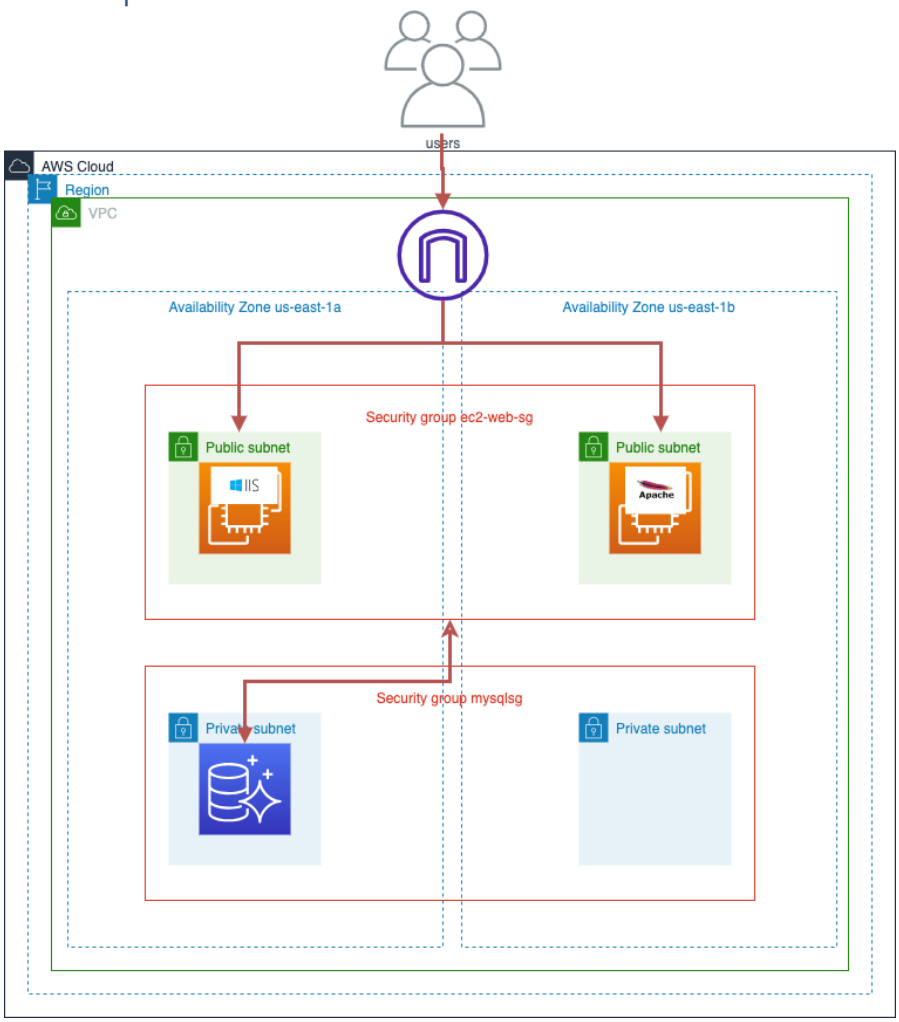
Creating a VPC with Database and EC2 Instances

Writeup



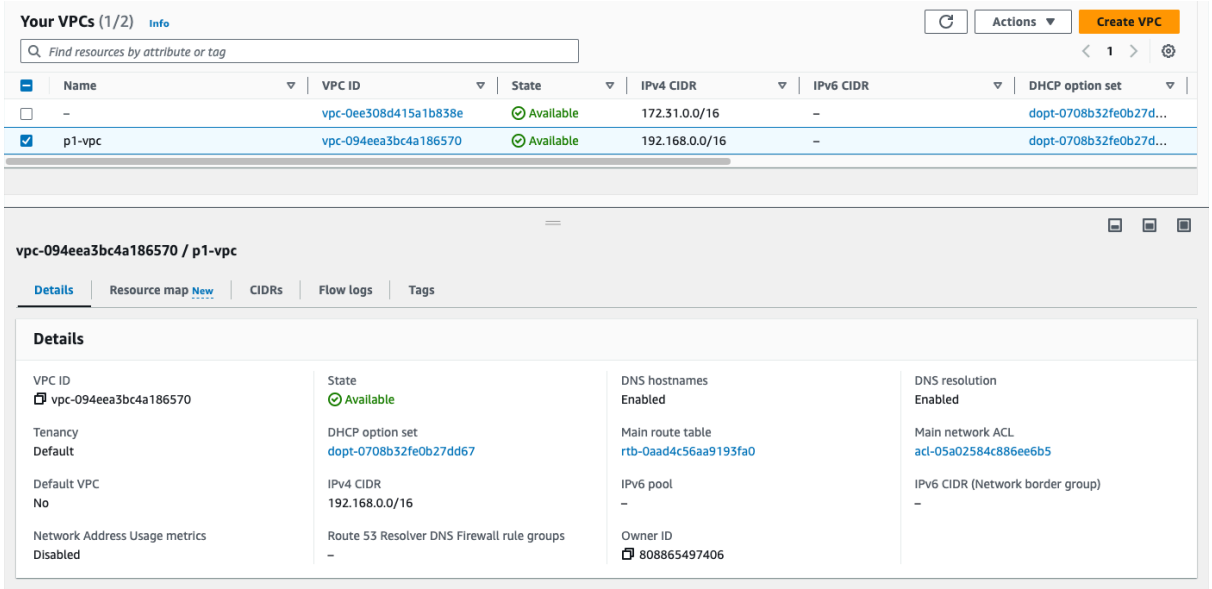
The diagram shows the architecture of the project result. The user's requests are received by the internet gateway and forwarded to the webserver of a EC2 instance in the public subnet dependent on the IP-Address. Only the EC2 instances within the security group ec2-web-sg are allowed to communicate with the mysql database instance in the private subnet.

Step by step instruction

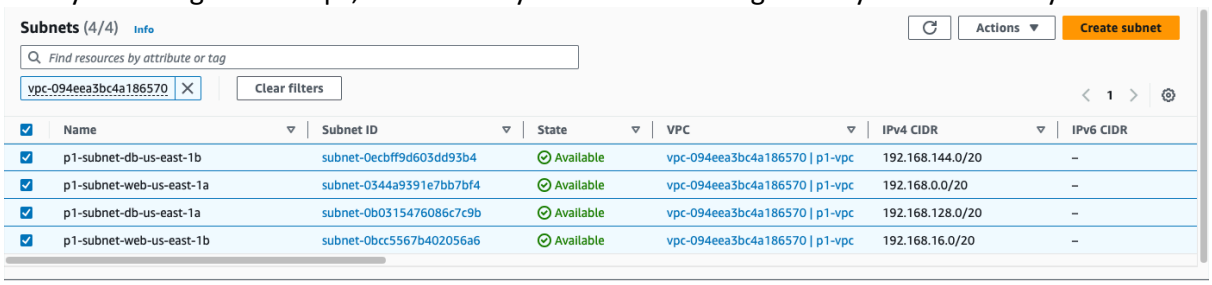
Create Virtual Private Cloud (VPC)

Go to AWS Management Console VPC->Your VPCs->Create VPC

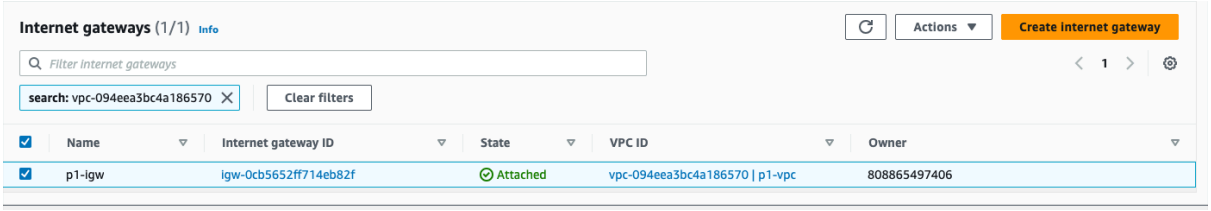
1. Ressources: “VPC and more”
2. Enable Auto-generate: „p1“
3. IPv4 CIDR: „192.168.0.0/16“
4. VPC endpoints: Select None
5. Keep the default for the remaining specifications
6. Create VPC
7. By following these steps, I successfully created and configured my AWS VPC.



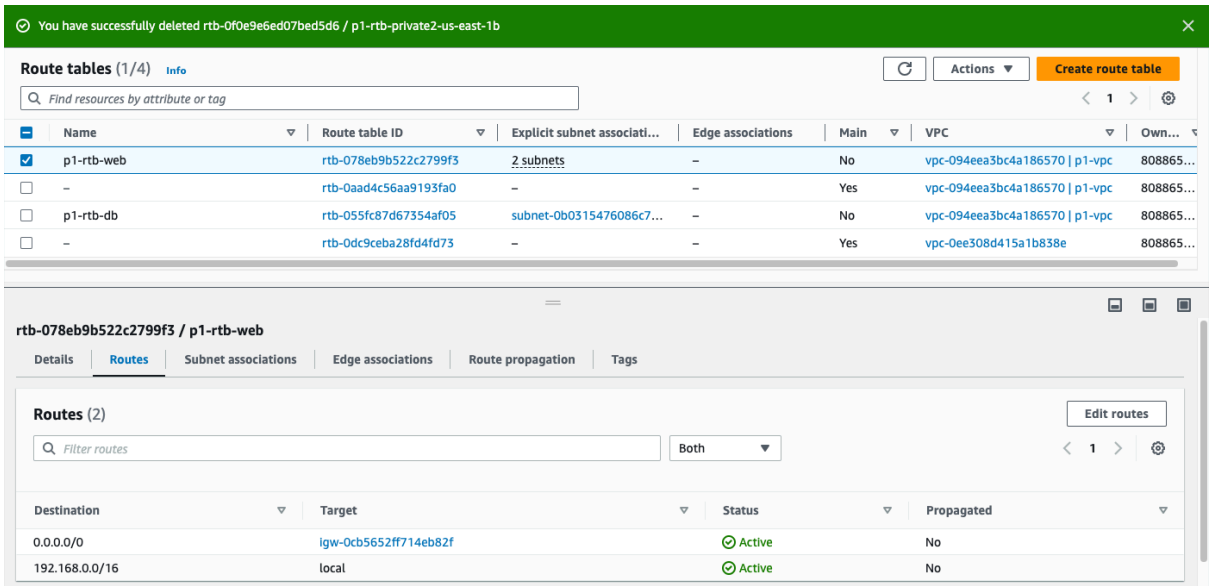
8. By following these steps, I successfully created and configured my subnets for my VPC.

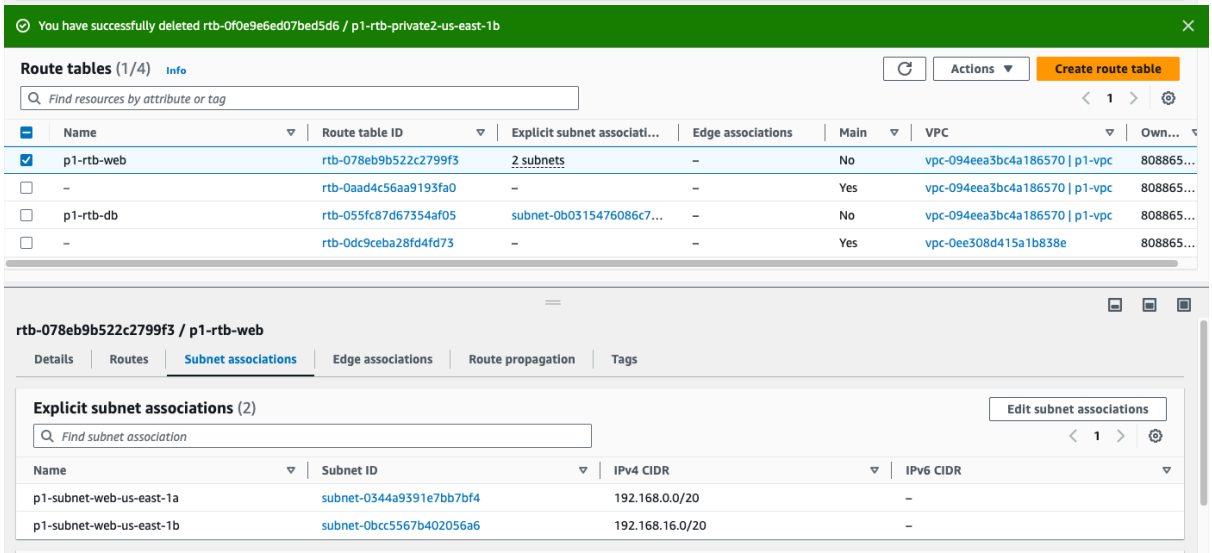


9. By following these steps, I successfully created my internet gateway and attached it to my VPC.

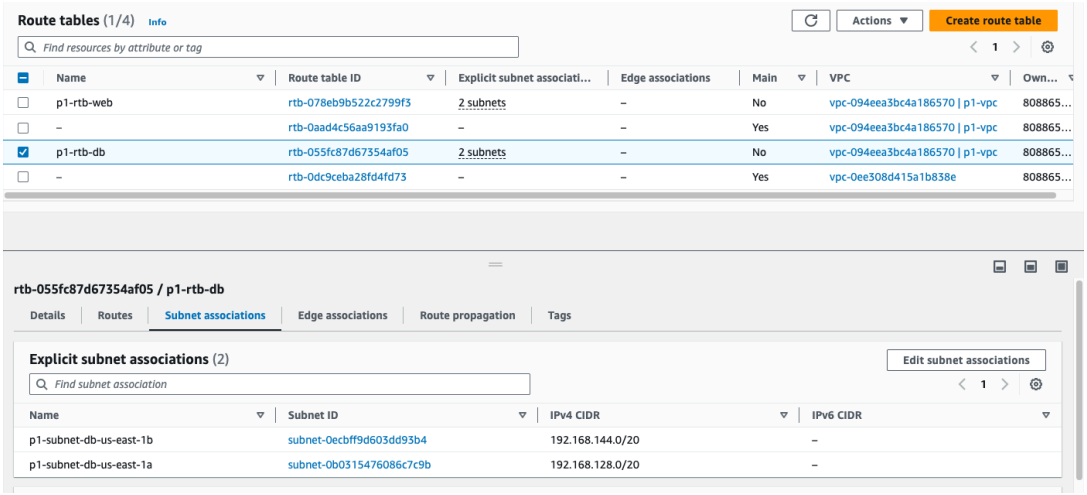


10. By following these steps, I successfully created my route tables for my VPC.
Rename public routing table to “p1-rtb-web” and add web-subnets to routing table





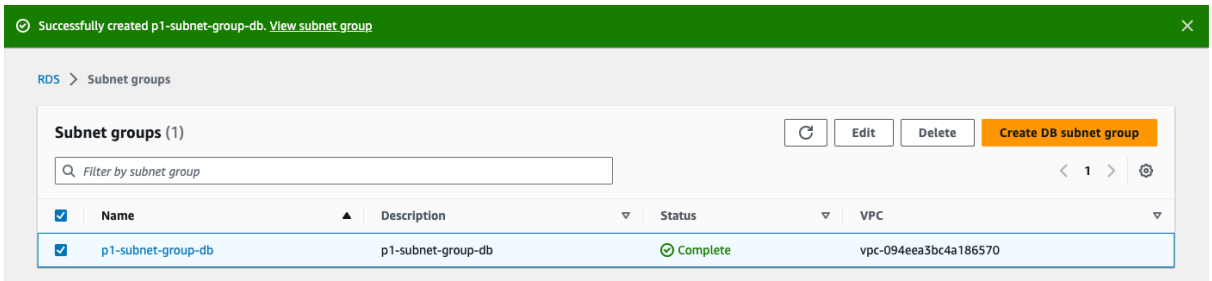
Rename private routing table to “p1-rtb-db” and add private db-subnets to routing table



Create database subnet group

Go to AWS Management Console RDS->Subnet groups->Create db subnet group

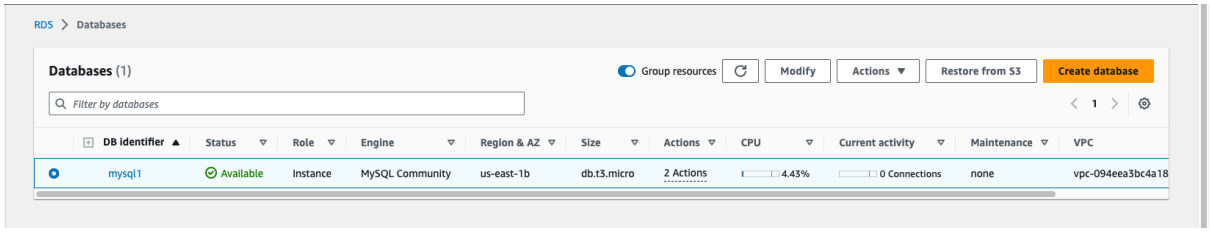
1. Name: “p1-subnet-group-db”
2. VPC: p1-vpc
3. Availability Zone: Select the zones from the private db-subnets
4. Subnets: Select the private db-subnets
5. Create



Create relational database

Go to AWS Management Console RDS->Create database

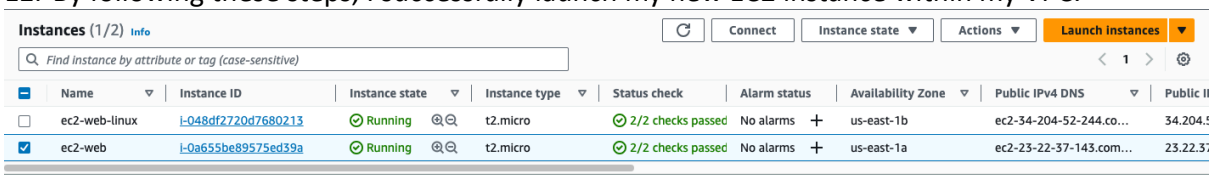
6. Select Standard create
7. Engine options: Select MySQL
8. Engine Version: Select newest Version MySQL 8.0.34
9. Templates: Dev/Test with Multi-AZ DB instance
10. DB instance identifier: “mysql1”
11. Type Master Password/Confirm master password
12. DB instance classe: Select Burstable classes: db.t3.micro
13. Storage type: Select General Puropose SSD (gp2)
14. Allocated storage: 20
15. Maximum storage threshold: 50
16. Connectivity. Compute resource: Select Don’t connect to an EC2 compute ressource
17. VPC: Select p1-vpc
18. VPC security group: Create new with security group name: “mysqlsg”
19. Public Access: No
20. Database authentication options: Password and IAM authentication
21. Disable Monitoring
22. Create database

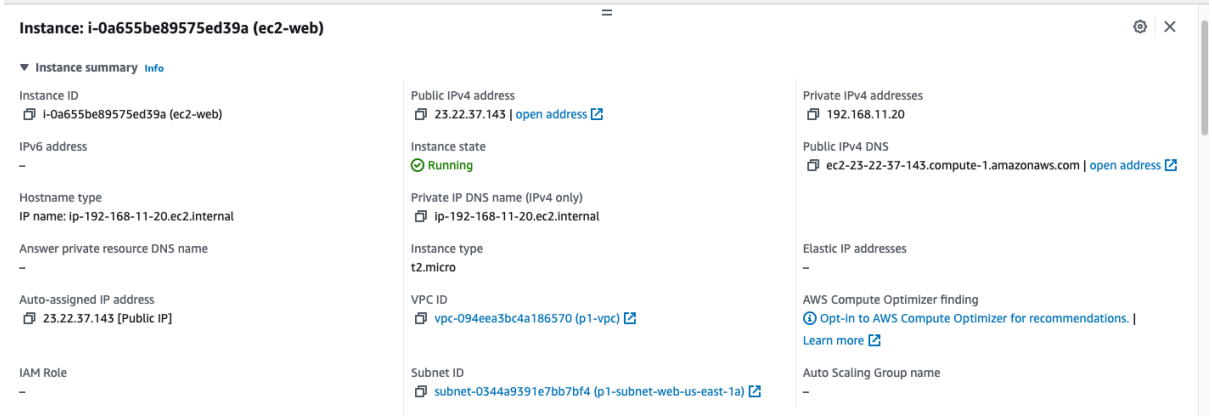


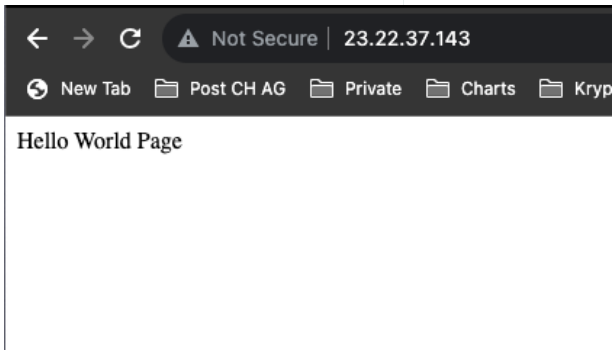
Create and launch the EC2-Windows instance

Go to AWS Management Console EC2->Instances->Launch an instance

1. Name: “ec2-web”
2. Application and OS Images: Select Windows
3. Instance type: Select t2.micro
4. Key pair(login) : Create new key pair
   Key pair name: “windows1”
   Create key pair
5. Edit Network settings.
   VPC: Select “p1-vpc”
   Subnet: Select one of the web-subnet
6. Enable Auto-assign public IP
7. Security group name: “ec2-web-sg”
8. Firewall->Add security group rule: Type=Http, Souryetype=Anywhere
9. UserData: Add commands:
   <powershell>
   Install-WindowsFeature -name Web-Server -IncludeManagementTools
   New-Item -Path C:\inetpub\wwwroot\index.html -ItemType File -Value “Hello World Page” -Force
   </powershell>
10. Launch instance
11. Keep the default for the remaining specifications
12. By following these steps, I successfully launch my new EC2 instance within my VPC.





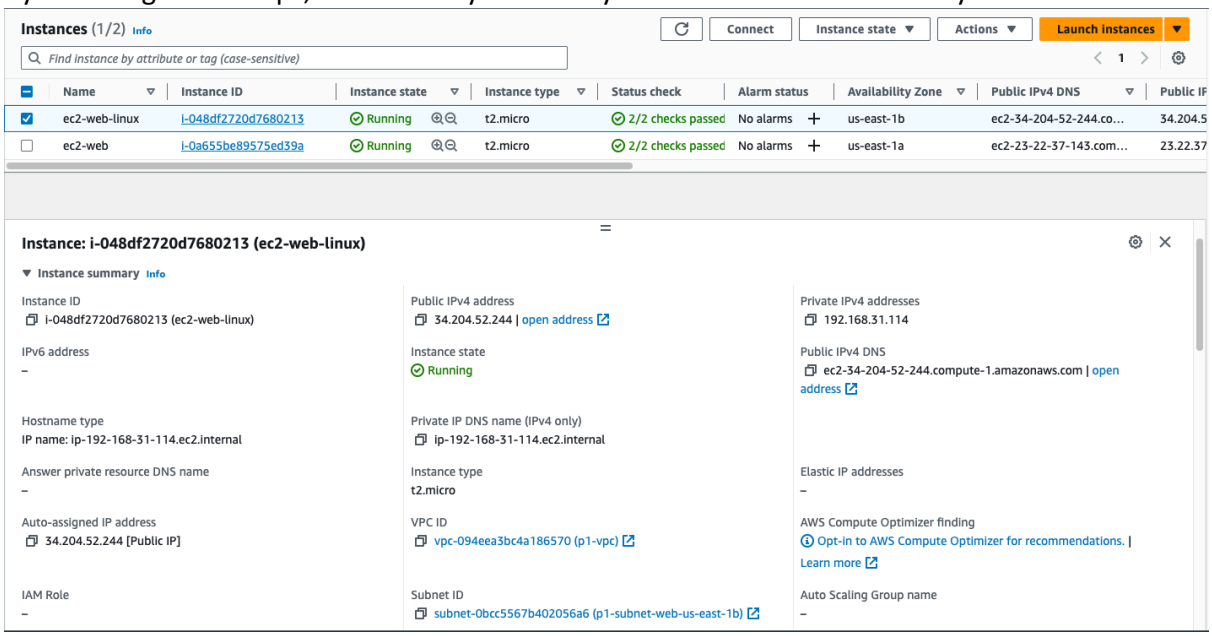


Create and launch the EC2-Linux instance

Go to AWS Management Console EC2->Instances->Launch an instance

1. Name: “ec2-web-linux”
2. Application and OS Images: Select Amazon Linux
3. Instance type: Select t2.micro
4. Key pair(login) : Create new key pair
   Key pair name: “linux1”
   Create key pair
5. Edit Network settings.
   VPC: Select “p1-vpc”
   Subnet: Select one of the web-subnet
6. Firewall->Select existing security group rule: “ec2-web-sg”
7. Launch instance
8. Keep the default for the remaining specifications

By following these steps, I successfully launch my new EC2 instance within my VPC.



Extend inbound rule of security group “ec2-web-sg” to enable ssh

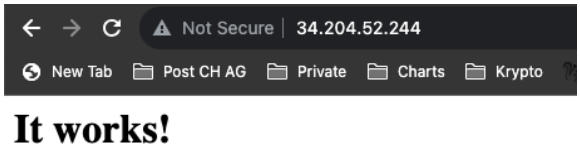
Go to AWS Management Console EC2->Security groups->”ec2-web-sg->Edit inbound rules

1. Add rule: Type=SSH, Source=Custom:0.0.0.0/0
2. Save rules

Install Apache Web-Server on EC2-Linux instance

Go to AWS Management Console EC2->Instances->EC2-Linux instance->Connect to instance
Select EC2 Instance Connect

3. sudo su
4. yum install httpd -y
5. service httpd status (optional:check status)
6. service httpd start



Extend inbound rule of db security group “mysqlsg” to enable access from ec2-web-sg

Go to AWS Management Console EC2->Security groups->”mysqlsg”->Edit inbound rules

1. Add rule: Type=All traffic, Source=Custom: “ex2-weg-sg”
2. Add rule: Type=All traffic, Source=Custom: “ex2-weg-sg”
3. Save rules