

**School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)**

Subject : Advanced Cloud Computing (P)

Name of the Student: **Prakhar Anil Sharma**

PRN: **20220801121**

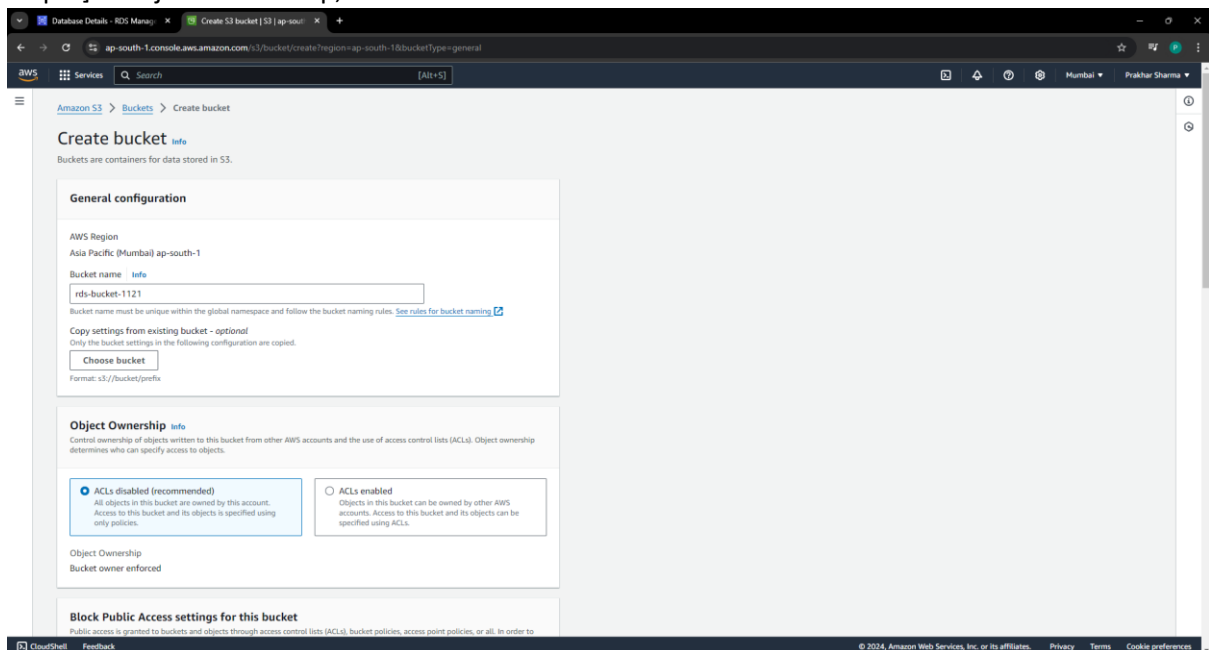
Title of Practical : **Export Amazon RDS DB Snapshot to S3**

Step-1]Go to Amazon S3.

Step-2] Click on Buckets then click on create bucket.

Step-3]Name your bucket.

step-4]In Object Ownership, select ACLs disabled.



Step-5]In Block Public access settings, tick the checkbox of Block all Public Access.

Step-6]Bucket Versioning, Disable.

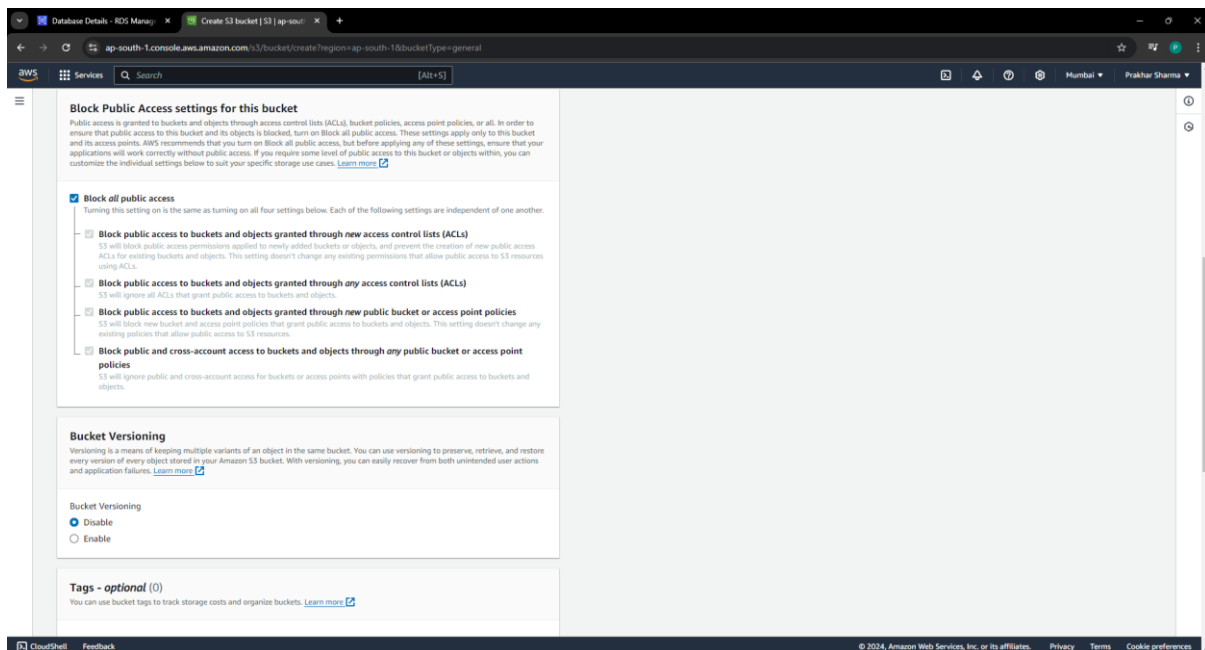
**School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)**

Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma

PRN: 20220801121

Title of Practical : Export Amazon RDS DB Snapshot to S3



Step-7]In Default encryption

- Select SSE-S3 as encryption type
- Select Bucket Type – enable

**School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)**

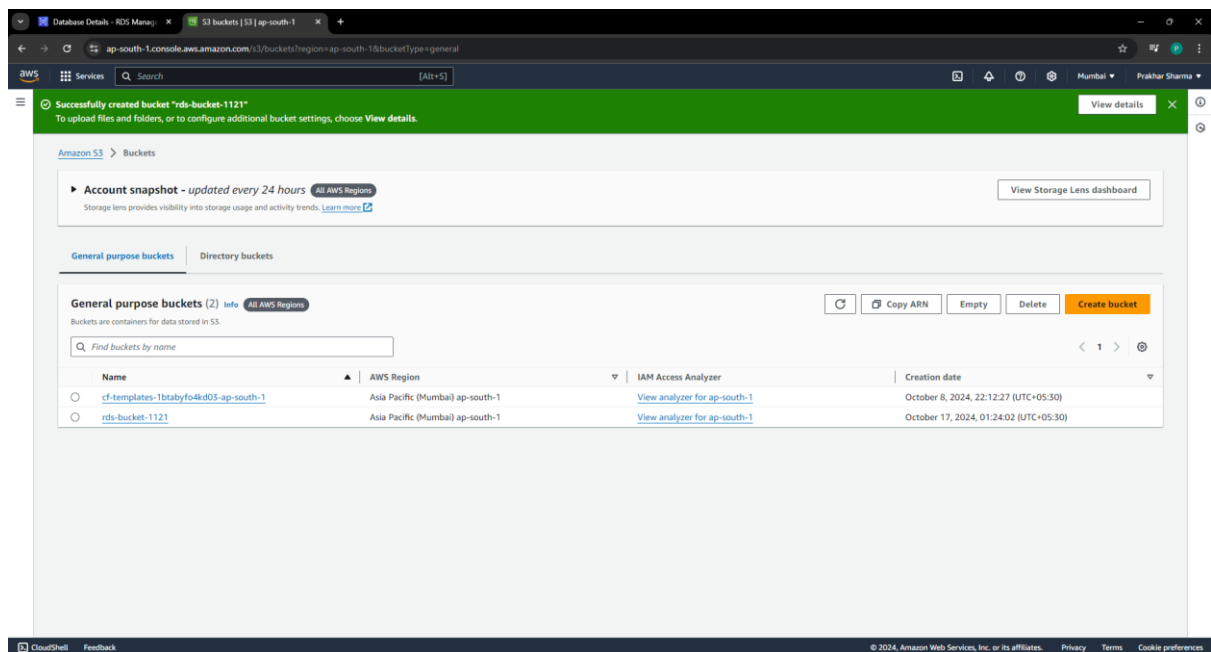
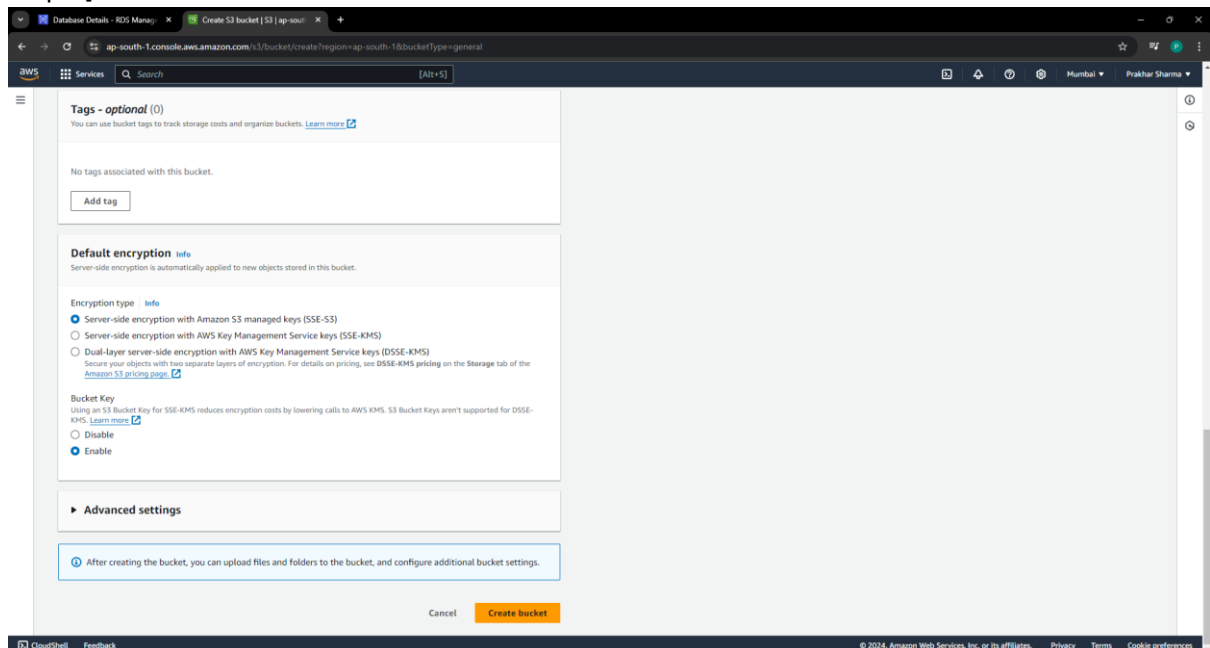
Subject : Advanced Cloud Computing (P)

Name of the Student: **Prakhar Anil Sharma**

PRN: 20220801121

Title of Practical : **Export Amazon RDS DB Snapshot to S3**

Step-8] Click on create bucket.



School of Computer Science, Engineering and Applications(SCSEA)

B.C.A. TY (CCSA)

Subject : Advanced Cloud Computing (P)

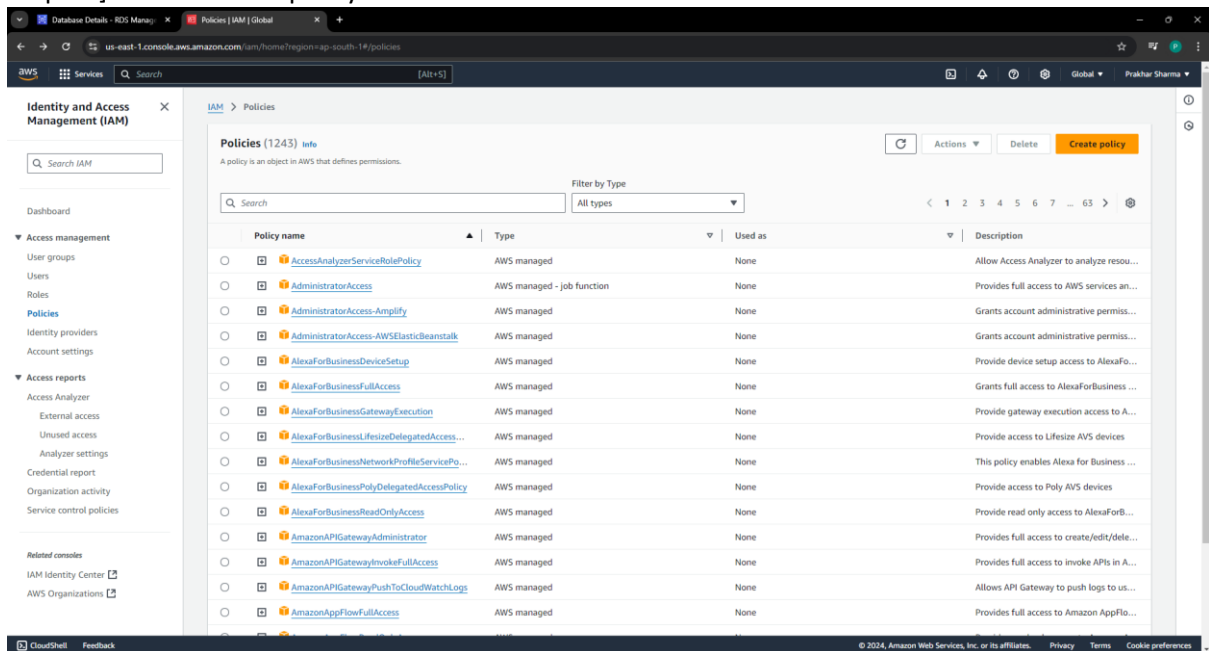
Name of the Student: Prakhar Anil Sharma

PRN: 20220801121

Title of Practical : Export Amazon RDS DB Snapshot to S3

Step-9]Go to IAM , Click on Policies.

Step-10]Click on create policy.



School of Computer Science, Engineering and Applications(SCSEA)

B.C.A. TY (CCSA)

Subject : Advanced Cloud Computing (P)

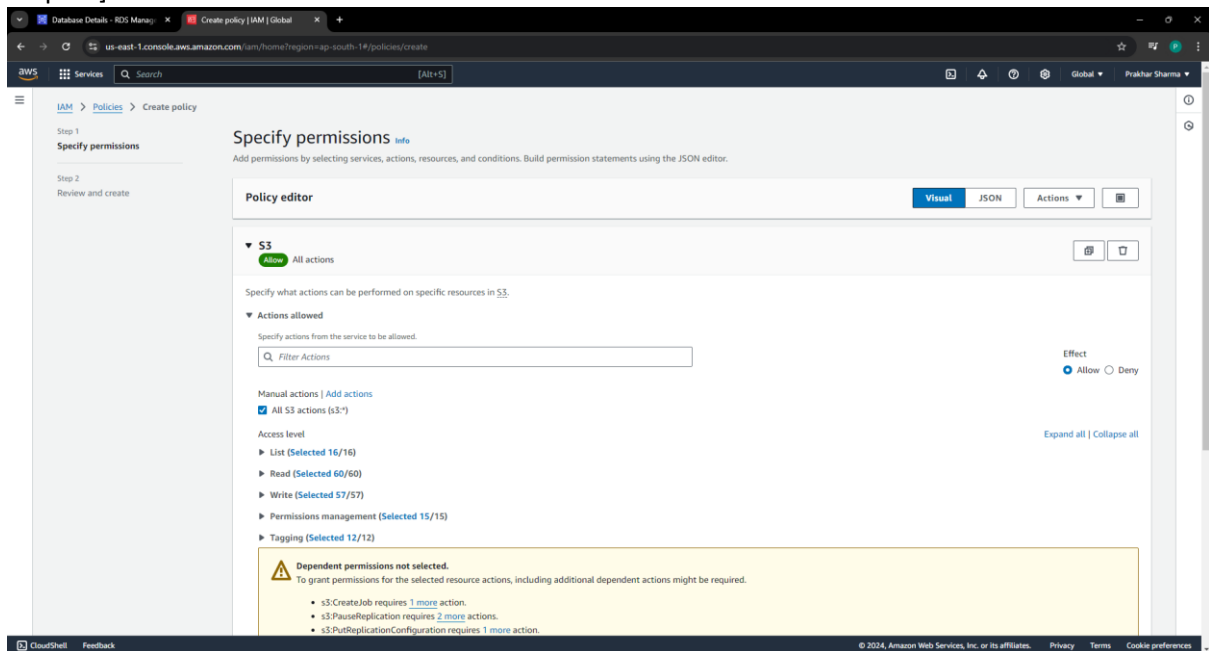
Name of the Student: Prakhar Anil Sharma

PRN: 20220801121

Title of Practical : Export Amazon RDS DB Snapshot to S3

Step-11] In Specify permission, Select S3 as a service.

Step-12] Tick the checkbox of All S3 action



School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)
Subject : Advanced Cloud Computing (P)

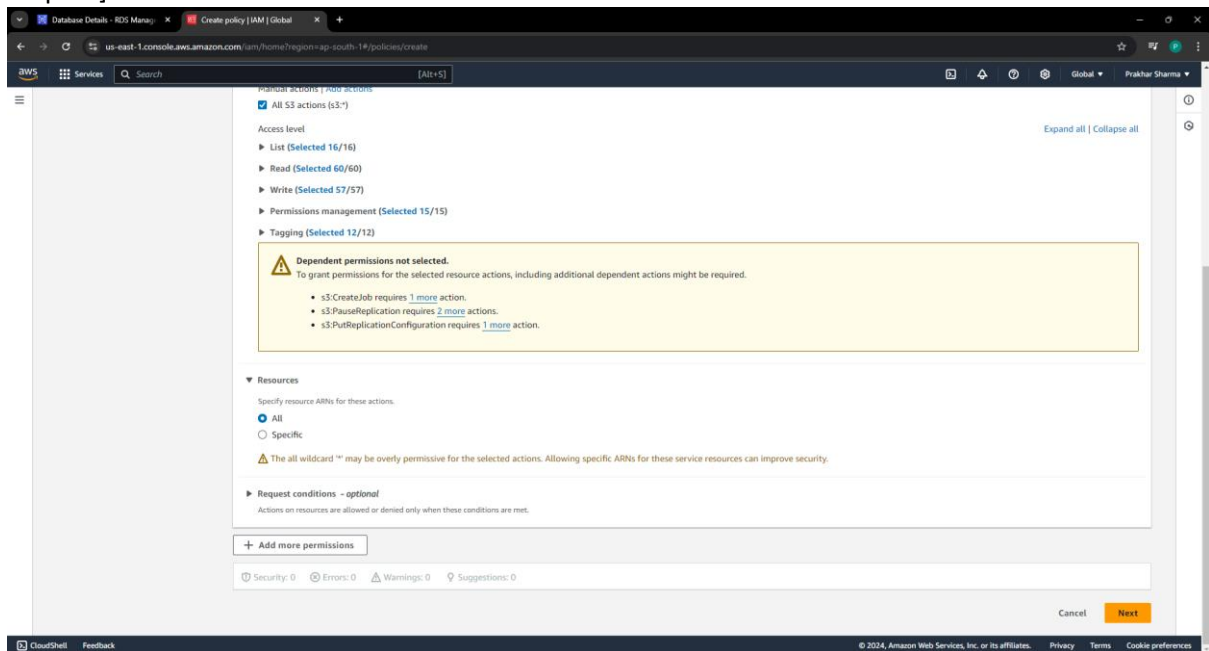
Name of the Student: **Prakhar Anil Sharma**

PRN: **20220801121**

Title of Practical : **Export Amazon RDS DB Snapshot to S3**

Step-13] In Resources, Select All.

Step-14] Click on Next.





School of Computer Science, Engineering and Applications(SCSEA)

B.C.A. TY (CCSA)

Subject : Advanced Cloud Computing (P)

Name of the Student: **Prakhar Anil Sharma**

PRN: **20220801121**

Title of Practical : **Export Amazon RDS DB Snapshot to S3**

Step-15]Name the policy.

Step-16]Click on create policy.

The screenshot shows the 'Review and create' step in the AWS IAM console. The policy name is 'rds-s3-1121'. The permissions are defined as 'Allow (1 of 423 services)' with 'Full access' for 'All resources'. The 'Request condition' is set to 'None'. The 'Add tags - optional' section is empty.

Service	Access level	Resource	Request condition
S3	Full access	All resources	None

The screenshot shows the 'Policies (1244)' list in the AWS IAM console. The table lists various AWS managed policies, including 'AccessAnalyzerServiceRolePolicy', 'AdministratorAccess', 'AdministratorAccess-Amplify', 'AdministratorAccess-AWSElasticBeanstalk', 'AlexaForBusinessDeviceSetup', 'AlexaForBusinessFullAccess', 'AlexaForBusinessGatewayExecution', 'AlexaForBusinessLifecycleDelegatedAccess...', 'AlexaForBusinessNetworkProfileServicePo...', 'AlexaForBusinessPolyDelegatedAccessPolicy', 'AlexaForBusinessReadOnlyAccess', 'AmazonAPIGatewayAdministrator', 'AmazonAPIGatewayInvokeFullAccess', and 'AmazonAPIGatewayPushToCloudWatchLogs'.

Policy name	Type	Used as	Description
AccessAnalyzerServiceRolePolicy	AWS managed	None	Allow Access Analyzer to analyze resou...
AdministratorAccess	AWS managed - job function	None	Provides full access to AWS services an...
AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permis...
AdministratorAccess-AWSElasticBeanstalk	AWS managed	None	Grants account administrative permis...
AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaFo...
AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness ...
AlexaForBusinessGatewayExecution	AWS managed	None	Provide gateway execution access to A...
AlexaForBusinessLifecycleDelegatedAccess...	AWS managed	None	Provide access to Lifesize AVS devices
AlexaForBusinessNetworkProfileServicePo...	AWS managed	None	This policy enables Alexa for Business ...
AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	None	Provide access to Poly AWS devices
AlexaForBusinessReadOnlyAccess	AWS managed	None	Provide read only access to AlexaForB...
AmazonAPIGatewayAdministrator	AWS managed	None	Provides full access to create/edit/dele...
AmazonAPIGatewayInvokeFullAccess	AWS managed	None	Provides full access to invoke APIs in A...
AmazonAPIGatewayPushToCloudWatchLogs	AWS managed	None	Allows API Gateway to push logs to us...

**School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)**

Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma

PRN: 20220801121

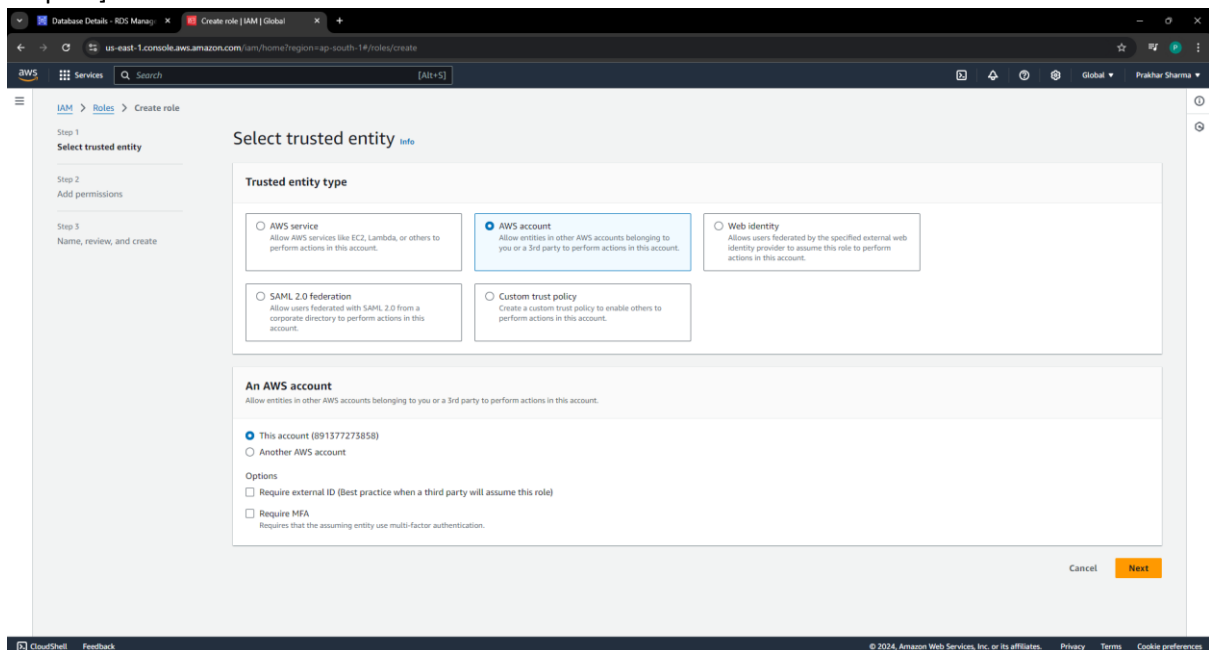
Title of Practical : Export Amazon RDS DB Snapshot to S3

Step-17]Go to IAM ,Click on Roles.

Step-18]Click on create role.

Step-19]Select Trusted entity type as AWS account.

Step-20]Click on Next.



The screenshot shows the AWS IAM console 'Create role' wizard. The browser address bar indicates the URL is `us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/create`. The left sidebar shows the navigation menu with 'IAM' > 'Roles' > 'Create role'. The main content area is titled 'Select trusted entity' and includes a 'Trusted entity type' section with five radio button options: 'AWS service', 'AWS account' (selected), 'Web identity', 'SAML 2.0 federation', and 'Custom trust policy'. Below this is the 'An AWS account' section with two radio button options: 'This account (89137273858)' (selected) and 'Another AWS account'. At the bottom, the 'Options' section has two checkboxes: 'Require external ID (Best practice when a third party will assume this role)' and 'Require MFA', both of which are unchecked. 'Cancel' and 'Next' buttons are located at the bottom right of the form.

Step-21]In Add permissions Search and select the RDS Policy You Just created.

Step-22]Click on Next.

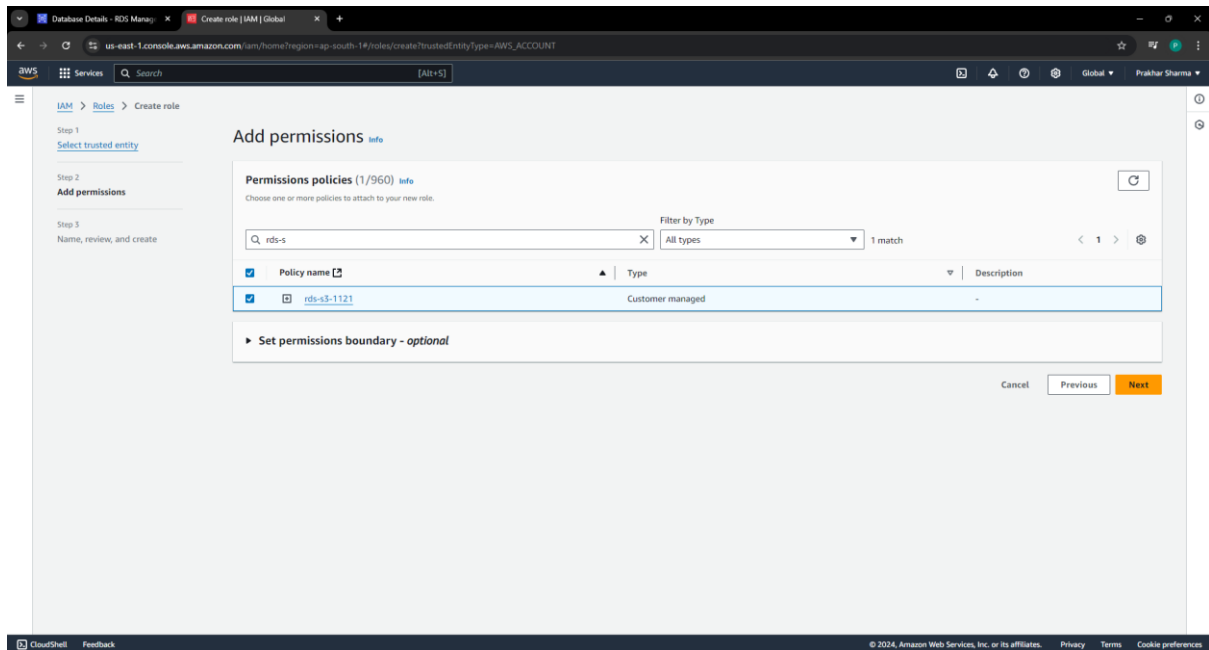
**School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)**

Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma

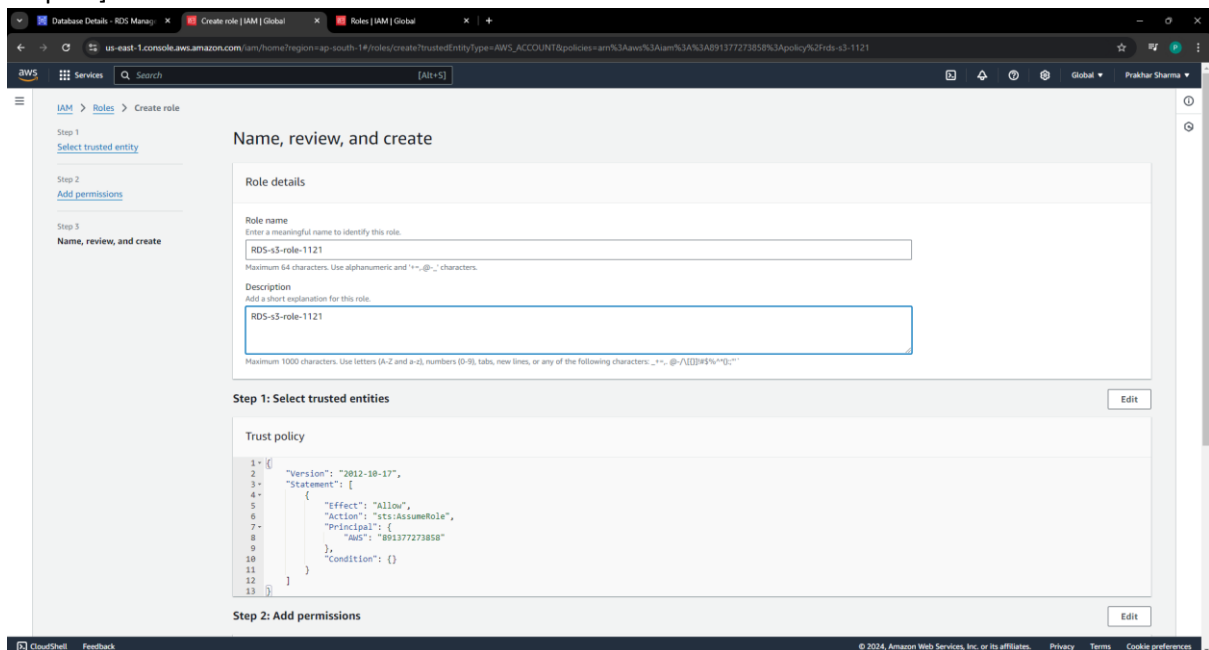
PRN: 20220801121

Title of Practical : Export Amazon RDS DB Snapshot to S3



Step-23]Give Role Name.

Step-24]Click on create role.



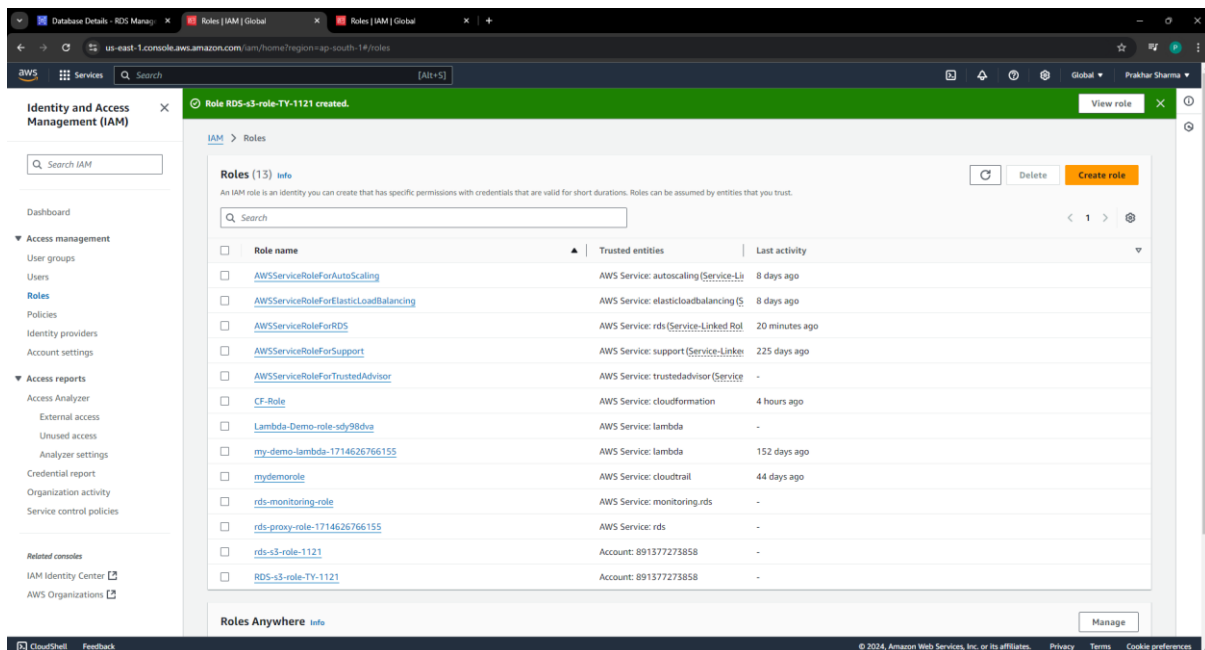
**School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)**

Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma

PRN: 20220801121

Title of Practical : Export Amazon RDS DB Snapshot to S3



Step-25]Go to KMS.

Step-26]Click on customer-managed keys.

Step-27]Click on create key.

Step-28]In Configure Key, Select Key Type as Symmetric and Key Usage as Encrypt and Decrypt.

School of Computer Science, Engineering and Applications(SCSEA)

B.C.A. TY (CCSA)

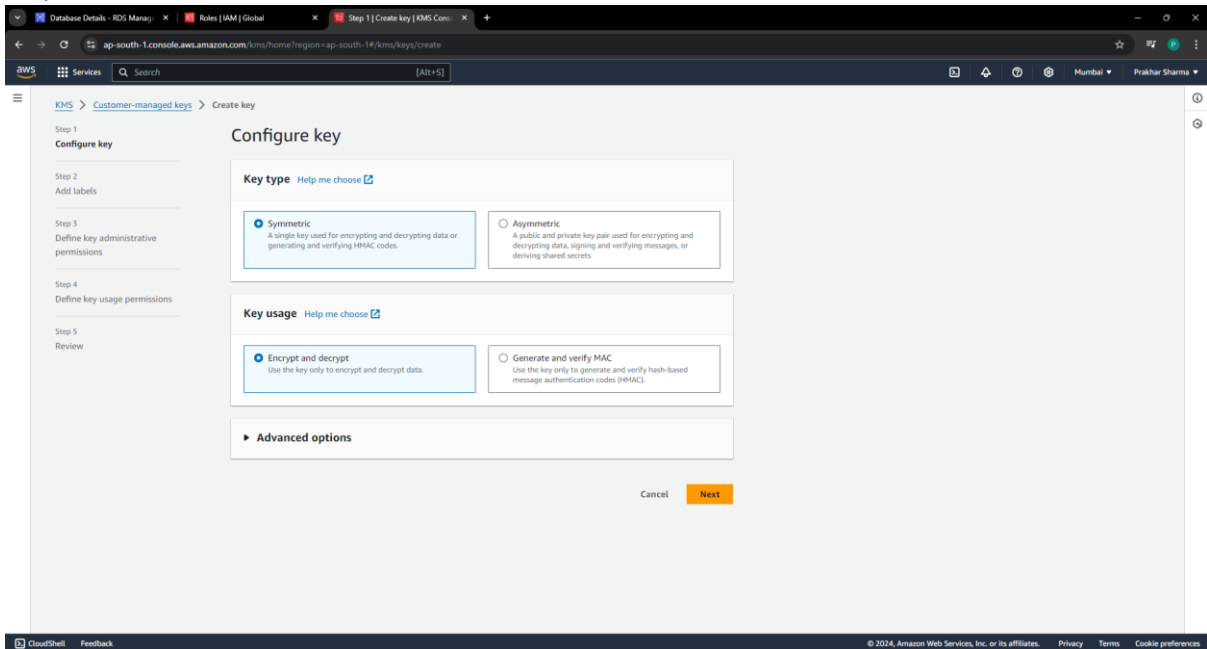
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma

PRN: 20220801121

Title of Practical : Export Amazon RDS DB Snapshot to S3

Step-29] Click on Next.



The screenshot shows the AWS IAM console 'Create key' page. The left sidebar lists the steps: Step 1: Configure key, Step 2: Add labels, Step 3: Define key administrative permissions, Step 4: Define key usage permissions, and Step 5: Review. The main content area is titled 'Configure key' and contains two sections: 'Key type' and 'Key usage'. In the 'Key type' section, 'Symmetric' is selected, with a description: 'A single key used for encrypting and decrypting data or generating and verifying HMAC codes.' In the 'Key usage' section, 'Encrypt and decrypt' is selected, with a description: 'Use the key only to encrypt and decrypt data.' There are 'Cancel' and 'Next' buttons at the bottom right of the form.

PRN: 20220801121

1
1

School of Computer Science, Engineering and Applications(SCSEA)

B.C.A. TY (CCSA)

Subject : Advanced Cloud Computing (P)

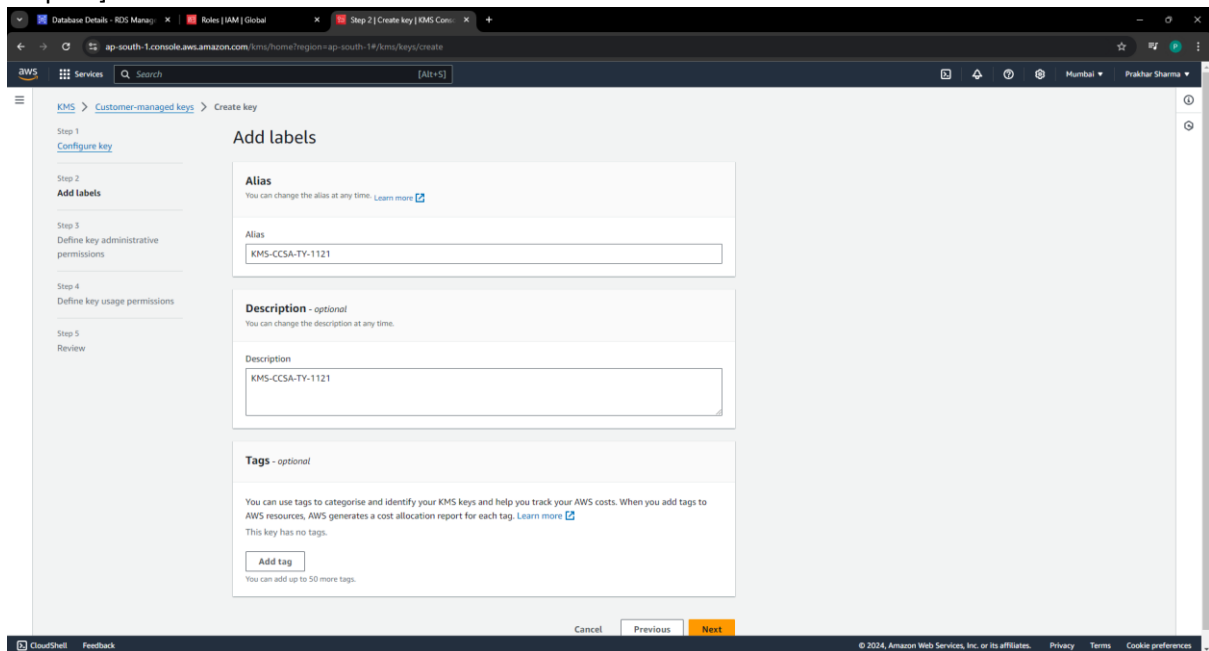
Name of the Student: Prakhar Anil Sharma

PRN: 20220801121

Title of Practical : Export Amazon RDS DB Snapshot to S3

Step-30]In Add labels, Name the Alias.

Step-31]Click on Next.



The screenshot shows the AWS Management Console interface for creating a new KMS key. The 'Add labels' step is active, showing a sidebar with steps 1 through 5. The main content area has three sections: 'Alias' with a text input field containing 'KMS-CCSA-TY-1121', 'Description - optional' with a text area containing 'KMS-CCSA-TY-1121', and 'Tags - optional' with an 'Add tag' button. At the bottom, there are 'Cancel', 'Previous', and 'Next' buttons, with 'Next' being highlighted in orange.

Step-32]In Define Key usage permissions, Select the IAM Role you created .

Step-33]Click on Next.

School of Computer Science, Engineering and Applications(SCSEA)

B.C.A. TY (CCSA)

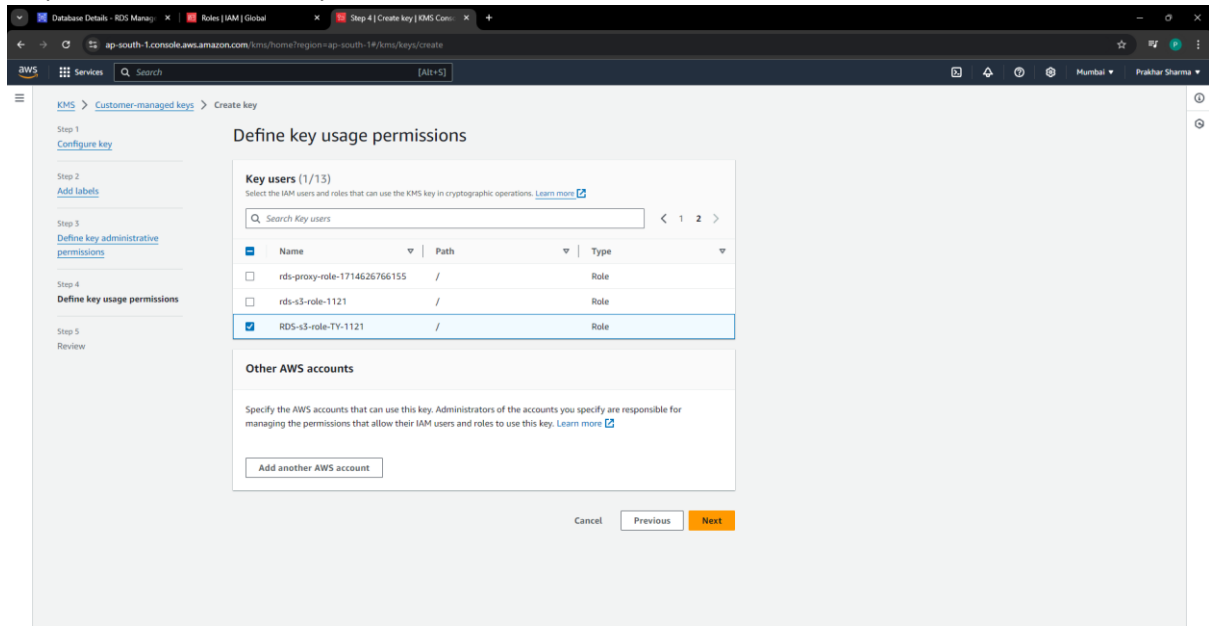
Subject : Advanced Cloud Computing (P)

Name of the Student: **Prakhar Anil Sharma**

PRN: **20220801121**

Title of Practical : **Export Amazon RDS DB Snapshot to S3**

Step-34]Click on create key.



Step 1: Configure key
Step 2: Add labels
Step 3: Define key administrative permissions
Step 4: Define key usage permissions
Step 5: Review

Define key usage permissions

Key users (1/13)
Select the IAM users and roles that can use the KMS key in cryptographic operations. [Learn more](#)

Search Key users

	Name	Path	Type
<input type="checkbox"/>	rds-proxy-role-1714626766155	/	Role
<input type="checkbox"/>	rds-s3-role-1121	/	Role
<input checked="" type="checkbox"/>	RDS-s3-role-TY-1121	/	Role

Other AWS accounts

Specify the AWS accounts that can use this key. Administrators of the accounts you specify are responsible for managing the permissions that allow their IAM users and roles to use this key. [Learn more](#)

Success
Your AWS KMS key was created with alias **KMS-CCSA-TY-1121** and key ID **e9eaa181-084f-453e-a2fb-3f125baae855**. [View key](#)

Customer-managed keys (1)

Filter keys by properties or tags

	Aliases	Key ID	Status	Key type	Key spec	Key usage
<input type="checkbox"/>	KMS-CCSA-TY-1121	e9eaa181-084f-453e-a2fb-3f...	Enabled	Symmetric	SYMMETRIC_DEFAULT	Encrypt and decrypt

PRN: 20220801121

1
3

School of Computer Science, Engineering and Applications(SCSEA)

B.C.A. TY (CCSA)

Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma

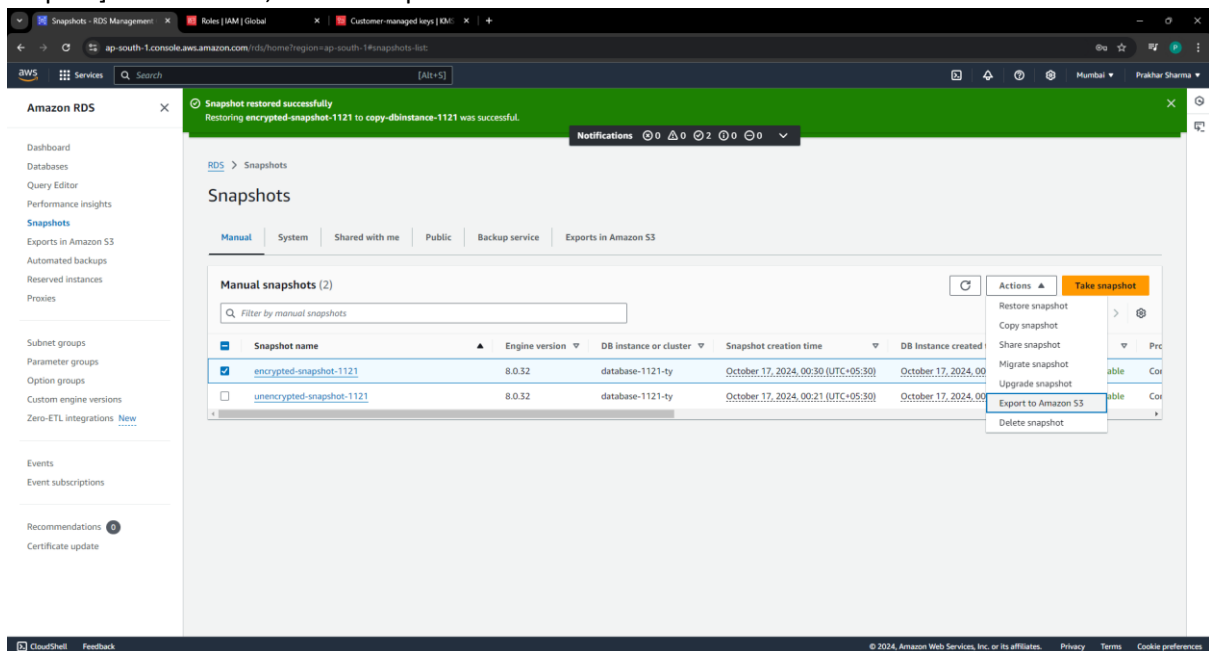
PRN: 20220801121

Title of Practical : Export Amazon RDS DB Snapshot to S3

Step-35]Go to RDS Snapshots.

Step-36] Select the encrypted snapshot you created .

Step-37]Go to actions, Click on Export to Amazon S3.



The screenshot shows the Amazon RDS Snapshots console. A notification at the top states: "Snapshot restored successfully. Restoring encrypted-snapshot-1121 to copy-dbinstance-1121 was successful." The left sidebar shows the navigation menu with "Snapshots" selected. The main content area displays the "Manual snapshots (2)" table. The table has the following data:

Snapshot name	Engine version	DB instance or cluster	Snapshot creation time	DB Instance created
<input checked="" type="checkbox"/> encrypted-snapshot-1121	8.0.32	database-1121-ty	October 17, 2024, 00:30 (UTC+05:30)	October 17, 2024, 00:30 (UTC+05:30)
<input type="checkbox"/> unencrypted-snapshot-1121	8.0.32	database-1121-ty	October 17, 2024, 00:21 (UTC+05:30)	October 17, 2024, 00:21 (UTC+05:30)

The "Actions" menu is open for the selected snapshot, showing options: Restore snapshot, Copy snapshot, Share snapshot, Migrate snapshot, Upgrade snapshot, **Export to Amazon S3**, and Delete snapshot.

School of Computer Science, Engineering and Applications(SCSEA)

B.C.A. TY (CCSA)

Subject : Advanced Cloud Computing (P)

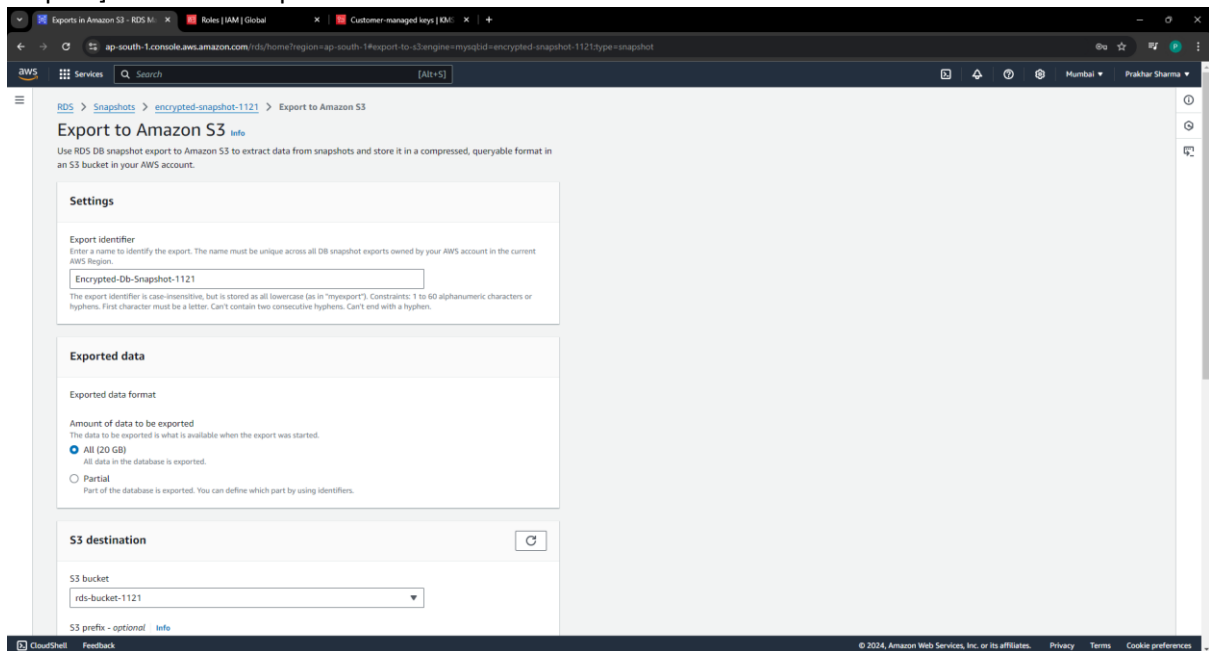
Name of the Student: Prakhar Anil Sharma

PRN: 20220801121

Title of Practical : Export Amazon RDS DB Snapshot to S3

Step-38]In Settings, Name the Export identifier.

Step-39]Select All in Exported data.



The screenshot shows the AWS Management Console interface for the 'Export to Amazon S3' task. The breadcrumb navigation is 'RDS > Snapshots > encrypted-snapshot-1121 > Export to Amazon S3'. The page title is 'Export to Amazon S3'. Below the title, there is a brief description: 'Use RDS DB snapshot export to Amazon S3 to extract data from snapshots and store it in a compressed, queryable format in an S3 bucket in your AWS account.' The main content area is divided into three sections: 'Settings', 'Exported data', and 'S3 destination'. In the 'Settings' section, the 'Export identifier' is set to 'Encrypted-Db-Snapshot-1121'. In the 'Exported data' section, the 'Amount of data to be exported' is set to 'All (20 GB)'. In the 'S3 destination' section, the 'S3 bucket' is set to 'rds-bucket-1121'.

Step-40] In S3 destination, Select the S3 bucket you created from the dropdown.

Step-41]In IAM Role, Select the IAM Role you created from the dropdown.

**School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)**

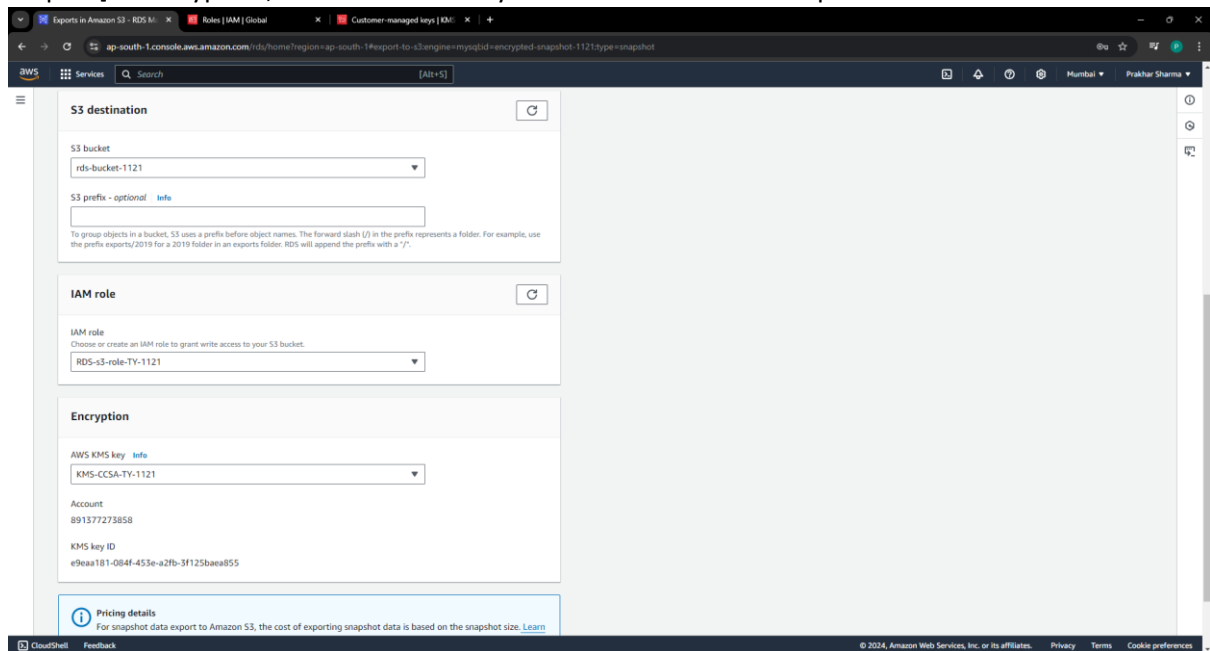
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma

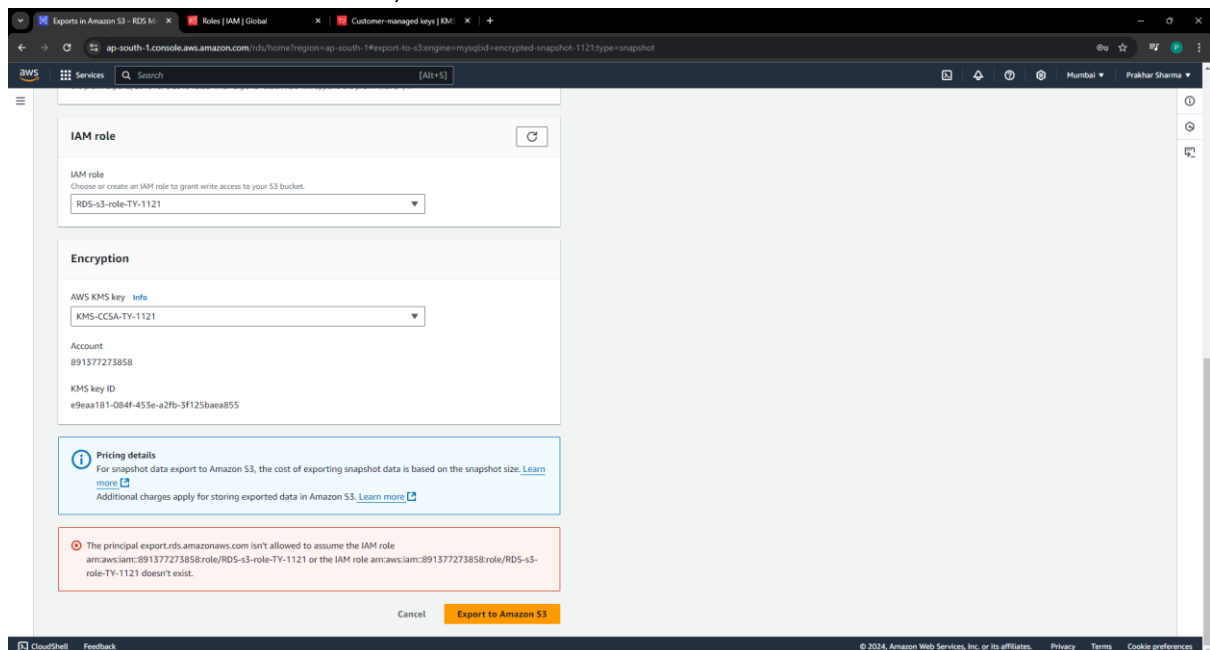
PRN: 20220801121

Title of Practical : Export Amazon RDS DB Snapshot to S3

Step-41]In Encryption, Select the KMS Key You created from the dropdown.



You will see a red box at the end, to resolve this Go to IAM Role.



PRN: 20220801121

**School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)**

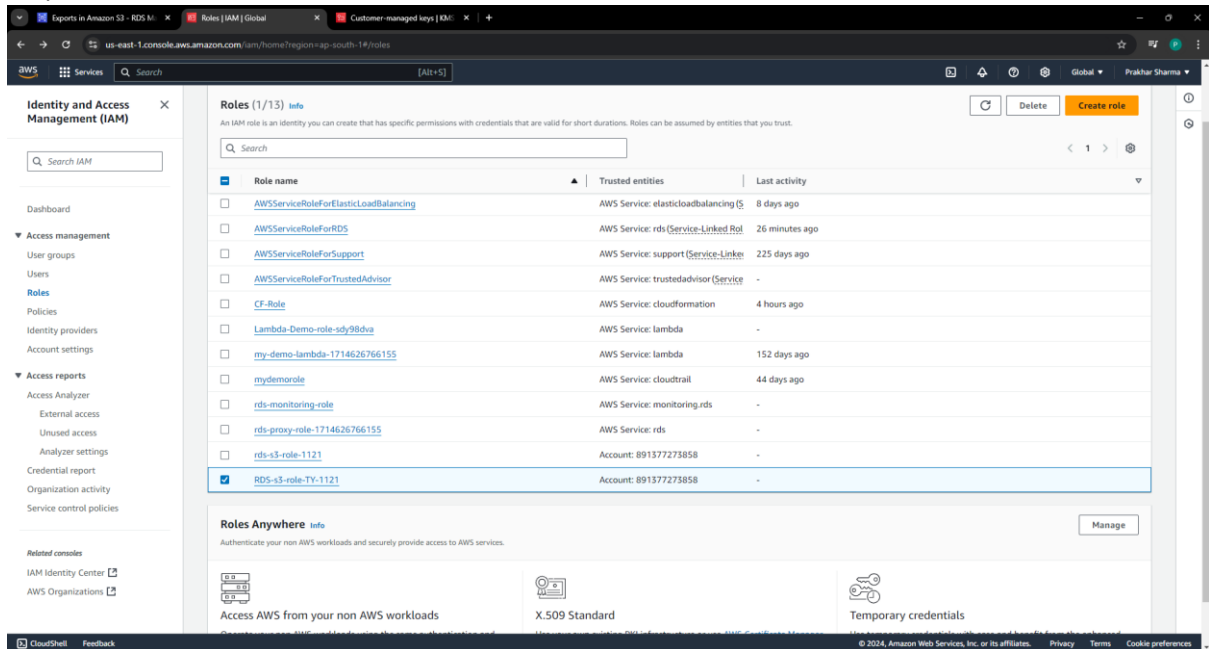
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma

PRN: 20220801121

Title of Practical : Export Amazon RDS DB Snapshot to S3

Step-42]Select and click on the RDS role.



The screenshot shows the AWS IAM console 'Roles' page. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, Access reports, and Related consoles. The main content area displays a table of roles. The role 'RDS-s3-role-TY-1121' is selected, highlighted in blue. Below the table, there are sections for 'Roles Anywhere' and 'Temporary credentials'.

Role name	Trusted entities	Last activity
AWSServiceRoleForElasticLoadBalancing	AWS Service: elasticloadbalancing	8 days ago
AWSServiceRoleForRDS	AWS Service: rds (Service-Linked Role)	26 minutes ago
AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	225 days ago
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-
CF-Role	AWS Service: cloudformation	4 hours ago
Lambda-Demo-role-sdy98dvg	AWS Service: lambda	-
my-demo-lambda-1714626766155	AWS Service: lambda	152 days ago
mydemorole	AWS Service: cloudtrail	44 days ago
rds-monitoring-role	AWS Service: monitoring.rds	-
rds-proxy-role-1714626766155	AWS Service: rds	-
rds-s3-role-1121	Account: 891377273858	-
RDS-s3-role-TY-1121	Account: 891377273858	-

School of Computer Science, Engineering and Applications(SCSEA)

B.C.A. TY (CCSA)

Subject : Advanced Cloud Computing (P)

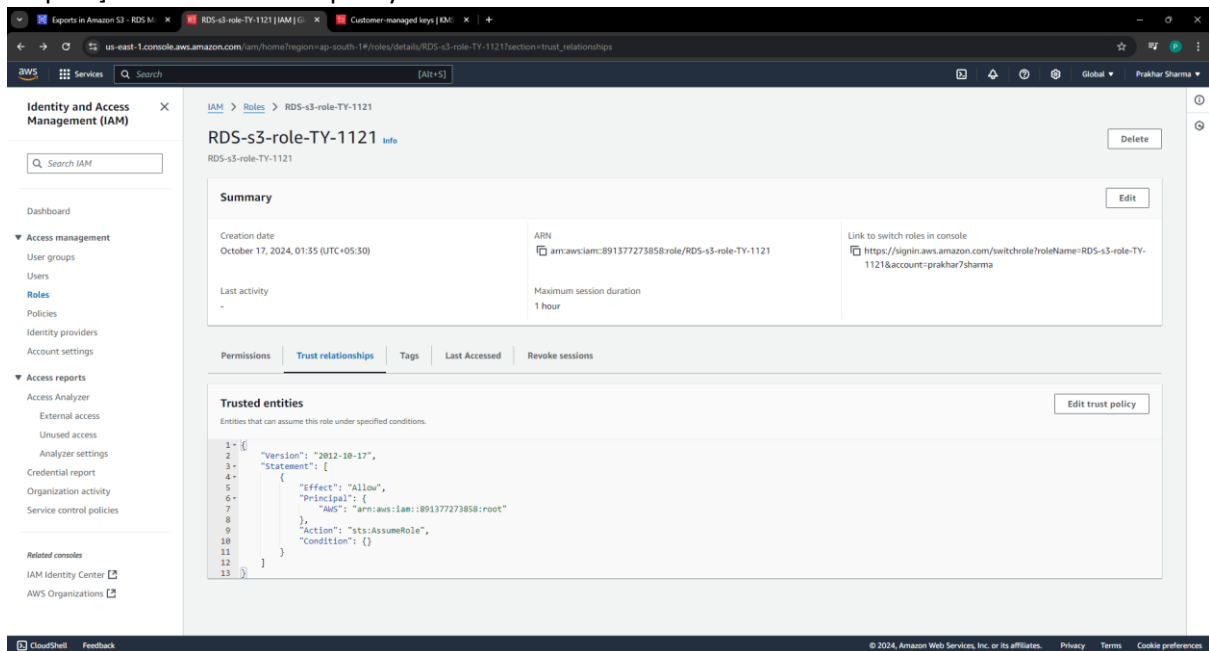
Name of the Student: Prakhar Anil Sharma

PRN: 20220801121

Title of Practical : Export Amazon RDS DB Snapshot to S3

Step-43]Go to Trust relationships tab.

Step-44] Click on edit trust policy.



The screenshot shows the AWS IAM console interface. The left sidebar contains navigation links for Identity and Access Management (IAM), including Dashboard, Access management, Users, Roles, Policies, Identity providers, Account settings, Access reports, Access Analyzer, External access, Unused access, Analyzer settings, Credential report, Organization activity, and Service control policies. The main content area displays the 'RDS-s3-role-TY-1121' role details. The 'Trust relationships' tab is selected, showing a list of trusted entities. The 'Trusted entities' section displays a JSON policy snippet with line numbers 1-13. Line 7 is highlighted, corresponding to the instruction in Step-45.

```
1- {  
2-   "Version": "2012-10-17",  
3-   "Statement": [  
4-     {  
5-       "Effect": "Allow",  
6-       "Principal": {  
7-         "AWS": "arn:aws:iam::891377273858:root"  
8-       },  
9-       "Action": "sts:AssumeRole",  
10-      "Condition": {}  
11-    }  
12-  ]  
13- }
```

Step-45]In edit trust policy code, add this line below 7th line

- "Service": "export.rds.amazonaws.com"



School of Computer Science, Engineering and Applications(SCSEA)

B.C.A. TY (CCSA)

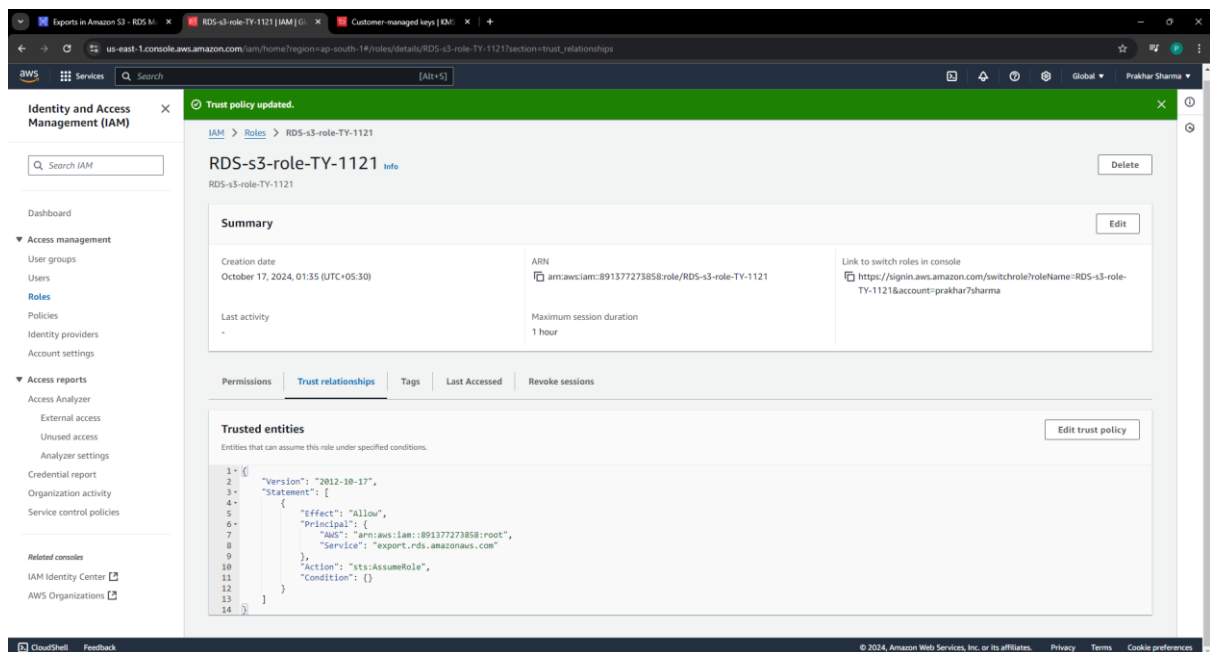
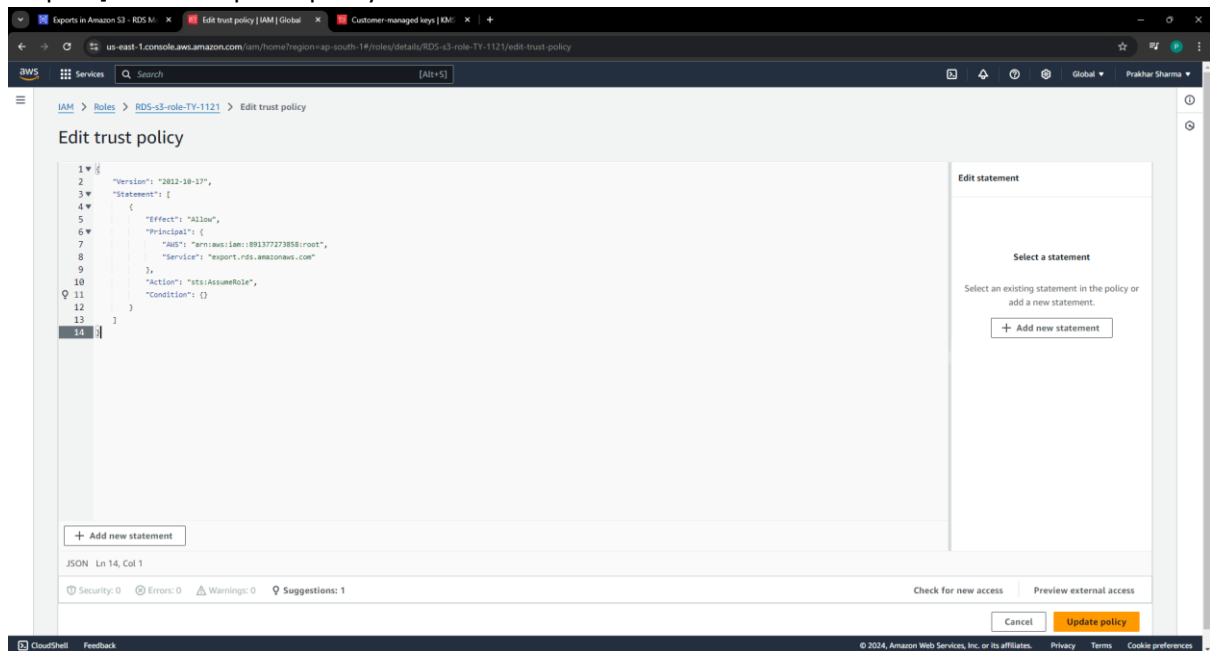
Subject : Advanced Cloud Computing (P)

Name of the Student: **Prakhar Anil Sharma**

PRN: **20220801121**

Title of Practical : **Export Amazon RDS DB Snapshot to S3**

Step-46] Click on Update policy.



PRN: 20220801121

1
9

School of Computer Science, Engineering and Applications(SCSEA)

B.C.A. TY (CCSA)

Subject : Advanced Cloud Computing (P)

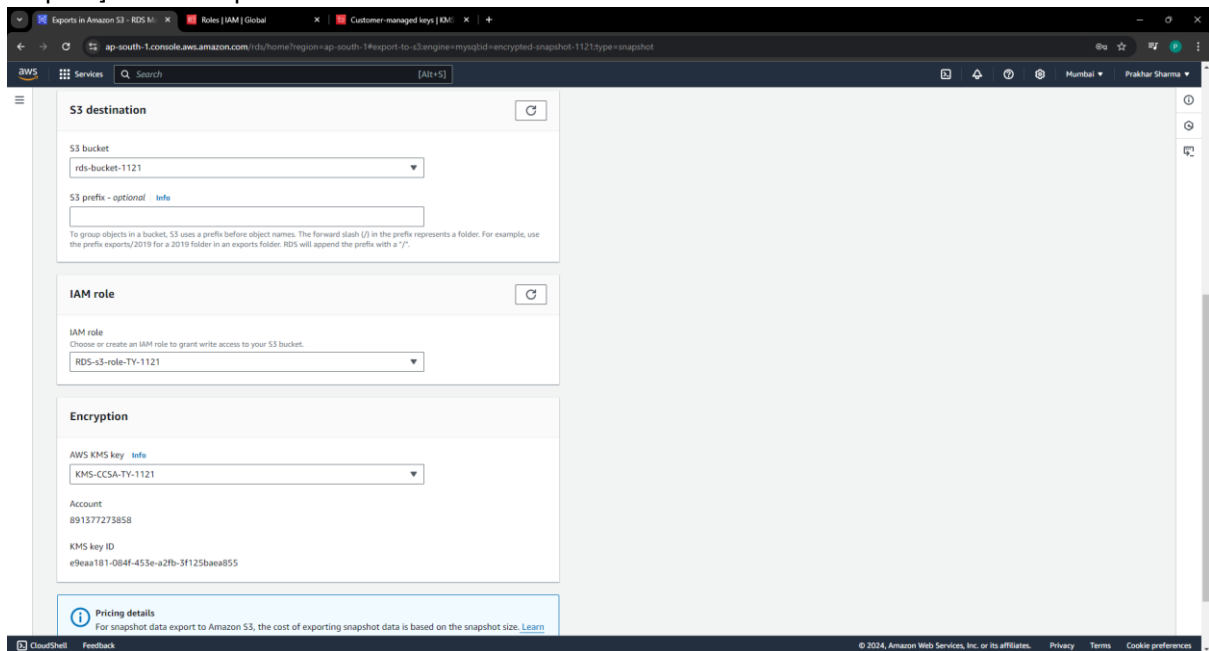
Name of the Student: Prakhar Anil Sharma

PRN: 20220801121

Title of Practical : Export Amazon RDS DB Snapshot to S3

Now go back to the RDS Export to Amazon S3 Tab ,their you can see the error is gone.

Step-47]Click on Export to Amazon S3.



The screenshot shows the AWS Management Console interface for configuring an export to Amazon S3. The page is titled 'Exports in Amazon S3 - RDS M...' and the URL is 'ap-south-1.console.aws.amazon.com/rds/home?region=ap-south-1#export-to-s3:engine=mysql&id=encrypted-snapshot-1121?type=snapshot'. The configuration is divided into three main sections: 'S3 destination', 'IAM role', and 'Encryption'. In the 'S3 destination' section, the 'S3 bucket' is set to 'rds-bucket-1121' and the 'S3 prefix - optional' is empty. In the 'IAM role' section, the 'IAM role' is set to 'RDS-s3-role-TY-1121'. In the 'Encryption' section, the 'AWS KMS key' is set to 'KMS-CCSA-TY-1121'. Below these sections, there is a 'Pricing details' section with a note: 'For snapshot data export to Amazon S3, the cost of exporting snapshot data is based on the snapshot size. [Learn](#)'. The footer of the console shows 'CloudShell', 'Feedback', and copyright information for Amazon Web Services, Inc. or its affiliates.

**School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)**

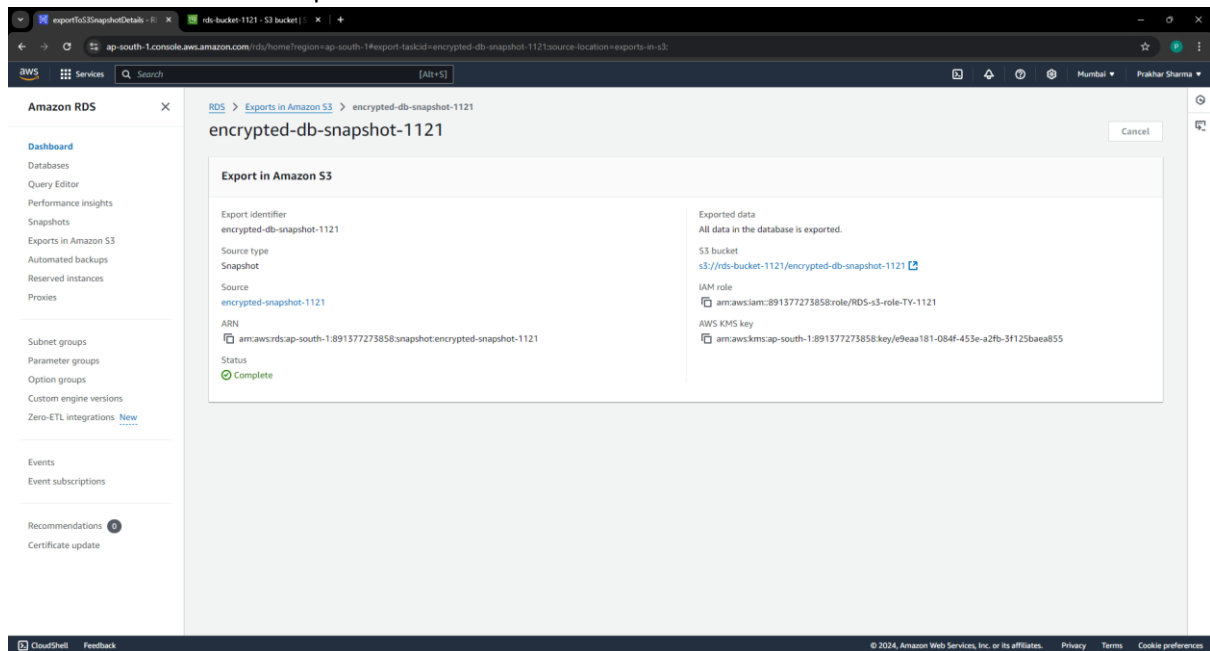
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma

PRN: 20220801121

Title of Practical : Export Amazon RDS DB Snapshot to S3

Wait till the status is Complete.



Step-48]Now Go to S3.

Step-49]Go to Buckets.

Step-50]Click on the RDS Bucket.

Step-51]Go to Objects tab.

**School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (CCSA)**

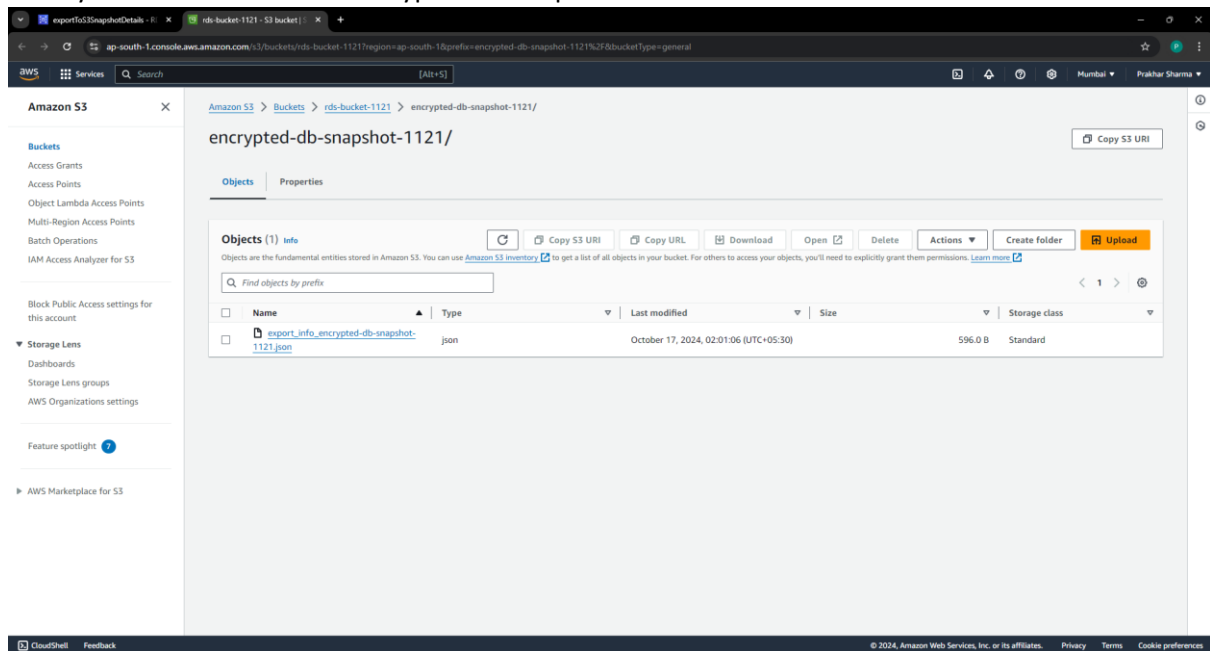
Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma

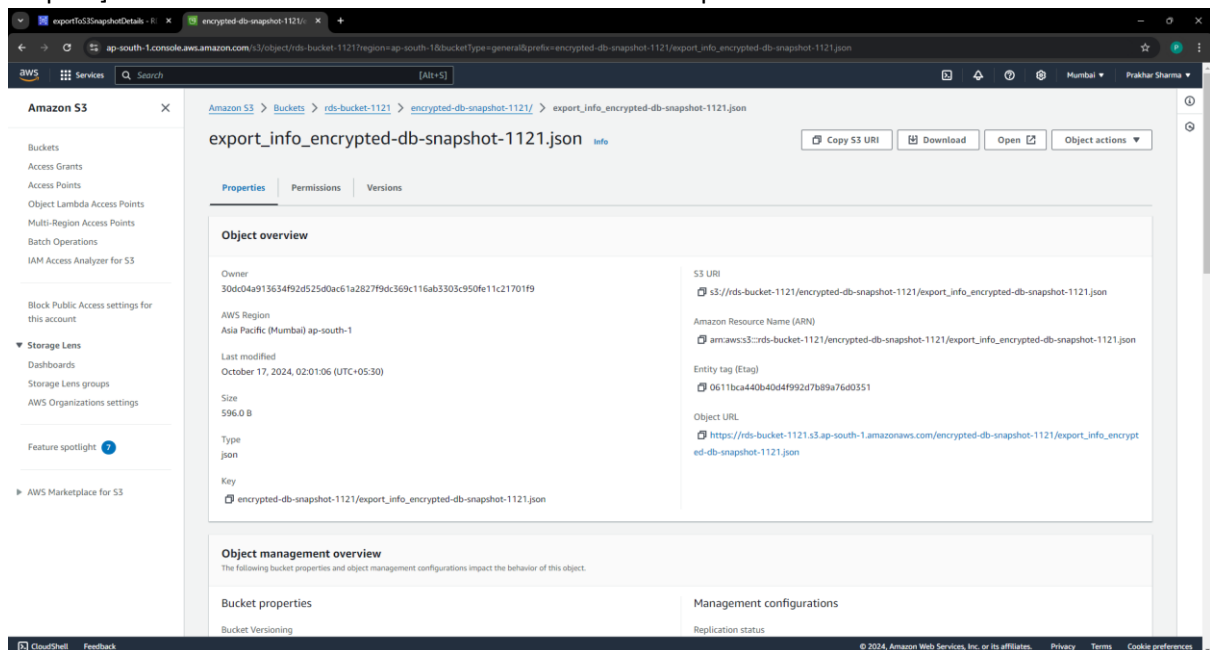
PRN: 20220801121

Title of Practical : Export Amazon RDS DB Snapshot to S3

Their you can see one file of encrypted db snapshot is visible.



Step-52]Click on the file to see the details of the file in Properties.



PRN: 20220801121

2
2



D Y PATIL
INTERNATIONAL
UNIVERSITY
AKURDI PUNE

School of Computer Science, Engineering and Applications(SCSEA)

B.C.A. TY (CCSA)

Subject : Advanced Cloud Computing (P)

Name of the Student: Prakhar Anil Sharma

PRN: 20220801121

Title of Practical : Export Amazon RDS DB Snapshot to S3