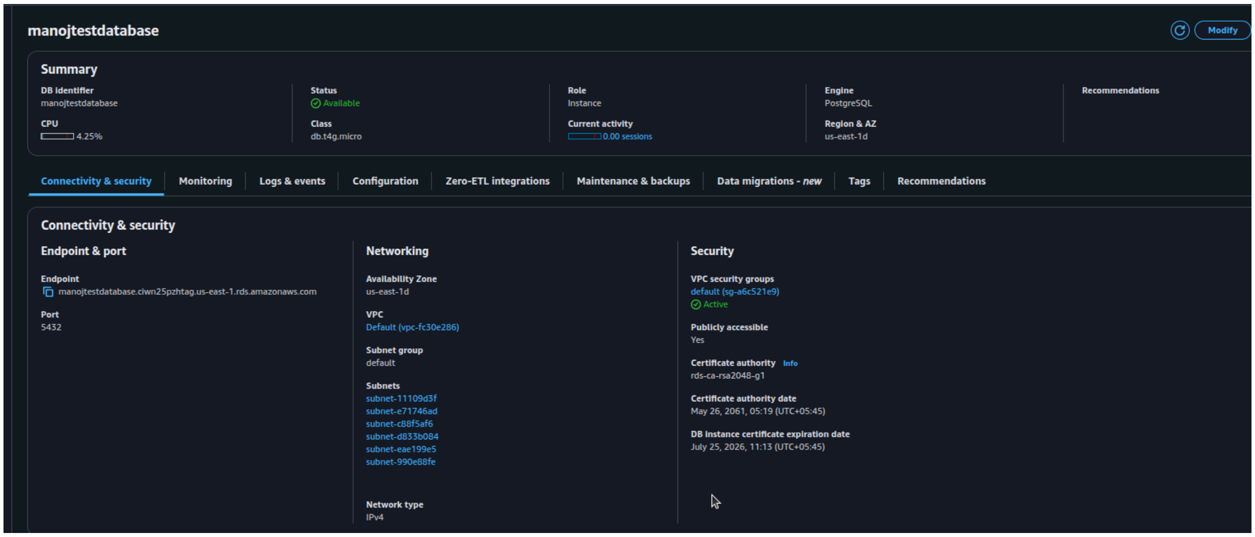
# Encrypted Postgres RDS instance Migration

## 1. The initial Database configurations:

Database info



manojtestdatabase

Summary

DB identifier
manojtestdatabase

CPU
4.25%

Status
Available

Class
db.t4g.micro

Role
Instance

Current activity
0.00 sessions

Engine
PostgreSQL

Region & AZ
us-east-1d

Recommendations

Connectivity & security

Endpoint & port

Endpoint
manojtestdatabase.ciwn25pzhtag.us-east-1.rds.amazonaws.com

Port
5432

Networking

Availability Zone
us-east-1d

VPC
Default (vpc-fc30e286)

Subnet group
default

Subnets
subnet-11109d3f
subnet-e71746ad
subnet-c88f5af6
subnet-d833b084
subnet-eae199e5
subnet-990e88fe

Network type
IPv4

Security

VPC security groups
default (sg-a6c521e9)
Active

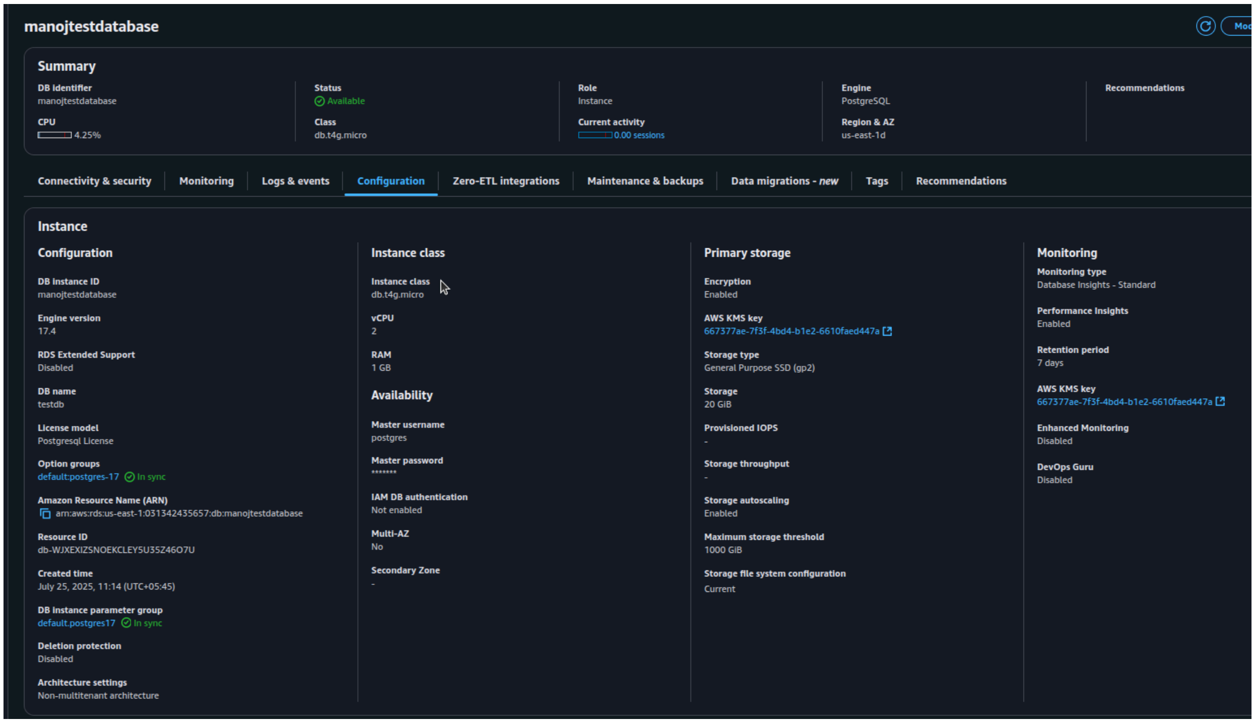
Publicly accessible
Yes

Certificate authority Info
rds-ca-rsa2048-g1

Certificate authority date
May 26, 2061, 05:19 (UTC+05:45)

DB instance certificate expiration date
July 25, 2026, 11:13 (UTC+05:45)

Configuration: **Encryption managed by AWS KMS (Encryption at rest)**



manojtestdatabase

Summary

DB identifier
manojtestdatabase

CPU
4.25%

Status
Available

Class
db.t4g.micro

Role
Instance

Current activity
0.00 sessions

Engine
PostgreSQL

Region & AZ
us-east-1d

Recommendations

Instance

Configuration

DB instance ID
manojtestdatabase

Engine version
17.4

RDS Extended Support
Disabled

DB name
testdb

License model
Postgresql License

Option groups
default:postgres-17 In sync

Amazon Resource Name (ARN)
arn:aws:rds:us-east-1:031342435657:db:manojtestdatabase

Resource ID
db-WJXEXIZSNOEKCLEY5U35Z46O7U

Created time
July 25, 2025, 11:14 (UTC+05:45)

DB instance parameter group
default.postgres17 In sync

Deletion protection
Disabled

Architecture settings
Non-multitenant architecture

Instance class

Instance class
db.t4g.micro

vCPU
2

RAM
1 GB

Availability

Master username
postgres

Master password
*******

IAM DB authentication
Not enabled

Multi-AZ
No

Secondary Zone
-

Primary storage

Encryption
Enabled

AWS KMS key
667377ae-7f3f-4bd4-b1e2-6610faed447a

Storage type
General Purpose SSD (gp2)

Storage
20 GiB

Provisioned IOPS
-

Storage throughput
-

Storage autoscaling
Enabled

Maximum storage threshold
1000 GiB

Storage file system configuration
Current

Monitoring

Monitoring type
Database Insights - Standard

Performance Insights
Enabled

Retention period
7 days

AWS KMS key
667377ae-7f3f-4bd4-b1e2-6610faed447a

Enhanced Monitoring
Disabled

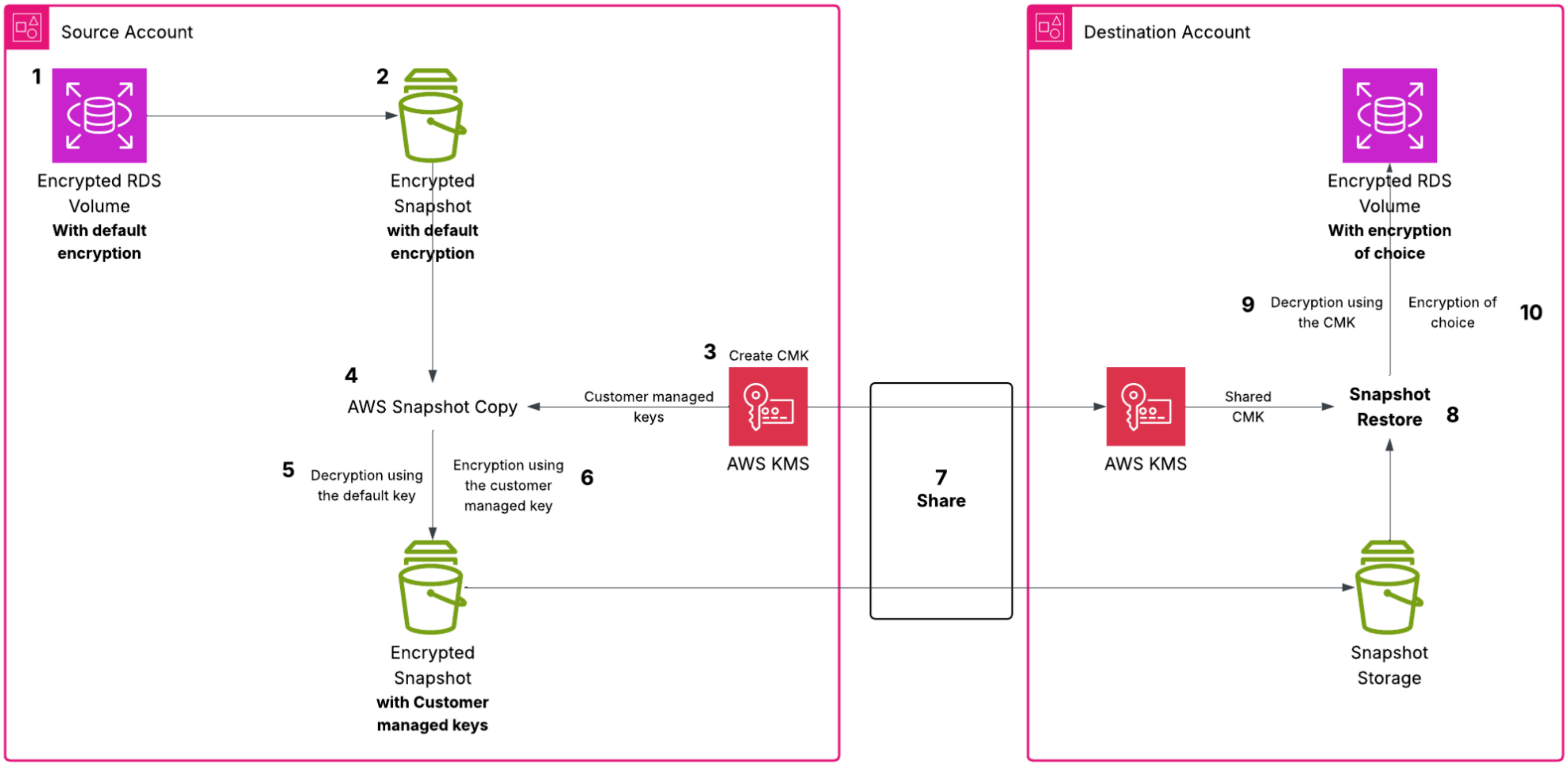
DevOps Guru
Disabled

## 2. Creating snapshot:

Ref:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/share-encrypted-snapshot.html

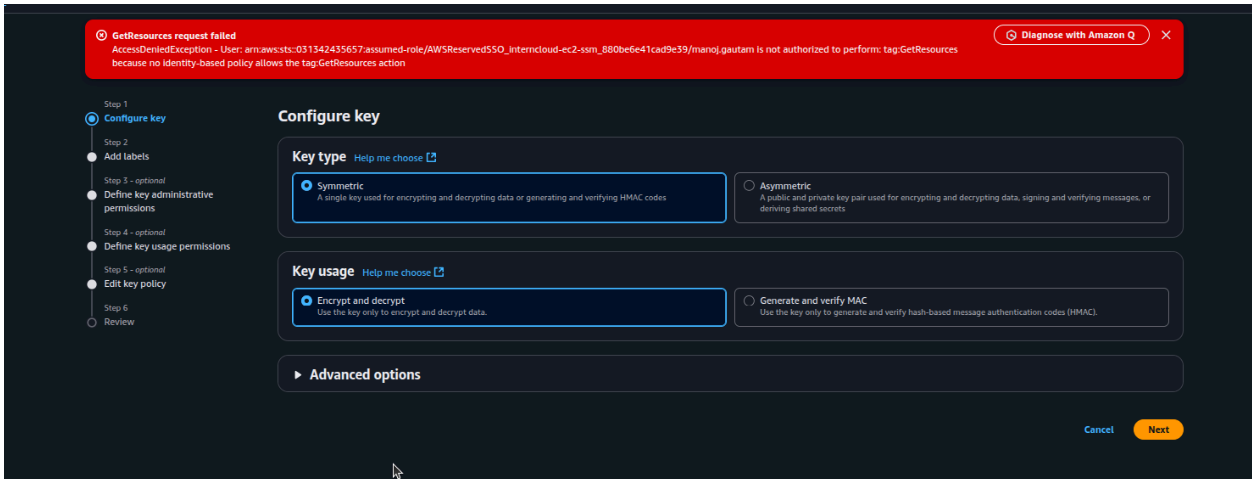
**“You can't share a snapshot that has been encrypted using the default KMS key of the AWS account that shared the snapshot.”**

So with the official documentation, I've made a workflow with some internal operations, here's the overview.



***Note: The steps 5 and 9 happens in the background***

# Customer Managed Keys Configuration:



**GetResources request failed**
AccessDeniedException - User: arn:aws:sts::031342435657:assumed-role/AWSReservedSSO_interncloud-ec2-ssm_880be6e41cad9e39/manoj.gautam is not authorized to perform: tag:GetResources because no identity-based policy allows the tag:GetResources action

Step 1
Configure key
Step 2
Add labels
Step 3 - *optional*
Define key administrative permissions
Step 4 - *optional*
Define key usage permissions
Step 5 - *optional*
Edit key policy
Step 6
Review

## Configure key

**Key type** Help me choose

● Symmetric
A single key used for encrypting and decrypting data or generating and verifying HMAC codes

○ Asymmetric
A public and private key pair used for encrypting and decrypting data, signing and verifying messages, or deriving shared secrets

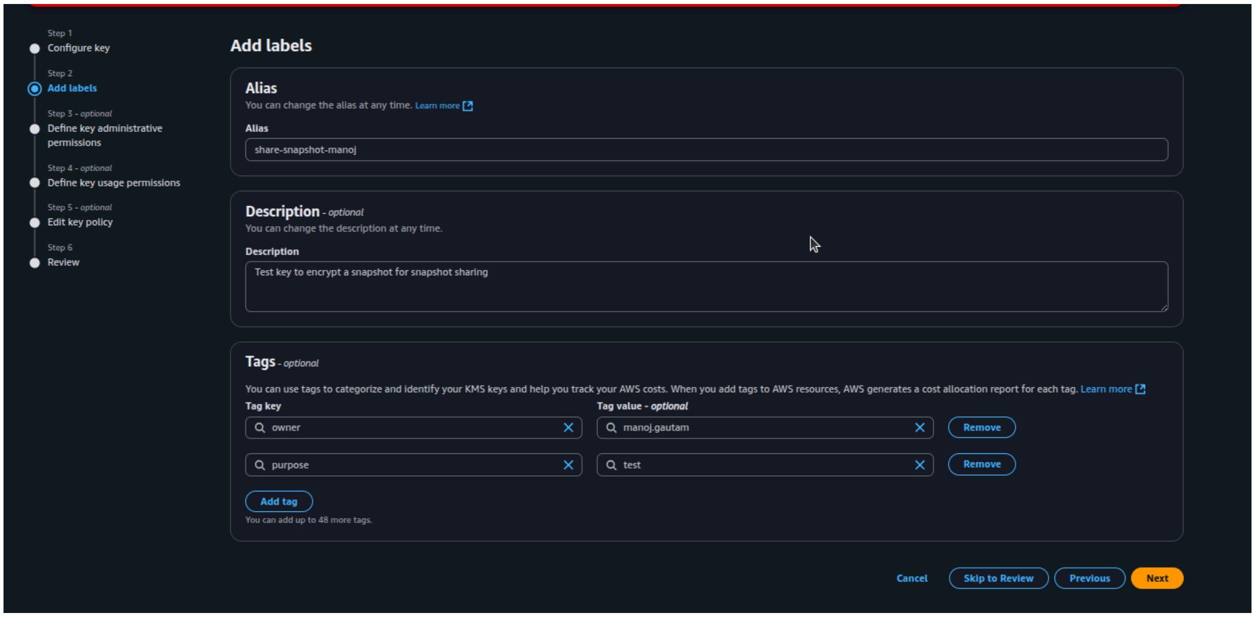
**Key usage** Help me choose

● Encrypt and decrypt
Use the key only to encrypt and decrypt data.

○ Generate and verify MAC
Use the key only to generate and verify hash-based message authentication codes (HMAC).

▸ Advanced options

Make alias and have labels



Step 1
Configure key
Step 2
Add labels
Step 3 - *optional*
Define key administrative permissions
Step 4 - *optional*
Define key usage permissions
Step 5 - *optional*
Edit key policy
Step 6
Review

## Add labels

**Alias**
You can change the alias at any time. Learn more

Alias: share-snapshot-manoj

**Description** - *optional*
You can change the description at any time.

Description: Test key to encrypt a snapshot for snapshot sharing

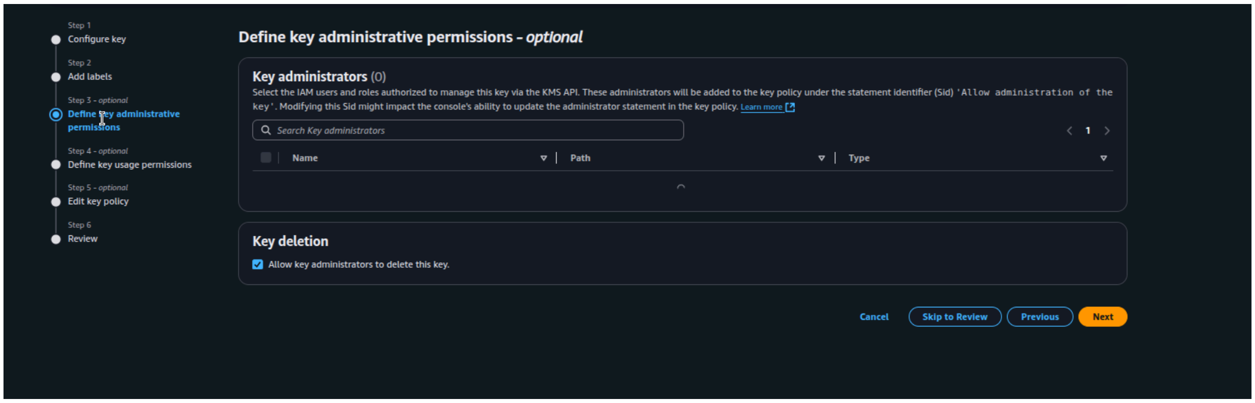
**Tags** - *optional*
You can use tags to categorize and identify your KMS keys and help you track your AWS costs. When you add tags to AWS resources, AWS generates a cost allocation report for each tag. Learn more

| Tag key | Tag value - *optional* |
|---|---|
| owner | manoj.gautam |
| purpose | test |

You can add up to 48 more tags.

Heres a youtube video for sharing KMS keys: [https://youtu.be/AjhaqY1GOrc](https://youtu.be/AjhaqY1GOrc)

Skip through this page



Step 1
Configure key

Step 2
Add labels

Step 3 - *optional*
Define key administrative permissions

Step 4 - *optional*
Define key usage permissions

Step 5 - *optional*
Edit key policy

Step 6
Review

**Define key administrative permissions - *optional***

**Key administrators** (0)

Select the IAM users and roles authorized to manage this key via the KMS API. These administrators will be added to the key policy under the statement identifier (Sid) `'Allow administration of the key'`. Modifying this Sid might impact the console's ability to update the administrator statement in the key policy. Learn more

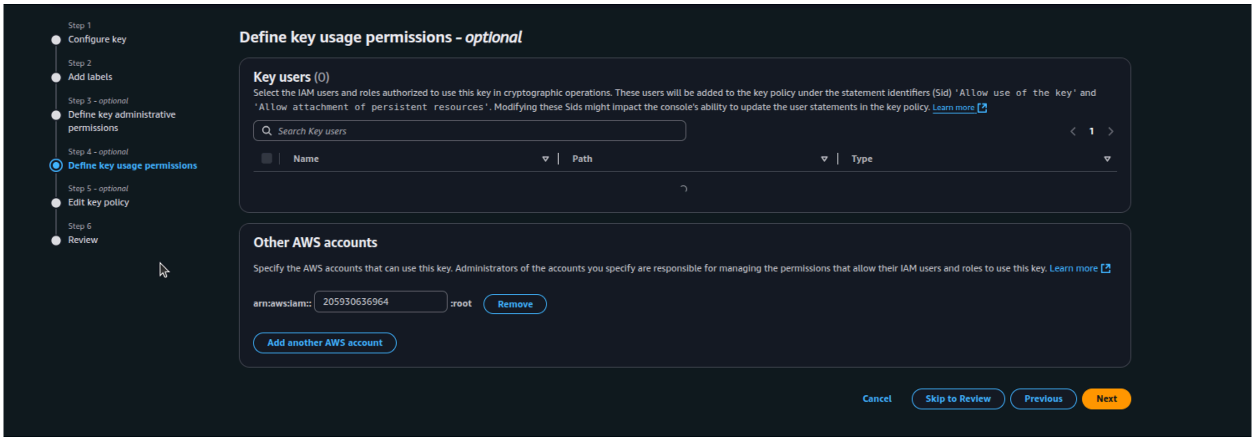
| □ Name | Path | Type |
|---|---|---|

**Key deletion**

☑ Allow key administrators to delete this key.

This is the important part:

In **Other AWS accounts,** insert ID of the destination account so that the destination account can also use the customer managed key



Step 1
Configure key

Step 2
Add labels

Step 3 - *optional*
Define key administrative permissions

Step 4 - *optional*
Define key usage permissions

Step 5 - *optional*
Edit key policy

Step 6
Review

**Define key usage permissions - *optional***

**Key users** (0)

Select the IAM users and roles authorized to use this key in cryptographic operations. These users will be added to the key policy under the statement identifiers (Sid) `'Allow use of the key'` and `'Allow attachment of persistent resources'`. Modifying these Sids might impact the console's ability to update the user statements in the key policy. Learn more

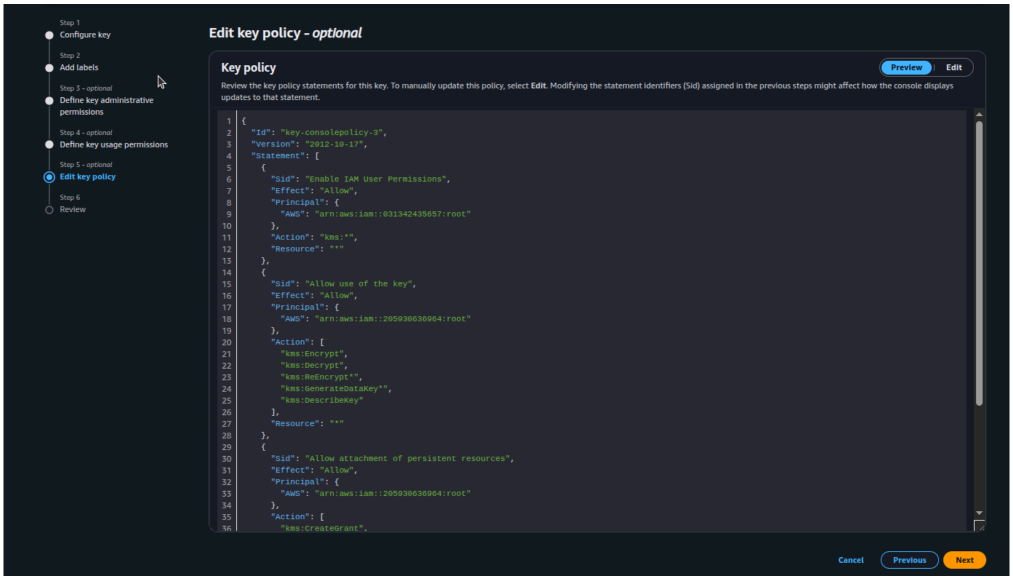
| □ Name | Path | Type |
|---|---|---|

**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

arn:aws:iam:: 205930636964 :root

**Critical Note: The Key does not appear in the console of the destination account even though it's shared. But we can use it for the actions described in the KMS policy(Source account).**



Edit key policy - *optional*

Key policy

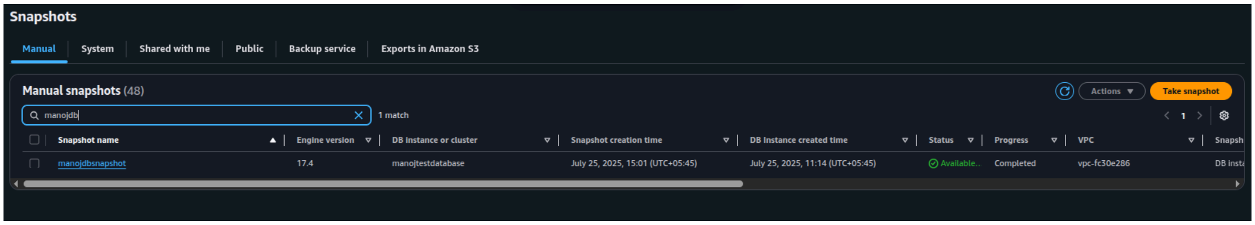
Review the key policy statements for this key. To manually update this policy, select **Edit**. Modifying the statement identifiers (Sid) assigned in the previous steps might affect how the console displays updates to that statement.

```
{
  "Id": "key-consolepolicy-3",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::031342435657:root"
      },
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Sid": "Allow use of the key",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::205930636964:root"
      },
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    },
    {
      "Sid": "Allow attachment of persistent resources",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::205930636964:root"
      },
      "Action": [
        "kms:CreateGrant",
```

## 3. Snapshot Sharing:

Now for the most important part, snapshot sharing.

First make an original snapshot,

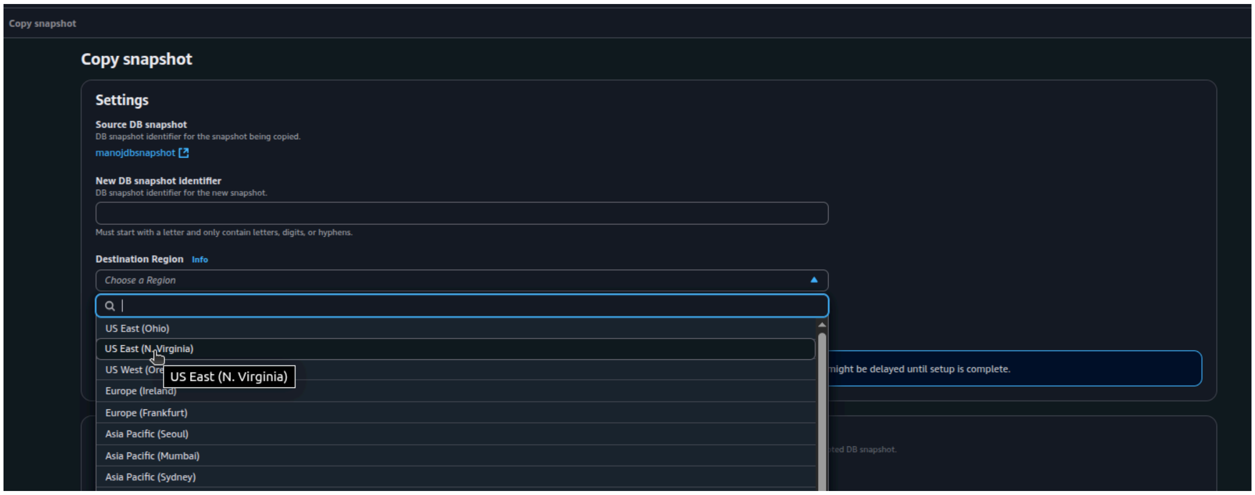


Manual snapshots (48)

Search: manojdb — 1 match

| □ | Snapshot name | Engine version | DB instance or cluster | Snapshot creation time | DB Instance created time | Status | Progress | VPC | Snapsh |
|---|---|---|---|---|---|---|---|---|---|
| □ | manojdbsnapshot | 17.4 | manojtestdatabase | July 25, 2025, 15:01 (UTC+05:45) | July 25, 2025, 11:14 (UTC+05:45) | ✓ Available.. | Completed | vpc-fc30e286 | DB insta |

Now make a **copy snapshot** (*necessary for encryption with our customer managed KMS key*). First while copying, make sure that the snapshot is in the **same region** as the key.



Copy snapshot

Settings

**Source DB snapshot**
DB snapshot identifier for the snapshot being copied.
manojdbsnapshot

**New DB snapshot identifier**
DB snapshot identifier for the new snapshot.
Must start with a letter and only contain letters, digits, or hyphens.

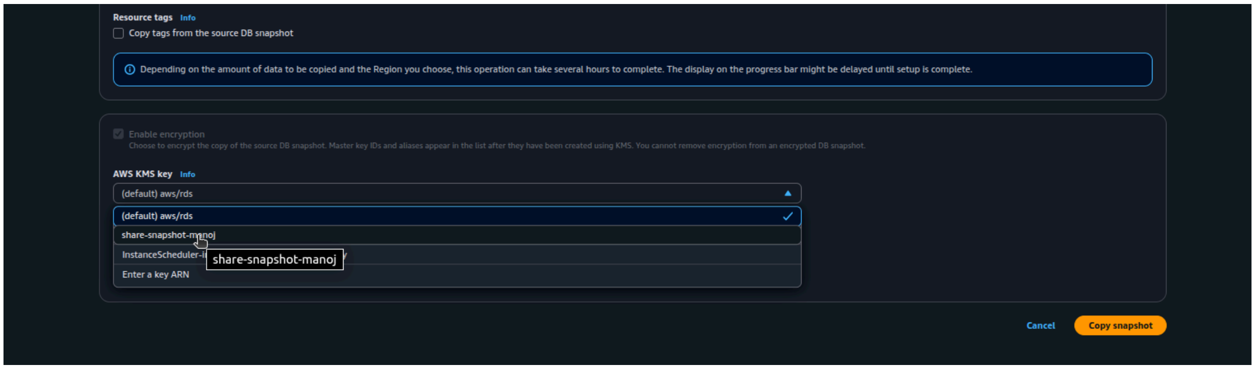
**Destination Region**
Choose a Region

- US East (Ohio)
- US East (N. Virginia)
- US West (Ore
- Europe (Ireland)
- Europe (Frankfurt)
- Asia Pacific (Seoul)
- Asia Pacific (Mumbai)
- Asia Pacific (Sydney)

might be delayed until setup is complete.

ted DB snapshot.

Then select the KMS key as our newly created customer managed KMS Key.



**Resource tags** Info

□ Copy tags from the source DB snapshot

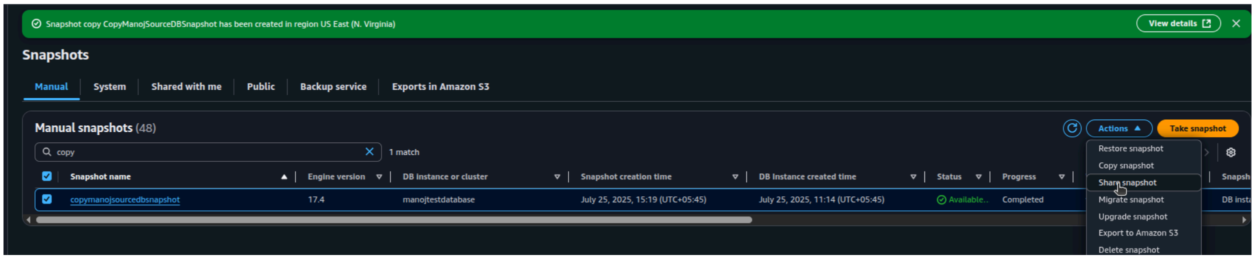
ⓘ Depending on the amount of data to be copied and the Region you choose, this operation can take several hours to complete. The display on the progress bar might be delayed until setup is complete.

☑ Enable encryption
Choose to encrypt the copy of the source DB snapshot. Master key IDs and aliases appear in the list after they have been created using KMS. You cannot remove encryption from an encrypted DB snapshot.

**AWS KMS key** Info

(default) aws/rds

Now we can go ahead and share our newly encrypted snapshot with the destination account.



Snapshot copy CopyManojSourceDBSnapshot has been created in region US East (N. Virginia)

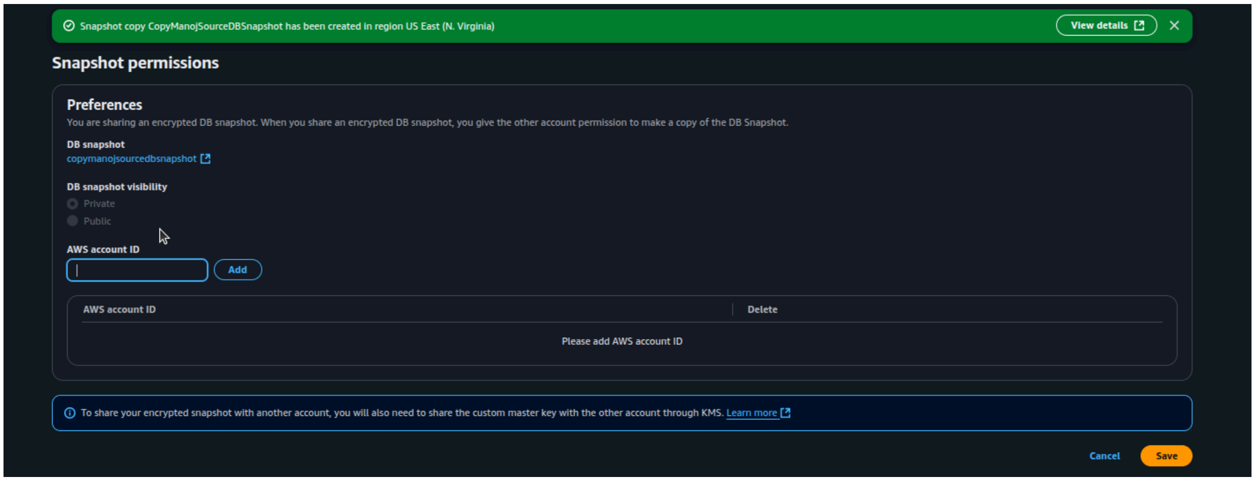
**Snapshots**

**Manual snapshots** (48)

copy — 1 match

| ☑ | Snapshot name | Engine version | DB instance or cluster | Snapshot creation time | DB Instance created time | Status | Progress | Snapsh |
|---|---|---|---|---|---|---|---|---|
| ☑ | copymanojsourcedbsnapshot | 17.4 | manojtestdatabase | July 25, 2025, 15:19 (UTC+05:45) | July 25, 2025, 11:14 (UTC+05:45) | Available.. | Completed | DB insta |

Add the account number of destination account:



Snapshot copy CopyManojSourceDBSnapshot has been created in region US East (N. Virginia)

**Snapshot permissions**

**Preferences**

You are sharing an encrypted DB snapshot. When you share an encrypted DB snapshot, you give the other account permission to make a copy of the DB Snapshot.

**DB snapshot**
copymanojsourcedbsnapshot

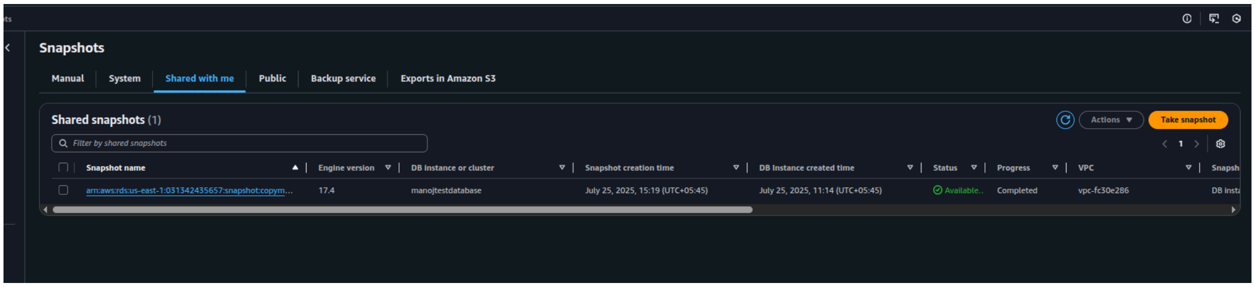
**DB snapshot visibility**
○ Private
○ Public

**AWS account ID**

| AWS account ID | Delete |
|---|---|
| Please add AWS account ID | |

ⓘ To share your encrypted snapshot with another account, you will also need to share the custom master key with the other account through KMS. Learn more

Confirm that you can see the snapshot in **Shared with me** section,



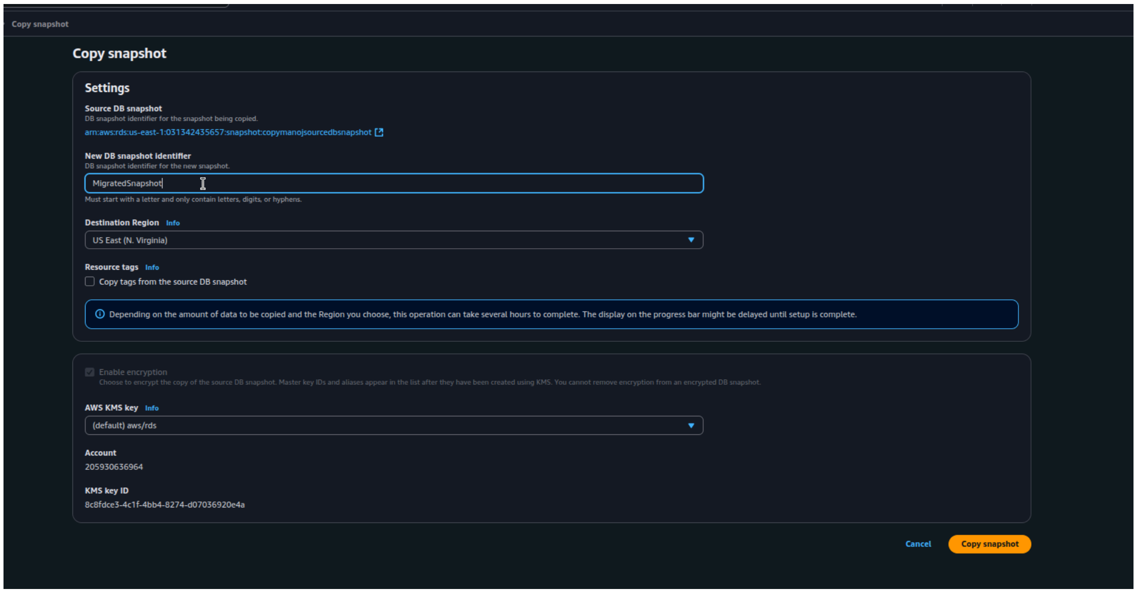
**Snapshots**

**Shared snapshots** (1)

Filter by shared snapshots

| □ | Snapshot name | Engine version | DB instance or cluster | Snapshot creation time | DB Instance created time | Status | Progress | VPC | Snapsh |
|---|---|---|---|---|---|---|---|---|---|
| □ | arn:aws:rds:us-east-1:031342435657:snapshot:copym... | 17.4 | manojtestdatabase | July 25, 2025, 15:19 (UTC+05:45) | July 25, 2025, 11:14 (UTC+05:45) | Available.. | Completed | vpc-fc30e286 | DB insta |

Now again copy the snapshot, now we are using the default KMS dey for encryption:



Copy snapshot

## Copy snapshot

### Settings

**Source DB snapshot**
DB snapshot identifier for the snapshot being copied.
arn:aws:rds:us-east-1:031342435657:snapshot:copymanojsourcedbsnapshot

**New DB snapshot identifier**
DB snapshot identifier for the new snapshot.
MigratedSnapshot
Must start with a letter and only contain letters, digits, or hyphens.

**Destination Region** Info
US East (N. Virginia)

**Resource tags** Info
□ Copy tags from the source DB snapshot

ⓘ Depending on the amount of data to be copied and the Region you choose, this operation can take several hours to complete. The display on the progress bar might be delayed until setup is complete.

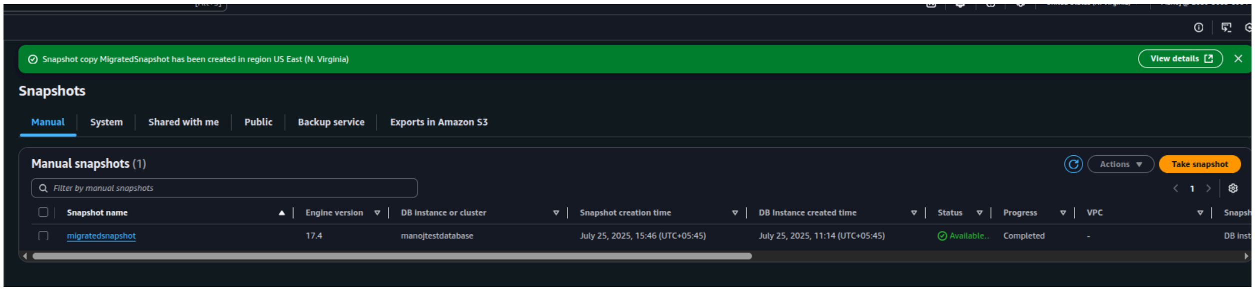
☑ Enable encryption
Choose to encrypt the copy of the source DB snapshot. Master key IDs and aliases appear in the list after they have been created using KMS. You cannot remove encryption from an encrypted DB snapshot.

**AWS KMS key** Info
(default) aws/rds

**Account**
205930636964

**KMS key ID**
8c8fdce3-4c1f-4bb4-8274-d07036920e4a

The snapshot has been copied



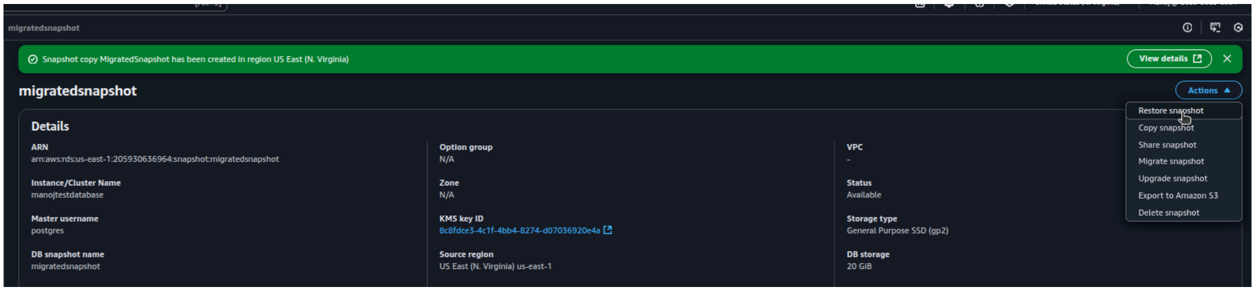
Snapshot copy MigratedSnapshot has been created in region US East (N. Virginia)

## Snapshots

**Manual snapshots** (1)

| Snapshot name | Engine version | DB instance or cluster | Snapshot creation time | DB instance created time | Status | Progress | VPC | Snapsh |
|---|---|---|---|---|---|---|---|---|
| migratedsnapshot | 17.4 | manojtestdatabase | July 25, 2025, 15:46 (UTC+05:45) | July 25, 2025, 11:14 (UTC+05:45) | Available.. | Completed | - | DB inst |

Now we restore the snapshot, we use the default KMS key.



migratedsnapshot

Snapshot copy MigratedSnapshot has been created in region US East (N. Virginia)

## migratedsnapshot

### Details

**ARN**
arn:aws:rds:us-east-1:205930636964:snapshot:migratedsnapshot

**Instance/Cluster Name**
manojtestdatabase

**Master username**
postgres

**DB snapshot name**
migratedsnapshot

**Option group**
N/A

**Zone**
N/A

**KMS key ID**
8c8fdce3-4c1f-4bb4-8274-d07036920e4a

**Source region**
US East (N. Virginia) us-east-1

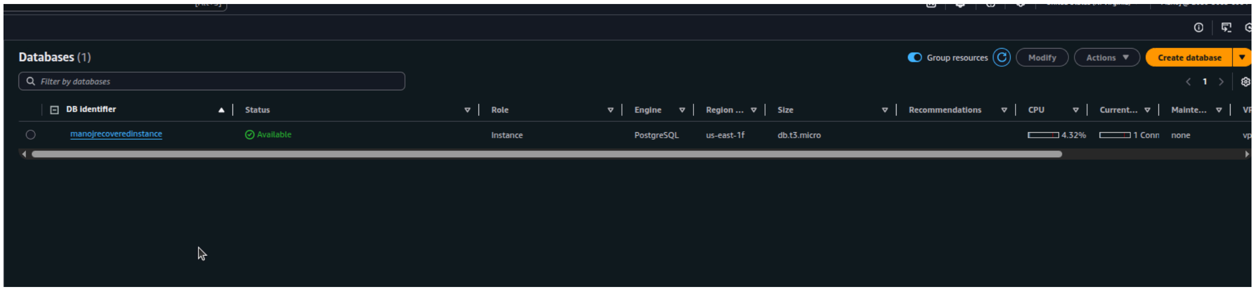
**VPC**
-

**Status**
Available

**Storage type**
General Purpose SSD (gp2)

**DB storage**
20 GiB

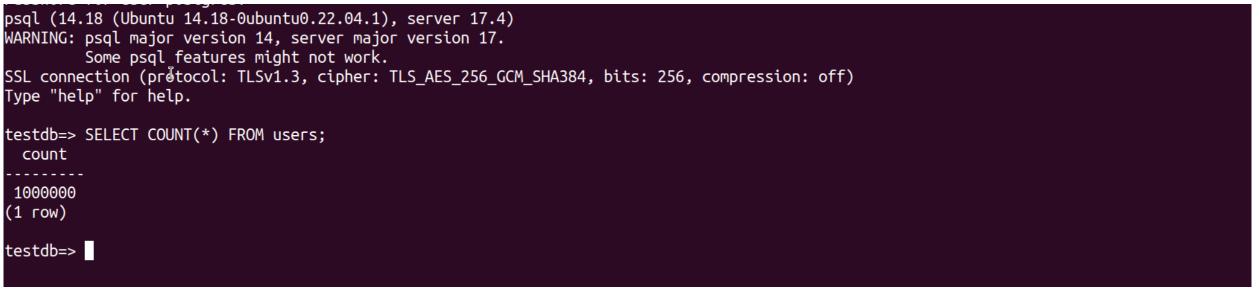
Now the database has been successfully restored.



**Databases** (1)

| DB identifier | Status | Role | Engine | Region ... | Size | Recommendations | CPU | Current... | Mainte... | VP |
|---|---|---|---|---|---|---|---|---|---|---|
| manojrecoveredinstance | Available | Instance | PostgreSQL | us-east-1f | db.t3.micro |  | 4.32% | 1 Conn | none | vp |

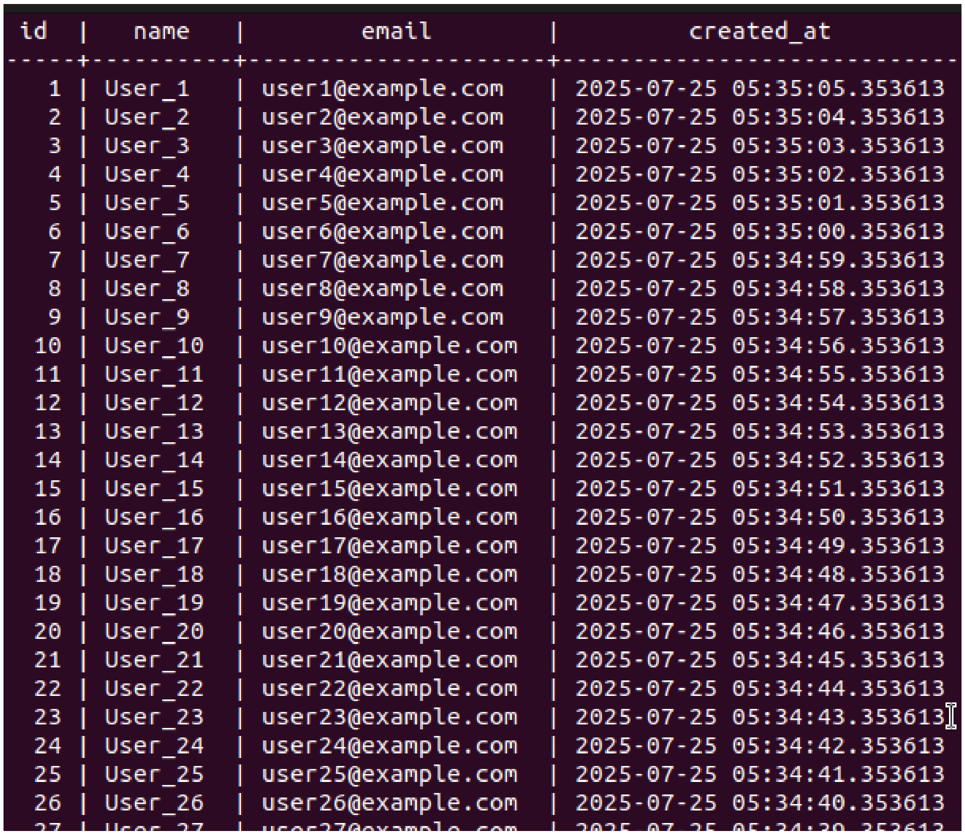
Checking the database Integrity:



```
psql (14.18 (Ubuntu 14.18-0ubuntu0.22.04.1), server 17.4)
WARNING: psql major version 14, server major version 17.
         Some psql features might not work.
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, bits: 256, compression: off)
Type "help" for help.

testdb=> SELECT COUNT(*) FROM users;
  count
---------
 1000000
(1 row)

testdb=> 
```



```
 id  |   name   |        email         |         created_at
-----+----------+----------------------+----------------------------
   1 | User_1   | user1@example.com    | 2025-07-25 05:35:05.353613
   2 | User_2   | user2@example.com    | 2025-07-25 05:35:04.353613
   3 | User_3   | user3@example.com    | 2025-07-25 05:35:03.353613
   4 | User_4   | user4@example.com    | 2025-07-25 05:35:02.353613
   5 | User_5   | user5@example.com    | 2025-07-25 05:35:01.353613
   6 | User_6   | user6@example.com    | 2025-07-25 05:35:00.353613
   7 | User_7   | user7@example.com    | 2025-07-25 05:34:59.353613
   8 | User_8   | user8@example.com    | 2025-07-25 05:34:58.353613
   9 | User_9   | user9@example.com    | 2025-07-25 05:34:57.353613
  10 | User_10  | user10@example.com   | 2025-07-25 05:34:56.353613
  11 | User_11  | user11@example.com   | 2025-07-25 05:34:55.353613
  12 | User_12  | user12@example.com   | 2025-07-25 05:34:54.353613
  13 | User_13  | user13@example.com   | 2025-07-25 05:34:53.353613
  14 | User_14  | user14@example.com   | 2025-07-25 05:34:52.353613
  15 | User_15  | user15@example.com   | 2025-07-25 05:34:51.353613
  16 | User_16  | user16@example.com   | 2025-07-25 05:34:50.353613
  17 | User_17  | user17@example.com   | 2025-07-25 05:34:49.353613
  18 | User_18  | user18@example.com   | 2025-07-25 05:34:48.353613
  19 | User_19  | user19@example.com   | 2025-07-25 05:34:47.353613
  20 | User_20  | user20@example.com   | 2025-07-25 05:34:46.353613
  21 | User_21  | user21@example.com   | 2025-07-25 05:34:45.353613
  22 | User_22  | user22@example.com   | 2025-07-25 05:34:44.353613
  23 | User_23  | user23@example.com   | 2025-07-25 05:34:43.353613
  24 | User_24  | user24@example.com   | 2025-07-25 05:34:42.353613
  25 | User_25  | user25@example.com   | 2025-07-25 05:34:41.353613
  26 | User_26  | user26@example.com   | 2025-07-25 05:34:40.353613
```

**This deems our procedure as success !**