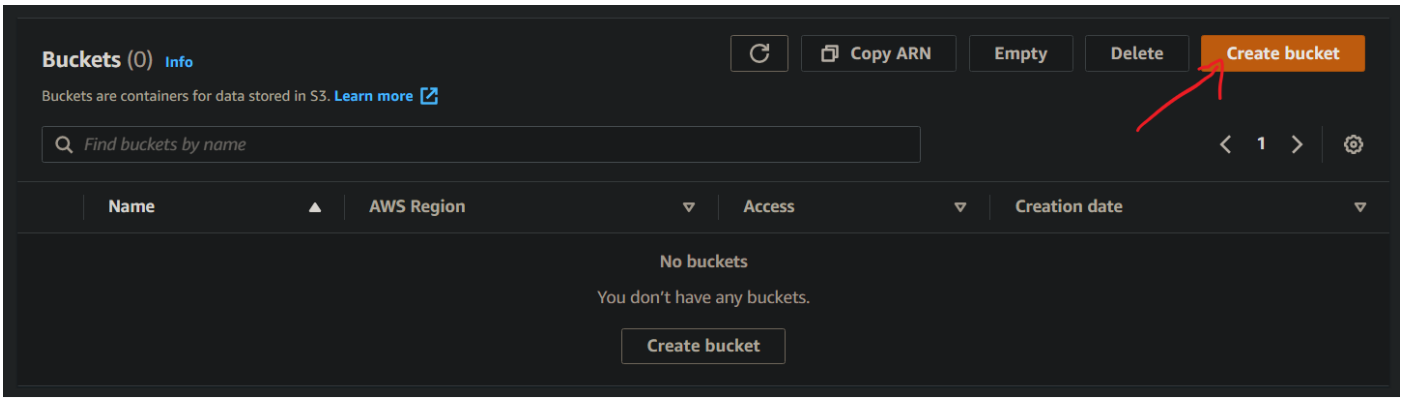
Ahmed Shawky: Task 3

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

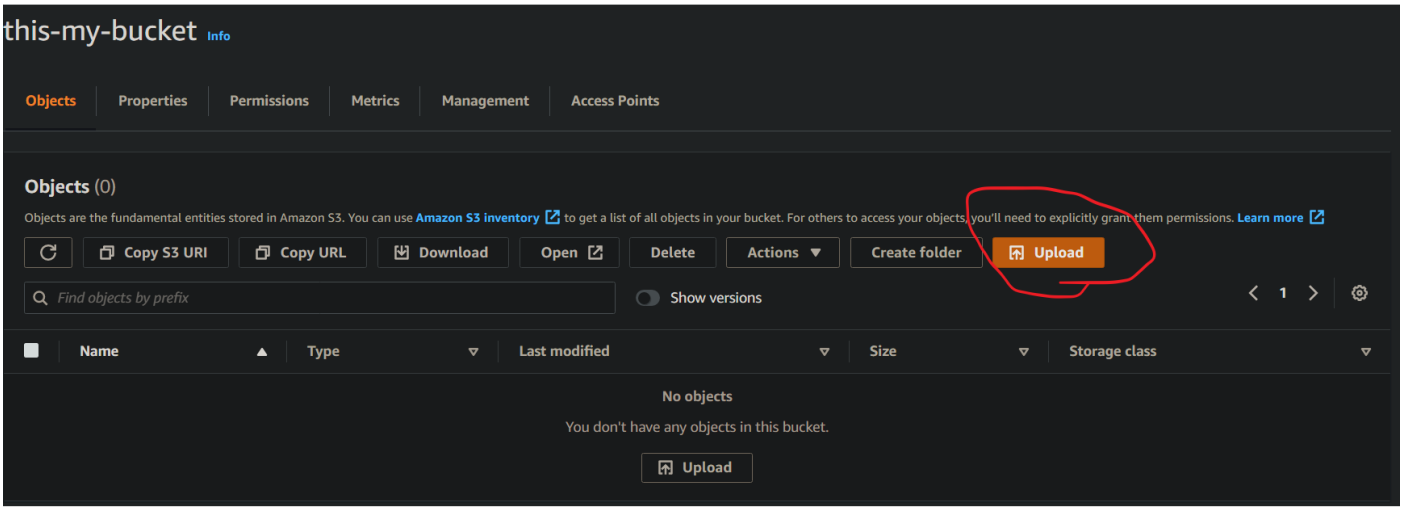
- (•) Disable
- ( ) Enable

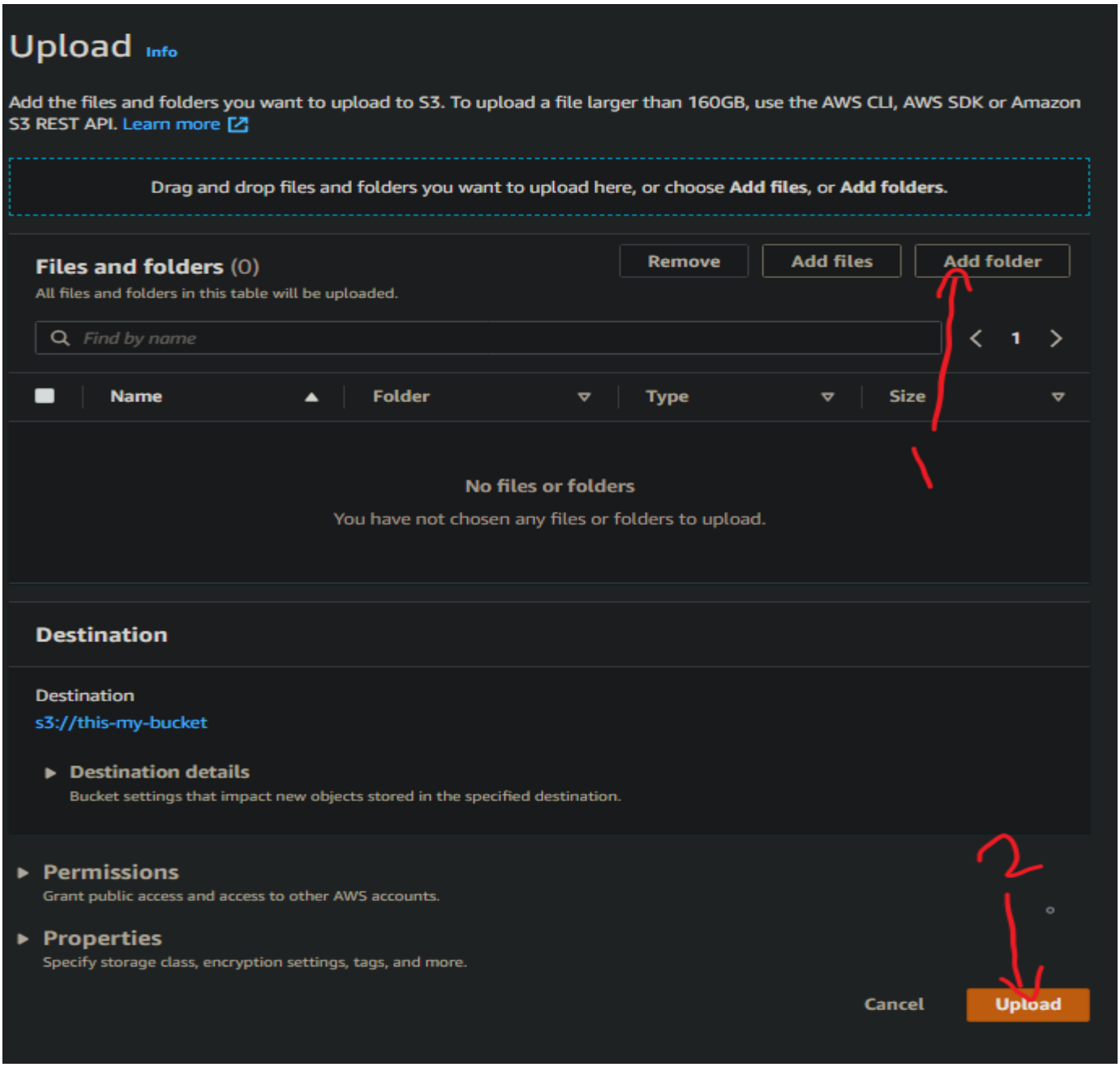
▸ Advanced settings

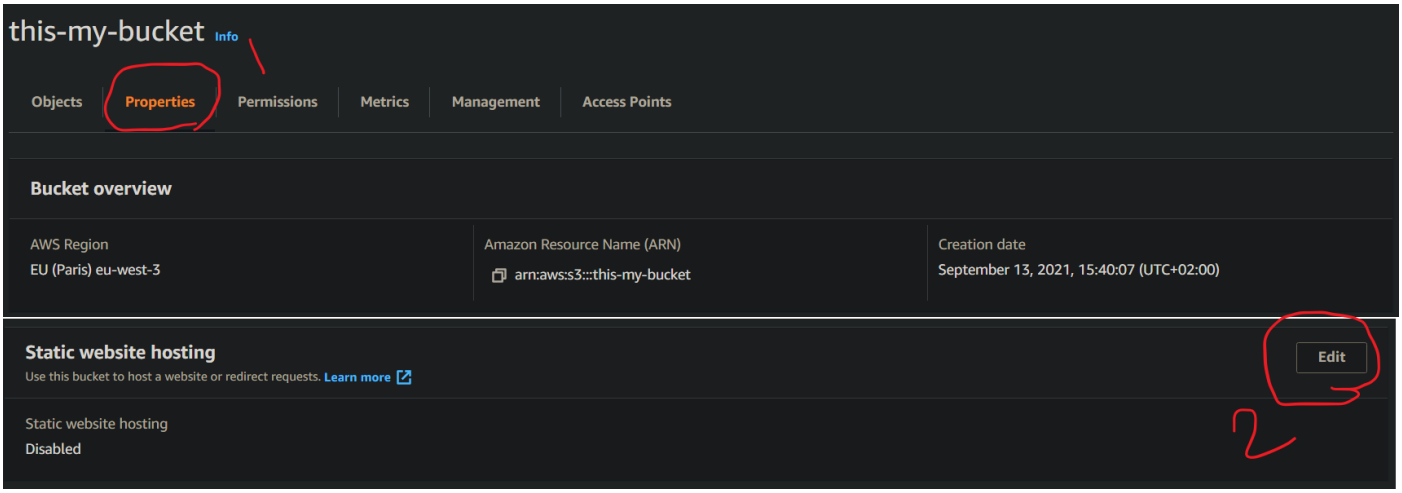
ⓘ After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.

Cancel | Create bucket

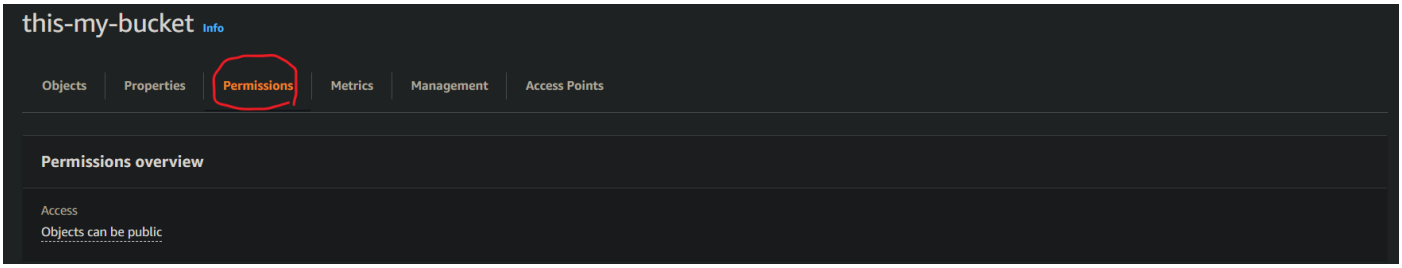
2- config s3 as a site

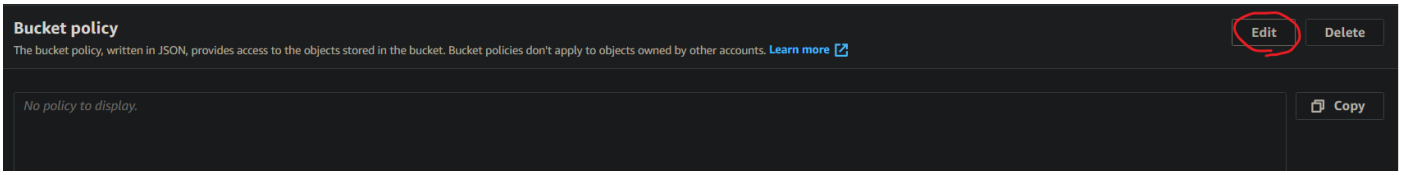


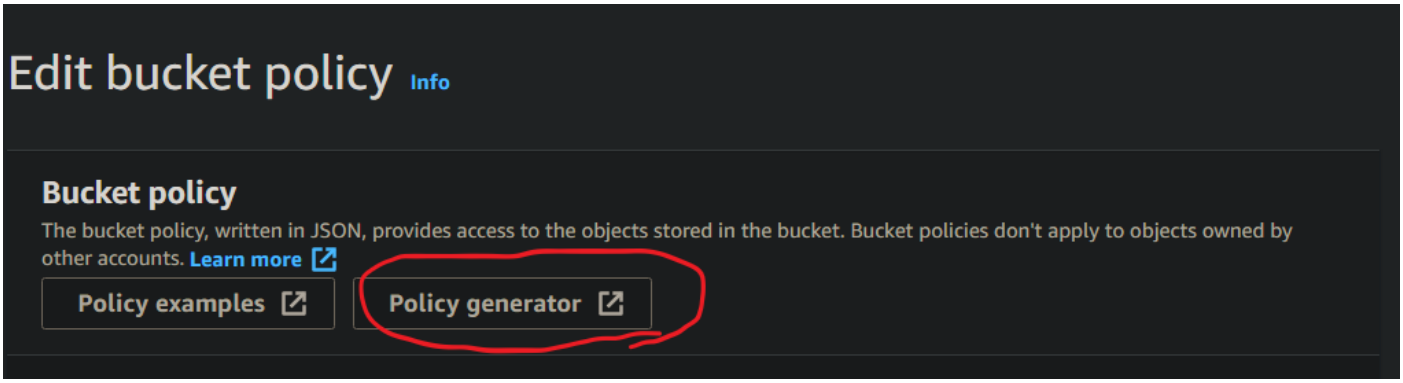


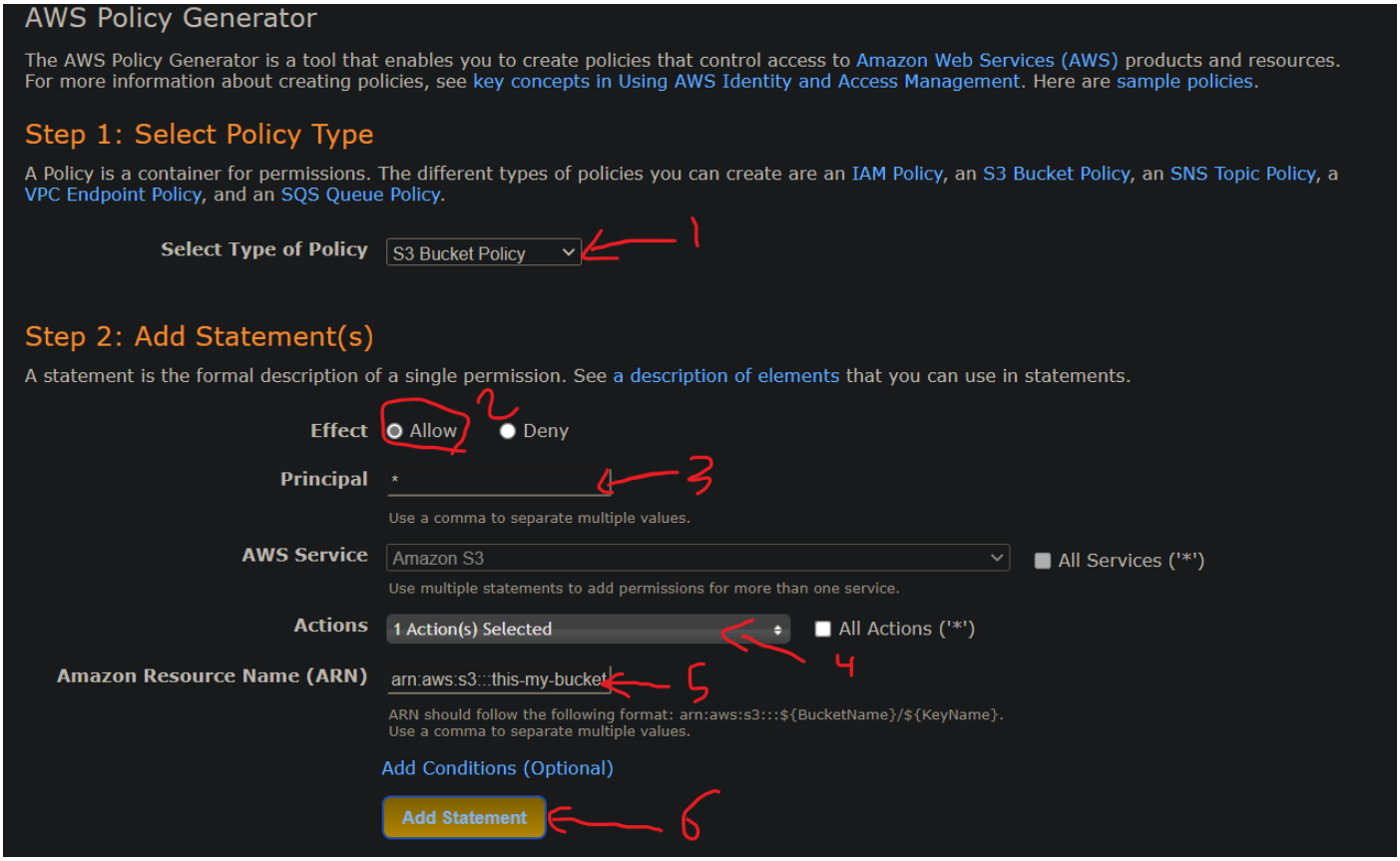

this-my-bucket Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Bucket overview
AWS Region
EU (Paris) eu-west-3
Amazon Resource Name (ARN)
arn:aws:s3:::this-my-bucket
Creation date
September 13, 2021, 15:40:07 (UTC+02:00)
Static website hosting
Use this bucket to host a website or redirect requests. Learn more
Edit
Static website hosting
Disabled
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
1
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
2
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


this-my-bucket Info
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
1
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
2
Principal
*
3
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 ('*')
4
Amazon Resource Name (ARN)
arn:aws:s3:::this-my-bucket
5
ARN should follow the following format: arn:aws:s3:::${BucketName}/${KeyName}.
Use a comma to separate multiple values.
Add Conditions (Optional)
Add Statement
6

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.**

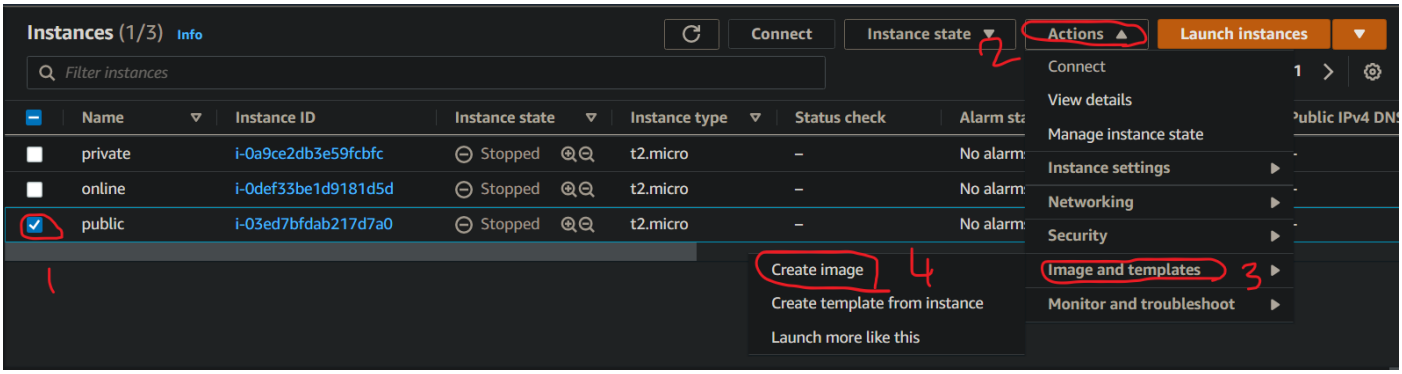
```
{
  "Id": "Policy1631542431090",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1631542409306",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::this-my-bucket/*",
      "Principal": "*"
    }
  ]
}
```

copy all

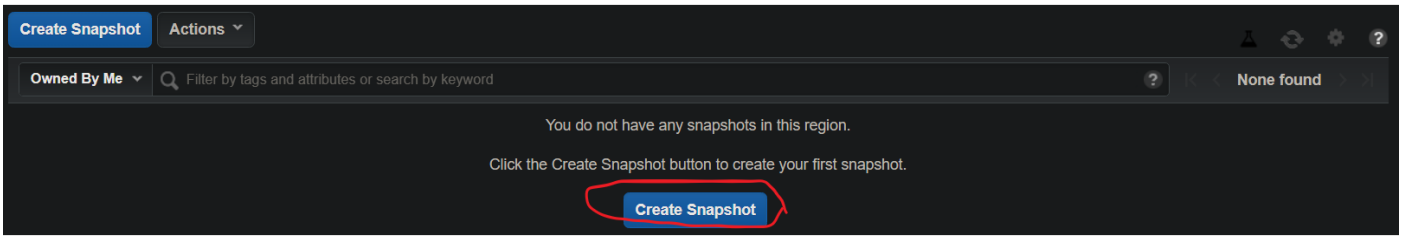
Close 2

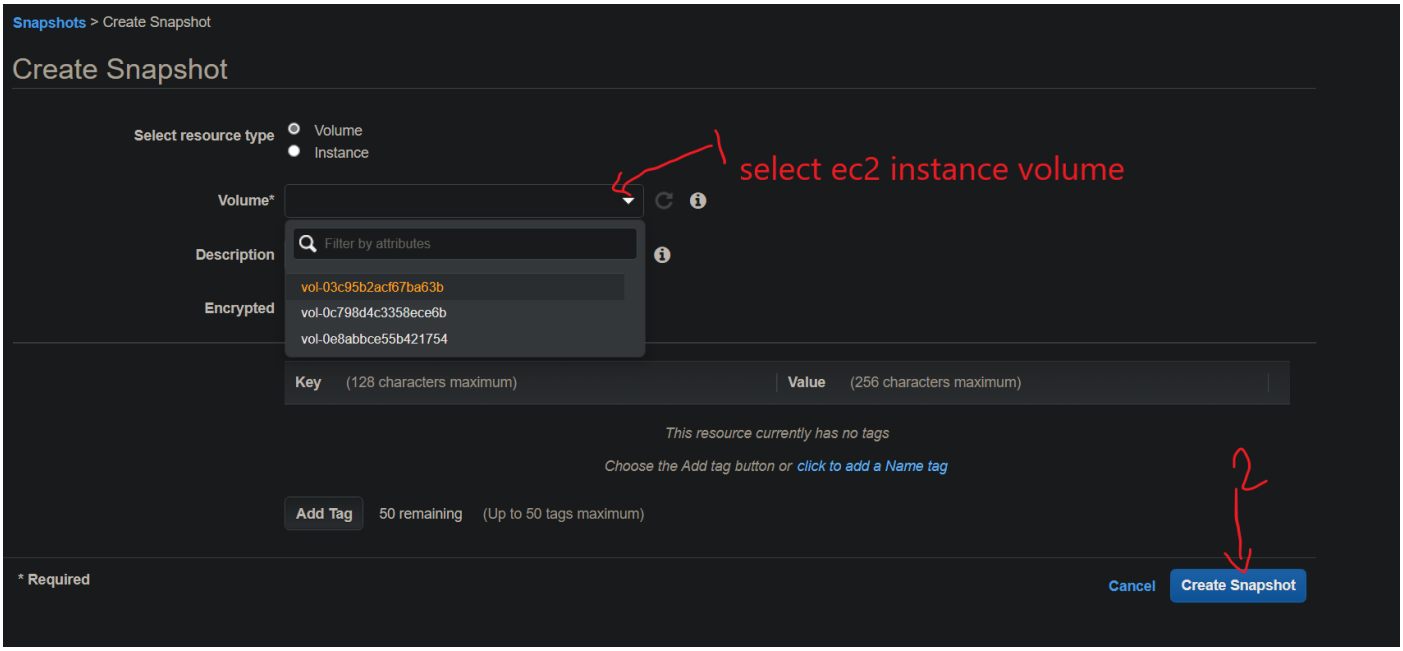

Policy
{
"Id": "Policy1631542431090",
"Version": "2012-10-17",
"Statement": [
{
"Sid": "Stmt1631542409306",
"Action": [
"s3:GetObject"
],
"Effect": "Allow",
"Resource": "arn:aws:s3:::this-my-bucket/*",
"Principal": "*"
}
]
}
1
past
Preview external access
Preview and validate Access Analyzer findings 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
2
Cancel
Save changes

3- create image of public and private ec2s



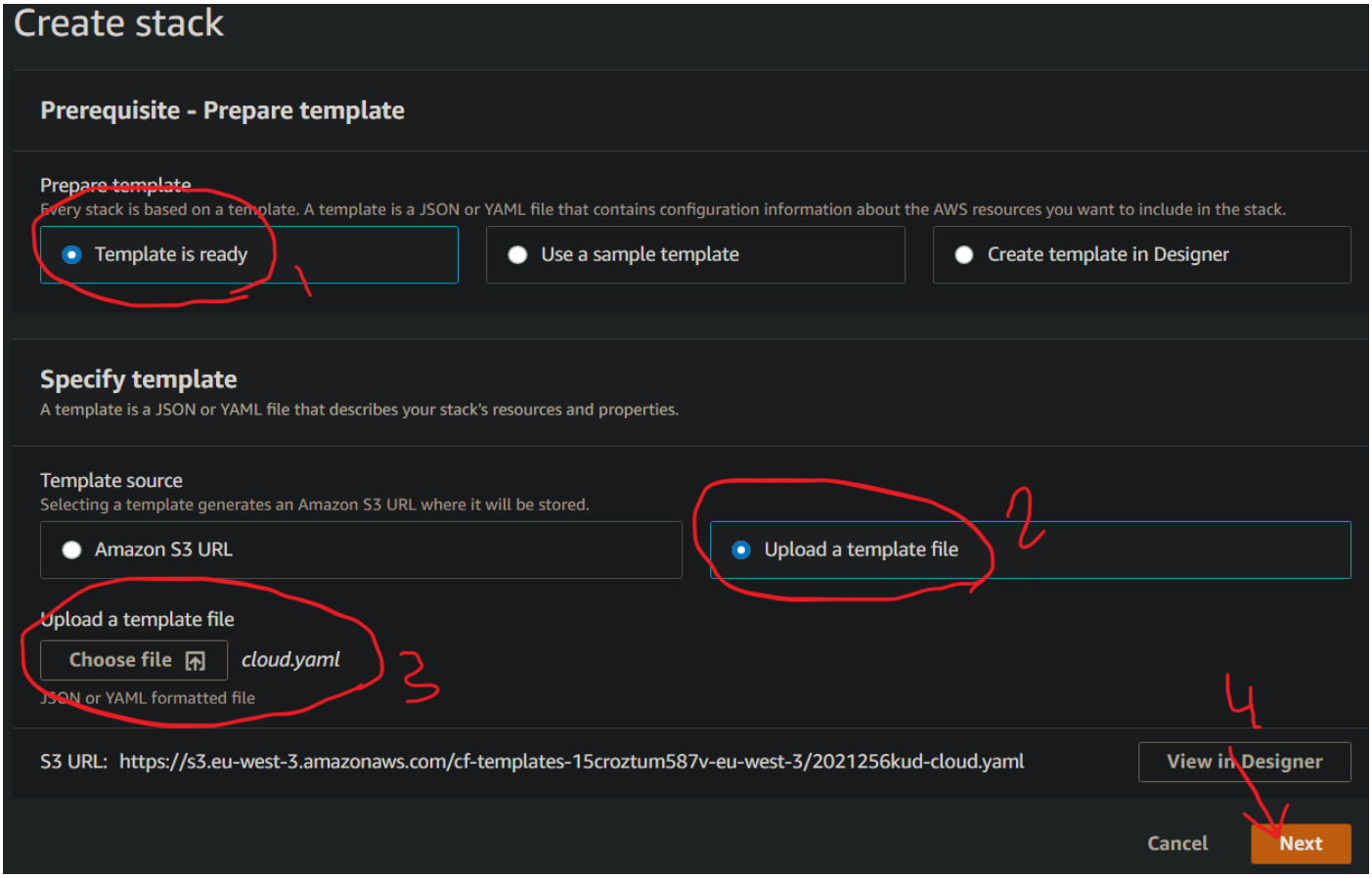
4- snapshots of ebs volumes attached with afformentioned ec2s

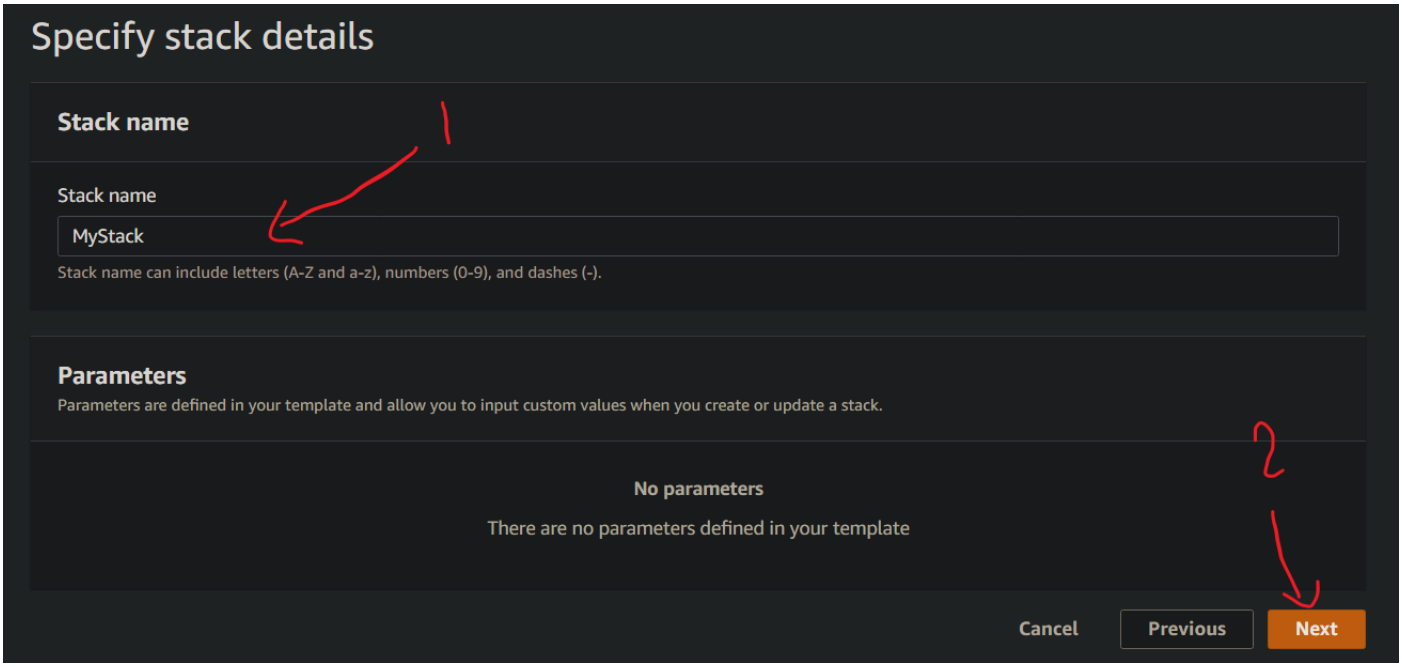


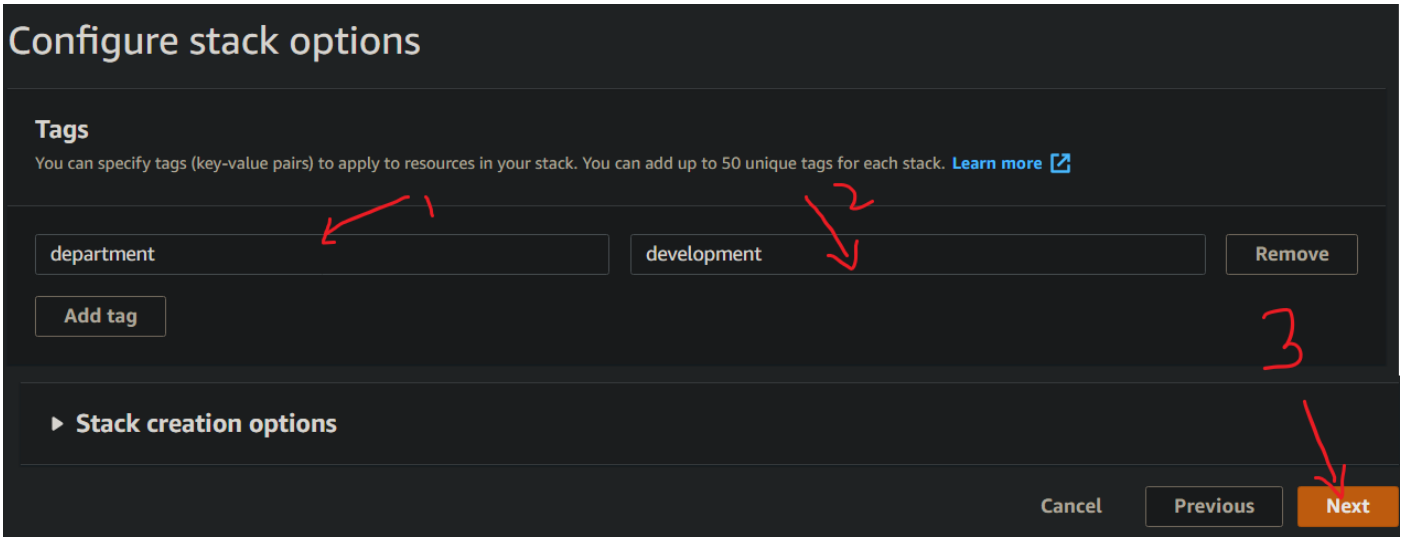


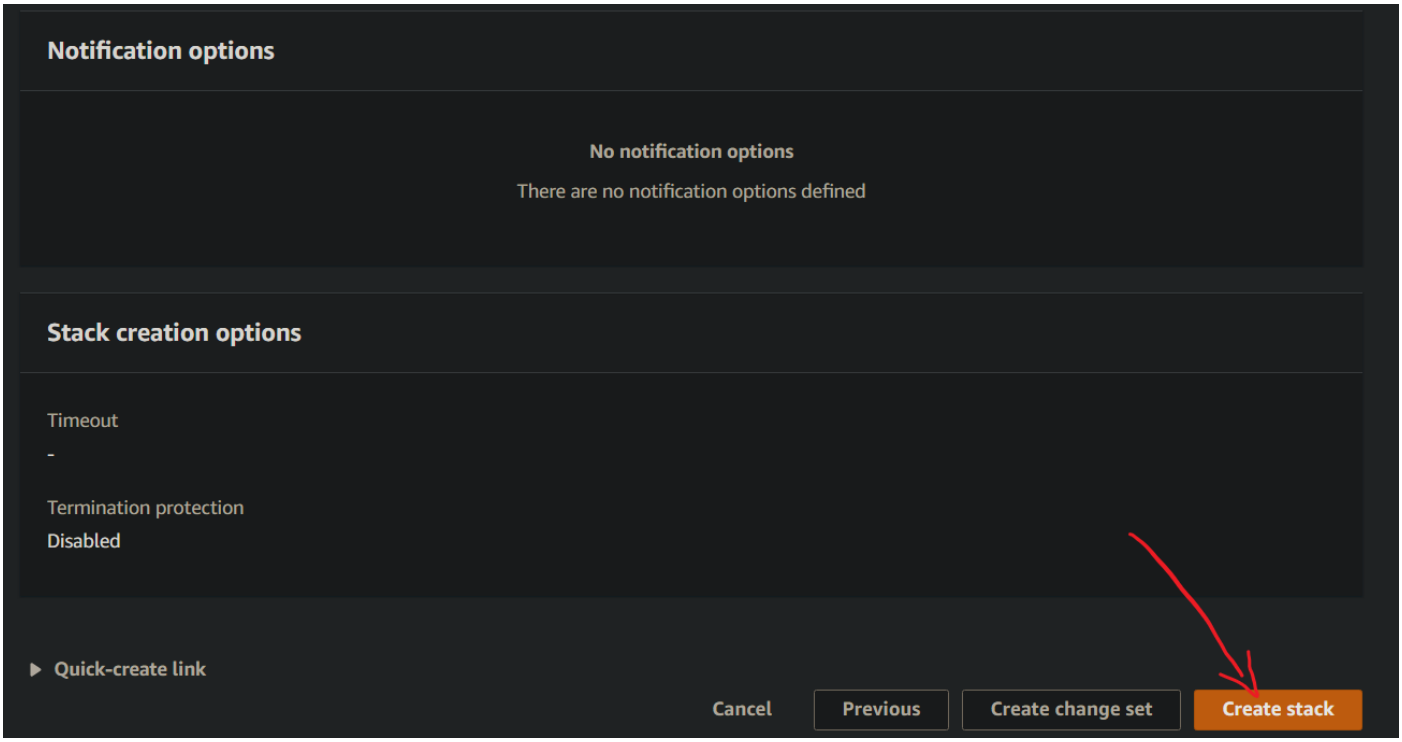
5- create cloudformations template with:

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




Specify stack details
Stack name
1
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
2
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
1
2
department
development
Remove
Add tag
3
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