

# Module 8: Case Study - 1

1. Web tier: Launched an instance in the public subnet so that the instance should allow only HTTP and SSH from the internet.

The screenshot shows the AWS Management Console 'Instances' page. The 'webtier' instance (i-0bf97a140a3292670) is selected. The 'Networking details' section shows the instance is in the 'us-west-2a' availability zone, with a public IP address of 54.187.101.199 and a public DNS of ec2-54-187-101-199.us-west-2.compute.amazonaws.com. The instance is running on the t2.micro instance type.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...
webtier	i-0bf97a140a3292670	Running	t2.micro	2/2 checks passed	No alarms	us-west-2a	ec2-54-187-101-199.us...	54.187.101.199
applicatintier	i-085bc95e941729525	Running	t2.micro	-	No alarms	us-west-2a	ec2-35-92-235-83.us-w...	35.92.235.83

**Instance: i-0bf97a140a3292670 (webtier)**

**Networking details**

Public IPv4 address: 54.187.101.199 | [open address](#)

Public IPv4 DNS: ec2-54-187-101-199.us-west-2.compute.amazonaws.com | [open address](#)

Subnet ID: subnet-0dee6e8ee31ad611f (multi-vpc-subnet-public1-us-west-2a) | [open](#)

Private IPv4 addresses: 10.0.3.195

VPC ID: vpc-01cfaad21ab42bbe (multi-vpc-vpc) | [open](#)

Private IP DNS name (IPv4 only): ip-10-0-3-195.us-west-2.compute.internal

IPv6 addresses: -

Secondary private IPv4 addresses: -

The screenshot shows the AWS Management Console 'Instances' page. The 'webtier' instance (i-0bf97a140a3292670) is selected. The 'Inbound rules' section shows the instance has two security group rules: one for port 22 (SSH) and one for port 80 (HTTP). The instance is running on the t2.micro instance type.

Name	Security group rule ID	Port range	Protocol	Source	Security groups	Description
-	sg-0540b7f9e44e85709	22	TCP	0.0.0.0/0	webtier	-
-	sg-09282dbd3c4a15bb3	80	TCP	0.0.0.0/0	webtier	-

**Instance: i-0bf97a140a3292670 (webtier)**

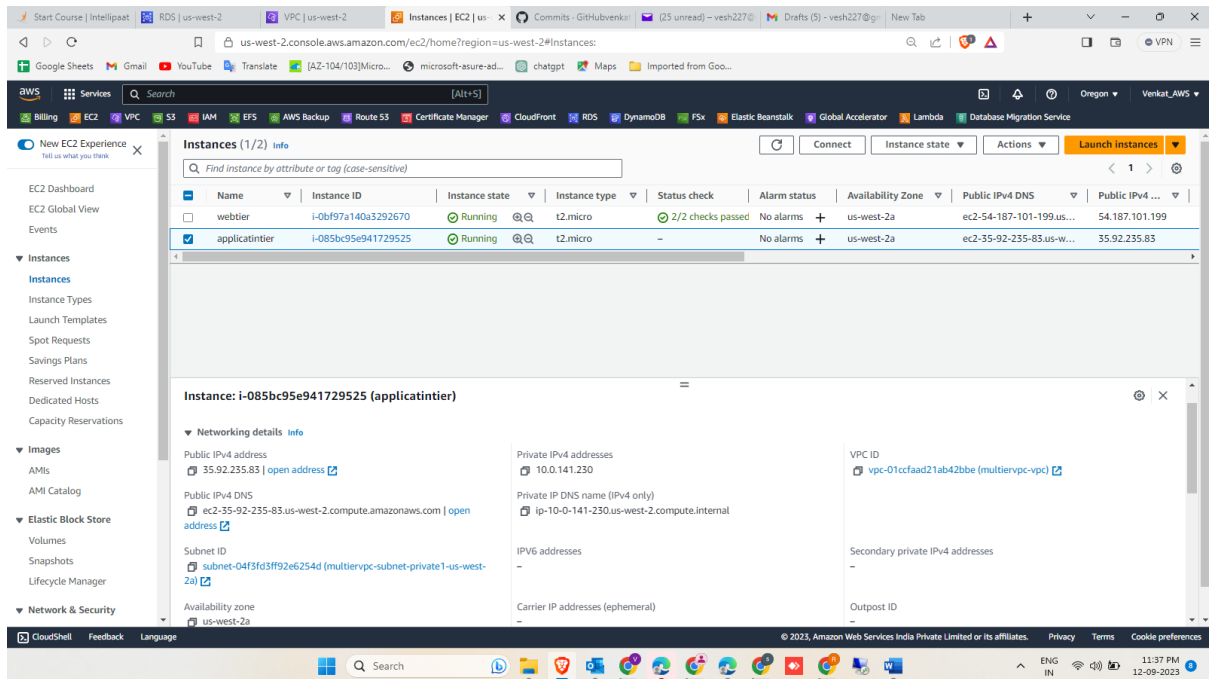
**Inbound rules**

Filter rules

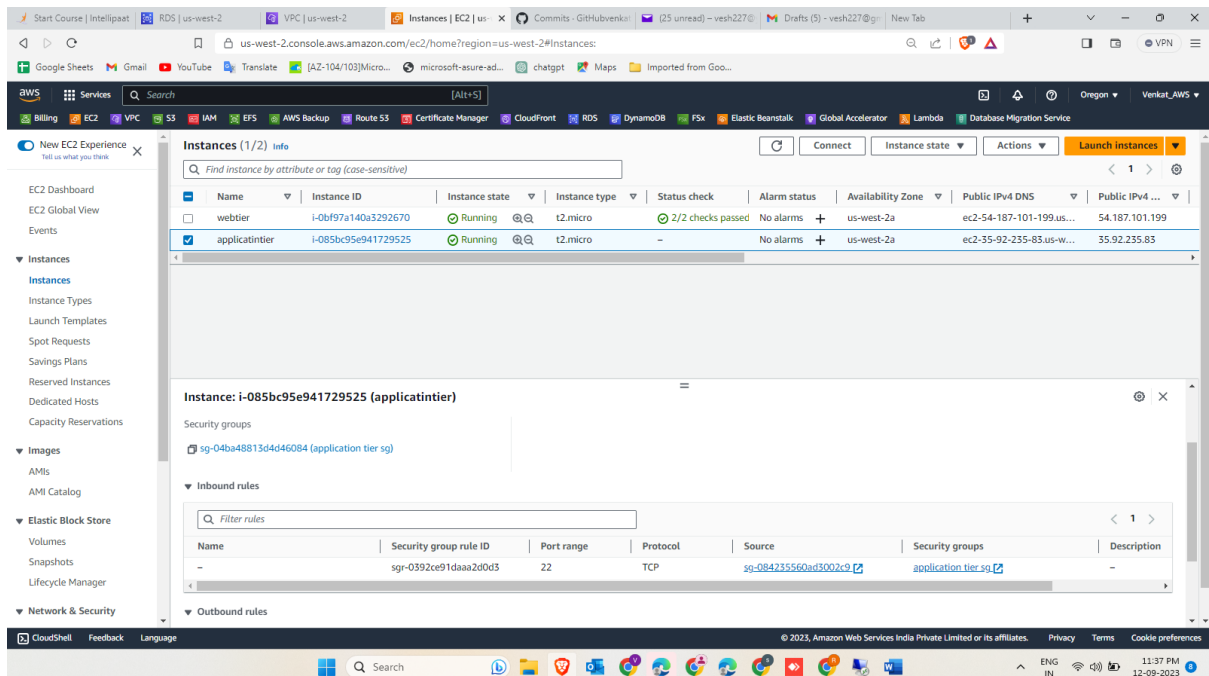
1

# Module 8: Case Study - 1

- Application tier: Launched an instance in the private subnet of the web tier, and it should allow only SSH from the public subnet of the web tier.



- So that I have chosen source SSH from the public subnet of the web tier



# Module 8: Case Study - 1

4. DB launched in the private subnet, and it should allow connection on port 3306 only from the private subnet of the application tier.

The screenshot shows the Amazon RDS console for a database instance named 'database-2'. The instance is in the 'Available' state and is a MySQL Community Edition instance. The 'Connectivity & security' tab is selected, showing the following details:

Endpoint & port	Networking	Security
Endpoint: database-2.cdt0k88u31b.us-west-2.rds.amazonaws.com Port: 3306	Availability Zone: us-west-2b VPC: multienvpc-vpc (vpc-01ccfaad21ab42bbe) Subnet group: default-vpc-01ccfaad21ab42bbe Subnets: subnet-0189bfff4c0162e370	VPC security groups: sg-0bf3b1b59226345c6 (Active) Publicly accessible: No Certificate authority: rds-ca-2019

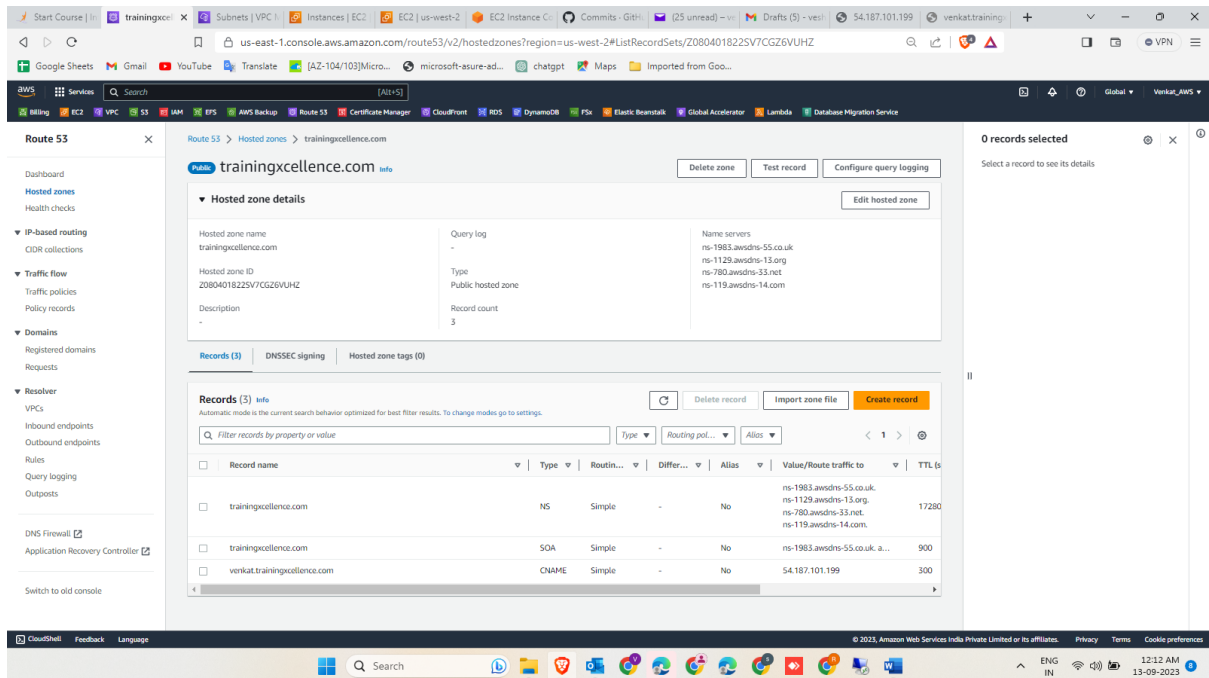
5. So that I have chosen 3306 source from the private subnet of the application tier.

The screenshot shows the Amazon VPC console for a security group named 'db sg'. The security group is associated with the VPC 'vpc-01ccfaad21ab42bbe'. The 'Inbound rules' tab is selected, showing the following details:

Security group rule...	IP version	Type	Protocol	Port range	Source
sg-0c8d256d94b976...	-	MySQL/Aurora	TCP	3306	sg-04ba48813d4d46084 / application tier sg

# Module 8: Case Study - 1

- Created Route 53 hosted zone, it will direct the traffic to the EC2 instance



- Deletion policy has been created, RDS DB Instance should not be deleted.

