**Task 1 Documentation: Secure RDS Deployment with IAM & Secrets Manager**

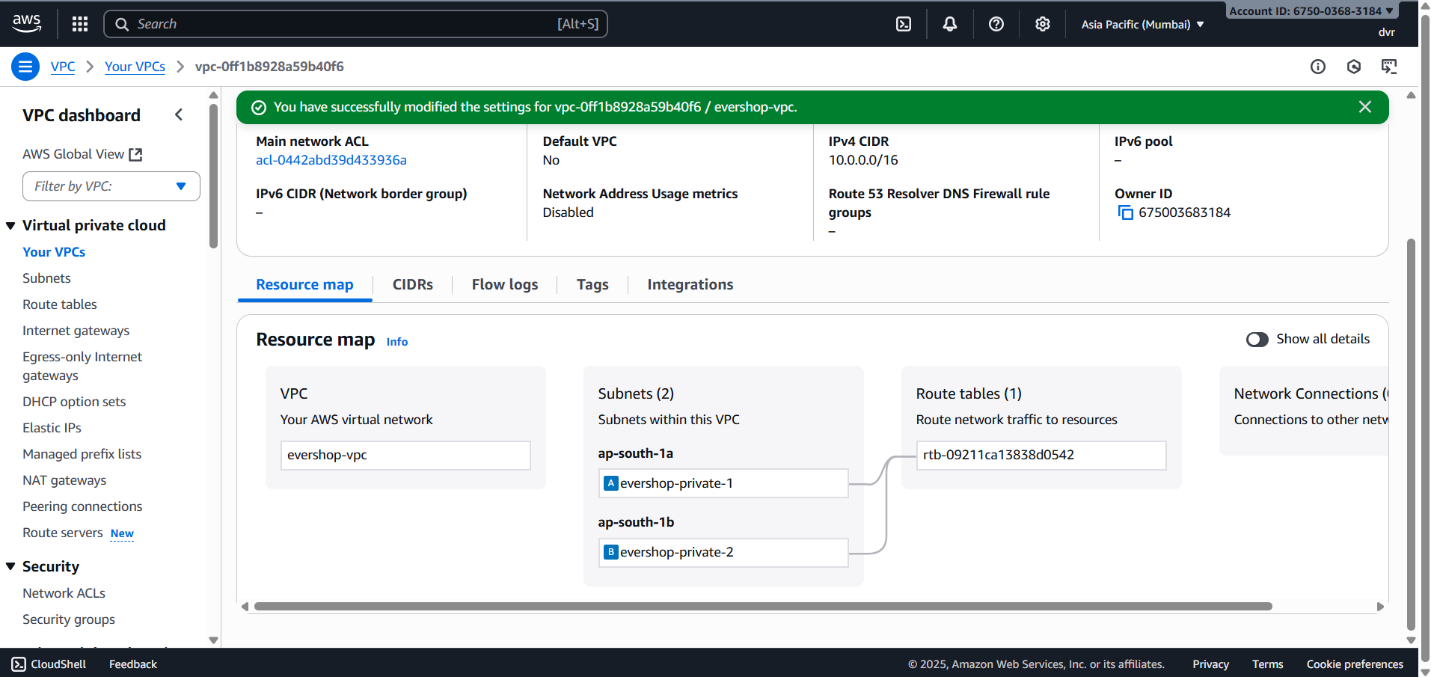
**Project Title:** Secure Multi-AZ MySQL RDS Deployment for EverShop Application

**Objective:** Deploy a highly secure MySQL RDS instance in private subnets with: - Multi-AZ deployment - No public access - IAM database authentication - TLS-only connections - Credentials managed via Secrets Manager with automatic rotation - EC2 instances retrieve temporary tokens dynamically - Point-in-time restore verified (RPO ≤ 5 minutes)

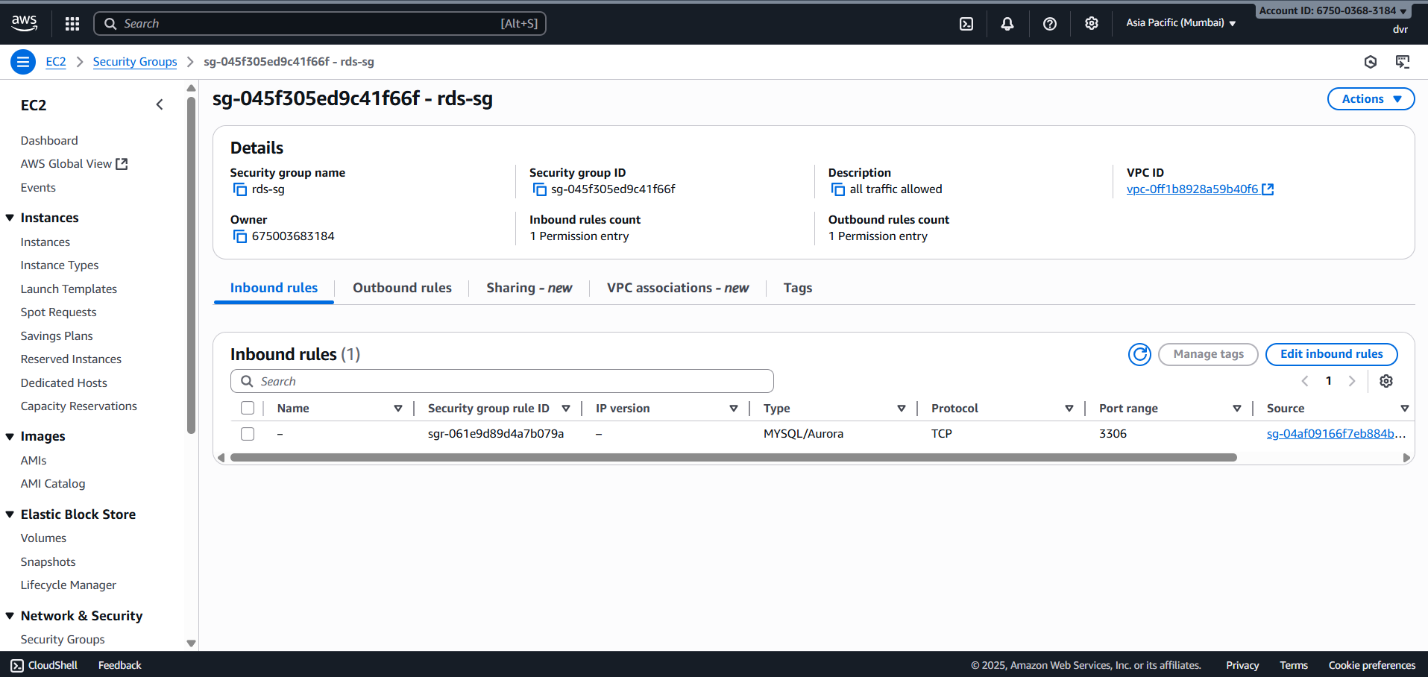
**Architecture Diagram:**

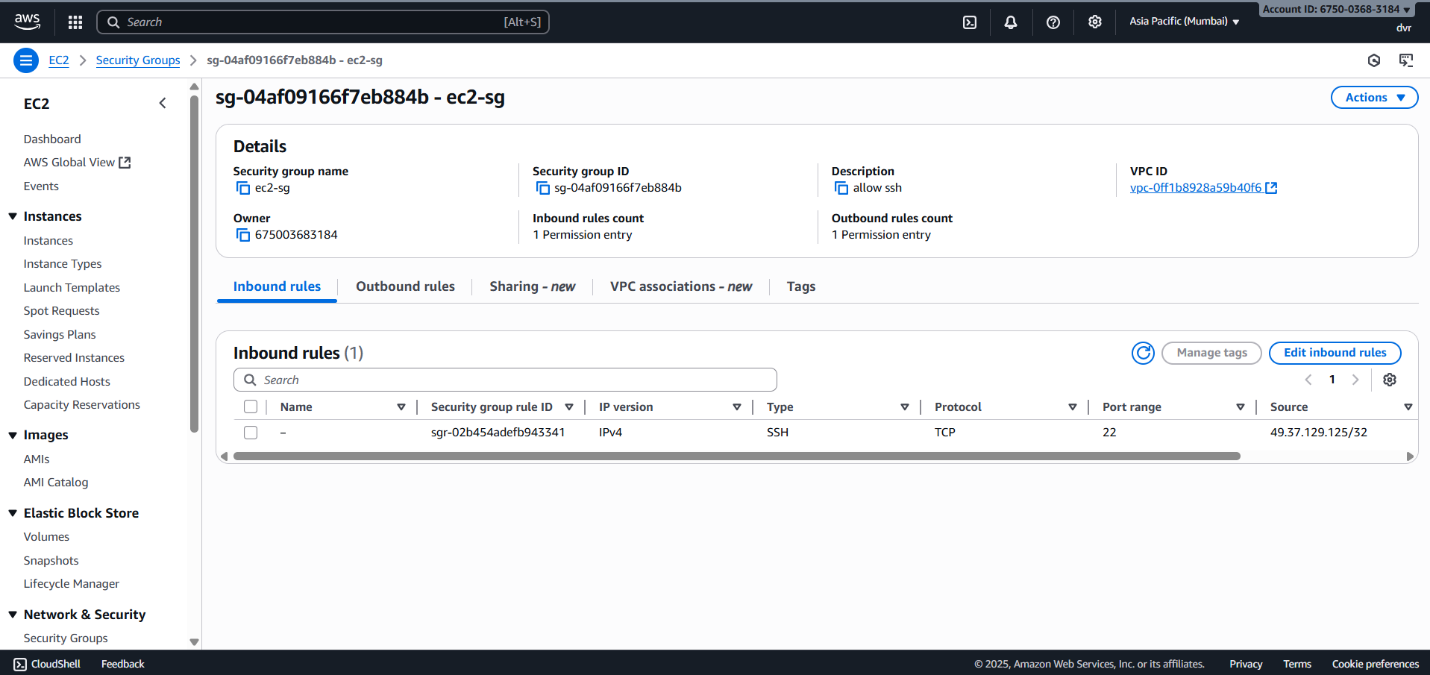
| Component | Description |
| --- | --- |
| Internet | Access point for EC2 / ALB |
| Public Subnet | Hosts EC2 Bastion / Application Load Balancer |
| Private Subnets | Hosts Multi-AZ RDS MySQL instances |
| Secrets Manager | Stores master credentials with rotation |

**Step 1: VPC and Subnets** 1. Created VPC evershop-vpc (CIDR: 10.0.0.0/16), DNS hostnames enabled. 2. Private subnets: - 10.0.1.0/24 → us-east-1a - 10.0.2.0/24 → us-east-1b 3. Public subnet (for SSH access): 10.0.3.0/24 → us-east-1a, IGW attached, route table 0.0.0.0/0 → IGW.



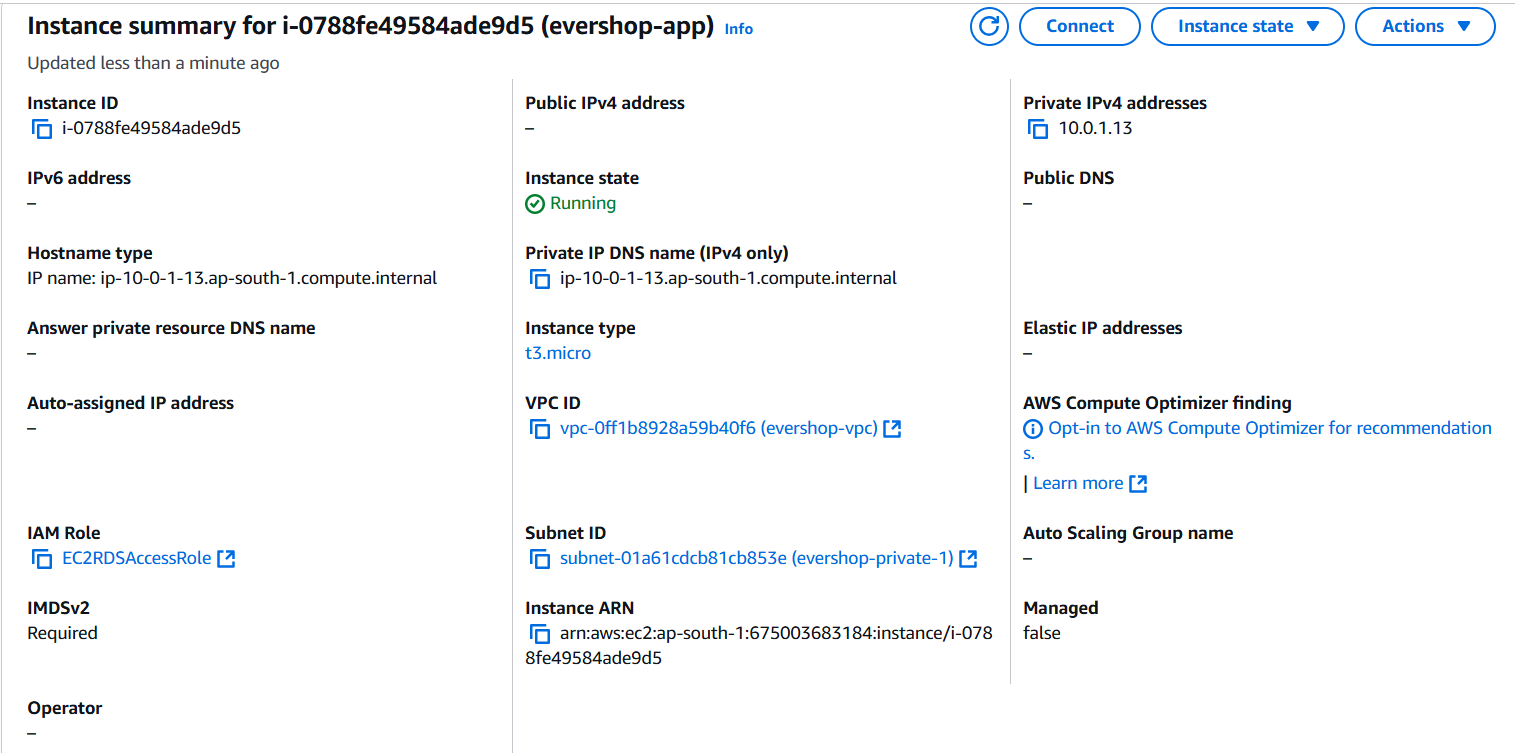
**Step 2: Security Groups** |Security Group | Rules | RDS SG | Inbound: MySQL (3306) from EC2 SG only; Outbound: All traffic | | EC2 SG | Inbound: SSH (22) from your IP; Outbound: All traffic

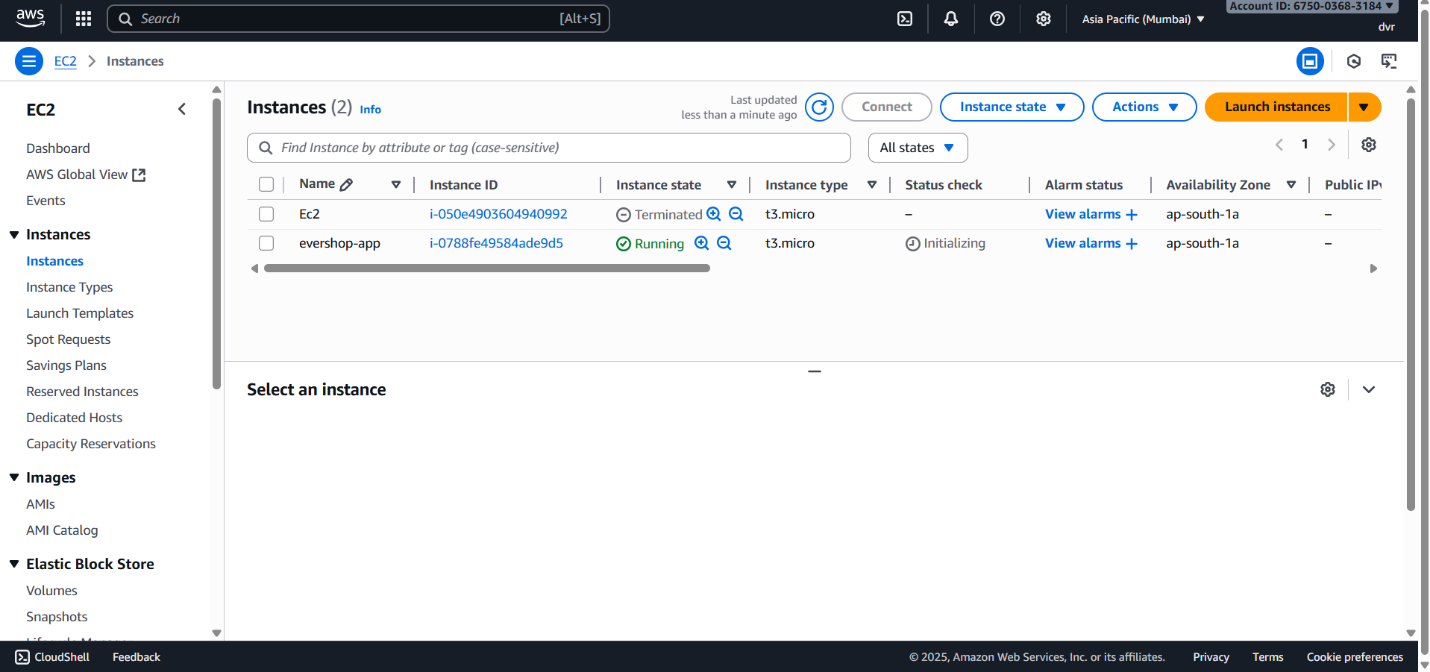




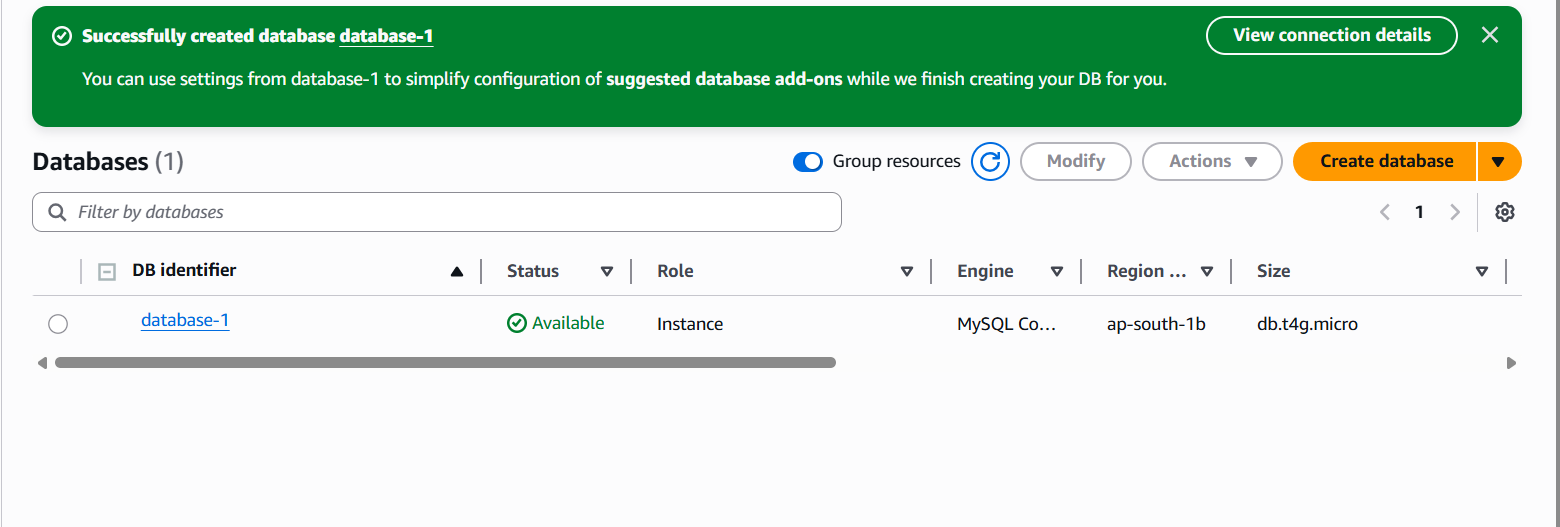
**Step 3: Launch EC2 Instance** - Amazon Linux 2 EC2 in public subnet. - IAM Role: EC2RDSAccessRole. - Key Pair: evershop-key.pem. - Installed MySQL client:

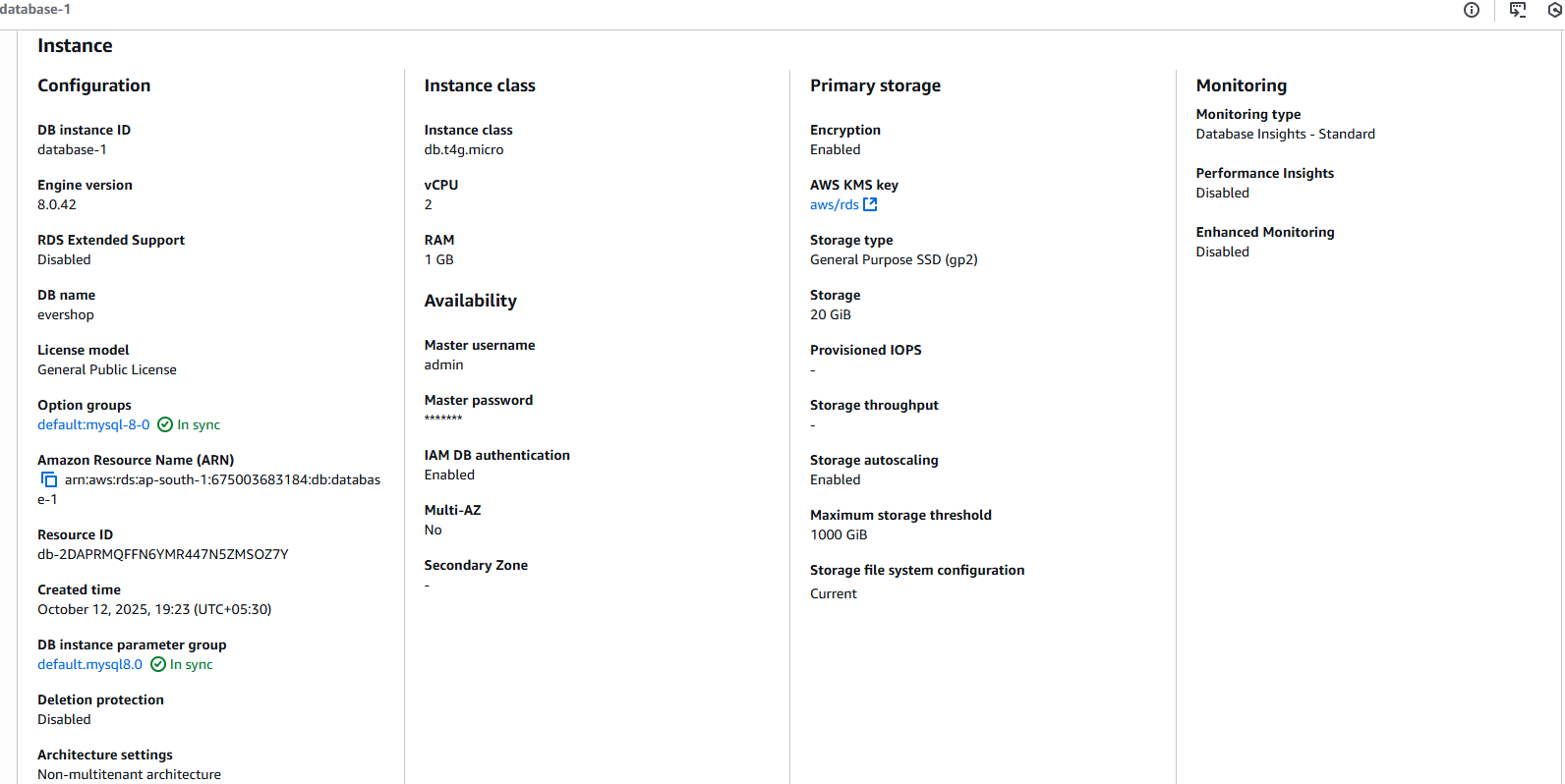
sudo yum update -y  
sudo amazon-linux-extras enable mysql8.0  
sudo yum install -y mysql  
mysql –version

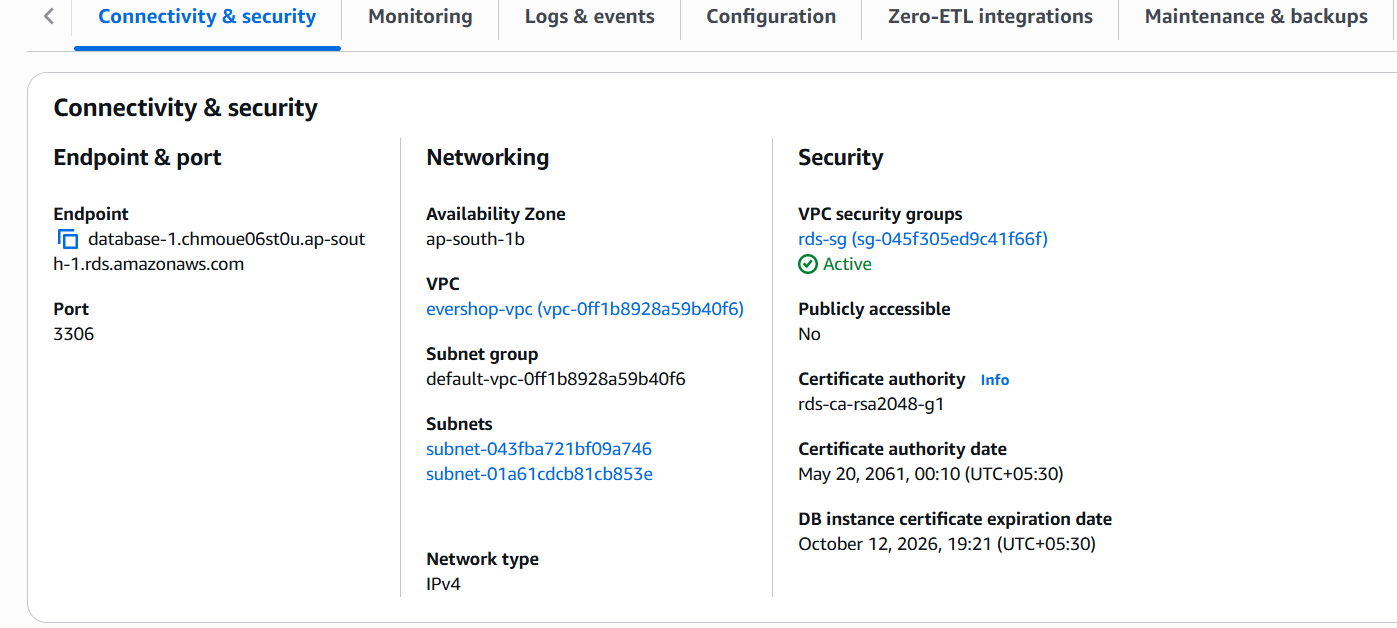




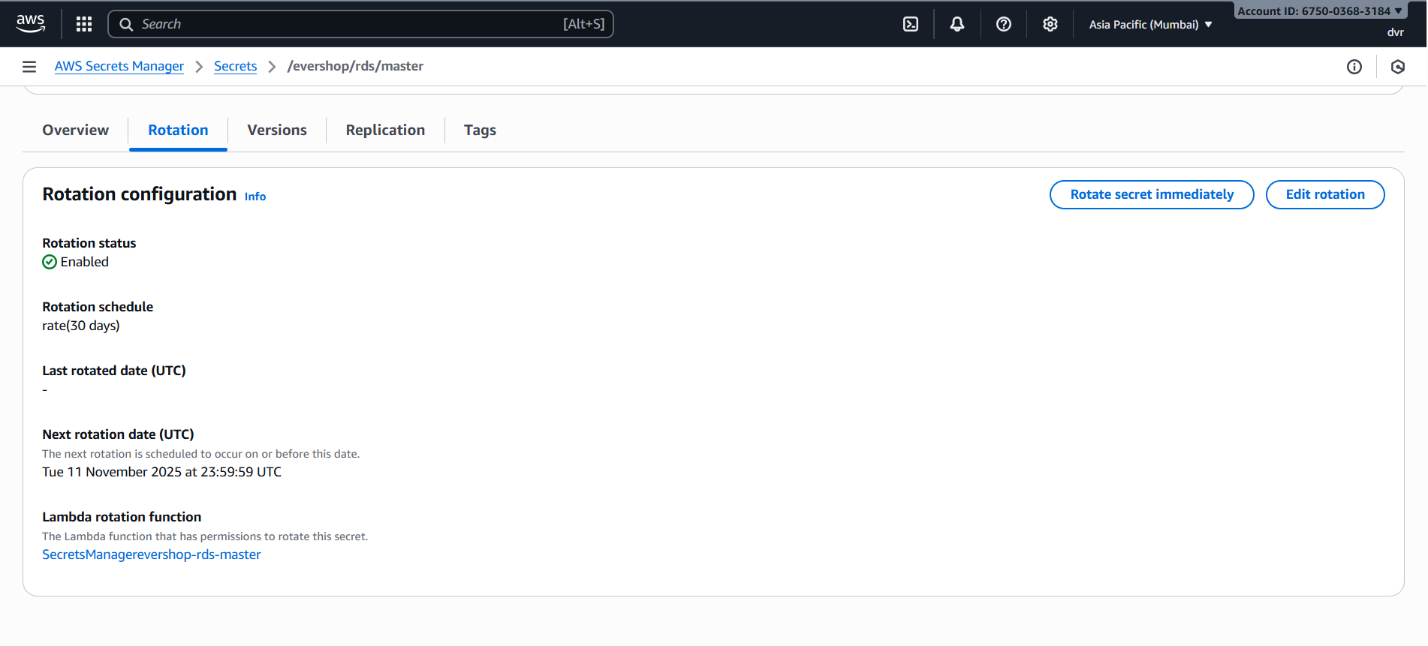
**Step 4: Create RDS MySQL Instance** - Engine: MySQL 8.0, Multi-AZ, private subnets. - Database authentication: Password + IAM. - Storage: 20GB SSD, Encryption: enabled, Backup: enabled. - DB name: evershop.





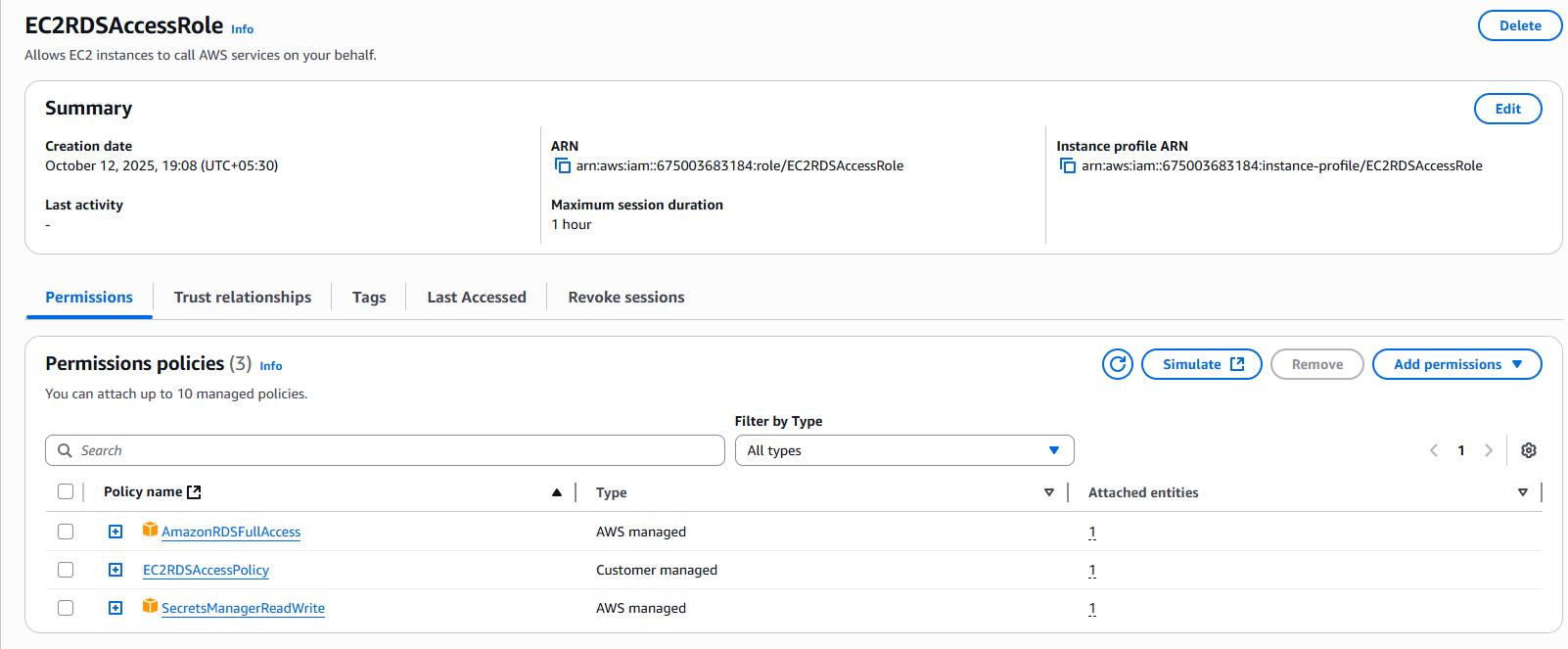


**Step 5: Store Credentials in Secrets Manager** - Secret Name: /evershop/rds/master - Credentials: RDS master username/password. - Automatic rotation: every 30 days, Single user strategy.



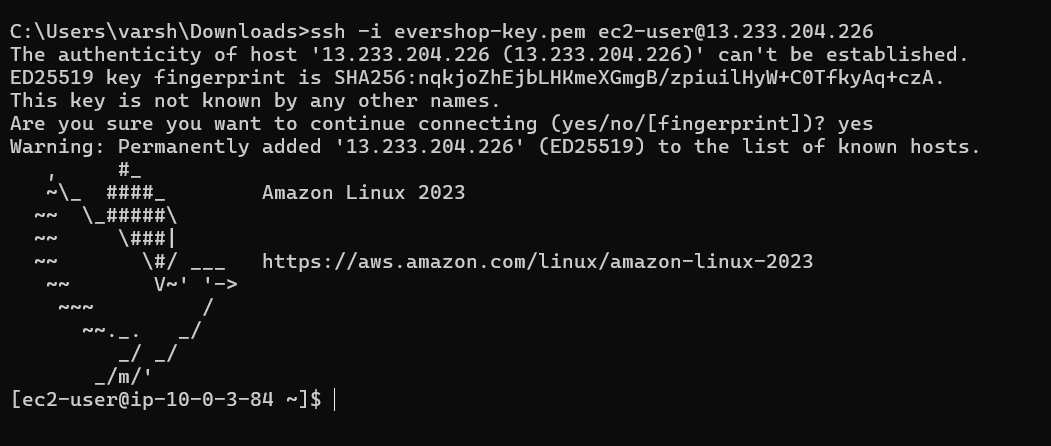
**Step 6: Attach IAM Policy to EC2**

{  
 "Version": "2012-10-17",  
 "Statement": [  
 {  
 "Effect": "Allow",  
 "Action": ["rds-db:connect", "secretsmanager:GetSecretValue"],  
 "Resource": "\*"  
 }  
 ]  
}



**Step 7: Connect to RDS Using IAM Token**

ssh -i evershop-key.pem ec2-user@<Public-IP>  
  
export DB\_HOST=<RDS-endpoint>  
export DB\_USER=admin  
export DB\_PORT=3306  
export REGION=us-east-1  
  
TOKEN=$(aws rds generate-db-auth-token --hostname $DB\_HOST --port $DB\_PORT --region $REGION --username $DB\_USER)  
  
mysql --host=$DB\_HOST --port=$DB\_PORT --user=$DB\_USER --enable-cleartext-plugin --ssl-ca=/etc/ssl/certs/ca-bundle.crt --password="$TOKEN"



**Step 8: Verify Point-in-Time Restore** 1. Insert sample data:

CREATE TABLE internship\_test (id INT AUTO\_INCREMENT PRIMARY KEY, note VARCHAR(100));  
INSERT INTO internship\_test (note) VALUES ('before\_restore');  
INSERT INTO internship\_test (note) VALUES ('after\_restore');

1. Restore to a point in time between inserts → new DB: evershop-db-restore.
2. Verify only first row exists.