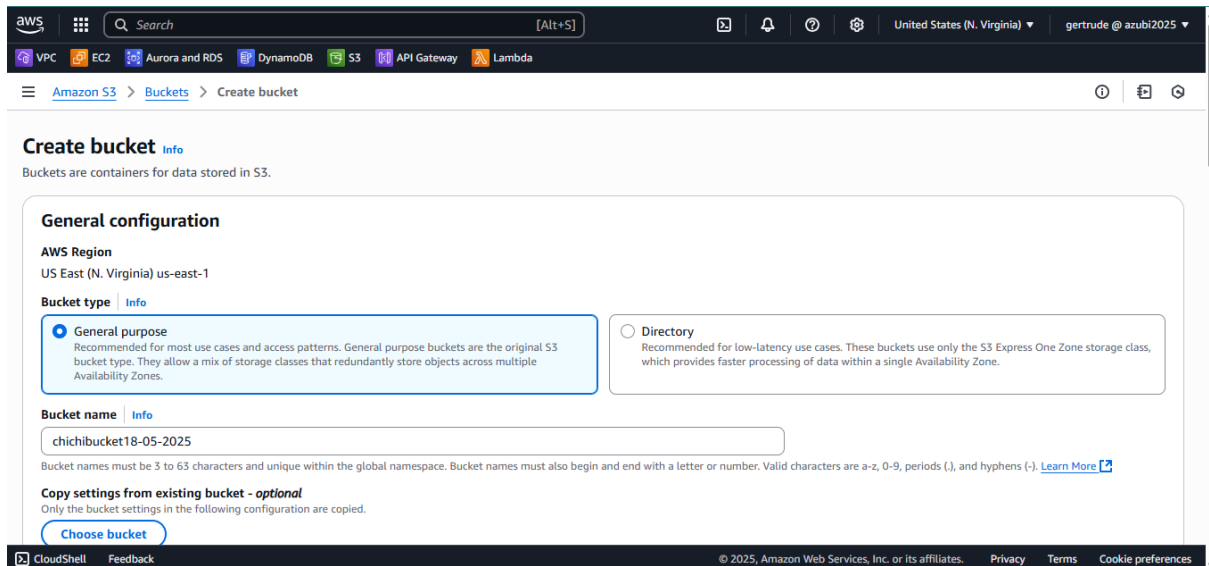


Step by step procedure on the AWS

management console

An S3 bucket was successfully created and all public access to the bucket was blocked



Create bucket [info](#)

Buckets are containers for data stored in S3.

General configuration

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

Bucket type [Info](#)

- ☒ **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 [Info](#)

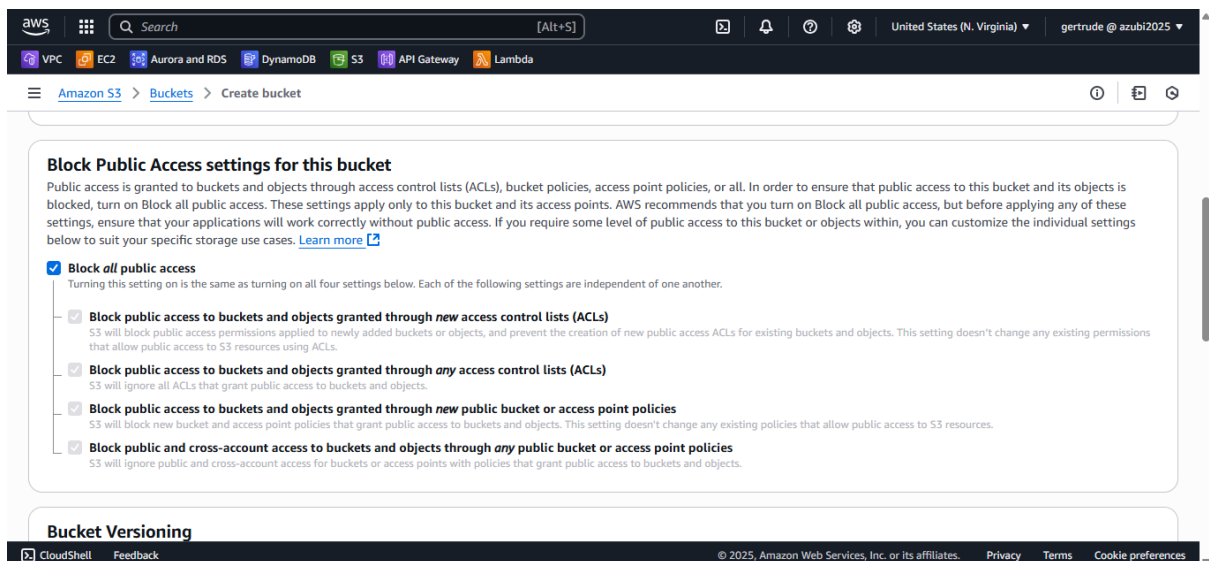
chichibucket18-05-2025

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](#)

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



Block Public Access settings for this bucket

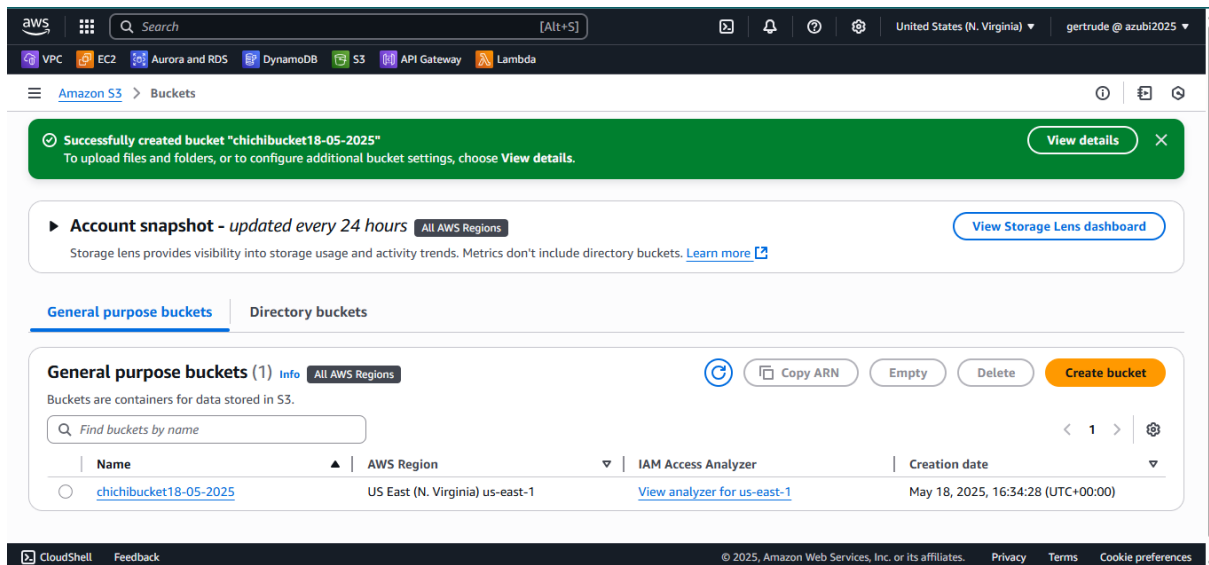
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access 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.

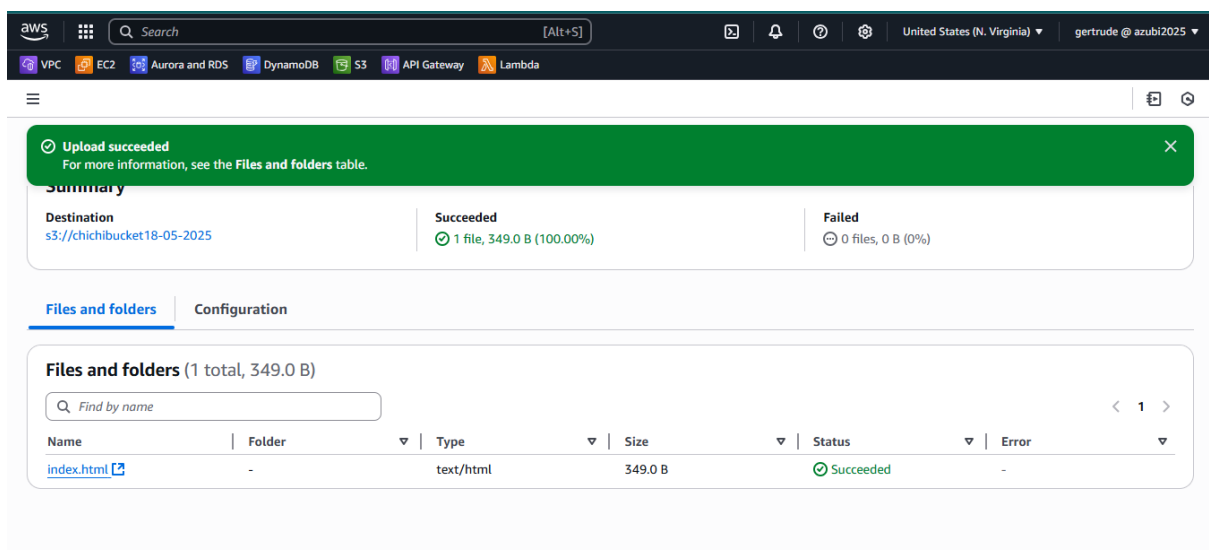
- ☒ **Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing 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

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



An index.html file was successfully uploaded in the S3 bucket.



The cloudfront distribution was configured with the origin access created as well.

aws Search [Alt+S] Global gertrude @ azubi2025

VPC EC2 Aurora and RDS DynamoDB S3 API Gateway Lambda

CloudFront > Distributions > Create

Distribution options [info](#) [amazonaws.com](#)

Choose the type of distribution that best fits your needs

☒ Single website or app
Choose if you have a single app or website

☐ Multi-tenant architecture - New
Choose when you have multiple domains that need to share configurations. This is a common architecture for SaaS providers.

Origin

Choose an AWS origin, or enter your origin's domain name. [Learn more](#)

Origin domain

chichibucket18-05-2025.s3.us-east-1.amazonaws.com

Enter a valid DNS domain name, such as an S3 bucket, HTTP server, or VPC origin ID.

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.

chichibucket18-05-2025.s3.us-east-1.amazonaws.com

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

aws Search [Alt+S] Global gertrude @ azubi2025

VPC EC2 Aurora and RDS DynamoDB S3 API Gateway Lambda

CloudFront > Distributions > Create

Name

Enter a name for this origin.

chichibucket18-05-2025.s3.us-east-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 bucket.

Origin access control

Select an existing origin access control (recommended) or create a new one.

Select an origin access control

Add custom header - optional

CloudFront includes this header in all requests that it sends to the origin.

Add header

Enable Origin Shield

Origin shield is an additional caching layer that can help reduce latency on your content and help protect your content from being hijacked.

Enable Origin Shield

Create new OAC

Name

The name must be unique. Valid characters: letters, numbers and most special characters. Use up to 64 characters.

chichibucket18-05-2025.s3.us-east-1.amazonaws.com

Description - optional

The description can have up to 256 characters.

Enter description

Signing behavior

☐ Do not sign requests

☒ Sign requests (recommended)

☐ Do not override authorization header
Do not sign if incoming request has authorization header.

Origin type

S3

The origin type must be the same type as origin domain.

Cancel Create

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

aws

Search

[Alt+S]

VPC

EC2

Aurora and RDS

DynamoDB

S3

API Gateway

Lambda

CloudFront > Distributions > Create

Name

Enter a name for this origin.

chichibucket18-05-2025.s3.us-east-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 control

Select an existing origin access control (recommended) or create a new control.

chichibucket18-05-2025.s3.us-east-1.amazonaws.com

Create new OAC

You must update the S3 bucket policy

CloudFront will provide you with the policy statement after creating the distribution.

Add custom header - optional

CloudFront includes this header in all requests that it sends to your origin.

aws

Search

[Alt+S]

VPC

EC2

Aurora and RDS

DynamoDB

S3

API Gateway

Lambda

CloudFront > Distributions > Create

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.

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

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

aws

Search

[Alt+S]

VPC

EC2

Aurora and RDS

DynamoDB

S3

API Gateway

Lambda

CloudFront > Distributions > E18FK4ZOI1UPX0

Successfully created new distribution.

To get in-depth monitoring information for your distribution's internet traffic, create an Internet Monitor

Notifications 0 1 1 0 0 0

E18FK4ZOI1UPX0

Standard

View metrics

General

Security

Origins

Behaviors

Error pages

Invalidations

Tags

Logging

Details

Distribution domain name

d39kl9ekitstd6.cloudfront.net

ARN

arn:aws:cloudfront::509399621215:distribution/E18FK4ZOI1UPX0

Last modified

Deploying

Settings

Edit

Description

Alternate domain names

Standard logging

Off

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

The bucket policy was updated

The screenshot shows the AWS IAM console interface. The breadcrumb navigation indicates the path: **Amazon S3** > **Buckets** > **chichibucket18-05-2025** > **Edit bucket policy**. The main content area is split into two panels. The left panel contains a code editor with the following JSON policy document:

```
1 {
2   "Version": "2008-10-17",
3   "Id": "PolicyForCloudFrontPrivateContent",
4   "Statement": [
5     {
6       "Sid": "AllowCloudFrontServicePrincipal",
7       "Effect": "Allow",
8       "Principal": {
9         "Service": "cloudfront.amazonaws.com"
10      },
11      "Action": "s3:GetObject",
12      "Resource": "arn:aws:s3:::chichibucket18-05-2025/*",
13      "Condition": {
14        "StringEquals": {
15          "AWS:SourceArn": "arn:aws:cloudfront::509399621215:distribution/E18FK4Z0I1UPX0"
16        }
17      }
18    }
19  ]
20 }
```

The right panel, titled "Edit statement", displays a "Select a statement" dialog. It instructs the user to "Select an existing statement in the policy or add a new statement." and features a blue button labeled "+ Add new statement".

At the bottom of the console, a status bar includes the "CloudShell" icon, a "Feedback" link, and copyright information: "© 2025, Amazon Web Services, Inc. or its affiliates." along with links for "Privacy", "Terms", and "Cookie preferences".

This screenshot shows the same AWS IAM console page after the policy has been successfully updated. A green banner at the top of the content area displays the message: "Successfully edited bucket policy." with a close button (X). The code editor on the left now contains the updated policy document:

```
{
  "Version": "2008-10-17",
  "Id": "PolicyForCloudFrontPrivateContent",
  "Statement": [
    {
      "Sid": "AllowCloudFrontServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudfront.amazonaws.com"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::chichibucket18-05-2025/*",
      "Condition": {
        "StringEquals": {
          "AWS:SourceArn": "arn:aws:cloudfront::509399621215:distribution/E18FK4Z0I1UPX0"
        }
      }
    }
  ]
}
```

The right panel now features a blue button labeled "Copy". The bottom status bar remains the same, showing "CloudShell", "Feedback", and copyright information.

The distributed domain name was pasted on the browser and it displayed the static website.

