

Module 7 – Assignment

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

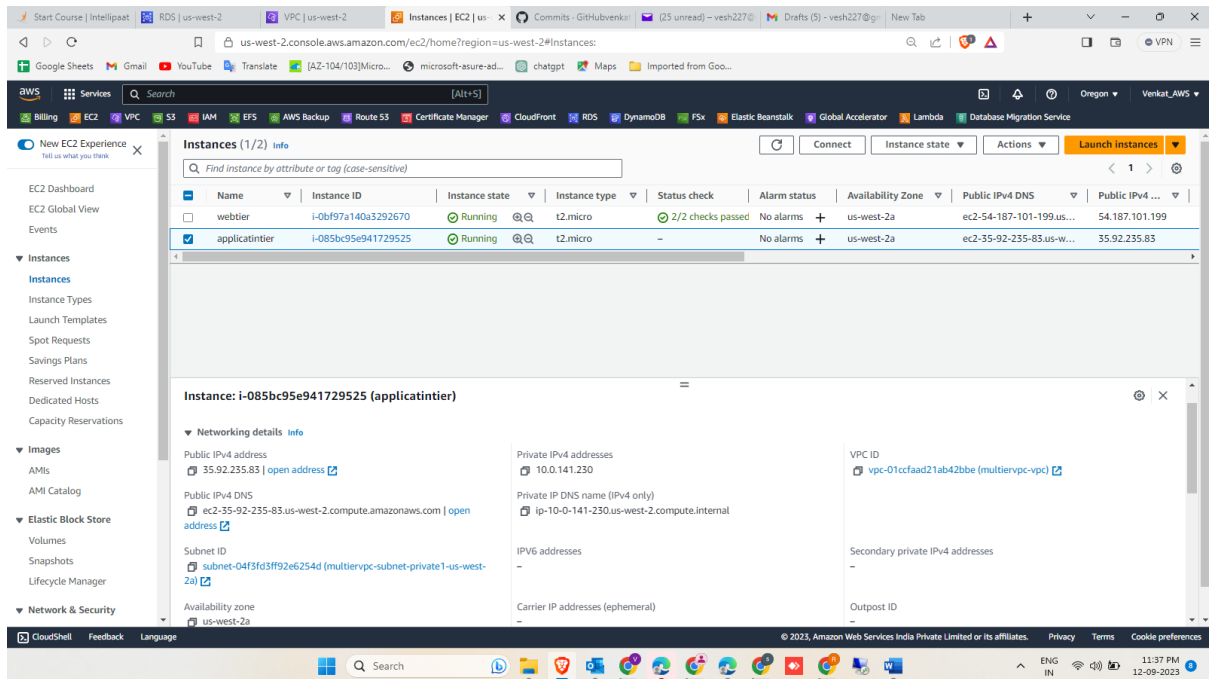
The screenshot shows the AWS Management Console interface. The left sidebar contains navigation links for EC2 Dashboard, EC2 Global View, Events, Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images, AMIs, AMI Catalog, Elastic Block Store, Volumes, Snapshots, Lifecycle Manager, and Network & Security. The main content area displays the 'Instances (1/2)' page. A table lists two instances: 'webtier' (Instance ID: i-0bf97a140a3292670, Instance state: Running, Instance type: t2.micro, Status check: 2/2 checks passed, Alarm status: No alarms, Availability Zone: us-west-2a, Public IPv4 DNS: ec2-54-187-101-199.us-... 54.187.101.199) and 'applicatintier' (Instance ID: i-085bc95e941729525, Instance state: Running, Instance type: t2.micro, Status check: -, Alarm status: No alarms, Availability Zone: us-west-2a, Public IPv4 DNS: ec2-35-92-235-83.us-w... 35.92.235.83). Below the table, the details for the 'webtier' instance are shown. The 'Networking details' section includes: Public IPv4 address: 54.187.101.199, Private IPv4 addresses: 10.0.3.195, VPC ID: vpc-01cfaad21ab42bbe, Public IPv4 DNS: ec2-54-187-101-199.us-west-2.compute.amazonaws.com, Private IP DNS name (IPv4 only): ip-10-0-3-195.us-west-2.compute.internal, Subnet ID: subnet-0dee6e8ee31ad611f, and IPV6 addresses: -.

The screenshot shows the AWS Management Console interface, specifically the 'Inbound rules' section for the 'webtier' instance. The 'Filter rules' section shows a table of inbound rules. The table has columns: Name, Security group rule ID, Port range, Protocol, Source, Security groups, and Description. The table contains two rules: one for port 22 (SSH) and one for port 80 (HTTP). The 'Source' column for both rules is 0.0.0.0/0. The 'Security groups' column for both rules is 'webtier'. The 'Description' column for both rules is '-'. Below the table, the 'Outbound rules' section is visible.

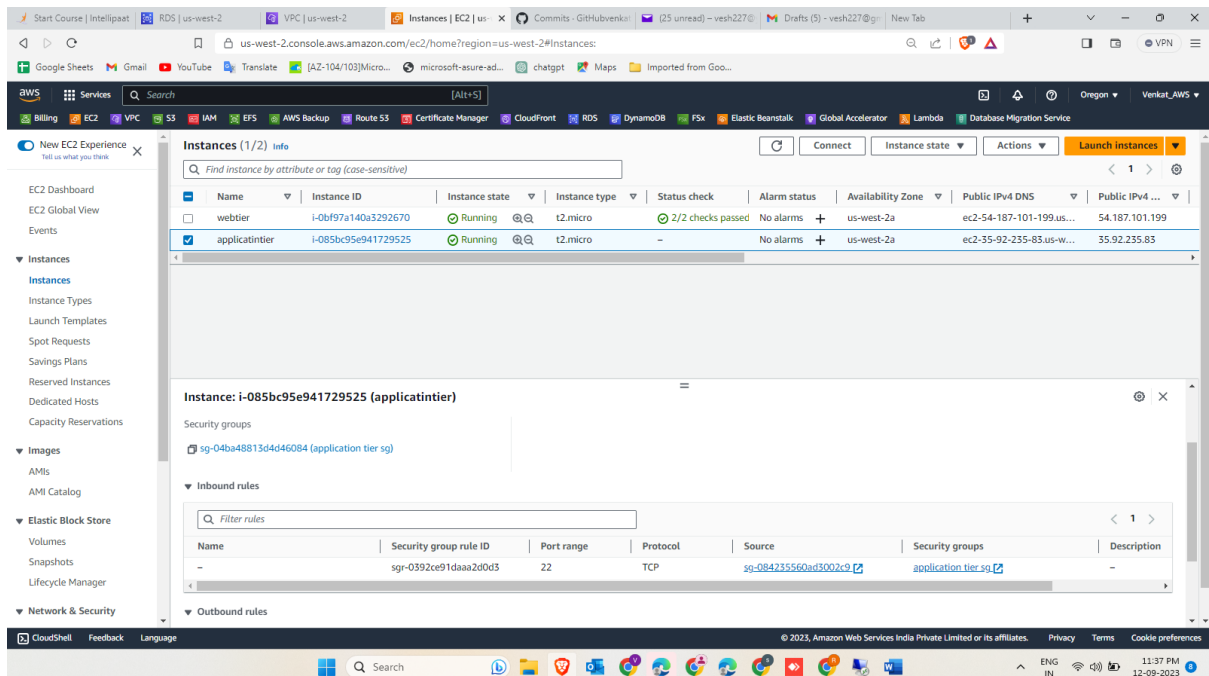
Name	Security group rule ID	Port range	Protocol	Source	Security groups	Description
-	sg-0540b7f9e44e85709	22	TCP	0.0.0.0/0	webtier	-
-	sg-09282dbd3c4a15bb3	80	TCP	0.0.0.0/0	webtier	-

Module 7 – Assignment

- 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 7 – Assignment

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 engine. The 'Connectivity & security' tab is selected, showing the endpoint 'database-2.cdt0k88u31b.us-west-2.rds.amazonaws.com' on port 3306. The VPC is 'multi-vpc-vpc (vpc-01ccfaad21ab42bbe)' and the subnet is 'subnet-0189bfff4c0162e370'. The security group is 'sg-0bf3b1b59226346c6'.

Summary			
DB identifier	database-2	CPU	-
Role	Instance	Status	Available
		Engine	MySQL Community
		Class	db.t3.micro
		Region & AZ	us-west-2b

Connectivity & security		
Endpoint & port	Networking	Security
Endpoint database-2.cdt0k88u31b.us-west-2.rds.amazonaws.com	Availability Zone us-west-2b	VPC security groups db sg (sg-0bf3b1b59226346c6)
Port 3306	VPC multi-vpc-vpc (vpc-01ccfaad21ab42bbe)	Publicly accessible No
	Subnet group default-vpc-01ccfaad21ab42bbe	Certificate authority rds-ca-2019
	Subnets subnet-0189bfff4c0162e370	Certificate authority date

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

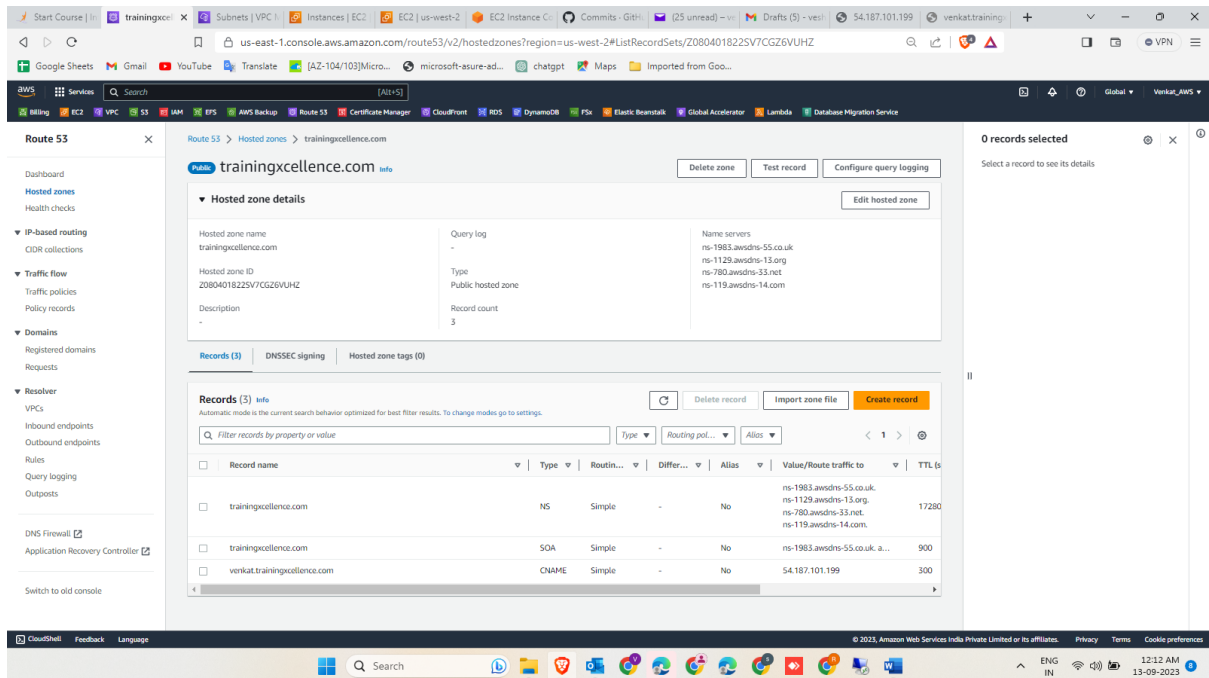
The screenshot shows the Amazon VPC console for a security group named 'db sg'. The security group is associated with the VPC 'vpc-01ccfaad21ab42bbe'. The 'Inbound rules' tab is selected, showing a single rule for MySQL/Aurora on port 3306, with the source set to 'sg-04ba48813d4d46084 / application tier sg'.

Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count
-	sg-06c1941ace2ccf3c	default	vpc-04bc8e7be0a623d86	default VPC security gr...	556609594559	1 Permission entry
-	sg-096d48d2becb8ea35	default	vpc-01ccfaad21ab42bbe	default VPC security gr...	556609594559	1 Permission entry
-	sg-0bb1b230ed1701f8	launch-wizard-2	vpc-04bc8e7be0a623d86	launch-wizard-2 create...	556609594559	1 Permission entry
Application tier sg	sg-04ba48813d4d46084	application tier sg	vpc-01ccfaad21ab42bbe	application tier sg	556609594559	1 Permission entry
db sg	sg-0bf3b1b59226346c6	db sg	vpc-01ccfaad21ab42bbe	Created by RDS manag...	556609594559	1 Permission entry
-	sg-04b10a3688dc101d6	launch-wizard-1	vpc-04bc8e7be0a623d86	launch-wizard-1 create...	556609594559	1 Permission entry
web tier sg	sg-08423556ad3002c9	web tier	vpc-01ccfaad21ab42bbe	web tier	556609594559	2 Permission entries

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

Module 7 – Assignment

- 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.

