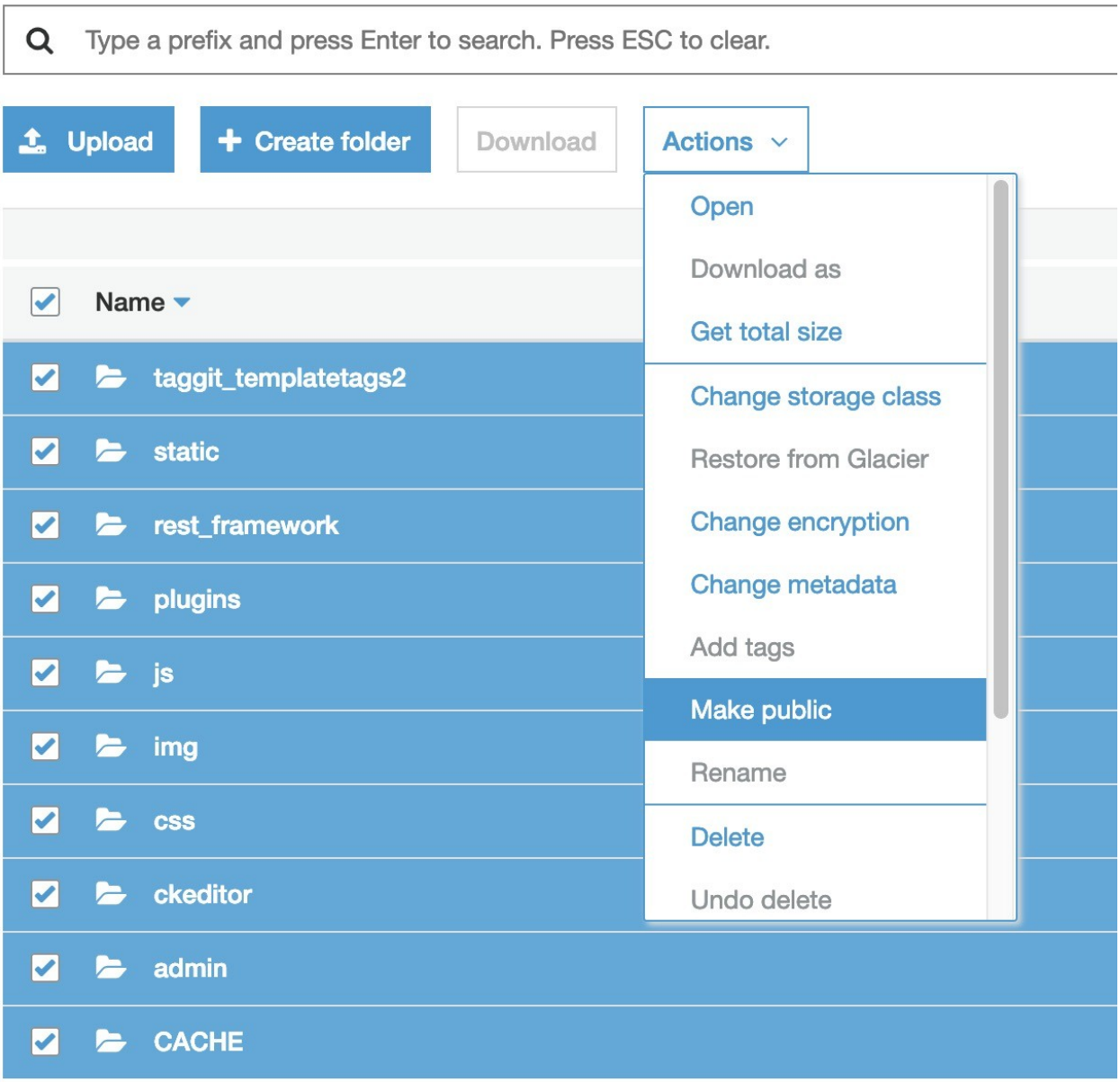
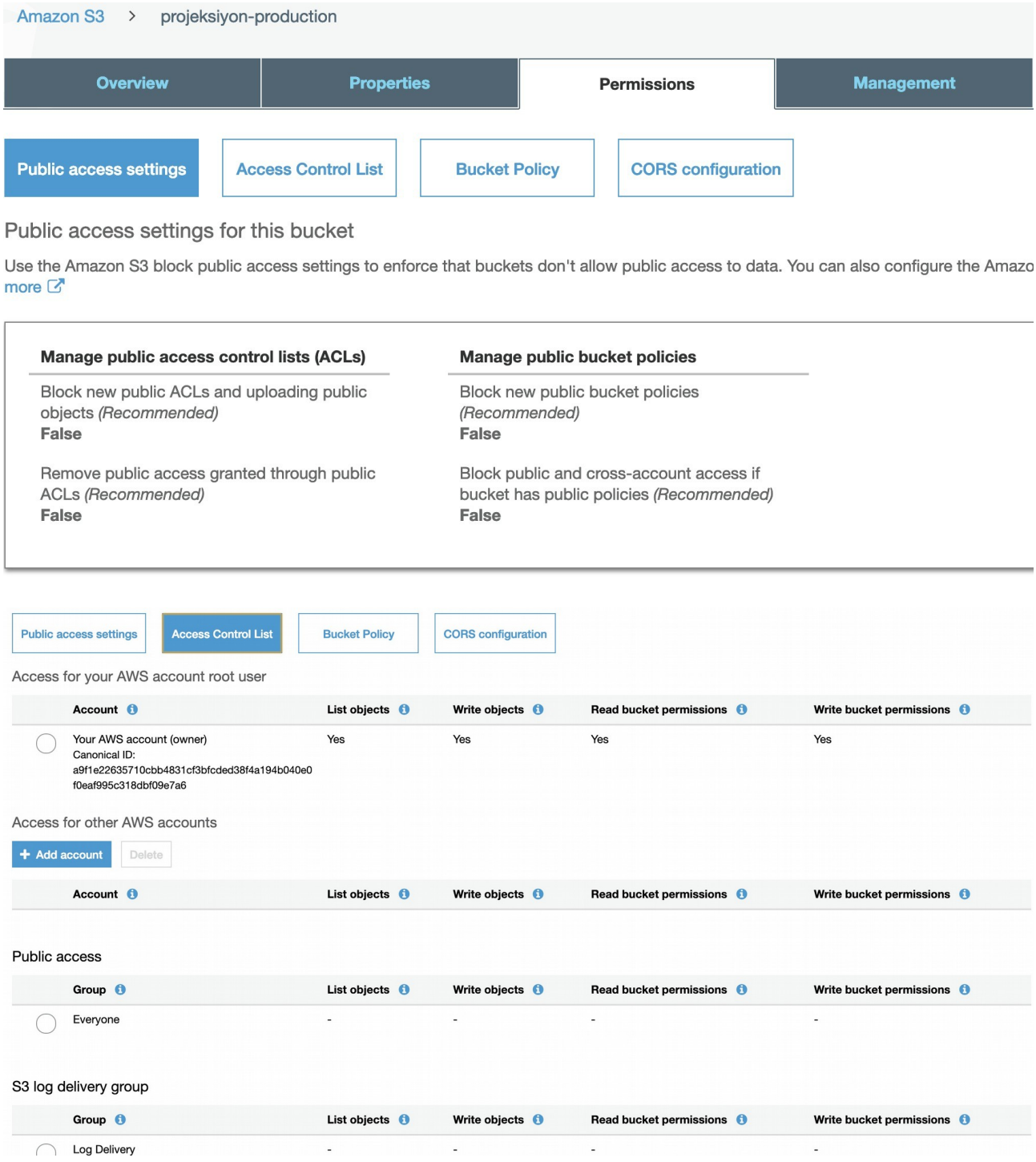
Önemli !!! Aşağıdaki şekilde public etmezsen cloudfront çalışmıyor:




Amazon S3 > projeksiyon-production
Overview
Properties
Permissions
Management
Public access settings
Access Control List
Bucket Policy
CORS configuration
Public access settings for this bucket
Use the Amazon S3 block public access settings to enforce that buckets don't allow public access to data. You can also configure the Amazo
more
Manage public access control lists (ACLs)
Block new public ACLs and uploading public objects (Recommended)
False
Remove public access granted through public ACLs (Recommended)
False
Manage public bucket policies
Block new public bucket policies (Recommended)
False
Block public and cross-account access if bucket has public policies (Recommended)
False
Public access settings
Access Control List
Bucket Policy
CORS configuration
Access for your AWS account root user
Account
List objects
Write objects
Read bucket permissions
Write bucket permissions
Your AWS account (owner)
Canonical ID:
a9f1e22635710cbb4831cf3bfcded38f4a194b040e0f0eaf995c318dbf09e7a6
Yes
Yes
Yes
Yes
Access for other AWS accounts
+ Add account
Delete
Account
List objects
Write objects
Read bucket permissions
Write bucket permissions
Public access
Group
List objects
Write objects
Read bucket permissions
Write bucket permissions
Everyone
-
-
-
-
S3 log delivery group
Group
List objects
Write objects
Read bucket permissions
Write bucket permissions
Log Delivery
-
-
-
-

Public access settings | Access Control List | Bucket Policy | CORS configuration

Bucket policy editor ARN: arn:aws:s3:::projeksiyon-production

Type to add a new policy or edit an existing policy in the text area below.

```
1
```

Public access settings | Access Control List | Bucket Policy | CORS configuration

CORS configuration editor ARN: arn:aws:s3:::projeksiyon-production

Add a new cors configuration or edit an existing one in the text area below.

```
1  <?xml version="1.0" encoding="UTF-8"?>
2  <CORSConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
3  <CORSRule>
4      <AllowedOrigin>*</AllowedOrigin>
5      <AllowedMethod>GET</AllowedMethod>
6      <MaxAgeSeconds>3000</MaxAgeSeconds>
7      <AllowedHeader>*</AllowedHeader>
8  </CORSRule>
9  </CORSConfiguration>
10
11
```

CloudFront Distributions > E2LOW8U51T7N9K

General | Origins and Origin Groups | Behaviors | Error Pages | Restrictions | Invalidations | Tags

Edit

Distribution ID	E2LOW8U51T7N9K
ARN	arn:aws:cloudfront::405026139771:distribution/E2LOW8U51T7N9K
Log Prefix	-
Delivery Method	Web
Cookie Logging	Off
Distribution Status	Deployed
Comment	-
Price Class	Use All Edge Locations (Best Performance)
AWS WAF Web ACL	-
State	Enabled
Alternate Domain Names (CNAMEs)	cdn.projeksiyon.com
SSL Certificate	Default CloudFront Certificate (*.cloudfront.net)
Domain Name	d1a9w4ni6rsc6h.cloudfront.net
Custom SSL Client Support	-
Security Policy	TLSv1
Supported HTTP Versions	HTTP/2, HTTP/1.1, HTTP/1.0
IPv6	Enabled
Default Root Object	-
Last Modified	2019-02-17 14:31 UTC+3
Log Bucket	-

Aşğaıdakinin devamı da bomboş...

CloudFront Distributions > E2LOW8U51T7N9K

General | Origins and Origin Groups | Behaviors | Error Pages | Restrictions | Invalidations | Tags

Origins

Create Origin | Edit | Delete

Origin Domain Name and Path	Origin ID	Origin Type	Origin Access Identity	Origin Protocol Policy	HTTPS Port	HTTP P
projeksiyon-production.s3.amazonaws.com	S3-projeksiyon-producti	S3 Origin	-	-	-	-

Edit Origin

Origin Settings

Origin Domain Name	projeksiyon-production.s3.amazonaws.c	
Origin Path		
Origin ID	S3-projeksiyon-production	
Restrict Bucket Access	○ Yes ◉ No	
Origin Custom Headers	**Header Name**	**Value**
	Access-Control-Allow-Origin	https://projeksiyon.com

General | Origins and Origin Groups | **Behaviors** | Error Pages | Restrictions | Invalidations | Tags

CloudFront compares a request for an object with the path patterns in your cache behaviors based on the order of the cache behaviors in your distribution. Arrange cache behaviors in the order in which you want CloudFront to evaluate them.

Create Behavior | Edit | Delete | Change Precedence: | Move Up | Move Down | Save

	Precedence	Path Pattern	Origin or Origin Group	Viewer Protocol Policy	Forwarded Query Str
☐	0	Default (*)	S3-projeksiyon-production	Redirect HTTP to HTTPS	No

CloudFront Distributions > E2LOW8U51T7N9K

General | Origins and Origin Groups | Behaviors | **Error Pages** | Restrictions | Invalidations | Tags

You can configure CloudFront to respond to requests using a custom error page when your origin returns an HTTP 4xx or 5xx status code. For example, when your custom origin is unavailable and returning 5xx responses, CloudFront can return a static error page that is hosted on Amazon S3. You can also specify a minimum TTL to control how long CloudFront caches errors. For more information, see Customizing Error Responses in the *Amazon CloudFront Developer Guide*.

Create Custom Error Response | Edit | Delete

	HTTP Error Code	Error Caching Minimum TTL	Response Page Path	HTTP Response Code
			No Data	

CloudFront Distributions > E2LOW8U51T7N9K

General | Origins and Origin Groups | Behaviors | Error Pages | **Restrictions** | Invalidations | Tags

If you need to prevent users in selected countries from accessing your content, you can specify either a whitelist (countries where they can access your content) or a blacklist (countries where they cannot). For more information, see Restricting the Geographic Distribution of Your Content in the *Amazon CloudFront Developer Guide*.

Edit

	Restriction	Status	Type
☐	Geo Restriction	Disabled	-