

😊 Providing Access to Object in S3

1. Login to AWS Console.
2. Then navigate to S3, and open your recently created bucket.
3. In the last lab you have stored some files or objects in S3.
4. In relation with that you have the authority to download that object or file and open that object or file.

The screenshot shows the AWS S3 console interface. A file named 'script.yml' is selected in the 'scripts/' folder of the 'datausr1234' bucket. The 'Object actions' button at the top right is highlighted with a red box. Below it, the 'Properties' tab is active, showing details like Owner (ea94e9301e0e9ed79a85aa0c0282dccbba7eabbae9b707dc9c2cfe1a489686), AWS Region (Europe (London) eu-west-2), Last modified (January 12, 2024, 19:57:53 (UTC+05:30)), Size (58.0 B), Type (yml), and Key (scripts/script.yml). The 'Object overview' section displays the S3 URI (s3://datausr1234/scripts/script.yml), Amazon Resource Name (ARN) (arn:aws:s3:::datausr1234/scripts/script.yml), Entity tag (Etag) (ad73a5cf35697e5cd3350aa0ce9f741), and Object URL (https://datausr1234.s3.eu-west-2.amazonaws.com/scripts/script.yml).

5. But if you will use the object URL and open that in a new tab you will see that it is giving you an access error.
6. This error is happening because of the permission that you have given to the bucket.
7. As you know this URL is basically used for third parties, who can access your bucket content and download or see them.

Object URL

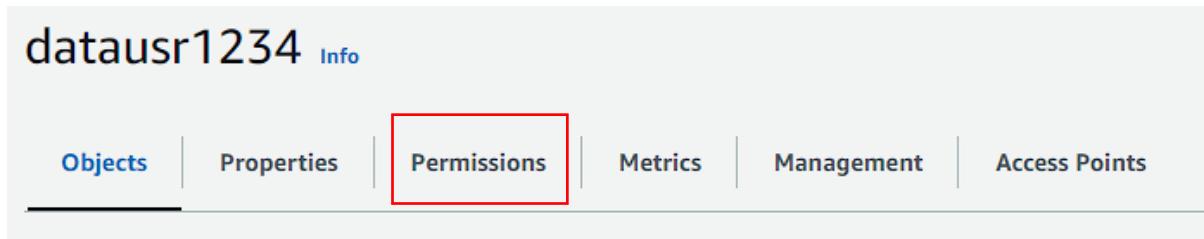
🔗 <https://datausr1234.s3.eu-west-2.amazonaws.com/scripts/script.yml>

The browser screenshot shows the URL https://datausr1234.s3.eu-west-2.amazonaws.com/scripts/script.yml in the address bar. The page content is an XML error response:

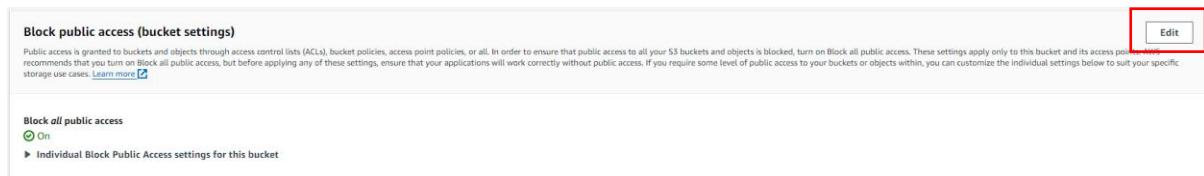
```
<Error>
<Code>AccessDenied</Code>
<Message>Access Denied</Message>
<RequestId>5FFGHB1V5BKPHE8F</RequestId>
<HostId>nfbJuIxctGCwusynlwzqBsZDHKaiedIpng2AQHPao1D0KY3a/lEeMz2ObNRQId347PNRTi/cU2ZU=</HostId>
</Error>
```

8. Now in this lab you are going to change those permission and create your own permission for the bucket.
9. For you to change those permissions, go back to your bucket.
10. There you will see this option for Permission. Click on it.

11. There you will have all set of permission which you want to change and use as you desire.



12. Now if you will see that the bucket does not have public access.
13. The public access has been blocked; it is because while you were creating the bucket you did not change any of the settings.
14. But now you are going to allow some access for the public.
15. For that click on Edit



16. Here you will see that you have to uncheck the third and forth option. These options will allow you to give some public access and also you can define your policy also.
17. Now click on save changes.

Edit Block public access (bucket settings) Info

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

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.

[Cancel](#)

[Save changes](#)

18. If you will see again, the option for public access is now turned on.

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

19. Now you have to provide it with a policy which will allow the public access.

20. Now to write a bucket policy, you have to click on edit.

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](#)

💡 Public access is blocked because Block Public Access settings are turned on for this bucket
To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about [using Amazon S3 Block Public Access](#)

21. Below is the bucket policy, remember to change the bucket name with your bucket name.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {
```

```
    "Effect": "Allow",
    "Principal": "*",
    "Action": [
        "s3:GetObject"
    ],
    "Resource": "arn:aws:s3:::your-bucket-name/*"
}
]
}
```

22. Now just click on save changes to save your bucket policy.
23. Once your bucket policy is saved go back to that URL and refresh it.
24. You will see that your file has been downloaded this time.
25. This happens because you have changed the bucket policy for your bucket.

