

Introduction

S: In these exercises you will learn how to:

- create IAM users in AWS;
- secure access to Object Storage S3 in AWS.

How to deliver your assignments?

Fill in this document with required information. Answer questions and upload the document to Canvas at most one week after the assignment is given.

Assignment 1: Create IAM users in AWS

Difficulty: ★★☆☆☆. Estimated time: 45-60 minutes.

Follow the demo of the class:

- Create 3 IAM users using your case-study group root account.
- Launch an EC2 instance
- Configure password policy, use more complex options than the default one
- Create access keys for one of the IAM user
- Install AWS CLI
- Configure AWS CLI with the access keys, run:

aws configure

- Demonstrate the EC2 instance running via AWS CLI. Run:

aws ec2 describe-instances

Provide a screenshot of AWS CLI configuration and EC2 instances overview

ch for services, features, blogs, docs, and more [Alt+S] Frankfurt edris @ group14

Instances (2) Info

Find instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
ubuntu	i-090cae819d2cabcee	Stopped	t2.micro	-	No alarms	eu-central-1a
SNO_assignment	<u>i-0f2b24a5d1fcb18e6</u>	<u>Running</u>	t2.micro	2/2 checks passed	No alarms	eu-central-1b

Instances (2) Info

Find instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status
ubuntu	i-090cae819d2cabcee	Stopped	t2.micro	-	No alarms
SNO_assignment	<u>i-0f2b24a5d1fcb18e6</u>	<u>Running</u>	t2.micro	2/2 checks passed	No alarms

Select an instance

```
{
  "AmiLaunchIndex": 0,
  "ImageId": "ami-065deachbaac64cf2",
  "InstanceId": "i-0f2b24a5d1fcb18e6",
  "InstanceType": "t2.micro",
  "KeyName": "UbuntuKey",
  "LaunchTime": "2022-09-12T20:58:26+00:00",
  "Monitoring": {
    "State": "disabled"
  },
  "Placement": {
    "AvailabilityZone": "eu-central-1b",
    "GroupName": "",
    "Tenancy": "default"
  },
  "PrivateDnsName": "ip-172-31-35-62.eu-central-1.compute.internal",
  "PrivateIpAddress": "172.31.35.62",
  "ProductCodes": [],
  "PublicDnsName": "ec2-3-126-84-153.eu-central-1.compute.amazonaws.com",
  "PublicIpAddress": "3.126.84.153",
  "State": {
    "Code": 16,
    "Name": "running"
  },
}
```

Assignment 2: Play with security controls of Object Storage S3 in AWS

Difficulty: ★★☆☆☆. Estimated time: 45-60 minutes.

- Create a group for the IAM users in exercise 1.
- Create several private buckets
- One bucket must be shared with all IAM users, other buckets must be visible only per IAM user
- Demonstrate a use of different policies for different type of files (use S3 tags if necessary)
- Demonstrate versioning system for the files in a bucket
- Demonstrate server-side encryption

- Create a bucket policy with a policy generator for certain files or folders – think about some useful scenario for your case-study?...

Provide a screenshots and descriptions of the steps above

group14admin

Delete

Summary

Edit

User group name

group14admin

Creation time

September 01, 2022, 15:48 (UTC+02:00)

ARN

arn:aws:iam::807013657668:group/group14admin

Users

Permissions

Access Advisor

Users in this group (3) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Search

< 1 >

☐

User name

ryan

1

Yesterday

17 days ago

☐

edris

1

Now

17 days ago

☐

heiko

1

3 days ago

18 days ago

I created a group named group14admin with all of our users in it.

	Name	AWS Region	Access	Creation date
<input type="radio"/>	snowweek2public	EU (Frankfurt) eu-central-1	Objects can be public	September 19, 2022, 22:44:59 (UTC+02:00)
<input type="radio"/>	snowweek2private	EU (Frankfurt) eu-central-1	Bucket and objects not public	September 19, 2022, 22:44:37 (UTC+02:00)

2 newly created buckets.

snowweek2private [Info](#)

- Objects
- Properties
- Permissions
- Metrics
- Management
- Access Points

Objects

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 explicitly grant them permissions. [Learn more](#)

Copy S3 URI

Copy URL

Download

Open

Delete

Actions ▼

Create folder

Upload

Find objects by prefix

Show versions

< 1 >

	Name	Type	Last modified	Size	Storage class
--	------	------	---------------	------	---------------

Insufficient permissions to list objects
After you or your AWS administrator have updated your permissions to allow the s3:ListBucket action, refresh the page. [Learn more about Identity and access management in Amazon S3](#)

Policy only allows user Ryan to access this private bucket.

Policy ARNarn:aws:iam::807013657668:policy/allow_snowweek2private_bucket

Description

Permissions

Policy usage

Tags

Policy versions

Access Advisor

▼ Permissions (2)

Attach this policy to an IAM entity to apply its permissions to the entity. [Learn more](#)

Attach

Detach

Filter: Filter

Search

Showing 2

<input type="checkbox"/>	Name	Type
<input type="checkbox"/>	edris	User
<input type="checkbox"/>	heiko	User

► Permissions boundaries

summary

Policy ARNarn:aws:iam::807013657668:policy/allow_snowweek2private_bucket

Description

Permissions

Policy usage

Tags

Policy versions

Access Advisor

Policy summary

{ } JSON

Edit policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Deny",
7       "Action": "s3:GetBucketLocation",
8       "Resource": "arn:aws:s3:*"
9     },
10    {
11      "Sid": "VisualEditor1",
12      "Effect": "Deny",
13      "Action": "s3:ListAllMyBuckets",
14      "Resource": "arn:aws:s3:*"
15    },
16    {
17      "Sid": "VisualEditor2",
18      "Effect": "Deny",
19      "Action": "s3:*",
20      "Resource": [
21        "arn:aws:s3:::snowweek2private",
22        "arn:aws:s3:::snowweek2private/*"
23      ]
24    }
25  ]
26 }
```

Policy in JSON.

The other bucket is accessible by everyone.

Bucket versioning:

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 Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

- ☐ Suspend
This suspends the creation of object versions for all operations but preserves any existing object versions.
- ☒ Enable

After enabling Bucket Versioning, you might need to update your lifecycle rules to manage previous versions of objects.

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, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

Disabled

ryansawsmss2 [Info](#)

Publicly accessible

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

Objects (7)

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 explicitly grant them permissions. [Learn more](#)

	Copy S3 URI	Copy URL	Download	Open	Delete	Actions ▼	Create folder	Upload
Find objects by prefix			Show versions		< 1 > ⚙			
<input type="checkbox"/>	Name ▲	Type	Version ID	Last modified	Size	Storage class		
<input type="checkbox"/>	AWSLogs/	Folder	-	-	-	-		
<input type="checkbox"/>	CSS/	Folder	-	-	-	-		
<input type="checkbox"/>	Images/	Folder	-	-	-	-		
<input type="checkbox"/>	page1.html	html	null	September 10, 2022, 10:33:28 (UTC+01:00)	1.3 KB	Standard		
<input type="checkbox"/>	Page2.html	html	null	September 10, 2022, 10:43:30 (UTC+01:00)	1.7 KB	Standard		
<input type="checkbox"/>	Page3.html	Delete marker	cFUx6Cjmdf.FKWIZzqsYye9K0KADpnry	September 22, 2022, 13:25:54 (UTC+01:00)	0 B	-		
<input type="checkbox"/>	Page3.html	html	null	September 10, 2022, 10:43:30 (UTC+01:00)	1.1 KB	Standard		

Server side encryption:

Default encryption

Automatically encrypt new objects stored in this bucket. [Learn more](#)

Server-side encryption

- ☐ Disable
- ☒ Enable

Encryption key type

To upload an object with a customer-provided encryption key (SSE-C), use the AWS CLI, AWS SDK, or Amazon S3 REST API.

- ☒ **Amazon S3-managed keys (SSE-S3)**
An encryption key that Amazon S3 creates, manages, and uses for you. [Learn more](#)
- ☐ **AWS Key Management Service key (SSE-KMS)**
An encryption key protected by AWS Key Management Service (AWS KMS). [Learn more](#)

Use of different policies for different type of files

[Policies](#) > [group14areawesome](#)

Summary

Delete policy

Policy ARN `arn:aws:iam::807013657668:policy/group14areawesome`

Description the test

Permissions

Policy usage

Tags

Policy versions

Access Advisor

Tags (1)

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

Manage tags

Key

Value

boogaloo

electric

Tags (2)

Track storage cost or other criteria by tagging your bucket. [Learn more](#)

Edit

Key

Value

boogaloo

electric

website

static