InnoMed Account

Group/Role	Role	User1	User2	User3	User4
System Administrator	Access All	Admin1	Admin2		
Database Administrator	Access DBS	Data1	Data2		
Monitor	Monitoring Infrastructure Resources	Monitor1	Monitor2	Monitor3	Monitor4

Users, Groups, And Roles

Group/Role #	Group/Role Name	Permissions
System Administrator	Administrator	1.AWS Management Console access 2.Own user name and password
Database Administrator	Database Management	Combination of user name and password
Monitor	Monitor	Monitoring Infrastructure Resources
Role: InnoMed Application	App_manager	1. read and write to S3 Bucket

VPC(InnoMed-VPC)

VPC Name: `InnoMed-VPC` IPv4 CIDR Block: `10.200.0.0/20`

VPC Name	Region	Purpose	Subnets	AZs	CIDR Range
InnoMod-VPC	N.Virginia	Null	4	us-east-1a, us-east-1f	10.200.0.0/20

Subnet

Application and Web subnet

Name	VPC	Subnet Type	AZ	Subnet Address
NAT-subnet-group1	InnoMod-VPC	Public	us-east-1a	10.200.0.0/24
WEB-subnet-group1(Web)	InnoMod-VPC	Private	us-east-1a	10.200.2.0/24
APP-subnet-group1(App)	InnoMod-VPC	Private	us-east-1a	10.200.4.0/24
DB-subnet-group1(DB)	InnoMod-VPC	Private	us-east-1a	10.200.6.0/24

Name	VPC	Subnet Type	AZ	Subnet Address
TestDev-subnet-group1(Test/Dev)	InnoMod-VPC	Private	us-east-1a	10.200.8.0/24
NAT-subnet-group2	InnoMod-VPC	Public	us-east-1f	10.200.1.0/24
WEB-subnet-group2(Web)	InnoMod-VPC	Private	us-east-1f	10.200.3.0/24
APP-subnet-group2(App)	InnoMod-VPC	Private	us-east-1f	10.200.5.0/24
DB-subnet-group2(App)	InnoMod-VPC	Private	us-east-1f	10.200.7.0/24
TestDev-subnet-group2(Test/Dev)	InnoMod-VPC	Private	us-east-1a	10.200.9.0/24

Route Table

Name	VPC	Route	Subnet Associations
Public Route Table	InnoMod-VPC	Des: 10.200.0.0/20 Target: local / Des:0.0.0.0/0 Target:Internet Gateway	Public Subnet 1&2
Private Route Table 1	InnoMod-VPC	Des: 10.200.0.0/20 Target: local / Des:0.0.0.0/0 Target:NAT 1	Public Subnet 1&2
Private Route Table 2	InnoMod-VPC	Des: 10.200.0.0/20 Target: local / Des:0.0.0.0/0 Target:NAT 2	Public Subnet 1&2

Internet Gateways

Name	VPC
InnoMed-Gateways	InnoMod-VPC

NAT Gateways

Name	VPC	Subnets	Features	ID
Public Subnet 1	InnoMod-VPC	Public Subnet 1	New EIP	Recode ID
Public Subnet 2	InnoMod-VPC	Public Subnet 2	New EIP	Recode ID

Network ACLs

Name	VPC	Subnets	Features	ID
ACL 1	InnoMod-VPC	Public Subnet 1 & Private Subnet 2		

Security Group

Name	VPC	Subnets	Features	ID
Web-Security-Group	InnoMod-VPC			

Name	VPC	Subnets	Features	ID
App-Security-Group	InnoMod-VPC			
DB-Security-Group	InnoMod-VPC			
Configuration Server	InnoMod-VPC			

DB-Security-Group Type: MySQL/Aurora (3306) Protocol: TCP(6) Source: Click in the field and select Web-Security-Group

> This is configuring the Database security group to permit inbound traffic on port 3306 from any EC2 instance that is associated with the Web-Security-Group

Configuration Server Inbound Rules:

Web Server Inbound Rules:

Auto Scaling Group

Tier	Launch Configuration	Group Name	Group Size	VPC	Subnets	ELB	Tags
Web	WebTier_configure	webTier					
App	AppTier_configure	Apptier					

WebTier_configure Group Name: `WebTier_configure` Group Size: `start with 2 instances` Network: `InnoMod-VPC` Subnet: Both Private Subnet and Private Subnet 2 Target Groups: 1 Key: `Name` Value: `WebTier_configure`

Instance Details

Tier	Tags/Name	OS	Type	Size	Security Group	Number	User Data
Config	web-config	Linux	t2.micro	8GB	Config Server	1	Yes
Web	web-tier	Linux	t2.micro	8GB	Web Server	2	Yes
App	app-tier	Linux	t2.micro	8GB	App Server	2	Yes
DB	db-tier	Linux	t2.micro	8GB	DB Server	2	Yes
Dev	dev-tier	Linux	t2.micro	16GB	Dev Server	2	Yes
Test	test-tier	Linux	t2.micro	16GB	Test Server	2	Yes

DB Instance

- For Use case, select Production - MySQL.
- DB instance class: db.t2.micro (The first option in the list)

- DB instance identifier: lab-db
- Master username: master
- Master password: lab-password
- Confirm password: lab-password

Advanced Setting:

- VPC: InnoMod-VPC
- Subnet group: db-subnet-group
- VPC security groups: Select existing VPC security groups
- Select VPC security groups: DB-Security-Group (VPC) and remove default (VPC)
- Database name: lab
- Backup retention period: 0 Days
- Enhanced monitoring: Disable enhanced monitoring

From: Lab 4

Build a original VPC-Web-Server

Create the Configuration Server

Network: `InnoMed-VPC` Subnet: `Public Subnet 1` Auto-assign Public IP: `Enable` Advanced Details: `Copy the followed thing` Add Tag: Key(`Name`) Value(`InnoMedConfiguration`) Select an existing security group: `web-config`

`ssh -i <path and name of pem> ec2-user@<Public IP>`

```
#!/bin/bash
sudo yum -y update
sudo yum -y install httpd php
sudo chkconfig httpd on
wget https://us-west-2-tcprod.s3.amazonaws.com/courses/AWS-100-
CCA/v3.1.0/lab8-ha/scripts/phpapp.zip
sudo unzip phpapp.zip -d /var/www/html/
sudo service httpd start
```

```
#!/bin/bash
yum -y update
yum -y install httpd
chkconfig httpd on
service httpd start
echo "<html><h1>Hello From Your Test Server!</h1></html>" >
/var/www/html/index.html
```

Create Image

Name: `Web server`

Create An Application Load Balancer

Choose: Application Load Balancer Name: `LB1` VPC: `InnoMed-VPC` AZ: `Choose all the public Subnets` Configure Security Group: `Security group for the web servers(Only HTTP incoming traffic.)` Configure Routing: Name: Group 1 Healthy Threshold: 2 Interval 10 secondes