

Successfully created s3 bucket:

The screenshot shows the AWS S3 Buckets page. At the top, there are tabs for "General purpose buckets" (selected) and "Directory buckets". Below the tabs, a message states "Buckets are containers for data stored in S3." A search bar is present with the placeholder "Find buckets by name". A table lists one bucket entry:

Name	AWS Region	Creation date
my-741021496497-static-website-hosting	US East (N. Virginia) us-east-1	November 5, 2025, 21:12:05 (UTC+05:30)

Actions for this bucket include "Copy ARN", "Empty", "Delete", and a prominent orange "Create bucket" button. To the right of the bucket list, there are two callout boxes: "Account snapshot" (updated daily) which provides visibility into storage usage and activity trends, and "External access summary - new" (updated daily) which helps identify bucket permissions for public or external access.

Uploaded all the files to S3:

The screenshot shows the AWS S3 console interface. The browser tab is titled "my-741021496497-static-website-hosting". The navigation bar shows "Amazon S3 > Buckets > my-741021496497-static-website-hosting". The main content area is titled "Objects (5)". A table lists the objects in the bucket:

Name	Type	Last modified	Size	Storage class
css/	Folder	-	-	-
img/	Folder	-	-	-
index.html	html	November 5, 2025, 22:10:16 (UTC+05:30)	6.1 KB	Standard
README.txt	txt	November 5, 2025, 22:06:42 (UTC+05:30)	382.0 B	Standard
vendor/	Folder	-	-	-

At the bottom of the page, there are links for CloudShell, Feedback, Copyright notice (© 2025, Amazon Web Services, Inc. or its affiliates.), Privacy, Terms, and Cookie preferences.

Bucket public access:

The screenshot shows the AWS S3 Bucket Permissions Overview page for the bucket 'my-741021496497-static-website-hosting'. The 'Block public access (bucket settings)' section is visible, showing that 'Block all public access' is currently off. The 'Bucket policy' section indicates there is no explicit policy defined.

Permissions overview

Access finding
Access findings are provided by IAM external access analyzers. Learn more about [How IAM analyzer findings work](#).

Block public access (bucket settings)

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 all your S3 buckets and 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 your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access
Off

► Individual Block Public Access settings for this bucket

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Editing the bucket policy

The screenshot shows the 'Edit bucket policy' page for an S3 bucket. The URL in the browser is `us-east-1.console.aws.amazon.com/s3/bucket/my-741021496497-static-website-hosting/property/policy/edit?region=us-east-1`. The left sidebar lists various S3 features like General purpose buckets, Access Grants, and IAM Access Analyzer. The main area displays the bucket ARN (`arn:aws:s3:::my-741021496497-static-website-hosting`) and the current policy in JSON format:

```
1 "Version": "2012-10-17",
2 "Statement": [
3     {
4         "Sid": "AddPerm",
5         "Effect": "Allow",
6         "Principal": "*",
7         "Action": ["s3:GetObject"],
8         "Resource": ["arn:aws:s3:::my-741021496497-static-website-hosting/*"]
9     }
10 ]
11
12 ]
```

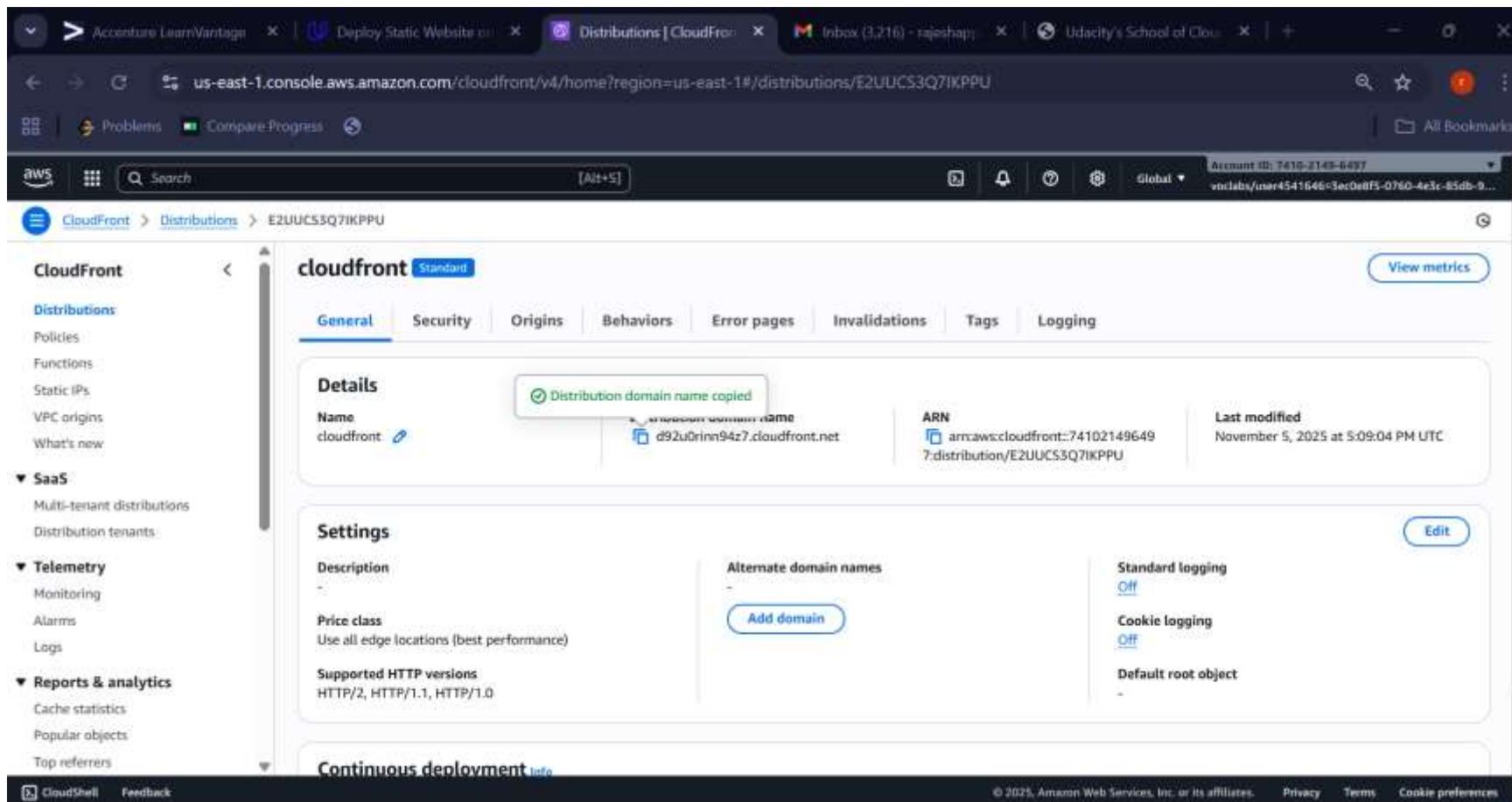
To the right of the policy, there's a panel titled 'Edit statement' with a sub-section 'Select a statement'. It says 'Select an existing statement in the policy or add a new statement' and has a button '+ Add new statement'.

Showing Distribution status as Enabled:

The screenshot shows the AWS CloudFront Distributions page. On the left, there's a sidebar with navigation links for CloudFront (Distributions, Policies, Functions, Static IPs, VPC origins, What's new), SaaS (Multi-tenant distributions, Distribution tenants), Telemetry (Monitoring, Alarms, Logs), and Reports & analytics (Cache statistics, Popular objects, Top referrers). The main content area has a title 'Distributions (1) info'. It includes a search bar ('Search all distributions') and a filter dropdown ('Filter type: All distributions'). A table lists one distribution: ID E2UUCS3Q7IKPPU, Status Enabled, Type Standard, Domain name d92u0rinn..., and Last modified November 5, 2023. At the top right, there are buttons for Enable (highlighted in red), Disable, Delete, and Create distribution.

ID	Status	Description	Type	Domain name	Alternate domain names	Origins	Last modified
E2UUCS3Q7IKPPU	Enabled	-	Standard	d92u0rinn...	-	my-741021496497-	November 5, 2023

Successfully done deploying:



Cloud front
working:<https://d92u0rinn94z7.cloudfront.net/>

