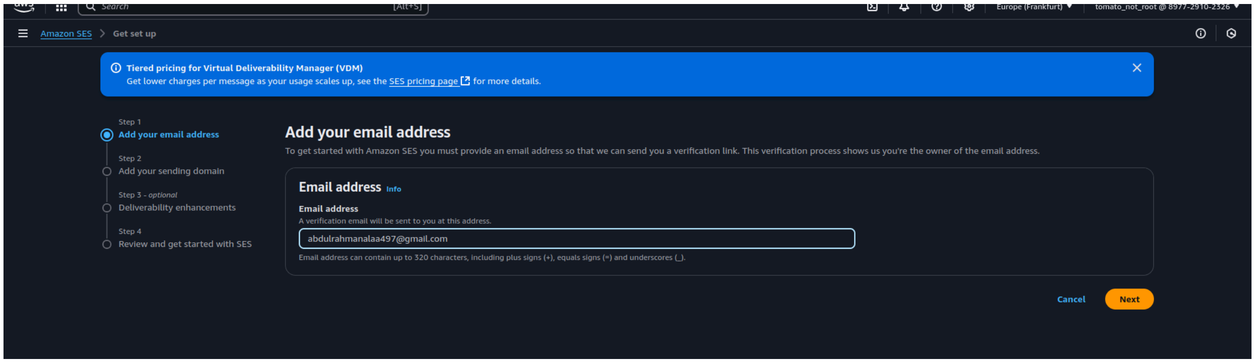
Q1:

Segmenting the aws_networking schema into its own module

https://github.com/abdulrahmanalaa123/ITI-sessions/tree/master/IAC/Lab3

Q2:

Verify the email on amazon SES



Tiered pricing for Virtual Deliverability Manager (VDM)
Get lower charges per message as your usage scales up, see the SES pricing page for more details.

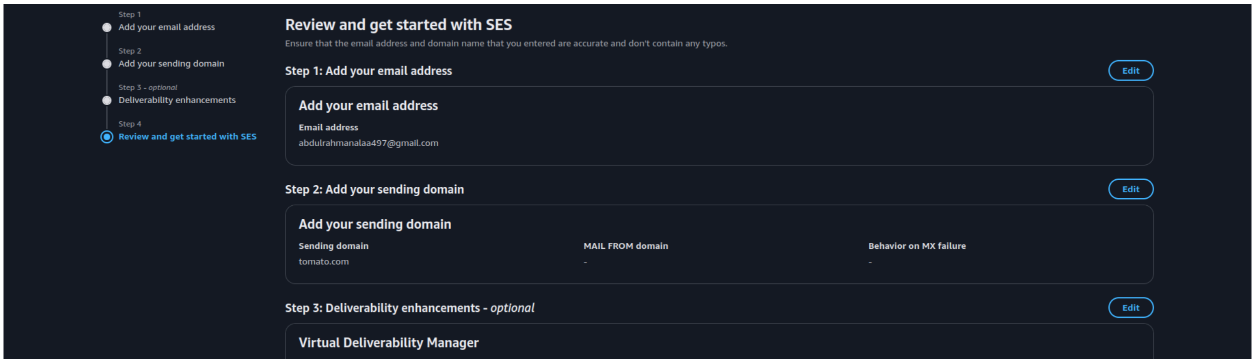
Step 1
Add your email address
Step 2
Add your sending domain
Step 3 - *optional*
Deliverability enhancements
Step 4
Review and get started with SES

Add your email address

To get started with Amazon SES you must provide an email address so that we can send you a verification link. This verification process shows us you're the owner of the email address.

Email address

Email address
A verification email will be sent to you at this address.
abdulrahmanalaa497@gmail.com
Email address can contain up to 320 characters, including plus signs (+), equals signs (=) and underscores (_).



Step 1
Add your email address
Step 2
Add your sending domain
Step 3 - *optional*
Deliverability enhancements
Step 4
Review and get started with SES

Review and get started with SES

Ensure that the email address and domain name that you entered are accurate and don't contain any typos.

Step 1: Add your email address

Add your email address
Email address
abdulrahmanalaa497@gmail.com

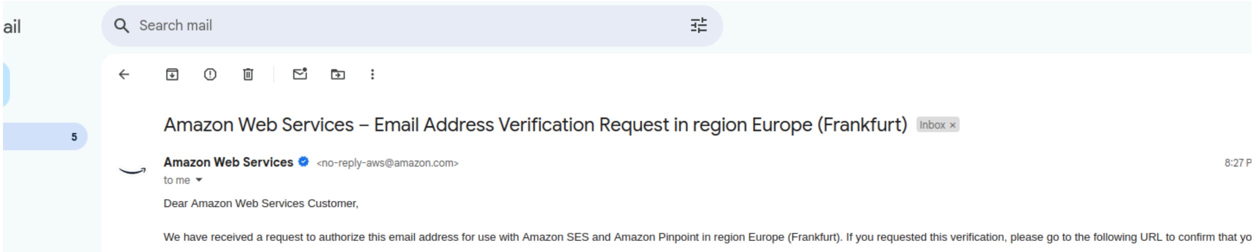
Step 2: Add your sending domain

Add your sending domain

Sending domain	MAIL FROM domain	Behavior on MX failure
tomato.com	-	-

Step 3: Deliverability enhancements - *optional*

Virtual Deliverability Manager

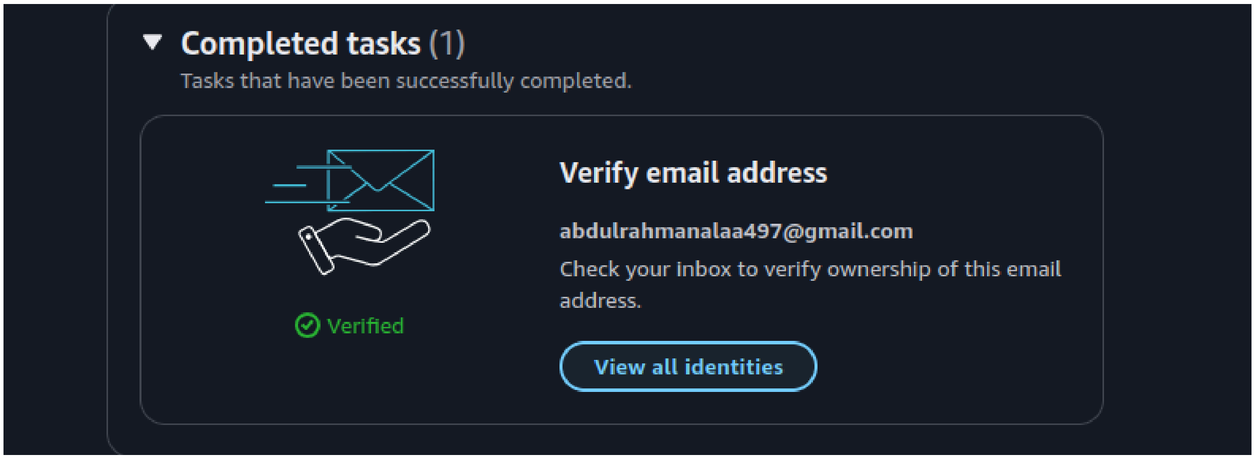


Amazon Web Services – Email Address Verification Request in region Europe (Frankfurt)

Amazon Web Services <no-reply-aws@amazon.com>
to me

Dear Amazon Web Services Customer,

We have received a request to authorize this email address for use with Amazon SES and Amazon Pinpoint in region Europe (Frankfurt). If you requested this verification, please go to the following URL to confirm that yo

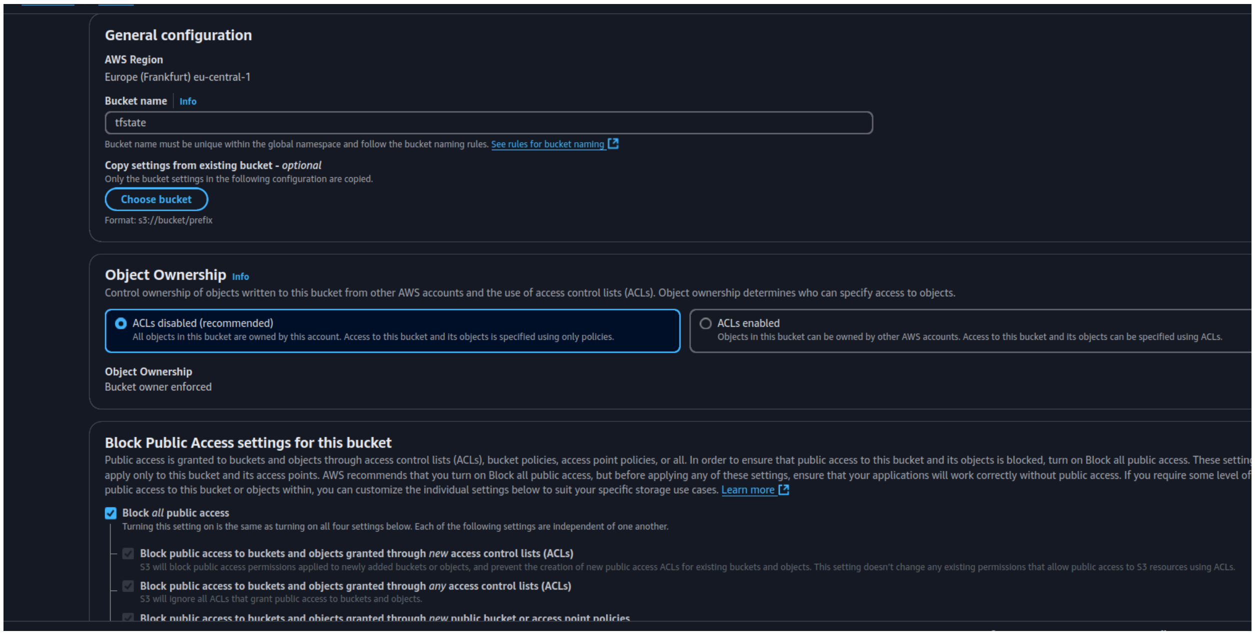


Completed tasks (1)
Tasks that have been successfully completed.

Verified

Verify email address
abdulrahmanalaa497@gmail.com
Check your inbox to verify ownership of this email address.

Q3:create S3 bucket



General configuration

AWS Region
Europe (Frankfurt) eu-central-1

Bucket name

tfstate

Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

Copy settings from existing bucket - ***optional***
Only the bucket settings in the following configuration are copied.

Format: s3://bucket/prefix

Object Ownership

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 enforced

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 setting 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**

And the rest of the configurations are on the github link
https://github.com/abdulrahmanalaa123/ITI-sessions/tree/master/IAC/Lab3