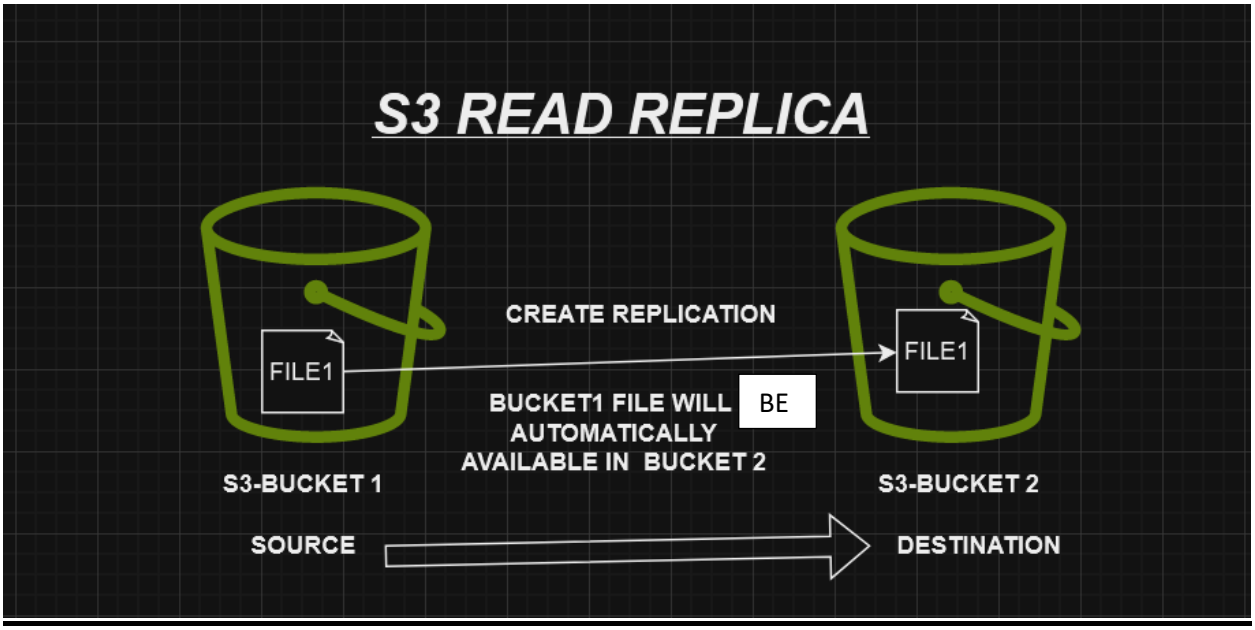
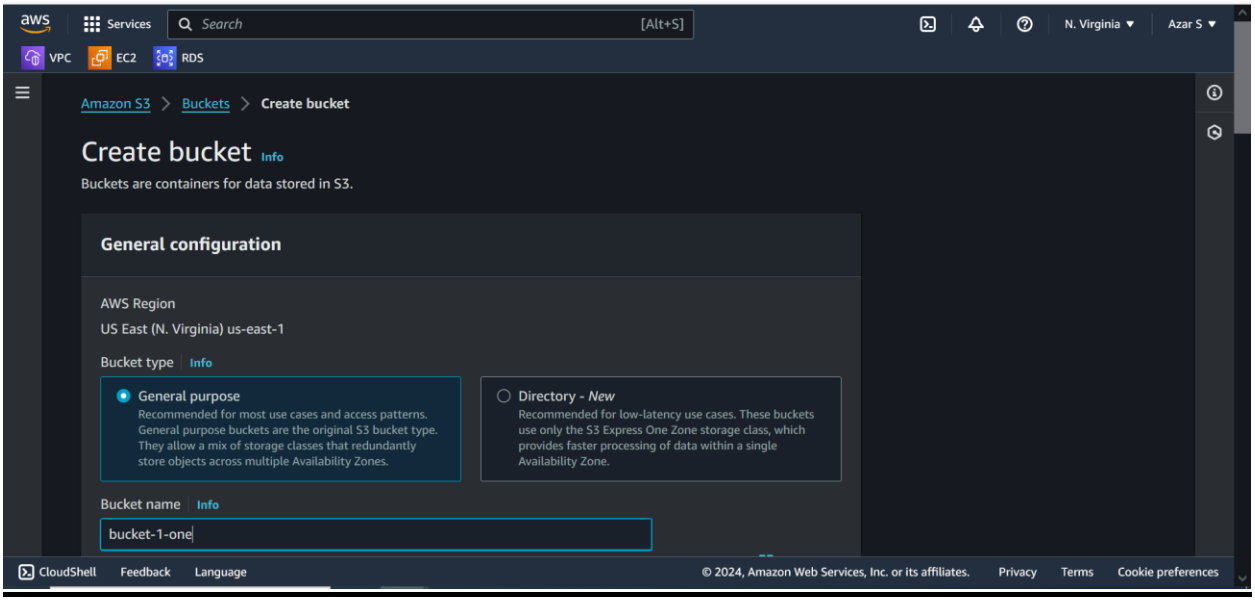
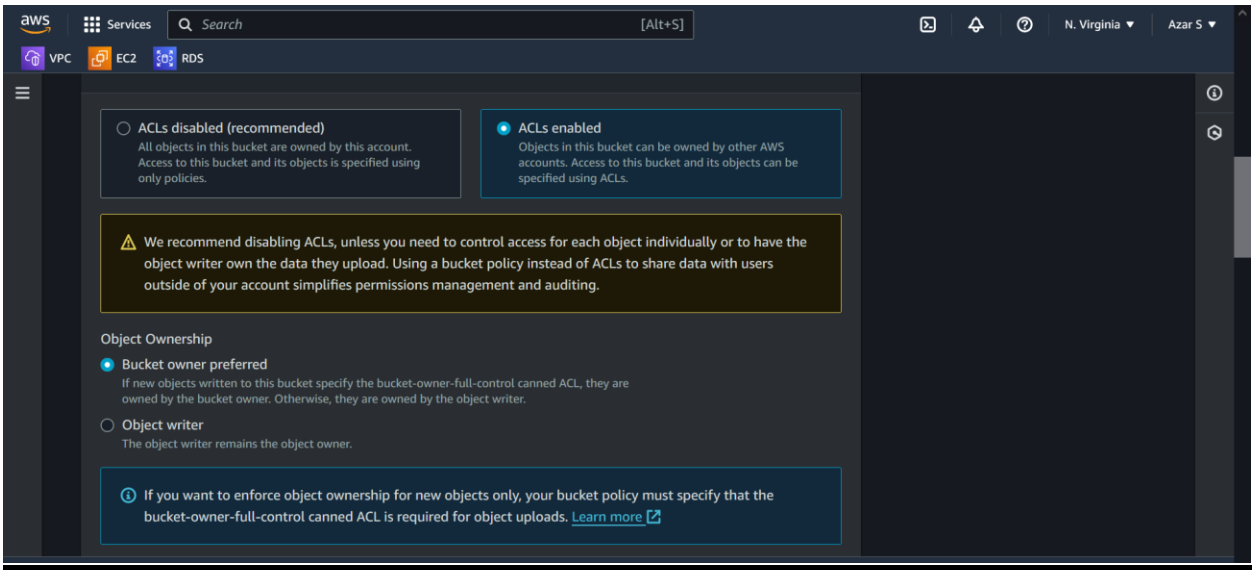
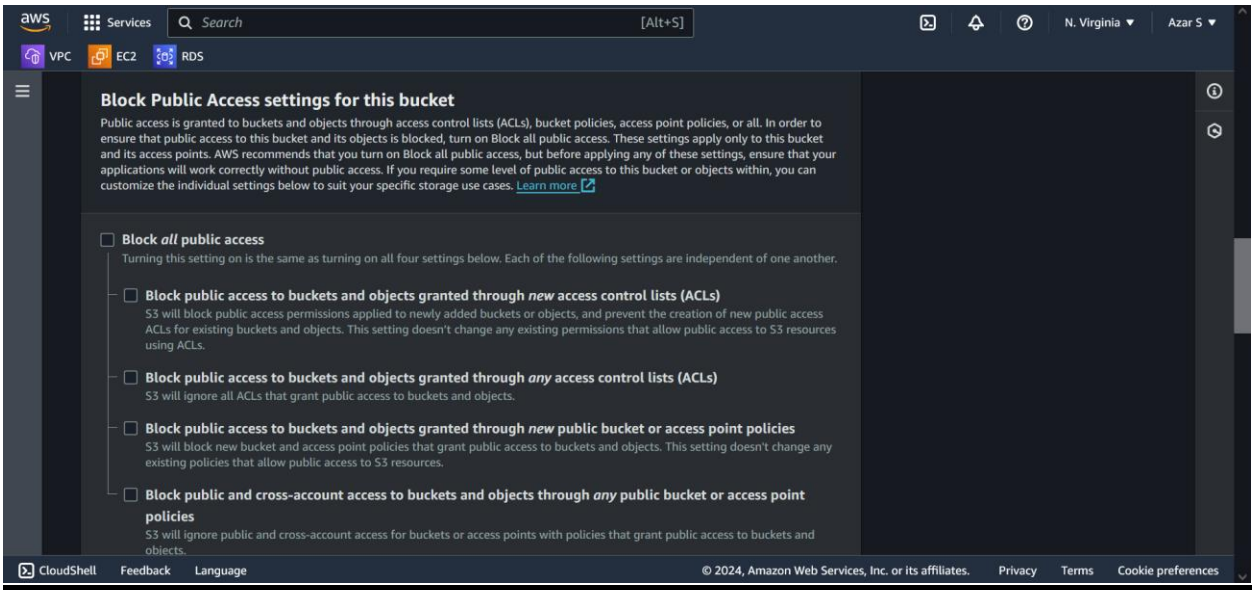
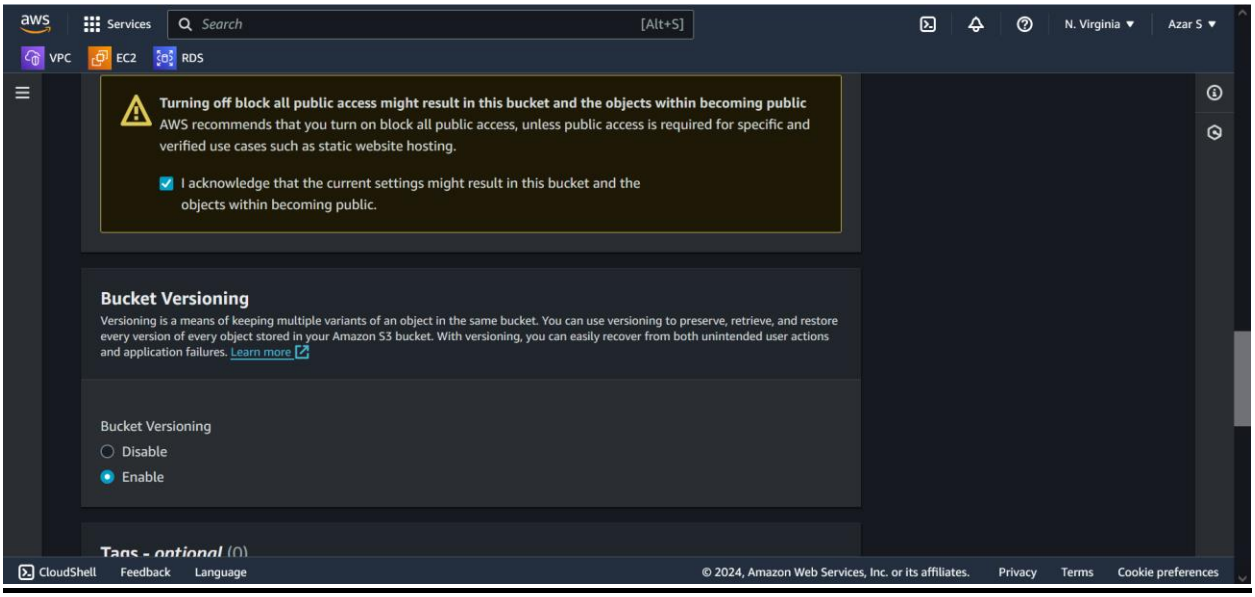
S3 READ REPLICA:

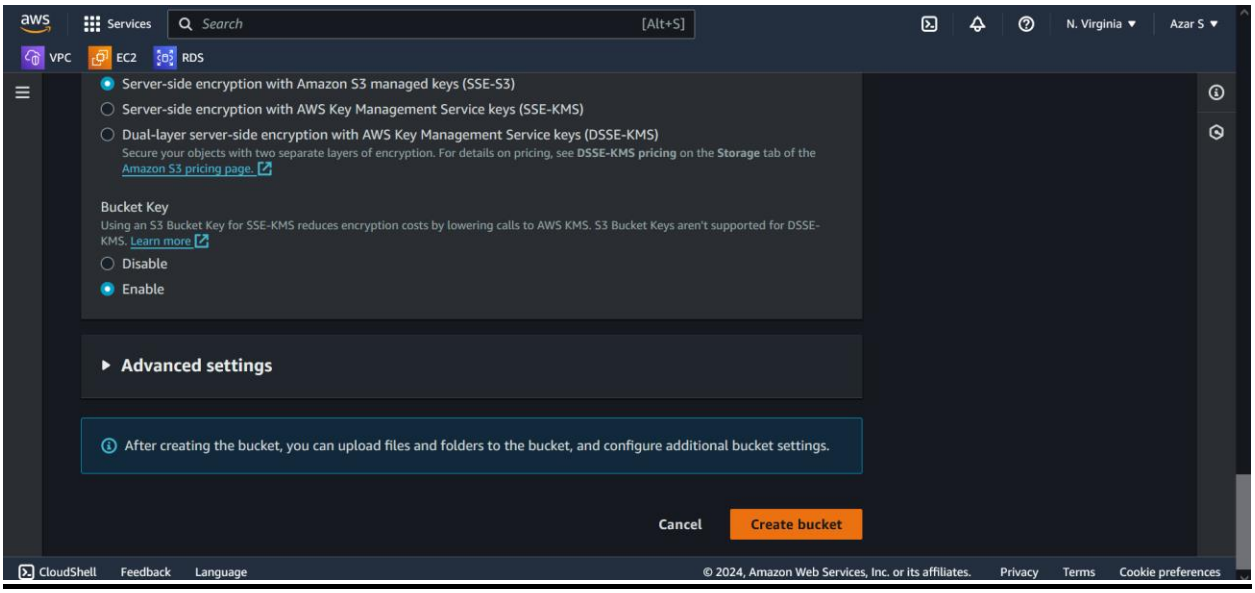


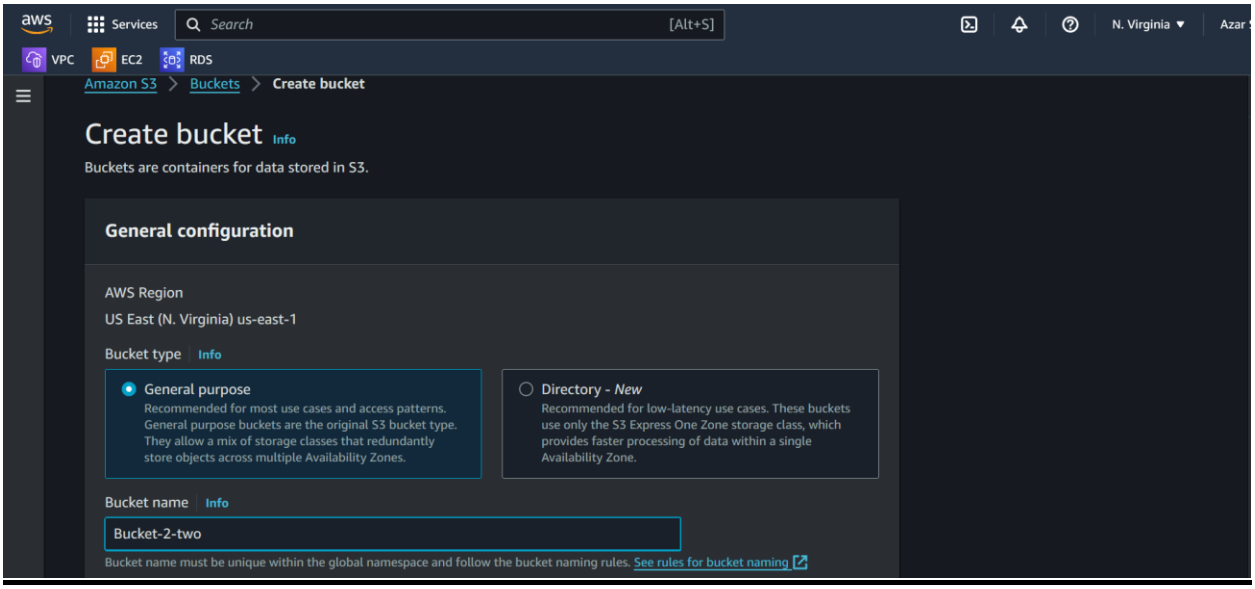


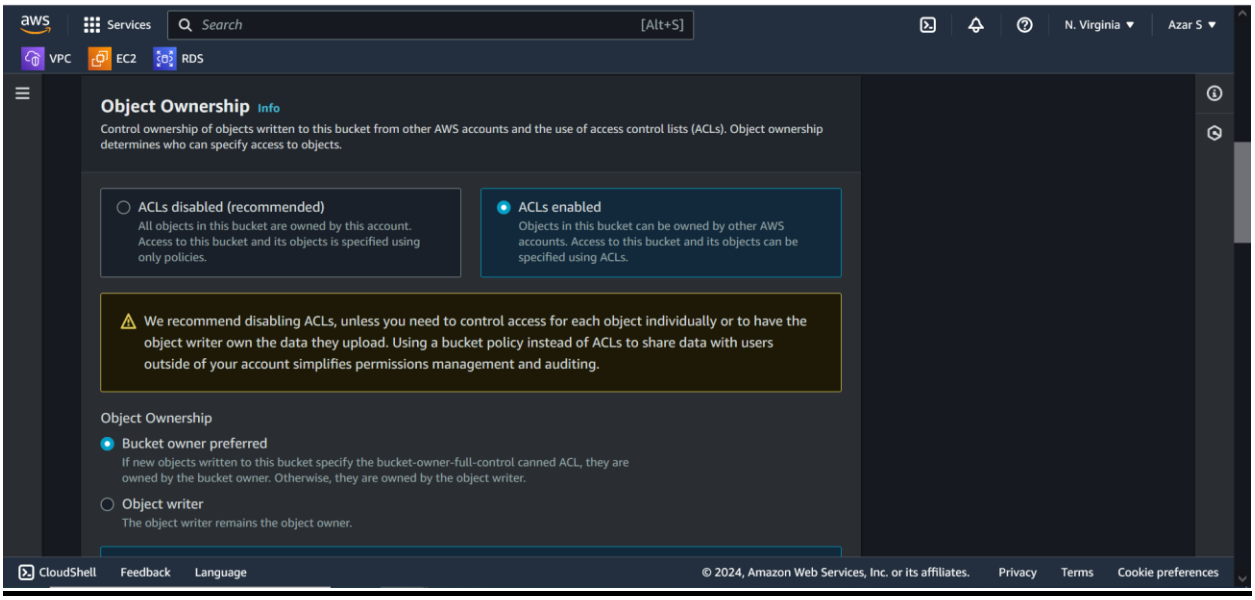

aws
Services
Search
[Alt+S]
N. Virginia
Azar S
VPC
EC2
RDS
ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.
We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.
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
The object writer remains the object owner.
If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. Learn more

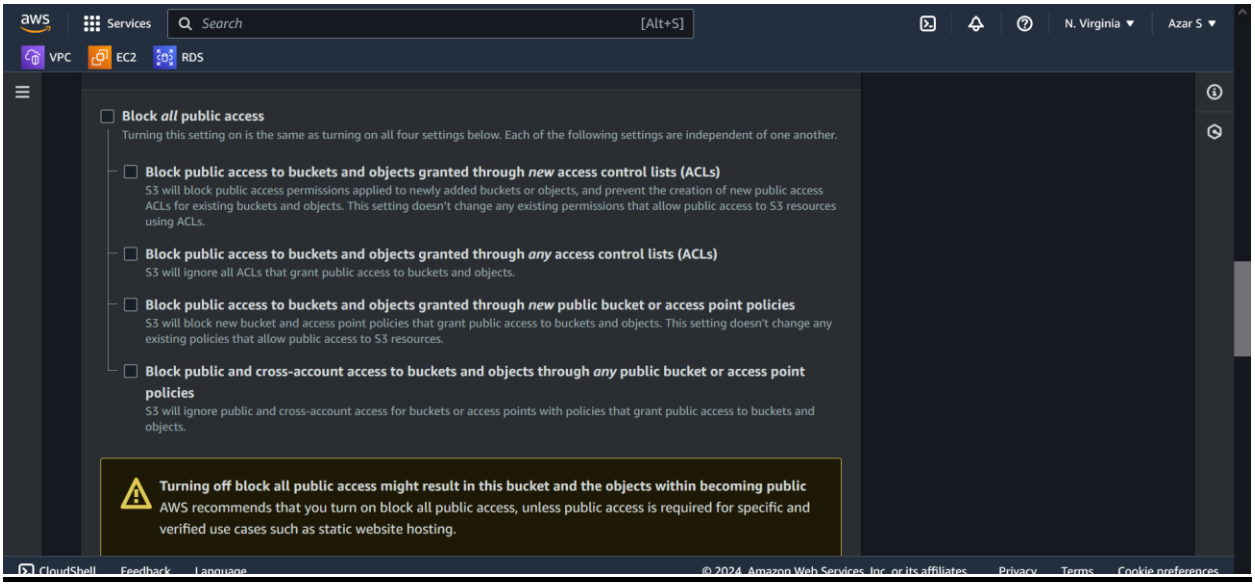

aws
Services
Search
[Alt+S]
N. Virginia
Azar S
VPC
EC2
RDS
Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects 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.
CloudShell
Feedback
Language
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

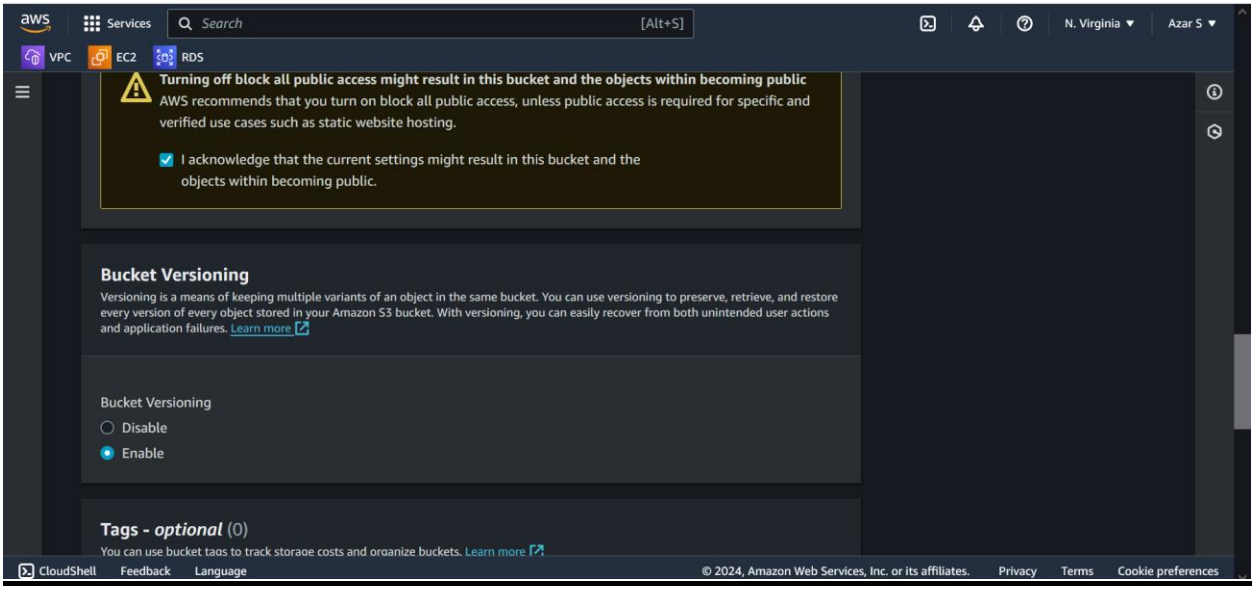

aws
Services
Search
[Alt+S]
N. Virginia
Azar S
VPC
EC2
RDS
Turning off block all public access might result in this bucket and the objects within becoming public
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.
I acknowledge that the current settings might result in this bucket and the objects within becoming public.
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
Bucket Versioning
Disable
Enable
Tags - optional (0)
CloudShell
Feedback
Language
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

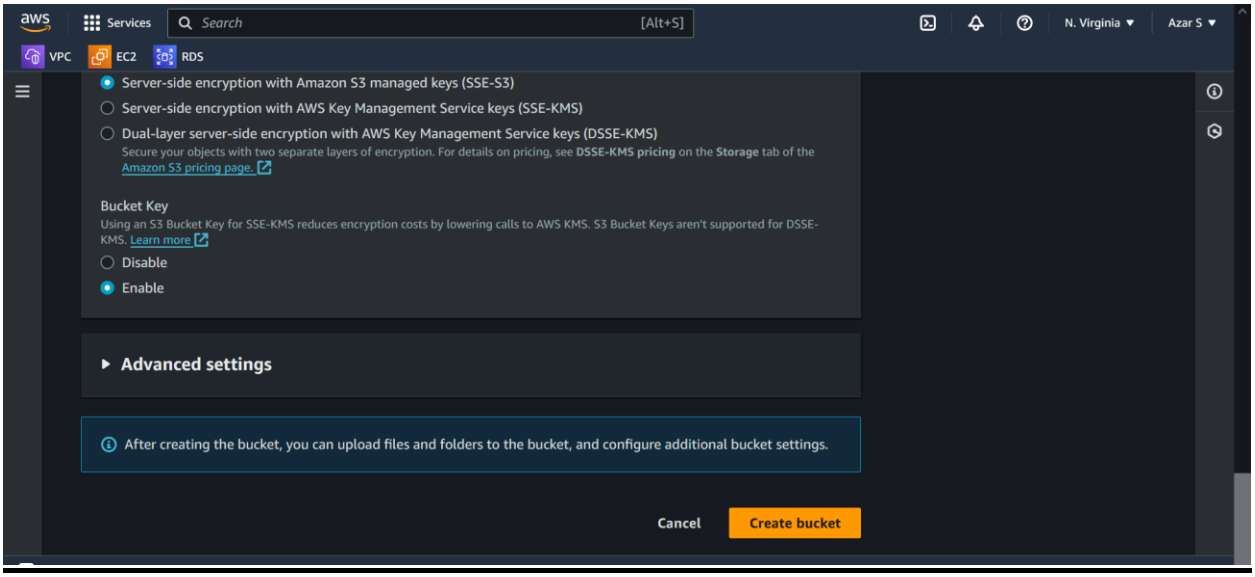

aws
Services
Search
[Alt+S]
N. Virginia
Azar S
VPC
EC2
RDS
Server-side encryption with Amazon S3 managed keys (SSE-S3)
Server-side encryption with AWS Key Management Service keys (SSE-KMS)
Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage 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
Advanced settings
After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.
Cancel
Create bucket
CloudShell
Feedback
Language
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

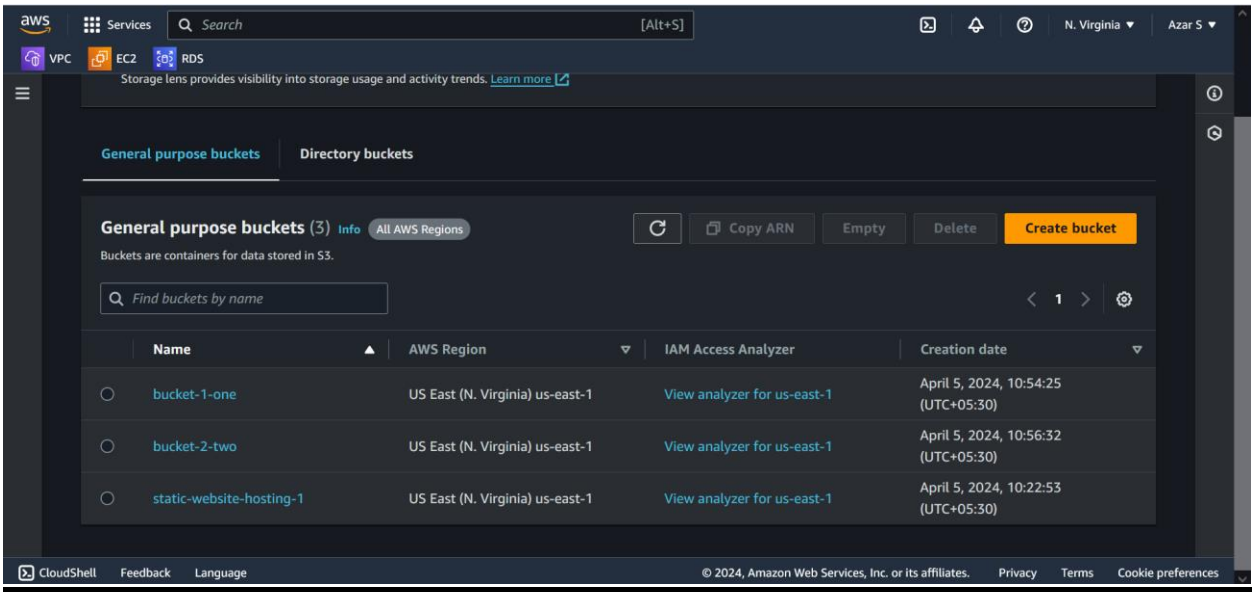

aws
Services
Search
[Alt+S]
N. Virginia
VPC
EC2
RDS
Amazon S3 > Buckets > Create bucket
Create bucket Info
Buckets are containers for data stored in S3.
General configuration
AWS Region
US East (N. Virginia) us-east-1
Bucket type Info
General purpose
Recommended for most use cases and access patterns. 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 - New
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
Bucket-2-two
Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

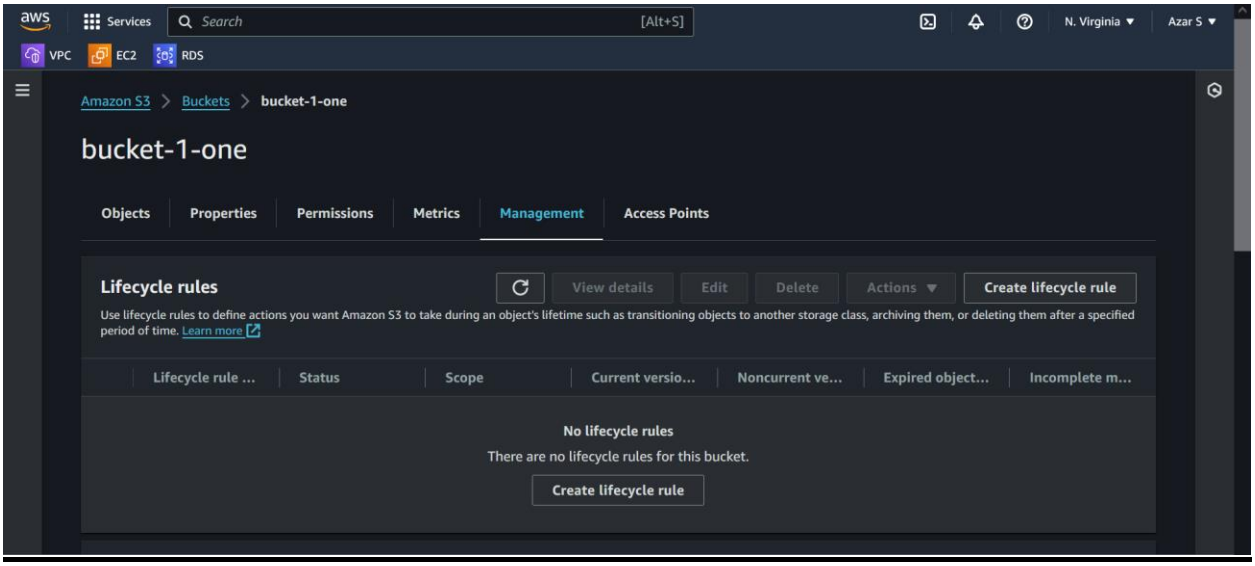

aws
Services
Search
[Alt+S]
N. Virginia
Azar S
VPC
EC2
RDS
Object Ownership Info
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
ACLs disabled (recommended)
All objects 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.
We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.
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
The object writer remains the object owner.
CloudShell
Feedback
Language
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

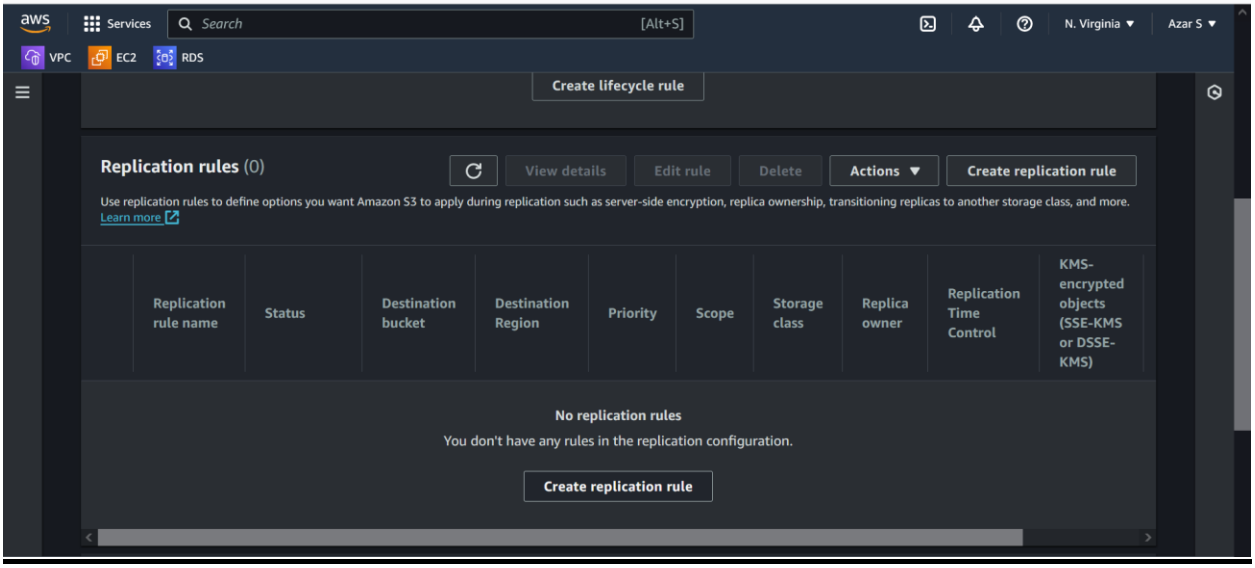

aws
Services
Search
[Alt+S]
N. Virginia
Azar S
VPC
EC2
RDS
Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
Block public access to buckets and objects granted through new access control lists (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.
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.
CloudShell
Feedback
Language
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

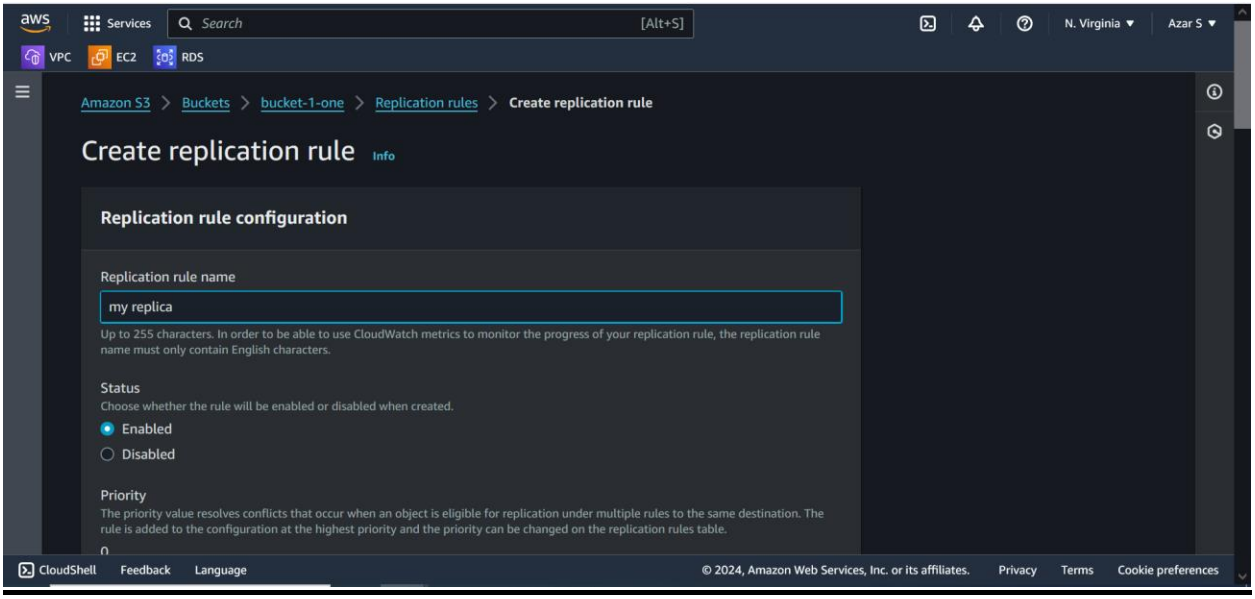

aws
Services
Search
[Alt+S]
N. Virginia
Azar S
VPC
EC2
RDS
Turning off block all public access might result in this bucket and the objects within becoming public
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.
I acknowledge that the current settings might result in this bucket and the objects within becoming public.
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
Bucket Versioning
Disable
Enable
Tags - optional (0)
You can use bucket tags to track storage costs and organize buckets. Learn more
CloudShell
Feedback
Language
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

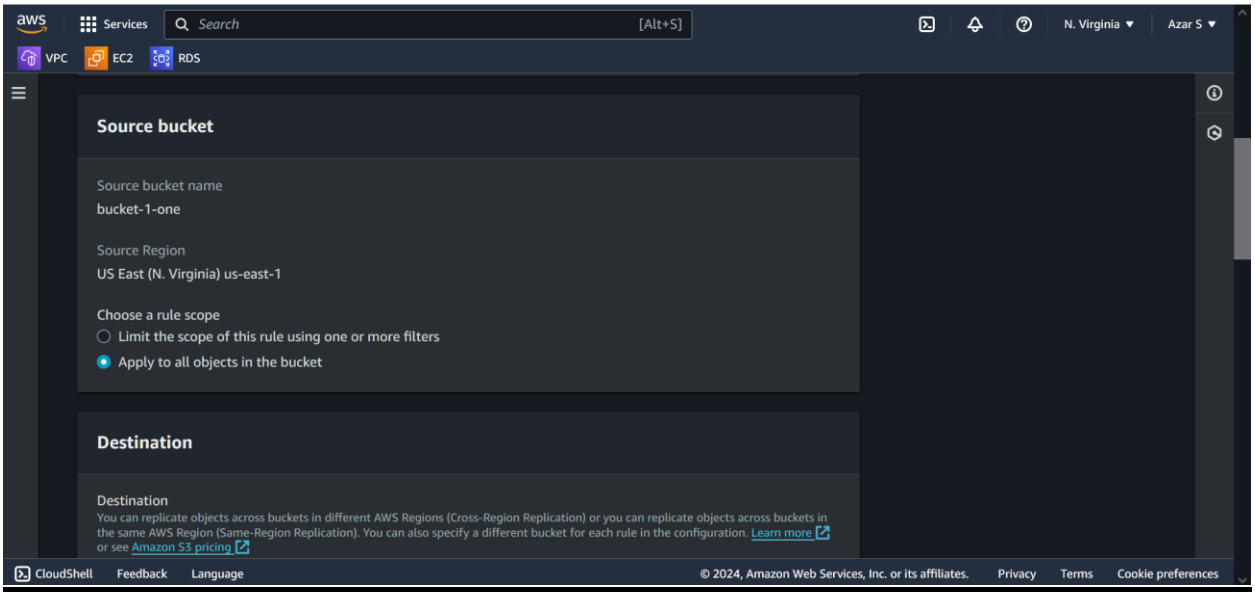

Services
Search
[Alt+S]
N. Virginia
Azar S
VPC
EC2
RDS
Server-side encryption with Amazon S3 managed keys (SSE-S3)
Server-side encryption with AWS Key Management Service keys (SSE-KMS)
Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage 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
Advanced settings
After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.
Cancel
Create bucket

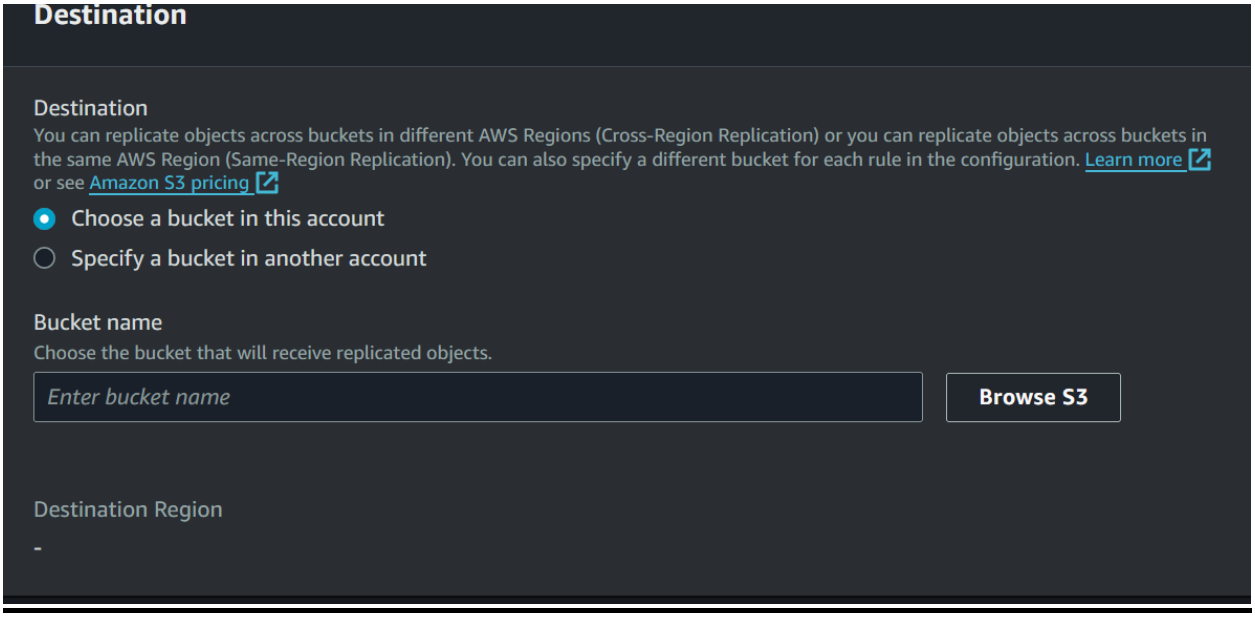

Services
Search
[Alt+S]
N. Virginia
Azar S
VPC
EC2
RDS
Storage lens provides visibility into storage usage and activity trends. Learn more
General purpose buckets
Directory buckets
General purpose buckets (3) Info All AWS Regions
Buckets are containers for data stored in S3.
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
1
Name
AWS Region
IAM Access Analyzer
Creation date
bucket-1-one
US East (N. Virginia) us-east-1
View analyzer for us-east-1
April 5, 2024, 10:54:25 (UTC+05:30)
bucket-2-two
US East (N. Virginia) us-east-1
View analyzer for us-east-1
April 5, 2024, 10:56:32 (UTC+05:30)
static-website-hosting-1
US East (N. Virginia) us-east-1
View analyzer for us-east-1
April 5, 2024, 10:22:53 (UTC+05:30)
CloudShell
Feedback
Language
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

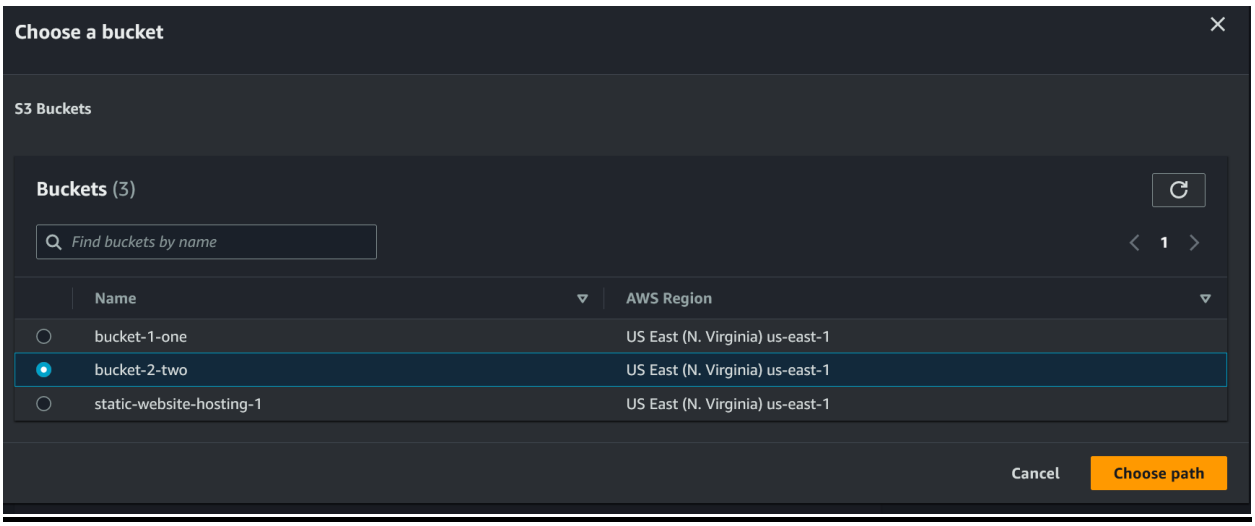

aws
Services
Search
[Alt+S]
N. Virginia
Azar S
VPC
EC2
RDS
Amazon S3 > Buckets > bucket-1-one
bucket-1-one
Objects
Properties
Permissions
Metrics
Management
Access Points
Lifecycle rules
View details
Edit
Delete
Actions
Create lifecycle rule
Use lifecycle rules to define actions you want Amazon S3 to take during an object's lifetime such as transitioning objects to another storage class, archiving them, or deleting them after a specified period of time. Learn more
Lifecycle rule ...
Status
Scope
Current versio...
Noncurrent ve...
Expired object...
Incomplete m...
No lifecycle rules
There are no lifecycle rules for this bucket.
Create lifecycle rule

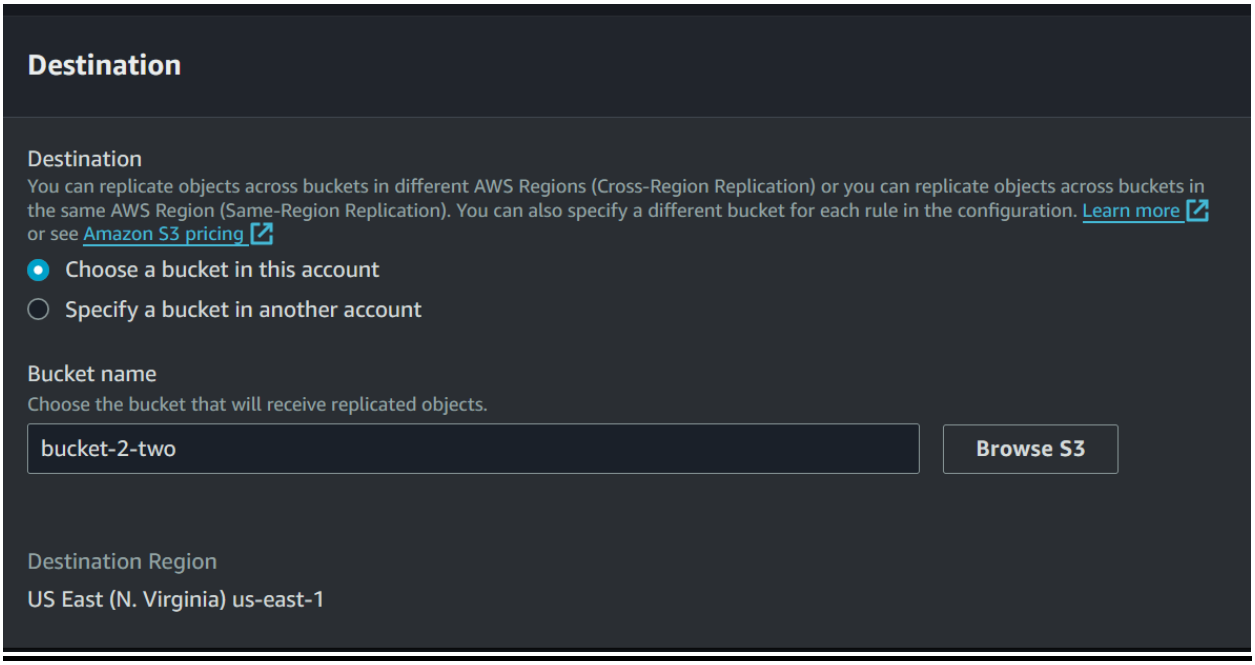

aws
Services
Search
[Alt+S]
N. Virginia
Azar S
VPC
EC2
RDS
Create lifecycle rule
Replication rules (0)
View details
Edit rule
Delete
Actions
Create replication rule
Use replication rules to define options you want Amazon S3 to apply during replication such as server-side encryption, replica ownership, transitioning replicas to another storage class, and more. Learn more
Replication rule name
Status
Destination bucket
Destination Region
Priority
Scope
Storage class
Replica owner
Replication Time Control
KMS-encrypted objects (SSE-KMS or DSSE-KMS)
No replication rules
You don't have any rules in the replication configuration.
Create replication rule


aws
Services
Search
[Alt+S]
N. Virginia
Azar S
VPC
EC2
RDS
Amazon S3 > Buckets > bucket-1-one > Replication rules > Create replication rule
Create replication rule Info
Replication rule configuration
Replication rule name
my replica
Up to 255 characters. In order to be able to use CloudWatch metrics to monitor the progress of your replication rule, the replication rule name must only contain English characters.
Status
Choose whether the rule will be enabled or disabled when created.
Enabled
Disabled
Priority
The priority value resolves conflicts that occur when an object is eligible for replication under multiple rules to the same destination. The rule is added to the configuration at the highest priority and the priority can be changed on the replication rules table.
0
CloudShell
Feedback
Language
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

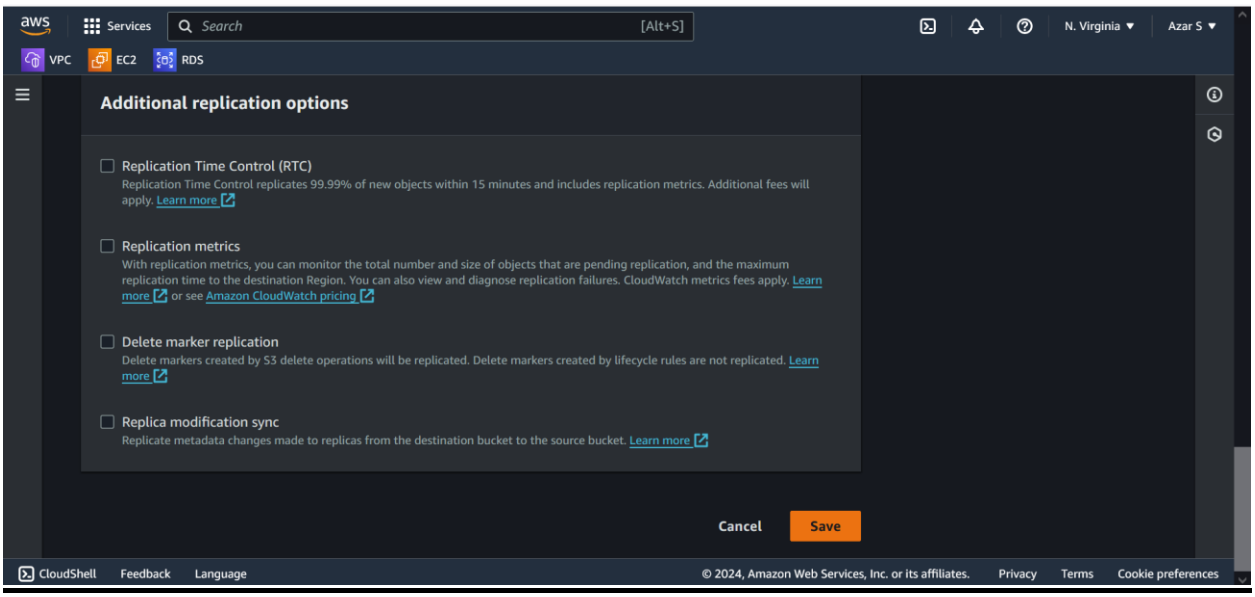

aws
Services
Search
[Alt+S]
N. Virginia
Azar S
VPC
EC2
RDS
Source bucket
Source bucket name
bucket-1-one
Source Region
US East (N. Virginia) us-east-1
Choose a rule scope
Limit the scope of this rule using one or more filters
Apply to all objects in the bucket
Destination
Destination
You can replicate objects across buckets in different AWS Regions (Cross-Region Replication) or you can replicate objects across buckets in the same AWS Region (Same-Region Replication). You can also specify a different bucket for each rule in the configuration. Learn more
or see Amazon S3 pricing
CloudShell
Feedback
Language
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

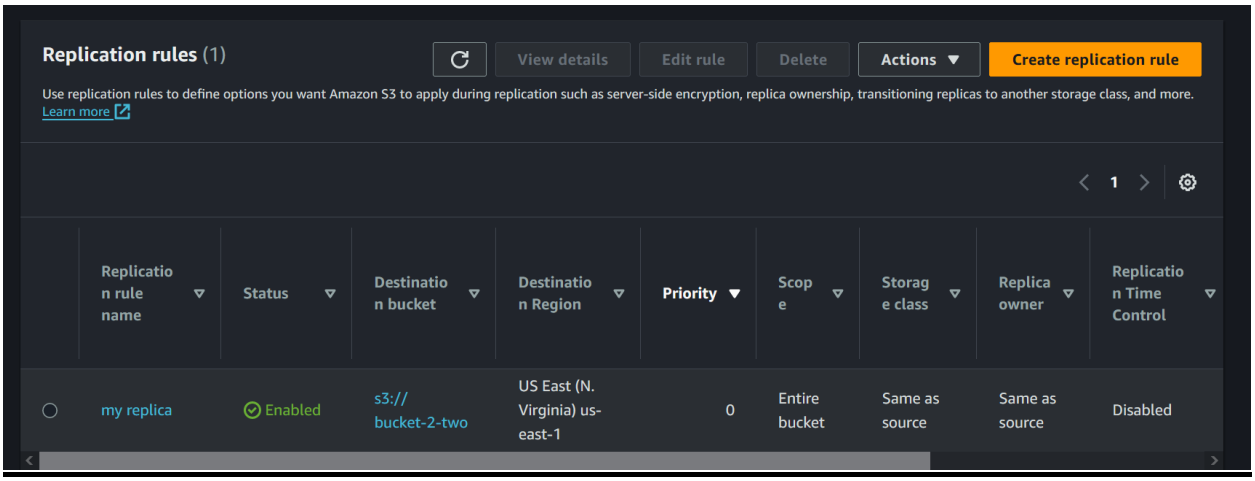

Destination
Destination
You can replicate objects across buckets in different AWS Regions (Cross-Region Replication) or you can replicate objects across buckets in the same AWS Region (Same-Region Replication). You can also specify a different bucket for each rule in the configuration. Learn more
or see Amazon S3 pricing
Choose a bucket in this account
Specify a bucket in another account
Bucket name
Choose the bucket that will receive replicated objects.
Enter bucket name
Browse S3
Destination Region
-

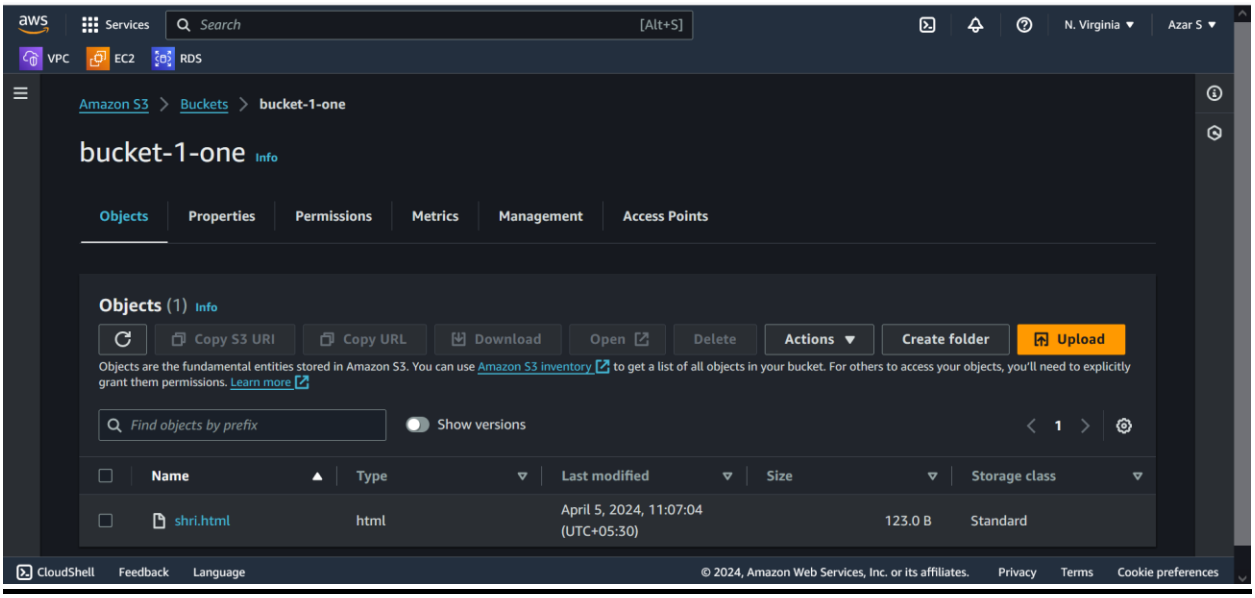

Choose a bucket
S3 Buckets
Buckets (3)
Find buckets by name
1
Name
AWS Region
bucket-1-one
US East (N. Virginia) us-east-1
bucket-2-two
US East (N. Virginia) us-east-1
static-website-hosting-1
US East (N. Virginia) us-east-1
Cancel
Choose path

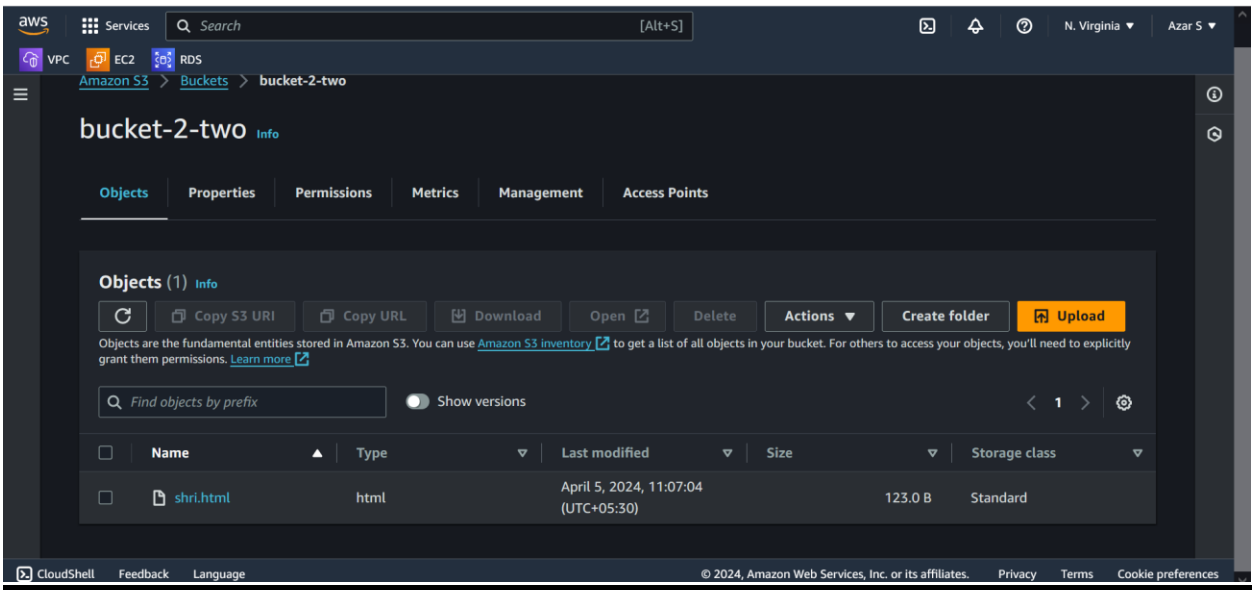

Destination
Destination
You can replicate objects across buckets in different AWS Regions (Cross-Region Replication) or you can replicate objects across buckets in the same AWS Region (Same-Region Replication). You can also specify a different bucket for each rule in the configuration. Learn more
or see Amazon S3 pricing
Choose a bucket in this account
Specify a bucket in another account
Bucket name
Choose the bucket that will receive replicated objects.
bucket-2-two
Browse S3
Destination Region
US East (N. Virginia) us-east-1


IAM role
Create new role
Choose from existing IAM roles
Enter IAM role ARN
Encryption
Server-side encryption protects data at rest.
Replicate objects encrypted with AWS Key Management Service (AWS KMS)
Replicate SSE-KMS and DSSE-KMS encrypted objects.
Destination storage class


aws
Services
Search
[Alt+S]
N. Virginia
Azar S
VPC
EC2
RDS
Additional replication options
Replication Time Control (RTC)
Replication Time Control replicates 99.99% of new objects within 15 minutes and includes replication metrics. Additional fees will apply. Learn more
Replication metrics
With replication metrics, you can monitor the total number and size of objects that are pending replication, and the maximum replication time to the destination Region. You can also view and diagnose replication failures. CloudWatch metrics fees apply. Learn more or see Amazon CloudWatch pricing
Delete marker replication
Delete markers created by S3 delete operations will be replicated. Delete markers created by lifecycle rules are not replicated. Learn more
Replica modification sync
Replicate metadata changes made to replicas from the destination bucket to the source bucket. Learn more
Cancel
Save
CloudShell
Feedback
Language
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Replication rules (1)
View details
Edit rule
Delete
Actions
Create replication rule
Use replication rules to define options you want Amazon S3 to apply during replication such as server-side encryption, replica ownership, transitioning replicas to another storage class, and more. Learn more
1
Replication rule name
Status
Destination bucket
Destination Region
Priority
Scope
Storage class
Replica owner
Replication Time Control
my replica
Enabled
s3://bucket-2-two
US East (N. Virginia) us-east-1
0
Entire bucket
Same as source
Same as source
Disabled


aws
Services
Search
[Alt+S]
N. Virginia
Azar S
VPC
EC2
RDS
Amazon S3 > Buckets > bucket-1-one
bucket-1-one Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (1) Info
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
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
Find objects by prefix
Show versions
1
Name
Type
Last modified
Size
Storage class
shri.html
html
April 5, 2024, 11:07:04 (UTC+05:30)
123.0 B
Standard
CloudShell
Feedback
Language
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
N. Virginia
Azar S
VPC
EC2
RDS
Amazon S3 > Buckets > bucket-2-two
bucket-2-two Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (1) Info
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
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
Find objects by prefix
Show versions
1
Name
Type
Last modified
Size
Storage class
shri.html
html
April 5, 2024, 11:07:04 (UTC+05:30)
123.0 B
Standard
CloudShell
Feedback
Language
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences