

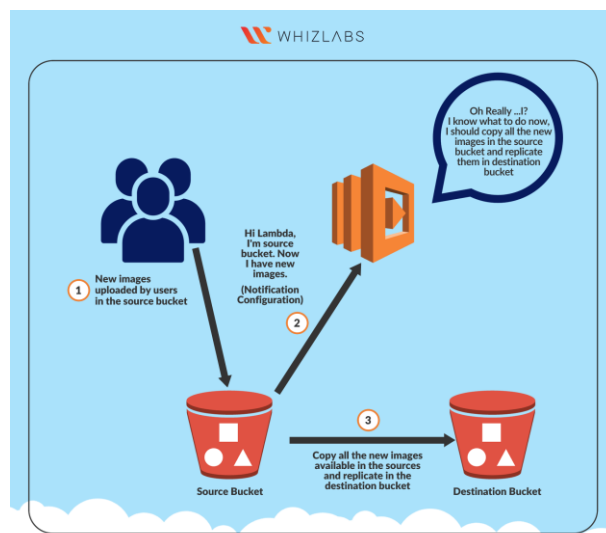
Laboratorio Lambda de AWS

Detalles del laboratorio

1. Esta práctica de laboratorio lo guiará a través de la creación y el uso de un servicio de AWS sin servidor llamado AWS Lambda. En esta práctica de laboratorio, crearemos una función Lambda de muestra que se activará en un evento de carga de objetos S3. La función lambda hará una copia de ese objeto y lo colocará en un depósito s3 diferente.

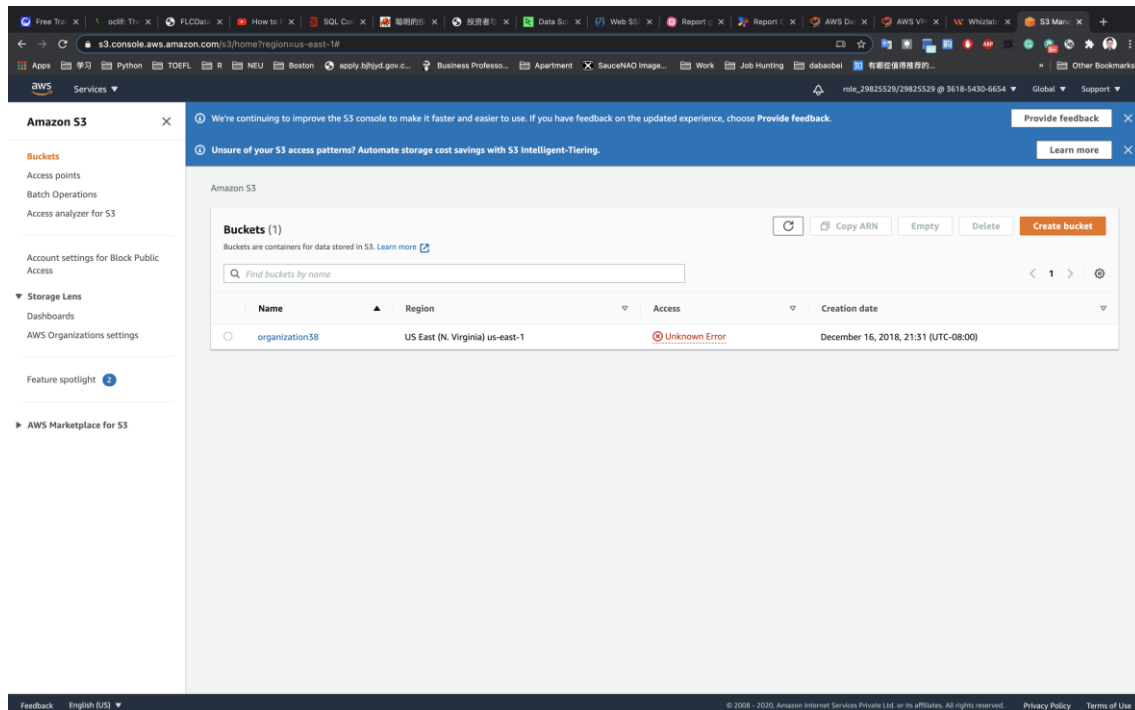
Detalles de la tarea

1. Inicie sesión en la Consola de administración de AWS.
2. Cree dos depósitos de S3. Uno para el origen y otro para el destino.
3. Cree una función Lambda para copiar el objeto de un depósito a otro depósito.
4. Pruebe la función Lambda.



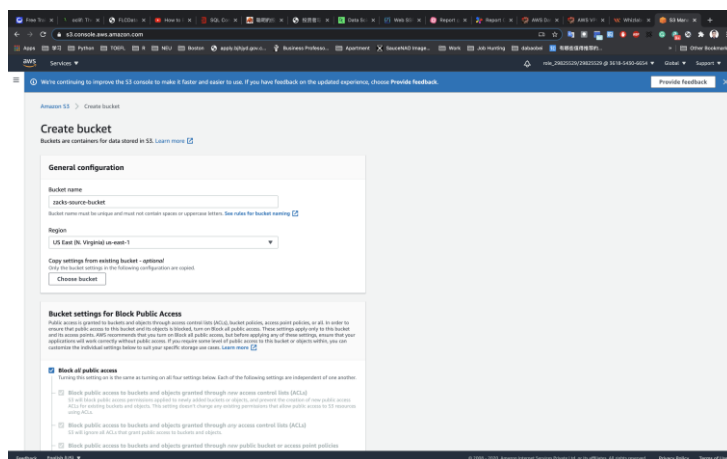
Crear depósito de Amazon S3 (depósito de origen)

Haga clic en **Create bucket**.

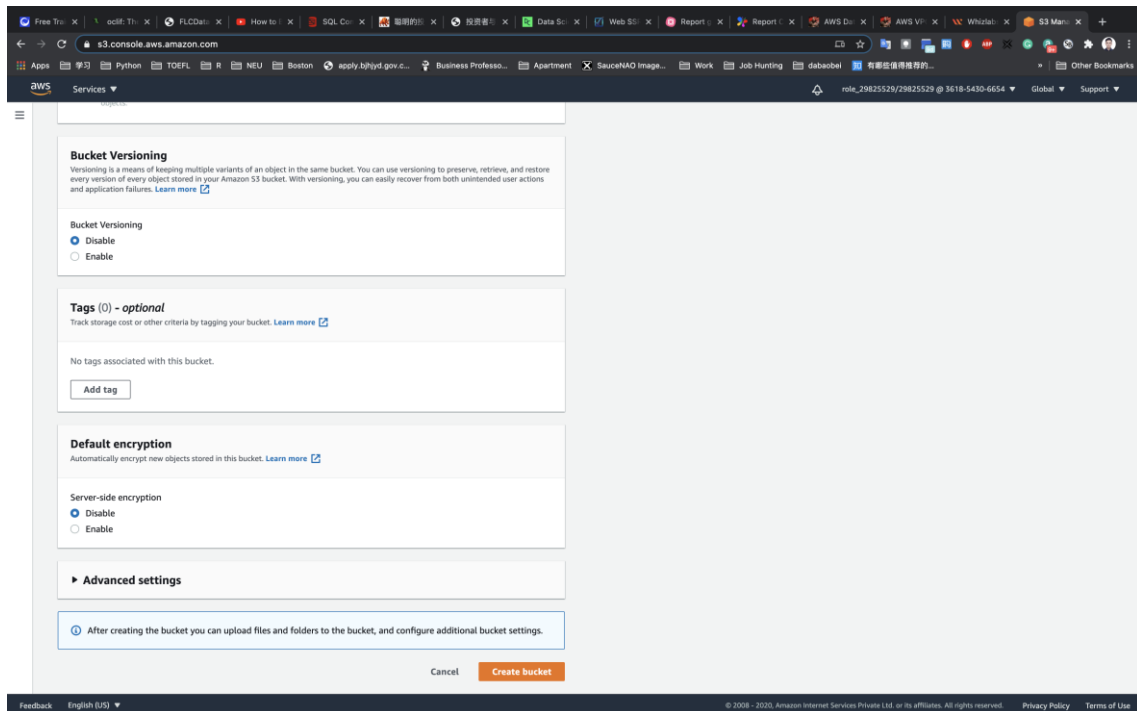


- Nombre del depósito: `your_source_bucket_name`
- Región: US East (N. Virginia)

Nota : Cada nombre de depósito de S3 es único a nivel mundial, por lo tanto, cree el depósito con un nombre que no esté en uso actualmente.



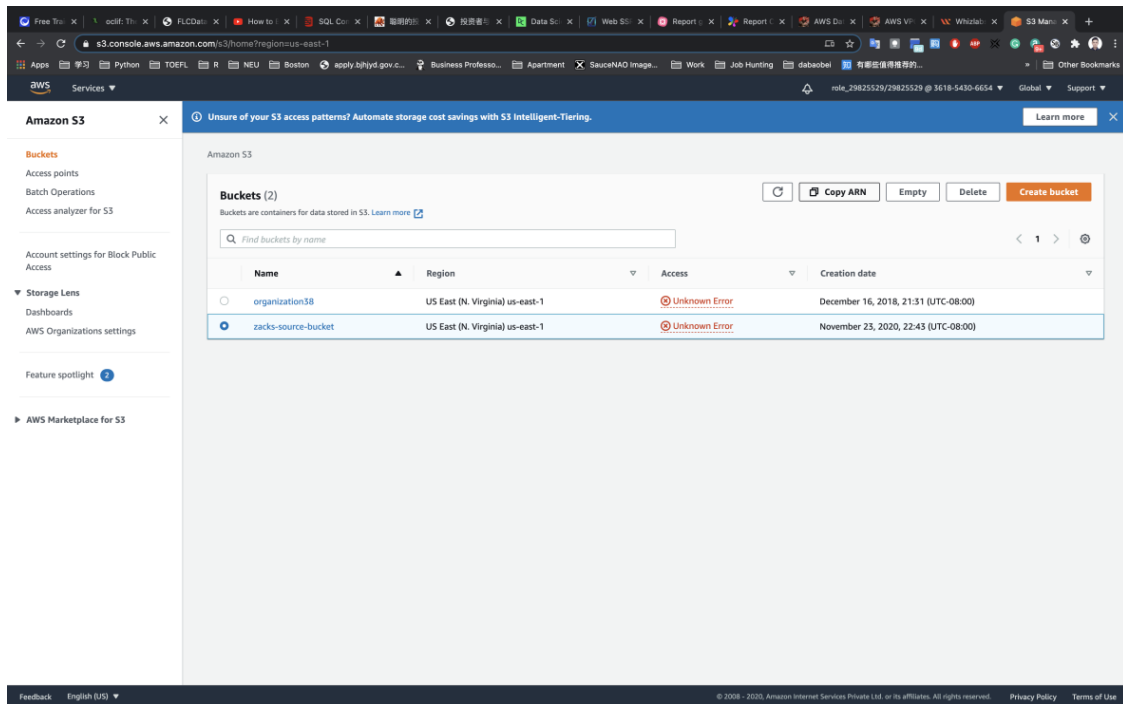
Deje otras configuraciones por defecto y haga clic en el **Create** botón.



Una vez que el depósito se haya creado correctamente, seleccione su depósito S3 (haga clic en la casilla de verificación).

Haga clic en **Copy Bucket ARN** para copiar el ARN.

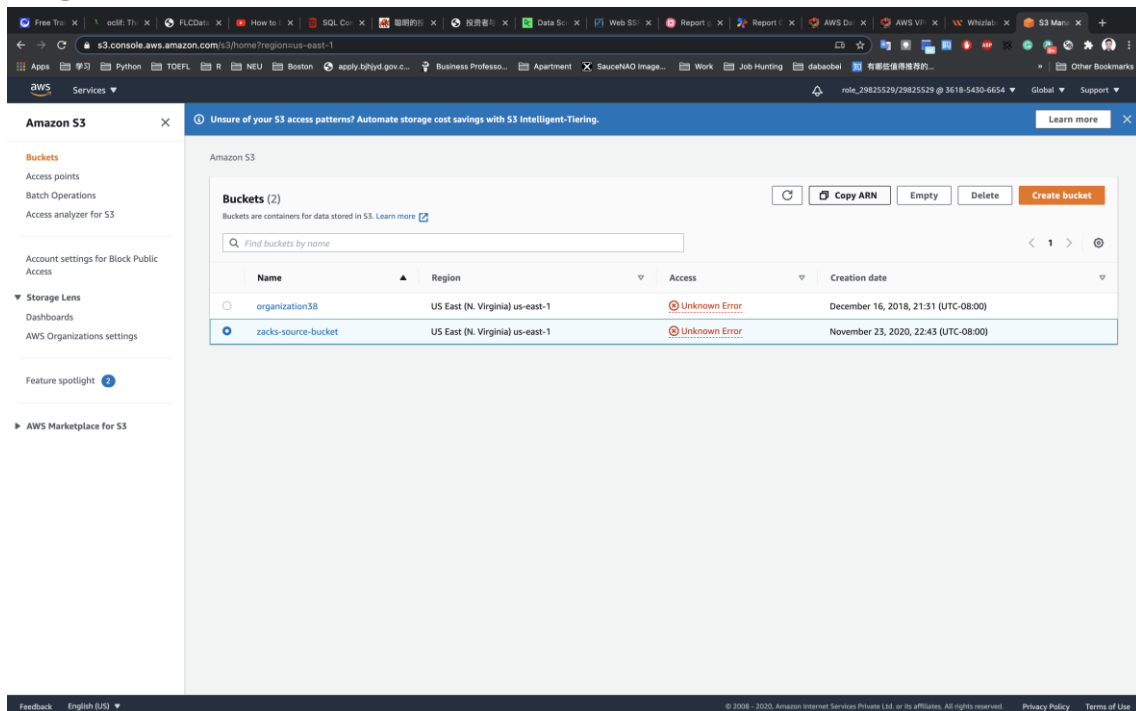
- `arn:aws:s3:::zacks-source-bucket`



Guarde el ARN del depósito de origen en un archivo de texto para su uso posterior.

Crear depósito de Amazon S3 (depósito de destino)

Haga clic en Create bucket.



- Nombre del depósito: your_destination_bucket_name
- Región: US East (N. Virginia)

Nota : Cada nombre de depósito de S3 es único a nivel mundial, por lo tanto, cree el depósito con un nombre que no esté en uso actualmente.

Amazon S3 > Create bucket

Create bucket

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

General configuration

Bucket name

zacks-destination-bucket

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

Region

US East (N. Virginia) us-east-1

Copy settings from existing bucket - optional

Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Bucket settings for Block Public Access

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](#)

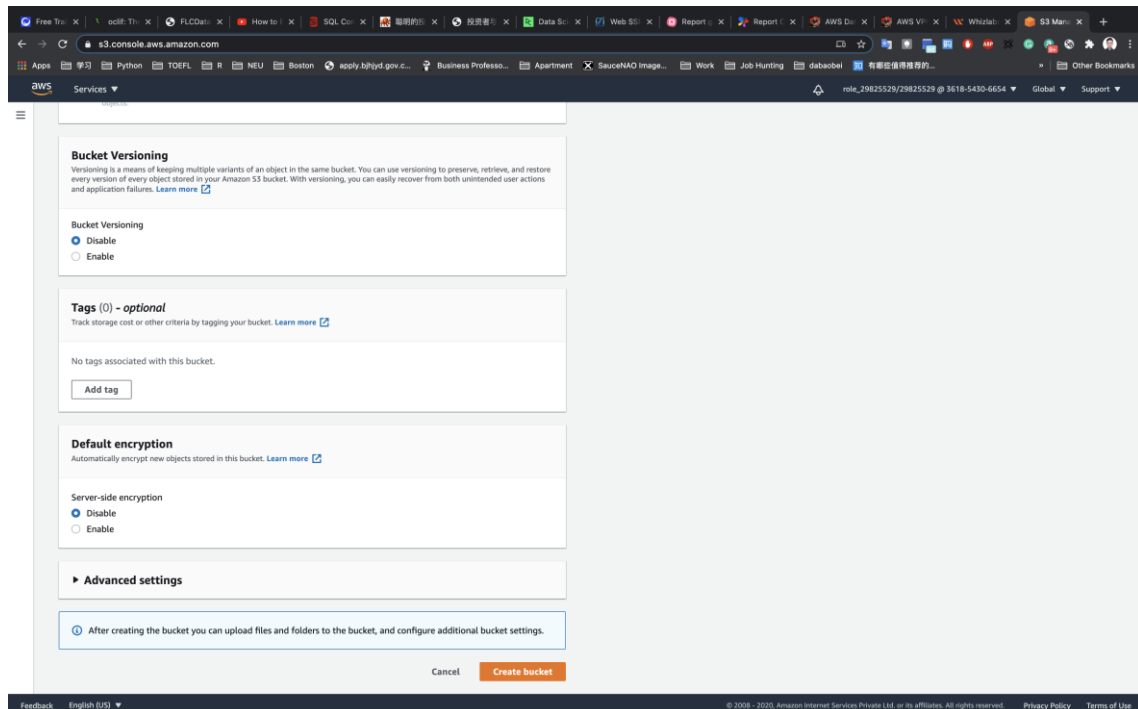
☒ **Block all public access**

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

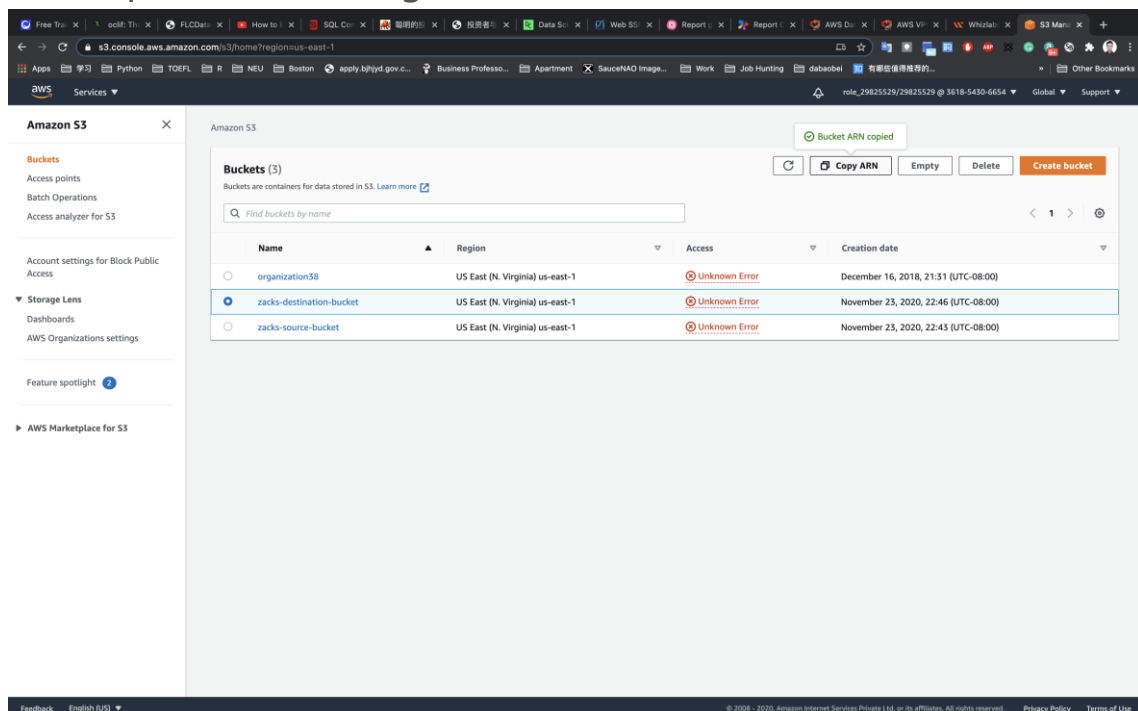
- ☒ **Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing 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.

Feedback English (US) © 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

Deje otras configuraciones por defecto y haga clic en el create botón.



Una vez que el depósito se haya creado correctamente, seleccione su depósito S3 (haga clic en la casilla de verificación).



Haga clic en Copy Bucket ARN para copiar el ARN.

- arn:aws:s3:::zacks-destination-bucket

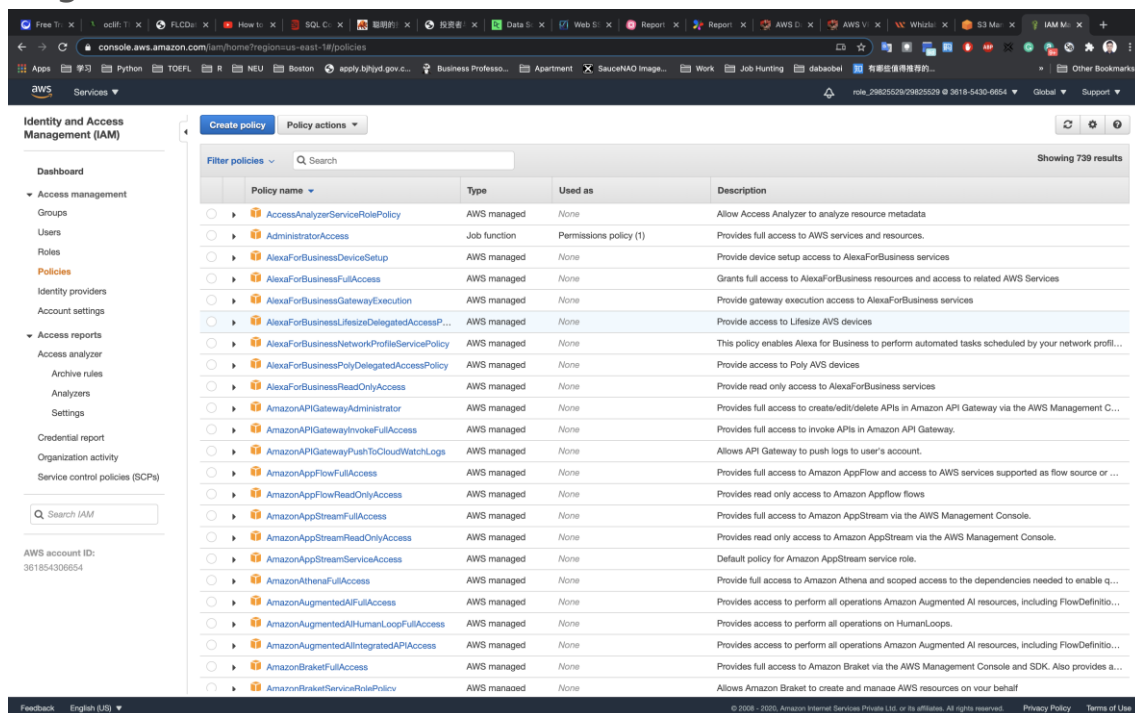
Guarde el ARN del depósito de origen en un archivo de texto para su uso posterior.

Ahora tenemos dos depósitos de S3 (origen y destino). Utilizaremos nuestra función AWS Lambda para copiar el contenido del depósito de origen al depósito de destino.

Crear una política de IAM

Como requisito previo para crear la función Lambda, debemos crear un rol de usuario con una política personalizada.

Haga clic en la pestaña **Policy actions** en **Create policy**.



Haga clic en la pestaña **JSON** y copie y pegue la siguiente declaración de política en el editor:

Política JSON

```
{  
  
  "Version":"2012-10-17",  
  
  "Statement":[  
  
    {  
  
      "Effect":"Allow",  
  
      "Action":[  
  
        "s3:GetObject"  
  
      ],  
  
      "Resource":[  
  
        "arn:aws:s3:::your_source_bucket_name/*"  
  
      ]  
  
    },  
  
    {  
  
      "Effect":"Allow",  
  
      "Action":[  
  
        "s3:PutObject"  
  
      ],  
  
      "Resource":[
```



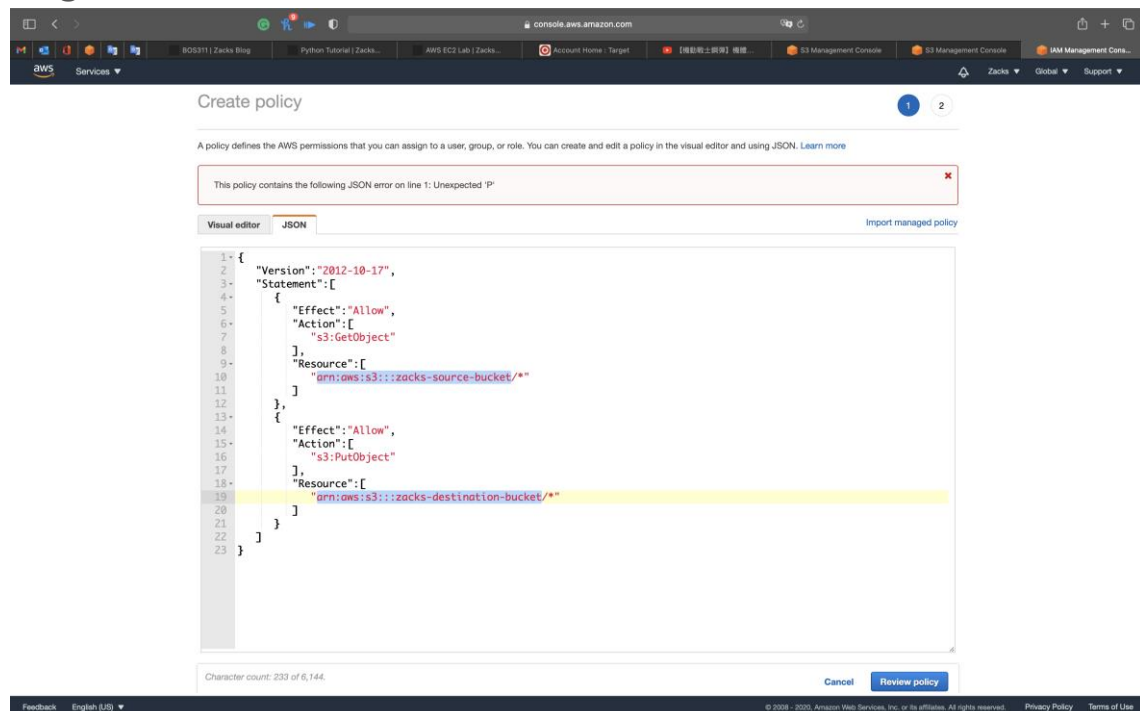
```

    "arn:aws:s3:::your_destination_bucket_name/*"
  ]
}
]
}

```

Asegúrese de tener /* después del nombre de arn.

Haga clic en Review policy.



En la página Crear política:

- Nombre de directiva: mypolicy.

Haga clic en el Create policybotón.

Create policy

Review policy

Name* mypolicy

Description

Summary

Service	Access level	Resource	Request condition
Allow (1 of 246 services) Show remaining 245			
S3	Limited: Read, Write	Multiple	None

* Required

Cancel Previous Create policy

Se crea una política de IAM con el nombre mypolicy.

Identity and Access Management (IAM)

Dashboard

Access management

Groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analysts

Settings

Credential report

Organization activity

Service control policies (SCPs)

Search IAM

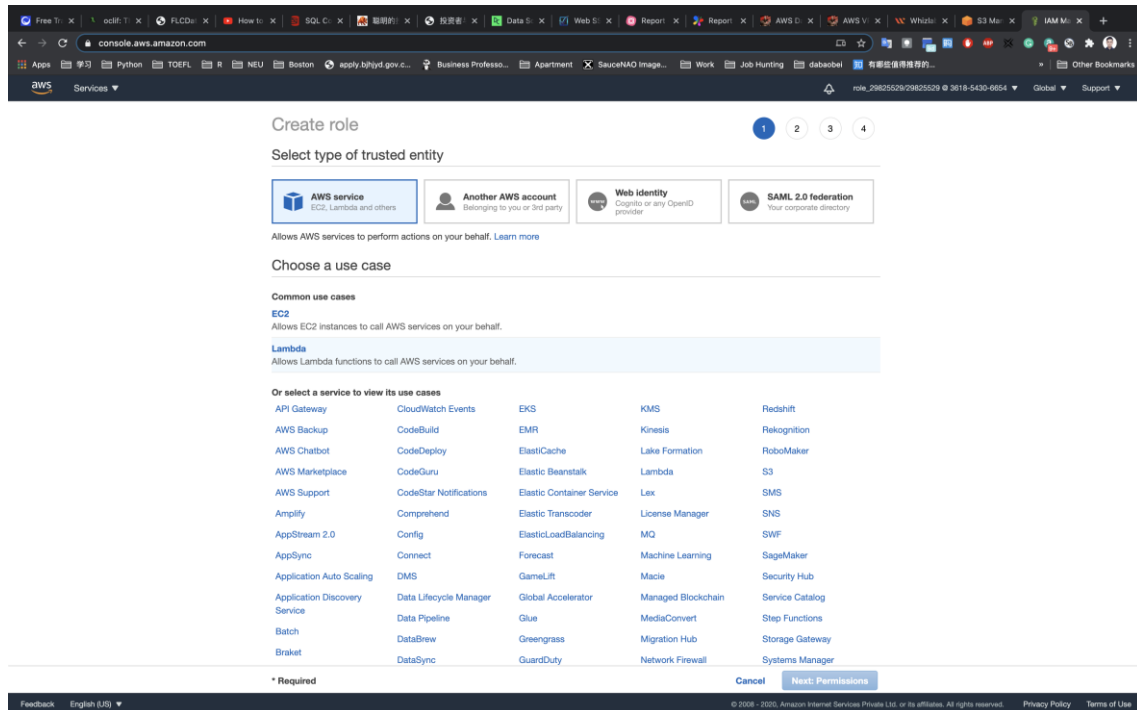
AWS account ID: 36185430654

Feedback English (US)

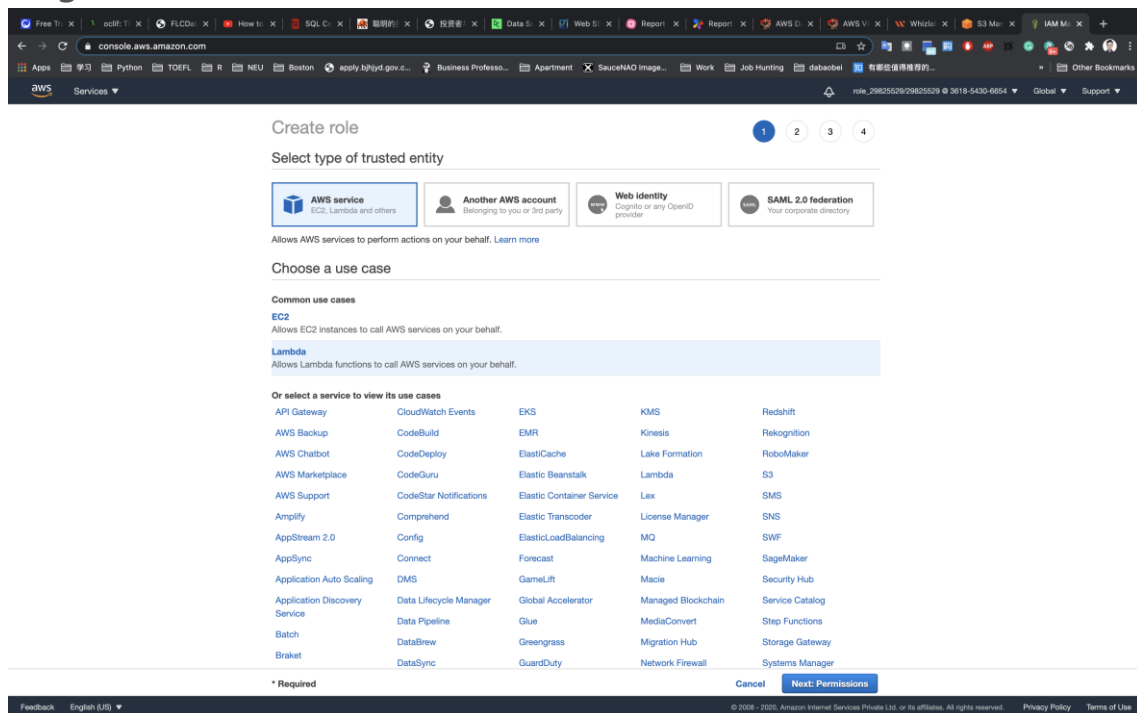
© 2009 - 2020 Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Crear una función de IAM

En el menú de la izquierda, haga clic en Roles. Haga clic en el Create role botón.

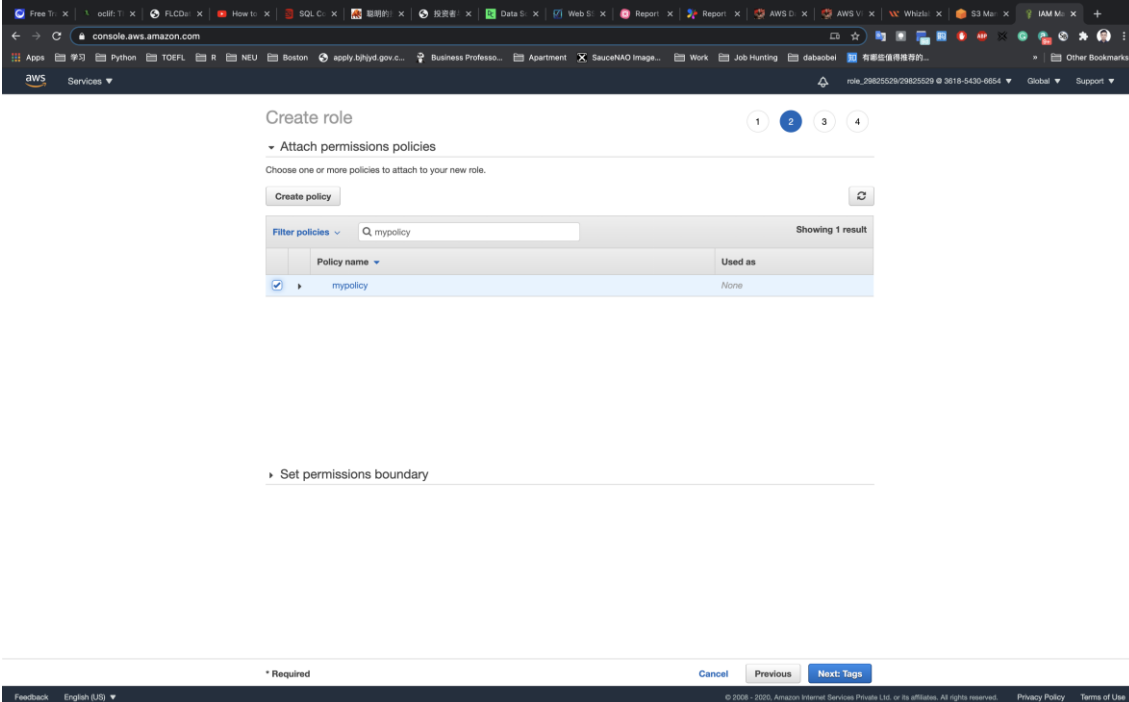


Seleccione Lambda de la lista de servicios de AWS. Haga clic en Next: Permissions.



Filtrar políticas: ahora puede ver una lista de políticas. Busque su política por nombre (`mypolicy`).

Seleccione su política y haga clic en **Next: Tags**.

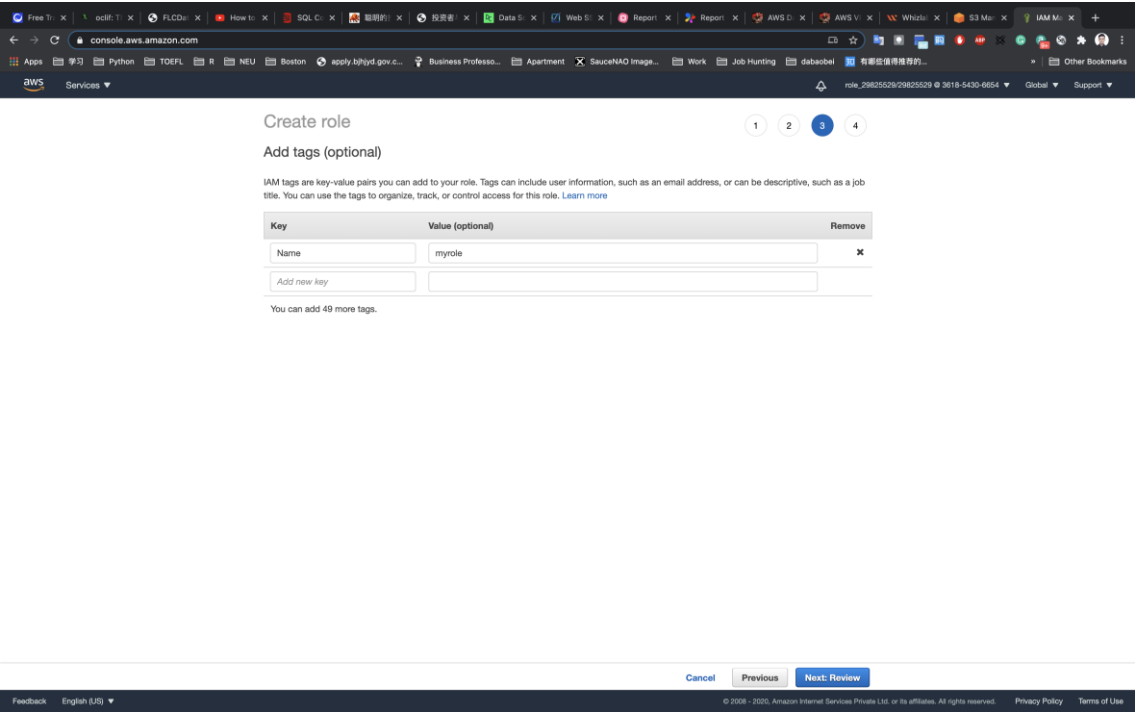


The screenshot shows the AWS IAM console 'Create role' page, step 2: Attach permissions policies. The page has a breadcrumb trail: 'Create role' > 'Attach permissions policies'. Below the breadcrumb, it says 'Choose one or more policies to attach to your new role.' There is a 'Create policy' button and a 'Filter policies' dropdown. A search bar contains 'mypolicy' and shows 'Showing 1 result'. Below the search bar is a table with one row: 'mypolicy' with a checkbox selected and 'Used as' set to 'None'. At the bottom of the page, there are buttons for 'Cancel', 'Previous', and 'Next: Tags'. The footer contains copyright information and links to 'Privacy Policy' and 'Terms of Use'.

Policy name	Used as
<input checked="" type="checkbox"/> mypolicy	None

Agregar etiquetas: proporcione un par clave-valor para el rol:

- Llave:Name
- Valor:myrole



Nombre de rol:

- Nombre de rol:myrole

Haga clic en el Create rolebotón.

Create role

1 2 3 4

Review

Provide the required information below and review this role before you create it.

Role name* myrole
Use alphanumeric and '+', '=', '@', '-' characters. Maximum 64 characters.

Role description Allows Lambda functions to call AWS services on your behalf.
Maximum 1000 characters. Use alphanumeric and '+', '=', '@', '-' characters.

Trusted entities AWS service: lambda.amazonaws.com

Policies mypolicy

Permissions boundary Permissions boundary is not set

The new role will receive the following tag

Key	Value
Name	myrole

* Required

Cancel Previous Create role

Feedback English (US)

© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Ha creado correctamente una función de IAM por nombre myrole.

Identity and Access Management (IAM)

Create role Delete role

Showing 16 results

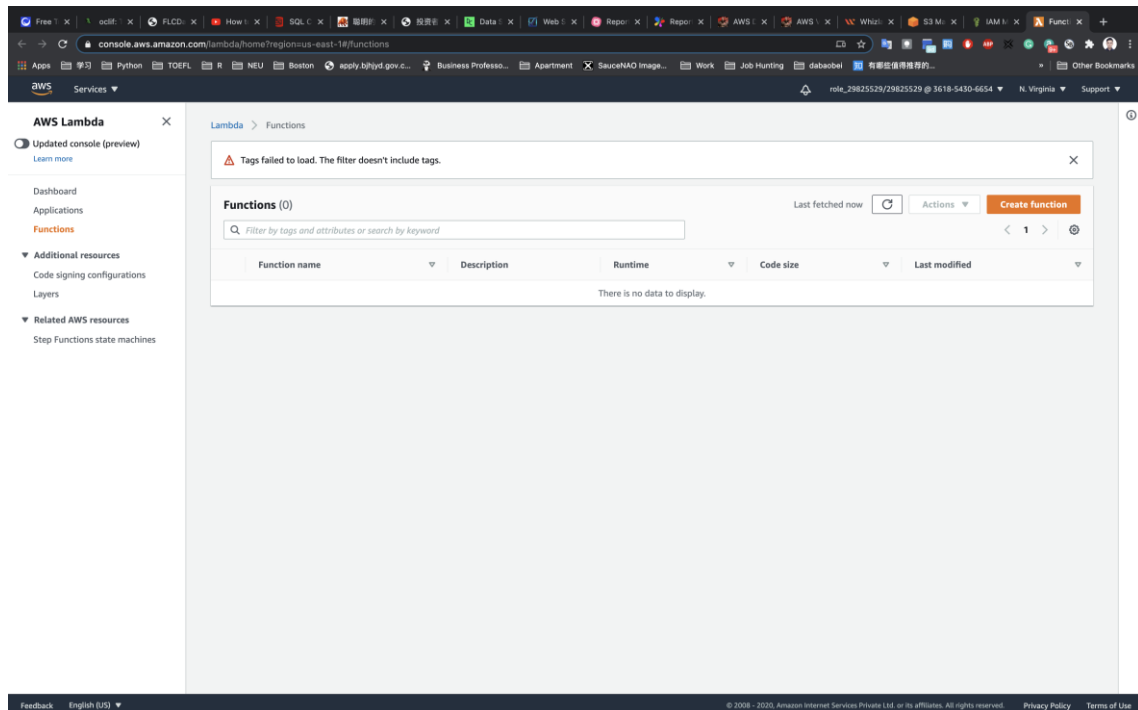
Role name	Trusted entities	Last activity
<input type="checkbox"/> AWSServiceRoleForAmazonElasticFileSystem	AWS service: elasticfilesystem (Service-Link...	Yesterday
<input type="checkbox"/> AWSServiceRoleForAmazonGuardDuty	AWS service: guardduty (Service-Linked role)	53 days
<input type="checkbox"/> AWSServiceRoleForAutoScaling	AWS service: autoscaling (Service-Linked role)	Today
<input type="checkbox"/> AWSServiceRoleForCloudTrail	AWS service: cloudtrail (Service-Linked role)	290 days
<input type="checkbox"/> AWSServiceRoleForEC2Spot	AWS service: spot (Service-Linked role)	None
<input type="checkbox"/> AWSServiceRoleForECS	AWS service: ecs (Service-Linked role)	Yesterday
<input type="checkbox"/> AWSServiceRoleForElasticBeanstalkManagedUpdates	AWS service: managedupdates.elasticbeans...	None
<input type="checkbox"/> AWSServiceRoleForElasticLoadBalancing	AWS service: elasticloadbalancing (Service-...	Today
<input type="checkbox"/> AWSServiceRoleForLexBots	AWS service: lex (Service-Linked role)	None
<input type="checkbox"/> AWSServiceRoleForOrganizations	AWS service: organizations (Service-Linked r...	304 days
<input type="checkbox"/> AWSServiceRoleForRDS	AWS service: rds (Service-Linked role)	Today
<input type="checkbox"/> AWSServiceRoleForSupport	AWS service: support (Service-Linked role)	None
<input type="checkbox"/> AWSServiceRoleForTrustedAdvisor	AWS service: trustedadvisor (Service-Linked ...	None
<input checked="" type="checkbox"/> myrole	AWS service: lambda	None
<input type="checkbox"/> OrganizationAccountAccessRole	Account: 370754977826	None
<input type="checkbox"/> role_29825529	Account: 370754977826	Today

Feedback English (US)

© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Crear una función Lambda

Haga clic en el **Create a function** botón.



Elegir Author from scratch.

- Nombre de la función: `mylambdafunction`
- Tiempo de ejecución: Seleccionar `Node.js 12x`

Función: en la sección de permisos, seleccione use an existing role.

- Rol existente: Seleccionar `myrole`

Haga

clic

en

function

The screenshot shows the AWS Lambda 'Create function' page. The 'Author from scratch' option is selected. In the 'Basic information' section, the function name is 'mylambdafunction', the runtime is 'Node.js 12.x', and the execution role is 'myrole'. The page also includes a 'Permissions' section with a link to 'Change default execution role'.

Página de configuración: en esta página, necesitamos configurar nuestra función lambda.

Si se desplaza un poco hacia abajo, podrá ver la sección **Código de función**. Aquí necesitamos escribir una función de NodeJs que copie el objeto del depósito de origen y lo pegue en el depósito de destino.

Elimine el código existente en AWS lambda index.js. Copie el siguiente código y péguelo en su archivo lambda index.js.

```
var AWS = require("aws-sdk");
```

```
exports.handler = (event, context, callback) => {
```

```
    var s3 = new AWS.S3();
```



```

var sourceBucket = "your_source_bucket_name";

var destinationBucket = "your_destination_bucket_name";

var objectKey = event.Records[0].s3.object.key;

var copySource = encodeURIComponent(sourceBucket + "/" + objectKey);

var copyParams = { Bucket: destinationBucket, CopySource:
copySource, Key: objectKey };

        s3.copyObject(copyParams, function(err, data)
{

    if (err) {

        console.log(err, err.stack);

    } else {

        console.log("S3 object copy successful.");

    }

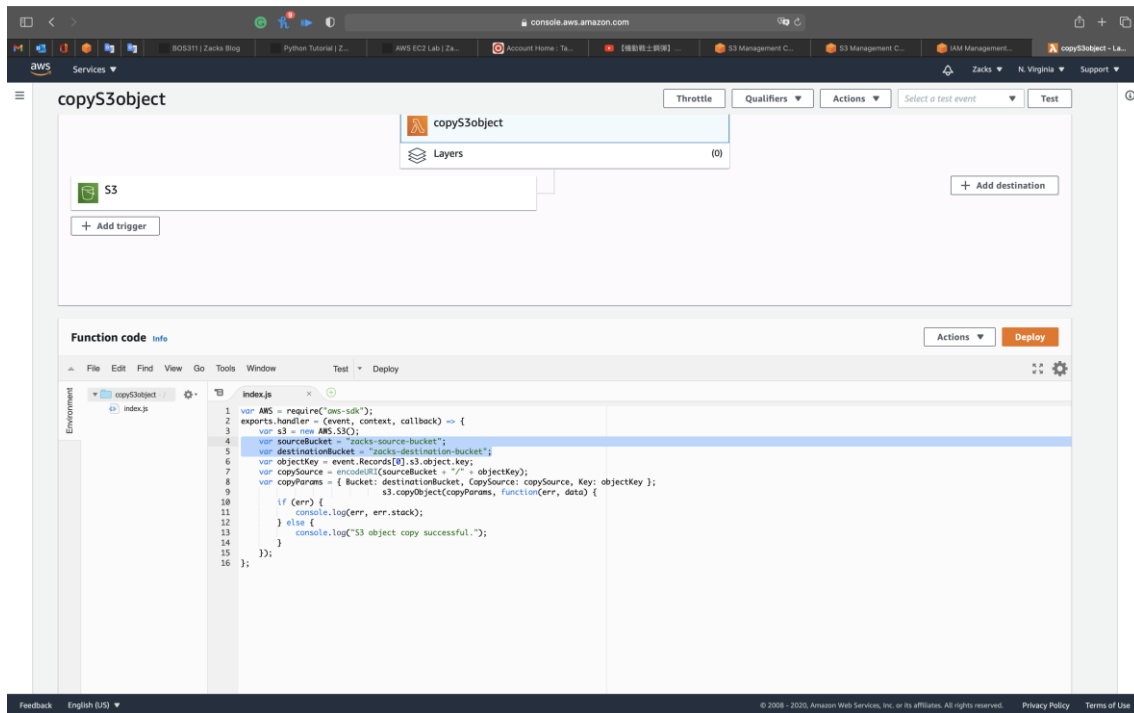
});

};

```

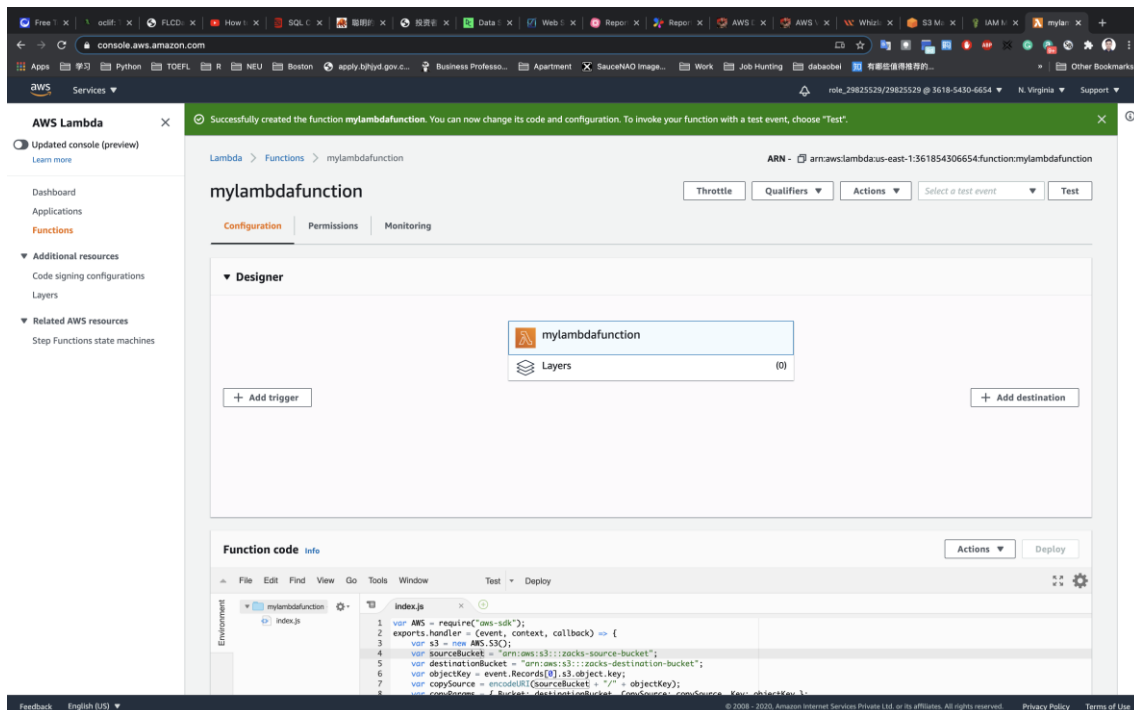
Necesitas cambiar el nombre del depósito de origen y destino (¡no ARN!) en el archivo index.js según los nombres de sus depósitos.

Guarde la función haciendo clic en `Deploy` en la esquina derecha.



Agregar disparadores a la función Lambda

Vaya a la página superior e izquierda, haga clic en `+ Add trigger Diseñador`.



Desplácese hacia abajo en la lista y seleccione S3 en la lista de activadores. Una vez que seleccione S3, aparecerá un formulario. Ingrese estos detalles:

- Depósito: seleccione su depósito de origen
- your_source_bucket_name.
- Tipo de evento: All object create events

Deje otros campos por defecto.

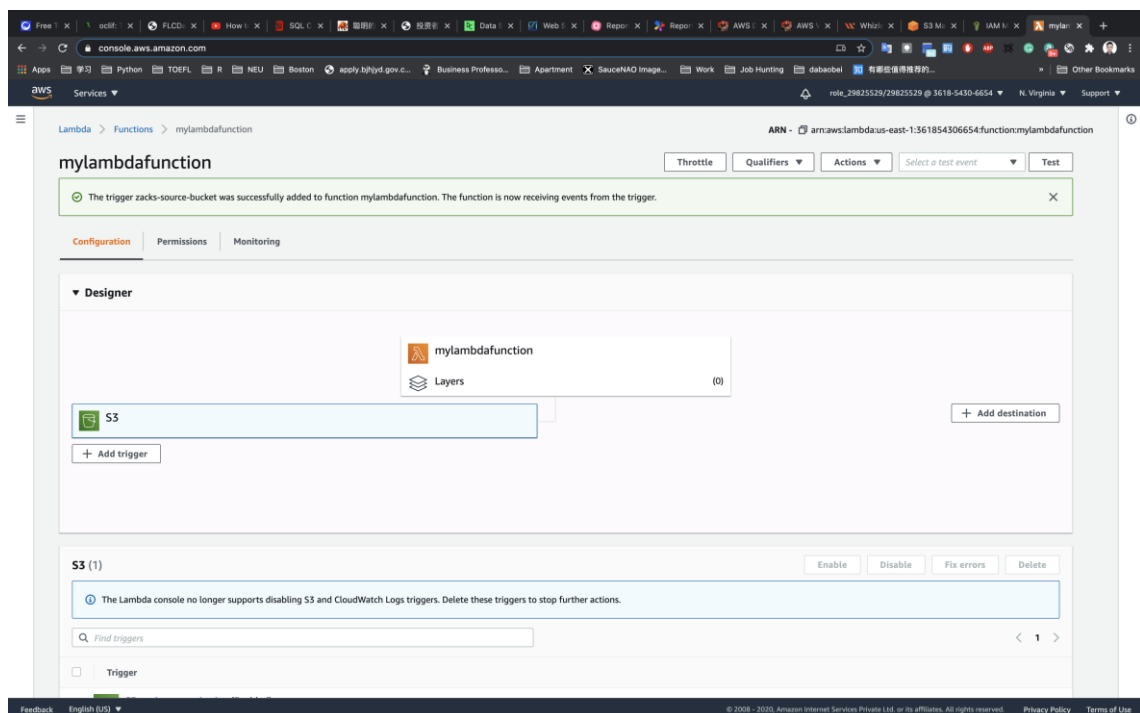
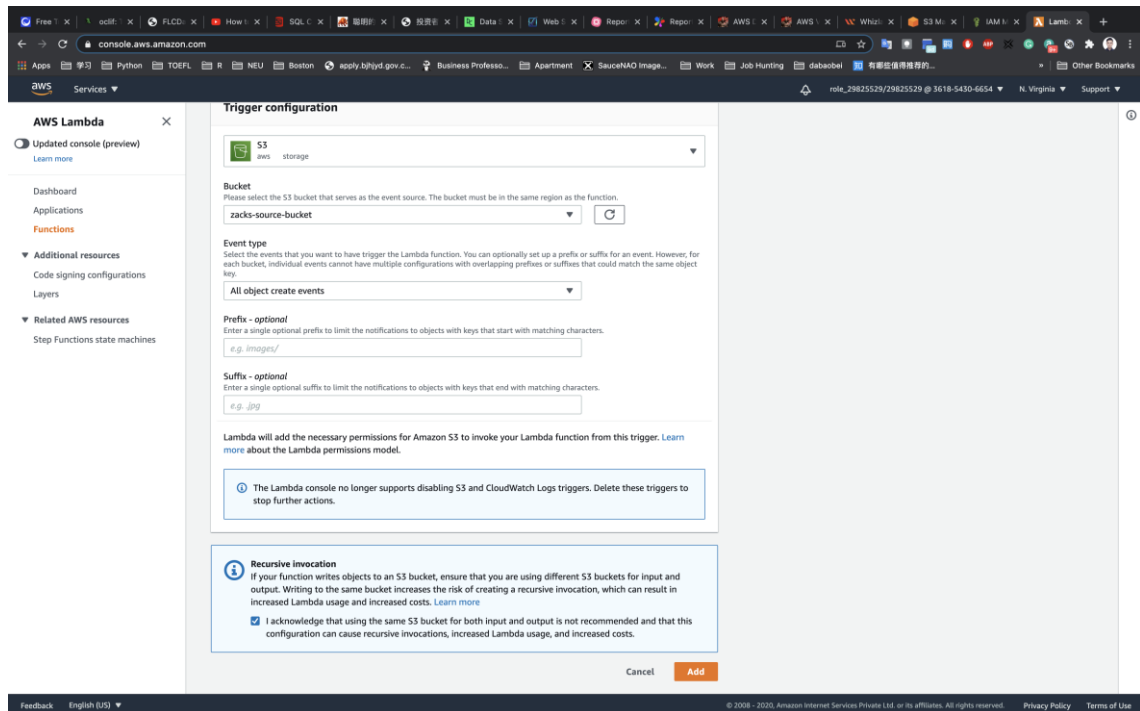
The screenshot shows the AWS Lambda console interface for adding a new trigger. The left sidebar contains navigation links for Dashboard, Applications, Functions, and Additional resources. The main content area is titled 'Add trigger' and includes a 'Trigger configuration' section. In this section, 'S3' is selected as the trigger provider. Below this, the 'Bucket' field is populated with 'zacks-source-bucket'. The 'Event type' is set to 'All object create events'. There are also input fields for 'Prefix - optional' (with the example 'e.g. images/') and 'Suffix - optional' (with the example 'e.g. .jpg'). A blue information box states: 'The Lambda console no longer supports disabling S3 and CloudWatch Logs triggers. Delete these triggers to stop further actions.' At the bottom, there is a 'Recursive invocation' warning: 'If your function writes objects to an S3 bucket, ensure that you are using different S3 buckets for input and output. Writing to the same bucket increases the risk of creating a recursive invocation, which can result in increased Lambda usage and increased costs. Learn more.' The footer of the console shows 'Feedback', 'English (US)', and copyright information for 2018-2020.

Y marque esta opción de **invocación recursiva** para evitar fallas en caso de que cargue varios archivos a la vez.

Haga

clic

en Add.



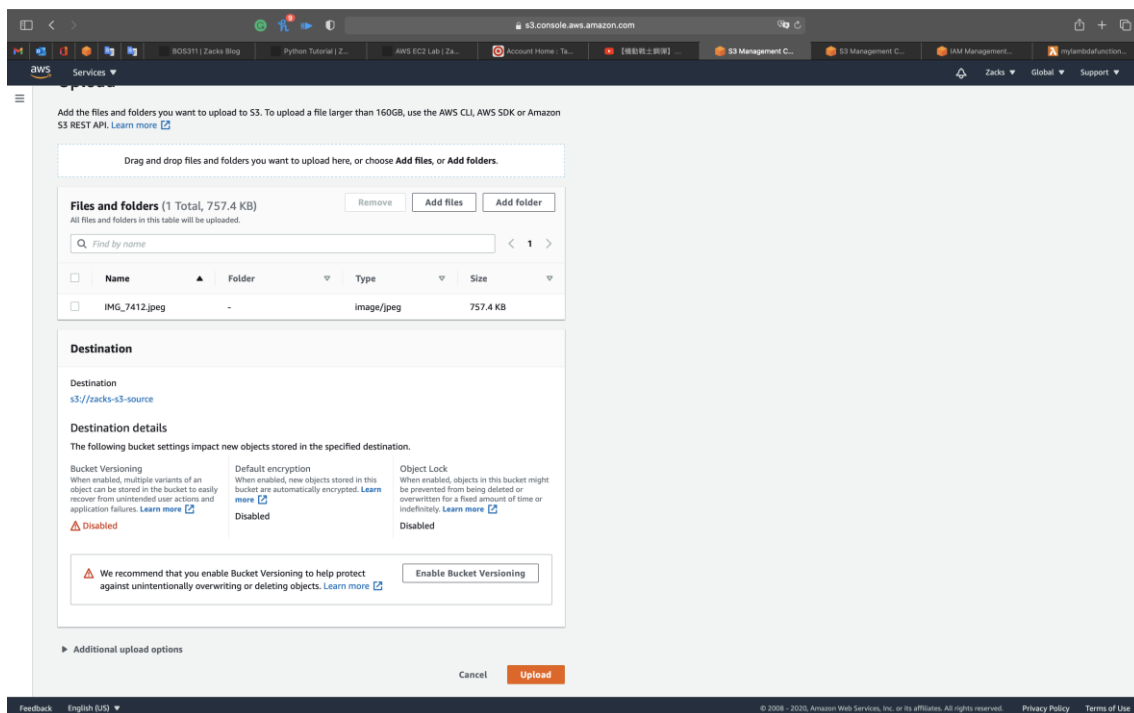
Prueba de validación

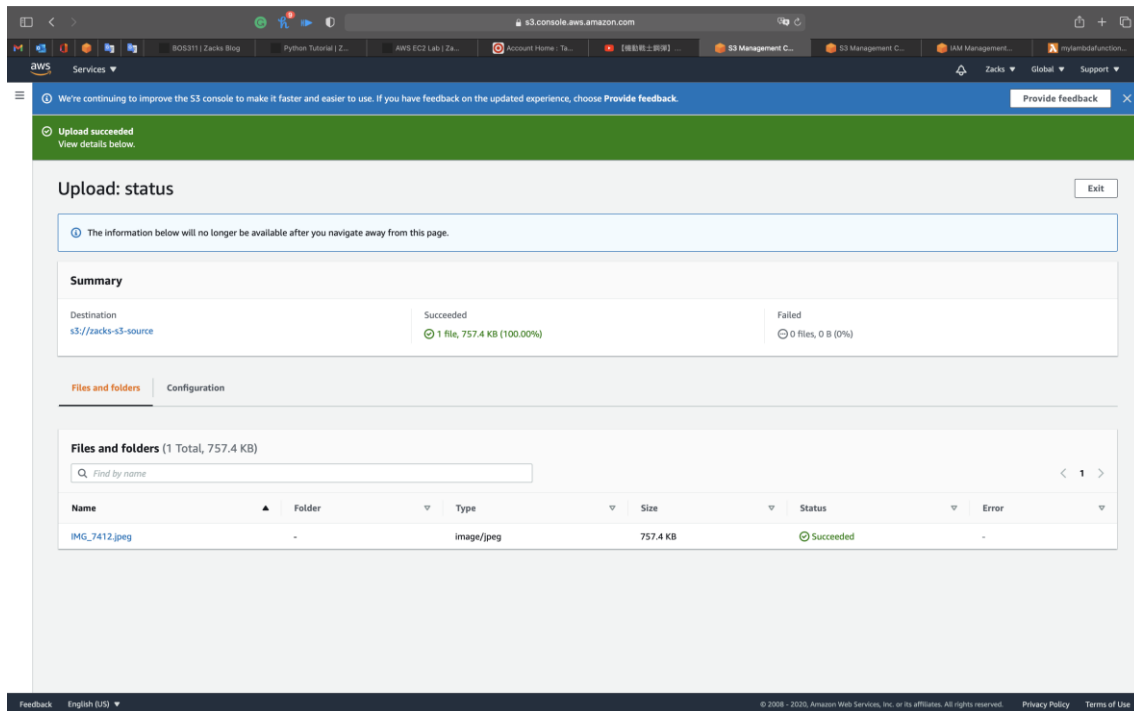
Prepare una imagen en su máquina local.

Vaya a la lista de depósitos y haga clic en el depósito de origen
- `your_source_bucket_name`.

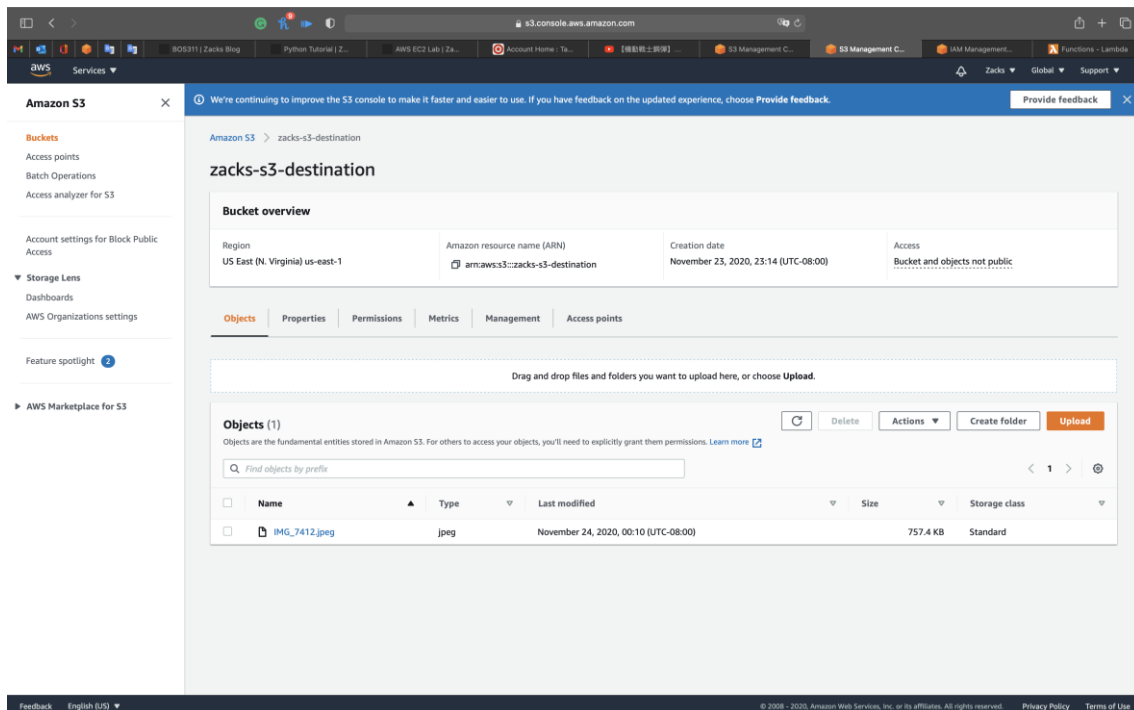
Cargue la imagen al depósito S3 de origen. Para hacer eso:

- Haga clic en el `upload` botón.
- Haga clic en `Add files` para agregar los archivos.
- Seleccione la imagen y haga clic en el `upload` botón para cargar la imagen.

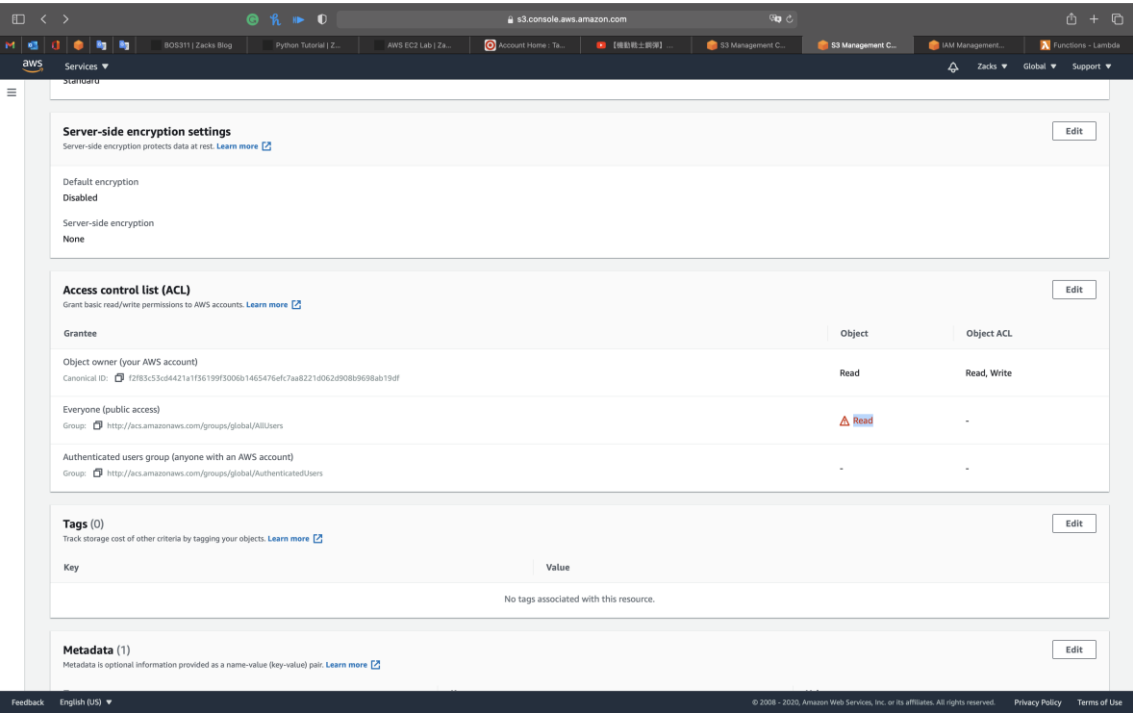




Ahora regrese a la lista de S3 y abra su depósito de destino: `your_destination_bucket_name`.



Para abrir el objeto, desplácese hacia abajo y cambie ACL - Everyone Read



Puede ver una copia de la imagen del depósito de origen cargada en el depósito de destino.