AWS — Production-Ready VPC + Private RDS (MySQL)

Complete, step-by-step implementation guide (console + CLI + verification + hardening + testing + cleanup). Replace placeholder values (<...>) with your own names/IDs.

Quick project summary / goals

- Create an isolated, production-style VPC with public and private subnets (multi-AZ ready).
- Deploy RDS (MySQL) in private subnets (no public IP).
- Deploy an EC2 bastion/app server in the public subnet to access RDS.
- Implement route tables, security groups, IAM role for secrets, backups, encryption, and cleanup.
- Deliverables: working RDS accessible only from bastion, automated backups, monitoring & alerts, secure credential handling via Secrets Manager.

Table of contents

    - RDS instance (MySQL) — production options (Multi-AZ, encryption, monitoring)
    - IAM role & Secrets Manager (EC2 reads DB credentials)
    - EC2 bastion/app server (attach role & test)
    - Optional: Snapshot export to S3 (IAM role + export task)
5. Tests & validation checklist (exact commands/SQL)
6. Troubleshooting common errors & fixes
7. Cleanup steps (console + CLI)

1) Naming & placeholders (replace everywhere)

Use a consistent prefix: `proj` or `harshitha-rds`
Examples used below:

- VPC: `prod-vpc`
- Public subnet(s): `prod-public-a` (CIDR `10.0.1.0/24`), `prod-public-b` (optional)
- Private subnets: `prod-private-a` (`10.0.1.0/24`), `prod-private-b` (`10.0.2.0/24`)
- Internet Gateway: `prod-igw`
- Route tables: `prod-public-rt`, `prod-private-rt`
- Security groups: `sg-bastion`, `sg-rds`
- DB subnet group: `prod-db-subnet-group`
- RDS instance id: `prod-rds-db`
- EC2 bastion: `prod-bastion`
- Secrets Manager secret name: `prod/rds/harshi`
- IAM role for EC2: `EC2SecretsRole`

- S3 exported snapshot bucket: `prod-rds-exports-<suffix>`
- Region: `<REGION>` (e.g., `ap-south-1`)
- Account id: `<ACCOUNT_ID>`

2) Architecture

Why this layout:

- Public subnet = bastion (only place with public IP).
- RDS in private subnets - no public endpoint.
- Internet Gateway provides internet access.
- Security groups reference each other (SG→SG) — recommended.