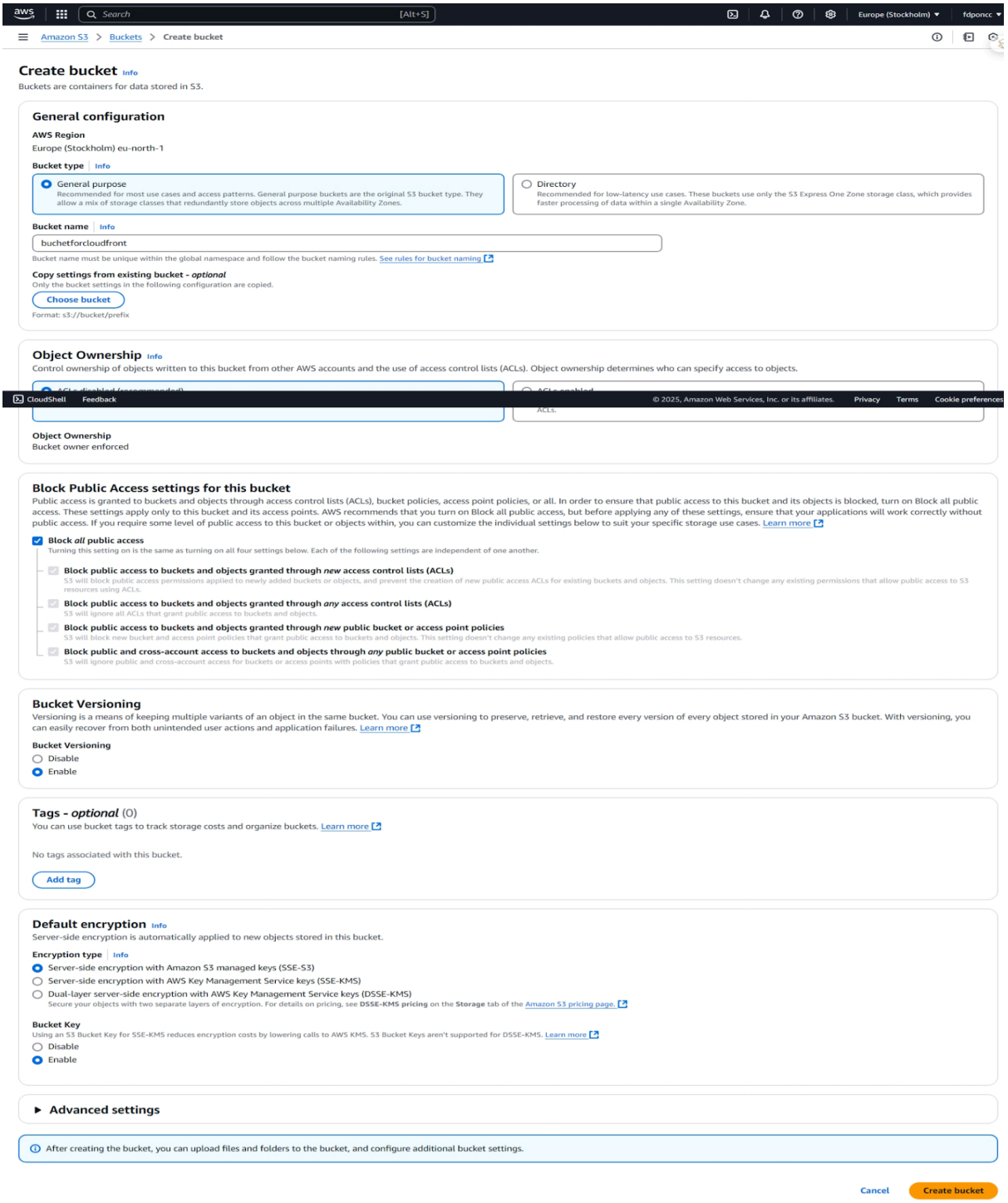
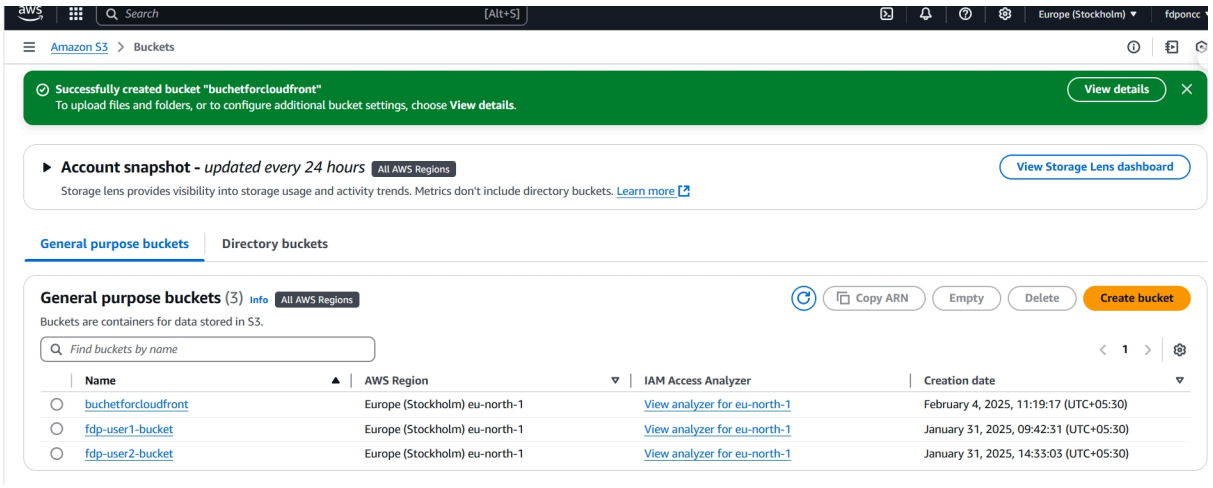
AWS CLOUDFRONT

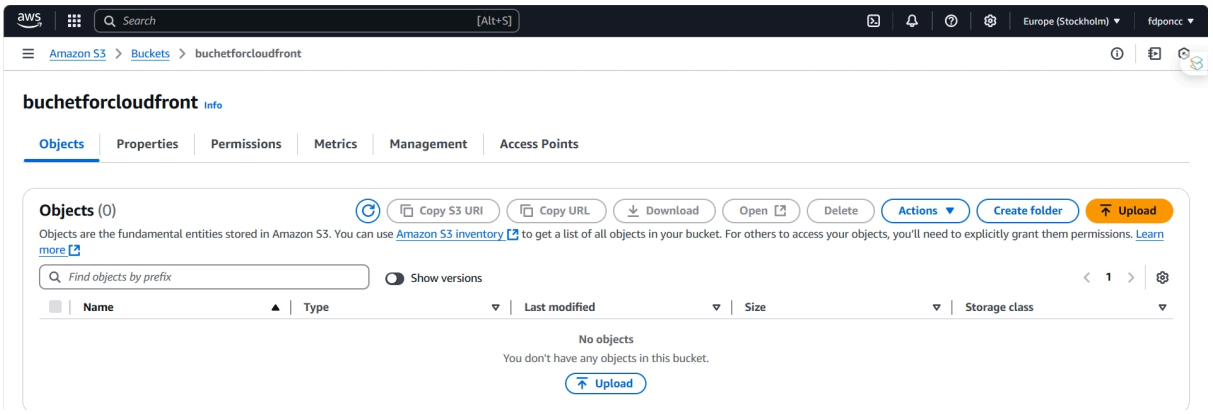
GO TO S3 & CREATE A BUCKET

GIVE BUCKET NAME AND KEEP ALL DEFAULTS

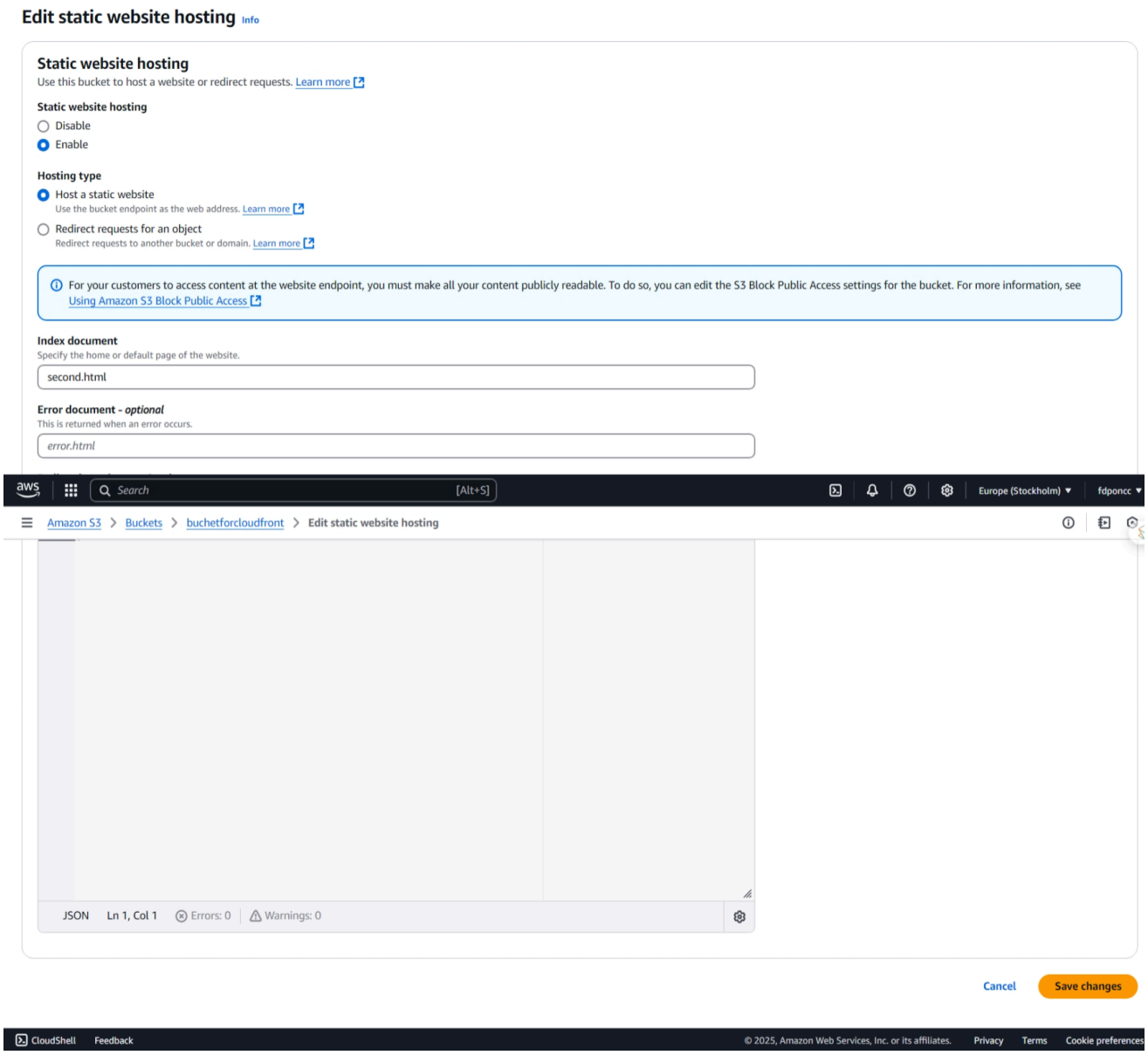




GO TO BUCKET CREATED

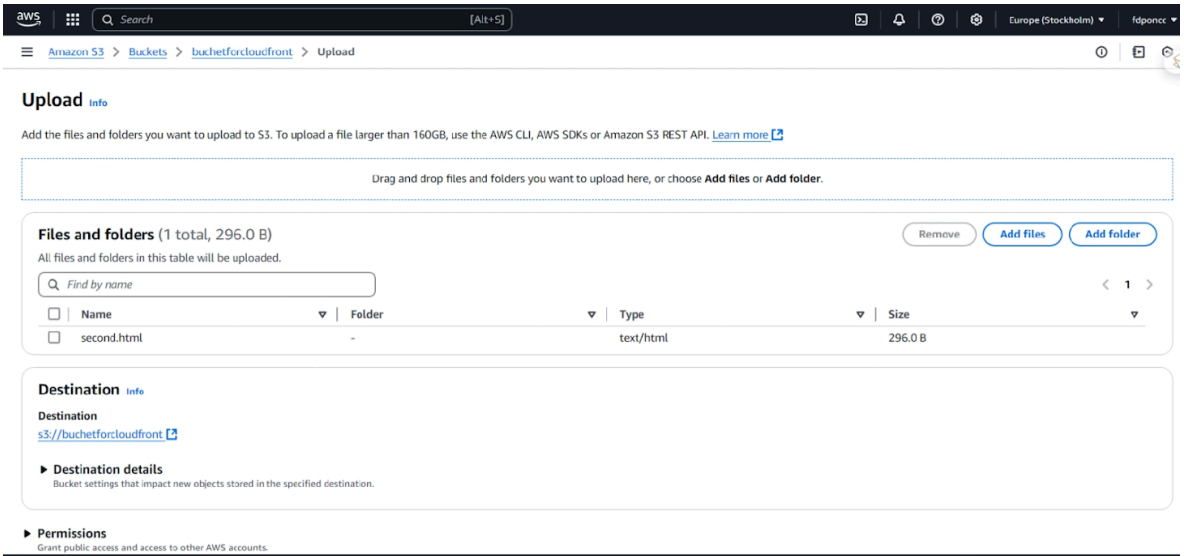


GO TO PROPERTIES AND HOST STATIC WEBSITE



SAVE CHANGES

GO TO OBJECT AND UPLOAD A FILE (HTML)



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, 296.0 B)

Remove | Add files | Add folder

All files and folders in this table will be uploaded.

Find by name

1

Name	Folder	Type	Size
second.html	-	text/html	296.0 B

Destination Info

Destination

s3://buchetforcloudfront

▶ **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.

Storage class Info

Amazon S3 offers a range of storage classes designed for different use cases. Learn more or see Amazon S3 pricing

	Storage class	Designed for	Bucket type	Availability Zones	Min storage duration	Min billable object size	Monitoring and auto-tiering fees	Retrieval fees
◉	Standard	Frequently accessed data (more than once a month) with milliseconds access	General purpose	≥ 3	-	-	-	-
○	Intelligent-Tiering	Data with changing or unknown access patterns	General purpose	≥ 3	-	-	Per-object fees apply for objects >= 128 KB	-
○	Standard-IA	Infrequently accessed data (once a month) with milliseconds access	General purpose	≥ 3	30 days	128 KB	-	Per-GB fees apply
○	One Zone-IA	Recreatable, infrequently accessed data (once a month) with milliseconds access	General purpose or directory	1	30 days	128 KB	-	Per-GB fees apply
○	Glacier Instant Retrieval	Long-lived archive data accessed once a quarter with instant retrieval in milliseconds	General purpose	≥ 3	90 days	128 KB	-	Per-GB fees apply
○	Glacier Flexible Retrieval (formerly Glacier)	Long-lived archive data accessed once a year with retrieval of minutes to hours	General purpose	≥ 3	90 days	-	-	Per-GB fees apply
○	Glacier Deep Archive	Long-lived archive data accessed less than once a year with retrieval of hours	General purpose	≥ 3	180 days	-	-	Per-GB fees apply
○	Reduced redundancy	Noncritical, frequently accessed data with milliseconds access (not recommended as S3 Standard is more cost effective)	General purpose	≥ 3	-	-	-	Per-GB fees apply

Server-side encryption Info

Server-side encryption protects data at rest.

Server-side encryption

◉ Don't specify an encryption key
The bucket settings for default encryption are used to encrypt objects when storing them in Amazon S3.

○ Specify an encryption key
The specified encryption key is used to encrypt objects before storing them in Amazon S3.

⚠ If your bucket policy requires objects to be encrypted with a specific encryption key, you must specify the same encryption key when you upload objects. Otherwise, uploads will fail.

Checksums

Checksums are used for data integrity verification of new objects. Learn more

Checksum function

Checksum functions are used to calculate the checksum value. For objects smaller than 16 MB, only the full object checksum type is supported, for all checksum algorithms.

CRC64NVME (recommended)

Precalculated value - *optional*

When you provide a precalculated value for a single object, S3 compares it to the value it calculates using the selected checksum function. If the values don't match, the upload will fail. Learn more

Enter value

The precalculated value must be a Base64 encoded string. It must not exceed 128 characters, and can contain only letters (a-z, A-Z), numbers (0-9), forward slash (/), plus (+), or equals (=).

Tags - *optional*

You can use object tags to analyze, manage, and specify permissions for objects. Learn more

No tags associated with this resource.

Add tag

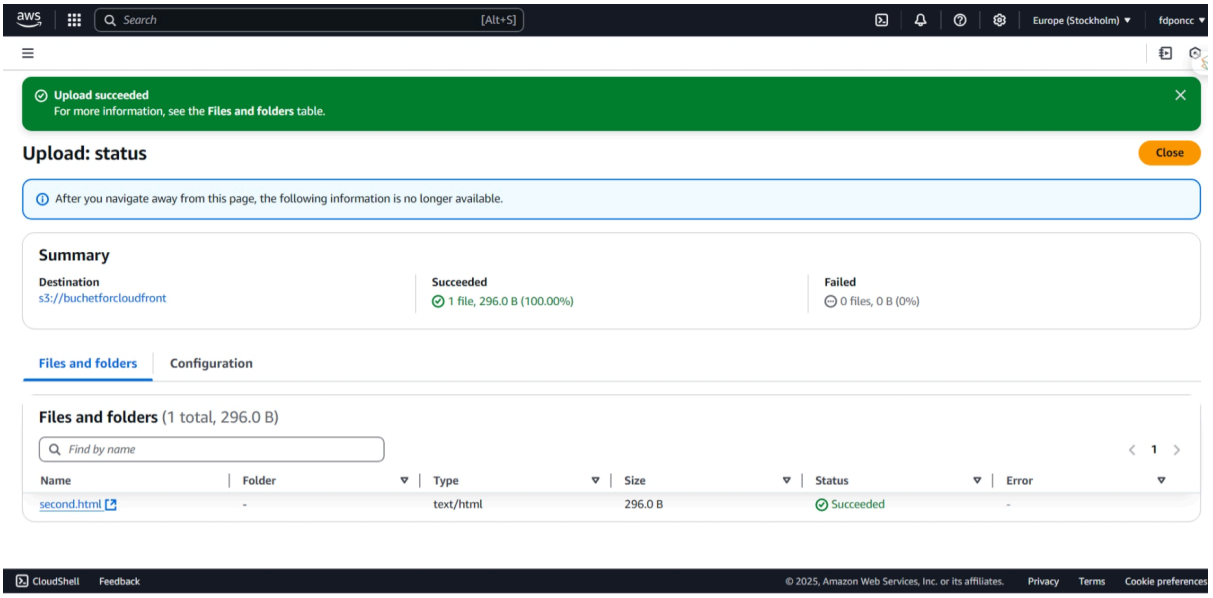
Metadata - *optional*

Metadata is optional information provided as a name-value (key-value) pair. Learn more

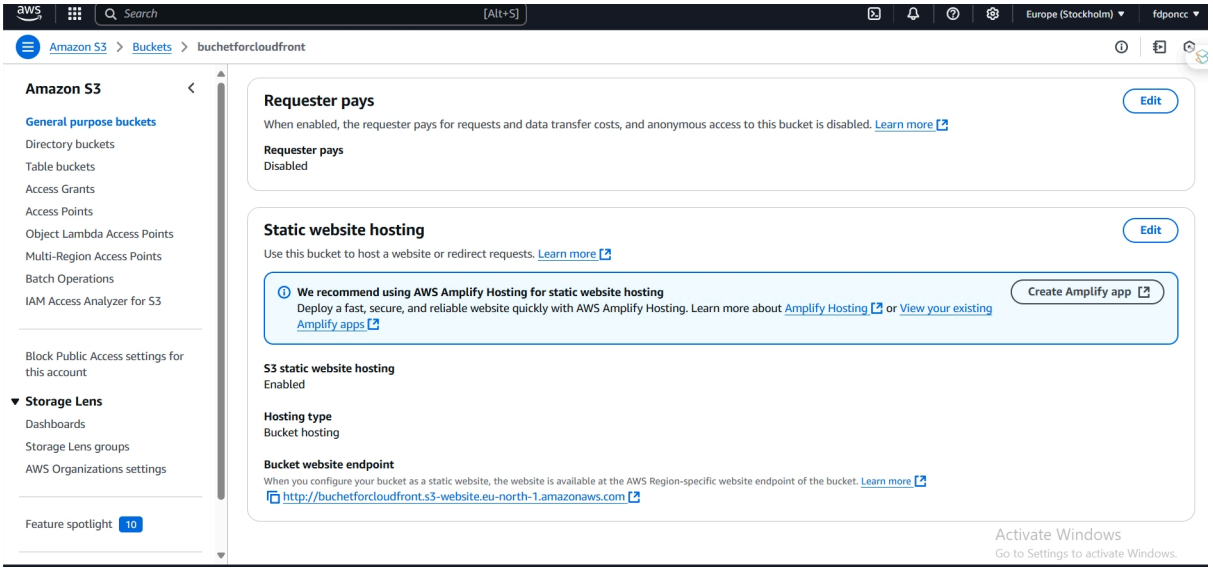
No metadata associated with this resource.

Add metadata

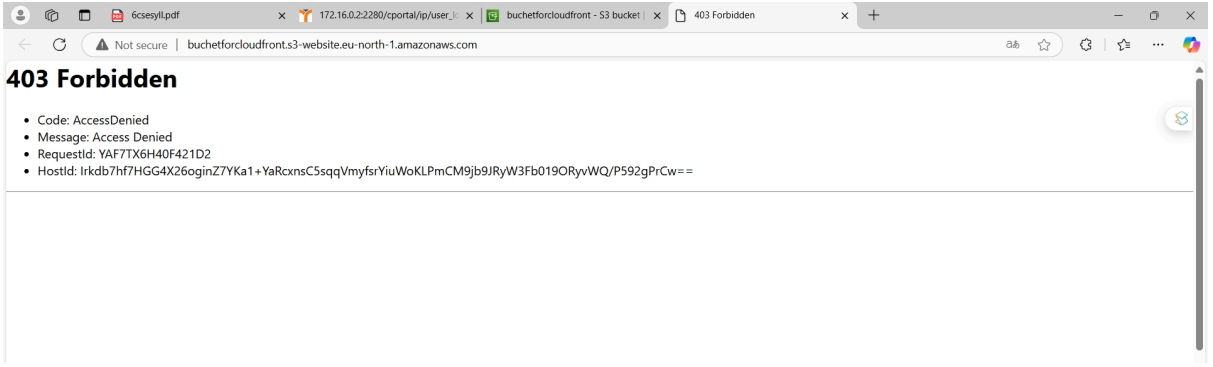
Cancel | Upload



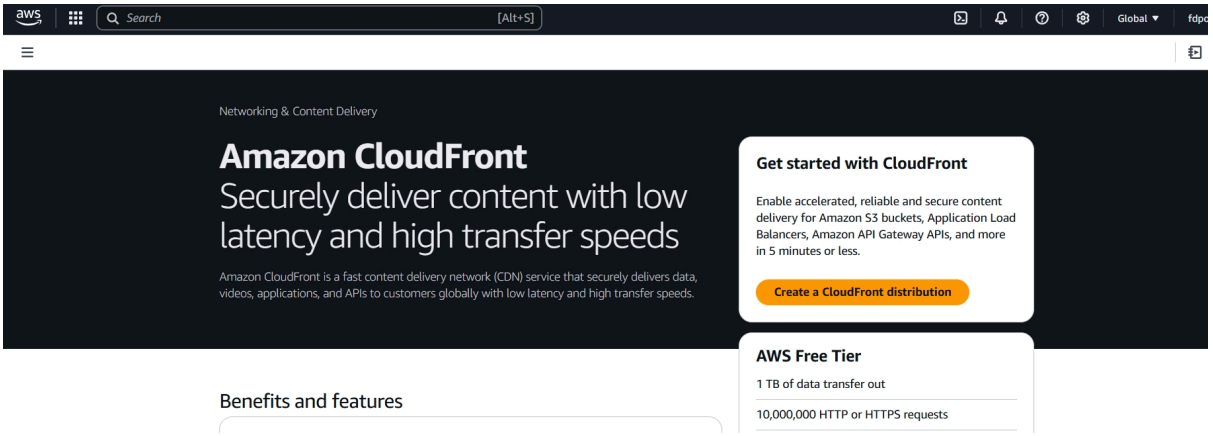
ACCESS URL FROM UR BUCKET -□ PROPERTIES-> STATIC WEB HOSTING □ SITE ADDRESS



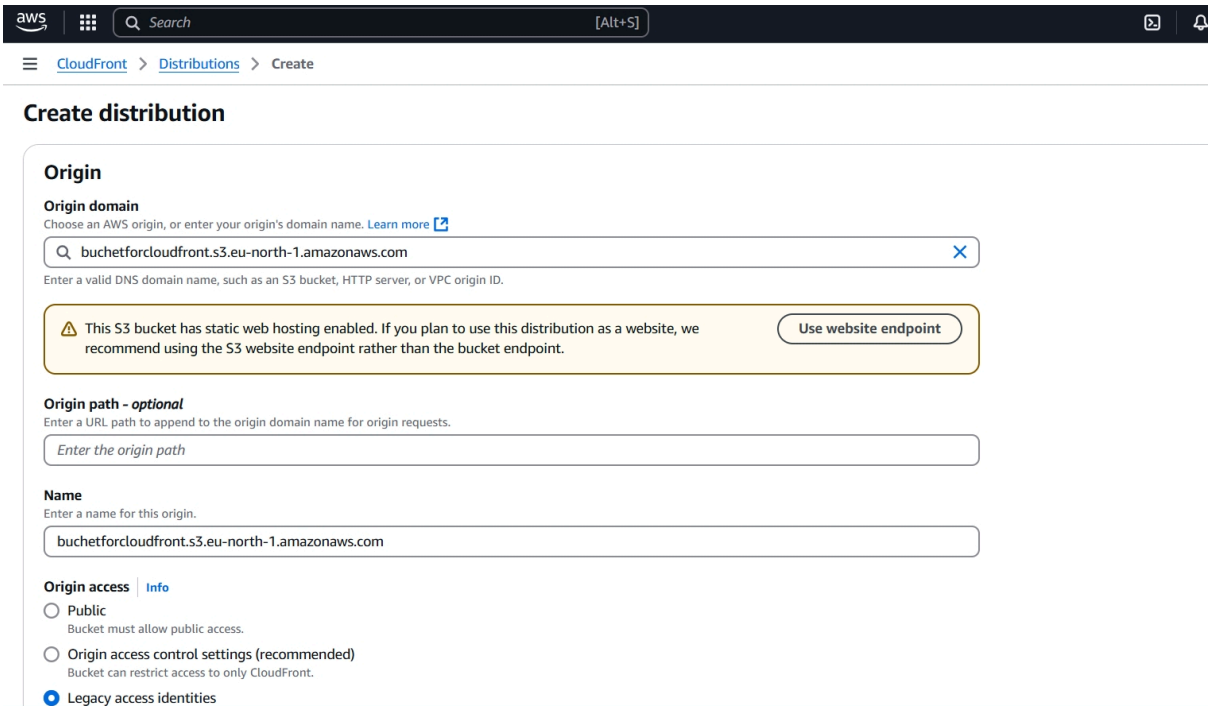
IF YOU TRY TO ACCESS THE URL



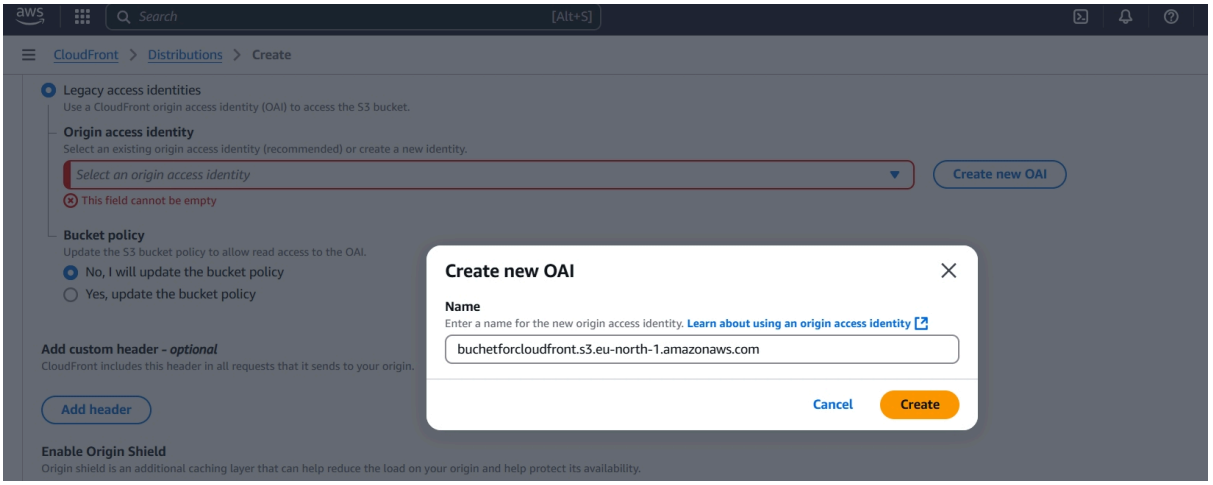
STEP 2: CLOUDFRONT

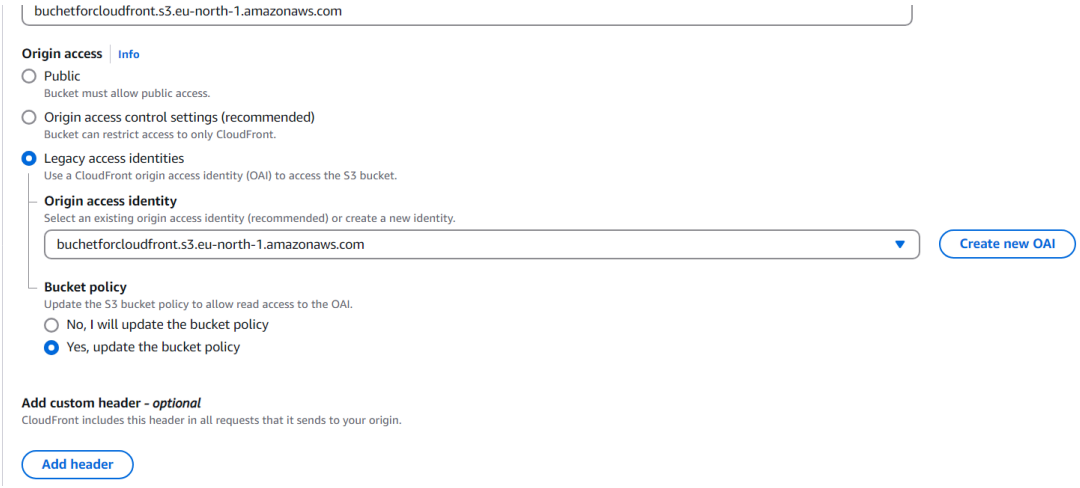


CREATE A DISTRIBUTION

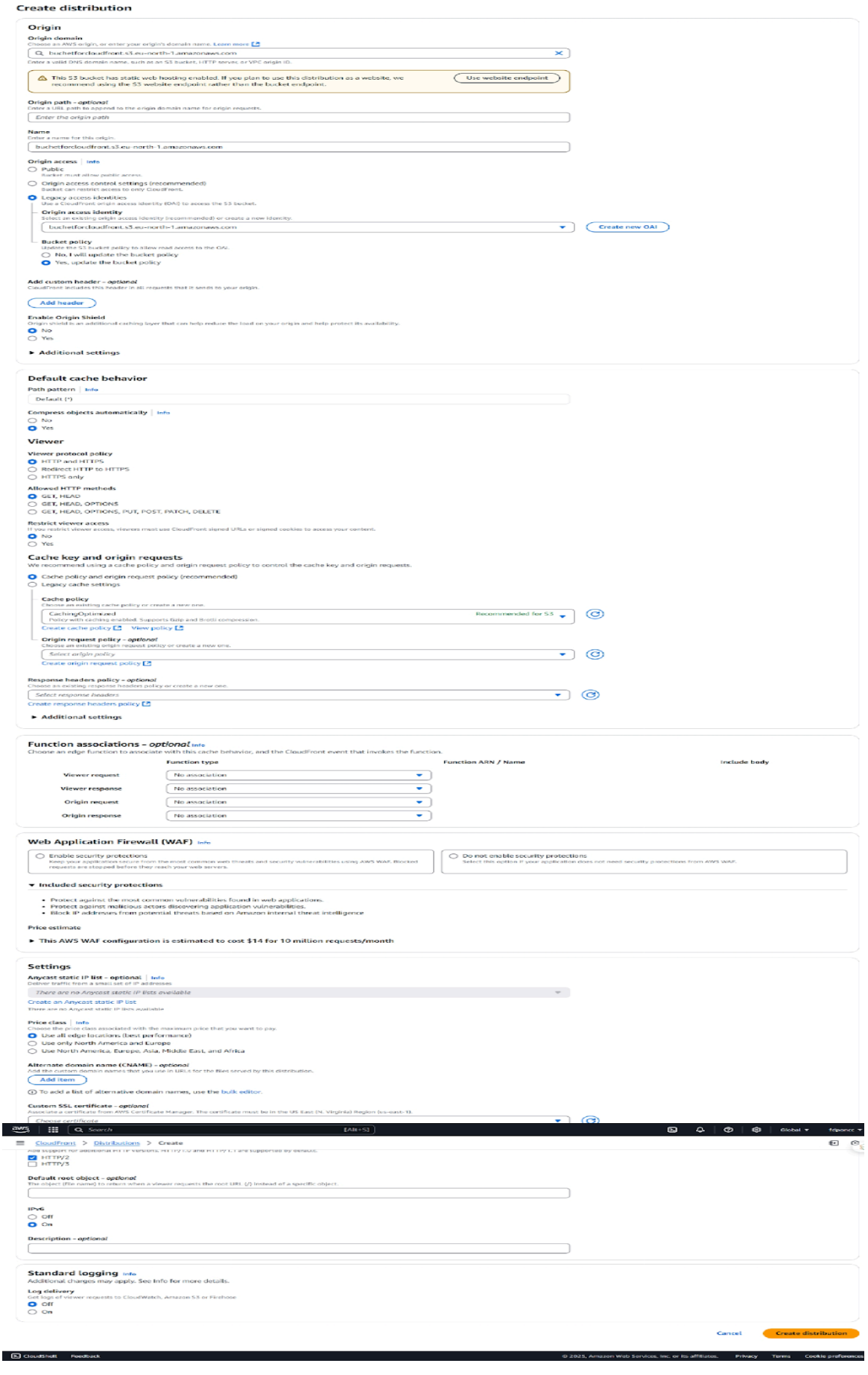


CREATE A NEW OAI





KEEP ALL SETTINGS DEFAULT


Create distribution
Origin
Origin domain
Choose an AWS origin, or enter your origin's domain name. Learn more
bucketforcloudfront.s3.eu-north-1.amazonaws.com
Enter a valid DNS domain name, such as an S3 bucket, HTTP server, or VPC origin ID.
This S3 bucket has static web hosting enabled. If you plan to use this distribution as a website, we recommend using the S3 website endpoint rather than the bucket endpoint.
Use website endpoint
Origin path - optional
Enter a URL path to append to the origin domain name for origin requests.
Enter the origin path
Name
Enter a name for this origin.
bucketforcloudfront.s3.eu-north-1.amazonaws.com
Origin access | Info
Public
Bucket must allow public access.
Origin access control settings (recommended)
Bucket can restrict access to only CloudFront.
Legacy access identities
Use a CloudFront origin access identity (OAI) to access the S3 bucket.
Origin access identity
Select an existing origin access identity (recommended) or create a new identity.
bucketforcloudfront.s3.eu-north-1.amazonaws.com
Create new OAI
Bucket policy
Update the S3 bucket policy to allow read access to the OAI.
No, I will update the bucket policy
Yes, update the bucket policy
Add custom header - optional
CloudFront includes this header in all requests that it sends to your origin.
Add header
Enable Origin Shield
Origin shield is an additional caching layer that can help reduce the load on your origin and help protect its availability.
No
Yes
Additional settings
Default cache behavior
Path pattern | Info
Default (*)
Compress objects automatically | Info
No
Yes
Viewer
Viewer protocol policy
HTTP and HTTPS
Redirect HTTP to HTTPS
HTTPS only
Allowed HTTP methods
GET, HEAD
GET, HEAD, OPTIONS
GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE
Restrict viewer access
If you restrict viewer access, viewers must use CloudFront signed URLs or signed cookies to access your content.
No
Yes
Cache key and origin requests
We recommend using a cache policy and origin request policy to control the cache key and origin requests.
Cache policy and origin request policy (recommended)
Legacy cache settings
Cache policy
Choose an existing cache policy or create a new one.
CachingOptimized
Policy with caching enabled. Supports Gzip and Brotli compression.
Recommended for S3
Create cache policy
View policy
Origin request policy - optional
Choose an existing origin request policy or create a new one.
Select origin policy
Create origin request policy
Response headers policy - optional
Choose an existing response headers policy or create a new one.
Select response headers
Create response headers policy
Additional settings
Function associations - optional Info
Choose an edge function to associate with this cache behavior, and the CloudFront event that invokes the function.
Function type
Function ARN / Name
Include body
Viewer request
No association
Viewer response
No association
Origin request
No association
Origin response
No association
Web Application Firewall (WAF) Info
Enable security protections
Keep your application secure from the most common web threats and security vulnerabilities using AWS WAF. Blocked requests are stopped before they reach your web servers.
Do not enable security protections
Select this option if your application does not need security protections from AWS WAF.
Included security protections
Protect against the most common vulnerabilities found in web applications.
Protect against malicious actors discovering application vulnerabilities.
Block IP addresses from potential threats based on Amazon internal threat intelligence
Price estimate
This AWS WAF configuration is estimated to cost $14 for 10 million requests/month
Settings
Anycast static IP list - optional | Info
Deliver traffic from a small set of IP addresses
There are no Anycast static IP lists available
Create an Anycast static IP list
There are no Anycast static IP lists available
Price class | Info
Choose the price class associated with the maximum price that you want to pay.
Use all edge locations (best performance)
Use only North America and Europe
Use North America, Europe, Asia, Middle East, and Africa
Alternate domain name (CNAME) - optional
Add the custom domain names that you use in URLs for the files served by this distribution.
Add item
To add a list of alternative domain names, use the bulk editor.
Custom SSL certificate - optional
Associate a certificate from AWS Certificate Manager. The certificate must be in the US East (N. Virginia) Region (us-east-1).
Choose certificate
Search
[Alt+S]
Global
frigorcc
CloudFront > Distributions > Create
HTTP/2
HTTP/3
Default root object - optional
The object (file name) to return when a viewer requests the root URL (/) instead of a specific object.
IPv6
Off
On
Description - optional
Standard logging Info
Additional charges may apply. See Info for more details.
Log delivery
Get logs of viewer requests to CloudWatch, Amazon S3 or Firehose.
Off
On
Cancel
Create distribution
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Default root object - *optional*
The object (file name) to return when a viewer requests the root URL (/) instead of a specific object.

/second.html

IPv6

- Off
- On

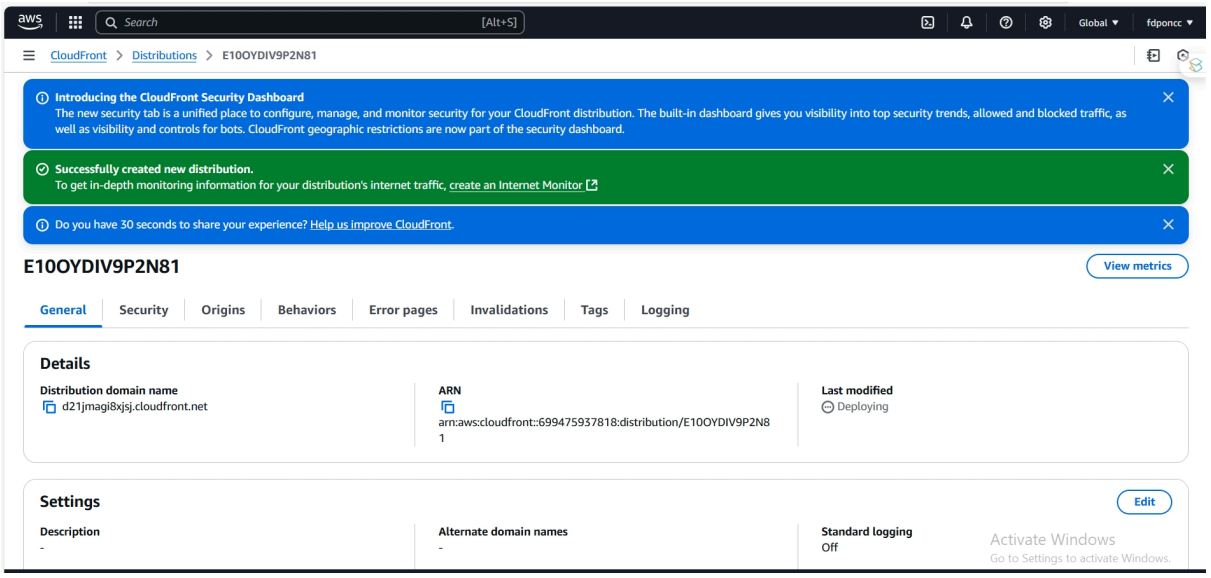
Description - *optional*

Standard logging Info
Additional charges may apply. See Info for more details.

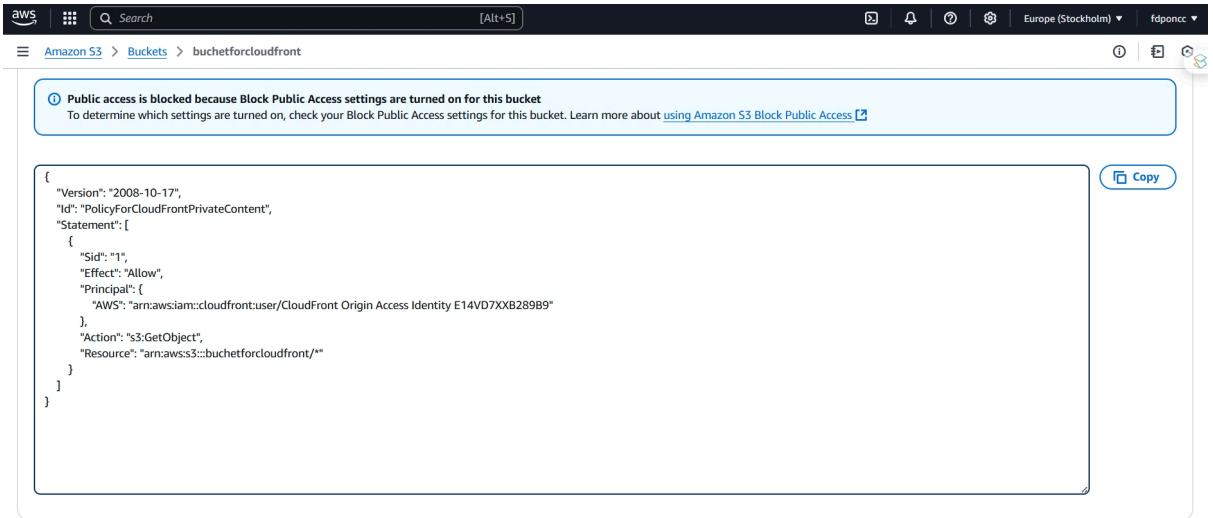
Log delivery
Get logs of viewer requests to CloudWatch, Amazon S3 or Firehose

- Off
- On

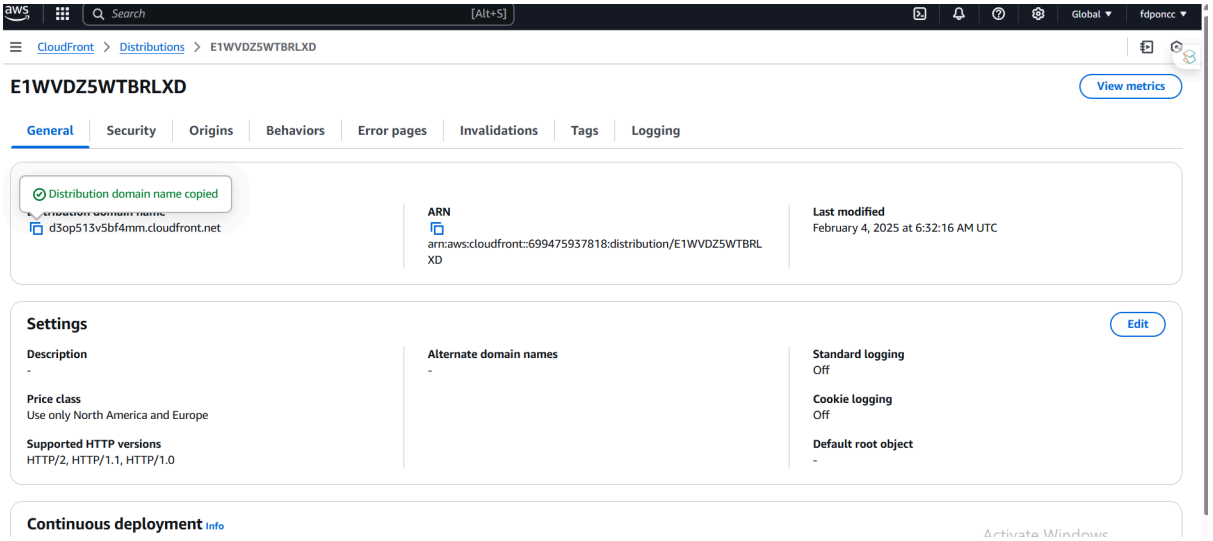
Cancel | Create distribution



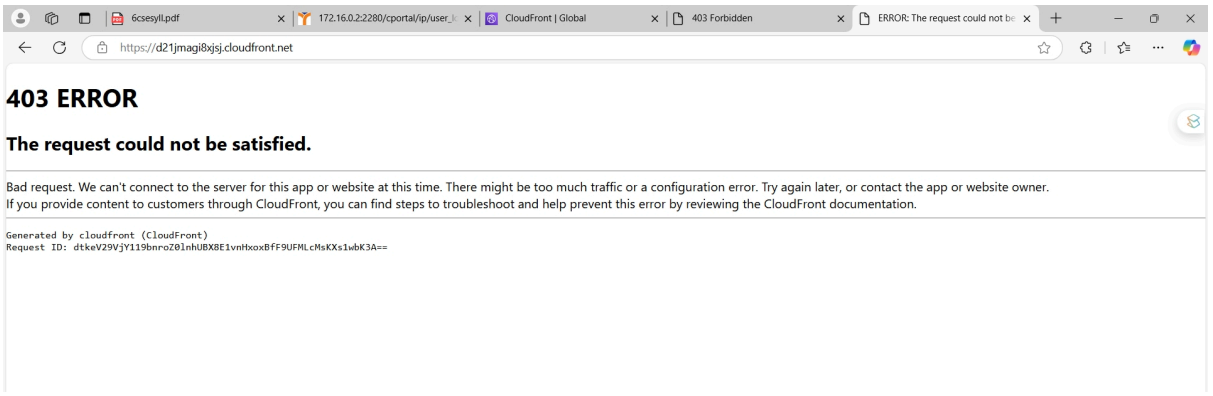
POLICY BEEN CREATED IN S3 BUCKET



GO TO THE LINK (DISTRIBUTION DOMAIN NAME)



S3 RESULT



CLOUD FRONT RESULT