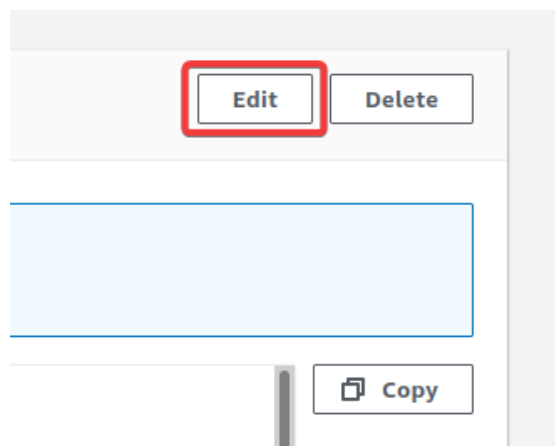
► Individual Block Public Access settings for this bucket

Bucket policy

To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about [using Amazon S3 Block Public Access](#)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::lab-bucket-ip-210855491654",
        "arn:aws:s3:::lab-bucket-ip-210855491654/*"
      ],
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "103.149.159.22"
        }
      }
    }
  ]
}
```

©PentesterAcademy.com

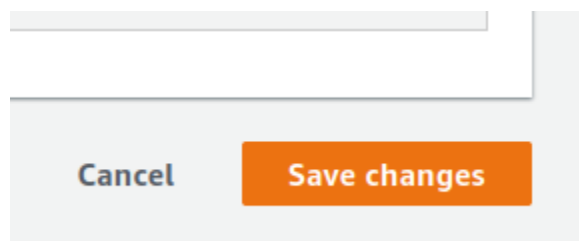


Change the Effect in the policy to “Deny”. This denies permissions to user having the specified IP address to perform Amazon S3 Read, Write, List operations.

Policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Deny",
6       "Principal": "*",
7       "Action": [
8         "s3:GetObject",
9         "s3:ListBucket",
10        "s3:PutObject"
11      ],
12      "Resource": [
13        "arn:aws:s3:::lab-bucket-ip-210855491654",
14        "arn:aws:s3:::lab-bucket-ip-210855491654/*"
15      ],
16      "Condition": {
17        "IpAddress": {
18          "aws:SourceIp": "103.149.159.22"
19        }
20      }
21    }
22  ]
23 }
```

Click on "Save changes".



Switch to the tab which has an access analyzer dashboard.

Step 23: On the finding page, Click on the "Rescan" button to run a scan again in this particular resource.



The access is removed, the status changed to Resolved.

.33bc-4093-a08a-b604c78d70b2 [Info](#)


	Updated	Status
3-a08a-b604c78d70b2	a few seconds ago	<div> Resolved</div> <div>The access is no longer allowed</div>

Step 24: Click on "Finding ID" of the resource "IAM Role" with the name "ad_role".

<input type="checkbox"/>	Finding ID	Resource	External principal	Condition	S
<input type="checkbox"/>	b5400d88-4d88-...	IAM Role TheOracle	AWS Account 719592403832	-	-
<input type="checkbox"/>	3b306705-ce94-4...	IAM Role TheOracle	AWS Account 002763723555	-	-
<input type="checkbox"/>	ecf2469d-1c2f-44...	IAM Role ad_role	All Principals	-	-
<input type="checkbox"/>	077a5e86-278f-4...	KMS Key aa94d1bb-5f4e-...	AWS Account 002763723555	-	-

Step 25: Right click on the resource arn and open the link in the new tab. This will navigate to the IAM dashboard.

ecf2469d-1c2f-4477-a8b9-75d9b62d6fb4 [Info](#) [Feedback](#)

 Public: this finding is for a resource that allows public access.

Details

Finding ID ecf2469d-1c2f-4477-a8b9-75d9b62d6fb4	Updated 26 minutes ago	Status Active	Shared through -
Resource arn:aws:iam::210855491654:role/ad_role	External principal All Principals	Condition -	Access level Write • sts:AssumeRole
Resource owner account 210855491654			

A trust policy is a document in which you define the principals that you trust to assume the role. A role trust policy is a required resource-based policy that is attached to a role in IAM. The principals that you can specify in the trust policy include users, roles, accounts, and services. This is an overly permissive trust policy.

IAM > Roles > ad_role

ad_role



Overly permissive trust policy exists in your trust relationships

Broad access: Principals that include a wildcard (*, ?) can be overly permissive.

Summary

Creation date

August 22, 2022, 01:15 (UTC-04:00)

ARN

arn:aws:iam::210855491654:role/ad_role

Last activity

None

Maximum session duration

1 hour

Step 26: Click on “Trust relationships”.

Permissions | **Trust relationships** | Tags | Access Advisor | Revoke ses

Permissions policies (1)
You can attach up to 10 managed policies.

Filter policies by property or policy name and press enter

<input type="checkbox"/>	Policy name	
<input type="checkbox"/>	AdministratorAccess	A

Step 27: Click on “Edit trust policy”.



Edit trust policy

Step 28: Change the Effect to “Deny”.


This trust policy allows full access to the AWS account and this can be assumed by anyone.

[IAM](#) > [Roles](#) > [ad_role](#) > Edit trust policy

Edit trust policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "",  
6       "Effect": "Deny",  
7       "Principal": {  
8         "AWS": "*"   
9       },  
10      "Action": "sts:AssumeRole"  
11    }  
12  ]  
13 }
```

Step 29: Update policy by clicking “Update policy”.



[Cancel](#) [Update policy](#)



Switch to the tab which has an access analyzer dashboard.

Step 30: On the finding page, Click on the “Rescan” button to run a scan again in this particular resource.

[Feedback](#) [Rescan](#)

The access is removed, the status changed to Resolved.

77-a8b9-75d9b62d6fb4 [Info](#)

d6fb4	Updated a few seconds ago	Status <div> Resolved</div> The access is no longer allowed
i_role 	External principal All Principals	Condition -

Step 31: Navigate back to the analyzer dashboard. Click on “Finding ID” of the resource “KMS Key” .

<input type="checkbox"/>	Finding ID	Resource	External principal
<input type="checkbox"/>	b5400d88-4d88-409...	IAM Role TheOracle	AWS Account 719592403832
<input type="checkbox"/>	3b306705-ce94-413...	IAM Role TheOracle	AWS Account 002763723555
<input type="checkbox"/>	077a5e86-278f-4abd...	KMS Key aa94d1bb-5f4e-48...	AWS Account 002763723555

Check the access level granted.

Access level

Permissions

- kms:CreateGrant
- kms:RetireGrant
- kms:RevokeGrant

Write

- kms:Decrypt
- kms:Encrypt
- kms:GenerateDataKey
- kms:GenerateDataKeyPair
- kms:GenerateDataKeyPairWithoutPlaintext
- kms:GenerateDataKeyWithoutPlaintext
- kms:ReEncryptFrom
- kms:ReEncryptTo
- kms:Sign
- kms:Verify

Read

- kms:DescribeKey
- kms:GetKeyRotationStatus
- kms:GetPublicKey

List

- kms:ListGrants

Step 32: Right click on the resource arn and open the link in the new tab. This will navigate to the KMS dashboard.

077a5e86-278f-4abd-958e-0087b5c1c9d3 [Info](#)

Details

Finding ID	Updated	Status
077a5e86-278f-4abd-958e-0087b5c1c9d3	31 minutes ago	Active
Resource	External principal (AWS Account)	Condition
arn:aws:kms:us-east-1:210855491654:key/aa94d1bb-5f4e-481d-9ff5-70c6a69e3a96	002763723555	-
Resource owner account		
210855491654		

AWS Key Management Service (KMS) gives you centralized control over the cryptographic keys used to protect your data. The service is integrated with other AWS services making it easy to encrypt data you store in these services and control access to the keys that decrypt it.

This key policy statement allows all actions (kms:*) to two AWS accounts on the KMS key. Remove the external AWS account from the key policy.

Key policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "EnableAnotherAWSAccountToReadKMS",
6       "Effect": "Allow",
7       "Principal": {
8         "AWS": [
9           "arn:aws:iam::210855491654:root",
10          "arn:aws:iam::002763723555:root"
11        ]
12      },
13      "Action": "kms:*",
14      "Resource": "*"
15    ]
16  }
```

The principal in this key policy statement is the account principal, which is represented by an ARN in this format: `arn:aws:iam::account-id:root`. The account principal represents the AWS account and its administrators.

Step 33: Remove the external AWS account from the principal and click on “Save changes”.



Key policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "EnableAnotherAWSAccountToReadKMS",  
6       "Effect": "Allow",  
7       "Principal": {  
8         "AWS": [  
9           "arn:aws:iam::210855491654:root"  
10        ]  
11      },  
12      "Action": "kms:*",  
13      "Resource": "*"   
14    }  
15  ]
```

Cancel Save changes

Switch to the tab which has an access analyzer dashboard.

Step 34: On the finding page, Click on the “Rescan” button to run a scan again in this particular resource.



The access is removed, the status changed to Resolved.

077a5e86-278f-4abd-958e-0087b5c1c9d3 [Info](#)

Details

Finding ID

077a5e86-278f-4abd-958e-0087b5c1c9d3

Updated

a few seconds ago

Status

✓ Resolved

The access is no longer allowed

Resource

[arn:aws:kms:us-east-1:210855491654:key/aa94d1bb-5f4e-481d-9ff5-70c6a69e3a96](#)

External principal (AWS Account)

002763723555

Condition

-

Resource owner account

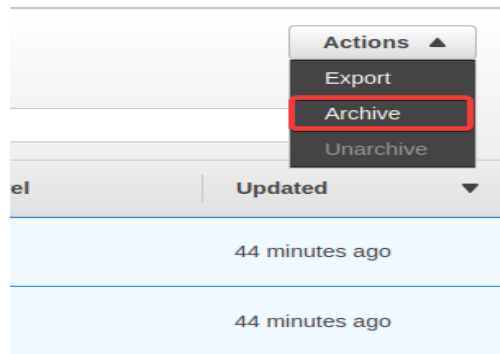
210855491654

Step 35: Navigate back to the analyzer dashboard. Select all the findings with the name “TheOracle” and archive the findings.

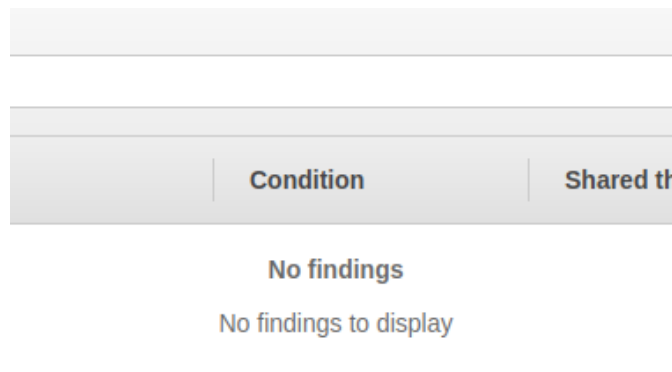
These findings are generated from an IAM role which was created intentionally for this lab and has no security threats. So archive the findings.

<input checked="" type="checkbox"/>	Finding ID	Resource	External principal
<input checked="" type="checkbox"/>	b5400d88-4d88-409...	IAM Role TheOracle	AWS Account 719592403832
<input checked="" type="checkbox"/>	3b306705-ce94-413...	IAM Role TheOracle	AWS Account 002763723555

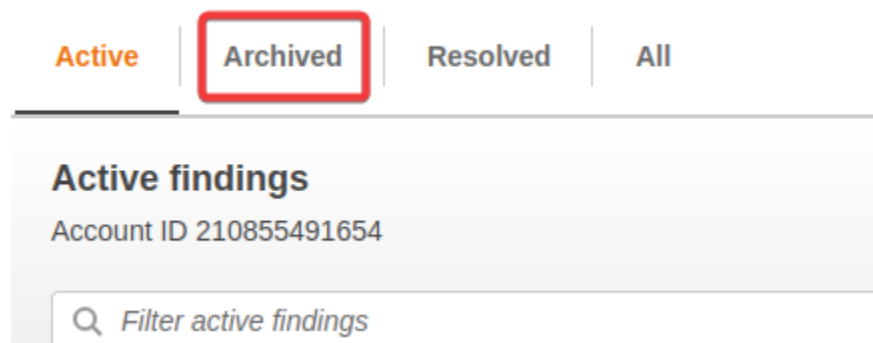
Step 36: Click on “Archive” under the actions.



When you archive a finding, it is removed from Active findings and the status changes to Archived.



Click on “Archived” and navigate to archived findings.



This will list all the archived findings.

Archived findings			
Account ID 210855491654			
<input type="text" value="Filter archived findings"/>			
<input type="checkbox"/>	Finding ID	Resource	External principal
<input type="checkbox"/>	b5400d88-4d88-409...	IAM Role TheOracle	AWS Account 719592403832
<input type="checkbox"/>	3b306705-ce94-413...	IAM Role TheOracle	AWS Account 002763723555

Click on “Resolved” and navigate to resolved findings.

Active	Archived	Resolved	All
Archived findings			
Account ID 210855491654			

This will list all the resolved findings.

Resolved findings

Account ID 210855491654

Filter resolved findings

<input type="checkbox"/>	Finding ID	Resource	External principal
<input type="checkbox"/>	077a5e86-278f-4abd...	KMS Key aa94d1bb-5f4e-48...	AWS Account 002763723555
<input type="checkbox"/>	ecf2469d-1c2f-4477-...	IAM Role ad_role	All Principals
<input type="checkbox"/>	1fb7c1b2-33bc-4093...	S3 Bucket lab-bucket-ip-2108...	All Principals
<input type="checkbox"/>	c673cc58-90f4-480c...	S3 Bucket lab-zone-21085549...	All Principals
<input type="checkbox"/>	32170698-9ae4-4aa...	Secret account-Uu6Tvt	AWS Account 002763723555

References:

1. AWS Access Analyzer
(<https://docs.aws.amazon.com/IAM/latest/UserGuide/what-is-access-analyzer.html>)