

Home / AWS / Guided Lab / How to Encrypt an Unencrypted RDS DB Instance

How to Encrypt an Unencrypted RDS DB Instance

Level: Intermediate

Amazon RDS Amazon Web Services



1h 18m 39s left



End Lab

Open Console

Validation



Whiz_User_80425.62576945



Password ⓘ

25441d01-d556-4366-a5cd-73dddffb4c77



Access Key ⓘ

AKIAVD6UN6VZCVSRU2PY



Secret Key ⓘ

jKLhxmEEoP9aqP9ZcSwsEsoDmBr6J+RB!ptA/ggE



Lab Resources






No Lab Resources Found

Support Documents



1. FAQs and Troubleshooting

Need help?

-  How to use Hands on Lab
-  Troubleshooting Lab
-  FAQs

[Submit Feedback](#)[Share](#)[Lab Overview](#)[Lab Steps](#)[Lab Validation](#)[Lab FAQs](#) Database Engineer Database

Lab Steps

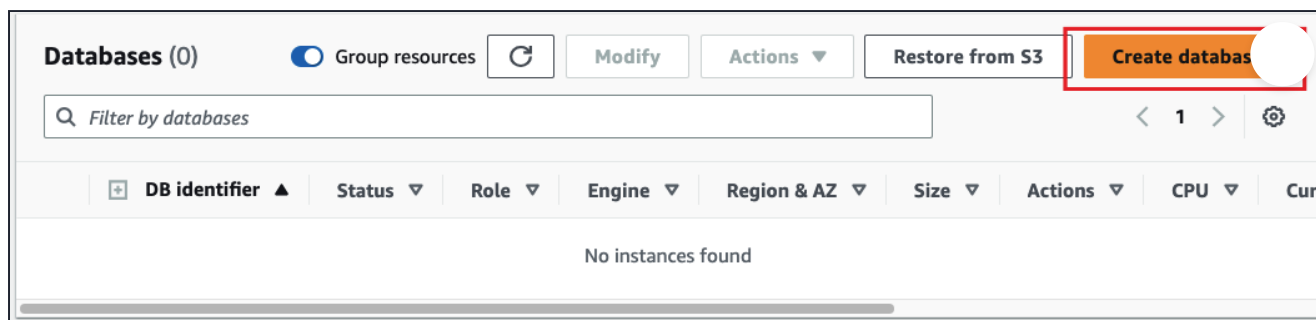
Task 1: Sign in to AWS Management Console

1. Click on the **Open Console** button, and you will get redirected to AWS Console in a new browser tab.
2. On the AWS sign-in page,
 - Leave the Account ID as default. Never edit/remove the 12 digit Account ID present in the AWS Console. otherwise, you cannot proceed with the lab.
 - Now copy your **User Name** and **Password** in the Lab Console to the **IAM Username and Password** in AWS Console and click on the **Sign in** button.
3. Once Signed In to the AWS Management Console, Make the default AWS Region as **US East (N. Virginia) us-east-1**.

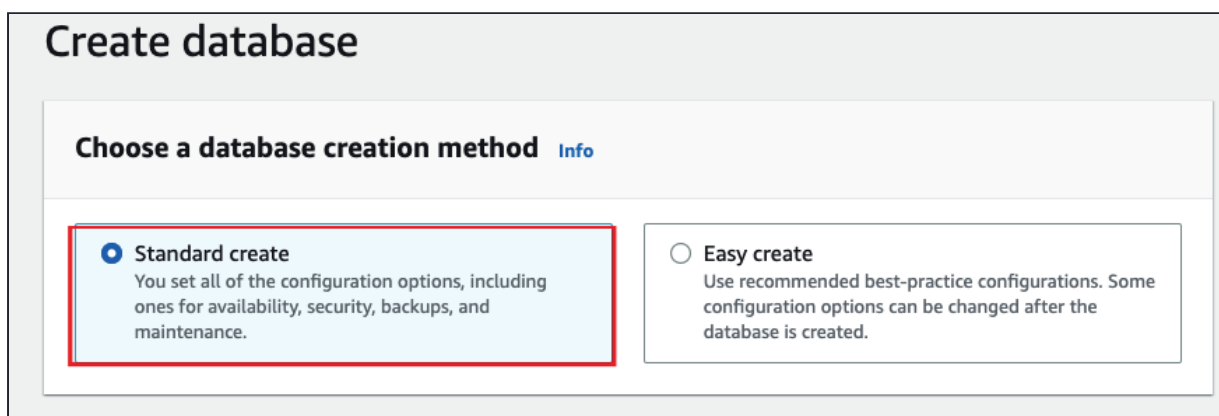
Task 2: Create an RDS DB Instance (without enabling the Encryption)

1. Navigate to the **Services** menu at the top left corner and click on **RDS** present under the **Database** section.
2. RDS dashboard is displayed.

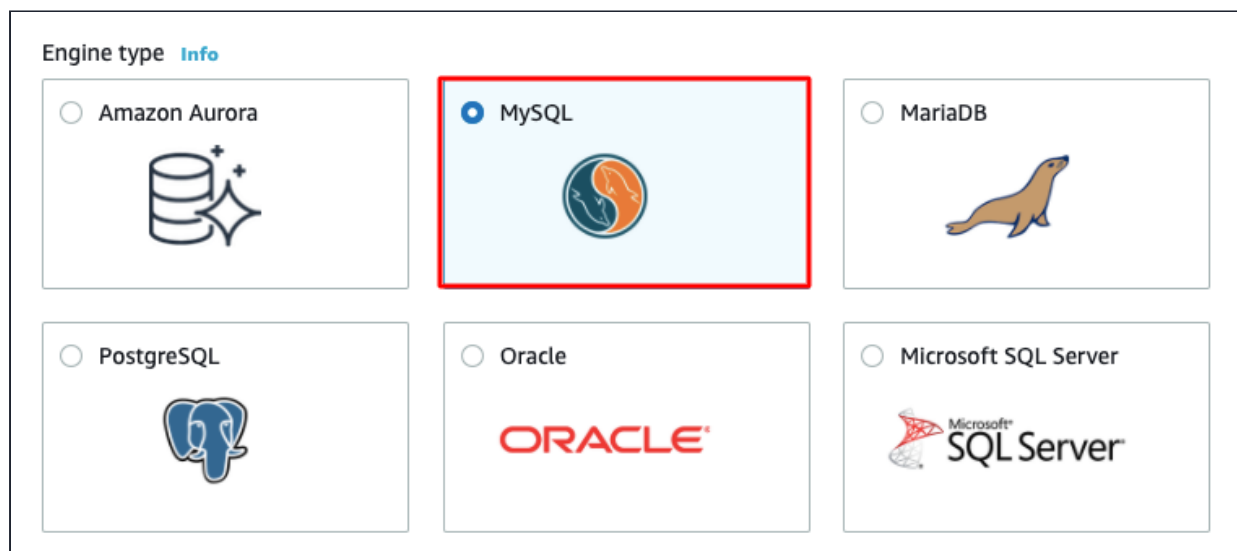
3. Click on **Create Database** and you are navigated to the page where you will provide all the required details to create a MySQL database.



4. On the page, click on the option **Standard create** a method for our lab requirement.



5. In the **Engine options**, select MySQL engine type.



6. **Edition:** Leave it as default

7. Under **Templates**, select the **Free tier** option.

Templates

Choose a sample template to meet your use case.

☐ **Production**
Use defaults for high availability and fast, consistent performance.

☐ **Dev/Test**
This instance is intended for development use outside of a production environment.

☒ **Free tier**
Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS.
[Info](#)

8. Under **Settings**, provide the following details.

- DB cluster identifier: Enter **test-db**
- Master username: Enter **master**
- Master password: Enter **Whizlabs123**
- Confirm password: Enter **Whizlabs123**

Note – Make sure the master and confirm passwords should be the same.

Settings

DB instance identifier [Info](#)
Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens (1 to 15 for SQL Server). First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

▼ Credentials Settings

Master username [Info](#)
Type a login ID for the master user of your DB instance.

1 to 16 alphanumeric characters. First character must be a letter
☐ **Auto generate a password**
Amazon RDS can generate a password for you, or you can specify your own password

Master password [Info](#)

Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), ' (single quote), " (double quote) and @ (at sign).

Confirm password [Info](#)

9. Under **DB instance class**, select **Burstable classes (includes t classes)** and select **db.t3.micro**

DB instance class

DB instance class [Info](#)
Choose a DB instance class that meets your processing power and memory requirements. The DB instance class options below are limited to those supported by the engine you selected above.

☐ Standard classes (includes m classes)

☐ Memory optimized classes (includes r and x classes)

☒ **Burstable classes (includes t classes)**

db.t3.micro
2 vCPUs 1 GiB RAM Network: 2,085 Mbps

☐ Include previous generation classes

10. Storage type : **General Purpose (SSD)**

11. Allocated storage : **20**

12. Uncheck **Enable storage autoscaling**.

13. Leave the **Availability and durability** as default.

14. Under **Connectivity**, make sure that **Public access** is **No**. Leave everything else as default.

15. Leave **Database Authentication** as default.

16. Expand the **Additional configuration**.

► Additional configuration
Database options, encryption enabled, backup enabled, backtrack disabled, delete protection enabled

17. In the displayed layout provide the following values under **Database options**.

- Initial database name : Enter ***projectdb***
- Leave **DB parameter group** and **Option group** as default.
- Under **Backup**, uncheck **Enable automatic backups**.
- IMPORTANT:** Uncheck **Enable encryption** option.






Encryption

☐ **Enable encryption**
Choose to encrypt the given instance. Master key IDs and aliases appear in the list after they have been created using the AWS Key Management Service console. [Info](#)

- Uncheck **Deletion protection**.

18. Click on **Create Database** to create the database. This process does take time between 5-10 minutes.

19. Once the database is created the status changes to **Available**.

Databases						
 Group resources			Modify	Actions ▼	Restore from S3	Create database
<input type="text" value="Filter databases"/> < 1 > 						
DB identifier	Role	Engine	Region & AZ	Size	Status	
 test-db	Instance	MySQL Community	us-east-1c	db.t3.micro	 Available	






20. Click on the database and navigate to the **Configuration** tab. You can notice that the **Encryption** is **not enabled**, as we wanted it to be,

Connectivity & security	Monitoring	Logs & events	Configuration	Maintenance & backups	Tags
Instance					
Configuration		Instance class	Storage	Performance Insights	
DB instance ID test-db		Instance class db.t3.micro	Encryption Not enabled	Performance Insights enabled No	
Engine version 8.0.20		vCPU 2	Storage type General Purpose (SSD)		
DB name projectdb		RAM 1 GB	IOPS -		
License model General Public License		Availability	Storage 20 GiB		
Option groups default:mysql-8-0		Master username master	Storage autoscaling Disabled		

21. If we select the database and go to modify it, we will not find an option to Encrypt the database.

Task 3: Take a snapshot from the existing DB Instance

1. Select the created DB Instance and click on **Actions**.
2. Click **Take snapshot** from the options.

Databases						
 Group resources			Modify	Actions ▲	Restore from S3	Create database
<input type="text" value="Filter databases"/> < 1 > 						
DB identifier	Role	Engine			Size	Status
 test-db	Instance	MySQL Com		Stop	db.t3.micro	 Available
				Reboot		
				Delete		
				Create read replica		
				Promote		
				Take snapshot		
				Restore to point in time		

3. Give a name to the snapshot, **test-snapshot-01** and click on the **Take snapshot** button.

Take DB snapshot

This feature is currently supported for InnoDB storage engine only. If you are using MyISAM, refer to details [here](#).

Settings

To take a snapshot of this DB instance you must provide a name for the snapshot.

DB instance
The unique key that identifies a DB instance. This parameter isn't case-sensitive.

test-db

Snapshot name
The identifier for the DB snapshot.

test-snapshot-01

Cancel
Take snapshot

4. The snapshot creation takes 3–5 minutes. Refresh after some time, the snapshot creation status will be **available**.

Task 4: Make a copy of the snapshot and encrypt it

1. It is not possible to encrypt the snapshot in this stage.
2. We need to encrypt the snapshot while taking a copy of it.
3. Under the **Manual snapshots**, select the created snapshot and click on **Actions**.
4. Click **Copy snapshot** from the options.

Snapshots

Manual | System | Shared with me | Public | Backup service | Exports in Amazon S3

Manual snapshots (1)

Filter manual snapshots

<input checked="" type="checkbox"/>	Snapshot name	DB instance or cluster	Snapshot creation time
<input checked="" type="checkbox"/>	test-snapshot-01	test-db	May 02, 2021, 8:07:44 AM UTC

Actions
Take snapshot

Restore snapshot
Copy snapshot
Share snapshot
Migrate snapshot
Export to Amazon S3
Delete snapshot

5. Under settings, provide the following details.

- Make sure the region is the same as the original DB Instance i.e, **US East (N.Virginia)**
- New DB Snapshot Identifier: Enter **test-snapshot-encrypted**
- Under **Encryption**, check **Enable Encryption**. Leave the master key as default as it is a demo.(**IMPORTANT**)

- Click on the **Copy snapshot** button.

Manual snapshots (2)				
<input type="text" value="Filter manual snapshots"/>				
<input type="checkbox"/>	Snapshot name	DB instance or cluster	Snapshot creation time	DB Instance created time
<input type="checkbox"/>	test-snapshot-encrypted	test-db	May 02, 2021, 8:51:37 AM UTC	May 02, 2021, 7:43:43 AM UTC

Task 5: Restore DB Instance from the encrypted snapshot

- Click on the encrypted snapshot and click on **Actions**.
- Click on **Restore snapshot** from the options.

Manual snapshots (2)				
<input type="text" value="Filter manual snapshots"/>				
<input type="checkbox"/>	Snapshot name	DB instance or cluster	Snapshot creation time	DB Instance created time
<input checked="" type="checkbox"/>	test-snapshot-encrypted	test-db	May 02, 2021, 8:51:37 AM UTC	May 02, 2021, 7:43:43 AM UTC
<input type="checkbox"/>	test-snapshot-01	test-db	May 02, 2021, 8:07:44 AM UTC	May 02, 2021, 7:43:43 AM UTC

- Under **Availability and Durability** select Single DB Instance zone

Availability and durability

Deployment options [Info](#)

The deployment options below are limited to those supported by the engine you selected above.

☐ **Multi-AZ DB Cluster - new**
Creates a DB cluster with a primary DB instance and two readable standby DB instances, with each DB instance in a different Availability Zone (AZ). Provides high availability, data redundancy and increases capacity to serve read workloads.

☐ **Multi-AZ DB instance**
Creates a primary DB instance and a standby DB instance in a different AZ. Provides high availability and data redundancy, but the standby DB instance doesn't support connections for read workloads.

☒ **Single DB instance**
Creates a single DB instance with no standby DB instances.

- Settings**, enter the name of DB Instance as **test-db-encrypted**.
- Make the other settings exactly as the original DB Instance.
- Under the **DB instance class**, select **Burstable classes (including t classes)** and select **db.t3.micro**

DB instance class

DB instance class [Info](#)

Choose a DB instance class that meets your processing power and memory requirements. The DB instance class options below are limited to those supported by the engine you selected above.

☐ Standard classes (includes m classes)
☐ Memory optimized classes (includes r and x classes)
☒ Burstable classes (includes t classes)

db.t3.micro
 2 vCPUs 1 GiB RAM Network: 2,085 Mbps

☐ Include previous generation classes

7. Under **Encryption**, you can see the **Enable Encryption** is enabled and **cannot make changes since the snapshot is encrypted**.

Encryption

Encryption [Info](#)

☒ **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.

Master key [Info](#)

(default) aws/rds

Account

922922497623

KMS key ID

990ac3d3-337e-4697-ba1a-6463e168ef56

8. Leave **DB parameter group** and **Option group** as default.

9. Click on **Restore DB Instance** button. The database creation takes around 5-10 minutes.

	DB identifier	Role	Engine	Region & AZ	Size	Status
<input type="radio"/>	test-db	Instance	MySQL Community	us-east-1c	db.t3.micro	Available
<input checked="" type="radio"/>	test-db-encrypted	Instance	MySQL Community	us-east-1a	db.t3.micro	Available

Task 6: Change the name of the original DB Instance

1. We have to make sure that the Endpoint of the restored DB Instance should be the same as the original DB Instance.
2. To do so, we have to change the names of the DB Instances as the names are unique.
3. Select the original DB Instance and click on **Modify**.

4. Change the DB Instance Identifier to **test-db-unencrypted**.

Settings

DB engine version
Version number of the database engine to be used for this database
MySQL 8.0.20

DB instance identifier [Info](#)
Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.
test-db-unencrypted
The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens (1 to 15 for SQL Server). First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

New master password [Info](#)

Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), '(single quote), "(double quote) and @ (at sign).

5. Leave everything as default and click on **Continue**.

6. Verify the new values of the DB Instance Identifier and the Endpoint.

7. Under **Scheduling of modifications**, select **Apply Immediately** and click on **Modify DB Instance** button.

Summary of modifications

You are about to submit the following modifications. Only values that will change are displayed. Carefully verify your changes and click Modify DB Instance.

Attribute	Current value	New value
DB instance identifier	test-db	test-db-unencrypted
Endpoint	test-db.c7owzvjtjkvz.us-east-1.rds.amazonaws.com	test-db-unencrypted.c7owzvjtjkvz.us-east-1.rds.amazonaws.com

Scheduling of modifications

When to apply modifications

☐ Apply during the next scheduled maintenance window
Current maintenance window: May 07, 2021 09:04 - 09:34 UTC+5.5

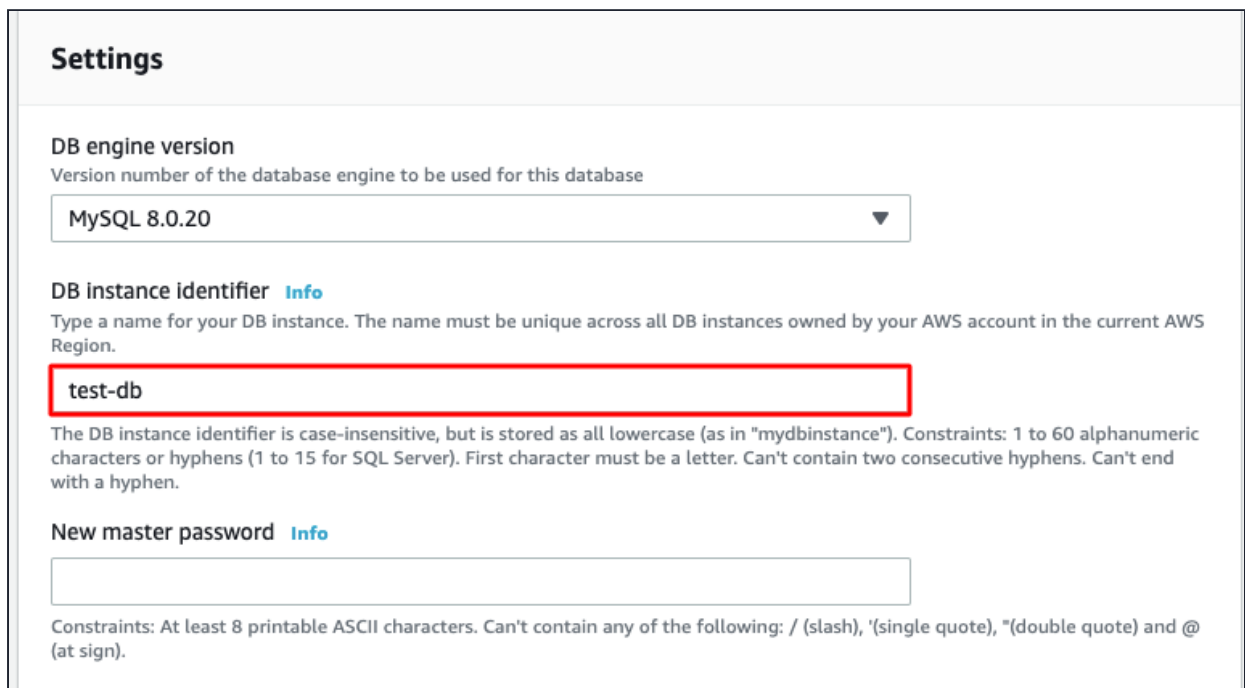
☒ **Apply immediately**
The modifications in this request and any pending modifications will be asynchronously applied as soon as possible, regardless of the maintenance window setting for this database instance.

Cancel Back **Modify DB Instance**

8. It might take some time to reboot the DB Instance. Press ctrl+R if you are not able to see the changes.

Task 7: Change the name of the Restored DB Instance to the original DB Instance name

1. Select on the restored database and click on **Modify**.
2. Change the DB Instance Identifier to **test-db**.



Settings

DB engine version
Version number of the database engine to be used for this database

MySQL 8.0.20 ▼

DB instance identifier [Info](#)
Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

test-db

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens (1 to 15 for SQL Server). First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

New master password [Info](#)

Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), ' (single quote), " (double quote) and @ (at sign).

3. Leave everything as default and click on **Continue**.
4. Verify the new values of the DB Instance Identifier and the Endpoint.
5. Under **Scheduling of modifications**, select **Apply Immediately** and click on **Modify DB Instance** button..

Summary of modifications

You are about to submit the following modifications. Only values that will change are displayed. Carefully verify your changes and click Modify DB Instance.

Attribute	Current value	New value
DB instance identifier	test-db-encrypted	test-db
Endpoint	test-db-encrypted.c7owzvjtjkvz.us-east-1.rds.amazonaws.com	test-db.c7owzvjtjkvz.us-east-1.rds.amazonaws.com

Scheduling of modifications

When to apply modifications

☐ Apply during the next scheduled maintenance window
 Current maintenance window: May 07, 2021 09:04 - 09:34 UTC+5.5


☒ **Apply immediately**
 The modifications in this request and any pending modifications will be asynchronously applied as soon as possible, regardless of the maintenance window setting for this database instance.

Cancel Back **Modify DB Instance**

- It might take some time to reboot the DB Instance. Press ctrl+R if you are not able to see the changes.
- Once the database is modified, click and open **test-db** i.e, the encrypted DB Instance.
- Click on the database and navigate to the **Configuration** tab. You can notice that the **Encryption** is **enabled**.

Connectivity & security	Monitoring	Logs & events	Configuration	Maintenance & backups	Tags
-------------------------	------------	---------------	---------------	-----------------------	------

Instance

Configuration	Instance class	Storage	Performance Insights
DB instance ID test-db	Instance class db.t3.micro	Encryption Enabled AWS KMS key aws/rds 	Performance Insights enabled No
Engine version 8.0.20	vCPU 2		
DB name projectdb	RAM 1 GB	Storage type General Purpose (SSD)	
License model General Public License	Availability	IOPS -	

Task 8: Delete the unencrypted RDS DB Instance and snapshot

- Since we have the encrypted DB Instance, we shall delete the unencrypted DB Instance and the snapshot associated.

2. Click on **Databases** present to the left of the screen.
3. Select the Unencrypted DB Instance (i.e **test-db-unencrypted**) and click on **Actions**.
4. Click on the **Delete** option.
5. Uncheck the Create final snapshot option.
6. Check the Acknowledge box.
7. Confirm the deletion by entering **delete me** and click on **delete**.

Delete test-db-unencrypted instance?

Are you sure you want to Delete the **test-db-unencrypted** DB Instance?

☐ **Create final snapshot?**
Determines whether a final DB Snapshot is created before the DB instance is deleted.

☒ I acknowledge that upon instance deletion, automated backups, including system snapshots and point-in-time recovery, will no longer be available.

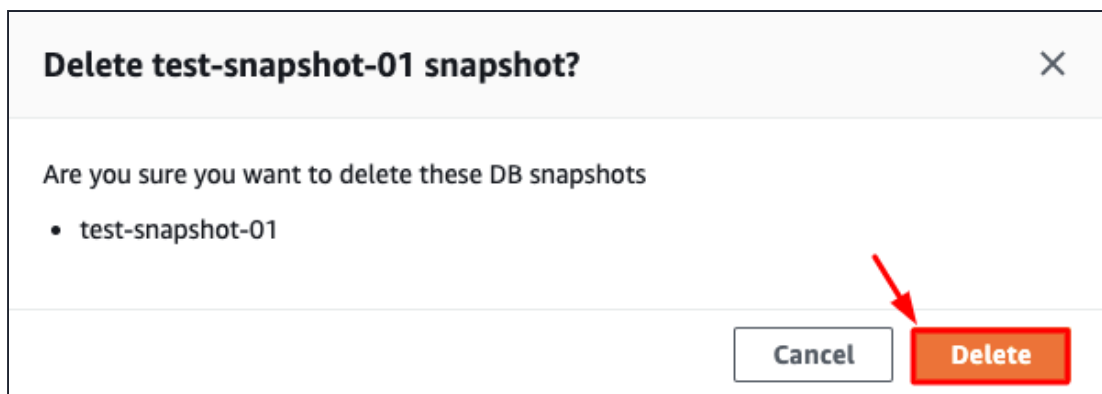
To confirm deletion, type *delete me* into the field

delete me

⚠ We strongly recommend taking a final snapshot before instance deletion since after your instance is deleted, automated backups will no longer be available.

Cancel **Delete**

8. Click on the **Snapshots** on the left of your screen.
9. Under **Manual snapshots**, select the unencrypted snapshot (i.e. **test-snapshot-01**) and click on **Actions**.
10. Click on the **Delete snapshot** option.
11. Confirm by clicking on the **Delete** button.



12. In this way, you can encrypt an unencrypted RDS DB Instance.

13. Wait till both resources are completely deleted. This step is to avoid confusion in the validation report.

Do you know?

Database encryption is a critical component of a comprehensive security strategy. It helps protect data from unauthorized access, complies with regulatory requirements, mitigates the impact of data breaches, enhances cloud security, builds trust with customers, and mitigates insider threats.

Task 9: Validation Test

1. Once the lab steps are completed, please click on the **Validation** button on the right-side panel.
2. This will validate the resources in the AWS account and displays whether you have completed this lab successfully or not.
3. Sample output :





Lab Overview


Lab Steps

Lab Validation

Lab FAQs

Check your Validation

If any checks fail , you can use the remaining time in the Lab to work on making the checks pass . Click Validate My Lab again to rerun the checks at any time.

Validate My Lab 

Launch an Encrypted MySQL RDS Instance
Check whether an Encrypted RDS Instance with MySQL engine is created or not.

Create RDS DB Snapshot
Check whether an DB Snapshot is created for mysql database or not

Task 10: Delete AWS Resources

Deleting the DB Instance

1. Click on **Databases** present to the left of the screen.
2. Select the DB Instance and click on **Actions**.
3. Click on the **Delete** option.
4. Uncheck the Create final snapshot option.
5. Check the Acknowledge box.
6. Confirm the deletion by entering **delete me** and click on **delete**.

Delete test-db instance?

Are you sure you want to Delete the **test-db** DB Instance?

☐ Create final snapshot?
Determines whether a final DB Snapshot is created before the DB instance is deleted.

☒ I acknowledge that upon instance deletion, automated backups, including system snapshots and point-in-time recovery, will no longer be available.

To confirm deletion, type *delete me* into the field

delete me

⚠ We strongly recommend taking a final snapshot before instance deletion since after your instance is deleted, automated backups will no longer be available.

Cancel Delete

7. The status changes to **Deleting** and the DB Instance gets deleted.

8. You can proceed to further steps even if it is in a **deleting** state.

Deleting the Snapshot

1. Click on the **Snapshots** on the left of your screen. Under **Manual snapshots**, select the unencrypted snapshot and click on **Actions**.
2. Click on the **Delete Snapshot** option.
3. Confirm by clicking on the **Delete** button.

Delete test-snapshot-encrypted snapshot?

Are you sure you want to delete these DB snapshots

- test-snapshot-encrypted

Cancel Delete

Completion and Conclusion

1. You have created an unencrypted Amazon RDS DB Instance.
2. You have taken the snapshot of the DB Instance.
3. You have made a copy of the snapshot and encrypted it.
4. You have restored the DB Instance with the copied snapshot.
5. You have changed the names of the original and restored DB instances.
6. You have made sure that the Endpoint of the restored database is the same as the originally created DB Instance.
7. You have deleted the Unencrypted DB Instance and snapshot.

End Lab

1. Sign out of AWS Management Console.
2. You have successfully completed the lab.
3. Once you have completed the steps, click on **End Lab** from your whizlabs lab console and wait till the process gets completed.

[About Us](#) [Subscription](#) [Instructions and Guidelines](#) [FAQ's](#) [Contact Us](#)



© 2024, Whizlabs Software Pvt. Ltd.

