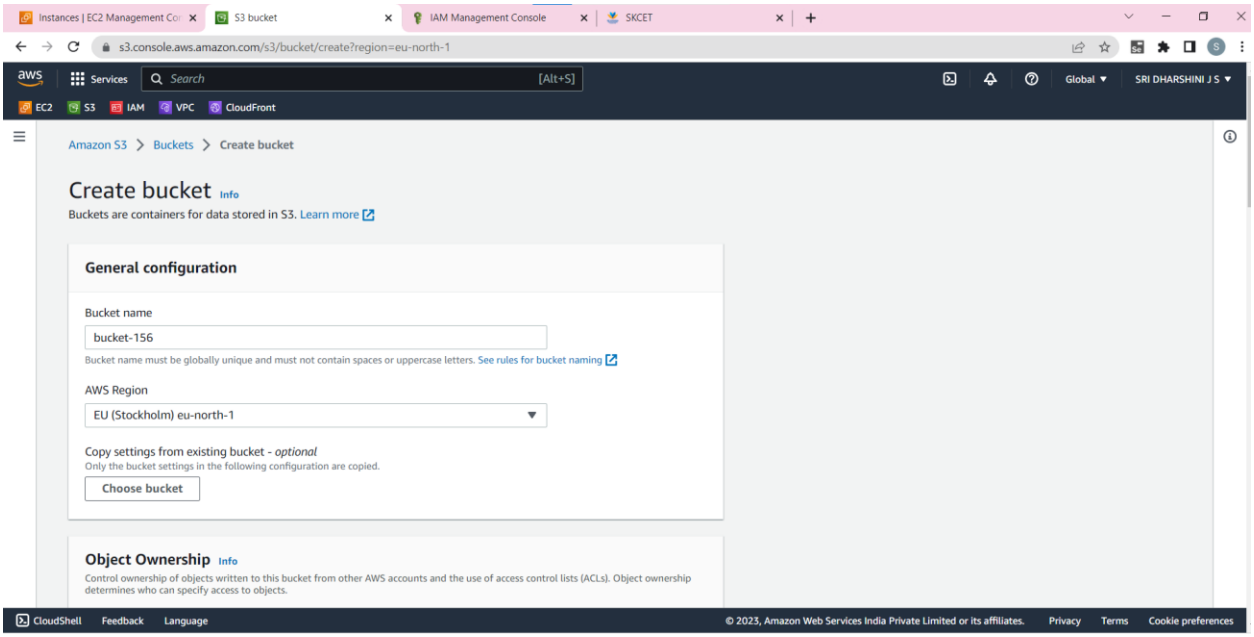
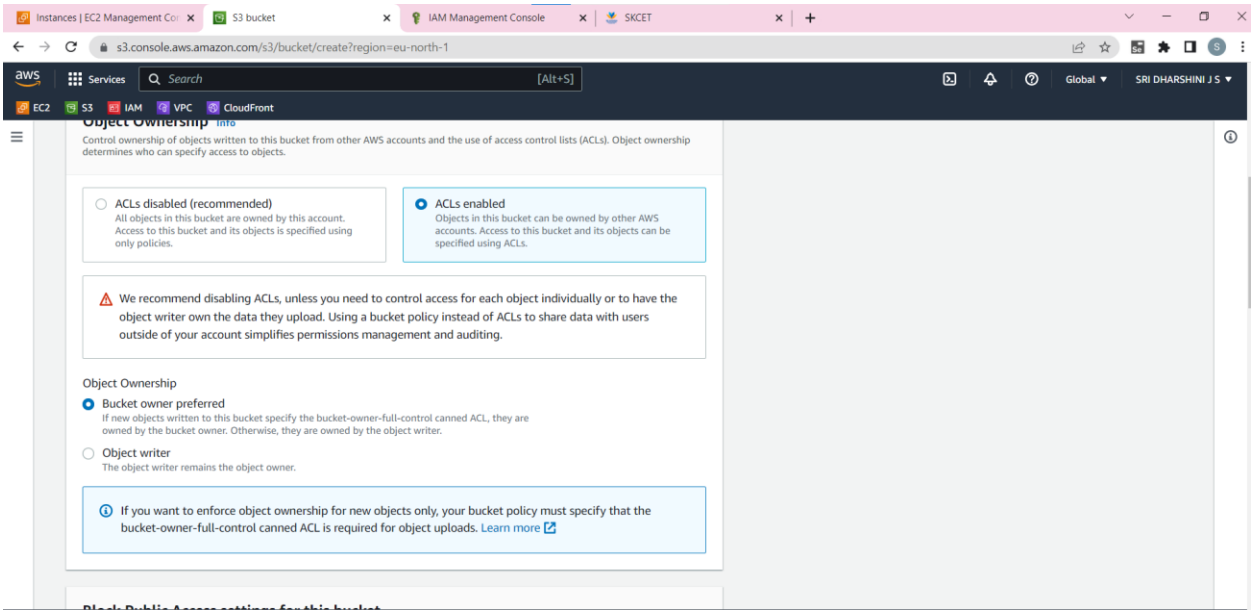
SRI DHARSHINI J S

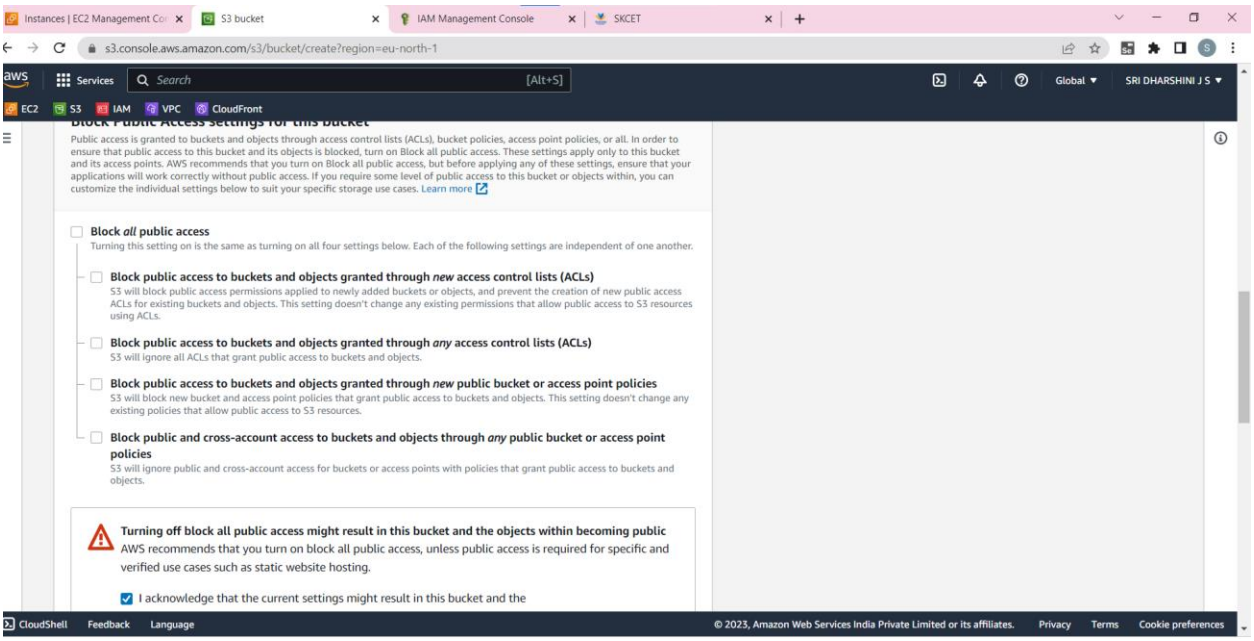
727721EUIT156

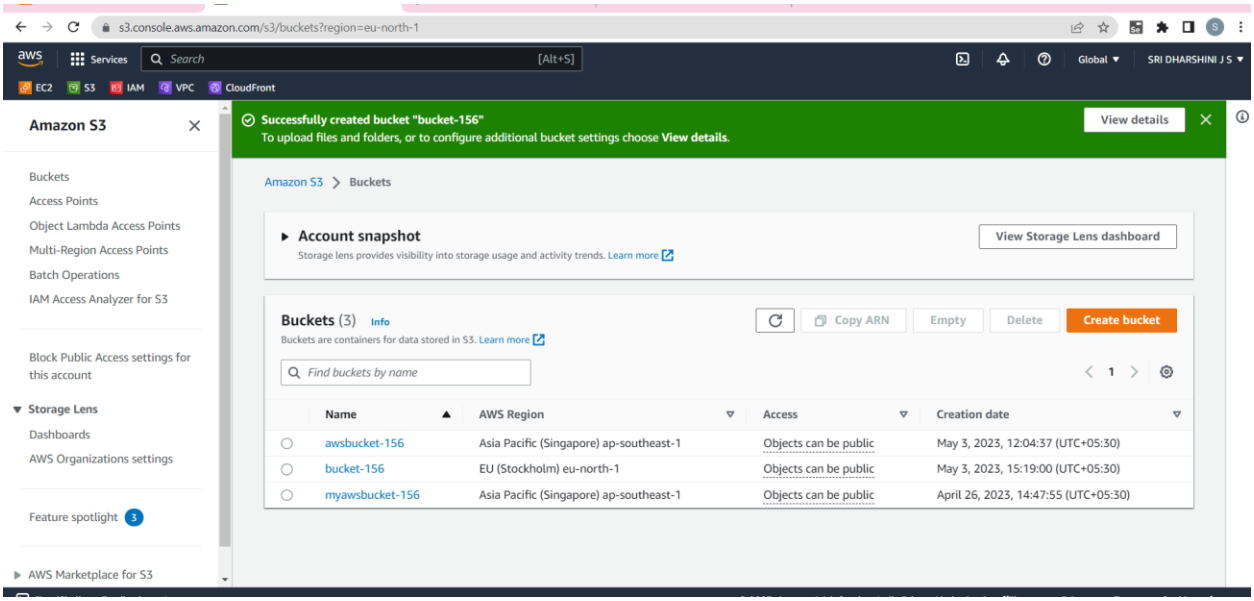
CC1

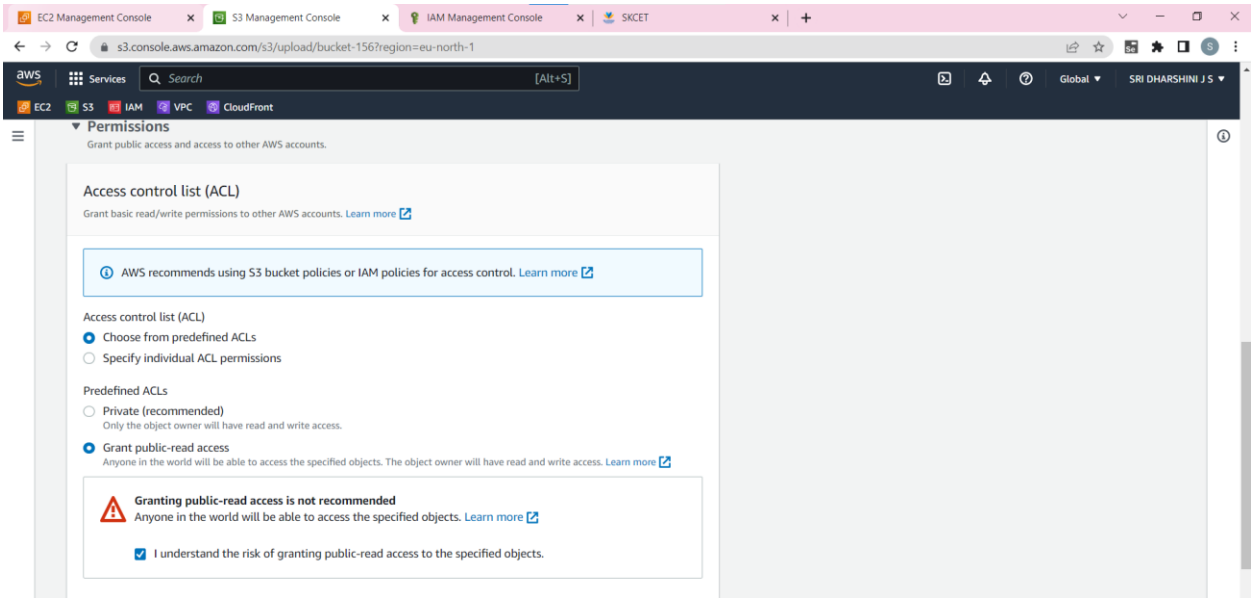
Q3:

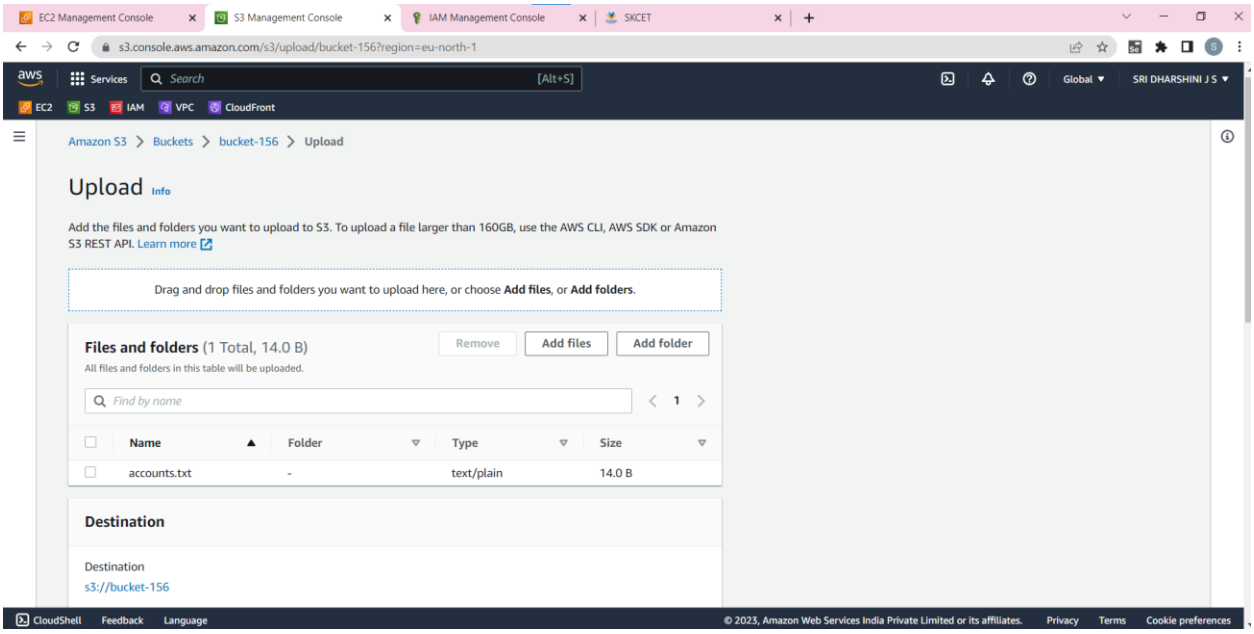


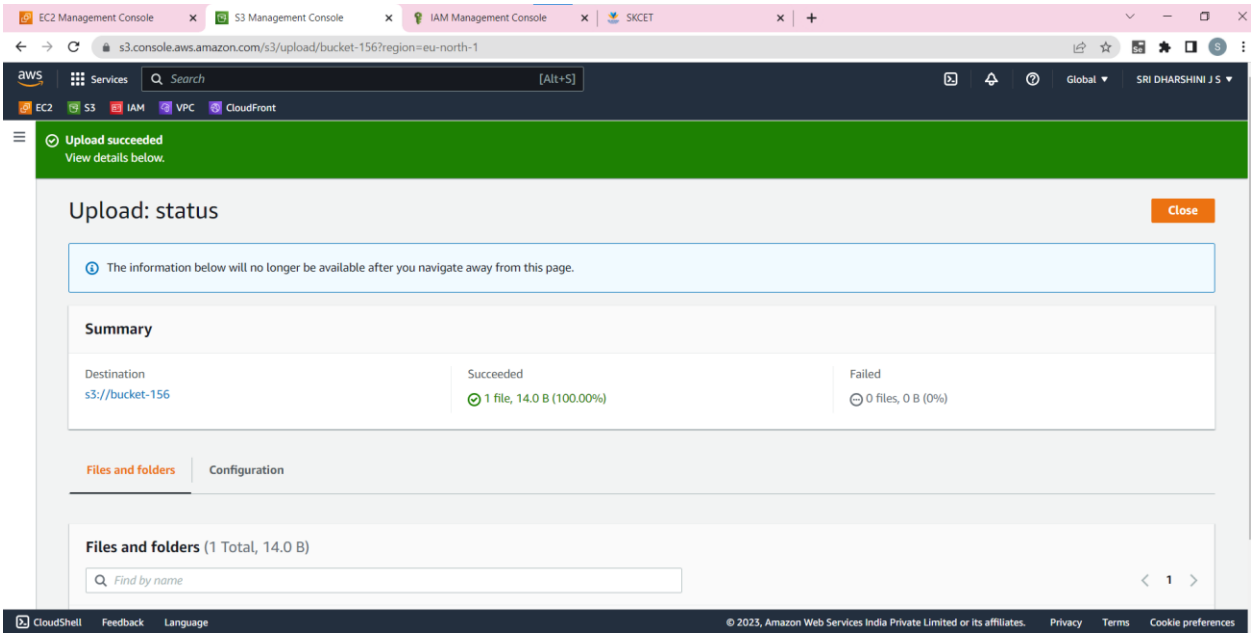


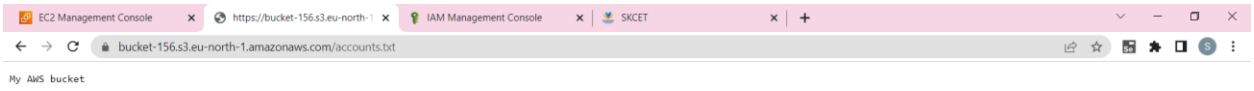

Instances | EC2 Management Cor
S3 bucket
IAM Management Console
SKCET
s3.console.aws.amazon.com/s3/bucket/create?region=eu-north-1
Services
Search
[Alt+S]
Global
SRI DHARSHINI J S
EC2
S3
IAM
VPC
CloudFront
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, 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.
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
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences


s3.console.aws.amazon.com/s3/buckets?region=eu-north-1
Services
Search
[Alt+S]
Global
SRI DHARSHINI J S
EC2
S3
IAM
VPC
CloudFront
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM 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 "bucket-156"
To upload files and folders, or to configure additional bucket settings choose View details.
View details
Amazon S3 > Buckets
Account snapshot
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
Buckets (3) Info
Buckets are containers for data stored in S3. Learn more
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
1
Name
AWS Region
Access
Creation date
awsbucket-156
Asia Pacific (Singapore) ap-southeast-1
Objects can be public
May 3, 2023, 12:04:37 (UTC+05:30)
bucket-156
EU (Stockholm) eu-north-1
Objects can be public
May 3, 2023, 15:19:00 (UTC+05:30)
myawsbucket-156
Asia Pacific (Singapore) ap-southeast-1
Objects can be public
April 26, 2023, 14:47:55 (UTC+05:30)


EC2 Management Console
S3 Management Console
IAM Management Console
SKCET
s3.console.aws.amazon.com/s3/upload/bucket-156?region=eu-north-1
Services
Search
[Alt+S]
Global
SRI DHARSHINI J S
EC2
S3
IAM
VPC
CloudFront
Permissions
Grant public access and access to other AWS accounts.
Access control list (ACL)
Grant basic read/write permissions to other AWS accounts. Learn more
AWS recommends using S3 bucket policies or IAM policies for access control. Learn more
Access control list (ACL)
Choose from predefined ACLs
Specify individual ACL permissions
Predefined ACLs
Private (recommended)
Only the object owner will have read and write access.
Grant public-read access
Anyone in the world will be able to access the specified objects. The object owner will have read and write access. Learn more
Granting public-read access is not recommended
Anyone in the world will be able to access the specified objects. Learn more
I understand the risk of granting public-read access to the specified objects.


EC2 Management Console
S3 Management Console
IAM Management Console
SKCET
s3.console.aws.amazon.com/s3/upload/bucket-156?region=eu-north-1
Services
Search
[Alt+S]
Global
SRI DHARSHINI J S
EC2
S3
IAM
VPC
CloudFront
Amazon S3 > Buckets > bucket-156 > Upload
Upload Info
Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more
Drag and drop files and folders you want to upload here, or choose Add files, or Add folders.
Files and folders (1 Total, 14.0 B)
All files and folders in this table will be uploaded.
Remove
Add files
Add folder
Find by name
1
Name
Folder
Type
Size
accounts.txt
-
text/plain
14.0 B
Destination
Destination
s3://bucket-156
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences






```
My AWS bucket
```