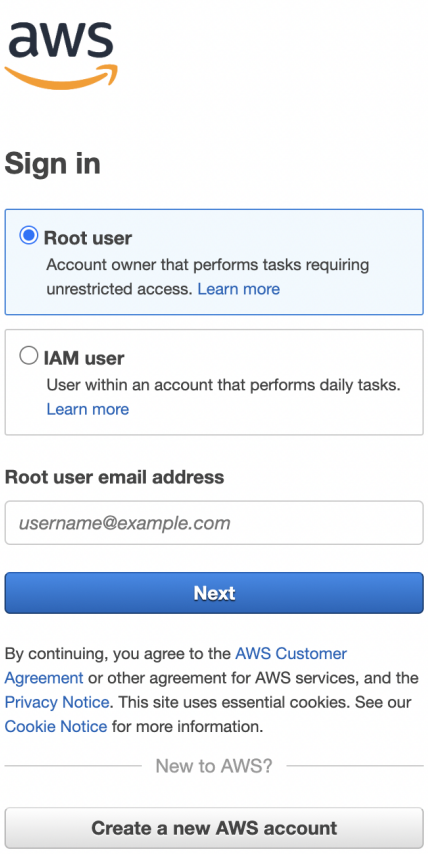
Config AWS Access Key

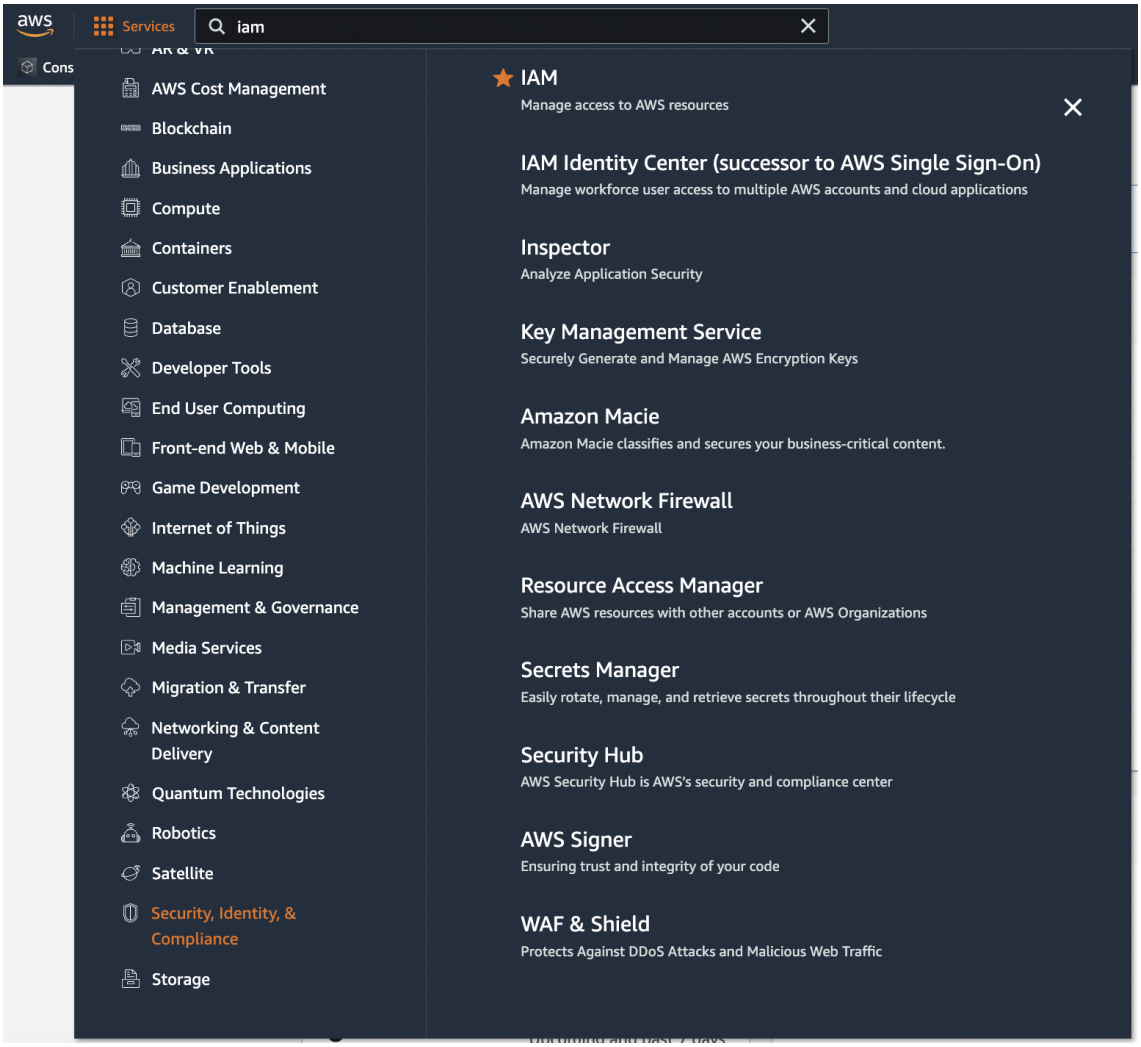
You can use the AWS Management Console to create/manage the access keys. Follow the below steps to create AWS Access Key 1. sign in to the AWS console.

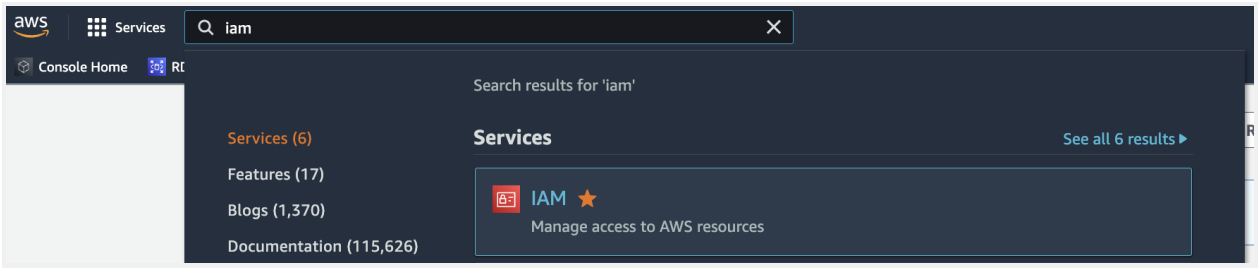


Select “Root User” and key in the email address and password.

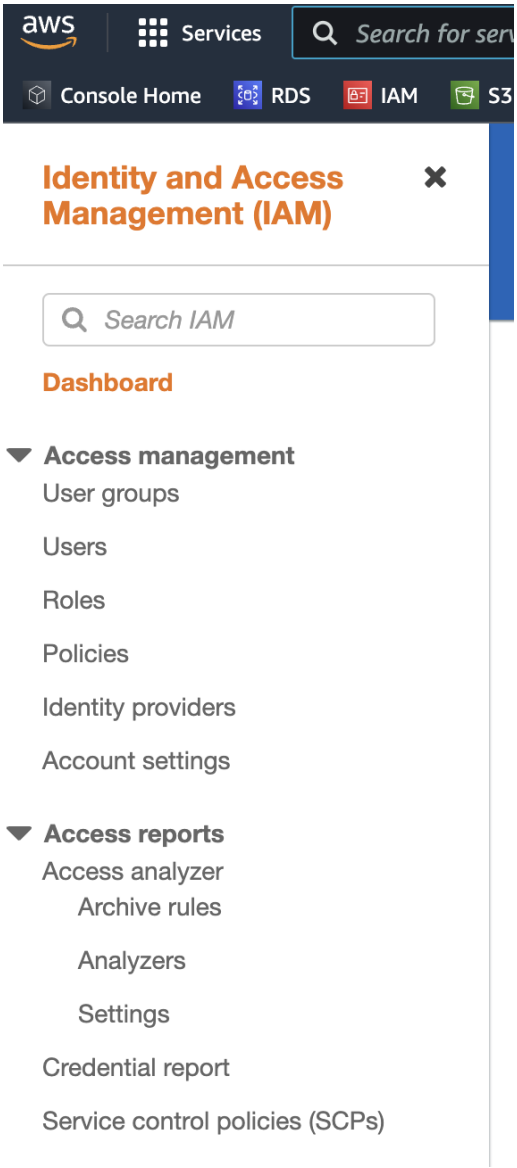
For your convenience, the AWS sign-in page uses a browser cookie to remember your user name and account information. If you previously signed in as a different user, choose Sign in to a different account near the bottom of the page to return to the main sign-in page.

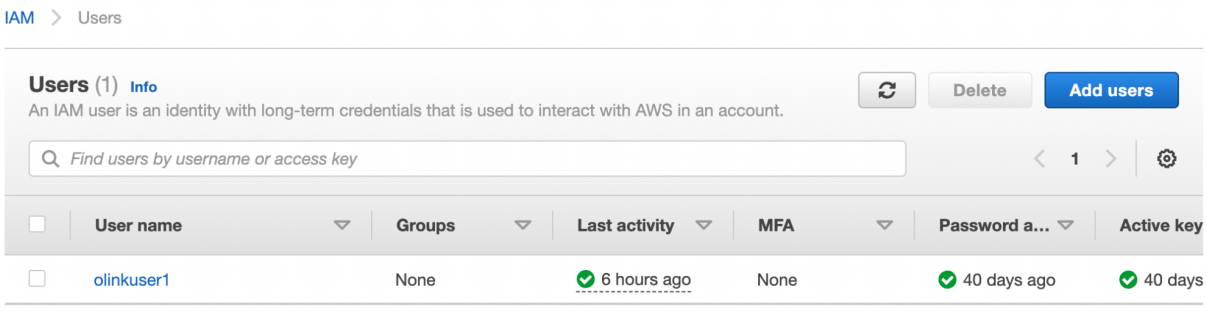
Click Services -> Security, Identity, & Compliance -> IAM. Or enter “iam” in the search box.



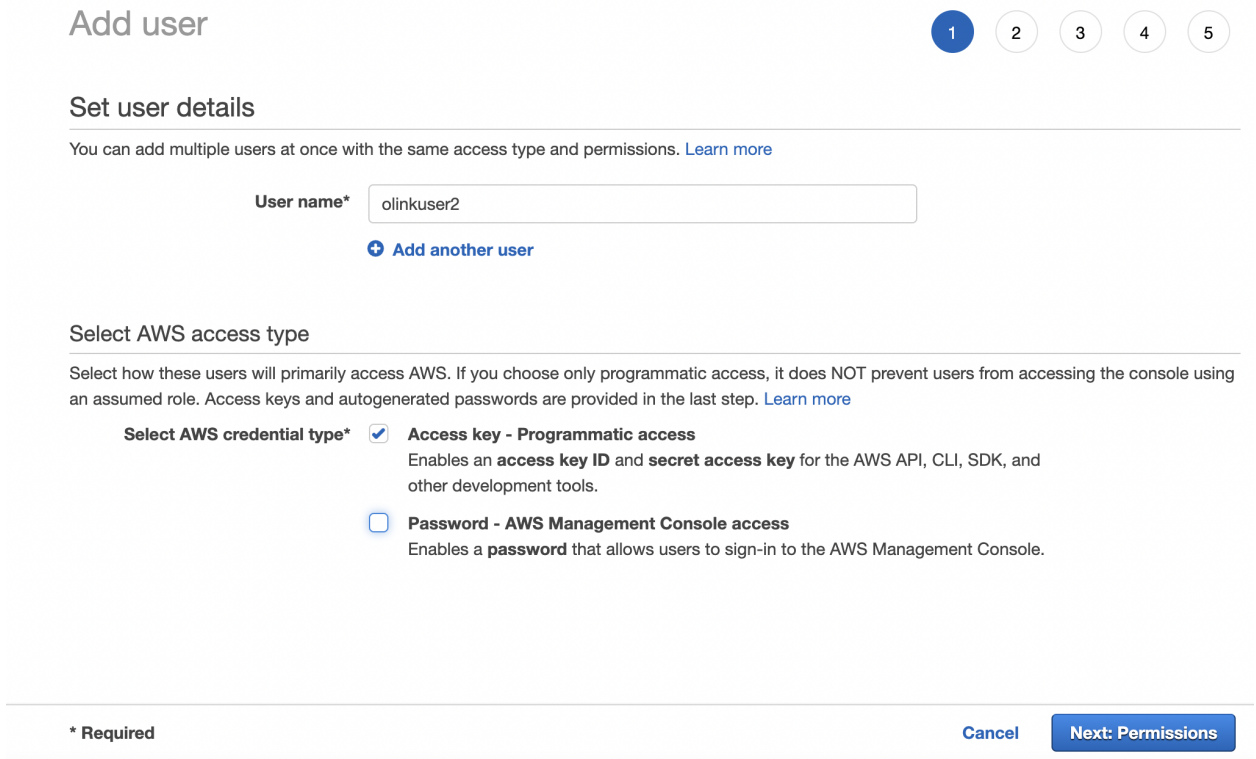


Select Users -> Add Users

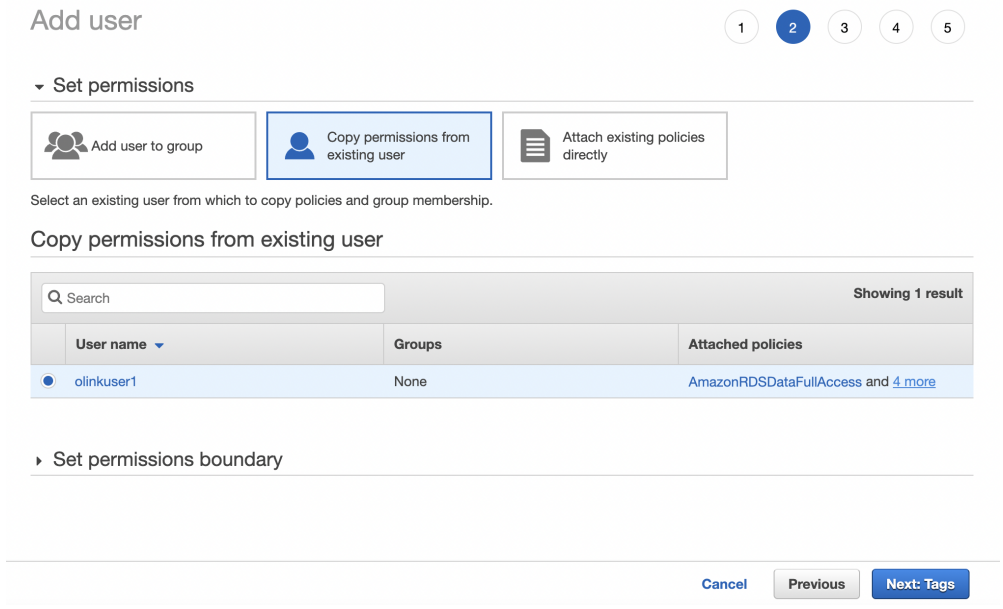




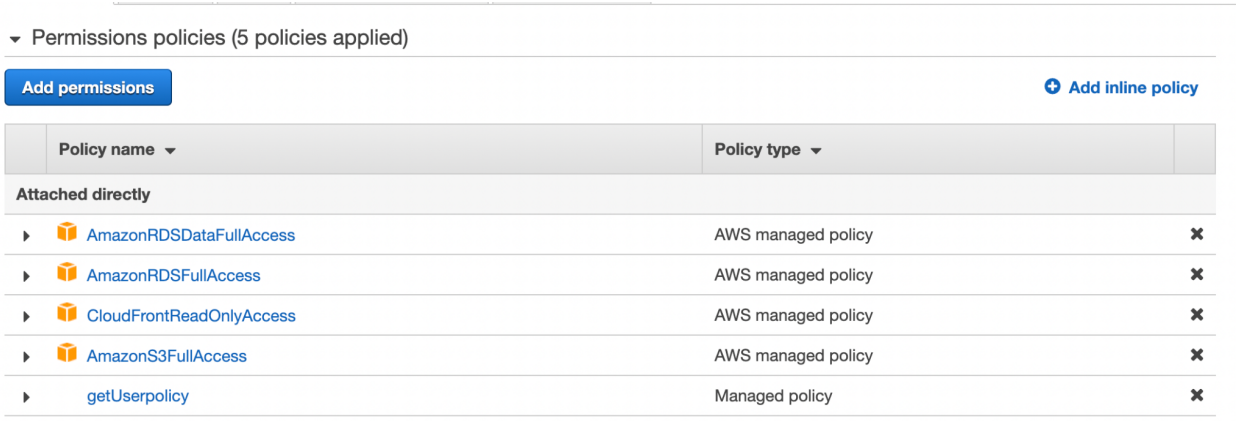
Key in “User Name”, Tick Access type: “Programmatic access” and , then click “Next Permissions”



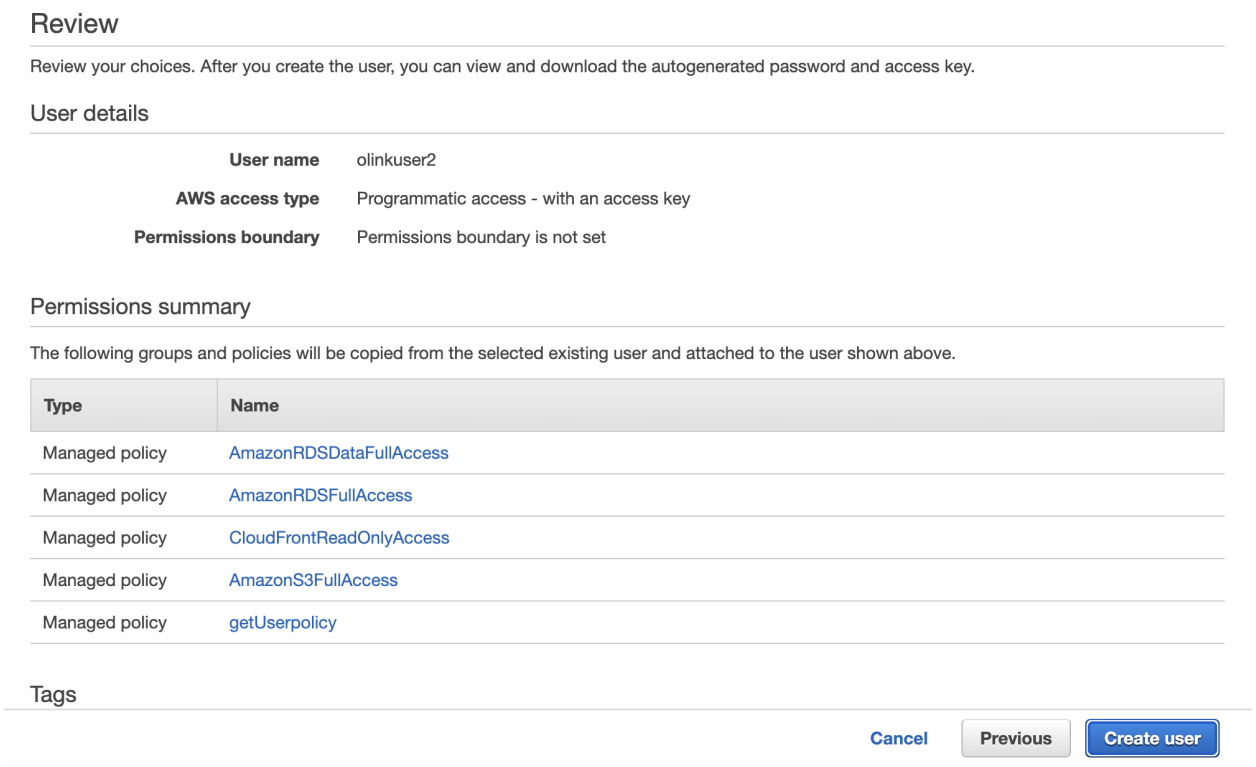
You may copy permissions from an existing user.



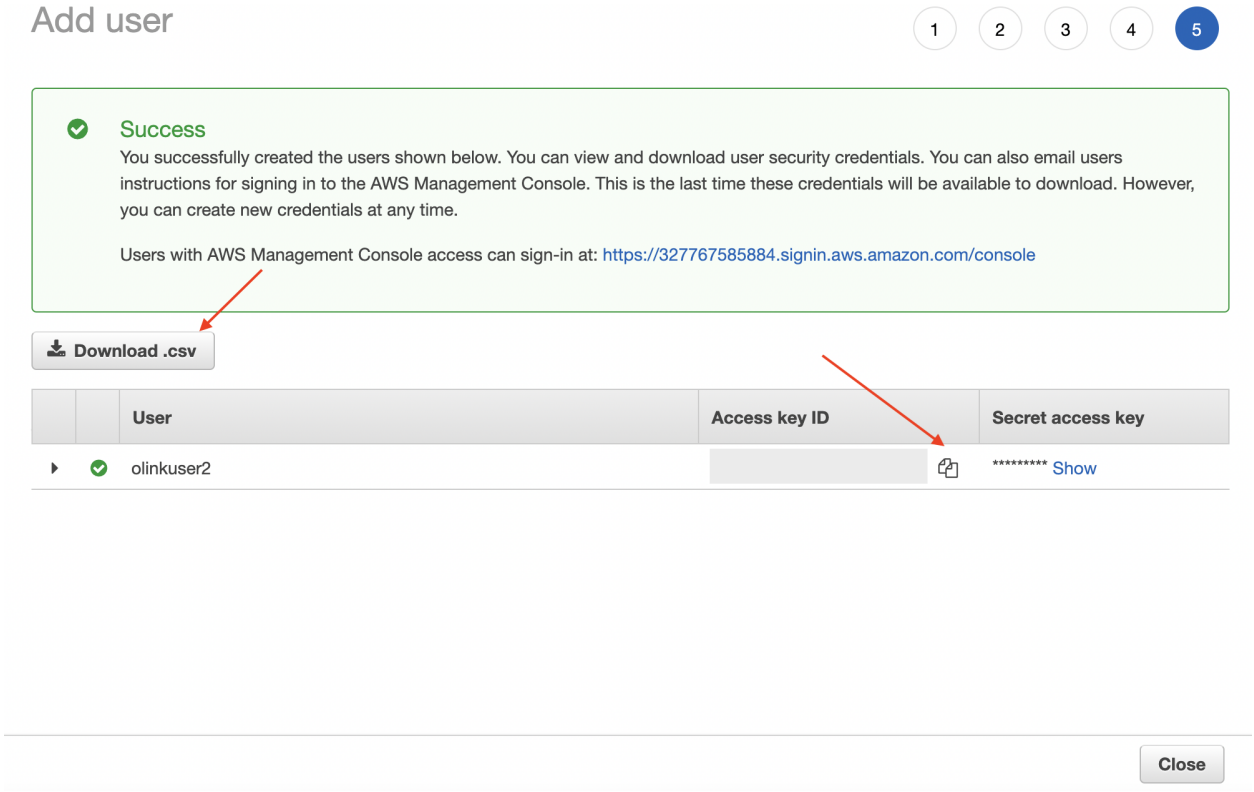
Or Search and select the following permissions: RDSDataFullAccess, RDSFullAccess, CloudFrontReadOnlyAccess, S3FullAccess, getUserpolicy.



"Add Tags" are optional, Click "Next: Review". Then, Click "Create User".



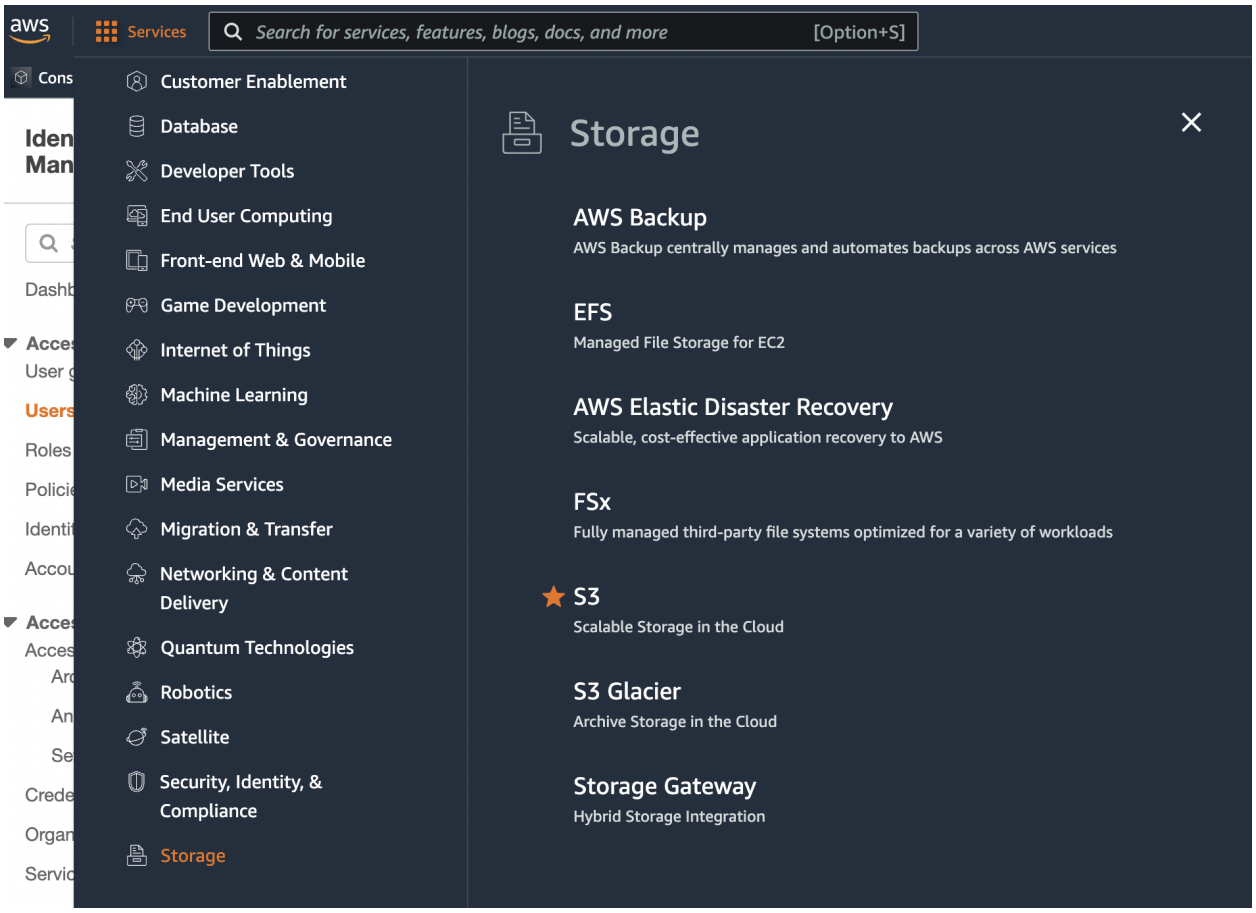
Click “Download .csv”, save it to the folder oLink installed, then click “Close”.

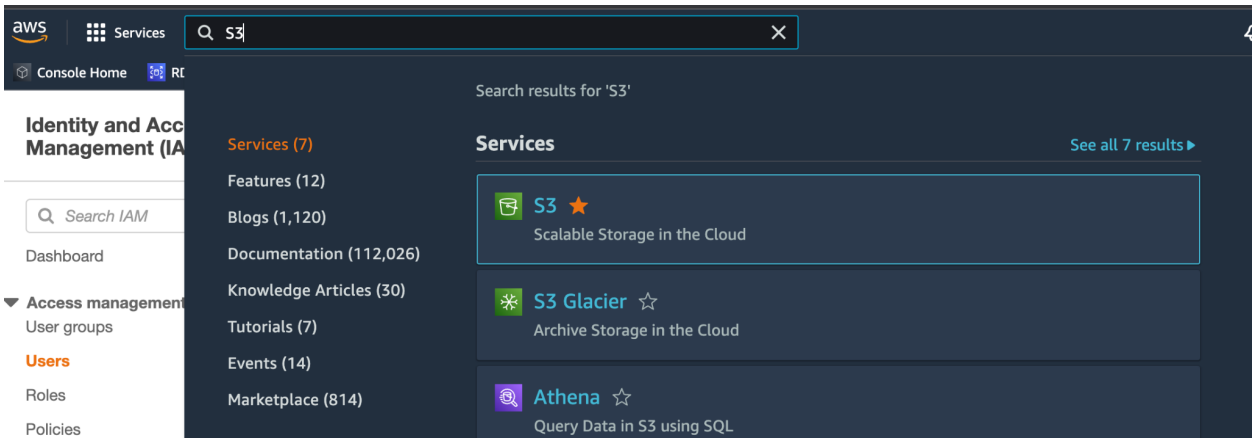


The Access credentials will be used in this screen in the olink application.

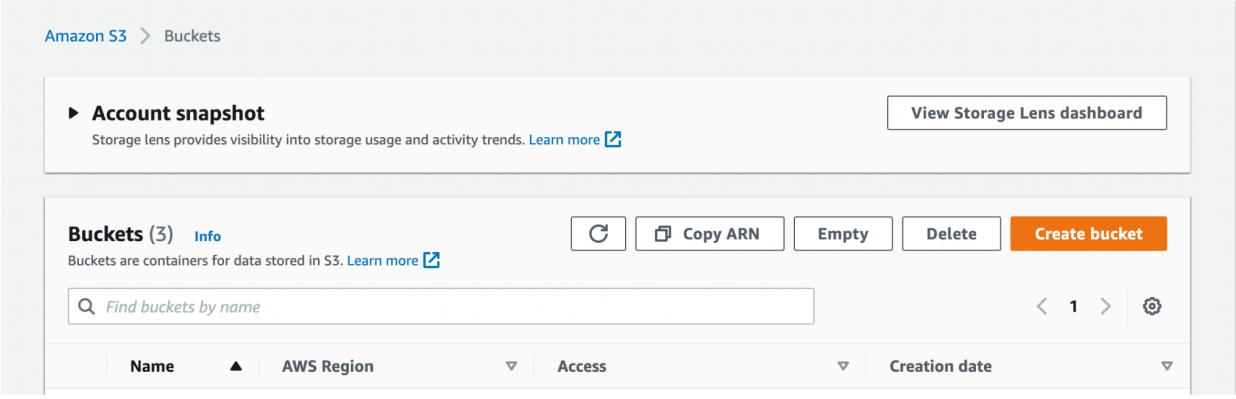
Create S3 Bucket

sign in to the AWS console using “Root User”. Click “All Services” -> S3. Or search S3 in the search box.





Click Button “Create Bucket”



In order for olink application to work smoothly, use this name convention.

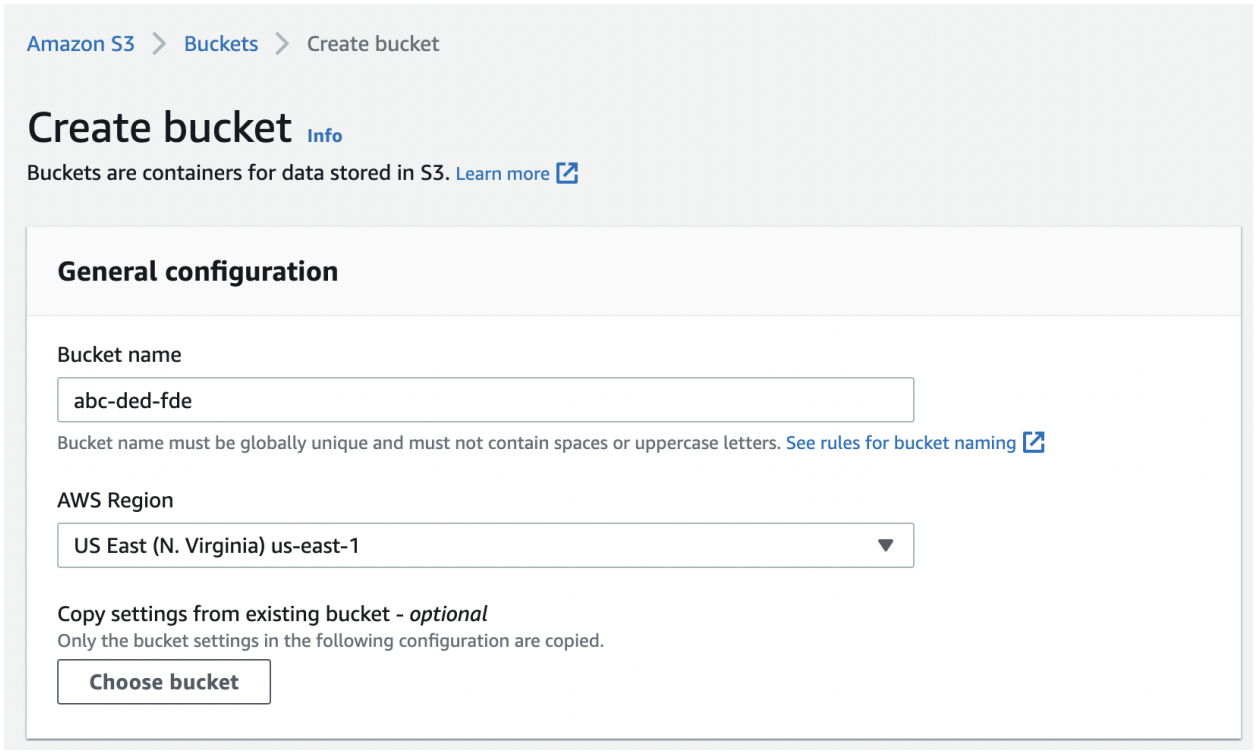
- **Naming rule: [username] + “-S3”**
- **[username] has to be the one who is supposed to have access to this bucket**
- **Example: olinkuser2-s3**

In Bucket name, enter a DNS-compliant name for your bucket.

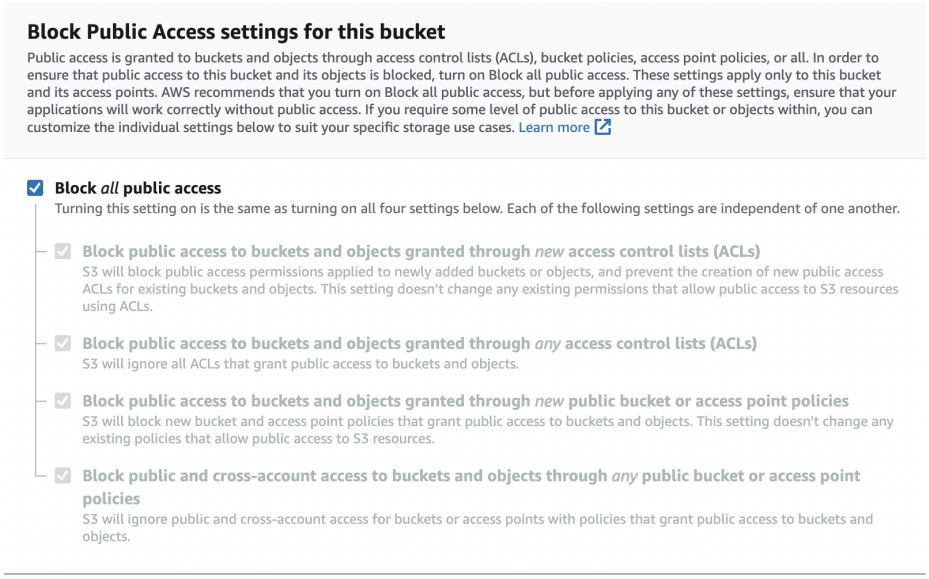
Also, the bucket name must

- Be unique across all of your Amazon S3.
- Bucket names must be between 3 (min) and 63 (max) characters long.
- Bucket names can consist only of lowercase letters, numbers, dots (.), and hyphens (-).
- Bucket names must begin and end with a letter or number.
- Bucket names must not contain two adjacent periods.
- Avoid including sensitive information, such as account numbers, in the bucket name. The bucket name is visible in the URLs that point to the objects in the bucket.
- MORE

After you create the bucket, you can't change its name. In Region, select “US East (N. Virginia) us-east-1”



Keeping “Block All Public Access” is recommended.



Click Button “Create Bucket”

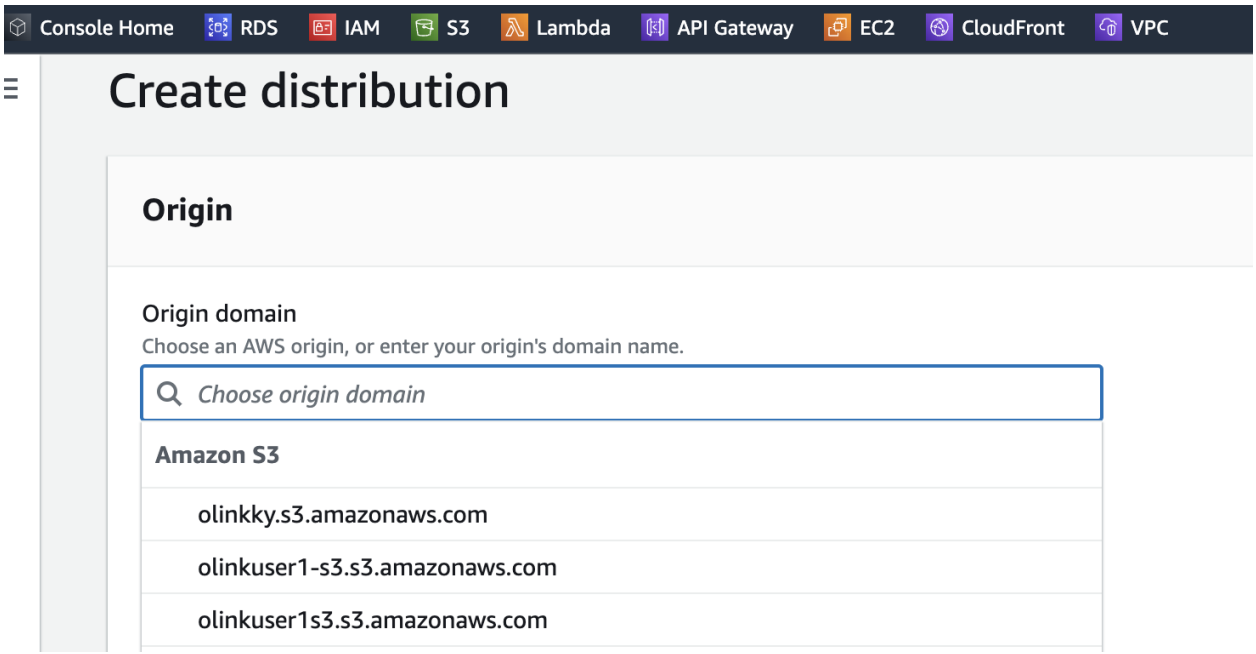
Save the bucket name as S3 Bucket in the oLink Management Console Tab.

USE “cloudfront.net” domain to hide and protect S3 bucket

Advantage:
Prevent S3 from being discovered
More Comprehensive settings are available to protect the buckets
Use your own domain name later on (Amazon Route53)
With CloudFront Functions, you can write lightweight functions in JavaScript for high-scale, latency-sensitive CDN customizations.
URL appears simpler

Steps:

Go to CloudFront service and click “Create Distribution”.
On the next screen, Choose an Origin such as a S3 bucket.

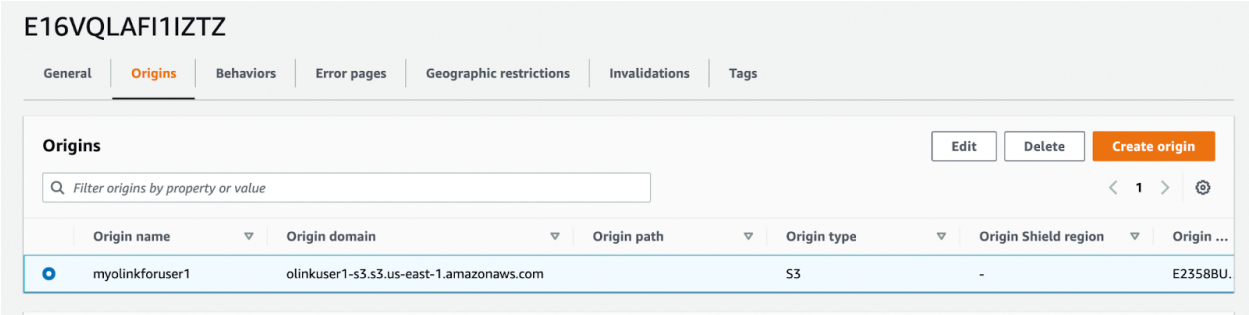


For “Origin Access”, select “Origin access control settings (recommended)” and click “Create control setting“ and give it a name e.g. “olinks-OAI”.
Click “Create Distribution” to save and here is the resulting Domain Name and URL to access the private bucket.
https://d1699jf5nad3mc.cloudfront.net/show.htm

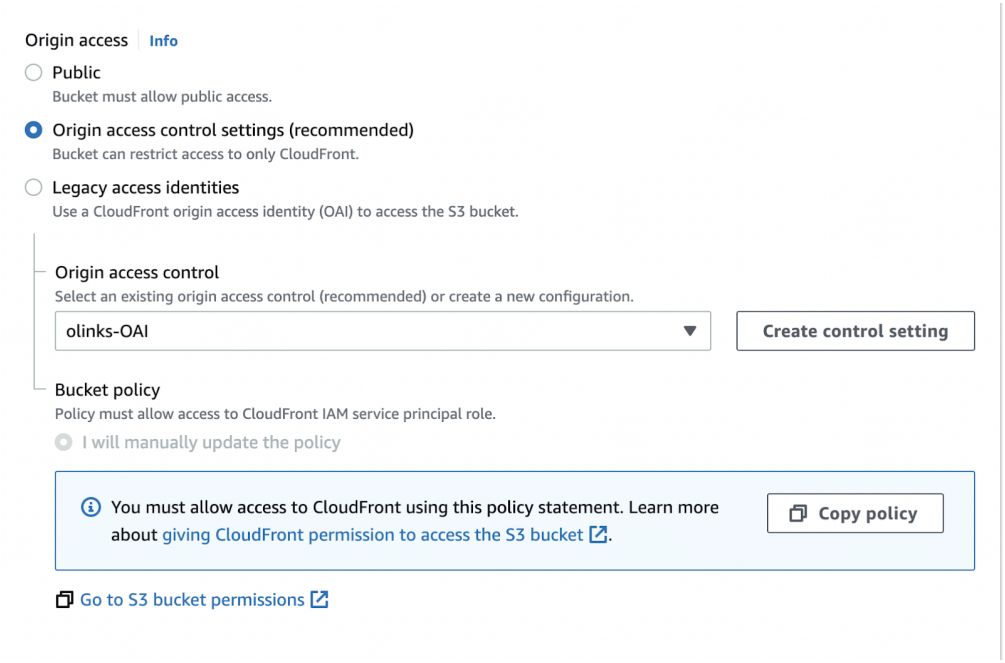
Distribution domain name “d1699jf5nad3mc.cloudfront.net”

Distribution ID “E16VQLAFI1IZTZ”
Distribution origin name “myolinkforuser1”

Select the ID and click “Edit” to “Edit origin”



In section “Origin access”, select “Origin access control settings (recommended)”, and select from the drop down “Origin access control” (e.g. “olinks-OAI”). Or click button “Create control setting”.



The click “Copy Policy”. The bold text below shows the copied bucket policy.

Bucket policy (permission)

{
"Version": "2008-10-17",

```
  "Id": "PolicyForCloudFrontPrivateContent",
  "Statement": [
    {
      "Sid": "AllowCloudFrontServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudfront.amazonaws.com"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::olinkuser1-s3/*",
      "Condition": {
        "StringEquals": {
          "AWS:SourceArn":
"arn:aws:cloudfront::327767585884:distribution/E16VQLAFI1IZTZ"
        }
      }
    }
  ]
}
```

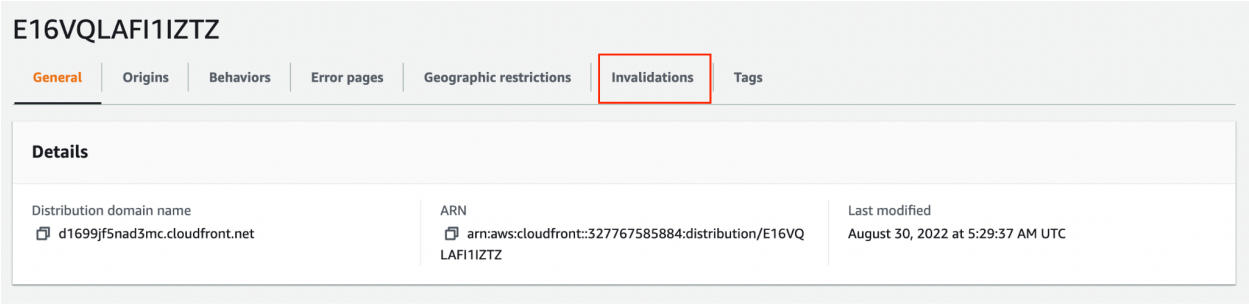
```
{
        "Version": "2008-10-17",
        "Id": "PolicyForCloudFrontPrivateContent",
        "Statement": [
                {
                        "Sid": "s3policyforcf",
                        "Effect": "Allow",
                        "Principal": {
                                "Service": "cloudfront.amazonaws.com"
                        },
                        "Action": "s3:GetObject",
                        "Resource": "arn:aws:s3:::olinkuser1-s3/*",
                        "Condition": {
                                "StringLike": {
                                        "AWS:SourceArn":
"arn:aws:cloudfront::327767585884:distribution/*"
                                }
                        }
                }
        ]
```

```
}
```

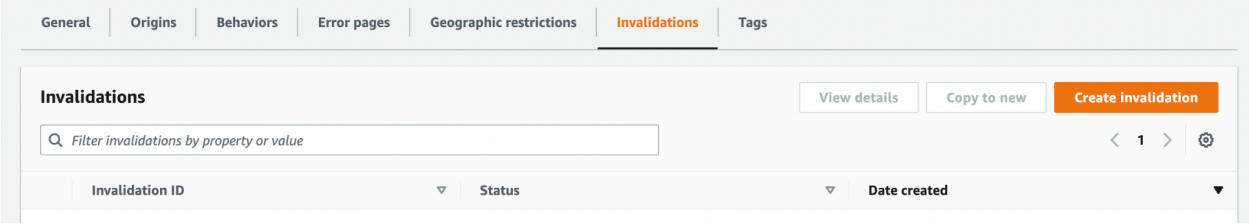
Public Access Policy

```
{
	"Version": "2012-10-17",
	"Statement": [
		{
			"Effect": "Allow",
			"Principal": "*",
			"Action": "s3:GetObject",
			"Resource": "arn:aws:s3:::olinkuser1-s3/*"
		}
	]
}
```

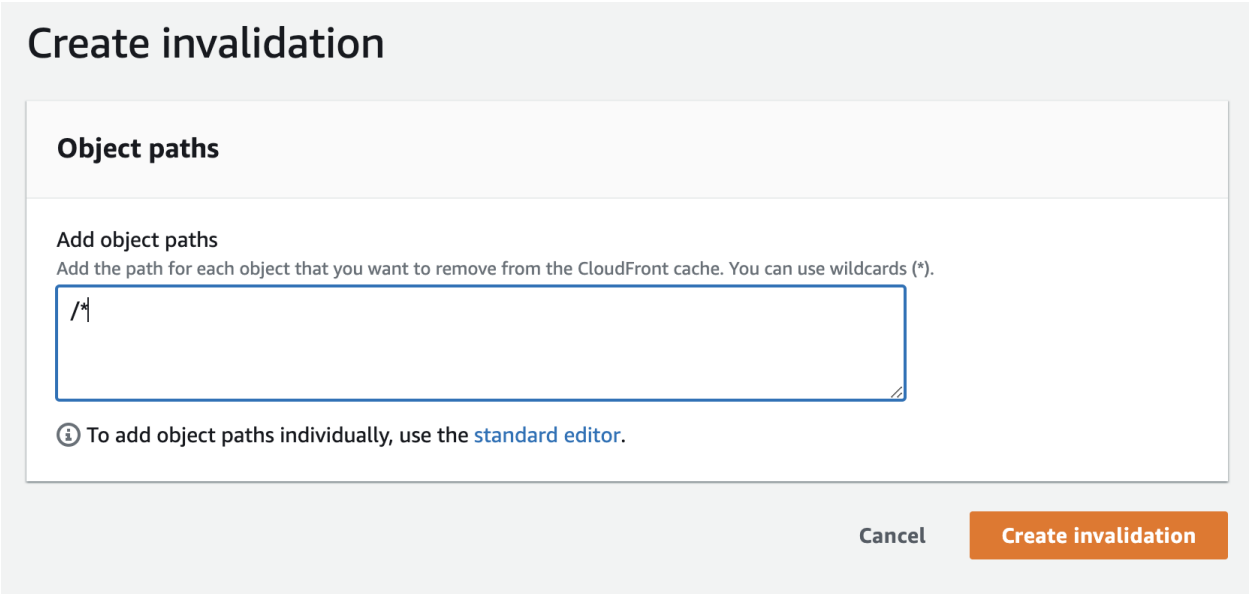
In order for CloudFront to refresh as S3 bucket updates its content, please add “Invalidation”.



Click “Create Invalidation” button



Type in “/*” in the “Add object paths” field and click “Create invalidation”.



CloudFront Background: Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment. https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html

REFERENCE

AWS CloudFront CDN for S3 Tutorial
https://www.youtube.com/watch?v=-DDGYzKtNwc

React App on AWS S3 with Static Hosting + Cloudfront
https://www.youtube.com/watch?v=mls8tiiI3uc

Developer's Guide to Cloudfront and static web
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AmazonCloudFront_DevGuide.pdf

Cloudfront Pricing

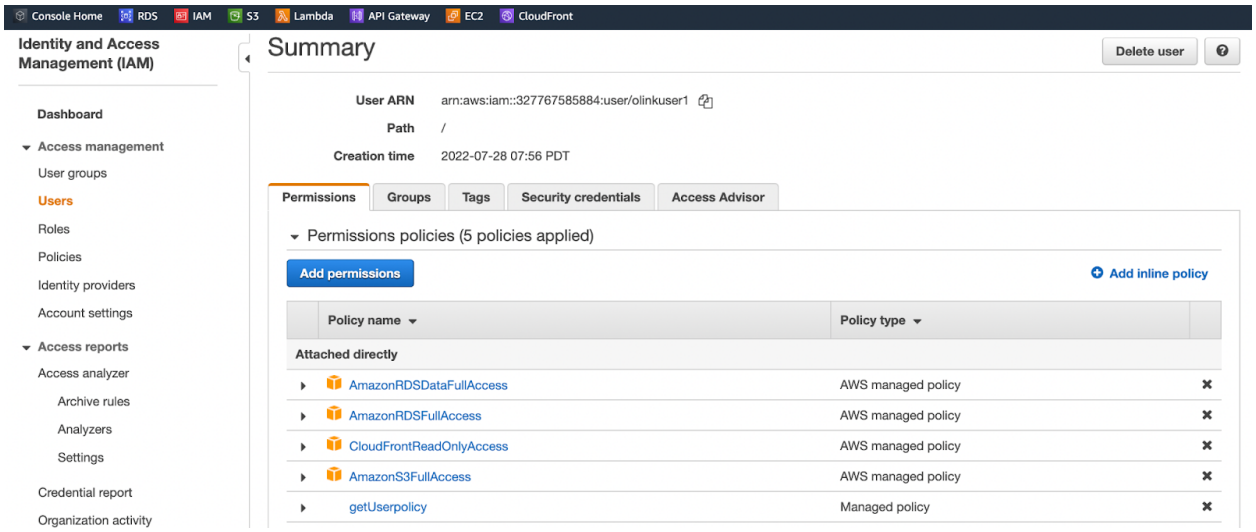
1 TB of data transfer out

10,000,000 HTTP or HTTPS Requests

2,000,000 CloudFront Function Invocations

USER creation and permissions

List of permissions to be added:



“AmazonRDSDataFullAccess”
“AmazonRDSFullAccess”
“CloudFrontReadOnlyAccess”
“AmazonS3FullAccess”
“getUserpolicy”: Allow GetUser (Read) from IAM service

ListDistributions()
ListDistributionResponse.DistributionList.Items[0]
Amazon.CloudFront.Model.DistributionSummary
Origins.Items[0]

<Amazon.CloudFront.Model.Origin>((<Amazon.CloudFront.Model.DistributionSummary>(dl.DistributionList.Items).Items[0]).Origins.Items).Items[0]).DomainName = "olinkuser1-s3.s3.us-east-1.amazonaws.com"
<Amazon.CloudFront.Model.Origin>((<Amazon.CloudFront.Model.DistributionSummary>(dl.DistributionList.Items).Items[0]).Origins.Items).Items[0]).Id = "myolinkforuser1"
(new System.Collections.Generic.Mscorlib_CollectionDebugView<Amazon.CloudFront.Model.Origin>((new System.Collections.Generic.Mscorlib_CollectionDebugView<Amazon.CloudFront.Model.DistributionSummary>(dl.DistributionList.Items).Items[0]).Origins.Items).Items[0]).OriginShield???
(new System.Collections.Generic.Mscorlib_CollectionDebugView<Amazon.CloudFront.Model.Origin>((new System.Collections.Generic.Mscorlib_CollectionDebugView<Amazon.CloudFront.Model.DistributionSummary>(dl.DistributionList.Items).Items[0]).Origins.Items).Items[0]).S3OriginConfig???