

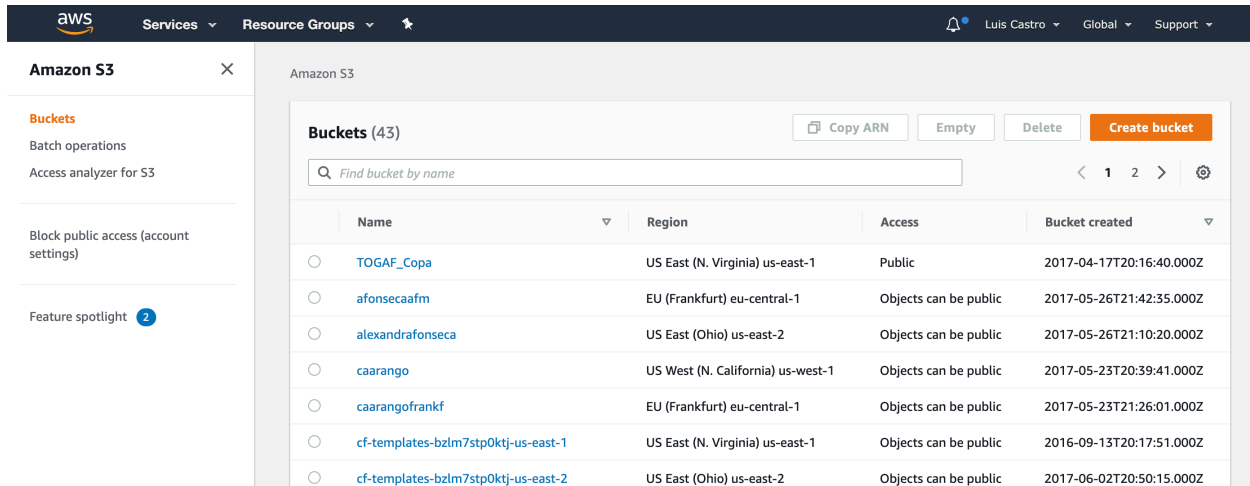
## Step 1

Access the AWS console through the following link:

<https://450006219561.signin.aws.amazon.com/console>

## Step 2

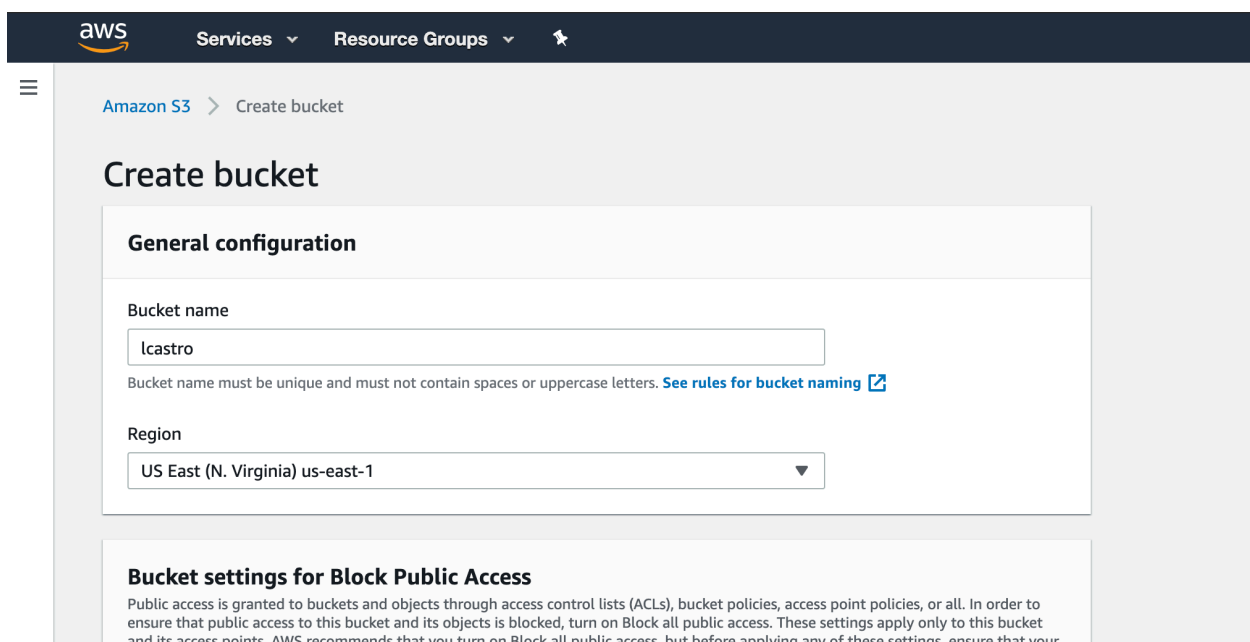
Access the S3 service



Name	Region	Access	Bucket created
TOGAF_Copa	US East (N. Virginia) us-east-1	Public	2017-04-17T20:16:40.000Z
afonsecaafm	EU (Frankfurt) eu-central-1	Objects can be public	2017-05-26T21:42:35.000Z
alexandrafonseca	US East (Ohio) us-east-2	Objects can be public	2017-05-26T21:10:20.000Z
caarango	US West (N. California) us-west-1	Objects can be public	2017-05-23T20:39:41.000Z
caarangofrankf	EU (Frankfurt) eu-central-1	Objects can be public	2017-05-23T21:26:01.000Z
cf-templates-bzlm7stp0ktj-us-east-1	US East (N. Virginia) us-east-1	Objects can be public	2016-09-13T20:17:51.000Z
cf-templates-bzlm7stp0ktj-us-east-2	US East (Ohio) us-east-2	Objects can be public	2017-06-02T20:50:15.000Z

## Step 3

Create a new Bucket with the username in Create Bucket, select the corresponding region and click Create Bucket



**General configuration**

Bucket name  
lcastro

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

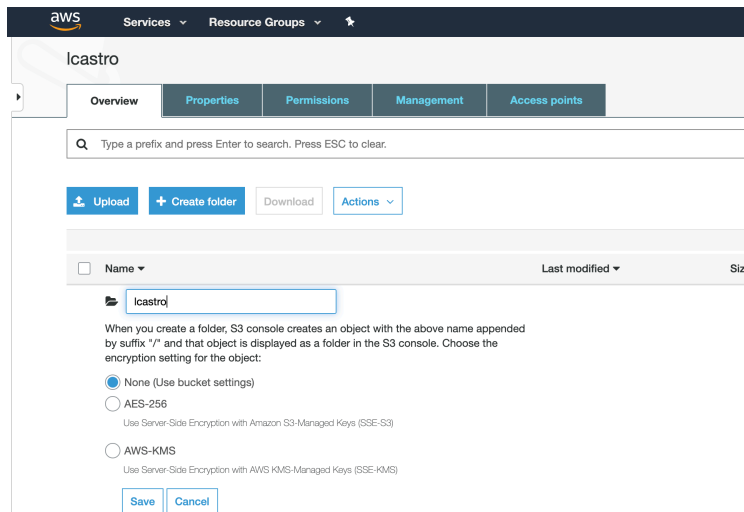
**Bucket settings for Block Public Access**

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

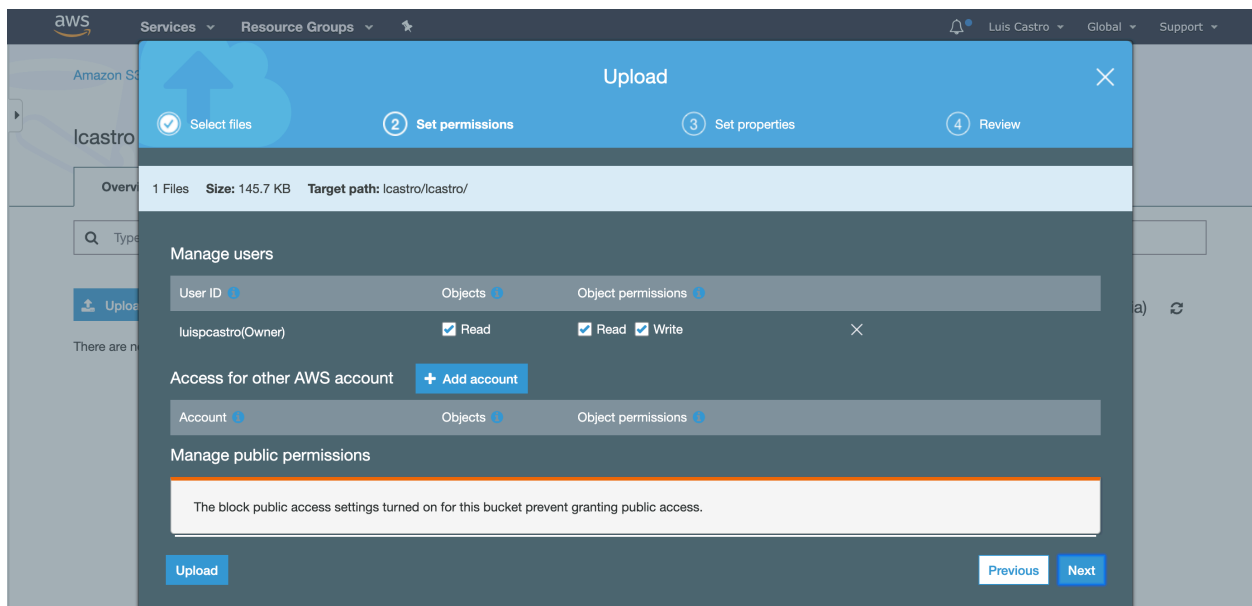
## Step 4

Inside the created Bucket create a new folder with the same username in Create Folder and upload the file sent via email / share:

**palo-alto-networks-product-summary-specsheet**

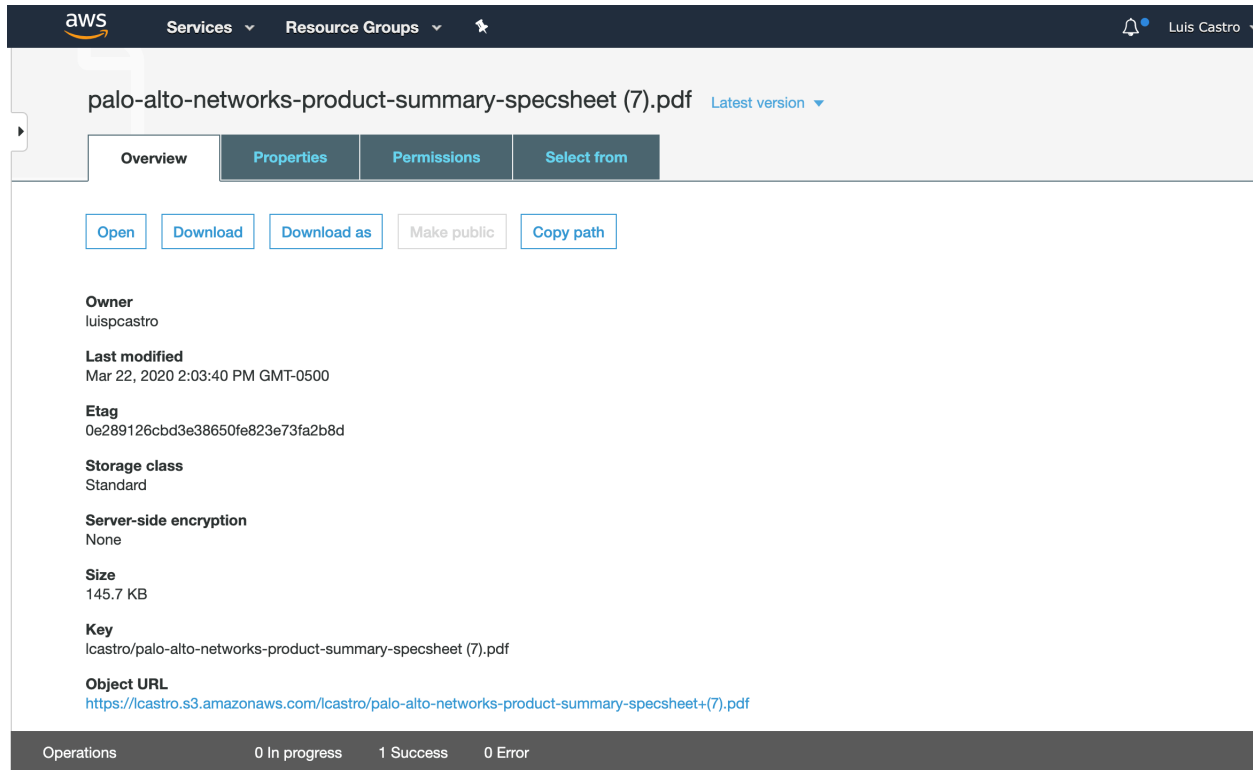


Click Upload and accept the values by Default



## Step 5

Check within the properties of the loaded file the link of the file and click to open the link



The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with 'aws', 'Services', 'Resource Groups', and a user profile 'Luis Castro'. Below this, the file name 'palo-alto-networks-product-summary-specsheet (7).pdf' is displayed with a 'Latest version' dropdown. A tabbed interface shows 'Overview', 'Properties', 'Permissions', and 'Select from'. Under 'Overview', there are buttons for 'Open', 'Download', 'Download as', 'Make public', and 'Copy path'. The 'Properties' section lists the following details:

- Owner:** luispcastro
- Last modified:** Mar 22, 2020 2:03:40 PM GMT-0500
- Etag:** 0e289126cbd3e38650fe823e73fa2b8d
- Storage class:** Standard
- Server-side encryption:** None
- Size:** 145.7 KB
- Key:** lcastro/palo-alto-networks-product-summary-specsheet (7).pdf
- Object URL:** [https://lcastro.s3.amazonaws.com/lcastro/palo-alto-networks-product-summary-specsheet+\(7\).pdf](https://lcastro.s3.amazonaws.com/lcastro/palo-alto-networks-product-summary-specsheet+(7).pdf)

At the bottom, an 'Operations' bar shows '0 In progress', '1 Success', and '0 Error'.

## Step 6

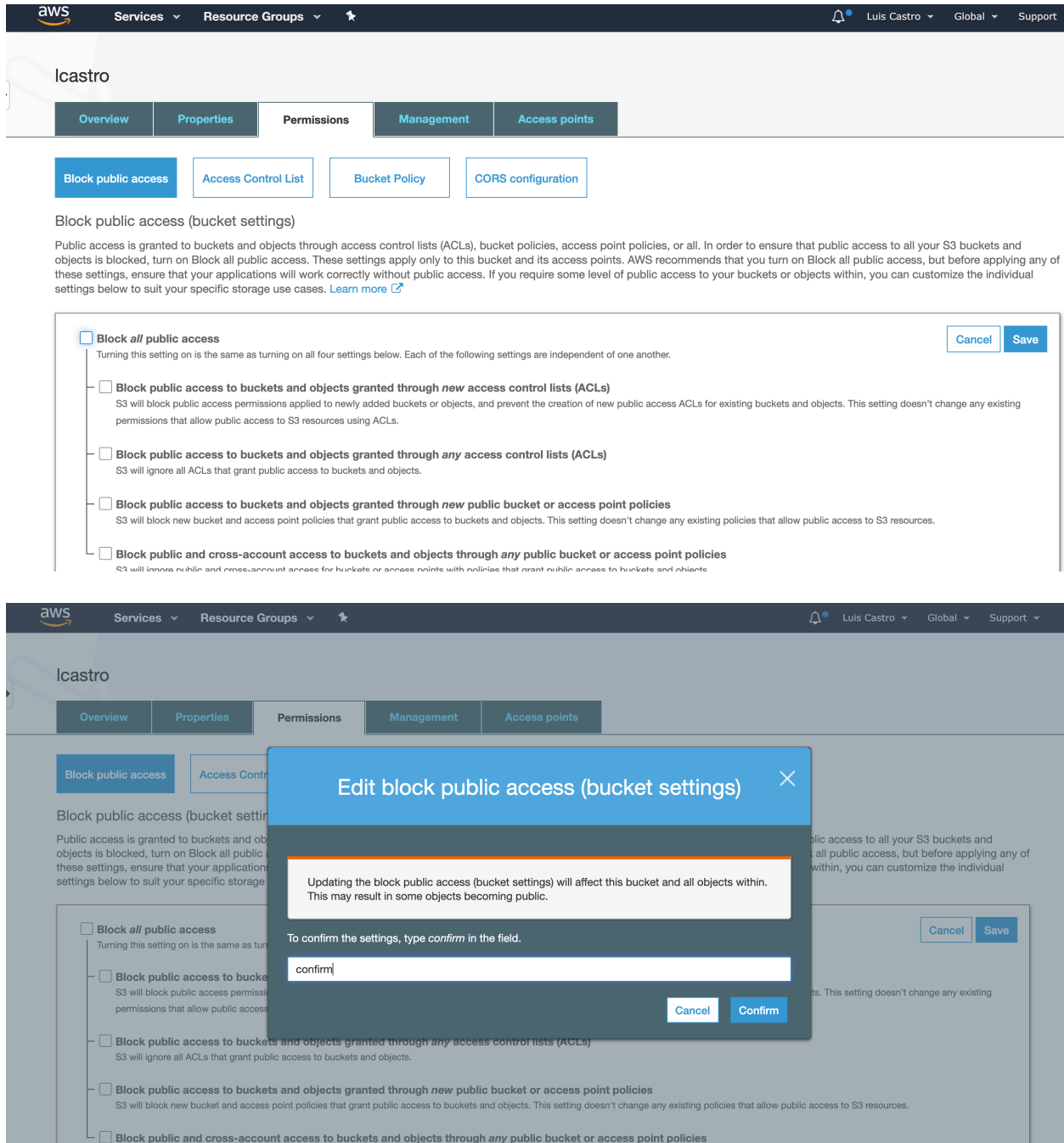
Click on the Object URL and validate the result

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0" encoding="UTF-8" ?>
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>48AC54C167AD02FF</RequestId>
  <HostId>
    FEOrnPKeneF7lGTgymX3B14Wcq7G2A356xovVzG5u8ztqRGBxS2A5Xij0iT6at+2exp925neK+U=
  </HostId>
</Error>
```

## Step 7

Give Public access to the Bucket, for this you must go directly to the Bucket, then click Permissions and click Edit on Block Public Access and deselect Block All public access, and click Save



The screenshot shows the AWS IAM console interface for a bucket named 'lcastro'. The 'Permissions' tab is selected, and the 'Block public access' button is highlighted. The 'Block public access (bucket settings)' section is expanded, showing the following settings:

- ☒ **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.

A modal dialog titled 'Edit block public access (bucket settings)' is open, displaying the following text:

Updating the block public access (bucket settings) will affect this bucket and all objects within. This may result in some objects becoming public.

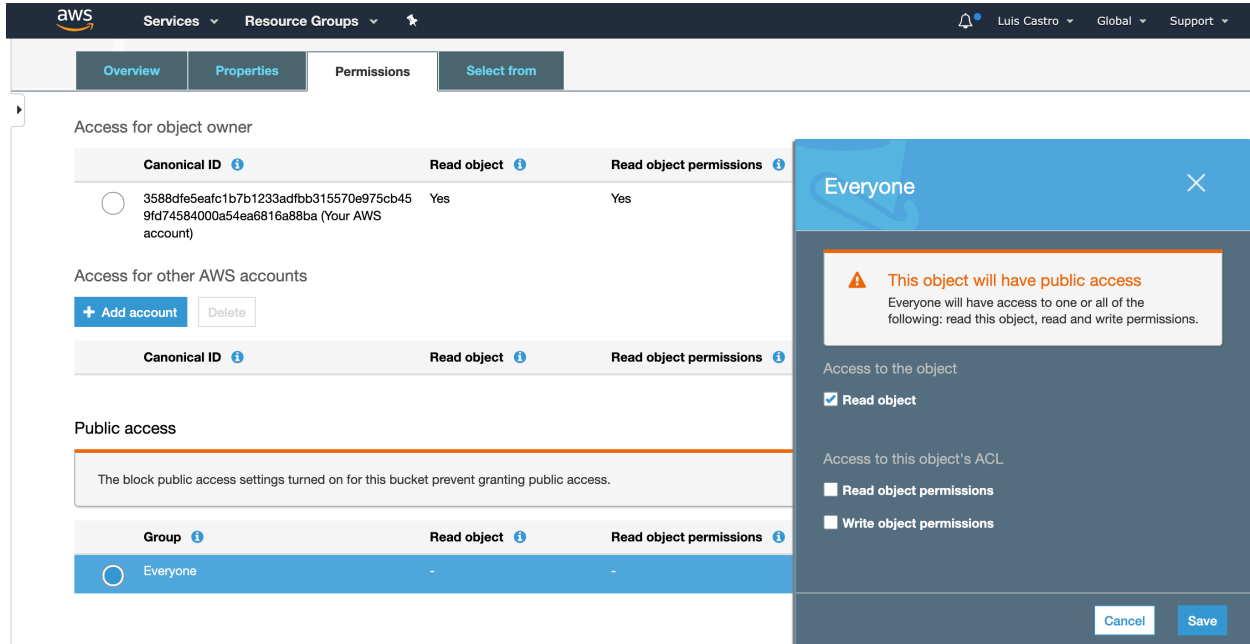
To confirm the settings, type *confirm* in the field.

The text input field contains the word 'confirm'. The dialog has 'Cancel' and 'Confirm' buttons.

Write confirm for the changes to take effect

## Step 8

Go to the created folder and click on Permissions and choose Public Access> Everyone> Access to the Object> Read Object and validate again the access to the link



Validate the URL: <bucket-name>.S3.amazonaws.com/<folder-name>/File Name

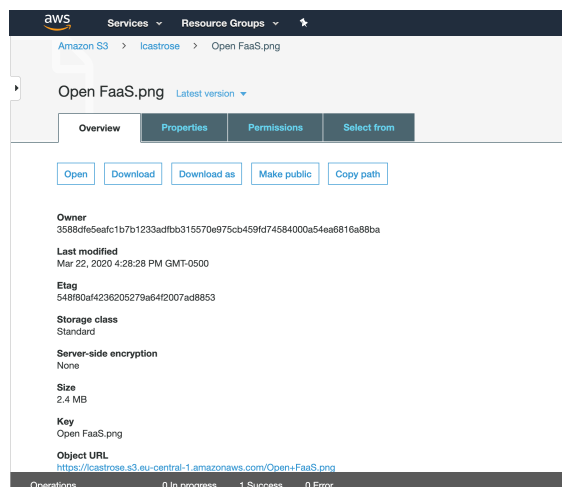
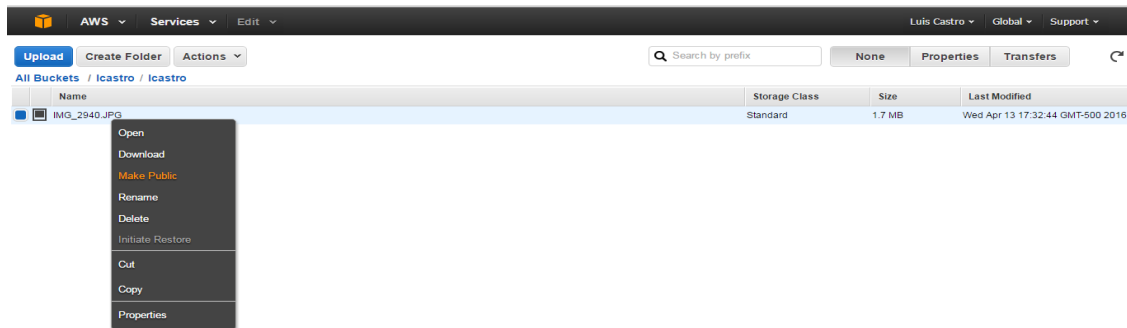
lcastro.s3.amazonaws.com/lcastro/palo-alto-networks-product-summary-specsheet+(7).pdf

Palo Alto Networks Platform Specifications and Features Summary						
Table 1: Firewall Performance and Capacities						
Performance and Capacities	PA-7080	PA-7050	PA-5280	PA-5260	PA-5250	PA-5220
Firewall throughput (App-ID, appmix)	700 Gbps	360 Gbps	56 Gbps	56 Gbps	40 Gbps	30 Gbps
Threat Prevention throughput (appmix)	350 Gbps	198 Gbps	31.5 Gbps	31.5 Gbps	21 Gbps	8.9 Gbps
IPsec VPN throughput	280 Gbps	168 Gbps	27 Gbps	27 Gbps	18 Gbps	10 Gbps
New sessions per second	4,800,000	2,900,000	390,000	390,000	284,000	150,000
Maximum sessions	330,000,000	192,000,000	64,000,000	32,000,000	8,000,000	4,000,000
Virtual systems (base/max)	25/225	25/225	25/225	25/225	25/225	10/30
Hardware Specifications	PA-7080	PA-7050	PA-5280	PA-5260	PA-5250	PA-5220
Interfaces supported NPC option 14	10/100/1000 (up to 120), SFP/ SFP+ (up to 80), QSFP+/QSFP28 (up to 40)	10/100/1000 (up to 72), SFP/ SFP+ (up to 48), QSFP+/QSFP28 (up to 24)	100/1000/10G Cu (4), 10/10G SFP/SFP+ (16), 40G/100G QSFP28 (4)	100/1000/10G Cu (4), 10/10G SFP/SFP+ (16), 40G/100G QSFP28 (4)	100/1000/10G Cu (4), 10/10G SFP/SFP+ (16), 40G/100G QSFP28 (4)	100/1000/10G Cu (4), 10/10G SFP/SFP+ (16), 40G/100G QSFP28 (4)
Management I/O	SFP/SFP+ MG7 (2), SFP/SFP+ HA1 (2), HSC1 HA2/HA3 QSFP+/QSFP28 (2), RJ45 serial console (1), Micro USB serial console (1)	10/100/1000 Cu (2), 10/100/1000 out-of-band management (1), RJ45 console (1)	40G/100G QSFP28 HA (1)	(1) 40G QSFP+ HA		
Size	19U, 19" standard rack	9U, 19" standard rack or 14U, 19" standard rack with optional PAN-AIRDUCT kit	3U, 19" standard rack			
Power supply	2500 W AC (2400 W / 2700 W) (4; expandable to 8)	2500 W AC (2400 W / 2700 W) (4)	1200 W AC or DC (1; fully redundant) (2)			
Redundant power supply	Yes	Yes	Yes			
Disk drives	240 GB SSD system drive, RAID1 (2)		System: 240 GB SSD, RAID1   Log: 2 TB HDD, RAID1			
Hot-swappable fans	Yes	Yes	Yes			
Performance and Capacities	PA-3260	PA-3250	PA-3220			
Firewall throughput (App-ID, appmix)	10 Gbps	6.6 Gbps	5 Gbps			
Threat Prevention throughput (appmix)	4.4 Gbps	3 Gbps	2.4 Gbps			
IPsec VPN throughput	4.8 Gbps	3.2 Gbps	2.7 Gbps			
New sessions per second	118,000	84,000	57,000			
Maximum sessions	3,000,000	2,000,000	1,000,000			

## Step 11

### Access the CloudFront service

Create a new Bucket in the Frankfurt region with the username followed by the name of the region (all pasted and in lowercase) and upload the photo sent by mail (Palo Alto Networks Platform Architecture.jpg), modify the permissions, make it Public and enter the image link and copy the link



### Example:

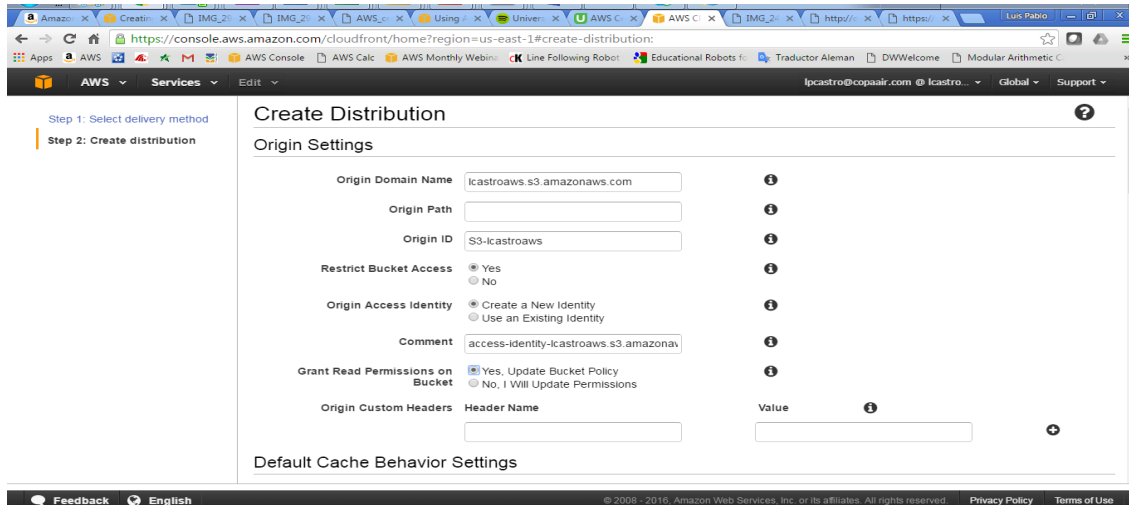
<https://lcastrose.s3.eu-central-1.amazonaws.com/Palo+Alto+Networks+Platform+Architecture.jpg>

## Step 12

Enter CloudFront and click Create Distribution, choose Web Content.

As Origin Domain Name look for the Bucket name you created earlier

Choose Restrict Bucket Access option, Create New Identity and Yes, Update Bucket Policy, leave all other parameters as default



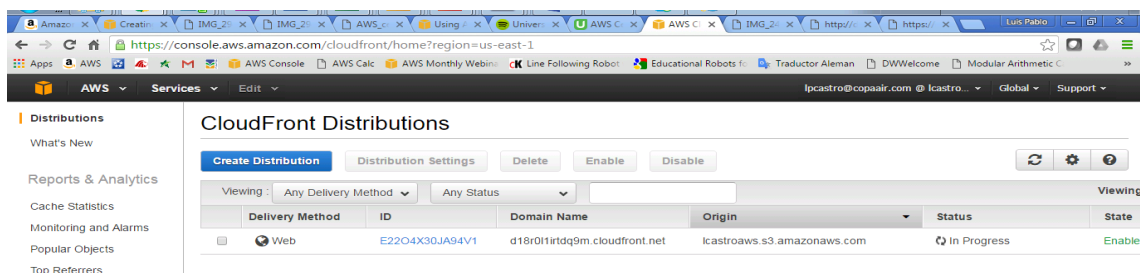
## Step 13

The distribution creation process can take approximately 15 minutes

Once created use the assigned domain name: d18r0l1irtdq9m.cloudfront.net

Replace it in the URL as follows and open the page again

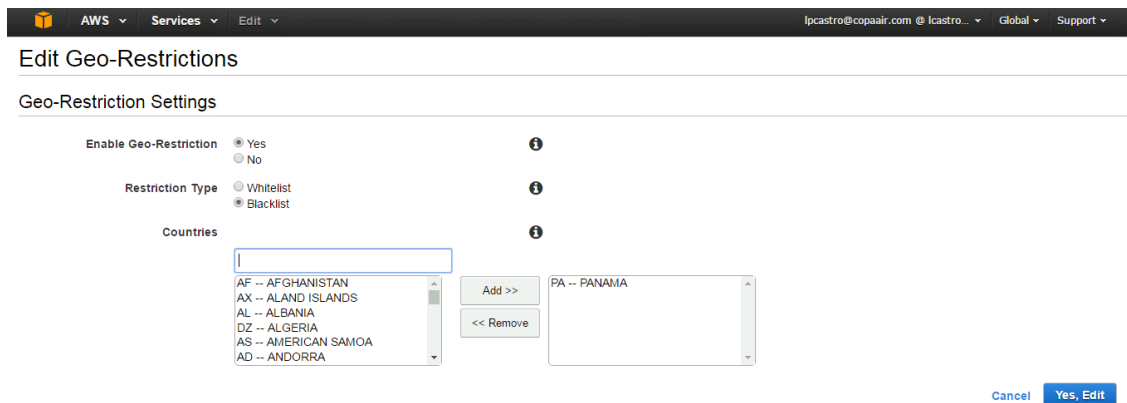
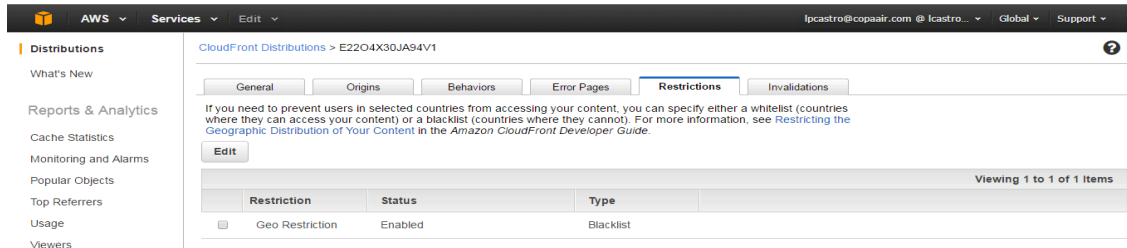
[https:// d18r0l1irtdq9m.cloudfront.net/Palo Alto Networks Platform Architecture.jpg](https://d18r0l1irtdq9m.cloudfront.net/Palo%20Alto%20Networks%20Platform%20Architecture.jpg)



Delivery Method	ID	Domain Name	Origin	Status	State
Web	E22O4X30JA94V1	d18r0l1irtdq9m.cloudfront.net	lcastroaws.s3.amazonaws.com	In Progress	Enable

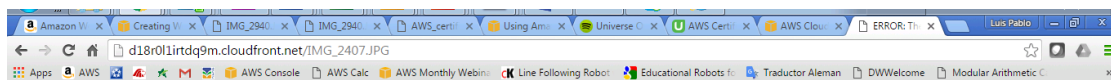
## Step 14

Modify the distribution to restrict access by Geo-Location and activate the Restriction Type - Blacklist and add your Country (Ex: Colombia) and check Yes, Edit



## Step 15

Validate after distribution is complete that access is restricted



### ERROR

The request could not be satisfied.

The Amazon CloudFront distribution is configured to block access from your country.

Generated by CloudFront (CloudFront)  
Request ID: K1CEa\_1eKa5hdhZvQ1hw7V20hdKGTbe77PHIdPCFu4vfy1hYT3-Dw==