

## Problem Statement:

You work for XYZ Corporation. Your corporation wants to launch a new web-based application. The development team has prepared the code but it is not tested yet. The development team needs the system admins to build a web server to test the code but the system admins are not available.

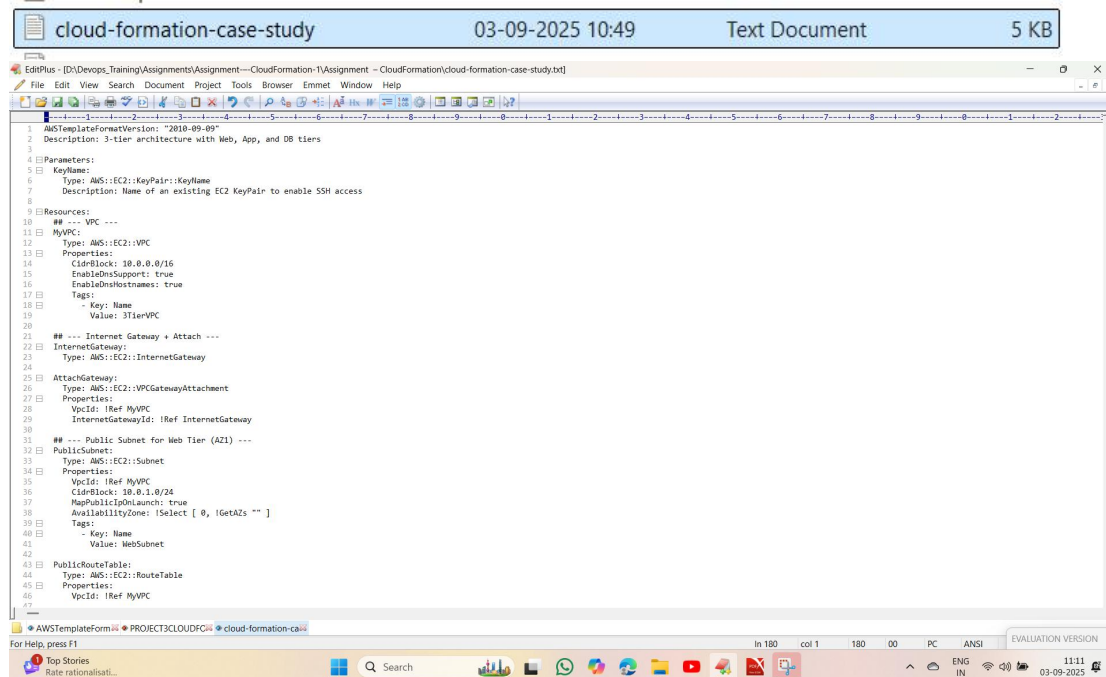
## Tasks To Be Performed:

1. Web tier: Launch an instance in a public subnet and that instance should allow HTTP and SSH from the internet.
2. Application tier: Launch an instance in a private subnet of the web tier and it should allow only SSH from the public subnet of Web Tier-3.
3. DB tier: Launch an RDS MYSQL instance in a private subnet and it should allow connection on port 3306 only from the private subnet of Application Tier-4.
4. Setup a Route 53 hosted zone and direct traffic to the EC2 instance.

You have been also asked to propose a solution so that:

1. Development team can test their code without having to involve the system admins and can invest their time in testing the code rather than provisioning, configuring and updating the resources needed to test the code.
2. Make sure when the development team deletes the stack, RDS DB instances should not be deleted.

## Create the stack by defining template:



The screenshot shows the AWS CloudFormation console with a template named "cloud-formation-case-study" created on 03-09-2025 at 10:49. The template is a Text Document, 5 KB in size. The console displays the template code, which defines a 3-tier architecture with Web, App, and DB tiers. The code includes parameters for KeyName and KeyPair, and resources for VPC, InternetGateway, AttachGateway, PublicSubnet, and PublicRouteTable. The template is written in JSON format and is currently in the "In Progress" state.

```
1 AWSTemplateFormatVersion: "2010-09-09"
2 Description: 3-tier architecture with Web, App, and DB tiers
3
4 Parameters:
5   KeyName:
6     Type: AWS::EC2::KeyPair::KeyName
7     Description: Name of an existing EC2 KeyPair to enable SSH access
8
9 Resources:
10   MyVPC:
11     Type: AWS::EC2::VPC
12     Properties:
13       CidrBlock: 10.0.0.0/16
14       EnableDnsSupport: true
15       EnableDnsHostnames: true
16       Tags:
17         - Key: Name
18           Value: 3TierVPC
19
20   InternetGateway:
21     Type: AWS::EC2::InternetGateway
22
23   AttachGateway:
24     Type: AWS::EC2::VPCGatewayAttachment
25     Properties:
26       VpcId: !Ref MyVPC
27       InternetGatewayId: !Ref InternetGateway
28
29   PublicSubnet:
30     Type: AWS::EC2::Subnet
31     Properties:
32       VpcId: !Ref MyVPC
33       CidrBlock: 10.0.1.0/24
34       MapPublicIpOnLaunch: true
35       AvailabilityZone: !Select [ 0, !GetAZs "" ]
36       Tags:
37         - Key: Name
38           Value: WebSubnet
39
40   PublicRouteTable:
41     Type: AWS::EC2::RouteTable
42     Properties:
43       VpcId: !Ref MyVPC
```

```
46 VpcId: !Ref MyVPC
47
48 PublicRoute:
49   Type: AWS::EC2::Route
50   DependsOn: AttachGateway
51   Properties:
52     RouteTableId: !Ref PublicRouteTable
53     DestinationCidrBlock: 0.0.0.0/0
54     GatewayId: !Ref InternetGateway
55
56 PublicSubnetRouteTableAssociation:
57   Type: AWS::EC2::SubnetRouteTableAssociation
58   Properties:
59     SubnetId: !Ref PublicSubnet
60     RouteTableId: !Ref PublicRouteTable
61
62 ## --- Private Subnet for App Tier (AZ1) ---
63 PrivateSubnetApp:
64   Type: AWS::EC2::Subnet
65   Properties:
66     VpcId: !Ref MyVPC
67     CidrBlock: 10.0.2.0/24
68     MapPublicIpOnLaunch: false
69     AvailabilityZone: !Select [ 0, !GetAZs "" ] # AZ1
70     Tags:
71       - Key: Name
72         Value: AppSubnet
73
74 ## --- Private Subnet for DB Tier (AZ2) ---
75 PrivateSubnetDB:
76   Type: AWS::EC2::Subnet
77   Properties:
78     VpcId: !Ref MyVPC
79     CidrBlock: 10.0.3.0/24
80     MapPublicIpOnLaunch: false
81     AvailabilityZone: !Select [ 1, !GetAZs "" ] # AZ2
82     Tags:
83       - Key: Name
84         Value: DBSubnet
85
86 ## --- Security Groups ---
87 WebSG:
88   Type: AWS::EC2::SecurityGroup
89   Properties:
90     GroupDescription: Allow HTTP and SSH from Internet
91     VpcId: !Ref MyVPC
92     Tags:
93       - Key: Name
94         Value: WebSG
```



```
94 FromPort: 22
95 ToPort: 22
96 CidrIp: 0.0.0.0/0
97 - IpProtocol: tcp
98 FromPort: 80
99 ToPort: 80
100 CidrIp: 0.0.0.0/0
101
102 AppSG:
103   Type: AWS::EC2::SecurityGroup
104   Properties:
105     GroupDescription: Allow SSH from Web Subnet
106     VpcId: !Ref MyVPC
107     SecurityGroupIngress:
108       - IpProtocol: tcp
109         FromPort: 22
110         ToPort: 22
111         SourceSecurityGroupId: !Ref WebSG
112
113 DBSG:
114   Type: AWS::EC2::SecurityGroup
115   Properties:
116     GroupDescription: Allow MySQL from App Subnet
117     VpcId: !Ref MyVPC
118     SecurityGroupIngress:
119       - IpProtocol: tcp
120         FromPort: 3306
121         ToPort: 3306
122         SourceSecurityGroupId: !Ref AppSG
123
124 ## --- EC2 Web Instance ---
125 WebInstance:
126   Type: AWS::EC2::Instance
127   Properties:
128     InstanceType: t2.micro
129     KeyName: !Ref KeyName
130     # Replace with appropriate AMI ID for your region
131     ImageId: !Sub ["${resolve:ssm:/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-default-x86_64}"]
132     SecurityGroups: [!Ref WebSG]
133     SubnetId: !Ref PublicSubnet
134     Tags:
135       - Key: Name
136         Value: WebInstance
137
138 ## --- EC2 App Instance ---
139 AppInstance:
140   Type: AWS::EC2::Instance
```



```
139 AppInstance:
140   Type: AWS::EC2::Instance
141   Properties:
142     InstanceType: t3.micro
143     KeyName: !Ref KeyName
144     ImageId: !Sub "${resolve:ssm:/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-default-x86_64}"
145     SecurityGroups: !Ref AppSG
146     SubnetId: !Ref PrivateSubnetApp
147     Tags:
148       - Key: Name
149         Value: AppInstance
150
151 ## --- RDS DB Instance ---
152 DBSubnetGroup:
153   Type: AWS::RDS::DBSubnetGroup
154   Properties:
155     DBSubnetGroupDescription: Subnet group for RDS
156     SubnetIds:
157       - !Ref PrivateSubnetApp
158       - !Ref PrivateSubnetDB
159
160 MyRDSInstance:
161   Type: AWS::RDS::DBInstance
162   DeletionPolicy: Retain
163   Properties:
164     DBName: mydb
165     Engine: mysql
166     MasterUsername: admin
167     MasterUserPassword: MySecurePass123
168     DBInstanceClass: db.t3.micro
169     AllocatedStorage: 20
170     VPCSecurityGroups:
171       - !Ref DBSG
172     DBSubnetGroupName: !Ref DBSubnetGroup
173     MultiAZ: false
174     PubliclyAccessible: false
175
176 Outputs:
177   WebInstancePublicIP:
178     Description: Public IP of the Web Tier Instance
179     Value: !GetAtt WebInstance.PublicIp
180
```

Edge AWS Management Console CloudFormation - Stack my-stack Instances | EC2 | us-east-1 Aurora and RDS | us-east-1 vpcs | VPC Console CloudFormation template

https://251985476962-ztjdpc-us-east-1.console.aws.amazon.com/cloudformation/home?region=us-east-1#/stacks/resources?filteringStatus=active&filteringText=8stackId=arn%3Aaws%3Acloudfo... Account ID: 2519-8547-6962 United States (N. Virginia) root

CloudFormation > Stacks > my-stack

Stacks (1)

Filter by stack name

Filter status: Active View nested

Stacks

my-stack  
2025-09-03 10:50:28 UTC+0530  
CREATE\_COMPLETE

my-stack

Delete Update stack Stack actions Create stack

Stack info Events Resources Outputs Parameters Template Change settings

Resources (16)

Search resources

Logical ID	Physical ID	Type	Status
AppInstance	<a href="#">i-0aa8712804cad95af</a>	AWS::EC2::Instance	CREATE_COMPLETE
AppSG	<a href="#">sg-076017cfb89e81ac9</a>	AWS::EC2::SecurityGroup	CREATE_COMPLETE
AttachGateway	IGWlvp-0d45d7e5e1cb30b27	AWS::EC2::VPCGatewayAttachment	CREATE_COMPLETE
DBSG	<a href="#">sg-04240fa72d69744a7</a>	AWS::EC2::SecurityGroup	CREATE_COMPLETE
DBSubnetGroup	<a href="#">my-stack-dbsubnetgroup-0lmeiZobmqed</a>	AWS::RDS::DBSubnetGroup	CREATE_COMPLETE

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

NIFTY -0.07%

Edge AWS Management Console CloudFormation - Stack my Instances | EC2 | us-east-1 Aurora and RDS | us-east-1 vpcs | VPC Console CloudFormation template

https://251985476962-ztjdprc-us-east-1.console.aws.amazon.com/cloudformation/home?region=us-east-1#/stacks/resources?filteringStatus=active&filteringText=&stackId=arn%3Aaws%3Acloudfo... Account ID: 2519-8547-6962 root

CloudFormation > Stacks > my-stack

### Stacks (1)

Filter by stack name Filter status Active View nested

Stacks

- my-stack  
2025-09-03 10:50:28 UTC+0530  
CREATE\_COMPLETE

### Resources (16)

Search resources

Logical ID	Physical ID	Type	Status
DBSubnetGroup	<a href="#">my-stack-dbsubnetgroup-0lmej2obmged</a>	AWS::RDS::DBSubnetGroup	CREATE_COMPLETE
InternetGateway	<a href="#">lgw-0d727590e2c3d0c2b</a>	AWS::EC2::InternetGateway	CREATE_COMPLETE
MyRDSInstance	<a href="#">my-stack-myrdinstance-juc6l400cmyp</a>	AWS::RDS::DBInstance	CREATE_COMPLETE
MyVPC	<a href="#">vpc-0d45d75e1cb30b27</a>	AWS::EC2::VPC	CREATE_COMPLETE
PrivateSubnetApp	<a href="#">subnet-0cf6e4b5cb486654d</a>	AWS::EC2::Subnet	CREATE_COMPLETE
PrivateSubnetDB	<a href="#">subnet-0afc33cfbc2799102</a>	AWS::EC2::Subnet	CREATE_COMPLETE
PublicRoute	<a href="#">rtb-07969ade37bec58e2j0.0.0/0</a>	AWS::EC2::Route	CREATE_COMPLETE
PublicRouteTable	<a href="#">rtb-07969ade37bec58e2</a>	AWS::EC2::RouteTable	CREATE_COMPLETE

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

NIFTY -0.07%

Edge AWS Management Console CloudFormation - Stack my Instances | EC2 | us-east-1 Aurora and RDS | us-east-1 vpcs | VPC Console CloudFormation template

https://251985476962-ztjdprc-us-east-1.console.aws.amazon.com/cloudformation/home?region=us-east-1#/stacks/resources?filteringStatus=active&filteringText=&stackId=arn%3Aaws%3Acloudfo... Account ID: 2519-8547-6962 root

CloudFormation > Stacks > my-stack

### Stacks (1)

Filter by stack name Filter status Active View nested

Stacks

- my-stack  
2025-09-03 10:50:28 UTC+0530  
CREATE\_COMPLETE

### Resources (16)

Search resources

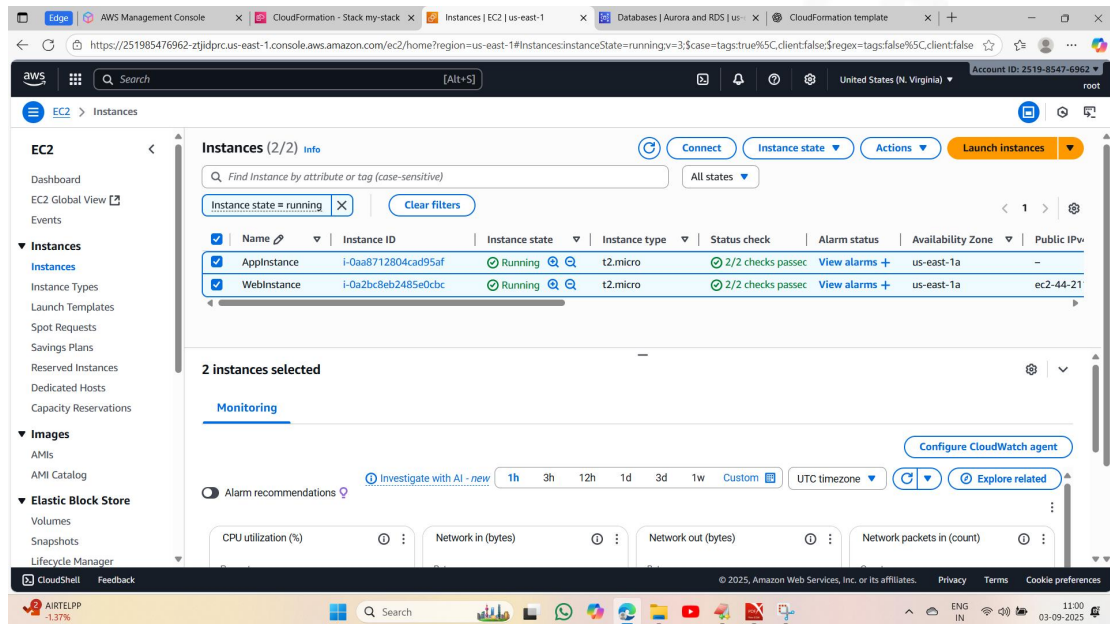
Logical ID	Physical ID	Type	Status
PrivateSubnetDB	<a href="#">subnet-0afc33cfbc2799102</a>	AWS::EC2::Subnet	CREATE_COMPLETE
PublicRoute	<a href="#">rtb-07969ade37bec58e2j0.0.0/0</a>	AWS::EC2::Route	CREATE_COMPLETE
PublicRouteTable	<a href="#">rtb-07969ade37bec58e2</a>	AWS::EC2::RouteTable	CREATE_COMPLETE
PublicSubnet	<a href="#">subnet-016d42c860f7f6c0e</a>	AWS::EC2::Subnet	CREATE_COMPLETE
PublicSubnetRouteTableAssociation	<a href="#">rtbassoc-06a8012d5b7ba3ad8</a>	AWS::EC2::SubnetRouteTableAssociation	CREATE_COMPLETE
WebInstance	<a href="#">i-0a2bc8eb2485e0cbc</a>	AWS::EC2::Instance	CREATE_COMPLETE
WebSG	<a href="#">sg-07f143d90de5786e4</a>	AWS::EC2::SecurityGroup	CREATE_COMPLETE

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

NIFTY -0.07%



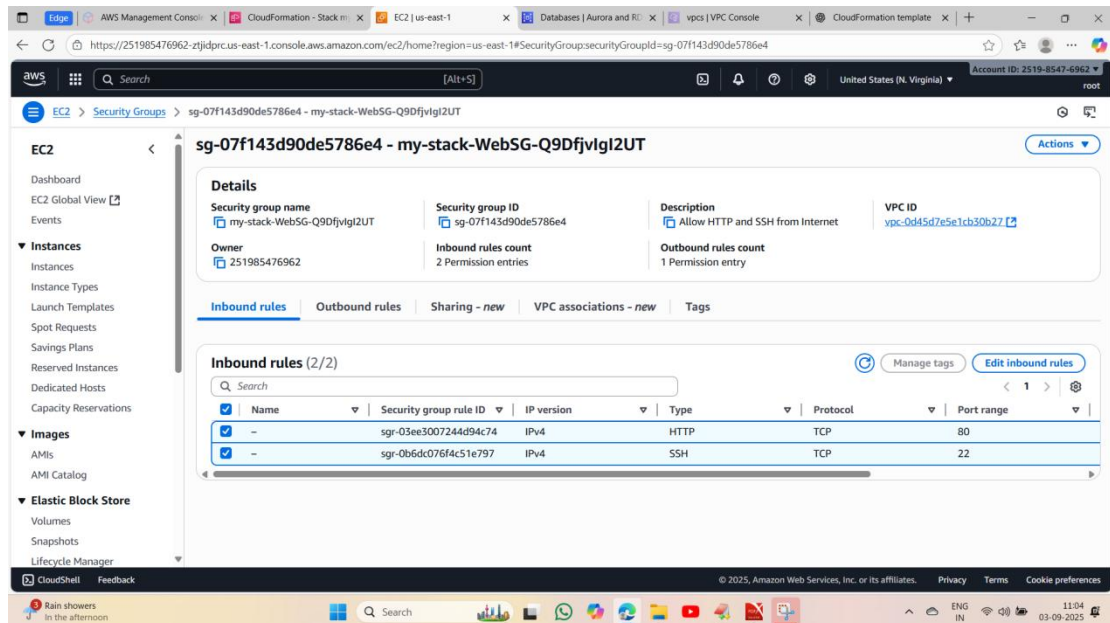
# 1. Web tier: Launch an instance in a public subnet and that instance should allow HTTP and SSH from the internet.



The screenshot shows the AWS Management Console for the 'us-east-1' region. The 'Instances' page displays two EC2 instances:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
AppInstance	i-0aa8712804cad95af	Running	t2.micro	2/2 checks passed	View alarms	us-east-1a	-
WebInstance	i-0a2bc8eb2485e0cbc	Running	t2.micro	2/2 checks passed	View alarms	us-east-1a	ec2-44-21

Below the table, the 'Monitoring' section shows '2 instances selected'. The 'Alarm recommendations' section is also visible.



The screenshot shows the details of the security group 'sg-07f143d90de5786e4 - my-stack-WebSG-Q9DfjvlgI2UT'. The 'Inbound rules' tab is selected, showing two rules:

Name	Security group rule ID	IP version	Type	Protocol	Port range
-	sgr-03ee3007244d94c74	IPv4	HTTP	TCP	80
-	sgr-0b6dc076f4c51e797	IPv4	SSH	TCP	22

Edge AWS Management Console CloudFormation - Stack my-stack SecurityGroup | EC2 | us-east-1 Databases | Aurora and RDS | vpcs | VPC Console CloudFormation template

https://251985476962-ztjdprc-us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#SecurityGroupgroupId=sg-07f143d90de5786e4

Account ID: 2519-8547-6962 United States (N. Virginia) root

EC2 > Security Groups > sg-07f143d90de5786e4 - my-stack-WebSG-Q9DfjvlgI2UT

### sg-07f143d90de5786e4 - my-stack-WebSG-Q9DfjvlgI2UT

**Details**

Security group name my-stack-WebSG-Q9DfjvlgI2UT	Security group ID sg-07f143d90de5786e4	Description Allow HTTP and SSH from Internet	VPC ID vpc-0d45d7e5e1cb30b27
Owner 251985476962	Inbound rules count 2 Permission entries	Outbound rules count 1 Permission entry	

**Inbound rules** Outbound rules Sharing - new VPC associations - new Tags

**Inbound rules (2)** Manage tags Edit inbound rules

	IP version	Type	Protocol	Port range	Source	Description
4	IPv4	HTTP	TCP	80	0.0.0.0/0	-
7	IPv4	SSH	TCP	22	0.0.0.0/0	-

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Nifty bank +0.09%

2. Application tier: Launch an instance in a private subnet of the web tier and it should allow only SSH from the public subnet of Web Tier-3.

Edge AWS Management Console CloudFormation - Stack my-stack Instances | EC2 | us-east-1 Databases | Aurora and RDS | CloudFormation template

https://251985476962-ztjdprc-us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#InstancesinstanceState=runningv=3;case=tags:true%5C,client:false%5C,client:false

Account ID: 2519-8547-6962 United States (N. Virginia) root

EC2 > Instances

### Instances (2/2) Info

Find Instance by attribute or tag (case-sensitive) All states

Instance state = running Clear filters

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv
<input checked="" type="checkbox"/>	AppInstance	i-0aa8712804cad95af	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	-
<input checked="" type="checkbox"/>	WebInstance	i-0a2bc8eb2485e0cbc	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	ec2-44-21

**2 instances selected**

**Monitoring**

Configure CloudWatch agent

Investigate with AI - new 1h 3h 12h 1d 3d 1w Custom UTC timezone Explore related

Alarm recommendations

CPU utilization (%) Network in (bytes) Network out (bytes) Network packets in (count)

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

AIRTELPP -1.37%

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

sg-076017cfb89e81ac9 - my-stack-AppSG-0aPixa2XPfom

Details

Security group name

my-stack-AppSG-0aPixa2XPfom

Security group ID

sg-076017cfb89e81ac9

Description

Allow SSH from Web Subnet

VPC ID

ypc-0d45d7e5e1cb30b27

Owner

251985476962

Inbound rules count

1 Permission entry

Outbound rules count

1 Permission entry

Inbound rules

Outbound rules

Sharing - new

VPC associations - new

Tags

Inbound rules (1/1)

Search

	Name	Security group rule ID	IP version	Type	Protocol	Port range
<input checked="" type="checkbox"/>	-	sgr-07d1e067b0978e1e5	-	SSH	TCP	22

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

NIFTY

-0.07%

Edge

AWS Management Console

CloudFormation - Stack m...

SecurityGroup | EC2 | us-e...

Databases | Aurora and R...

vpcs | VPC Console

CloudFormation template

https://251985476962-ztjdprc-us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#SecurityGroup:securityGroupId=sg-076017cfb89e81ac9

United States (N. Virginia)

Account ID: 2519-8547-6962

root

sg-076017cfb89e81ac9 - my-stack-AppSG-0aPixa2XPfom

Details

Security group name

my-stack-AppSG-0aPixa2XPfom

Security group ID

sg-076017cfb89e81ac9

Description

Allow SSH from Web Subnet

VPC ID

ypc-0d45d7e5e1cb30b27

Owner

251985476962

Inbound rules count

1 Permission entry

Outbound rules count

1 Permission entry

Inbound rules

Outbound rules

Sharing - new

VPC associations - new

Tags

Inbound rules (1)

Search

	IP version	Type	Protocol	Port range	Source	Description
<input checked="" type="checkbox"/>	-	SSH	TCP	22	sg-07f143d90de5786e...	-

CloudShell

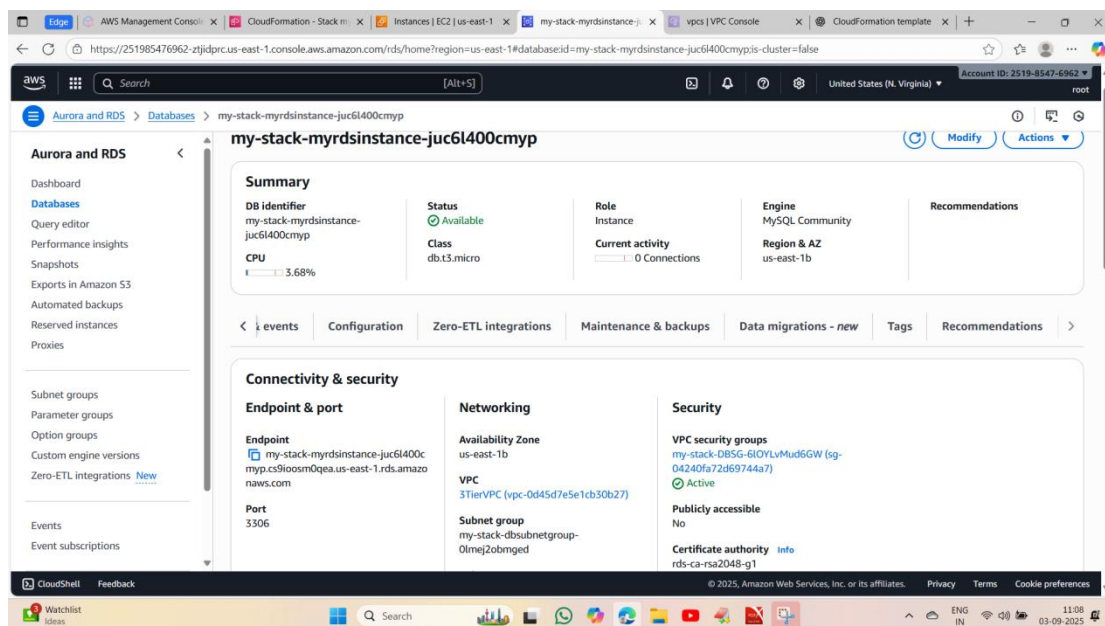
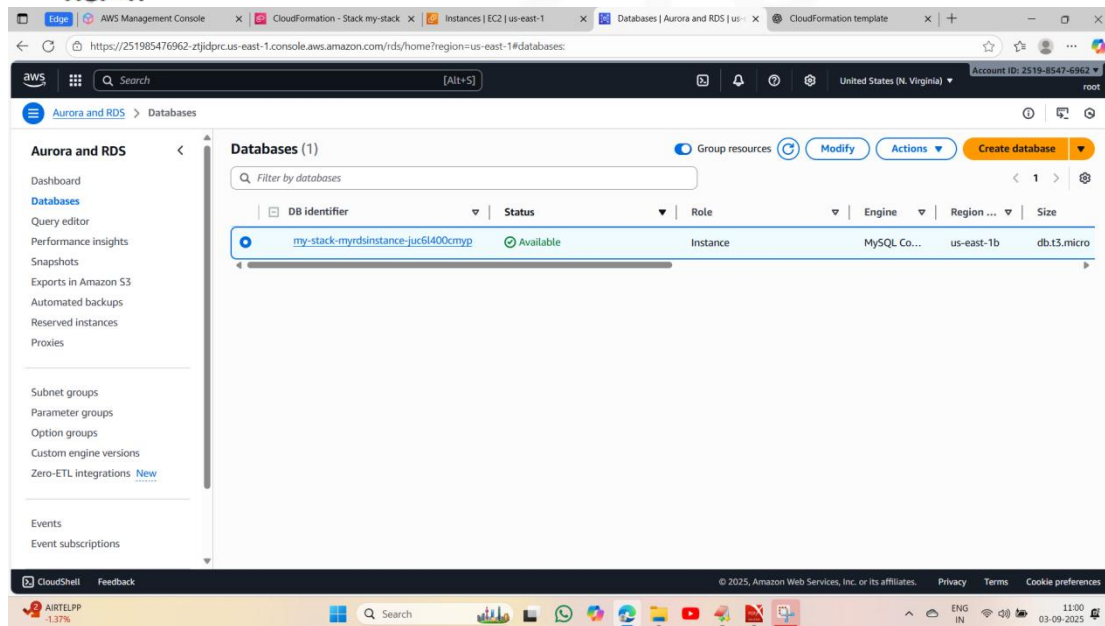
Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Nifty bank

+0.09%

3. DB tier: Launch an RDS MYSQL instance in a private subnet and it should allow connection on port 3306 only from the private subnet of Application Tier-4.



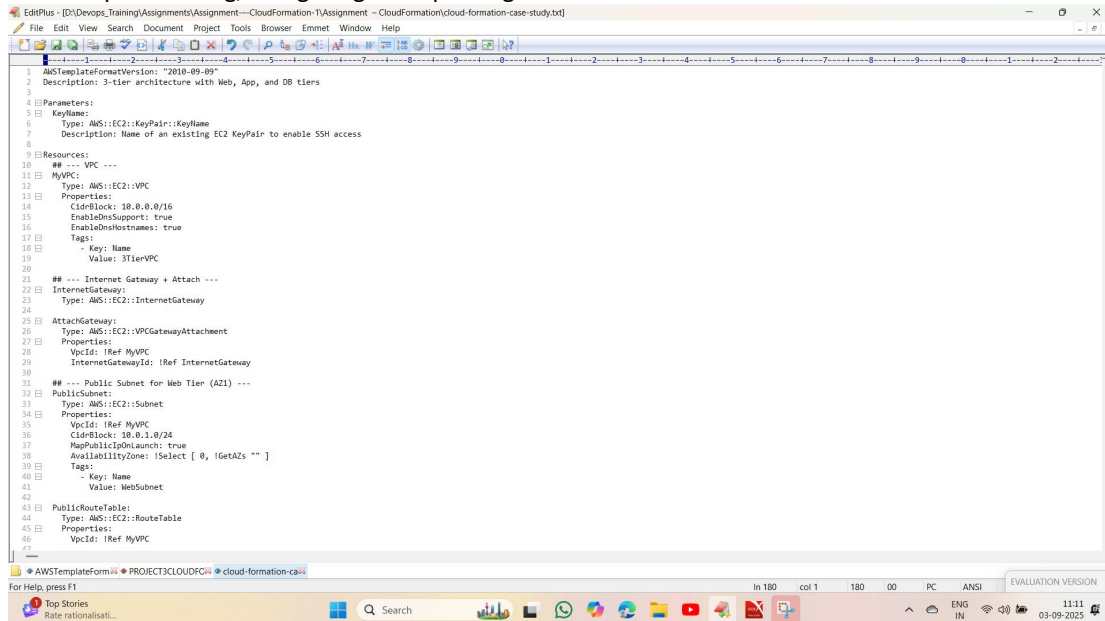
You have been also asked to propose a solution so that:

1. Development team can test their code without having to involve the system admins and can invest their time in testing the code rather than provisioning, configuring and updating the resources needed to test the code.
2. Make sure when the development team deletes the stack, RDS DB instances should not be deleted.



1. Development team can test their code without having to involve the system admins and can invest their time in testing the code rather than provisioning, configuring and updating the resources needed to test the code.

By making use of **template** development team can create **stack** and test their code without having to involve admins and can invest their time in testing the code rather than provisioning, configuring and updating the resources needed to test the code.

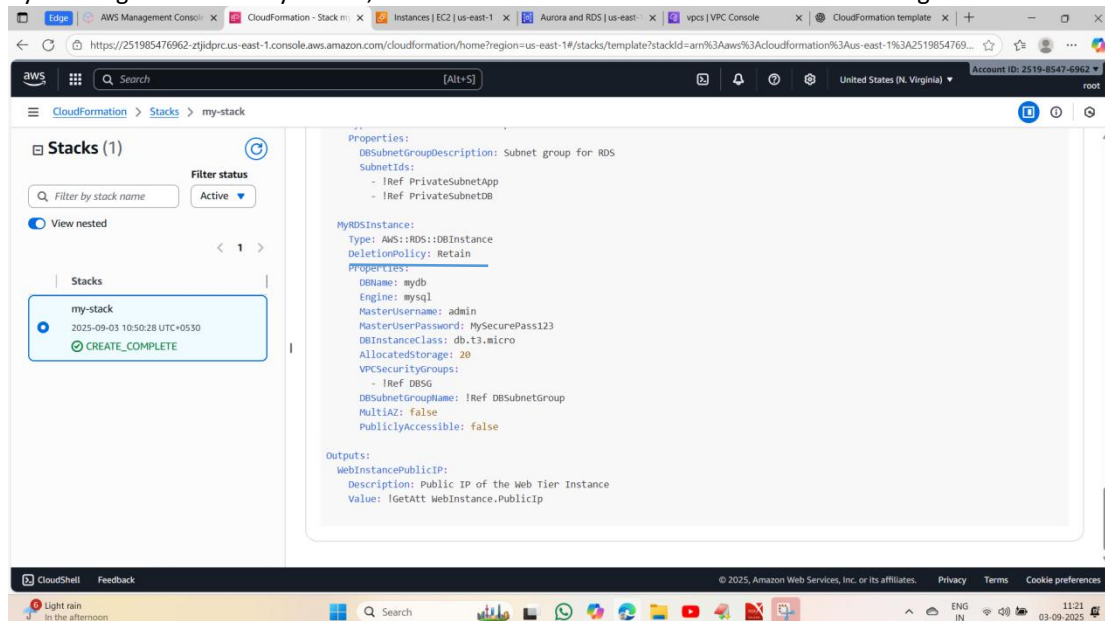


The screenshot shows an AWS CloudFormation template in an IDE. The template is for a 3-tier architecture with Web, App, and DB tiers. It includes parameters for KeyName, and resources for VPC, InternetGateway, AttachGateway, PublicSubnet, and PublicRouteTable. The template is written in JSON format.

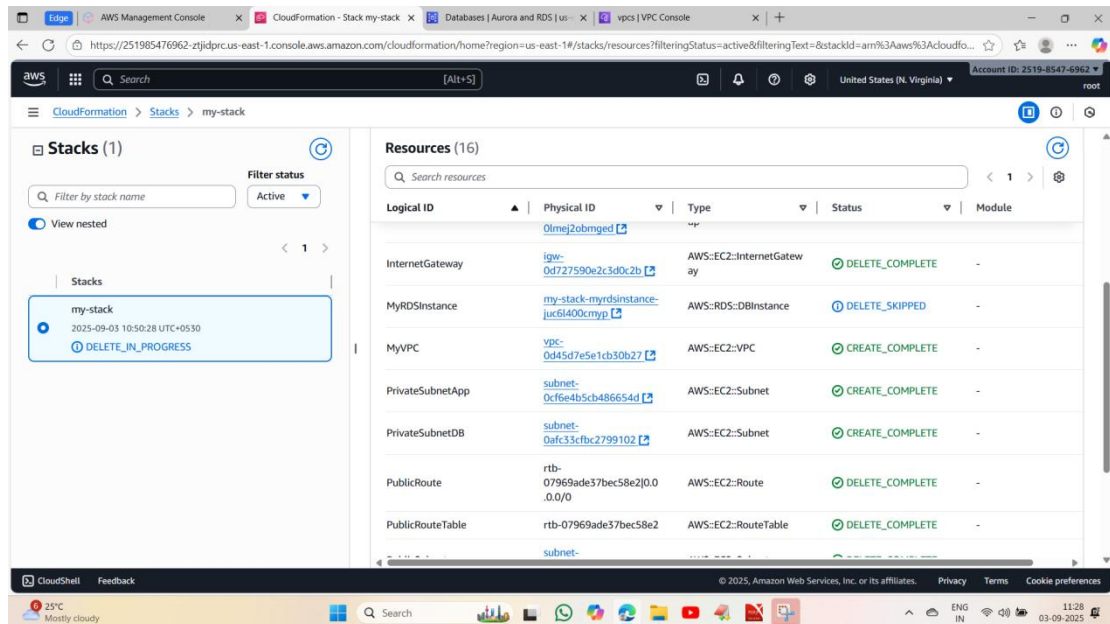
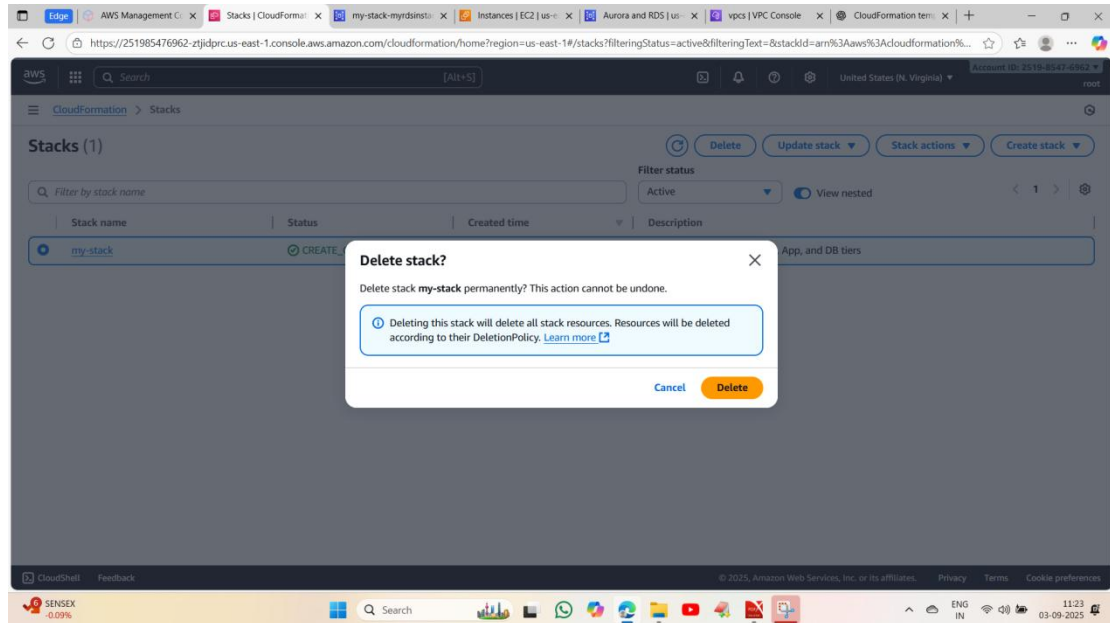
```
1 AWSTemplateFormatVersion: '2010-09-09'
2 Description: 3-tier architecture with Web, App, and DB tiers
3
4 Parameters:
5   KeyName:
6     Type: AWS::EC2::KeyPair::KeyName
7     Description: Name of an existing EC2 KeyPair to enable SSH access
8
9 Resources:
10   ## --- VPC ---
11   MyVPC:
12     Type: AWS::EC2::VPC
13     Properties:
14       CidrBlock: 10.0.0.0/16
15       EnableDnsSupport: true
16       EnableDnsHostnames: true
17     Tags:
18       - Key: Name
19         Value: 3TierVPC
20
21   ## --- Internet Gateway + Attach ---
22   InternetGateway:
23     Type: AWS::EC2::InternetGateway
24
25   AttachGateway:
26     Type: AWS::EC2::VPCGatewayAttachment
27     Properties:
28       VpcId: !Ref MyVPC
29       InternetGatewayId: !Ref InternetGateway
30
31   ## --- Public Subnet for Web Tier (AZ1) ---
32   PublicSubnet:
33     Type: AWS::EC2::Subnet
34     Properties:
35       VpcId: !Ref MyVPC
36       CidrBlock: 10.0.1.0/24
37       MapPublicIpOnLaunch: true
38       AvailabilityZone: !Select [ 0, !GetAZs "" ]
39     Tags:
40       - Key: Name
41         Value: WebSubnet
42
43   PublicRouteTable:
44     Type: AWS::EC2::RouteTable
45     Properties:
46       VpcId: !Ref MyVPC
```

2. Make sure when the development team deletes the stack, RDS DB instances should not be deleted.

By defining `DeletionPolicy:Retain`, we can make the RDS not to be deleted even though Stack deleted.



The screenshot shows the AWS CloudFormation console. On the left, there is a list of stacks under the 'my-stack' stack. The stack is in the 'CREATE\_COMPLETE' state. On the right, the properties of the stack are displayed. The 'MyRDSInstance' resource is highlighted, showing its properties: Type: AWS::RDS::DBInstance, DeletionPolicy: Retain, DBName: mydb, Engine: mysql, MasterUsername: admin, MasterUserPassword: MySecurePass123, DBInstanceClass: db.t3.micro, AllocatedStorage: 20, VPCSecurityGroups: !Ref DBSG, DBSubnetGroupName: !Ref DBSubnetGroup, MultiAZ: false, PubliclyAccessible: false. The outputs section shows 'WebInstancePublicIP' with a description 'Public IP of the Web Tier Instance' and a value 'IGetAtt WebInstance.Publicip'.



Edge AWS Management Console Databases | Aurora and RDS | us-east-1 vpcs | VPC Console Stacks | CloudFormation | us-east-1

https://251985476962-ztjldprc-us-east-1.console.aws.amazon.com/rds/home?region=us-east-1#databases:

Account ID: 2519-8547-6962 United States (N. Virginia) root

Aurora and RDS > Databases

**Aurora and RDS**

- Dashboard
- Databases**
- Query editor
- Performance insights
- Snapshots
- Exports in Amazon S3
- Automated backups
- Reserved instances
- Proxies
- Subnet groups
- Parameter groups
- Option groups
- Custom engine versions
- Zero-ETL integrations [New](#)
- Events
- Event subscriptions

**Databases (1)**

Filter by databases

Group resources Modify Actions Create database

DB identifier	Status	Role	Engine	Region ...	Size
my-stack-myrdinstance-juc6l400cmyp	Available	Instance	MySQL Co...	us-east-1b	db.t3.micro

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Rain coming in about 2.5 hours

Search

11:44 03-09-2025