

ATTACKDEFENSE LABS COURSES
PENTESTER ACADEMY TOOL BOX PENTESTING
JOINT WORLD-CLASS TRAINERS TRAINING HACKER
TOOL BOX PATV HACKER
HACKER PENTESTING
PATV RED TEAM LABS ATTACKDEFENSE LABS
TRAINING COURSES ACCESS POINT PENTESTER
TEAM LABS PENTESTER
ACCESS POINT WORLD-CLASS TRAINERS
WORLD-CLASS TRAINERS
ATTACKDEFENSE LABS TRAINING COURSE SPATV ACCESS
PENTESTER ACADEMY
ATTACKDEFENSE LABS PENTESTER ACADEMY
COURSES PENTESTER ACADEMY TOOL BOX PENTESTING
TOOL BOX
ACKER PENTESTING
PATV RED TEAM LABS ATTACKDEFENSE LABS
COURSES PENTESTER ACADEMY
PENTESTER ACADEMY ATTACKDEFENSE LABS
WORLD-CLASS TRAINERS
RED TEAM TRAINING
PENTESTER ACADEMY TOOL BOX
PENTESTING

ATTACK DEFENSE

by PentesterAcademy

Name	S3 Enumeration
URL	https://attackdefense.com/challengedetails?cid=2298
Type	AWS Cloud Security : S3

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:

Console Based Enumeration

Step 1: Sign in into AWS console using AWS access credentials.

Access Credentials to your AWS lab Account

Login URL	https://276384657722.signin.aws.amazon.com/console
Region	Asia Pacific (Singapore) ap-southeast-1
Username	BuIRCSiUfoyTKnSirgrA
Password	Ty9yi1O1VNWdKy7W
Access Key ID	AKIAUAWOPGE5BNVRX7UJ
Secret Access Key	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

Sign in as IAM user

Account ID (12 digits) or account alias

276384657722

IAM user name

BuIRCSiUfoyTKnSirgrA

Password

Sign in

[Sign in using root user email](#)

[Forgot password?](#)



Simplify persistent storage for containers

Customers can now use Amazon EFS, cloud-native, fully managed, shared storage for Amazon ECS and AWS Fargate

Step 2: Navigate to S3 dashboard.

Amazon S3

Access S3-backed file shares on premises and reduce local storage costs using AWS Storage Gateway.

Buckets (21)

Buckets are containers for data stored in S3. [Learn more](#)

Name	AWS Region	Access
ad-secret-bucket-for-role	US East (N. Virginia) us-east-1	Objects can be public
attackdefense-discover-bucket	Asia Pacific (Singapore) ap-southeast-1	Error
data-extractor-repo	US West (Oregon) us-west-2	
developers-secret-bucket	US East (Ohio) us-east-2	
file-uploader-saved-files	Asia Pacific (Singapore) ap-southeast-1	
insecurecorp-code	Asia Pacific (Singapore) ap-southeast-1	
insecurecorp-customer	Asia Pacific (Singapore) ap-southeast-1	
insecurecorp-documents	Asia Pacific (Singapore) ap-southeast-1	
ipcalc	Asia Pacific (Singapore) ap-southeast-1	

Step 3: Click on bucket name to check bucket objects.

data-extractor-repo

Objects Properties Permissions Metrics Management Access Points

Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 Inventory](#) to get a list of all objects in your bucket. For others to access your objects, you must grant them permission.

List versions  [Delete](#) [Actions ▾](#) [Create folder](#) [Upload](#)

 [Find objects by prefix](#)

<input type="checkbox"/>	Name	Type	Last modified
--------------------------	------	------	---------------

<input type="checkbox"/>	 DataExtractor.zip	zip	October 29, 2020, 14:54:56 (UTC-07:00)
--------------------------	---	-----	--

Step 4: Click on the properties tab to view bucket properties.

Objects **Properties** Permissions Metrics Management Access Points

Bucket overview

AWS Region

US West (Oregon) us-west-2

Amazon resource name (ARN)

 arn:aws:s3:::data-extractor-repo

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your bucket. Learn more .

[Edit](#)

Bucket Versioning

Enabled

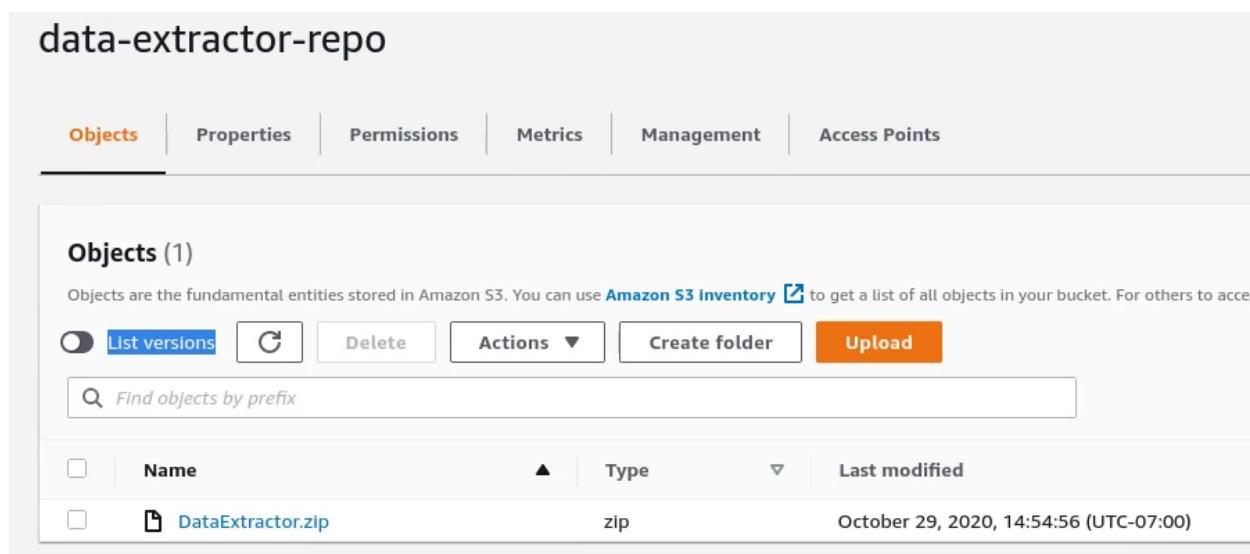
Multi-factor authentication (MFA) delete

An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, learn more .

Disabled

Bucket versioning is enabled !

Step 5: Check the object versions for the bucket on the objects tab.



data-extractor-repo

Objects Properties Permissions Metrics Management Access Points

Objects (1)

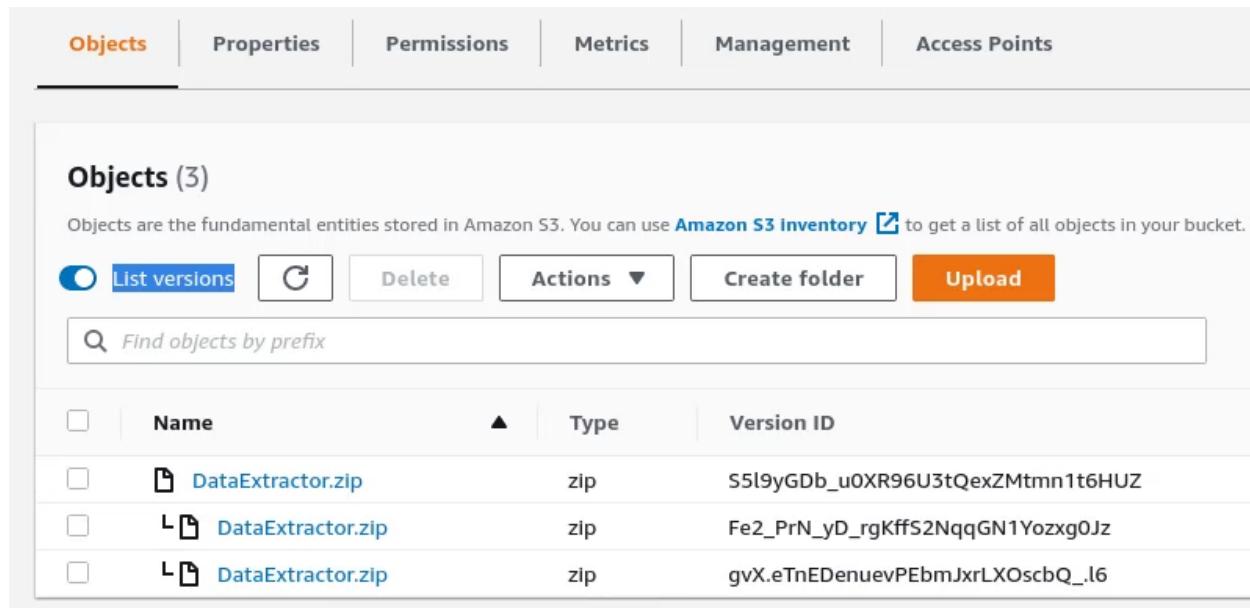
Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 Inventory](#) to get a list of all objects in your bucket. For others to access your objects, you must grant them permission to do so.

List versions Delete

Find objects by prefix

<input type="checkbox"/>	Name	Type	Last modified
<input type="checkbox"/>	DataExtractor.zip	zip	October 29, 2020, 14:54:56 (UTC-07:00)

Turn on “List versions”



Objects Properties Permissions Metrics Management Access Points

Objects (3)

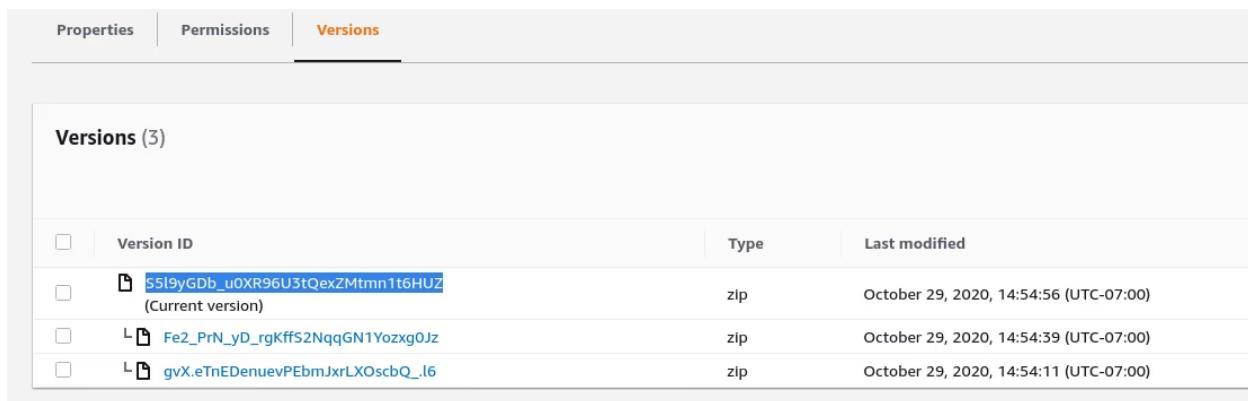
Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 Inventory](#) to get a list of all objects in your bucket. For others to access your objects, you must grant them permission to do so.

List versions Delete

Find objects by prefix

<input type="checkbox"/>	Name	Type	Version ID
<input type="checkbox"/>	DataExtractor.zip	zip	S5l9yGD... Fe2_PrN_yD_rgKffS2NqqGN1Yozxg0Jz gvX.eTnEDenuevPEbmJxrLXOscbQ_.l6

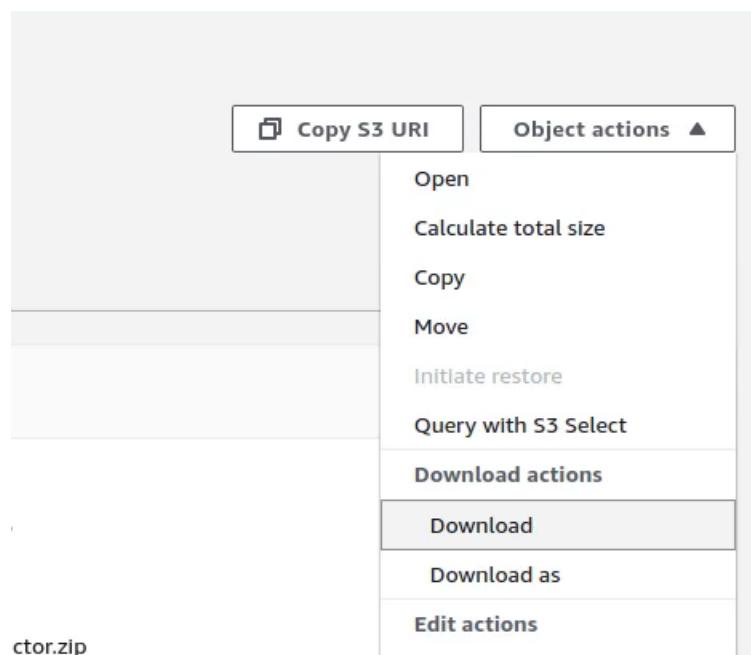
Step 6: Click on the object and navigate to the versions tab to check version details.

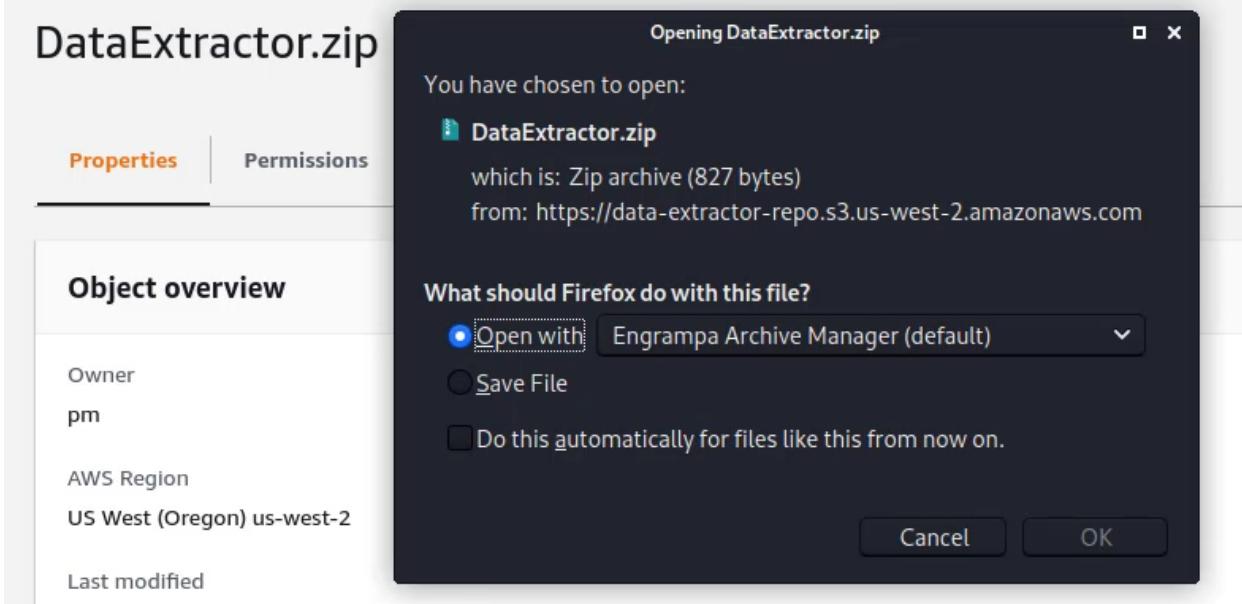


The screenshot shows the AWS S3 console with the 'Versions' tab selected. It displays three object versions for the file 'ctor.zip'. The columns are 'Version ID', 'Type', and 'Last modified'. The first version is the current version, while the other two are older versions.

Version ID	Type	Last modified
5s19yGDb_u0XR9GU3tQexZMtmn1t6HUZ (Current version)	zip	October 29, 2020, 14:54:56 (UTC-07:00)
Fe2_PrN_yD_rgKffS2NqqGN1Yozxg0Jz	zip	October 29, 2020, 14:54:39 (UTC-07:00)
gvX.eTnEDenuevPEbmJxrLXOscbQ_l6	zip	October 29, 2020, 14:54:11 (UTC-07:00)

Step 7: Navigate to properties tab and download object to enumerate contents.



A screenshot of a Vim editor window. The title bar says "lambda_function.py (~/.cache/fr-hsXiFn) - VIM". The menu bar includes File, Edit, Tools, Syntax, Buffers, Window, and Help. The toolbar below has icons for file operations like Open, Save, Print, and Undo/Redo. The main code area contains the following Python code:

```
def lambda_handler(event, context):
    response = None

    params = json.loads(event["body"])

    if params == None:
        response = { "msg": "error: missing parameters" }

    else:
        CardHolder = None
        TableName = "CardDetails"
        Operator = "EQ"

        if "CardHolder" in params:
            CardHolder = params["CardHolder"]

        else:
            response = { "msg": "error: missing parameters: CardHolder (required)" }
```

The status bar at the bottom right shows "46,1" and "76%".

Step 8: Go back to S3 bucket object list and click on the permissions tab to check bucket permissions.

Amazon S3 > data-extractor-repo

data-extractor-repo

Objects Properties Permissions Metrics Management Access Points

Permissions overview

Access

Bucket and objects not 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 all. In order to ensure that public access to all your S3 buckets and objects is blocked, 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. [Learn more](#)

Edit

Block all public access

On

- Block public access to buckets and objects granted through *new* access control lists (ACLs)
- Block public access to buckets and objects granted through *any* access control lists (ACLs)

Bucket is not public.

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

Public access is blocked because Block Public Access settings are turned on for this bucket.
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

No policy to display.

Bucket policy.



Object ownership

Assume ownership of new objects uploaded to this bucket. [Learn more](#)

Object ownership

Object writer

The object writer remains the object owner.

Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. [Learn more](#)

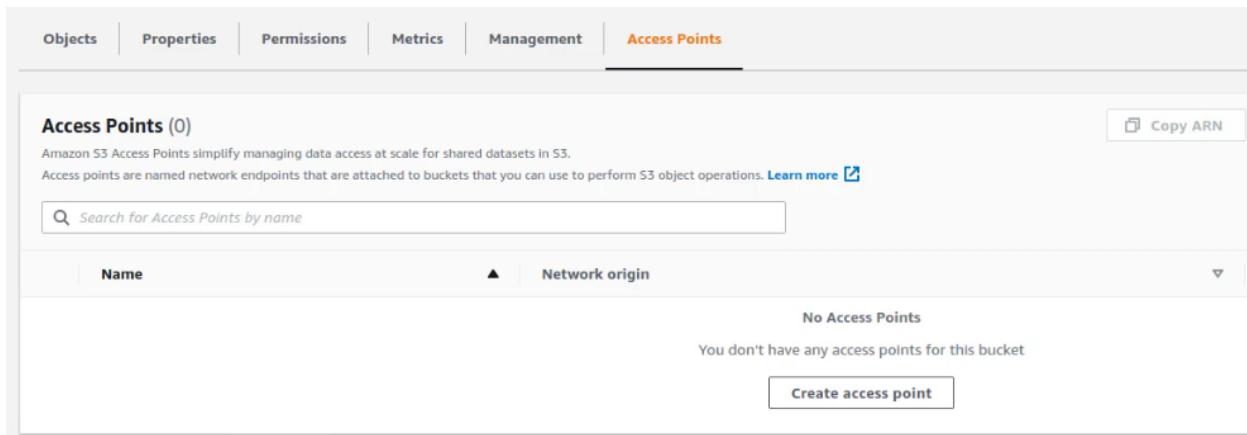
Public access is blocked because Block Public Access settings are turned on for this bucket.

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

Grantee	Objects
Bucket owner (your AWS account)	List, Write
Canonical ID: 7153c083c4d4c8b9bea0cdd3c5ec7d8ec99ba029736225369fa61ae449322de5	
Everyone (public access)	-
Group: http://acs.amazonaws.com/groups/global/AllUsers	

Bucket ownership and ACL.

Go to 'Access Points' tab to check the named network endpoints attached to the bucket.



The screenshot shows the AWS S3 bucket details page with the 'Access Points' tab selected. The 'Access Points (0)' section indicates there are no access points. A 'Create access point' button is available to add one.

Step 9: Similarly enumerate other buckets.

Buckets (21)

Buckets are containers for data stored in S3. [Learn more](#)

Name	AWS Region	Access
insecurecorp-code	Asia Pacific (Singapore) ap-southeast-1	Public
insecurecorp-customer	Asia Pacific (Singapore) ap-southeast-1	Public
insecurecorp-documents	Asia Pacific (Singapore) ap-southeast-1	Public
ipcalc-with-login	Asia Pacific (Singapore) ap-southeast-1	Public

Objects (16)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 Inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to

Name	Type	Last modified
apply.html	html	December 5, 2020, 06:40:08 (UTC-08:00)
css/	Folder	-
faq.html	html	December 5, 2020, 06:40:09 (UTC-08:00)
favicon.ico	ico	December 5, 2020, 06:40:09 (UTC-08:00)
fonts/	Folder	-
images/	Folder	-
index.html	html	December 5, 2020, 06:40:09 (UTC-08:00)

Bucket objects.

insecurecorp-code

Publicly accessible

Objects Properties Permissions Metrics Management Access Points

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 all. In order to ensure that public access to all your S3 buckets 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 with you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

[Edit](#)

Block all public access

 Off

Block public access to buckets and objects granted through new access control lists (ACLs)

 Off

Bucket is publicly accessible !

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Principal": "*",  
            "Action": [  
                "S3:Get*",  
                "S3>List*"  
            ],  
            "Resource": [  
                "arn:aws:s3:::insecurecorp-code",  
                "arn:aws:s3:::insecurecorp-code/*"  
            ]  
        },  
        {  
            "Effect": "Deny",  
            "Principal": "*",  
            "Action": "S3:Put*",  
            "Resource": "arn:aws:s3:::insecurecorp-code/*"  
        }  
    ]  
}
```

Bucket policy.

Object ownership
Assume ownership of new objects uploaded to this bucket. [Learn more](#)

Object ownership
Object writer
The object writer remains the object owner.

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: 7153c083c4d4c8b9bea0cd35ec7d8ec99ba029736225369fa61ae449322da5	List, Write	Read, Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	-	-

Ownership and ACL.

Step 10: Navigate to S3 storage lens dashboard from the left panel.

Amazon S3

- Buckets
- Access Points
- Batch Operations
- Access analyzer for S3

Block Public Access settings for this account

▼ Storage Lens **Dashboard**

AWS Organizations settings

Amazon S3 > Storage Lens

Storage Lens

Storage Lens provides visibility into storage usage and activity trends at the organization or account level.

▼ Getting started with Storage Lens

Dashboards (1)

In addition to the default-account-dashboard that is auto-generated for your account, you can create custom dashboards scoped to your AWS organization or specific accounts, Regions, and services.

Search dashboards

Dashboard name	Home Region
default-account-dashboard	US East (N. Virginia) us-east-1

Step 11: Click on the dashboard name to view details.

default-account-dashboard

▶ Filters

Apply temporary filters to further limit the scope of this dashboard.

Overview Account AWS Region Storage class Bucket

Snapshot for Mar 10, 2021

A glossary of metrics is available. [Learn more](#)

Total storage	Object count	Avg. object size	Active buckets
55.0 MB	401	140.5 KB	19

Metrics

Summary	Cost efficiency	Data protection	% change comparison	Day/day	Week/week
Metric name	Total for Mar 10, 2021	% change	30-day trend		
Total storage	55.0 MB	0%	⟳		
Object count	401	0%	⟳		
Avg. object size	140.5 KB	0%	⟳		
Active buckets	19	0%	⟳		
Accounts	1	0%	⟳		

CLI Based Enumeration

Step 1: Configure AWS CLI with AWS access keys

Command: aws configure

Access Credentials to your AWS lab Account

Login URL	https://276384657722.signin.aws.amazon.com/console
Region	Asia Pacific (Singapore) ap-southeast-1
Username	grLFsxUINbOQxwlXbNoS
Password	uJll1tZw4DElhy4
Access Key ID	AKIAUAWOPGE5P7XDAIFO
Secret Access Key	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

```
File Actions Edit View Help
⚡ root@Kali ➞ aws configure
AWS Access Key ID [*****AIFO]: AKIAUAWOPGE5P7XDAIFO
AWS Secret Access Key [*****SXJI]: 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
Default region name [ap-southeast-1]:
Default output format [None]:
⚡ root@Kali ➞ █
```

Step 2: List S3 buckets.

Command: aws s3api list-buckets

```
File Actions Edit View Help
$ root@Kali ~ ➔ aws s3api list-buckets
{
  "Buckets": [
    {
      "Name": "ad-secret-bucket-for-role",
      "CreationDate": "2021-01-20T08:28:42.000Z"
    },
    {
      "Name": "attackdefense-discover-bucket",
      "CreationDate": "2020-12-21T09:46:25.000Z"
    },
    {
      "Name": "data-extractor-repo",
      "CreationDate": "2020-10-29T21:53:54.000Z"
    },
    {
      "Name": "developers-secret-bucket",
      "CreationDate": "2020-12-21T10:10:59.000Z"
    },
    {
      "Name": "file-uploader-saved-files",
      "CreationDate": "2021-03-12T19:16:16.000Z"
    }
  ]
}
```

Step 3: Check bucket location.

Command: aws s3api get-bucket-location --bucket data-extractor-repo

```
File Actions Edit View Help
$ root@Kali ~ ➔ aws s3api get-bucket-location --bucket data-extractor-repo
{
  "LocationConstraint": "us-west-2"
}
$ root@Kali ~ ➔ █
```

Step 4: Enumerate bucket objects

Commands:

```
aws s3api list-objects-v2 --bucket data-extractor-repo
aws s3api list-objects --bucket file-uploader-saved-files
```

```
File Actions Edit View Help
$ root@Kali ~ ➔ aws s3api list-objects-v2 --bucket data-extractor-repo
{
  "Contents": [
    {
      "Key": "DataExtractor.zip",
      "LastModified": "2020-10-29T21:54:56.000Z",
      "ETag": "\"014458aab6fe8320f7c6a5e86563427b\"",
      "Size": 827,
      "StorageClass": "STANDARD"
    }
  ]
}
$ root@Kali ~ ➔ █
```

```
File Actions Edit View Help
$ root@Kali ~ ➔ aws s3api list-objects --bucket file-uploader-saved-files
{
  "Contents": [
    {
      "Key": "Flag",
      "LastModified": "2021-03-12T19:17:18.000Z",
      "ETag": "\"4d0569150897d2ec346e9b0ae5399dd5\"",
      "Size": 32,
      "StorageClass": "STANDARD",
      "Owner": {
        "DisplayName": "pm",
        "ID": "7153c083c4d4c8b9bea0cdd3c5ec7d8ec99ba029736225369fa61ae449322da5"
      }
    }
  ]
}
$ root@Kali ~ ➔ █
```

Step 5: Check object versions.

Command: aws s3api list-object-versions --bucket data-extractor-repo

```
File Actions Edit View Help
$ root@Kali ~ ➔ aws s3api list-object-versions --bucket data-extractor-repo
{
  "Versions": [
    {
      "ETag": "\"014458aab6fe8320f7c6a5e86563427b\"",
      "Size": 827,
      "StorageClass": "STANDARD",
      "Key": "DataExtractor.zip",
      "VersionId": "S5l9yGDb_u0XR96U3tQexZMtmn1t6HUZ",
      "IsLatest": true,
      "LastModified": "2020-10-29T21:54:56.000Z",
      "Owner": {
        "DisplayName": "pm",
        "ID": "7153c083c4d4c8b9bea0cdd3c5ec7d8ec99ba029736225369fa61ae449322da5"
      }
    },
    {
      "ETag": "\"7c437b026a869f8d51a2d2ddae25d874\"",
      "Size": 844,
      "StorageClass": "STANDARD",
      "Key": "DataExtractor.zip",
    }
  ]
}
```

Step 6: Check bucket ACLs and objects ACLs.

Commands:

```
aws s3api get-bucket-acl --bucket file-uploader-saved-files
aws s3api get-object-acl --bucket file-uploader-saved-files --key flag
```

```
File Actions Edit View Help
$ root@Kali ~ ➔ aws s3api get-bucket-acl --bucket file-uploader-saved-files
{
  "Owner": {
    "DisplayName": "pm",
    "ID": "7153c083c4d4c8b9bea0cdd3c5ec7d8ec99ba029736225369fa61ae449322da5"
  },
  "Grants": [
    {
      "Grantee": {
        "DisplayName": "pm",
        "ID": "7153c083c4d4c8b9bea0cdd3c5ec7d8ec99ba029736225369fa61ae449322da5",
        "Type": "CanonicalUser"
      },
      "Permission": "FULL_CONTROL"
    },
    {
      "Grantee": {
        "Type": "Group",
        "URI": "http://acs.amazonaws.com/groups/global/AllUsers"
      },
      "Permission": "READ"
    }
  ]
}
```

```
File Actions Edit View Help
$ root@Kali:~$ aws s3api get-object-acl --bucket file-uploader-saved-files --key flag
{
    "Owner": {
        "DisplayName": "pm",
        "ID": "7153c083c4d4c8b9bea0cdd3c5ec7d8ec99ba029736225369fa61ae449322da5"
    },
    "Grants": [
        {
            "Grantee": {
                "DisplayName": "pm",
                "ID": "7153c083c4d4c8b9bea0cdd3c5ec7d8ec99ba029736225369fa61ae449322da5",
                "Type": "CanonicalUser"
            },
            "Permission": "FULL_CONTROL"
        },
        {
            "Grantee": {
                "Type": "Group",
                "URI": "http://acs.amazonaws.com/groups/global/AllUsers"
            },
            "Permission": "READ_ACP"
        }
    ]
}
```

Step 7: Download objects from the S3 bucket.

Commands:

```
aws s3 cp s3://file-uploader-saved-files/flag .
cat flag
```

```
File Actions Edit View Help
$ root@Kali:~$ aws s3 cp s3://file-uploader-saved-files/flag .
download: s3://file-uploader-saved-files/flag to ./flag
$ root@Kali:~$ cat flag
643a3866a6a360a70219f7e387a1e528#
$ root@Kali:~$
```

Step 8: Check bucket policy status.

Command: aws s3api get-bucket-policy-status --bucket insecurecorp-code

```
* root@Kali ➤ aws s3api get-bucket-policy-status --bucket insecurecorp-code
{
    "PolicyStatus": {
        "IsPublic": true
    }
}
* root@Kali ➤
```

Step 9: Get bucket policy and beautify the output.

Command: aws s3api get-bucket-policy --bucket insecurecorp-code --output text | python -m json.tool

```
* root@Kali ➤ aws s3api get-bucket-policy --bucket insecurecorp-code --output text | python -m json.tool
{
    "Statement": [
        {
            "Action": [
                "s3:Get*",
                "s3>List*"
            ],
            "Effect": "Allow",
            "Principal": "*",
            "Resource": [
                "arn:aws:s3:::insecurecorp-code",
                "arn:aws:s3:::insecurecorp-code/*"
            ]
        },
        {
            "Action": "s3:Put*",
            "Effect": "Deny",
            "Principal": "*",
            "Resource": [
                "arn:aws:s3:::insecurecorp-code",
                "arn:aws:s3:::insecurecorp-code/*"
            ]
        }
    ],
    "Version": "2012-10-17"
}
* root@Kali ➤
```

Step 9: Check the public access block for a bucket.

Command: aws s3api get-public-access-block --bucket data-extractor-repo

```
{  
    "PublicAccessBlockConfiguration": {  
        "BlockPublicAcls": true,  
        "IgnorePublicAcls": true,  
        "BlockPublicPolicy": true,  
        "RestrictPublicBuckets": true  
    }  
}
```

References:

1. AWS CLI (<https://docs.aws.amazon.com/cli/latest/reference/>)