ATTACK DEFENSE

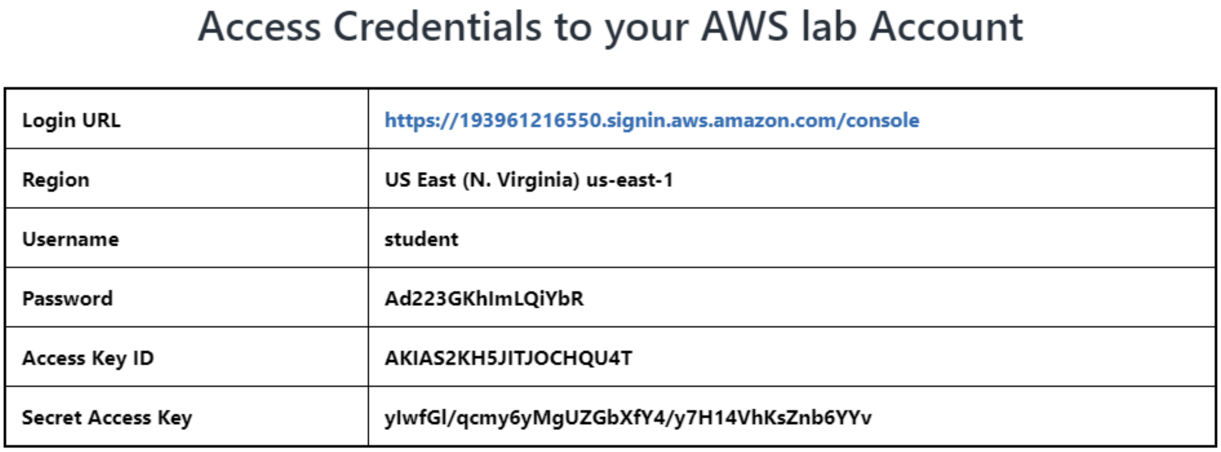
by PentesterAcademy

Name	Amazon Macie
URL	https://attackdefense.com/challengedetails?cid=2498
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:

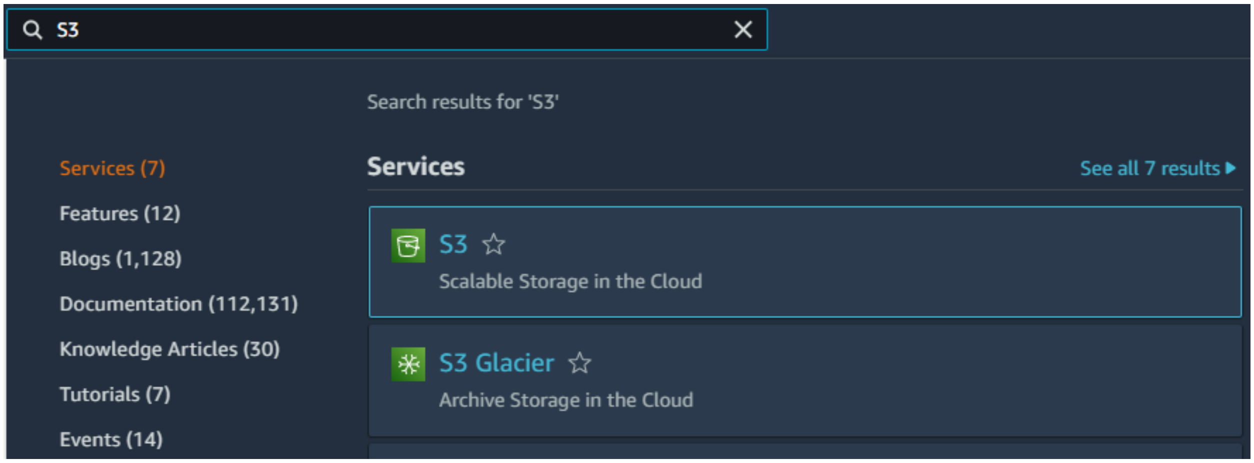
Step 1: Click the lab link button to get access credentials.



Access Credentials to your AWS lab Account

Login URL	https://193961216550.signin.aws.amazon.com/console
Region	US East (N. Virginia) us-east-1
Username	student
Password	Ad223GKhImLQiYbR
Access Key ID	AKIAS2KH5JITJOCHQU4T
Secret Access Key	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

Step 2: Create S3 bucket and upload sensitive data. Search for S3 in the search bar and navigate to the S3 dashboard.



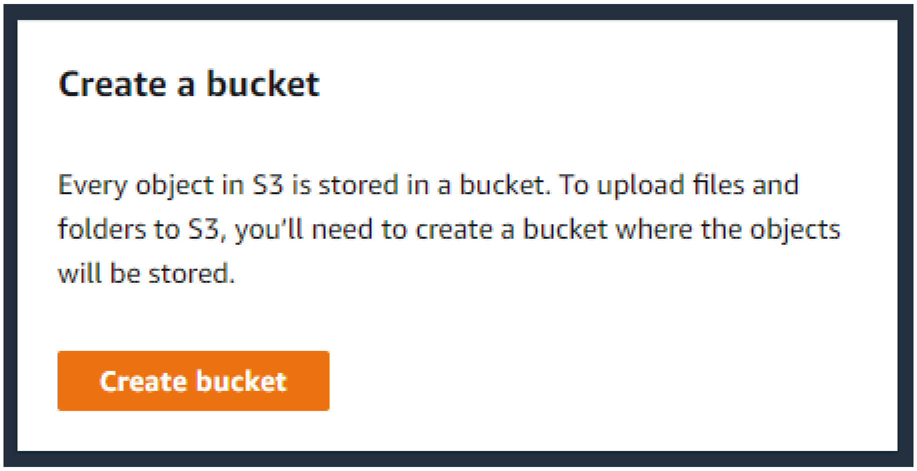
Search results for 'S3'

Services

S3 ☆
Scalable Storage in the Cloud

S3 Glacier ☆
Archive Storage in the Cloud

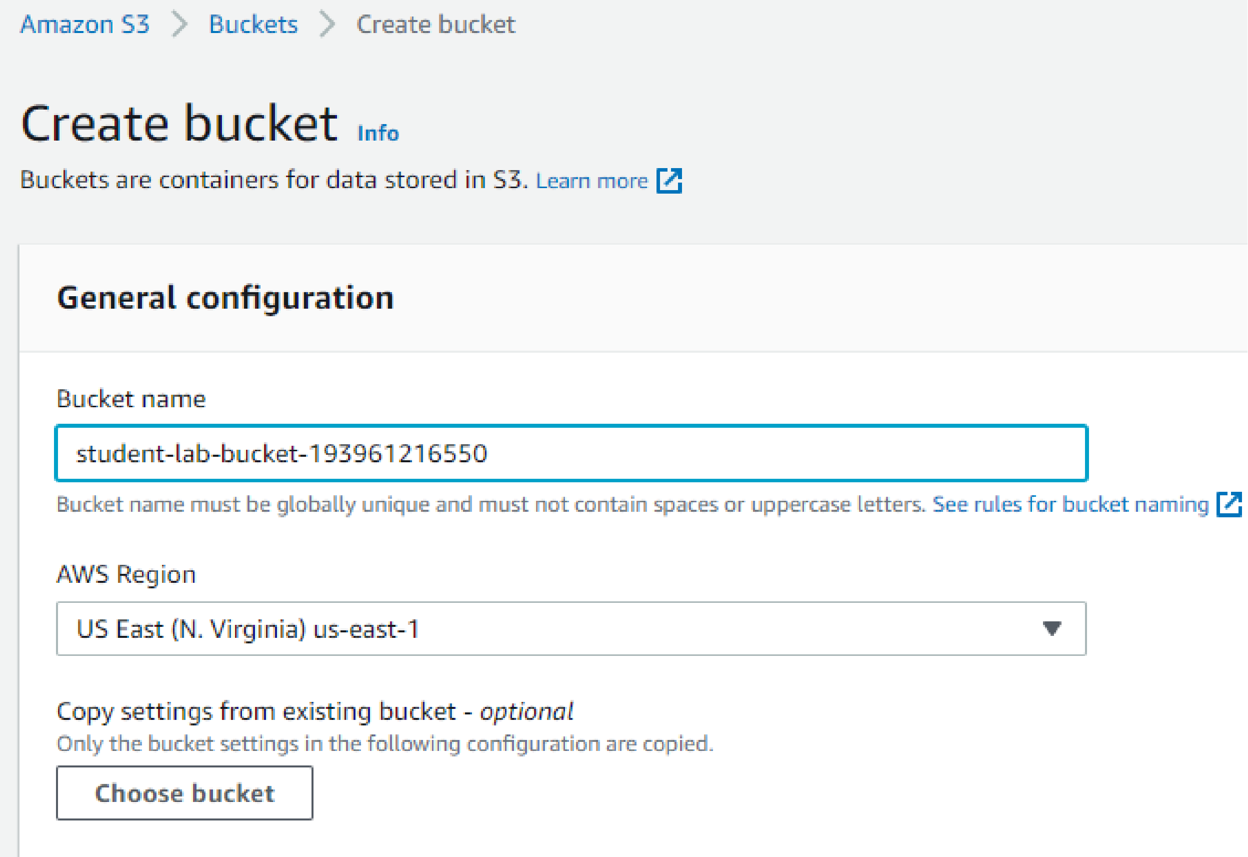
Step 3: Click on the “Create bucket” button.



Create a bucket

Every object in S3 is stored in a bucket. To upload files and folders to S3, you’ll need to create a bucket where the objects will be stored.

Step 4: Set the bucket name as “student-lab-bucket-” and append the account id at the end.



Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3. Learn more

General configuration

Bucket name

student-lab-bucket-193961216550

Bucket name must be globally unique and must not contain spaces or uppercase letters. See rules for bucket naming

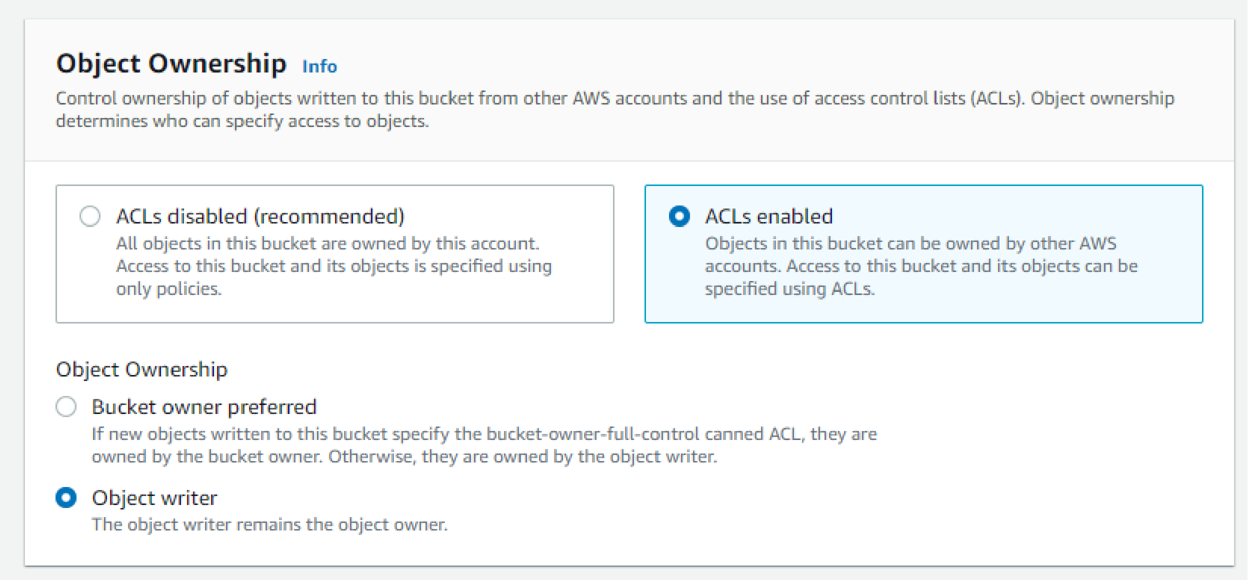
AWS Region

US East (N. Virginia) us-east-1

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Step 5: Enable ACLs and set the object ownership to “Object writer”.



Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

○ ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

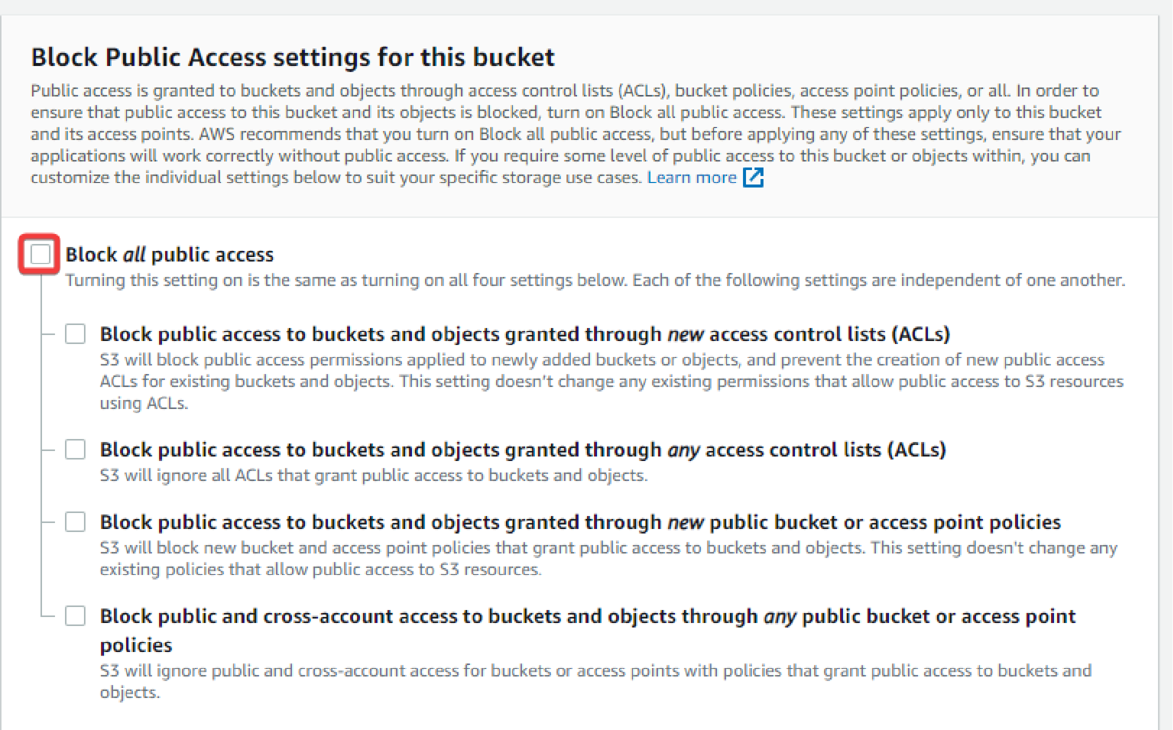
● ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership

○ Bucket owner preferred
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

● Object writer
The object writer remains the object owner.

Step 6: Uncheck the "Block all public access" and make the bucket public.



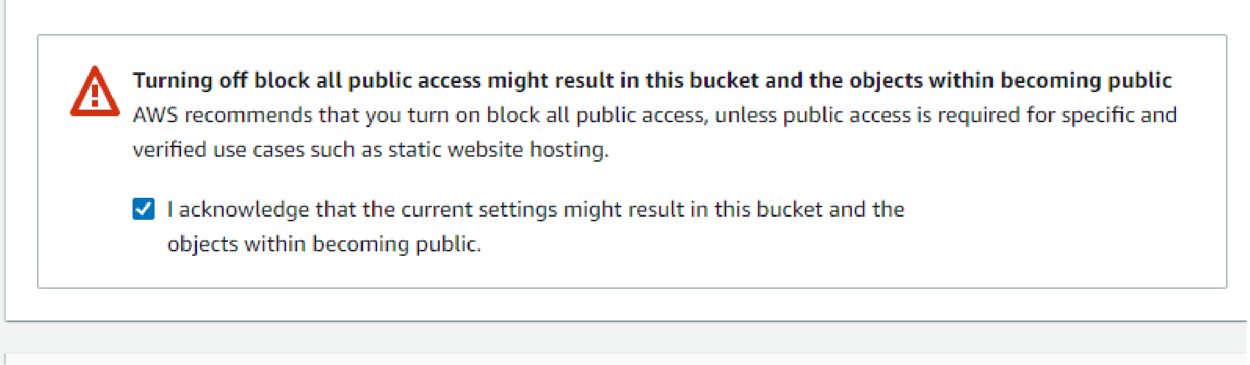
Block Public Access settings for this bucket

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 this bucket and its 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 this bucket 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.

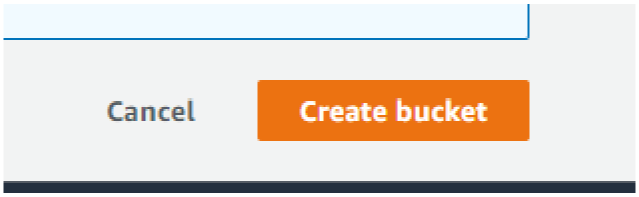
Confirm the action by checking the acknowledging the current settings.



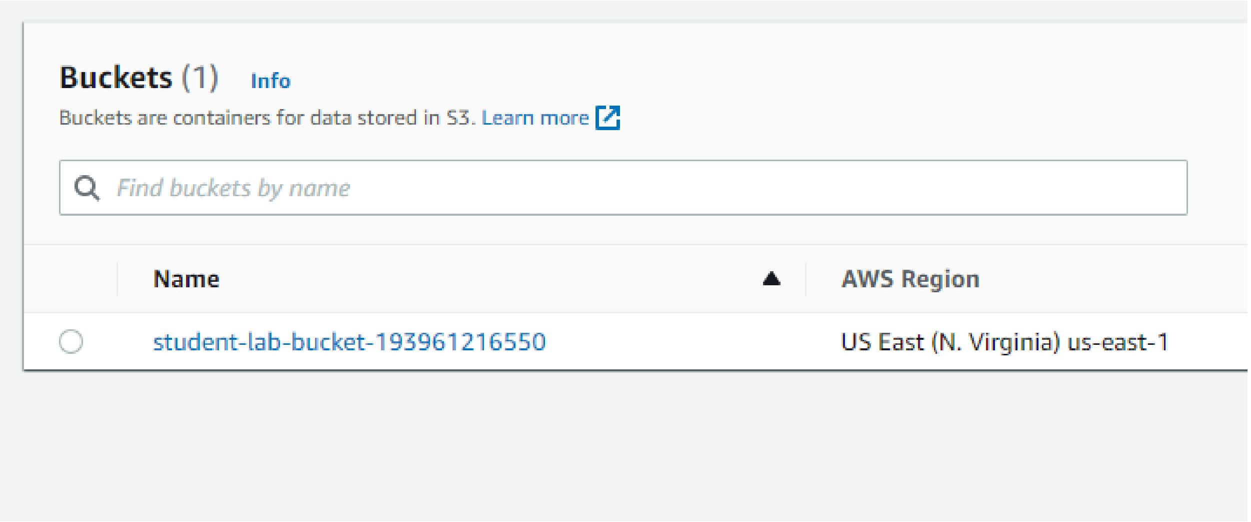
Turning off block all public access might result in this bucket and the objects within becoming public
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☑ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

Click on the "Create bucket" button.



Successfully created the bucket.

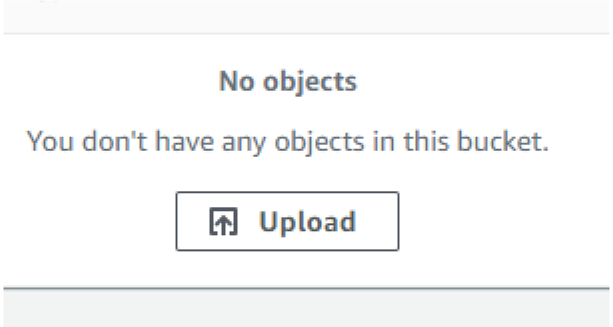


Buckets (1) Info

Buckets are containers for data stored in S3. Learn more

	Name	AWS Region
○	student-lab-bucket-193961216550	US East (N. Virginia) us-east-1

There are no objects available in the bucket. Upload files by clicking the “Upload” button.

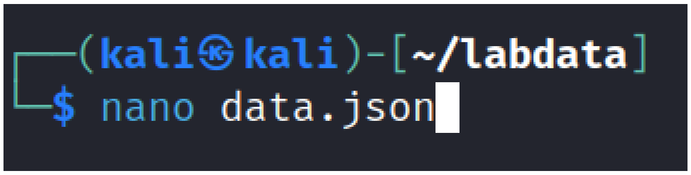


No objects

You don't have any objects in this bucket.

Step 7: Create a JSON file and set name as “data.json”.

Command: nano data.json



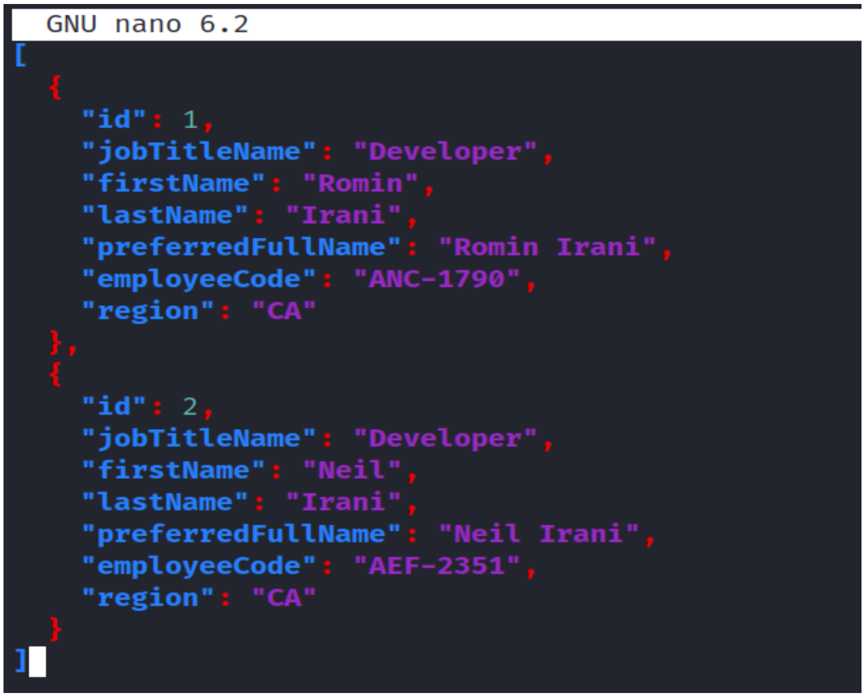
```
┌──(kali㉿kali)-[~/labdata]
└─$ nano data.json
```

Step 8: Copy and paste the following code inside the data.json file.

Code :

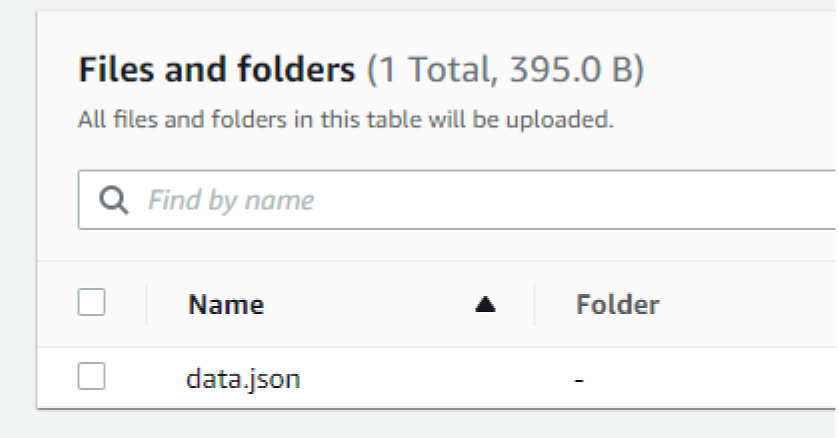
```
[
  {
    "id": 1,
    "jobTitleName": "Developer",
    "firstName": "Romin",
    "lastName": "Irani",
    "preferredFullName": "Romin Irani",
    "employeeCode": "ANC-1790",
    "region": "CA"
  },
  {
    "id": 2,
    "jobTitleName": "Developer",
    "firstName": "Neil",
    "lastName": "Irani",
    "preferredFullName": "Neil Irani",
    "employeeCode": "AEF-2351",
    "region": "CA"
  }
]
```

This is sample employee information. We are using employee code as sensitive information and detecting it with Amazon Macie.



```
  GNU nano 6.2
[
  {
    "id": 1,
    "jobTitleName": "Developer",
    "firstName": "Romin",
    "lastName": "Irani",
    "preferredFullName": "Romin Irani",
    "employeeCode": "ANC-1790",
    "region": "CA"
  },
  {
    "id": 2,
    "jobTitleName": "Developer",
    "firstName": "Neil",
    "lastName": "Irani",
    "preferredFullName": "Neil Irani",
    "employeeCode": "AEF-2351",
    "region": "CA"
  }
]
```

Step 9: Choose the “data.json” file to upload.

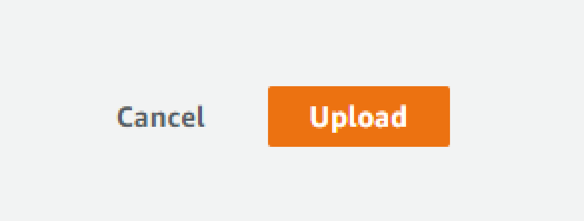


Files and folders (1 Total, 395.0 B)

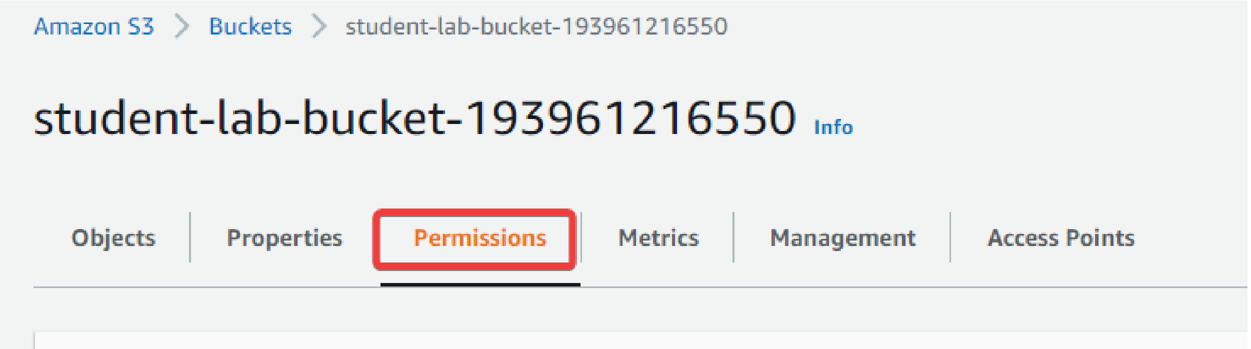
All files and folders in this table will be uploaded.

□	Name ▲	Folder
□	data.json	-

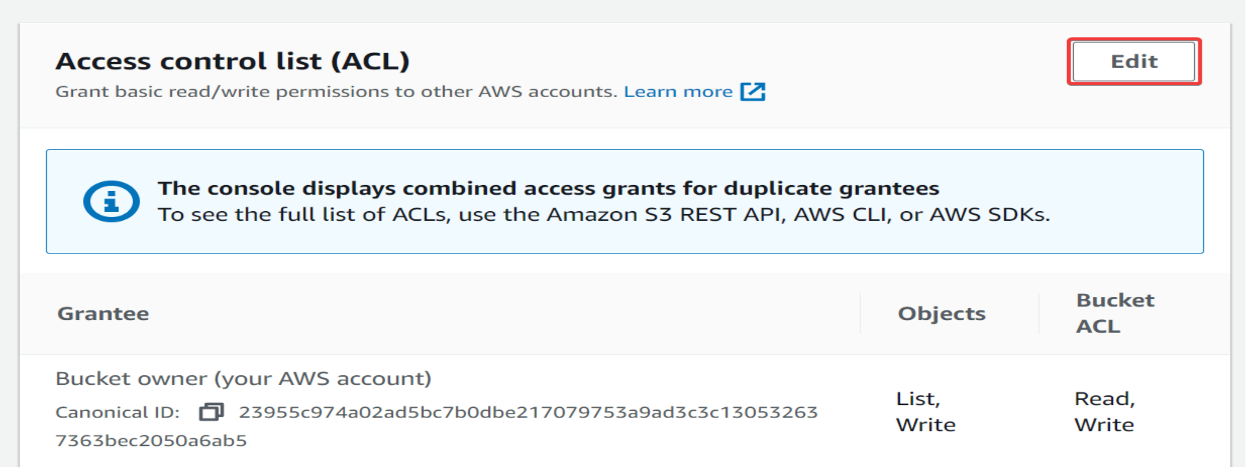
Click on the “Upload” button.



Step 10: Click on “Permissions” inside the created bucket.


Amazon S3 > Buckets > student-lab-bucket-193961216550
student-lab-bucket-193961216550 Info
Objects
Properties
Permissions
Metrics
Management
Access Points

Step 11: Click on “Edit” in the ACL block.



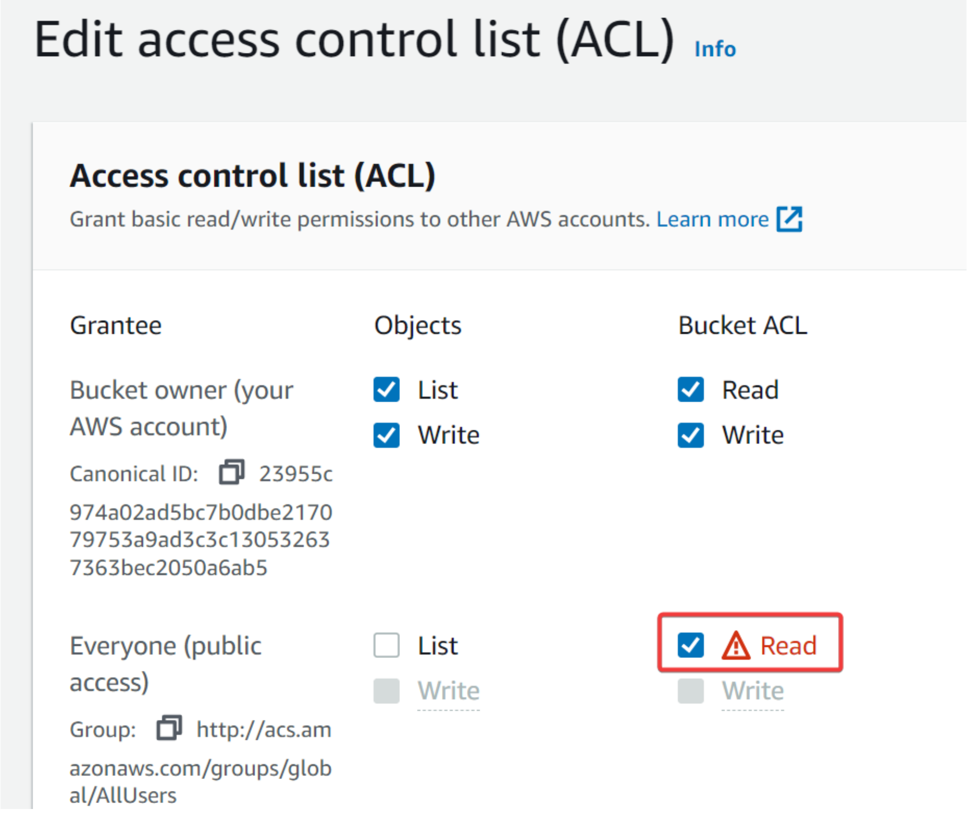
Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. Learn more

The console displays combined access grants for duplicate grantees
To see the full list of ACLs, use the Amazon S3 REST API, AWS CLI, or AWS SDKs.

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: 23955c974a02ad5bc7b0dbe217079753a9ad3c3c13053263 7363bec2050a6ab5	List, Write	Read, Write

Enable public read access.



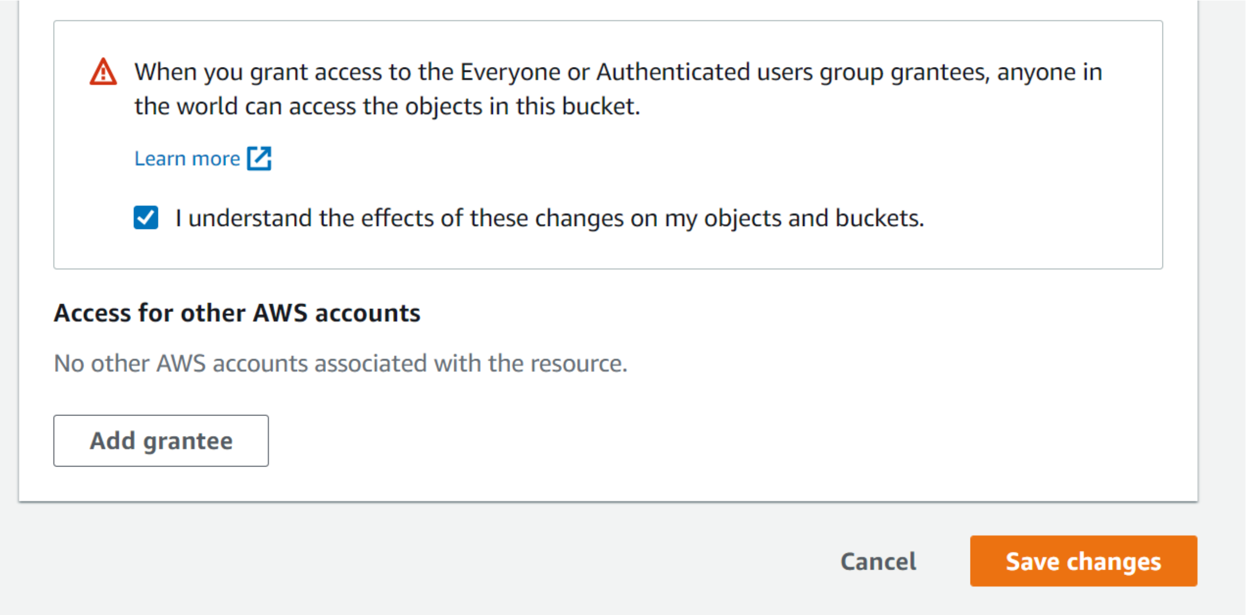
Edit access control list (ACL) Info

Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. Learn more

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: 23955c974a02ad5bc7b0dbe217079753a9ad3c3c130532637363bec2050a6ab5	☑ List ☑ Write	☑ Read ☑ Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	□ List □ Write	☑ ⚠ Read □ Write

Confirm the action by checking the acknowledging the current settings.



⚠ When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access the objects in this bucket.

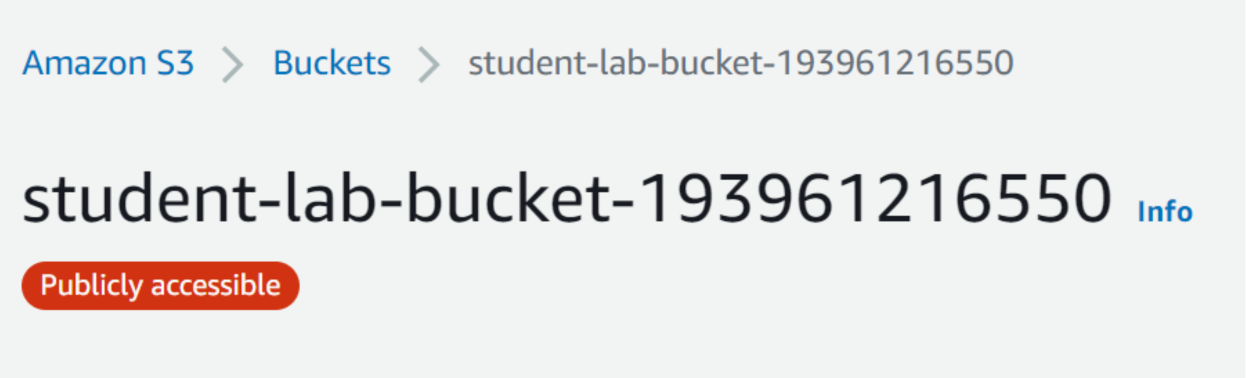
Learn more

☑ I understand the effects of these changes on my objects and buckets.

Access for other AWS accounts

No other AWS accounts associated with the resource.

Now the bucket is publicly accessible.

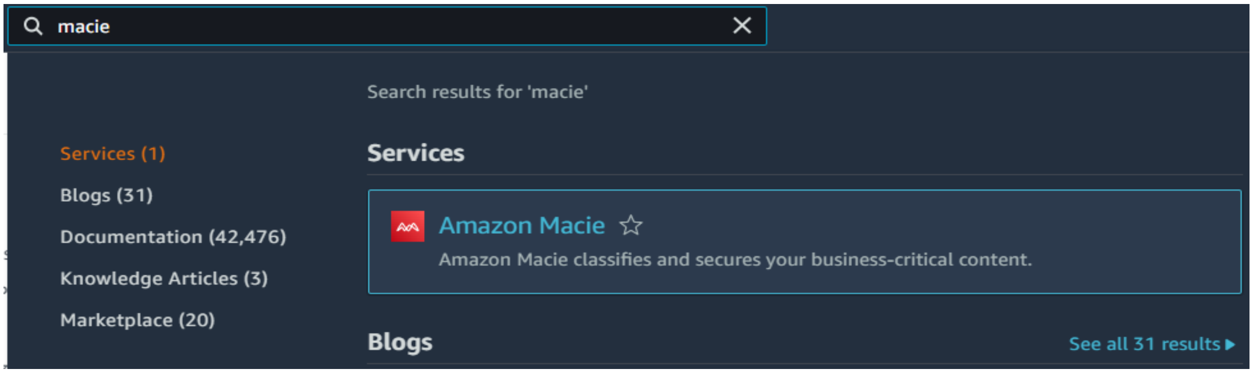


Amazon S3 > Buckets > student-lab-bucket-193961216550

student-lab-bucket-193961216550 Info

Publicly accessible

Step 12: Search for macie in the search bar and navigate to the Amazon Macie dashboard.



macie

Search results for 'macie'

Services

Amazon Macie ☆

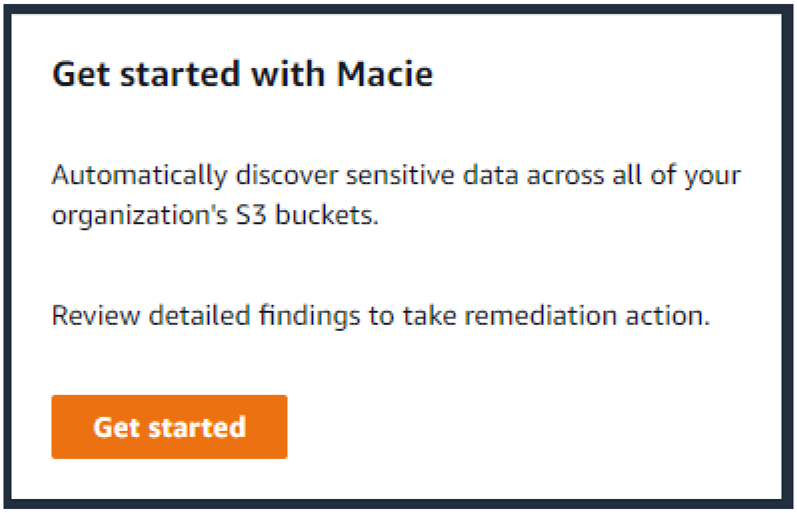
Amazon Macie classifies and secures your business-critical content.

Blogs

Amazon Macie uses pattern matching and machine learning to protect the sensitive data stored in S3 buckets.Macie automates the discovery of sensitive data, such as personally identifiable information (PII) and financial data, to provide you with a better understanding of the data that your organization stores in Amazon Simple Storage Service (Amazon S3). Macie also provides you with an inventory of your S3 buckets, and it automatically evaluates and monitors those buckets for security and access control.

Here we will create a custom data identifier where we will set a regular expression that matches the pattern of data present in the S3 bucket.

Click on the “Get started” button.

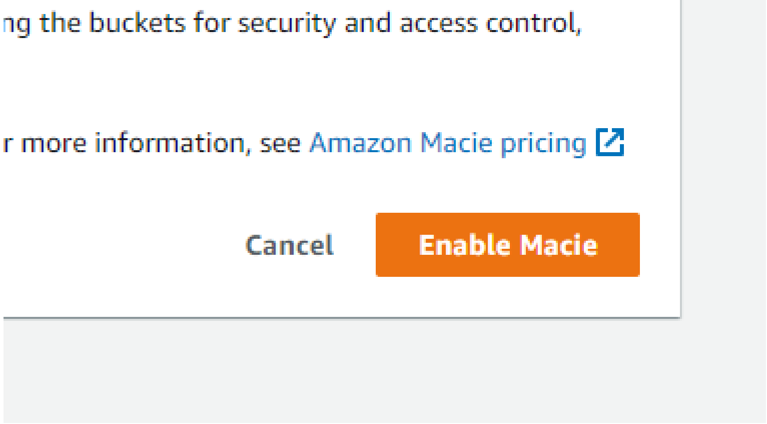


Get started with Macie

Automatically discover sensitive data across all of your organization's S3 buckets.

Review detailed findings to take remediation action.

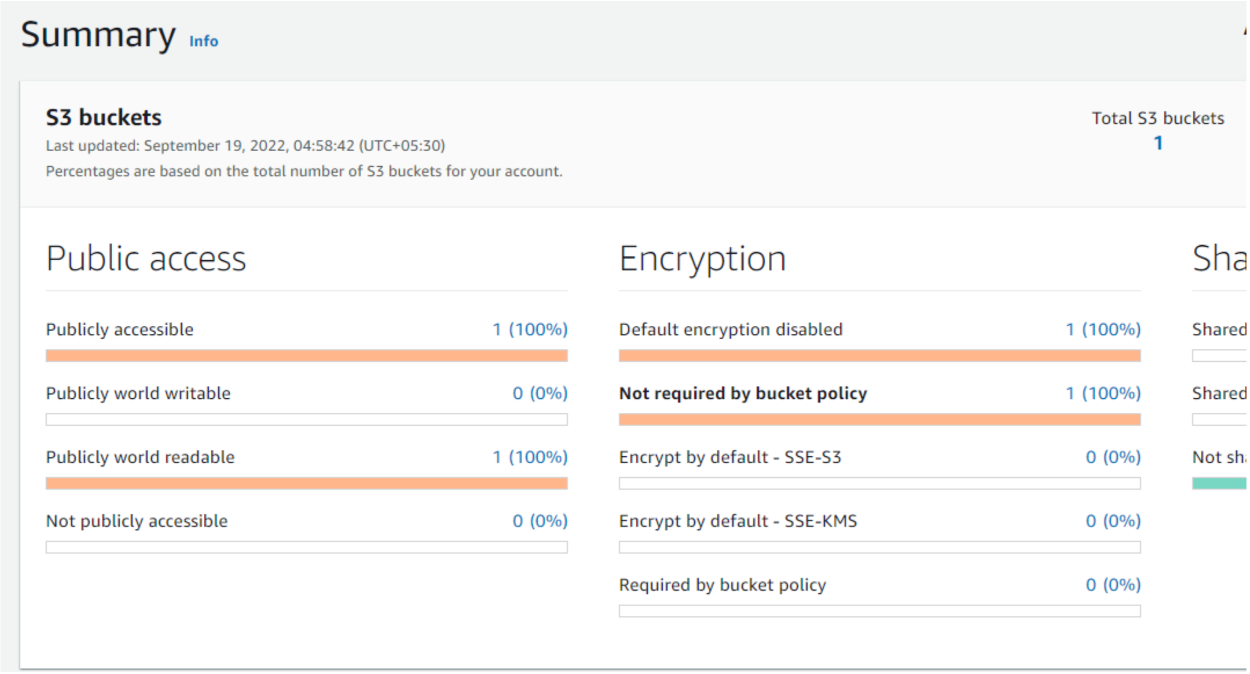
Step 13: Click on the “Enable Macie” button.



ng the buckets for security and access control,

r more information, see Amazon Macie pricing

As soon as Macie is enabled, it will automatically discover all the buckets and objects that are stored inside each bucket, and the Macie dashboard will appear based on the size and count of the buckets.



Summary Info

S3 buckets

Last updated: September 19, 2022, 04:58:42 (UTC+05:30)

Percentages are based on the total number of S3 buckets for your account.

Total S3 buckets
1

Public access

Publicly accessible	1 (100%)
Publicly world writable	0 (0%)
Publicly world readable	1 (100%)
Not publicly accessible	0 (0%)

Encryption

Default encryption disabled	1 (100%)
Not required by bucket policy	1 (100%)
Encrypt by default - SSE-S3	0 (0%)
Encrypt by default - SSE-KMS	0 (0%)
Required by bucket policy	0 (0%)

Sha

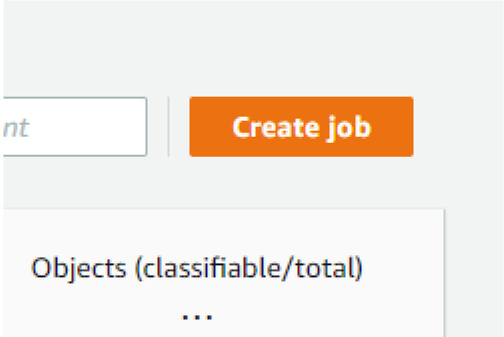
Shared

Shared

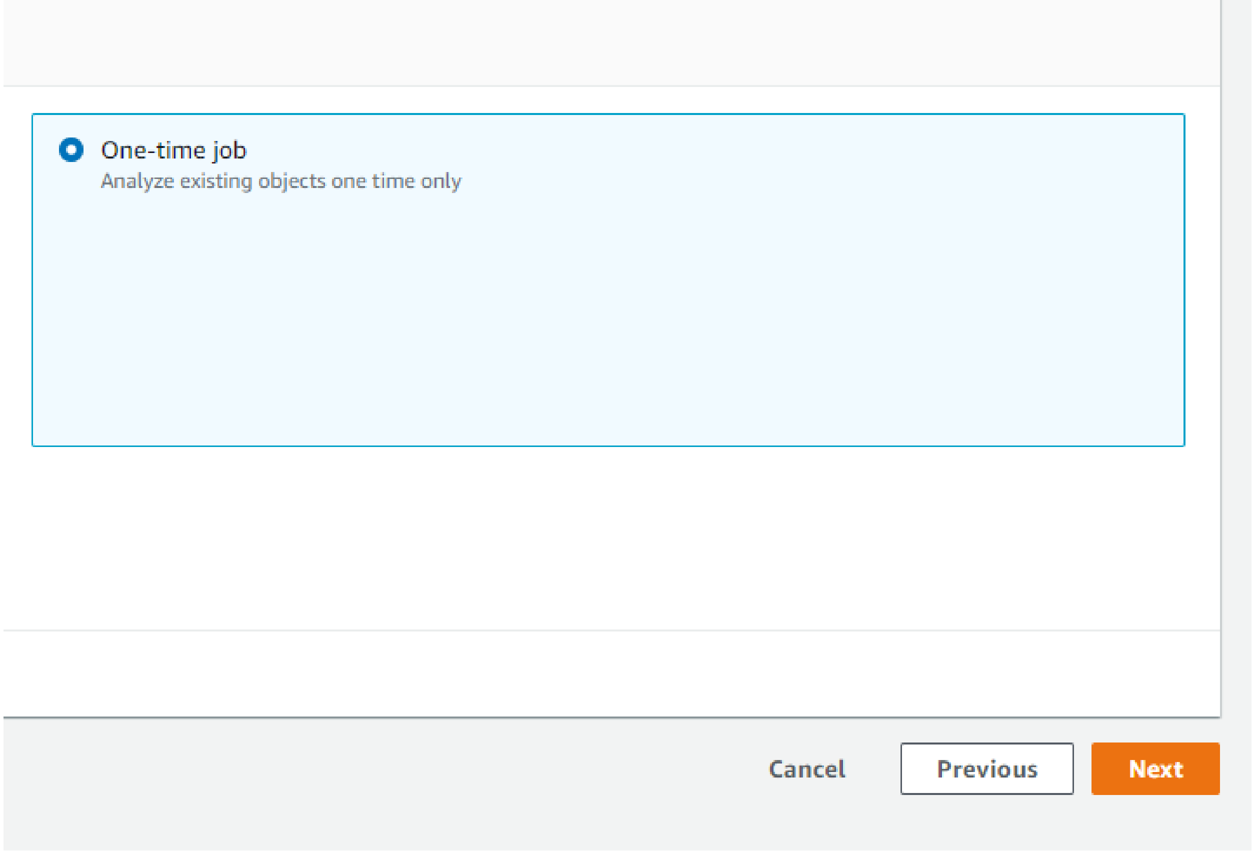
Not sh

Step 14: Click on the “Create job” button.

A sensitive data discovery job is a series of automated processing and analysis tasks that Macie performs to analyze objects in S3 buckets and determine whether the objects contain sensitive data.

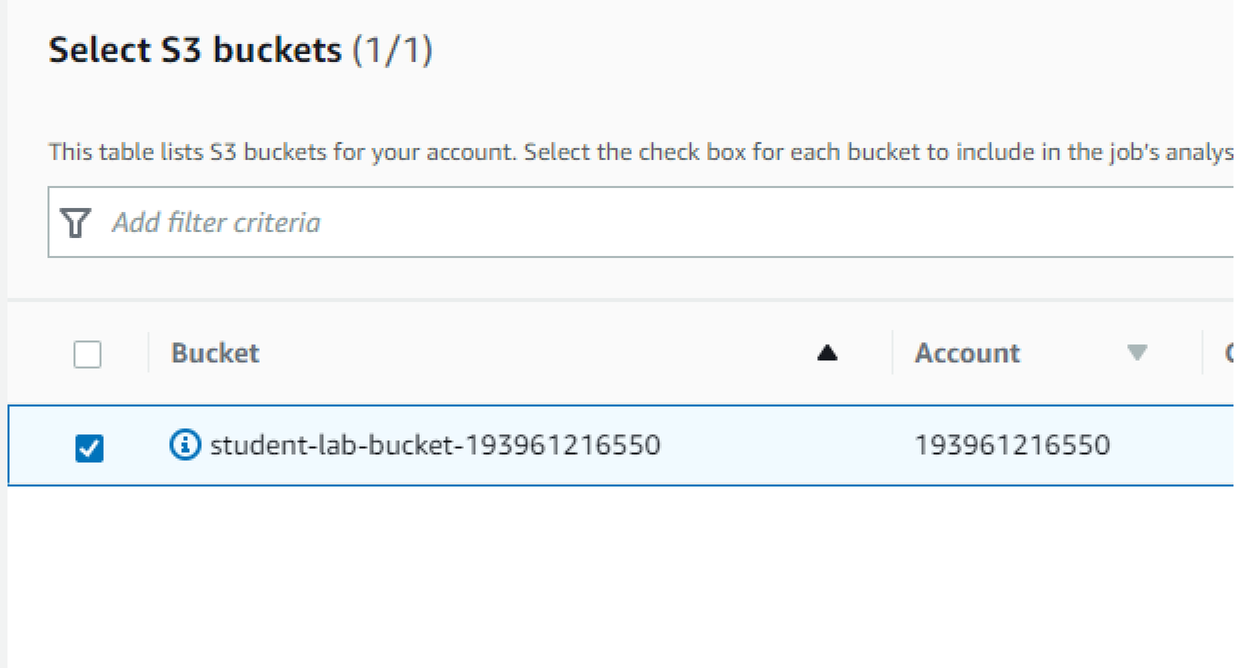


Step 15: For the Refine the scope step, choose One-time job, and then choose Next.



● One-time job
Analyze existing objects one time only

Step 16: Select the created S3 bucket.

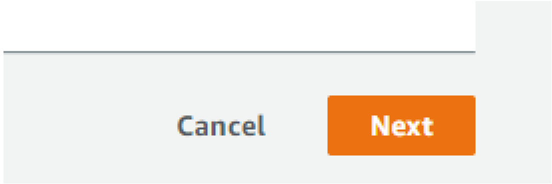


Select S3 buckets (1/1)

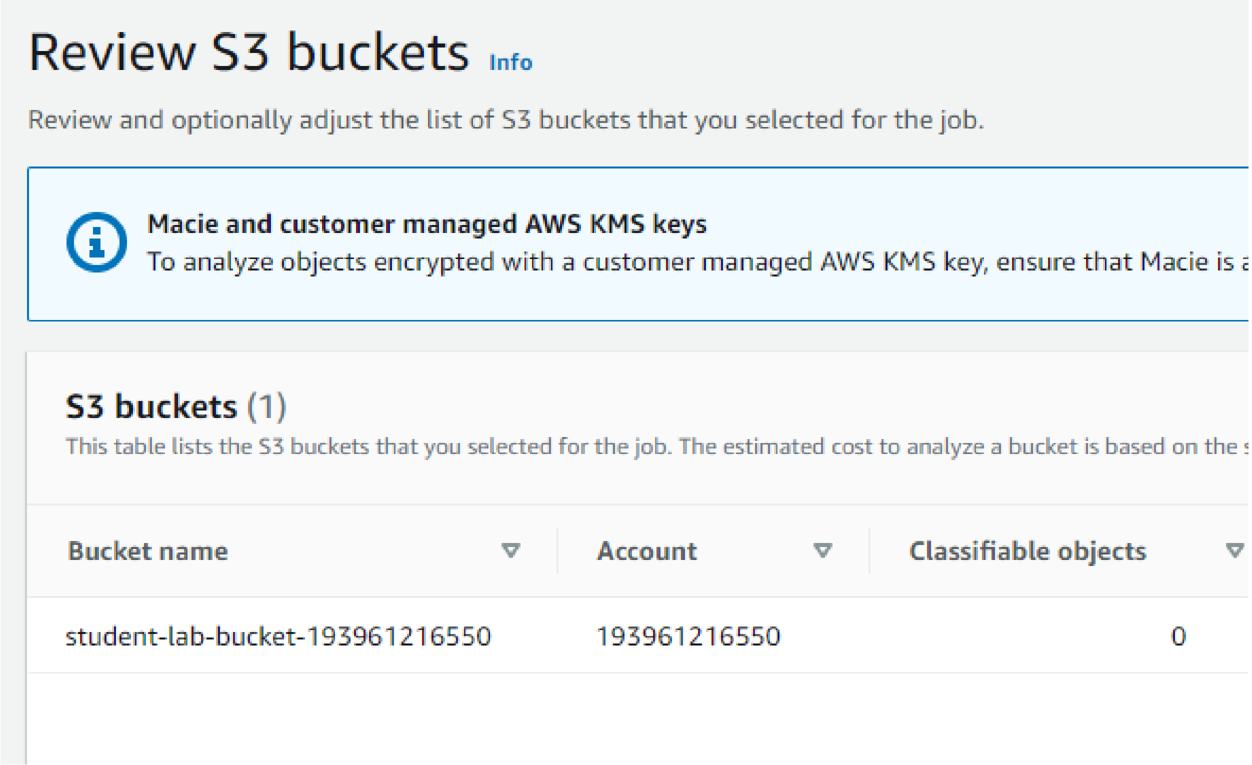
This table lists S3 buckets for your account. Select the check box for each bucket to include in the job's analys

□	Bucket ▲	Account ▼
☑	student-lab-bucket-193961216550	193961216550

Click on the “Next” button.



Review S3 bucket settings.



Review S3 buckets Info

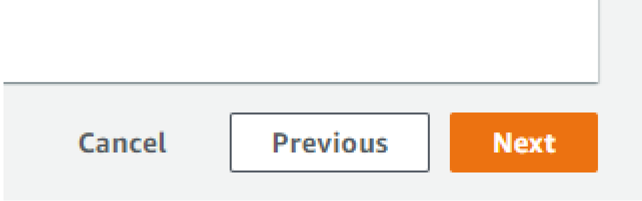
Review and optionally adjust the list of S3 buckets that you selected for the job.

Macie and customer managed AWS KMS keys
To analyze objects encrypted with a customer managed AWS KMS key, ensure that Macie is a

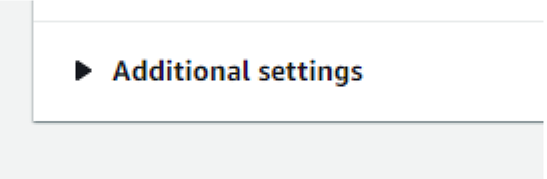
S3 buckets (1)
This table lists the S3 buckets that you selected for the job. The estimated cost to analyze a bucket is based on the s

Bucket name	Account	Classifiable objects
student-lab-bucket-193961216550	193961216550	0

Click on the “Next” button.

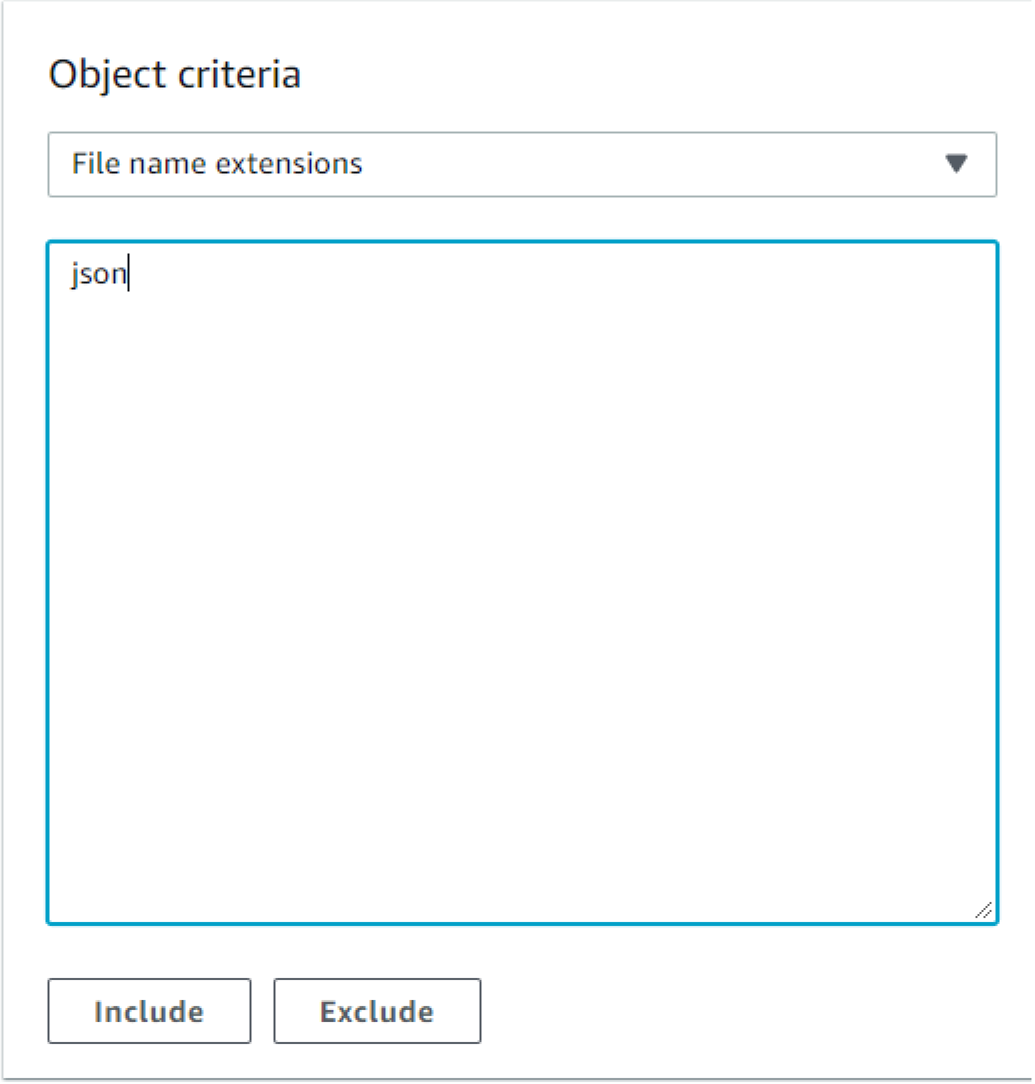


Step 17: Click on the arrow to expand the window of Additional settings.



Step 18: Let the Object criteria be default as File name extensions. Enter “json” in the textbox and click on the Include button.

Amazon Macie can analyze data in many different formats, including commonly used compression and archive formats.

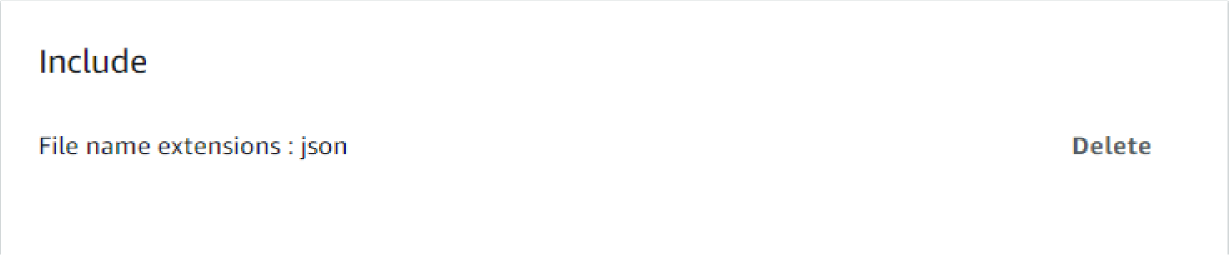


Object criteria

File name extensions

json

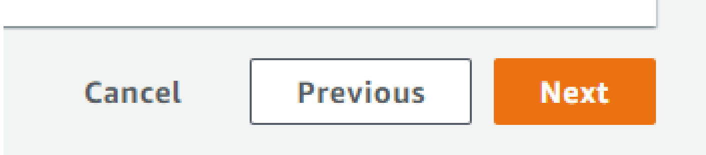
Successfully included the file extension “JSON”.



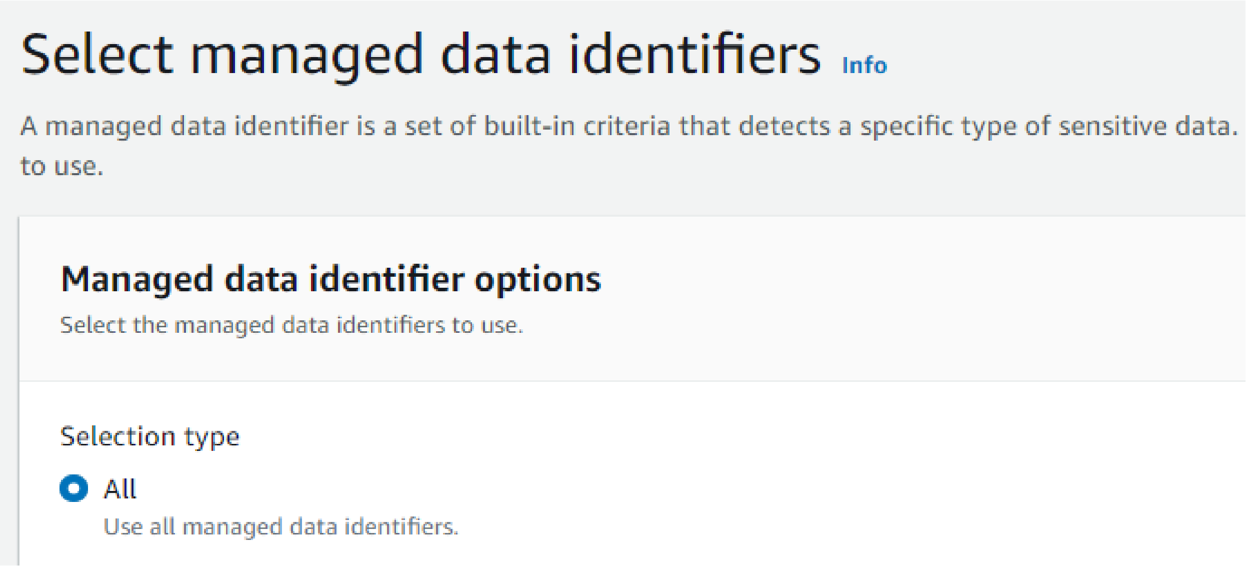
Include

File name extensions : json

Click on the “Next” button.



Step 19: Set selection type as “All”.



Select managed data identifiers

A managed data identifier is a set of built-in criteria that detects a specific type of sensitive data. to use.

Managed data identifier options

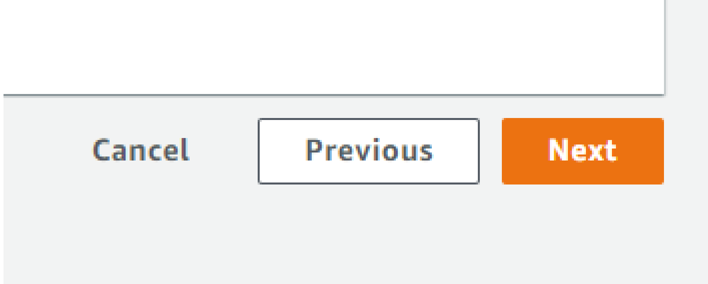
Select the managed data identifiers to use.

Selection type

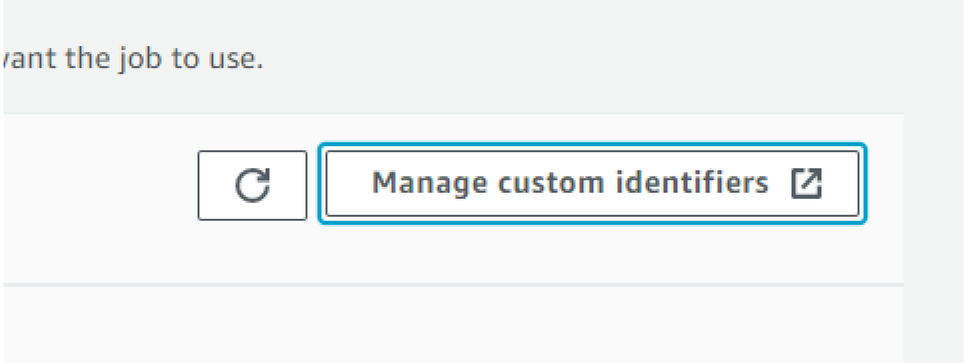
● All

Use all managed data identifiers.

Click on the “Next” button.

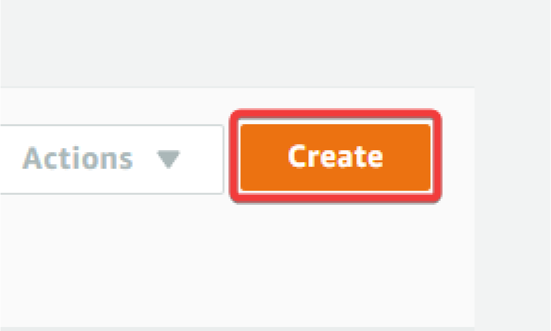


Step 20: Create a custom identifier to find the sensitive data from the json file. Click on “Manage custom identifier”.

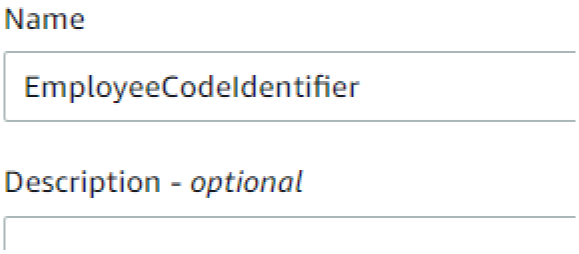


A custom data identifier is a set of criteria that you define to detect sensitive data. The criteria consist of a regular expression (regex) that defines a text pattern to match and, optionally, character sequences and a proximity rule that refine the results.

Step 21: Click on the “Create” button.



Step 22: Set the identifier name as “EmployeeCodeIdentifier”.



Name

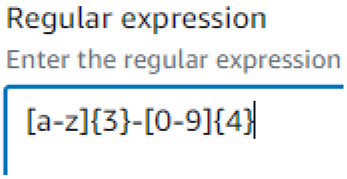
EmployeeCodeIdentifier

Description - *optional*

Step 23: Copy and paste the following regular expression to match the sensitive data in the file.

Regular expression: [a-z]{3}-[0-9]{4}

This identifier finds the data present in the format of ABC-0123 i.e. three characters, dash and followed by four numbers.

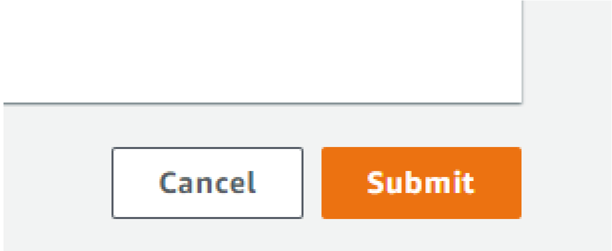


Regular expression

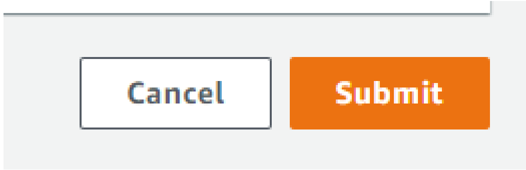
Enter the regular expression

[a-z]{3}-[0-9]{4}

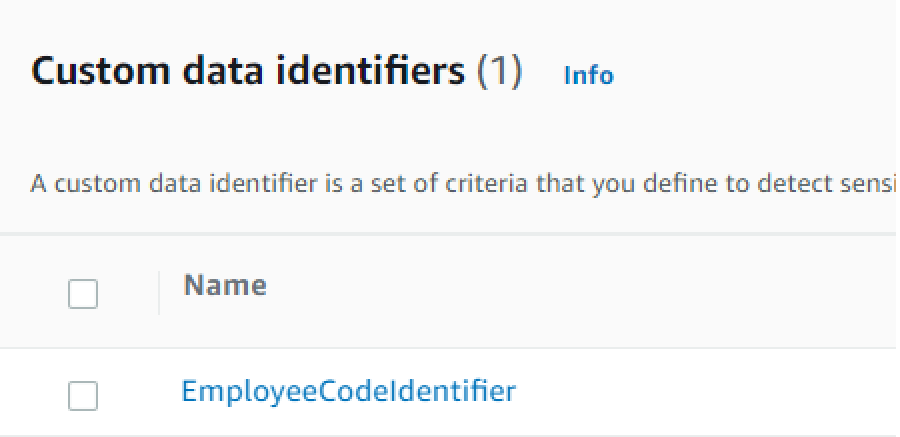
Click on "Submit".



Review the settings and click on "Submit" again.



Successfully created custom identifier.

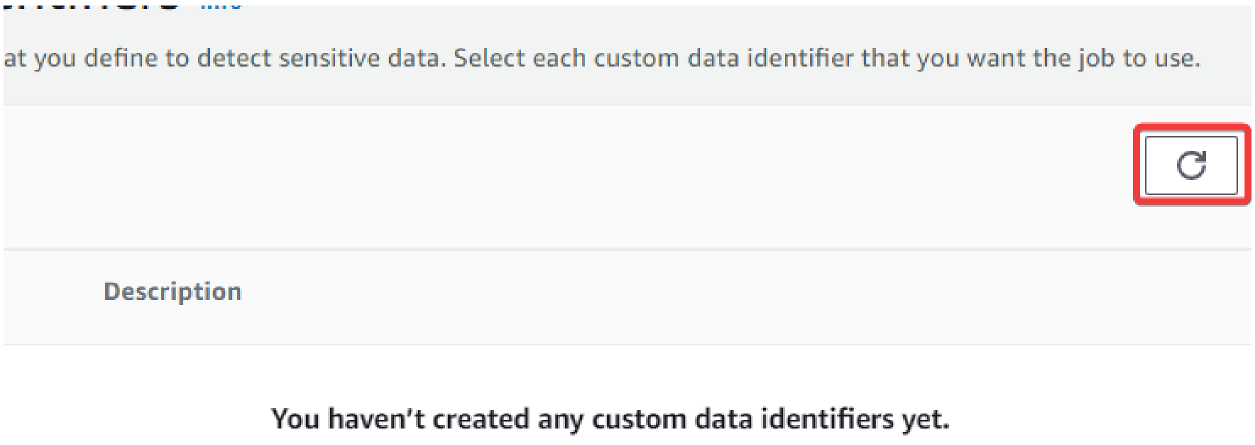


Custom data identifiers (1) Info

A custom data identifier is a set of criteria that you define to detect sensi

□	Name
□	EmployeeCodeIdentifier

Step 24: Navigate back to the job creation stage and click on the refresh button.

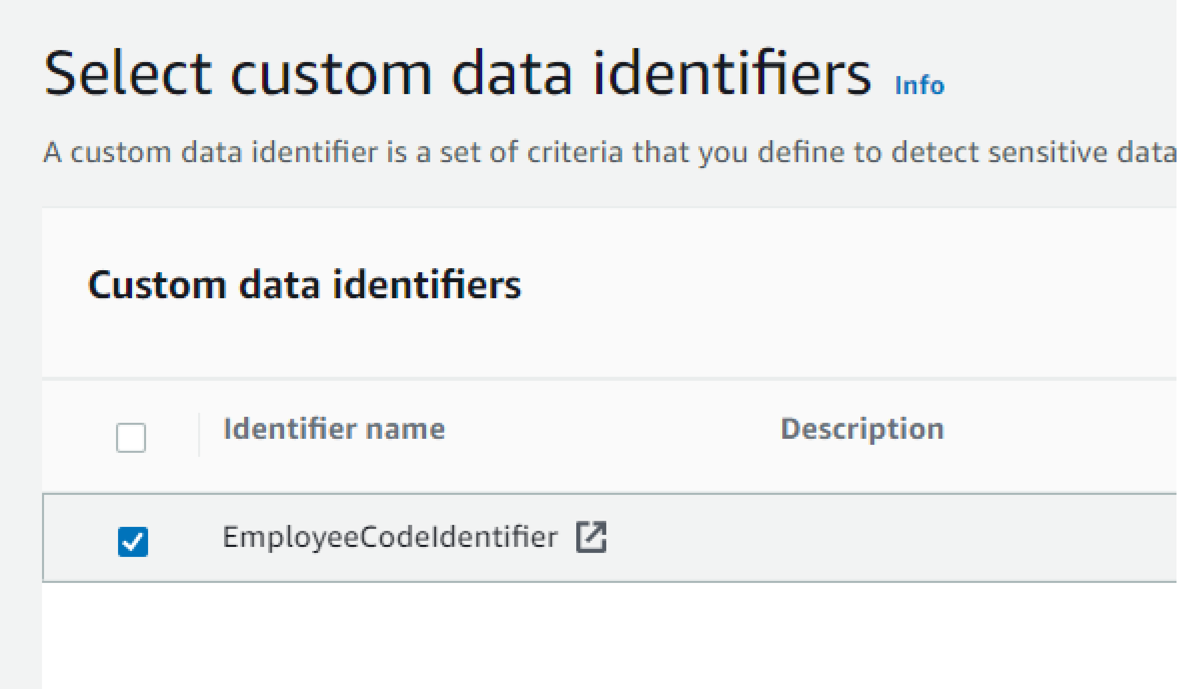


at you define to detect sensitive data. Select each custom data identifier that you want the job to use.

Description

You haven't created any custom data identifiers yet.

Step 25: Now select the created custom identifier.



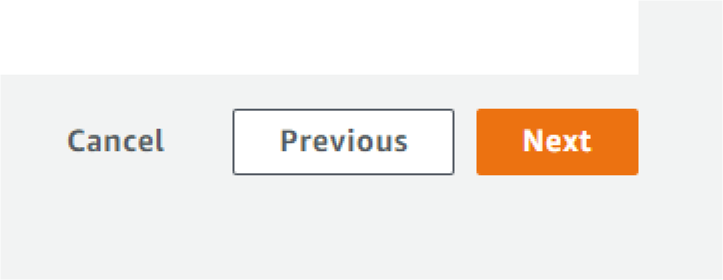
Select custom data identifiers

A custom data identifier is a set of criteria that you define to detect sensitive data

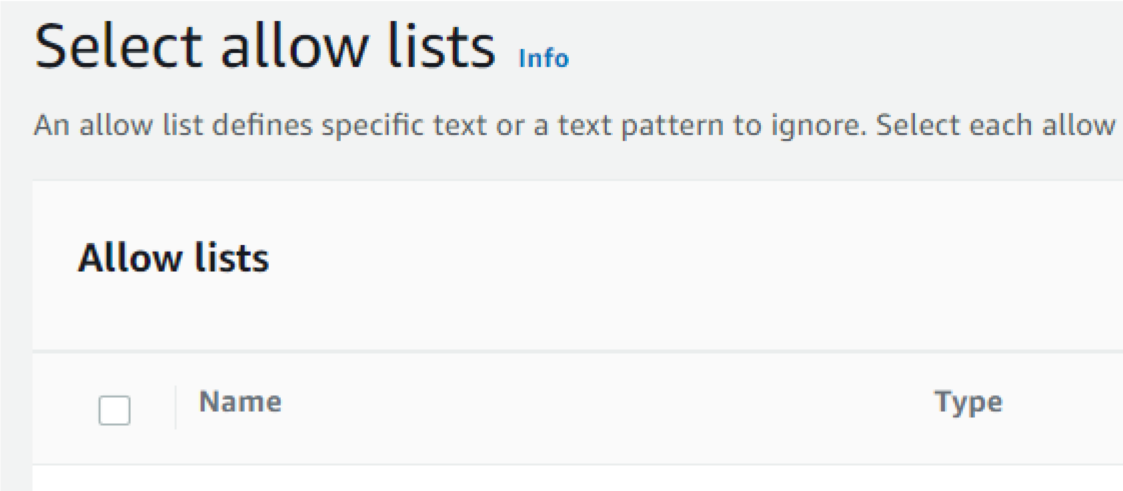
Custom data identifiers

□	Identifier name	Description
☑	EmployeeCodeIdentifier	

Click on the “Next” button.



Keep the allow lists as empty. With allow lists in Amazon Macie, you can define specific text and text patterns that you want Macie to ignore when it inspects Amazon S3 objects for sensitive data.



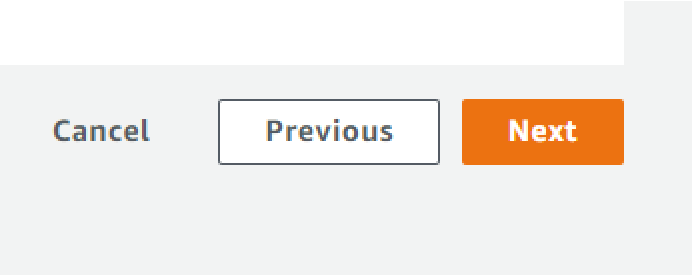
Select allow lists Info

An allow list defines specific text or a text pattern to ignore. Select each allow

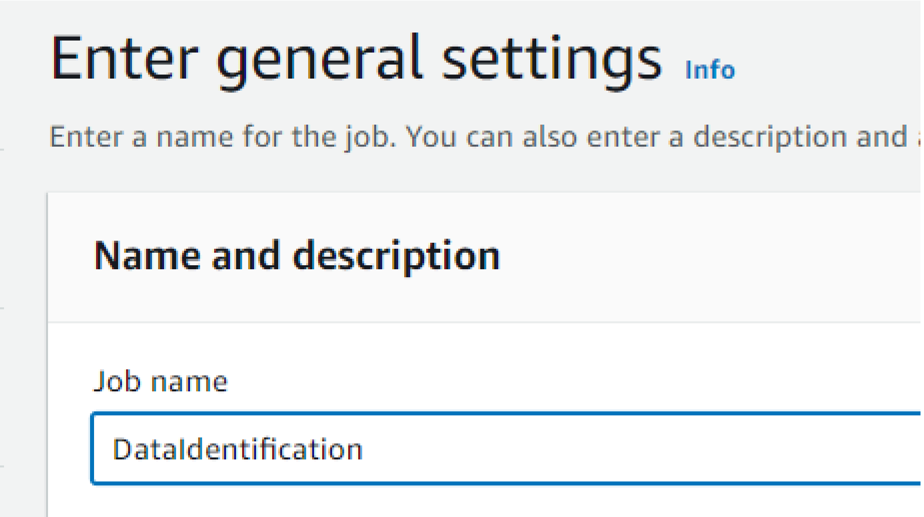
Allow lists

□	Name	Type

Click on the “Next” button.



Step 26: Enter the job name as “DataIdentification”.



Enter general settings Info

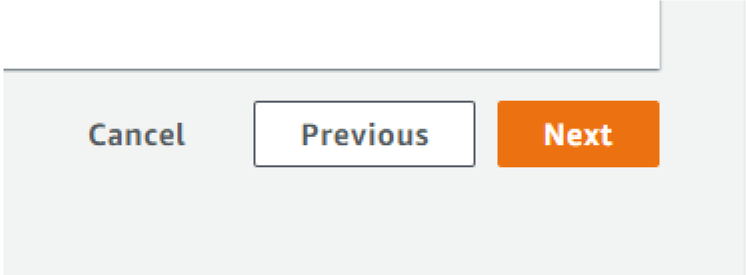
Enter a name for the job. You can also enter a description and

Name and description

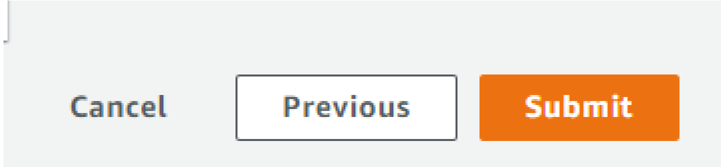
Job name

DataIdentification

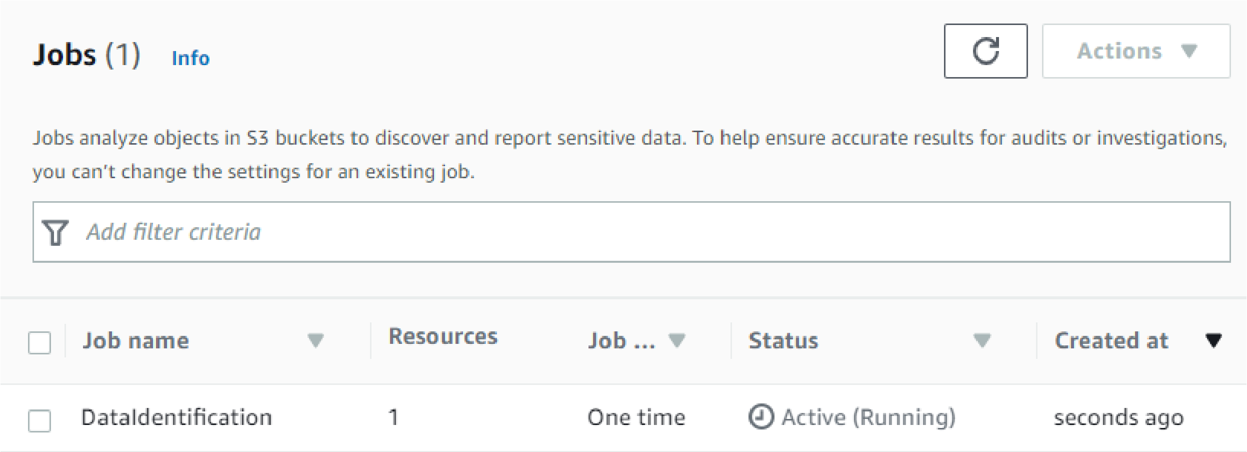
Now click on the “Next” button.



Now click on the “Submit” button.



Successfully created a macie job



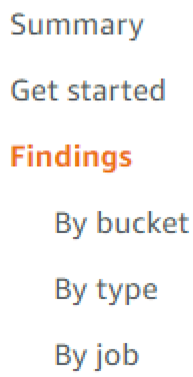
Jobs (1)

Jobs analyze objects in S3 buckets to discover and report sensitive data. To help ensure accurate results for audits or investigations, you can’t change the settings for an existing job.

Add filter criteria

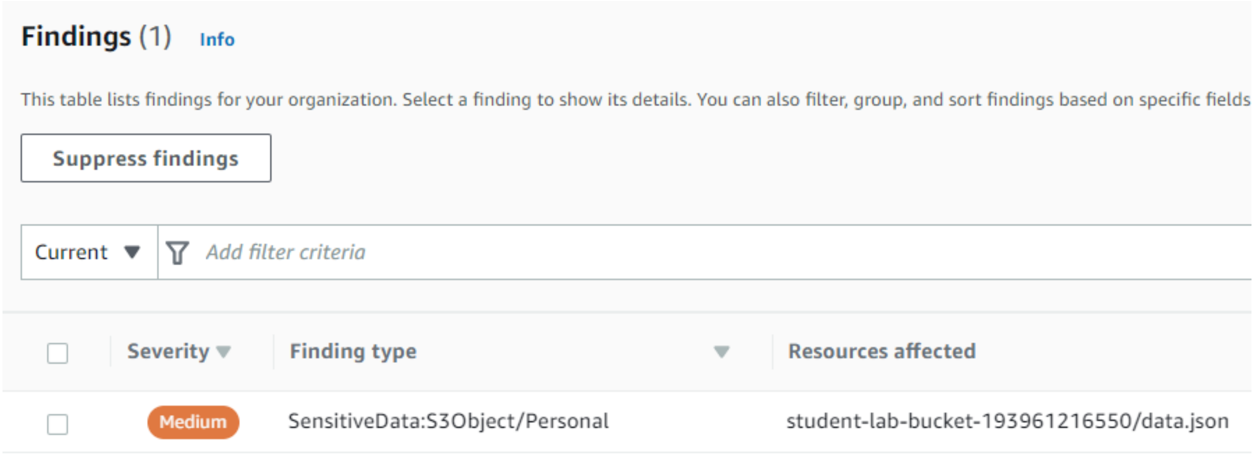
□	Job name	Resources	Job ...	Status	Created at
□	DataIdentification	1	One time	Active (Running)	seconds ago

Step 27: Click on “Findings”.



If Macie discovers sensitive data in an object, Macie creates a sensitive data finding. A sensitive data finding is a detailed report of sensitive data that Macie found in an object.

Step 28: Select the finding with the type “SensitiveData:S3Object/Personal”.

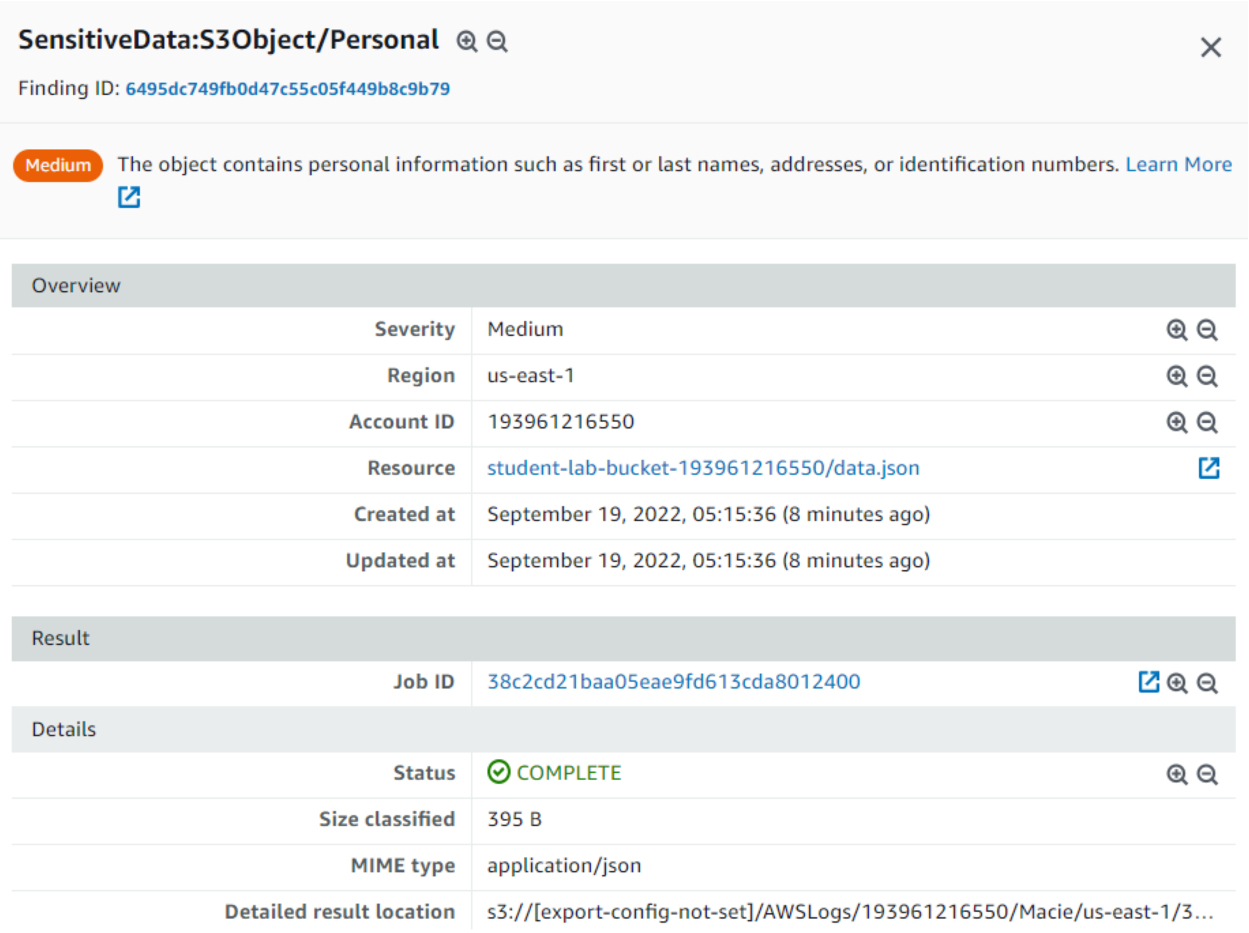

Findings (1) Info

This table lists findings for your organization. Select a finding to show its details. You can also filter, group, and sort findings based on specific fields

□	Severity ▼	Finding type ▼	Resources affected
□	Medium	SensitiveData:S3Object/Personal	student-lab-bucket-193961216550/data.json

A sensitive data finding is a detailed report of sensitive data in an S3 object. Macie generates these findings when it discovers sensitive data in S3 objects that you configure a sensitive data discovery job to analyze.

This finding indicates that the object contains personally identifiable information (such as full names or mailing addresses), personal health information (such as health insurance or medical identification numbers), or a combination of the two. In our case the sensitive data is the employee code.



SensitiveData:S3Object/Personal

Finding ID: 6495dc749fb0d47c55c05f449b8c9b79

Medium The object contains personal information such as first or last names, addresses, or identification numbers. Learn More

Overview

Severity	Medium
Region	us-east-1
Account ID	193961216550
Resource	student-lab-bucket-193961216550/data.json
Created at	September 19, 2022, 05:15:36 (8 minutes ago)
Updated at	September 19, 2022, 05:15:36 (8 minutes ago)

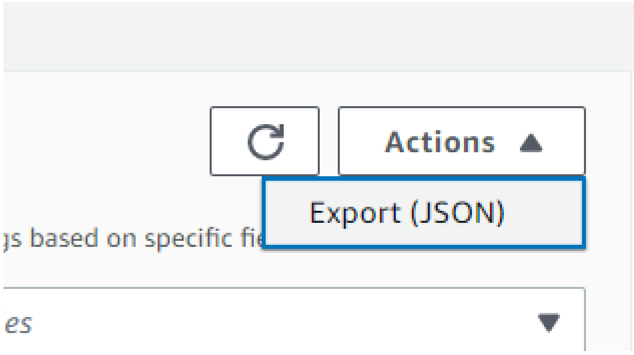
Result

Job ID	38c2cd21baa05eae9fd613cda8012400

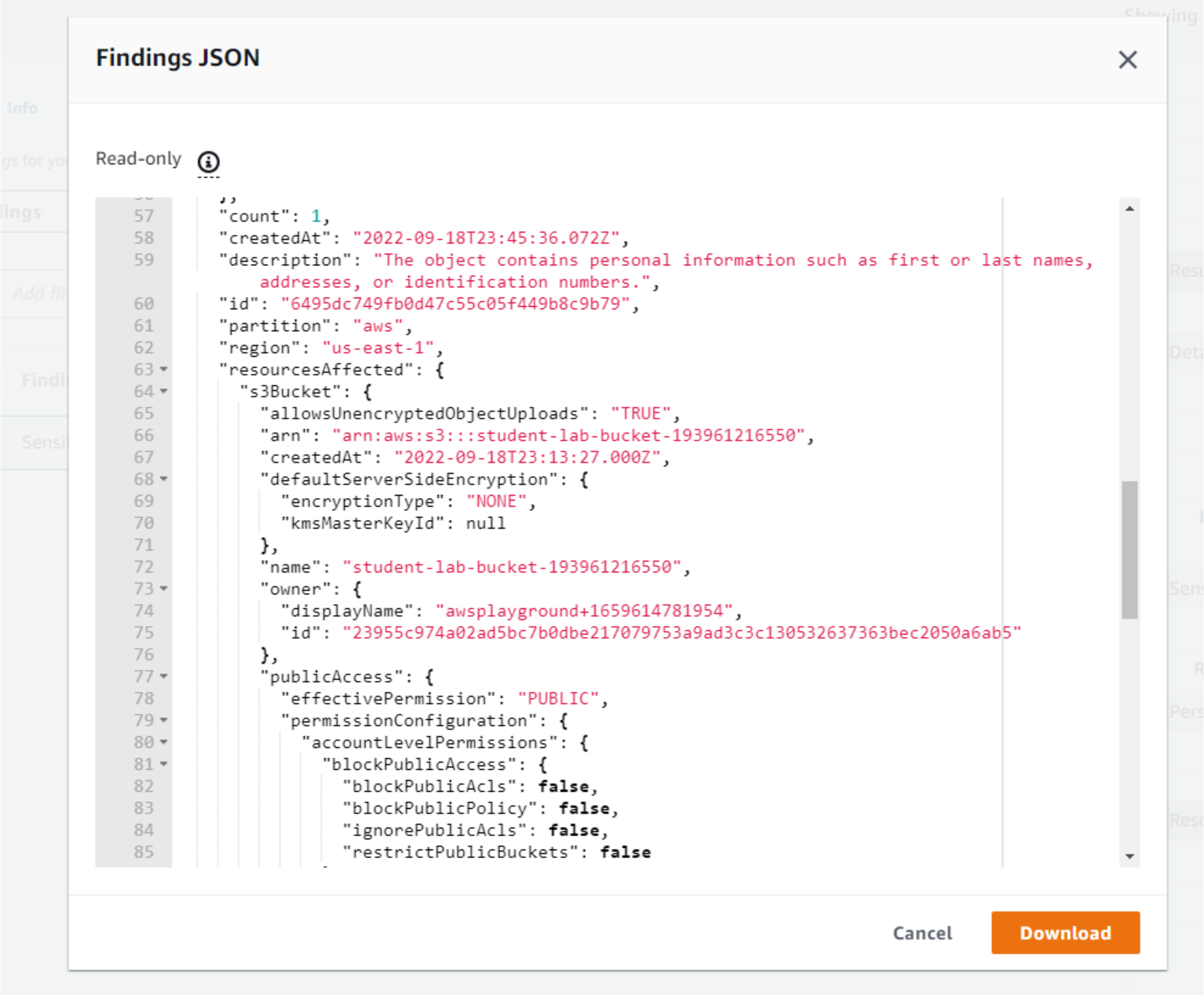
Details

Status	✓ COMPLETE
Size classified	395 B
MIME type	application/json
Detailed result location	s3://[export-config-not-set]/AWSLogs/193961216550/Macie/us-east-1/3…

Step 29: Select the finding and click on "Export(JSON) under Actions".



The complete detail of the finding will be available in the JSON.



```
  },
  "count": 1,
  "createdAt": "2022-09-18T23:45:36.072Z",
  "description": "The object contains personal information such as first or last names, addresses, or identification numbers.",
  "id": "6495dc749fb0d47c55c05f449b8c9b79",
  "partition": "aws",
  "region": "us-east-1",
  "resourcesAffected": {
    "s3Bucket": {
      "allowsUnencryptedObjectUploads": "TRUE",
      "arn": "arn:aws:s3:::student-lab-bucket-193961216550",
      "createdAt": "2022-09-18T23:13:27.000Z",
      "defaultServerSideEncryption": {
        "encryptionType": "NONE",
        "kmsMasterKeyId": null
      },
      "name": "student-lab-bucket-193961216550",
      "owner": {
        "displayName": "awsplayground+1659614781954",
        "id": "23955c974a02ad5bc7b0dbe217079753a9ad3c3c130532637363bec2050a6ab5"
      },
      "publicAccess": {
        "effectivePermission": "PUBLIC",
        "permissionConfiguration": {
          "accountLevelPermissions": {
            "blockPublicAccess": {
              "blockPublicAcls": false,
              "blockPublicPolicy": false,
              "ignorePublicAcls": false,
              "restrictPublicBuckets": false
```

References:

1. Amazon Macie (https://docs.aws.amazon.com/macie/latest/user/what-is-macie.html)