RITIK KR. TIWARI

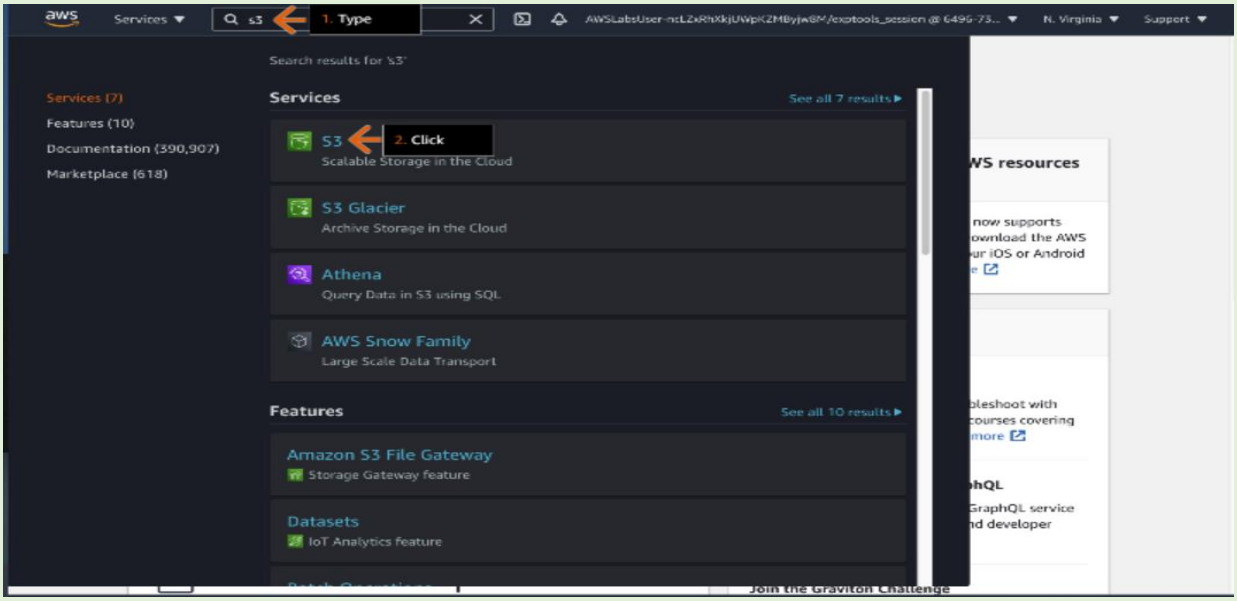
HOW TO HOST STATIC-WEBSITE

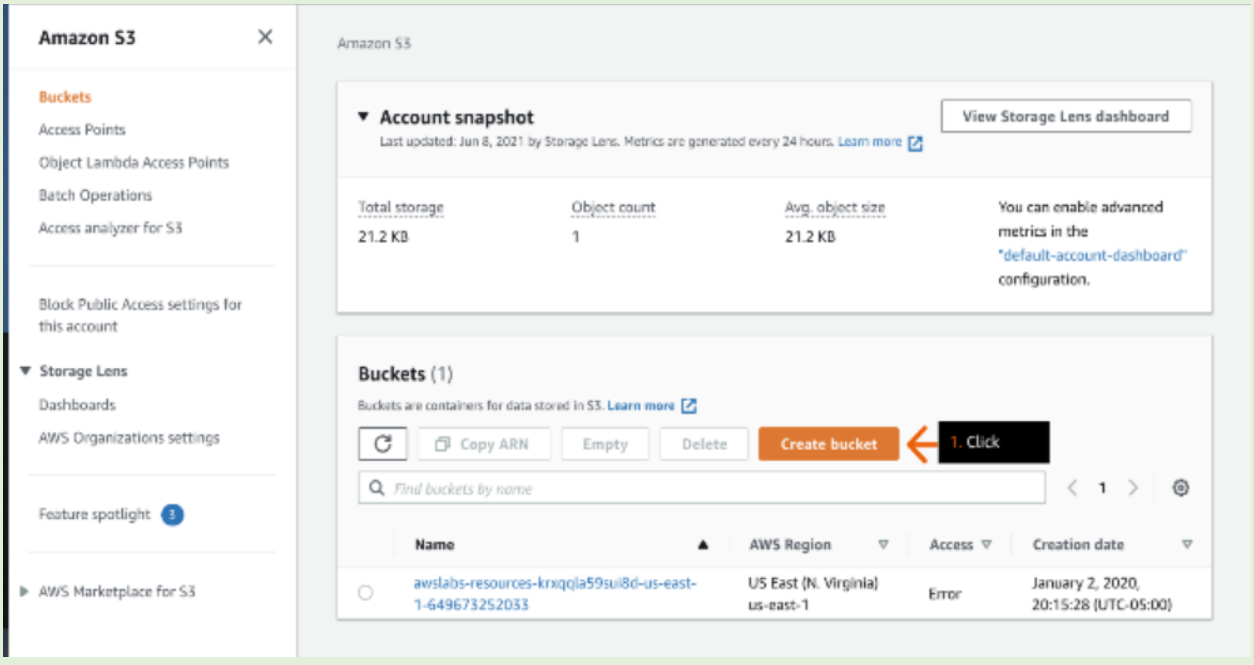
USING: S3 BUCKET
#HANDSONLAB
#LIVEDEMO

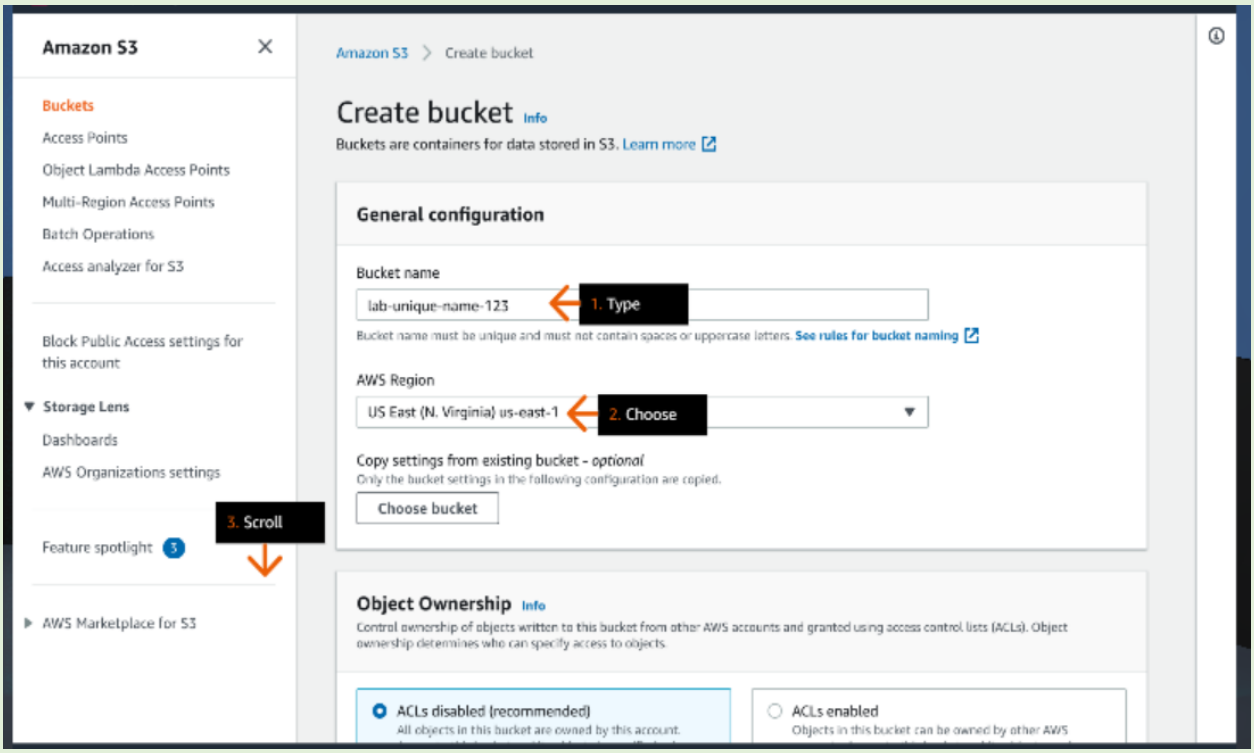
16-09-2023

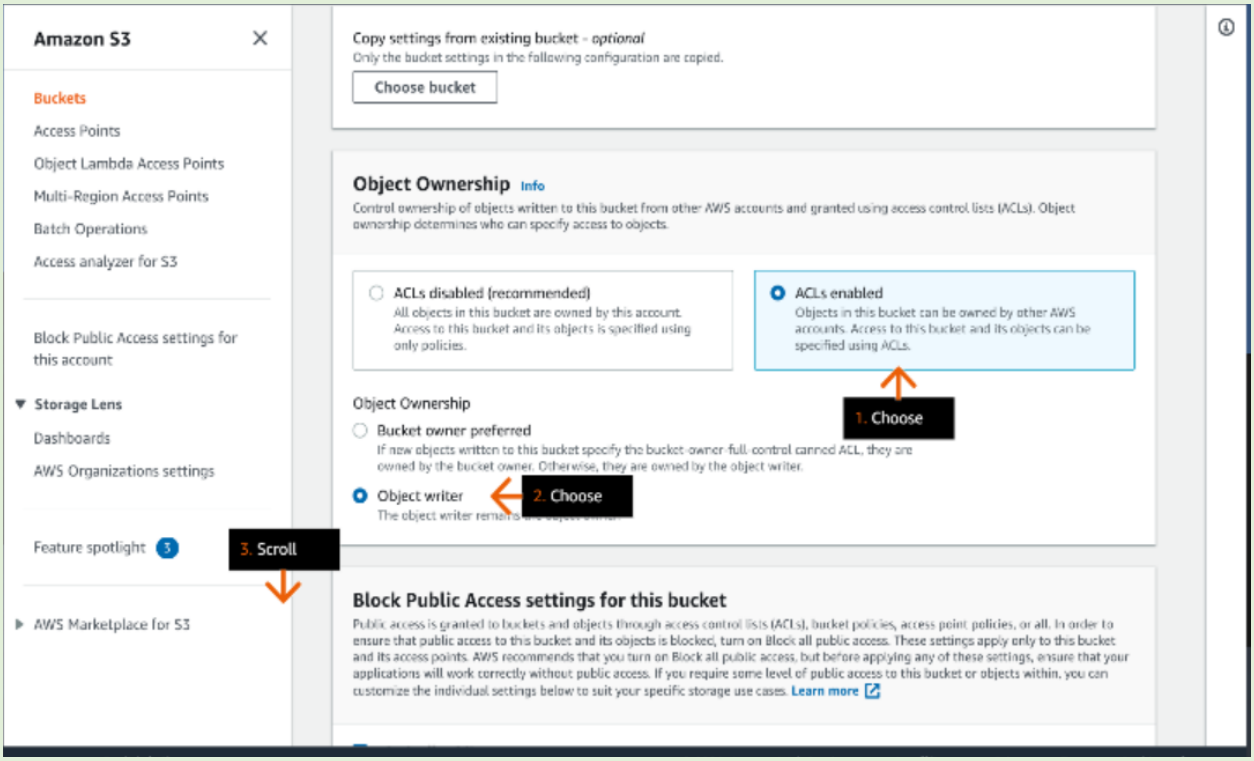
follow on LinkedIn
@Ritik Kumar Tiwari

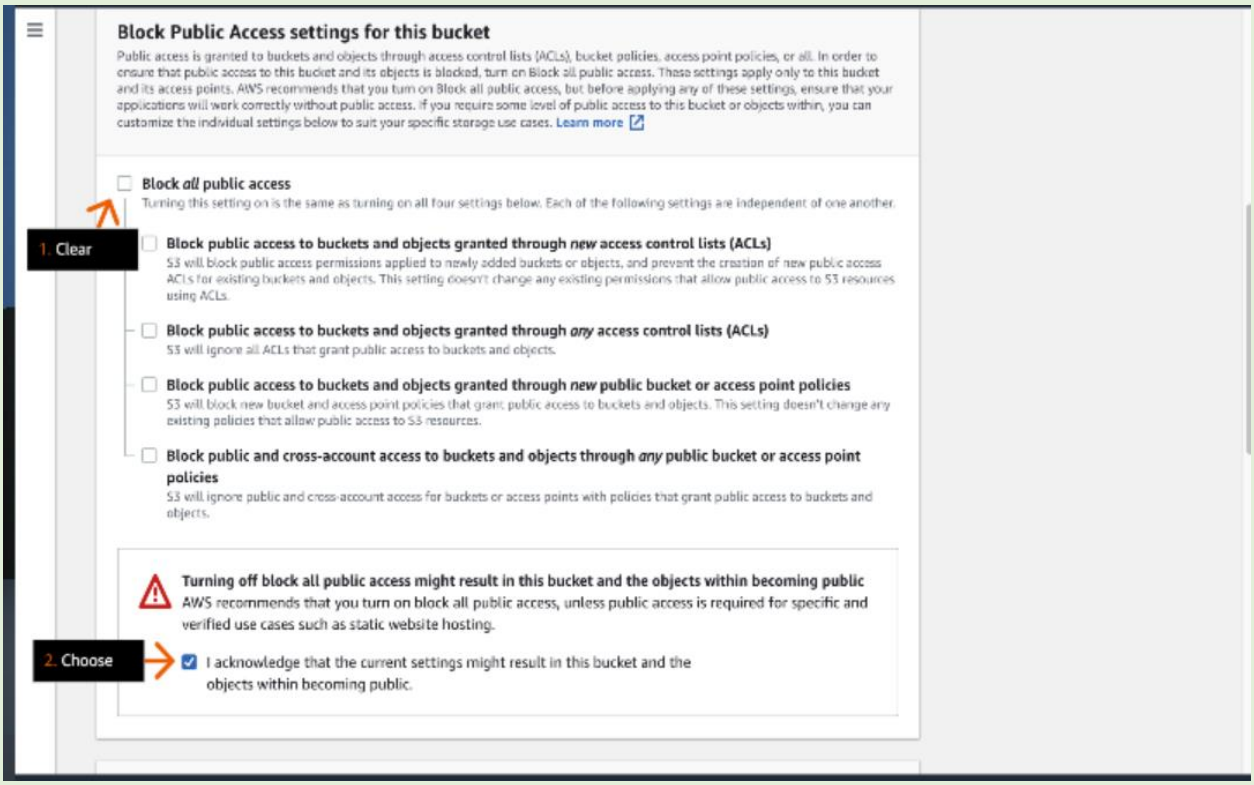
Initially, we have uploaded zip file on my GitHub. Following that, you'll need to download and extract them onto your physical laptop.: https://github.com/RitikPyCode/host-Static-website-s3

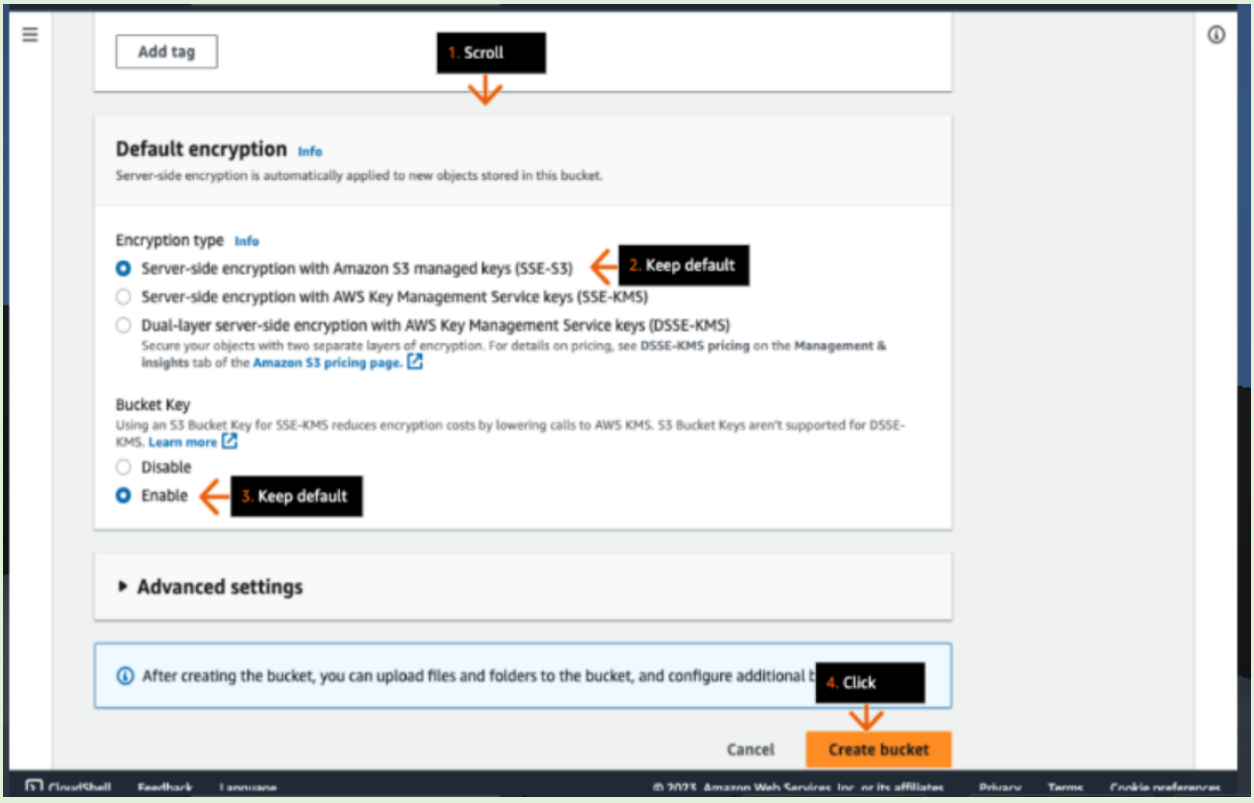


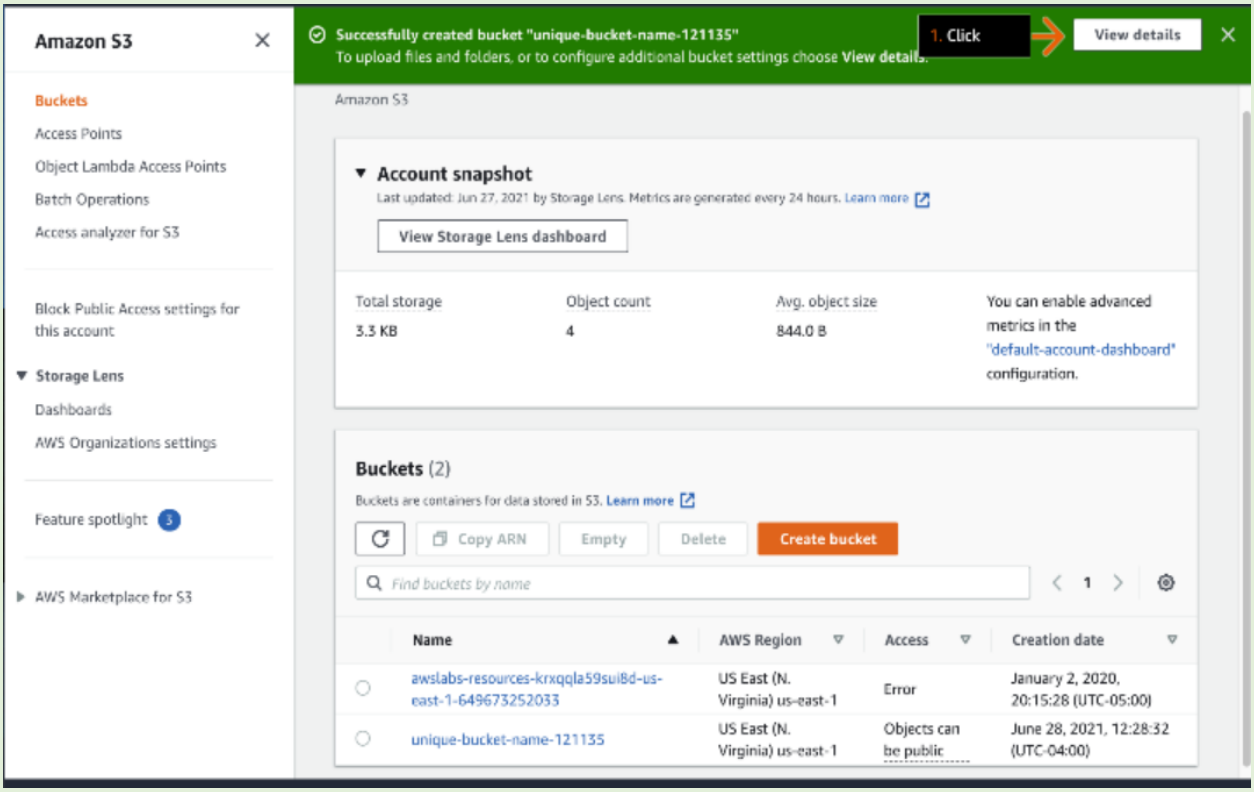


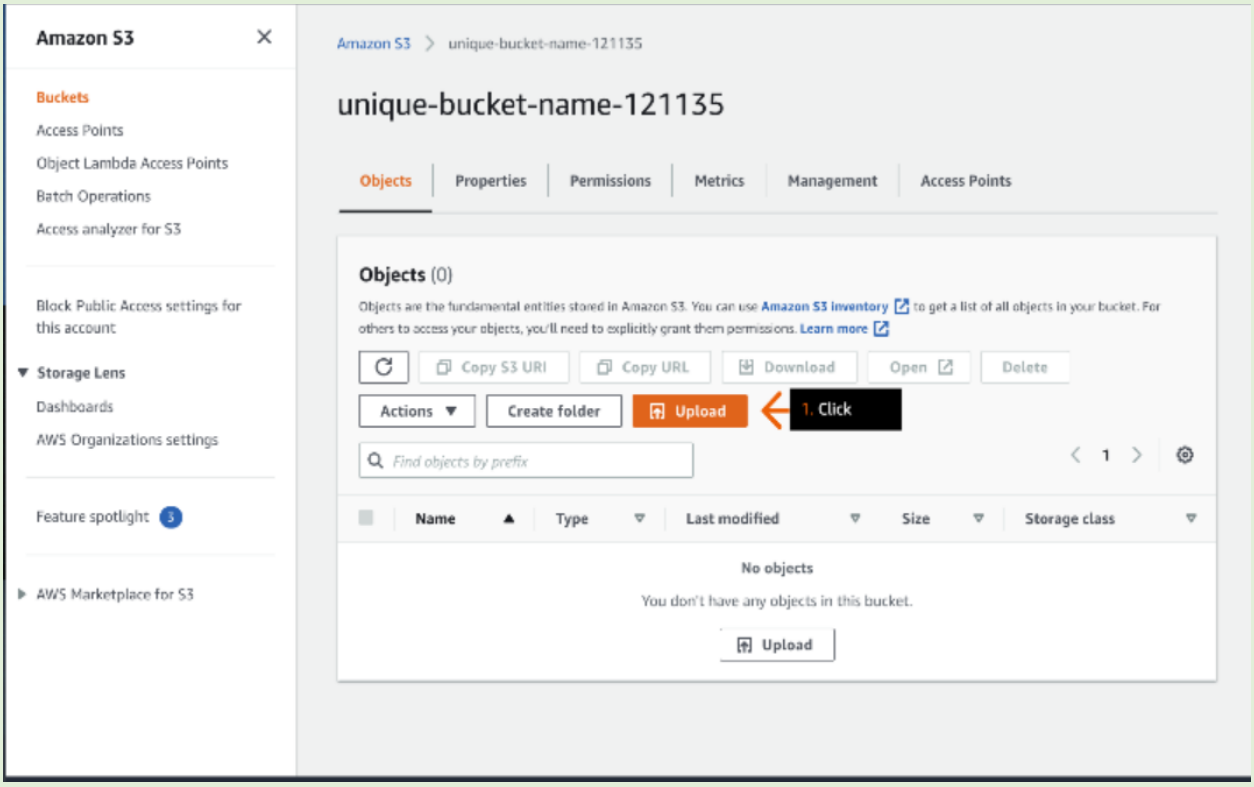

Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
Amazon S3 > Create bucket
Create bucket Info
Buckets are containers for data stored in S3. Learn more
General configuration
Bucket name
lab-unique-name-123
1. Type
Bucket name must be unique and must not contain spaces or uppercase letters. See rules for bucket naming
AWS Region
US East (N. Virginia) us-east-1
2. Choose
Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
Choose bucket
3. Scroll
Object Ownership Info
Control ownership of objects written to this bucket from other AWS accounts and granted using access control lists (ACLs). Object ownership determines who can specify access to objects.
ACLs disabled (recommended)
All objects in this bucket are owned by this account.
ACLs enabled
Objects in this bucket can be owned by other AWS

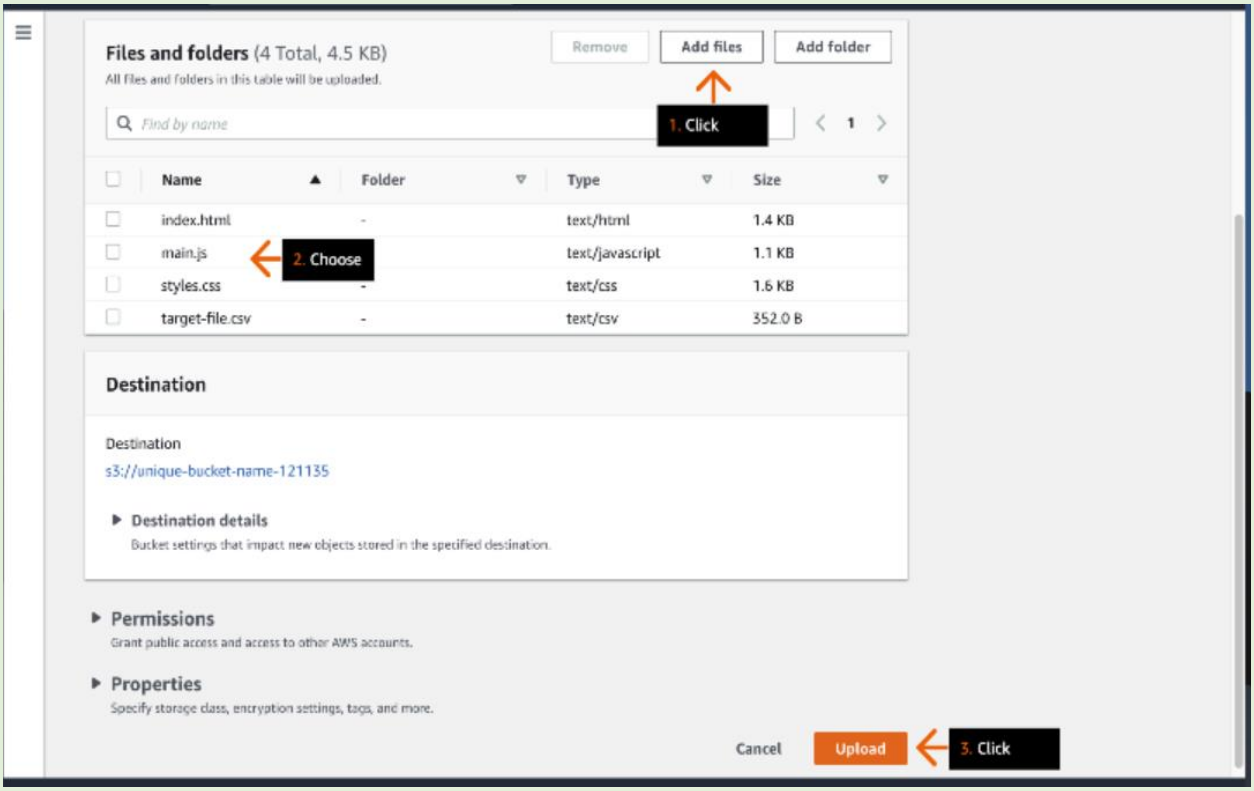

Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
Choose bucket
Object Ownership Info
Control ownership of objects written to this bucket from other AWS accounts and granted using access control lists (ACLs). Object ownership determines who can specify access to objects.
ACLs disabled (recommended)
All objects in this bucket are owned by this account.
Access to this bucket and its objects is specified using only policies.
ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.
1. Choose
Object Ownership
Bucket owner preferred
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.
Object writer
2. Choose
3. Scroll
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

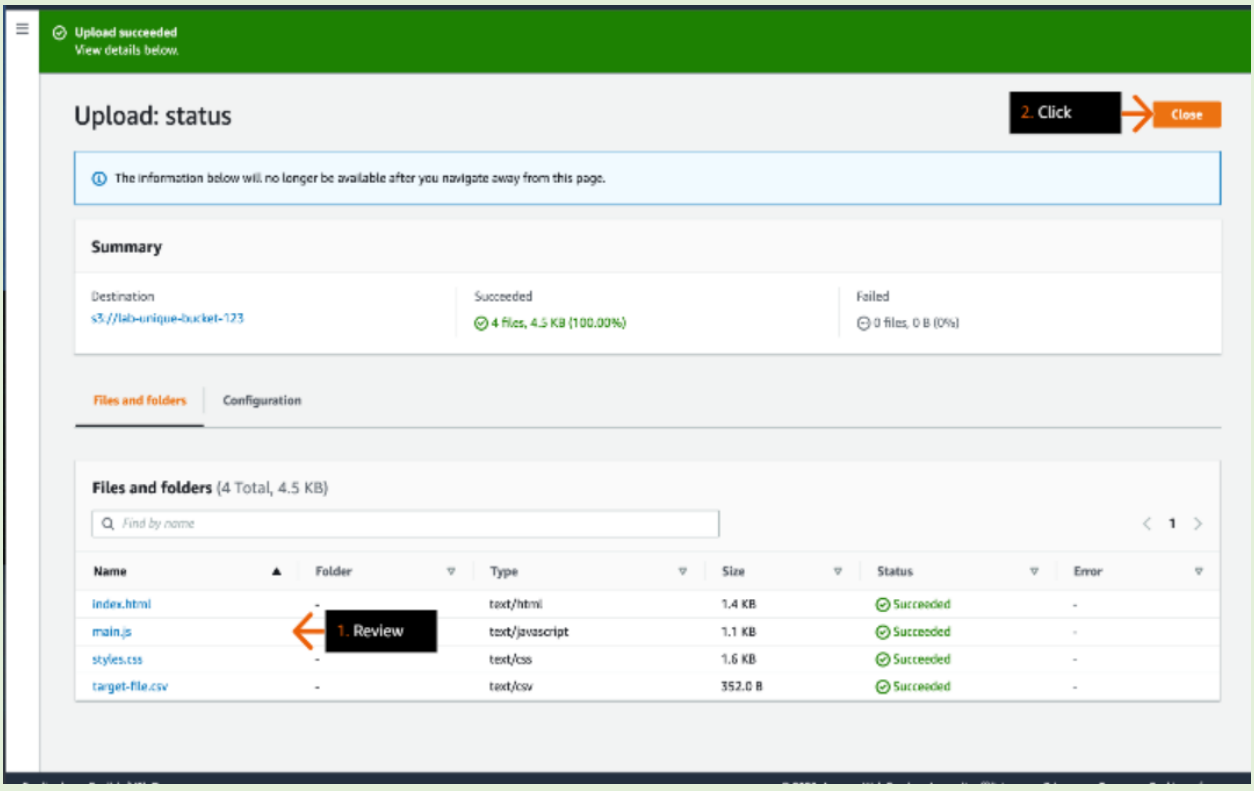

Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings 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.
1. Clear
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.
Turning off block all public access might result in this bucket and the objects within becoming public
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.
2. Choose
I acknowledge that the current settings might result in this bucket and the objects within becoming public.

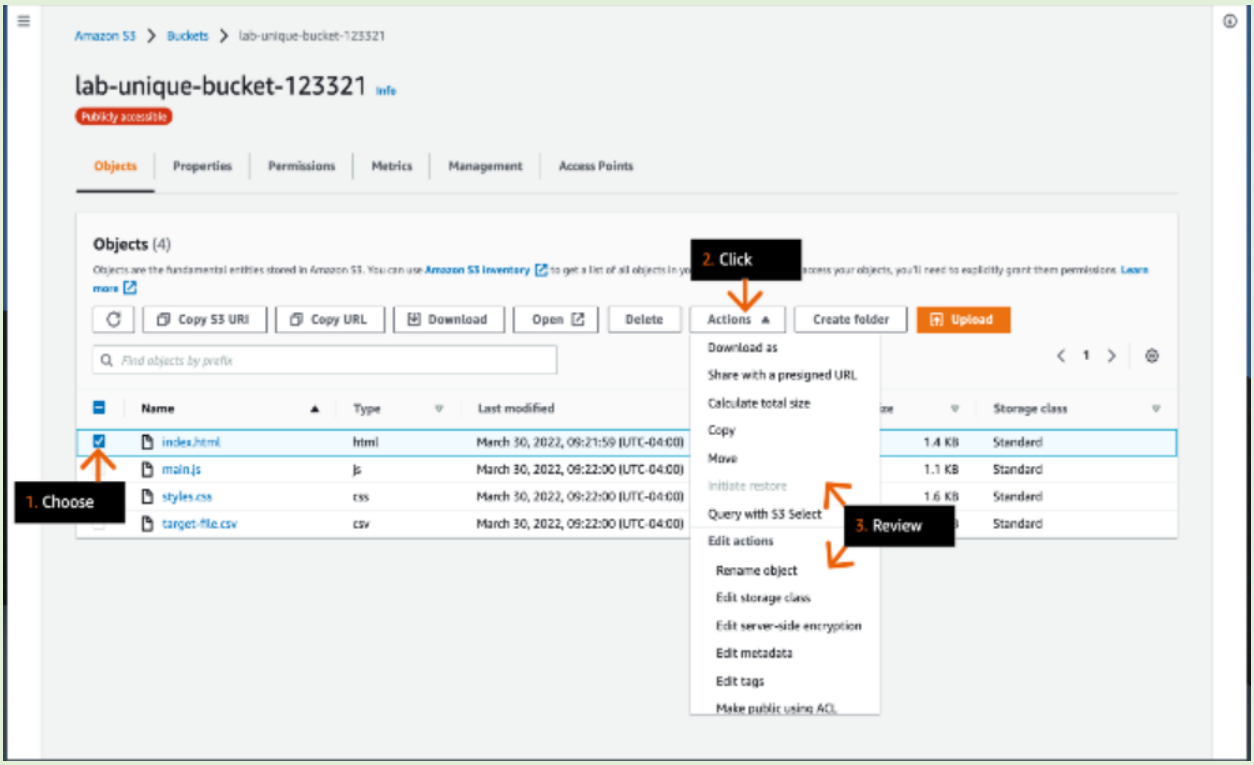

Add tag
1. Scroll
Default encryption Info
Server-side encryption is automatically applied to new objects stored in this bucket.
Encryption type Info
Server-side encryption with Amazon S3 managed keys (SSE-S3)
2. Keep default
Server-side encryption with AWS Key Management Service keys (SSE-KMS)
Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Management & insights tab of the Amazon S3 pricing page.
Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more
Disable
Enable
3. Keep default
Advanced settings
After creating the bucket, you can upload files and folders to the bucket, and configure additional t
4. Click
Cancel
Create bucket

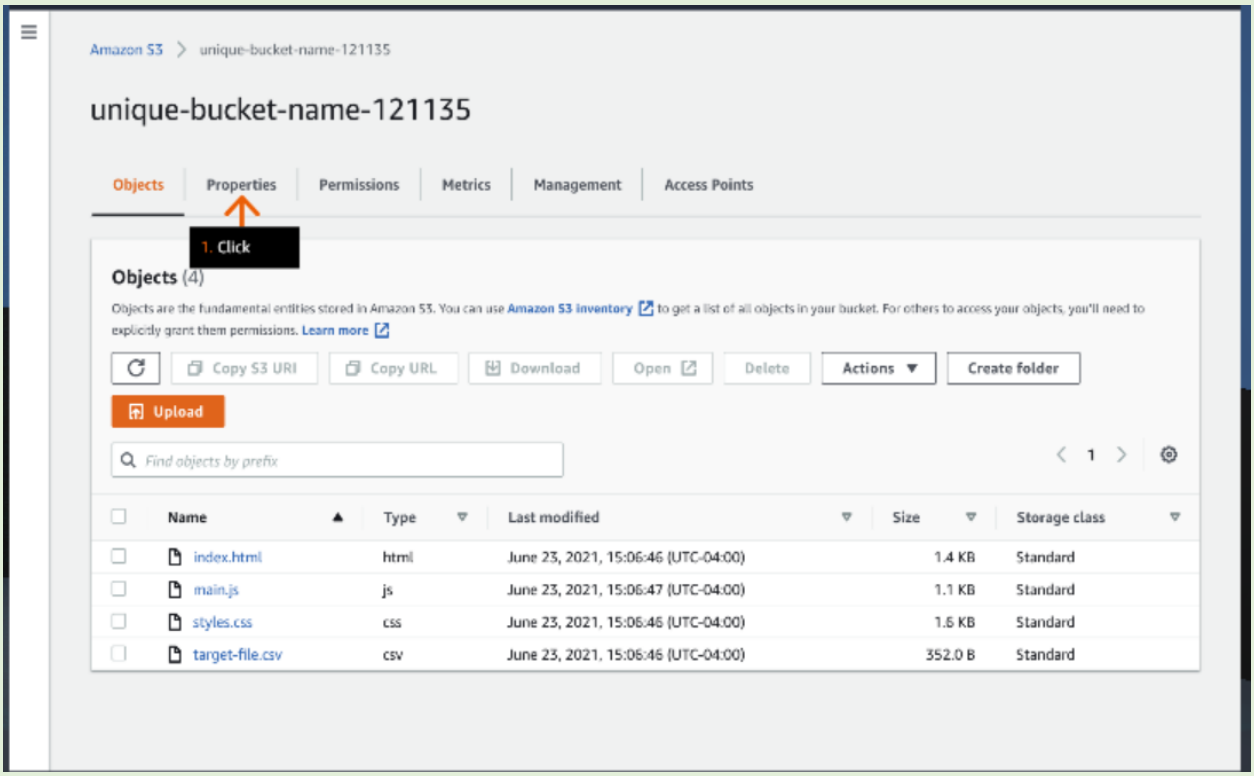

Amazon S3
Buckets
Access Points
Object Lambda Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
Successfully created bucket "unique-bucket-name-121135"
To upload files and folders, or to configure additional bucket settings choose View details.
1. Click
View details
Amazon S3
Account snapshot
Last updated: Jun 27, 2021 by Storage Lens. Metrics are generated every 24 hours. Learn more
View Storage Lens dashboard
Total storage
3.3 KB
Object count
4
Avg. object size
844.0 B
You can enable advanced metrics in the "default-account-dashboard" configuration.
Buckets (2)
Buckets are containers for data stored in S3. Learn more
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
Access
Creation date
awslabs-resources-krxqqla59sui8d-us-east-1-649673252033
US East (N. Virginia) us-east-1
Error
January 2, 2020, 20:15:28 (UTC-05:00)
unique-bucket-name-121135
US East (N. Virginia) us-east-1
Objects can be public
June 28, 2021, 12:28:32 (UTC-04:00)

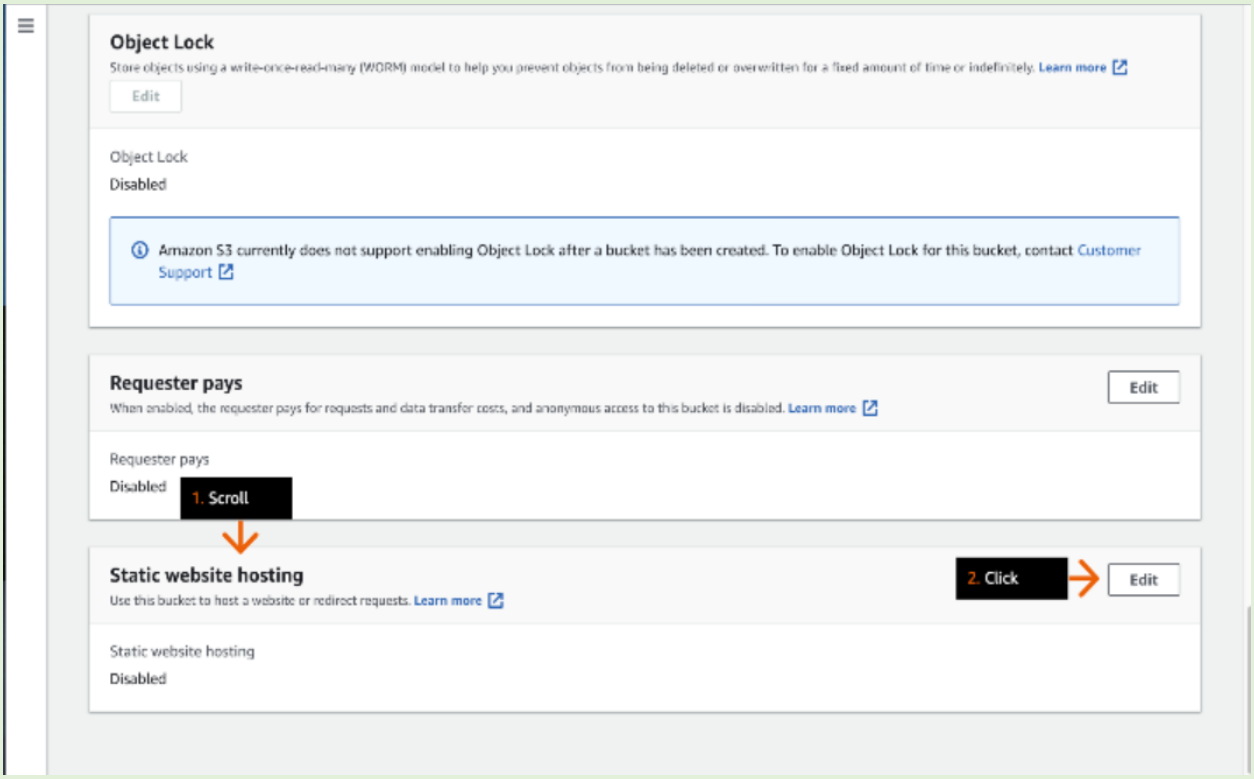

Amazon S3
Buckets
Access Points
Object Lambda Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
Amazon S3 > unique-bucket-name-121135
unique-bucket-name-121135
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (0)
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
1. Click
Find objects by prefix
Name
Type
Last modified
Size
Storage class
No objects
You don't have any objects in this bucket.
Upload

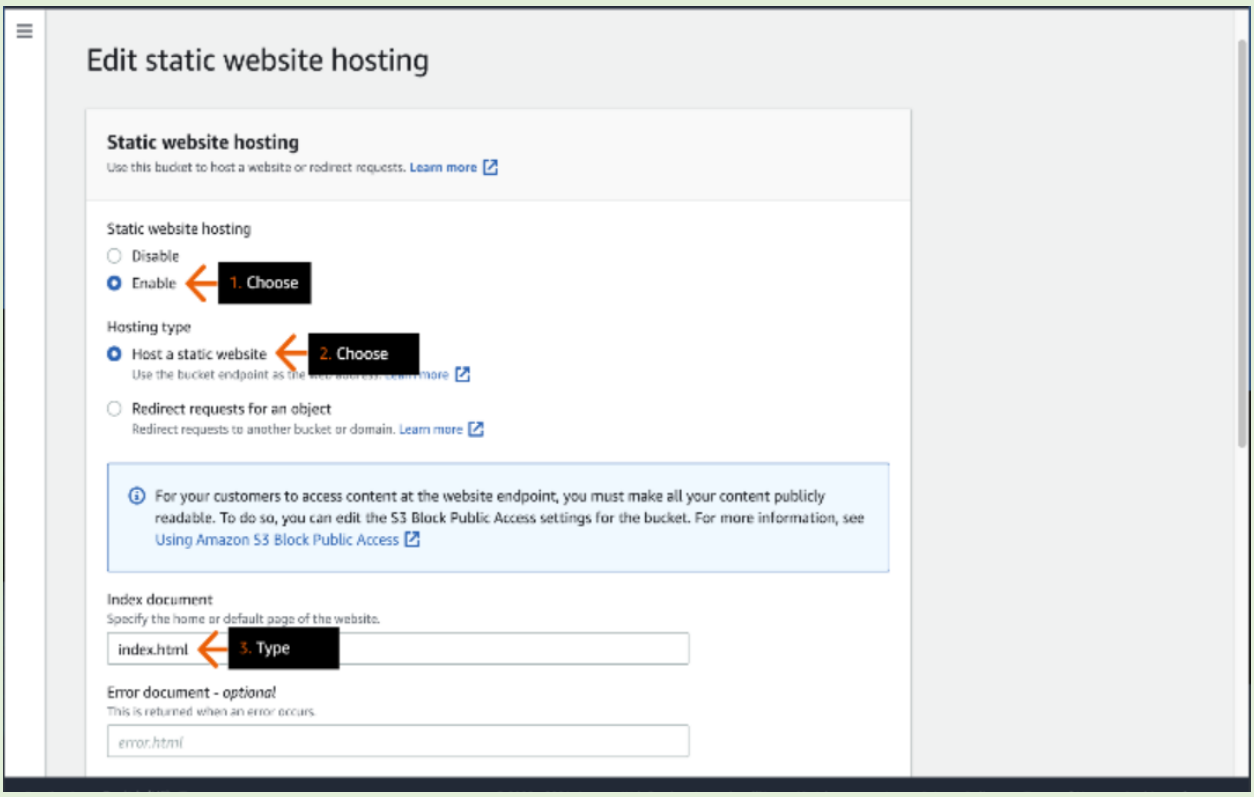

Files and folders (4 Total, 4.5 KB)
All files and folders in this table will be uploaded.
Remove
Add files
Add folder
Find by name
1. Click
Name
Folder
Type
Size
index.html
text/html
1.4 KB
main.js
2. Choose
text/javascript
1.1 KB
styles.css
text/css
1.6 KB
target-file.csv
text/csv
352.0 B
Destination
Destination
s3://unique-bucket-name-121135
Destination details
Bucket settings that impact new objects stored in the specified destination.
Permissions
Grant public access and access to other AWS accounts.
Properties
Specify storage class, encryption settings, tags, and more.
Cancel
Upload
3. Click

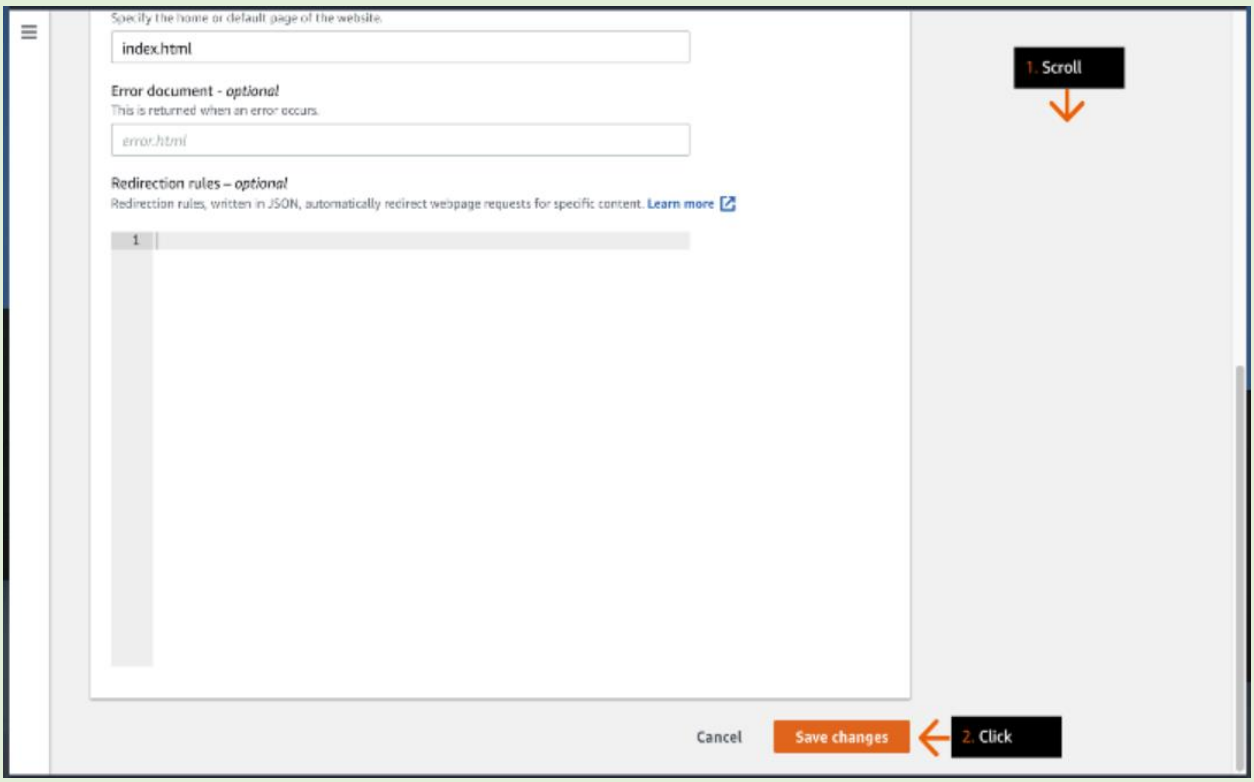

Upload succeeded
View details below.
Upload: status
2. Click
Close
The information below will no longer be available after you navigate away from this page.
Summary
Destination
s3://lab-unique-bucket-123
Succeeded
4 files, 4.5 KB (100.00%)
Failed
0 files, 0 B (0%)
Files and folders
Configuration
Files and folders (4 Total, 4.5 KB)
Find by name
Name
Folder
Type
Size
Status
Error
index.html
text/html
1.4 KB
Succeeded
main.js
1. Review
text/javascript
1.1 KB
Succeeded
styles.css
text/css
1.6 KB
Succeeded
target-file.csv
text/csv
352.0 B
Succeeded

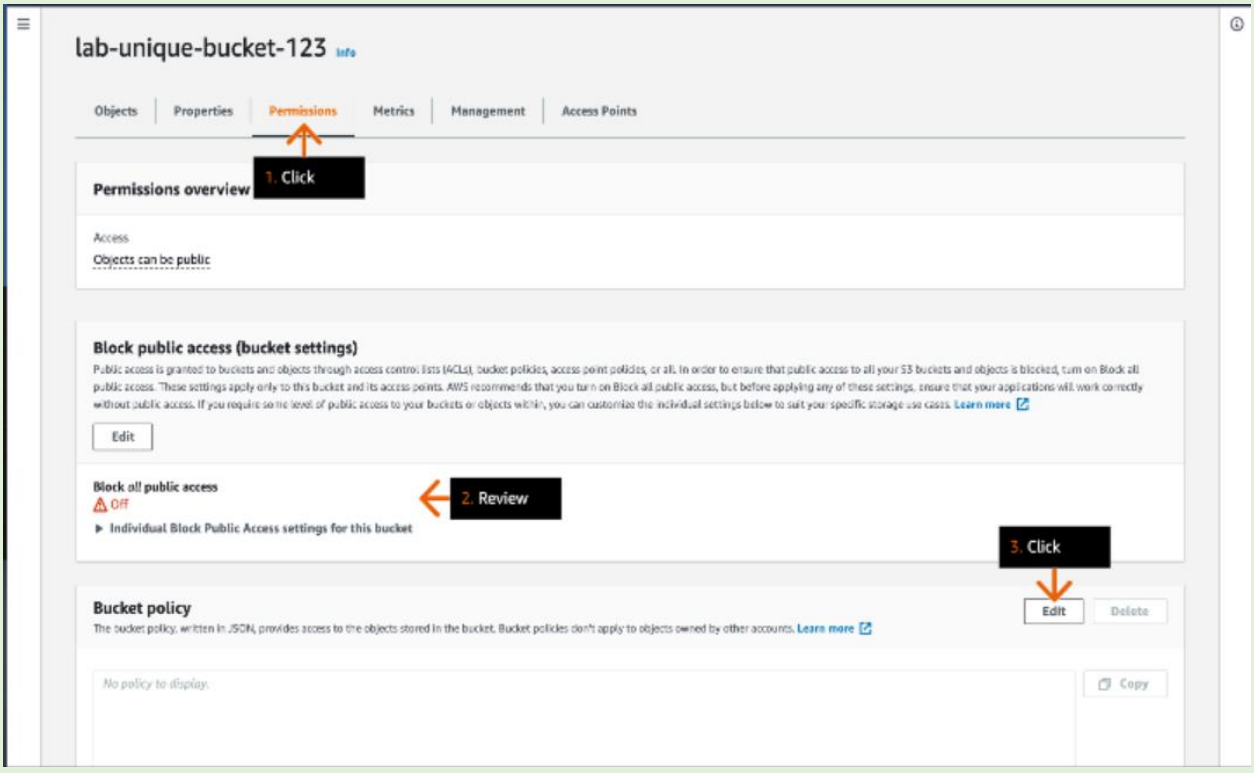

Amazon S3 > Buckets > lab-unique-bucket-123321
lab-unique-bucket-123321 Info
Publicly accessible
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (4)
2. Click
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Find objects by prefix
Name
Type
Last modified
Storage class
index.html
html
March 30, 2022, 09:21:59 (UTC-04:00)
1.4 KB
Standard
main.js
js
March 30, 2022, 09:22:00 (UTC-04:00)
1.1 KB
Standard
styles.css
css
March 30, 2022, 09:22:00 (UTC-04:00)
1.6 KB
Standard
target-file.csv
csv
March 30, 2022, 09:22:00 (UTC-04:00)
Standard
1. Choose
Download as
Share with a presigned URL
Calculate total size
Copy
Move
Initiate restore
Query with S3 Select
3. Review
Edit actions
Rename object
Edit storage class
Edit server-side encryption
Edit metadata
Edit tags
Make public using ACL

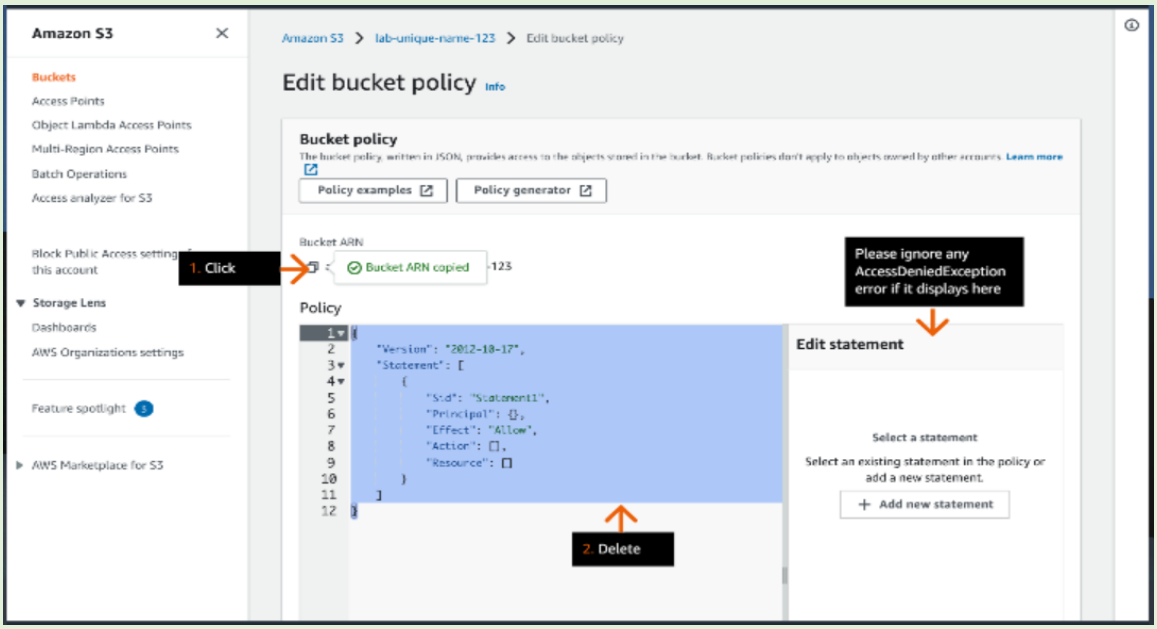

Amazon S3 > unique-bucket-name-121135
unique-bucket-name-121135
Objects
Properties
Permissions
Metrics
Management
Access Points
1. Click
Objects (4)
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Find objects by prefix
Name
Type
Last modified
Size
Storage class
index.html
html
June 23, 2021, 15:06:46 (UTC-04:00)
1.4 KB
Standard
main.js
js
June 23, 2021, 15:06:47 (UTC-04:00)
1.1 KB
Standard
styles.css
css
June 23, 2021, 15:06:46 (UTC-04:00)
1.6 KB
Standard
target-file.csv
csv
June 23, 2021, 15:06:46 (UTC-04:00)
352.0 B
Standard


Object Lock
Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Learn more
Edit
Object Lock
Disabled
Amazon S3 currently does not support enabling Object Lock after a bucket has been created. To enable Object Lock for this bucket, contact Customer Support
Requester pays
When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. Learn more
Edit
Requester pays
Disabled
1. Scroll
Static website hosting
Use this bucket to host a website or redirect requests. Learn more
2. Click
Edit
Static website hosting
Disabled

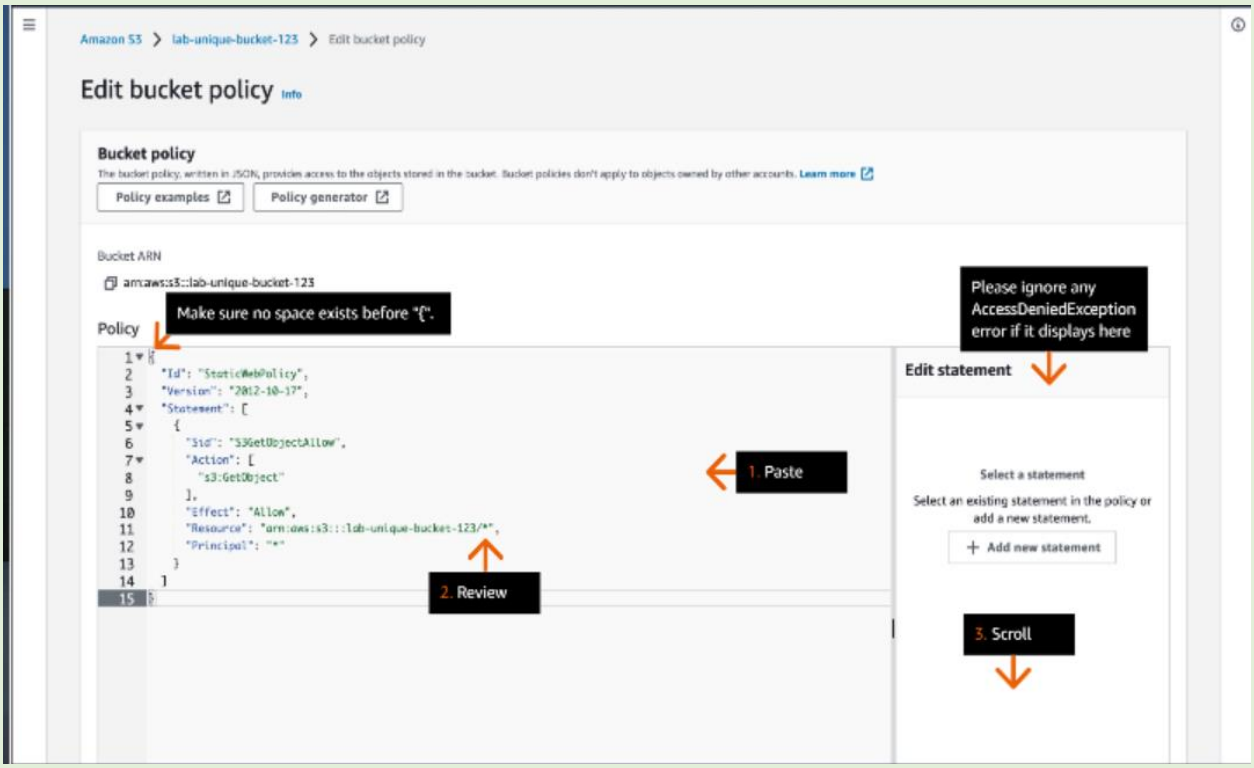

Edit static website hosting
Static website hosting
Use this bucket to host a website or redirect requests. Learn more
Static website hosting
Disable
Enable
1. Choose
Hosting type
Host a static website
2. Choose
Use the bucket endpoint as the
Redirect requests for an object
Redirect requests to another bucket or domain. Learn more
For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see Using Amazon S3 Block Public Access
Index document
Specify the home or default page of the website.
index.html
3. Type
Error document - optional
This is returned when an error occurs.
error.html

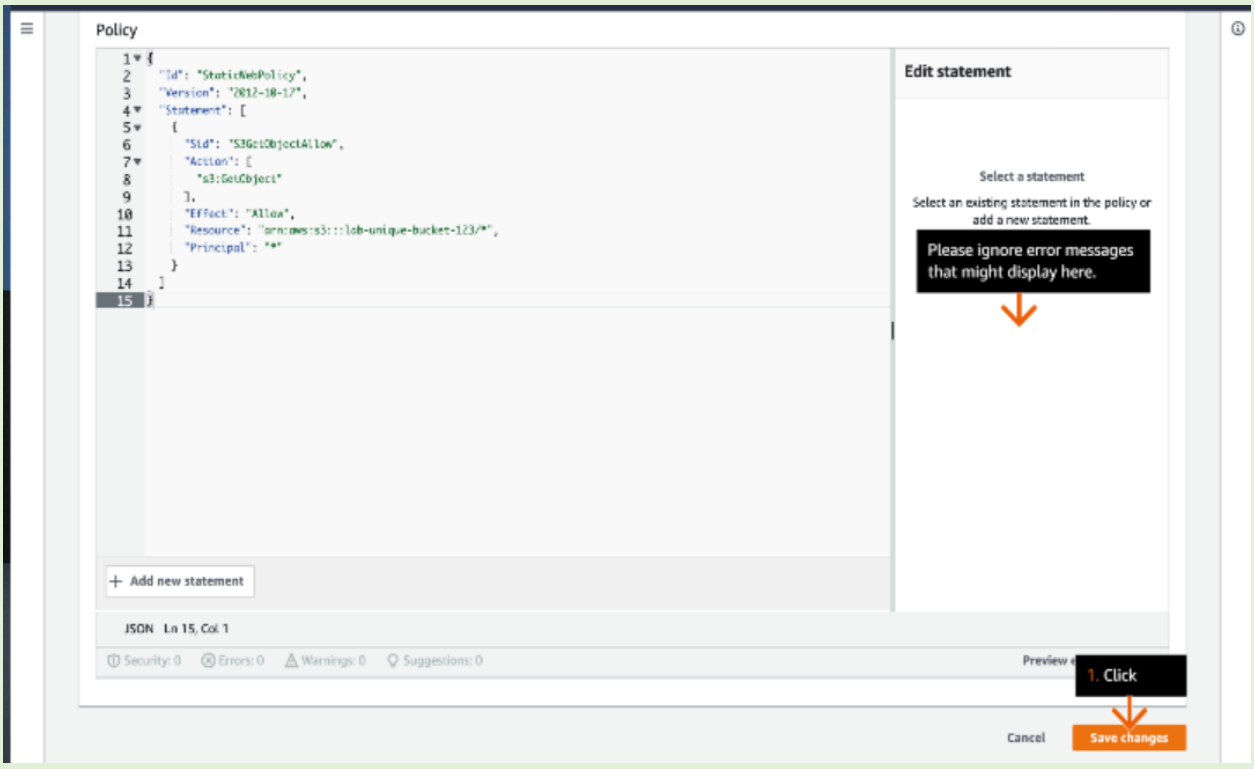

Specify the home or default page of the website.
index.html
Error document - optional
This is returned when an error occurs.
error.html
Redirection rules – optional
Redirection rules, written in JSON, automatically redirect webpage requests for specific content. Learn more
1
1. Scroll
Cancel
Save changes
2. Click

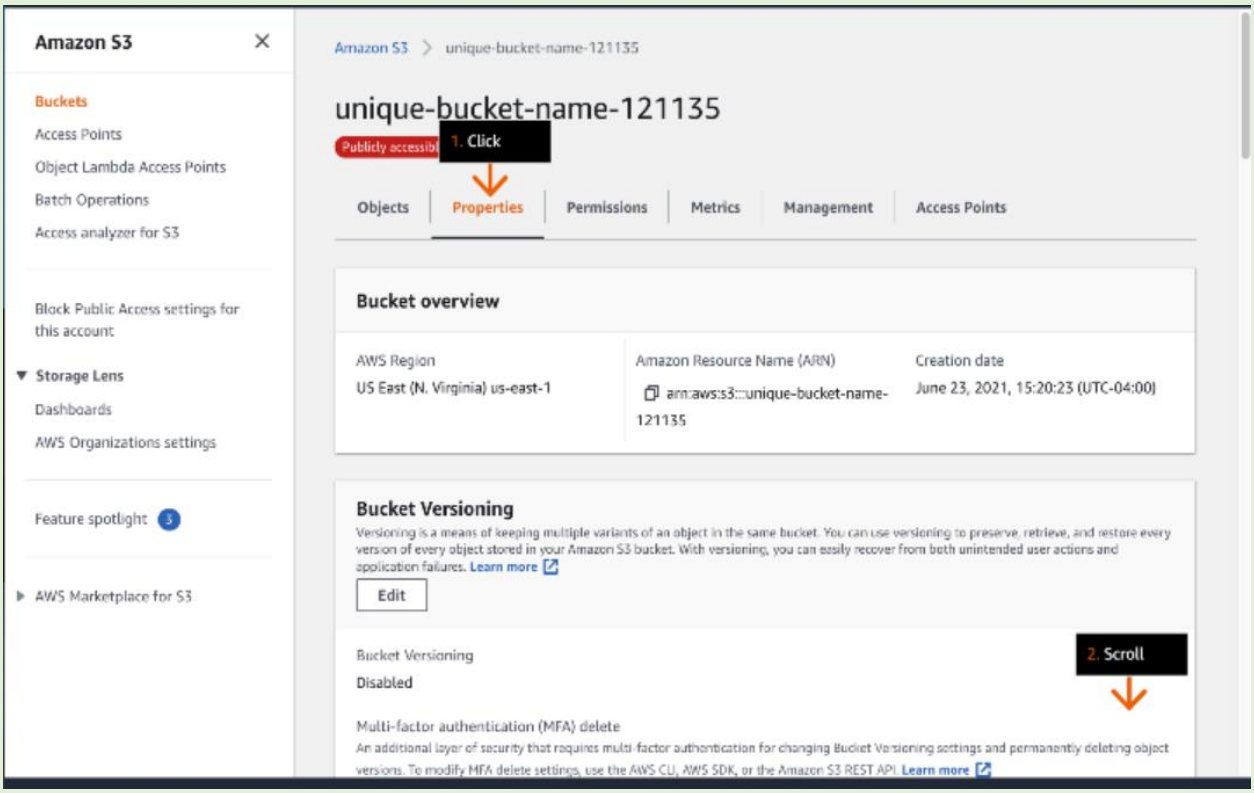

lab-unique-bucket-123 Info
Objects
Properties
Permissions
Metrics
Management
Access Points
1. Click
Permissions overview
Access
Objects can be public
Block public access (bucket settings)
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point 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
Edit
Block all public access
Off
Individual Block Public Access settings for this bucket
2. Review
3. Click
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
Edit
Delete
No policy to display.
Copy

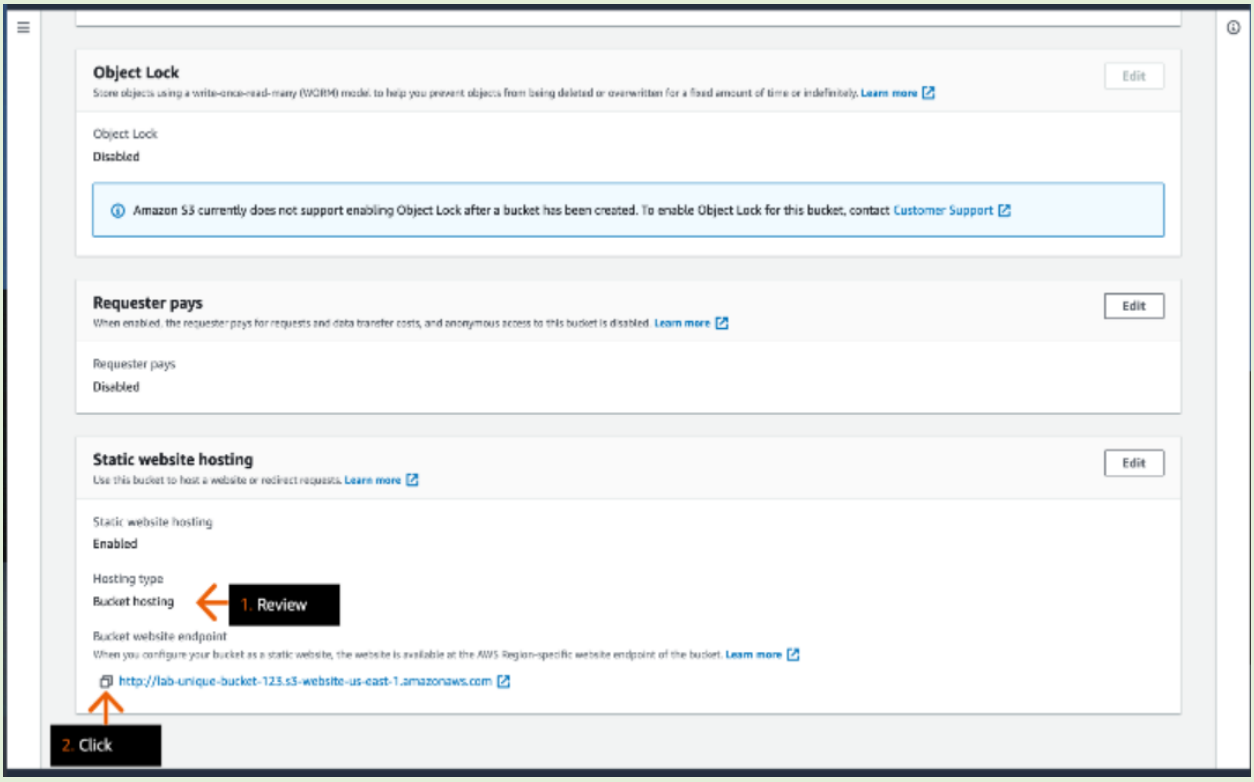


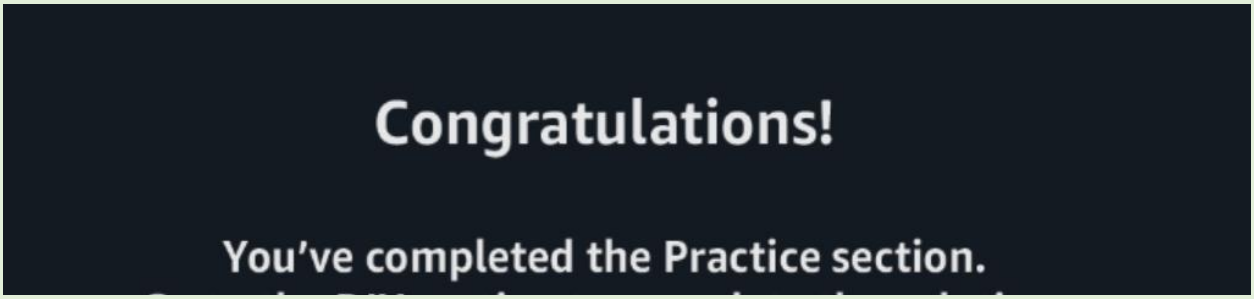
Open you policy file and copy & paste there, replace with ARN.

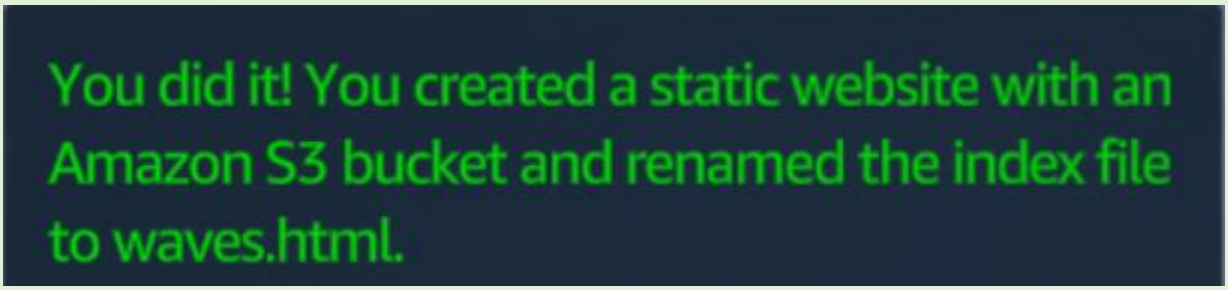

Amazon S3 > lab-unique-bucket-123 > Edit bucket policy
Edit bucket policy Info
Bucket policy
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more
Policy examples
Policy generator
Bucket ARN
arn:aws:s3:::lab-unique-bucket-123
Policy
Make sure no space exists before "{".
Please ignore any AccessDeniedException error if it displays here
Edit statement
1. Paste
2. Review
Select a statement
Select an existing statement in the policy or add a new statement.
+ Add new statement
3. Scroll


Policy
Edit statement
Select a statement
Select an existing statement in the policy or add a new statement.
Please ignore error messages that might display here.
+ Add new statement
JSON Ln 15, Col 1
Security: 0
Errors: 0
Warnings: 0
Suggestions: 0
1. Click
Cancel
Save changes


Amazon S3
Buckets
Access Points
Object Lambda Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Amazon S3 > unique-bucket-name-121135
unique-bucket-name-121135
1. Click
Objects
Properties
Permissions
Metrics
Management
Access Points
Bucket overview
AWS Region
US East (N. Virginia) us-east-1
Amazon Resource Name (ARN)
arn:aws:s3:::unique-bucket-name-121135
Creation date
June 23, 2021, 15:20:23 (UTC-04:00)
Bucket Versioning
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more
Edit
Bucket Versioning
Disabled
2. Scroll
Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more


Object Lock
Edit
Object Lock
Disabled
Amazon S3 currently does not support enabling Object Lock after a bucket has been created. To enable Object Lock for this bucket, contact Customer Support
Requester pays
Edit
Requester pays
Disabled
Static website hosting
Edit
Static website hosting
Enabled
Hosting type
Bucket hosting
1. Review
Bucket website endpoint
http://lab-unique-bucket-123.s3-website-us-east-1.amazonaws.com
2. Click





Author: Ritik Kumar Tiwari