

Examen Practico

Angel Gonzalez - angonpad@gmail.com

Actividad 1. PEM nuevas

The screenshot shows the 'Create key pair' page in the AWS Management Console. The breadcrumb navigation at the top indicates the path: EC2 > Key pairs > Create key pair. The main heading is 'Create key pair' with an 'Info' link. Below this, a description states: 'A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.' The form includes a 'Name' field with the value 'angonzalez-padillaEXAM' and a note: 'The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.' The 'Key pair type' section has two radio buttons: 'RSA' (selected) and 'ED25519'. The 'Private key file format' section has two radio buttons: '.pem' (selected) and '.ppk'. Below these are instructions: 'For use with OpenSSH' for .pem and 'For use with PuTTY' for .ppk. There is an 'Add new tag' button and a note: 'No tags associated with the resource. You can add up to 50 more tags.' At the bottom right are 'Cancel' and 'Create key pair' buttons.

Actividad 2. Creación de la instancia EC2 Asignación de Keys

The screenshot shows the 'Key pair (login)' section in the AWS Management Console. It includes a description: 'You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.' Below this is a 'Key pair name - required' dropdown menu with the value 'angonzalez-padillaEXAM' and a 'Create new key pair' button with a refresh icon.

Configuración de red

The screenshot shows the 'Network settings' section in the AWS Management Console. It includes a 'VPC - required' dropdown menu with the value 'vpc-00f479057476a2db8' and a '(default)' label. Below this is a 'Subnet' dropdown menu with the value 'subnet-0b2fbf6da06d9ba4b'. The 'Auto-assign public IP' section has a dropdown menu with the value 'Enable'. The 'Firewall (security groups)' section has two radio buttons: 'Create security group' (selected) and 'Select existing security group'. Below this is a 'Security group name - required' dropdown menu with the value 'angel-gonzalez-exam-sg'. The 'Description - required' dropdown menu has the value 'Sg creado para el examen'. At the bottom, there is a table for 'Inbound Security Group Rules' with one rule: 'Security group rule 1 (TCP, 22, 161.59.3.165/32, ssh-angelEXAM)'. The table has columns for 'Type', 'Protocol', and 'Port range'. The 'Type' column has the value 'ssh', the 'Protocol' column has the value 'TCP', and the 'Port range' column has the value '22'. There is a 'Remove' button next to the rule.

Creación de Security Group

Create security group

Select existing security group

Security group name - required

angel-gonzalez-exam-sg

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and _-./!@#%^&*~:[]{}|'`" ,; .

Description - required

Sg creado para el examen

Info

Inbound Security Group Rules

Security group rule 1 (TCP, 22, 181.59.3.163/32, ssh-angelEXAM)

Remove

Type

Info

ssh

Protocol

Info

TCP

Port range

Info

22

Source type

Info

My IP

Name

Info

181.59.3.163/32

Description - optional

Info

ssh-angelEXAM

Security group rule 2 (TCP, 80, 0.0.0.0/0)

Remove

Type

Info

HTTP

Protocol

Info

TCP

Port range

Info

80

Source type

Info

Anywhere

Source

Info

0.0.0.0/0

Description - optional

Info

e.g. SSH for admin desktop

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Add security group rule

Advanced network configuration

Configuración de parametros avanzados

User data - optional

Info

Upload a file with your user data or enter it in the field.

Choose file

```
#!/bin/bash
# Update system
dnf update -y
# Install required packages
dnf install -y httpd wget php php-fpm php-mysql php-ison php-devel
php-mbstring mariadb105 unzip
# Enable and start Apache
systemctl enable httpd
systemctl start httpd
# Install web app
cd /var/www/html
if [ ! -f immersion-day-app-php7.zip ]; then
  wget -O immersion-day-app-php7.zip
  https://static.us-east-1.prod.workshops.aws/public/0cf8e0cc-9aa4-41b3-aa
  e7-ea46d24b239e/assets/immersion-day-app-php7.zip
  unzip immersion-day-app-php7.zip
fi
# Install AWS SDK
if [ ! -d /var/www/html/vendor ]; then
  mkdir vendor
  cd vendor
  wget https://docs.aws.amazon.com/aws-sdk-php/v3/download/aws.zip
  unzip aws.zip
fi
```

User data has already been base64 encoded

Instancia EC2 creada con éxito

Instance summary for i-08083666d9af03a84 (Angel-Gonzalez-EXAMEN)

Info

Connect

Instance state

Actions

Updated less than a minute ago

Instance ID

i-08083666d9af03a84

IPv6 address

-

Hostname type

IP name: ip-172-31-23-100.ec2.internal

Answer private resource DNS name

IPv4 (A)

Auto-assigned IP address

54.80.3.62 [Public IP]

IAM role

-

IMDSv2

Required

Operator

-

Public IPv4 address

54.80.3.62 | open address

Instance state

Running

Private IP DNS name (IPv4 only)

ip-172-31-23-100.ec2.internal

Instance type

t3.micro

VPC ID

vpc-00f479057476a2db8

Subnet ID

subnet-0e946236dc39c8c58

Instance ARN

arn:aws:ec2:us-east-1:654654478122:instance/i-08083666d9af03a84

Private IPv4 addresses

172.31.23.100

Public DNS

ec2-54-80-3-62.compute-1.amazonaws.com | open address

Elastic IP addresses

-

AWS Compute Optimizer finding

User: arn:aws:iam::654654478122:user/students/anggonpad@gmail.com is not a authorized to perform: compute-optimizer:GetEnrollmentStatus on resource: * be cause no identity-based policy allows the compute-optimizer:GetEnrollmentStat us action

Auto Scaling Group name

-

Managed

false

Details

Status and alarms

Monitoring

Security

Networking

Storage

Tags

Verificación con SSH

```

~ 19:34
> ssh -i "angonzalez-padillaEXAM.pem" ec2-user@ec2-54-80-3-62.compute-1.amazonaws.com
The authenticity of host 'ec2-54-80-3-62.compute-1.amazonaws.com (54.80.3.62)' can't be established.
ED25519 key fingerprint is: SHA256:77HyDZ6IKr/+VSddfjQit3V6y7a2o5OTMlgm5q9A8Dc
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-54-80-3-62.compute-1.amazonaws.com' (ED25519) to the list of known hosts.
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html

#_
~\_ ##### Amazon Linux 2023
nn \#####\
nn \###\
nn \#/ --- https://aws.amazon.com/linux/amazon-linux-2023
nn V~' '→
nn
nn _ _/ _/
nn _/ _/
nn _/m/ '
[ec2-user@ip-172-31-23-100 ~]$

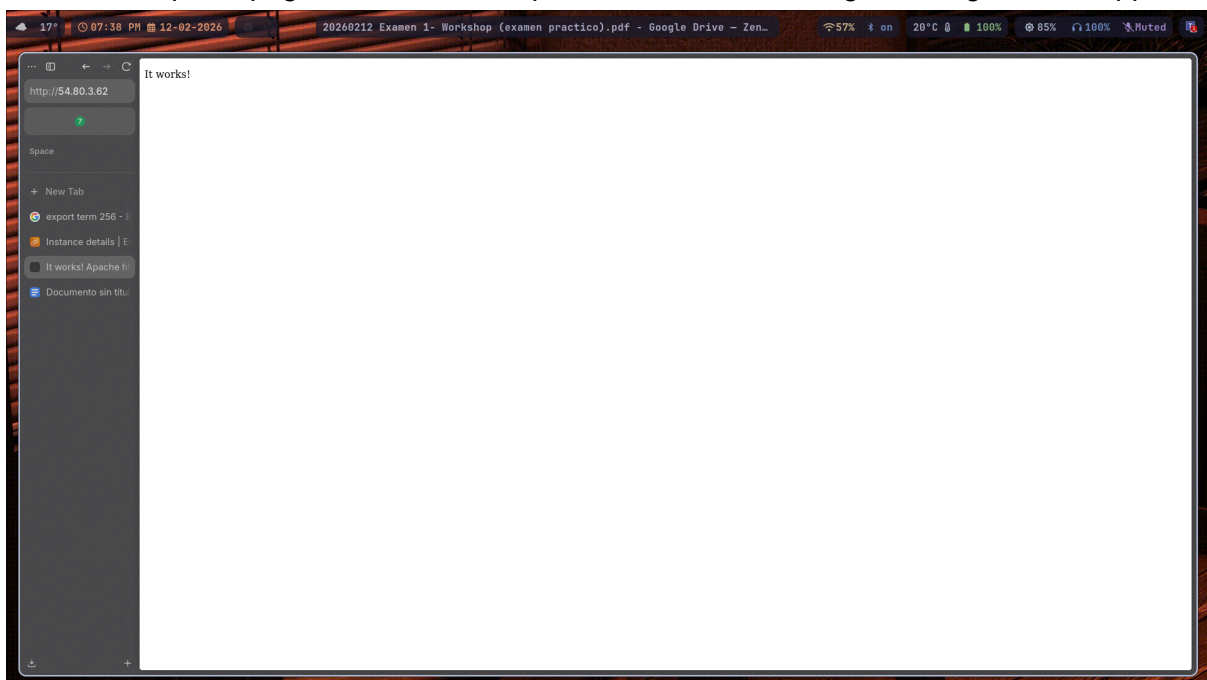
```

Comprobamos que apache esté corriendo

```
[ec2-user@ip-172-31-23-100 ~]$ sudo systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
   Drop-In: /usr/lib/systemd/system/httpd.service.d
            └─php-fpm.conf
   Active: active (running) since Fri 2026-02-13 00:34:04 UTC; 3min 0s ago
     Docs: man:httpd.service(8)
  Main PID: 3654 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes served/sec: 0 B/sec"
     Tasks: 177 (Limit: 1067)
    Memory: 17.2M
       CPU: 341ms
    CGroup: /system.slice/httpd.service
            └─3654 /usr/sbin/httpd -DFOREGROUND
              └─3871 /usr/sbin/httpd -DFOREGROUND
                └─3874 /usr/sbin/httpd -DFOREGROUND
                  └─3910 /usr/sbin/httpd -DFOREGROUND
                    └─3932 /usr/sbin/httpd -DFOREGROUND

Feb 13 00:34:04 ip-172-31-23-100.ec2.internal systemd[1]: Starting httpd.service - The Apache HTTP Server...
Feb 13 00:34:04 ip-172-31-23-100.ec2.internal systemd[1]: Started httpd.service - The Apache HTTP Server.
Feb 13 00:34:04 ip-172-31-23-100.ec2.internal httpd[3654]: Server configured, listening on: port 80
[ec2-user@ip-172-31-23-100 ~]$
```

Verificamos que la página sea accesible públicamente sin embargo no cargo la web app



Se corrige descargando manualmente desde ssh

```
[ec2-user@ip-172-31-23-100 html]$ ls -l
total 84
drwxr-xr-x. 3 root root 16384 Feb 13 01:02 __MACOSX
-rw-r--r--. 1 root root 463 Jul 24 2013 db-update.php
-rw-r--r--. 1 root root 368 Sep 17 2012 get-cpu-load.php
-rw-r--r--. 1 root root 1420 Jun 22 2023 get-index-meta-data.php
-rw-r--r--. 1 root root 14135 Dec 3 17:31 immersion-day-app-php7.zip
-rw-r--r--. 1 root root 370 Dec 29 2021 index.php
-rw-r--r--. 1 root root 371 Apr 10 2013 load.php
-rw-r--r--. 1 root root 357 May 4 2021 menu.php
-rw-r--r--. 1 root root 543 Oct 2 2014 put-cpu-load.php
-rw-r--r--. 1 root root 134 Dec 29 2021 rds-initialize.php
-rw-r--r--. 1 root root 3515 Jan 11 2022 rds-read-data.php
-rw-r--r--. 1 root root 1257 Dec 29 2021 rds-write-config.php
-rw-r--r--. 1 root root 3192 Jun 22 2023 rds.conf.php
-rw-r--r--. 1 root root 346 Dec 29 2021 rds.php
drwxr-xr-x. 2 root root 29 Dec 29 2021 sql
-rw-r--r--. 1 root root 877 Sep 6 2012 style.css
drwxr-xr-x. 6 root root 186 Feb 13 01:03 vendor
[ec2-user@ip-172-31-23-100 html]$
```

Al comprobar ya funciona



Actividad 4. EBS con tags

Se crea el EBS en la AZ correcta (en mi instancia es la us-east-1c)

Create volume [Info](#)

Create an Amazon EBS volume to attach to any EC2 instance in the same Availability Zone.

Volume settings


Volume type [Info](#)
General Purpose SSD (gp3) ▼

Size (GiB) [Info](#)
3 ▼
Min: 1 GiB, Max: 65536 GiB.

IOPS [Info](#)
3000 ▼
Min: 3000 IOPS, Max: 80000 IOPS.

Throughput (MiB/s) [Info](#)
125 ▼
Min: 125 MiB, Max: 2000 MiB. Baseline: 125 MiB/s.

Availability Zone [Info](#)
use1-az4 (us-east-1c) ▼

Snapshot ID - optional [Info](#)
Don't create volume from a snapshot ▼ 

Encryption [Info](#)
Use Amazon EBS encryption as an encryption solution for your EBS resources associated with your EC2 instances.
☐ Encrypt this volume

Agregamos el tag para identificarlo

Tags - optional [Info](#)

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional	
<input type="text" value="Q Name"/>	<input type="text" value="Q angel-gonzalezEXAMEN"/>	<input type="button" value="Remove"/>


You can add up to 49 more tags.

Le hacemos el attach a mi instancia

Attach volume [Info](#)


Attach a volume to an instance to use it as you would a regular physical hard disk drive.

Basic details

Volume ID
 vol-04b23fead9399e75a (angel-gonzalezEXAMEN)


Availability Zone
use1-az4 (us-east-1c)

Instance [Info](#)

(Angel-Gonzalez-EXAMEN) (running) 

Device name [Info](#)

Recommended device names for Linux: /dev/xvda for root volume, /dev/sd[f-p] for data volumes.

 Newer Linux kernels may rename your devices to /dev/xvdf through /dev/xvdp internally, even when the device name entered here (and shown in the details) is /dev/sdf through /dev/sdp.

Revisamos que se encuentre el disco

```
[ec2-user@ip-172-31-23-100 ~]$ lsblk
NAME                                MAJ:MIN RM  SIZE RO  TYPE MOUNTPOINTS
nvme0n1                             259:0    0   8G  0  disk
├─nvme0n1p1                         259:1    0   8G  0  part /
├─nvme0n1p127                      259:2    0   1M  0  part
└─nvme0n1p128                      259:3    0   1M  0  part /boot/efi
nvme1n1                             259:4    0   3G  0  disk
```

Actividad 5. Bucket S3

Create bucket

Buckets are containers for data stored in S3.

General configuration

AWS Region

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

Bucket type

General purpose

Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

Directory

Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name

angel-gonzalez-padilla-EXAMEN-S3

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). [Learn more](#)

Copy settings from existing bucket - optional

Only the bucket settings in the following configuration are copied.

Choose bucket

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.

Object Ownership

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 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.

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

Disable

Enable

Asignamos tag

Tags - optional

You can use bucket tags to analyze, manage and specify permissions for a bucket. [Learn more](#)

You can use s3:ListTagsForResource, s3:TagResource, and s3:UntagResource APIs to manage tags on S3 general purpose buckets for access control in addition to cost allocation and resource organization. To ensure a seamless transition, please provide permissions to s3:ListTagsForResource, s3:TagResource, and s3:UntagResource actions. [Learn more](#)

Key

Name

Value - optional

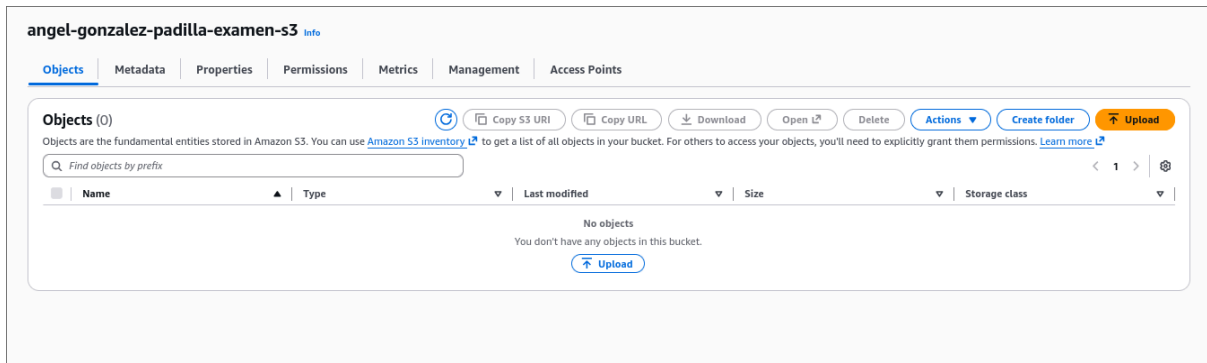
AngelGonzalez-ExamenS3

Remove

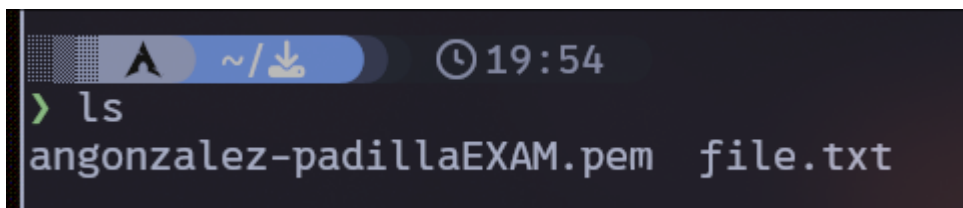
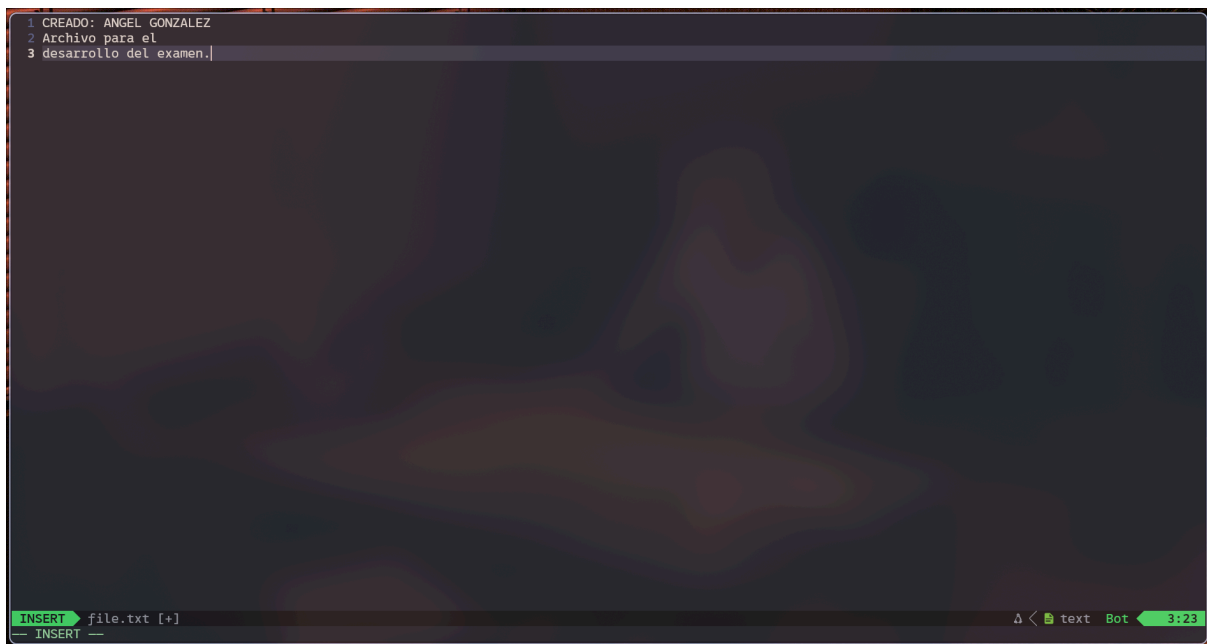
Add new tag

You can add up to 49 more tags.

Creado con éxito



Creamos un archivo .txt



Lo subimos al bucket

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 SDKs or Amazon S3 REST API. [Learn more](#)

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

Files and folders (1 total, 63.0 B)

RemoveAdd filesAdd folder

All files and folders in this table will be uploaded.

Q Find by name

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	file.txt	-	text/plain	63.0 B

Destination

Info

Destination

s3://angel-gonzalez-padilla-examen-s3

► 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

Subido con éxito

Upload succeeded

For more information, see the [Files and folders](#) table.

Upload: status

Close

After you navigate away from this page, the following information is no longer available.

Summary

Destination

s3://angel-gonzalez-padilla-examen-s3

Succeeded

✔ 1 file, 63.0 B (100.00%)

Failed

⊖ 0 files, 0 B (0%)

Files and folders

Configuration

Files and folders (1 total, 63.0 B)

Find by name

Name	Folder	Type	Size	Status	Error
file.txt	-	text/plain	63.0 B	✔ Succeeded	-