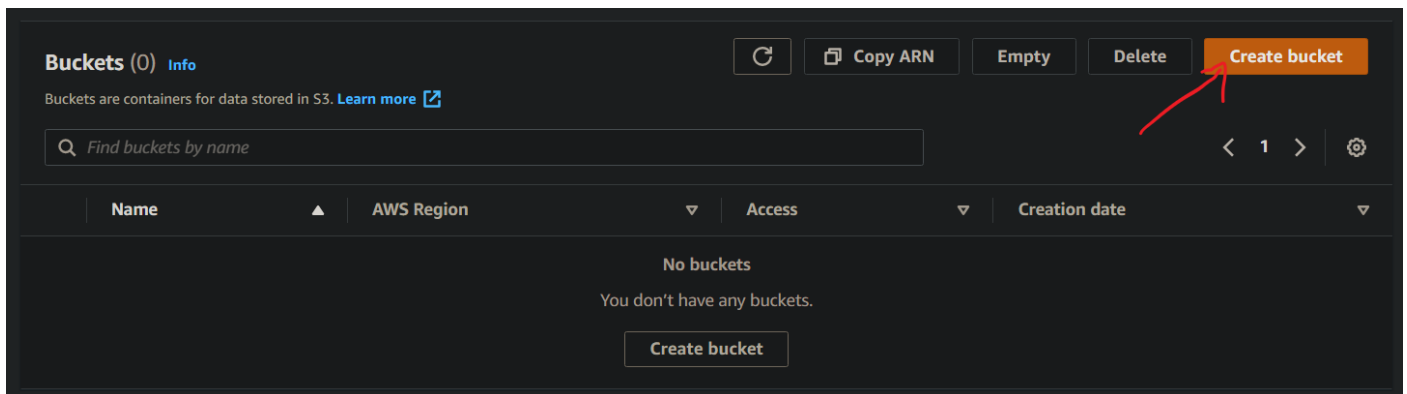


Ahmed Shawky: Task 3

1- create s3



Create bucket [Info](#)

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

General configuration

Bucket name

this-my-bucket

Bucket name must be unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region

EU (Paris) eu-west-3

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Choose bucket

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.

Default encryption

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

Server-side encryption

- ☒ Disable
☐ Enable

► Advanced settings

After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.

Cancel

Create bucket

2- config s3 as a site

this-my-bucket [Info](#)

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

Objects (0)

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](#)

[Refresh](#) [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

☐ Show versions < 1 > [Settings](#)

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
No objects					
You don't have any objects in this bucket.					
Upload					

Upload [Info](#)

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose **Add files**, or **Add folders**.

Files and folders (0) [Remove](#) [Add files](#) [Add folder](#)

All files and folders in this table will be uploaded.

< 1 >

<input type="checkbox"/>	Name	Folder	Type	Size
No files or folders				
You have not chosen any files or folders to upload.				

Destination

Destination
[s3://this-my-bucket](#)

► **Destination details**
Bucket settings that impact new objects stored in the specified destination.

► **Permissions**
Grant public access and access to other AWS accounts.

► **Properties**
Specify storage class, encryption settings, tags, and more.

[Cancel](#) [Upload](#)

this-my-bucket [Info](#)

Objects **Properties** Permissions Metrics Management Access Points

Bucket overview

AWS Region EU (Paris) eu-west-3	Amazon Resource Name (ARN) arn:aws:s3::this-my-bucket	Creation date September 13, 2021, 15:40:07 (UTC+02:00)
------------------------------------	--	---

Static website hosting
Use this bucket to host a website or redirect requests. [Learn more](#)

Static website hosting
Disabled

[Edit](#)

2

Edit static website hosting [Info](#)

Static website hosting
Use this bucket to host a website or redirect requests. [Learn more](#)

Static website hosting

☐ Disable

☒ Enable

Hosting type

☒ Host a static website
Use the bucket endpoint as the web address. [Learn more](#)

☐ Redirect requests for an object
Redirect requests to another bucket or domain. [Learn more](#)

For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see [Using Amazon S3 Block Public Access](#)

Index document
Specify the home or default page of the website.

index.html

Error document - optional
This is returned when an error occurs.

error.html

Redirection rules – optional
Redirection rules, written in JSON, automatically redirect webpage requests for specific content. [Learn more](#)

3

Cancel [Save changes](#)

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

Permissions overview

Access

Objects can be 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](#)[Edit](#)[Delete](#)

No policy to display.

[Copy](#)Edit bucket policy [Info](#)

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](#)[Policy examples](#)[Policy generator](#)

AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see [key concepts in Using AWS Identity and Access Management](#). Here are [sample policies](#).

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an [IAM Policy](#), an [S3 Bucket Policy](#), an [SNS Topic Policy](#), a [VPC Endpoint Policy](#), and an [SQS Queue Policy](#).Select Type of Policy S3 Bucket Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See [a description of elements](#) that you can use in statements.Effect ☒ Allow ☐ Deny

Principal *

Use a comma to separate multiple values.

AWS Service Amazon S3☐ All Services ('*')

Use multiple statements to add permissions for more than one service.

Actions 1 Action(s) Selected ☐ All Actions ('*')Amazon Resource Name (ARN) arn:aws:s3:::this-my-bucketARN should follow the following format: `arn:aws:s3:::{BucketName}/{KeyName}`.
Use a comma to separate multiple values.[Add Conditions \(Optional\)](#)[Add Statement](#)

You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource	Conditions
• *	Allow	• s3:GetObject	arn:aws:s3:::this-my-bucket/*	None

Step 3: Generate Policy

A *policy* is a document (written in the [Access Policy Language](#)) that acts as a container for one or more statements.

Generate Policy

Start Over

Policy JSON Document

Click below to edit. To save the policy, copy the text below to a text editor. Changes made below will **not be reflected in the policy generator tool**.

```
{
  "Id": "Policy1631542431090",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1631542409306",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::this-my-bucket/*",
      "Principal": "*"
    }
  ]
}
```

copy all

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided as is without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services.

Close

Policy

```
1 {  
2   "Id": "Policy1631542431090",  
3   "Version": "2012-10-17",  
4   "Statement": [  
5     {  
6       "Sid": "Stmnt1631542409306",  
7       "Action": [  
8         "s3:GetObject"  
9       ],  
10      "Effect": "Allow",  
11      "Resource": "arn:aws:s3:::this-my-bucket/*",  
12      "Principal": "*"   
13    }  
14  ]  
15 }
```

past

Preview external access

Preview and validate Access Analyzer findings for external access to your resource. [Learn more](#)



Preview external access to your bucket with Access Analyzer

Access Analyzer analyzes your bucket policy together with existing bucket permissions to preview findings for external access to your bucket. This helps you validate public and cross-account access to your bucket before you save your policy. Choose an analyzer and select preview to begin.

[Learn more about Access Analyzer](#)

No analyzers

To preview external access to your bucket, create an analyzer in your bucket's region

[Go to Access Analyzer](#)

Cancel

Save changes

3- create image of public and private ec2s

The screenshot shows the AWS Management Console 'Instances' page. A table lists three instances: 'private', 'online', and 'public'. The 'public' instance is selected. The 'Actions' dropdown menu is open, showing options like 'Connect', 'View details', and 'Create image'. The 'Create image' option is circled in red and labeled with a red '4'. The 'Image and templates' option in the right-hand menu is also circled in red and labeled with a red '3'. A red '2' points to the 'Actions' dropdown button. A red '1' points to the 'public' instance in the table.

Name	Instance ID	Instance state	Instance type	Status check	Alarm state
private	i-0a9ce2db3e59fcbfc	Stopped	t2.micro	-	No alarm
online	i-0def33be1d9181d5d	Stopped	t2.micro	-	No alarm
public	i-03ed7bfdab217d7a0	Stopped	t2.micro	-	No alarm

4- snapshots of ebs volumes attached with aforementioned ec2s

The screenshot shows the 'Create Snapshot' button in the AWS console, which is circled in red. The text 'You do not have any snapshots in this region.' and 'Click the Create Snapshot button to create your first snapshot.' are visible.

The screenshot shows the 'Create Snapshot' form in the AWS console. The 'Select resource type' is set to 'Volume'. The 'Volume' dropdown menu is open, showing a list of volumes. A red arrow points to the 'vol-03c95b2ac167ba63b' volume, with the text 'select ec2 instance volume' next to it. The 'Description' field is empty. The 'Encrypted' checkbox is checked. The 'Key' and 'Value' fields are empty. The 'Add Tag' button is visible. The 'Create Snapshot' button is circled in red.

Select resource type: ☐ Volume ☒ Instance

Volume:

Description:

Encrypted: ☒

Key: (128 characters maximum) Value: (256 characters maximum)

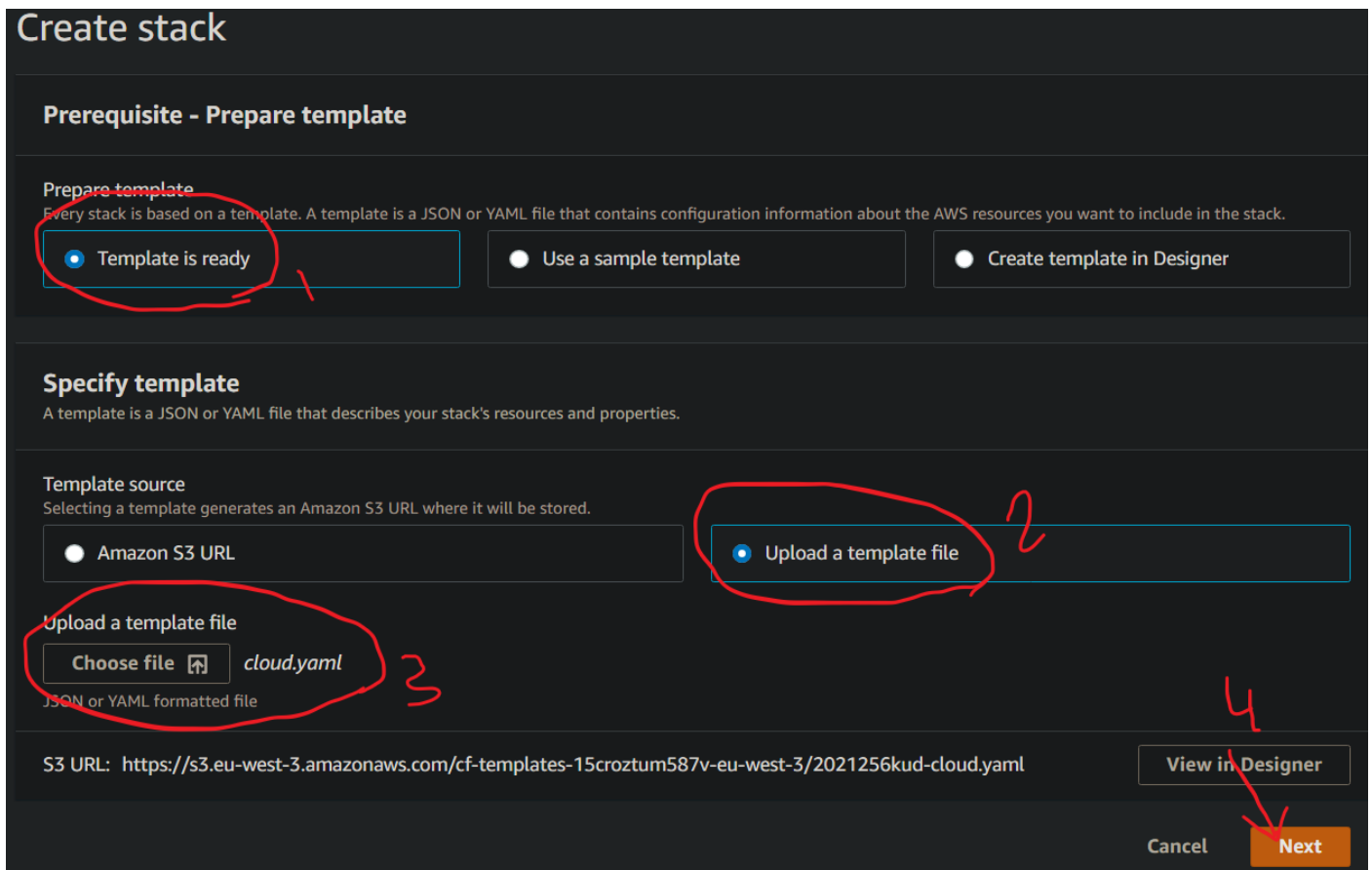
This resource currently has no tags. Choose the Add tag button or click to add a Name tag.

Add Tag 50 remaining (Up to 50 tags maximum)

* Required Cancel Create Snapshot

5- create cloudformations template with:

- Public subnet
- ec2
- security group (ssh and http enabled)



Specify stack details

Stack name

Stack name

MyStack

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

No parameters

There are no parameters defined in your template

Cancel

Previous

Next

Configure stack options

Tags

You can specify tags (key-value pairs) to apply to resources in your stack. You can add up to 50 unique tags for each stack. [Learn more](#)

department

development

Remove

Add tag

Stack creation options

Cancel

Previous

Next

Notification options

No notification options

There are no notification options defined

Stack creation options

Timeout

-

Termination protection

Disabled

Quick-create link

Cancel

Previous

Create change set

Create stack