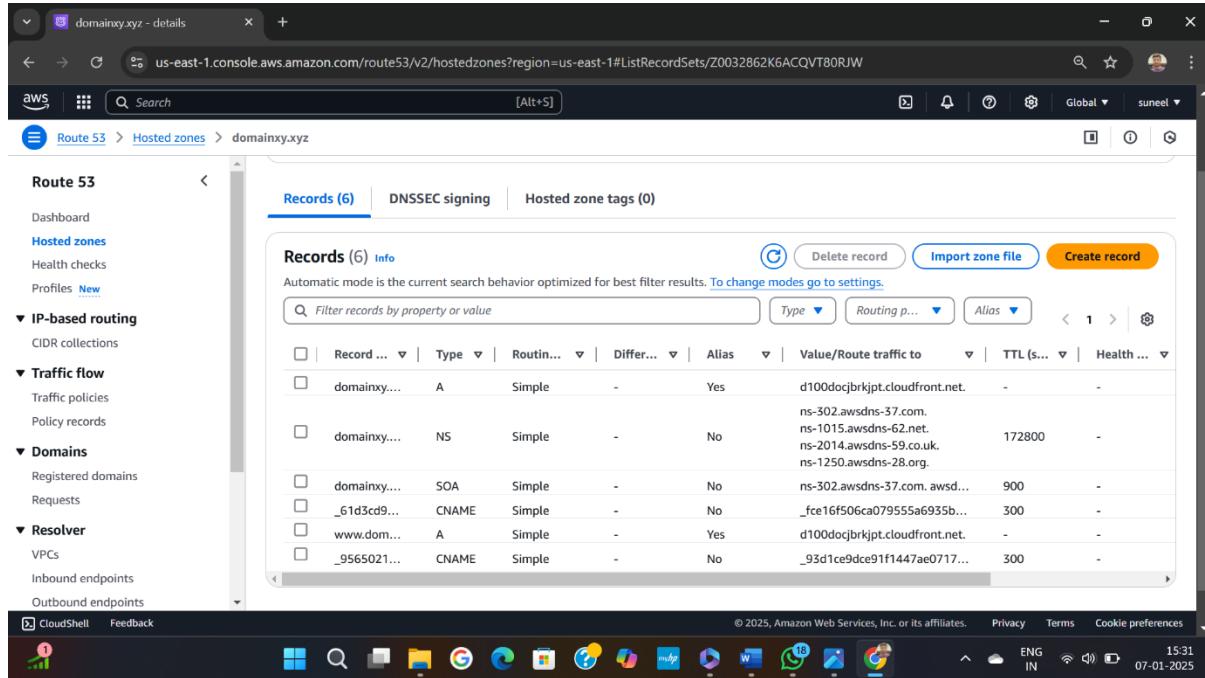


Step 1: Configure Route 53

Begin by creating a public hosted zone in AWS Route 53 for your domain name, domainxy.xyz. Upon creation, AWS will generate NS (Name Server) records for the domain. Add these NS records to your DNS provider to link the domain with AWS services.



The screenshot shows the AWS Route 53 console. On the left, a sidebar menu includes 'Route 53' (selected), 'Dashboard', 'Hosted zones' (selected), 'Health checks', 'Profiles New', 'IP-based routing', 'Traffic flow', 'Domains' (selected), and 'Resolver'. The main content area is titled 'Records (6)' and shows a table of DNS records for the domain 'domainxy....'. The table columns include Record, Type, Value, TTL, and Health. The records are:

Record	Type	Value	TTL	Health
domainxy....	A	d100docjbrkjpt.cloudfront.net.	-	-
domainxy....	NS	ns-302.awsdns-37.com. ns-1015.awsdns-62.net. ns-2014.awsdns-59.co.uk. ns-1250.awsdns-28.org.	172800	-
domainxy....	SOA	ns-502.awsdns-37.com awsd...	900	-
_61d3cd9...	CNAME	_fce16f506ca079555a6935b...	300	-
www.dom...	A	d100docjbrkjpt.cloudfront.net.	-	-
_9565021...	CNAME	_93d1ce9dce91f1447ae0717...	300	-

Step2: Public SSL Certificate using Amazon ACM

In AWS Certificate Manager (ACM), request a public SSL certificate for your domain, including both domainxy.xyz and www.chandrakiran.xyz. Use Route 53 to automatically create validation records, and once validated, the certificate will be issued.

Route 53

Records (6)

Record	Type	Value	TTL	Health
domainxyz...	A	d100docjbrkjpt.cloudfront.net.	-	Yes
domainxyz...	NS	ns-302.awsdns-37.com. ns-1015.awsdns-62.net. ns-2014.awsdns-59.co.uk. ns-1250.awsdns-28.org.	172800	No
domainxyz...	SOA	ns-302.awsdns-37.com.awsd...	900	No
_61d3cd9...	CNAME	_fce16f506ca079555a6935b...	300	No
www.dom...	A	d100docjbrkjpt.cloudfront.net.	-	Yes
_9565021...	CNAME	_93d1ce9dcce91f1447ae0717...	300	No

Step3: VPC Creation and subnets

Create a VPC named "3-Tier VPC" with two availability zones (AZs). Set up two public subnets and four private subnets. Attach a NAT Gateway to connect private subnets to the internet indirectly. Enable public IP auto-assignment for the public subnets.

Your VPCs (1/1)

Name	VPC ID	State	Block Public...	IPv4 CIDR	IPv6 CIDR
project-vpc	vpc-0759059a111bf23ab	Available	Off	10.0.0.0/16	-

Resource map

- VPC:** project-vpc
- Subnets (6):** us-east-1a (project-subnet-public1-us-east-1a), us-east-1b (project-subnet-private1-us-east-1a), us-east-1c (project-subnet-public2-us-east-1b), us-east-1d (project-subnet-private2-us-east-1b)
- Route tables (6):** project-rtb-private1-us-east-1a, project-rtb-private4-us-east-1b

Step 4: Bastion Host Security Group

Create a security group named Bastion Host within the 3-Tier VPC. Allow SSH (port 22) from any IPv4 source to enable secure remote administration.

Instance summary for i-03e1e2b96d77d0ef8 (bastion-host)

- Instance ID:** i-03e1e2b96d77d0ef8
- IPv6 address:** -
- Hostname type:** IP name: ip-10-0-7-89.ec2.internal
- Answer private resource DNS name:** -
- Auto-assigned IP address:** 54.235.226.16 [Public IP]
- IAM Role:** -
- Public IPv4 address:** 54.235.226.16 [open address]
- Instance state:** Running
- Private IP4 address:** 10.0.7.89
- Private IP DNS name (IPv4 only):** ip-10-0-7-89.ec2.internal
- Instance type:** t2.micro
- VPC ID:** vpc-0759059a111bf23ab (project-vpc)
- Subnet ID:** subnet-015e6d57c13e90ad1 (project-subnet-public1-us-east-1a)
- Elastic IP addresses:** -
- AWS Compute Optimizer finding:** Opt-in to AWS Compute Optimizer for recommendations.
- Auto Scaling Group name:** -

Step 5: Presentation Tier ALB Security Group

Set up a security group named Presentation Tier ALB in the VPC. Allow inbound HTTP (port 80) traffic from any IPv4 source for public web access.

Details

Load balancer type: Application	Status: Active	VPC: vpc-0759059a111bf23ab	Load balancer IP address type: IPv4
Scheme: Internet-facing	Hosted zone: Z355XDOTRQ7X7K	Availability Zones: subnet-05f31d989155a6059 us-east-1b (use1-az4), subnet-015e6d57c13e90ad1 us-east-1a (use1-az2)	Date created: January 6, 2025, 11:33 (UTC+05:30)
Load balancer ARN: arn:aws:elasticloadbalancing:us-east-1:605134464260:loadbalancer/app/presentation-tier-alb/18b32729a90a9d28		DNS name: presentation-tier-alb-1363431536.us-east-1.elb.amazonaws.com (A Record)	

Listeners and rules (1)

Step 6: Presentation Tier EC2 Security group

Create a security group named Presentation Tier EC2. Allow inbound SSH from the Bastion Host and HTTP traffic from the Presentation Tier ALB for web server communication.

sg-008109c2dd5489c5f - application-tier-ec2

Details

Security group name application-tier-ec2	Security group ID sg-008109c2dd5489c5f	Description application-tier-ec2	VPC ID vpc-0759059a111bf23ab
Owner 605134464260	Inbound rules count 2 Permission entries	Outbound rules count 1 Permission entry	

Inbound rules (2)

Name	Security group rule ID	IP version	Type	Protocol	Port
-	sgr-0f57d252a8cb3cc40	-	Custom TCP	TCP	32
-	sgr-042b3917d68c270e8	-	SSH	TCP	22

Step 7: Application Tier ALB Security Group

Create a security group named Application Tier ALB. Allow inbound

HTTP traffic from the Presentation Tier EC2 instances to ensure inter-tier

communication.

sg-03cb6bfa78fc70f01 - application-tier-alb

Details

Security group name application-tier-alb	Security group ID sg-03cb6bfa78fc70f01	Description application-tier-alb	VPC ID vpc-0759059a111bf23ab
Owner 605134464260	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

Inbound rules (1)

Name	Security group rule ID	IP version	Type	Protocol	Port
-	sgr-01348b7ded8c07b18	-	HTTP	TCP	80

Step 8: Application Tier EC2 Security Group

Set up a security group named Application Tier EC2. Allow inbound

SSH from the Bastion Host and custom TCP traffic on port 3200 from the

Application Tier ALB.

sg-008109c2dd5489c5f - application-tier-ec2

Inbound rules (2)

Name	Security group rule ID	Type	Protocol	Port
-	sgr-0f57d252a8cb3c40	Custom TCP	TCP	32
-	sgr-042b3917d68c270e8	SSH	TCP	22

Step 9: Data Tier Security Group

Create a security group named Data Tier. Allow inbound MySQL/Aurora (port 3306) traffic from both the Bastion Host and Application Tier EC2 instances for database access.

sg-07cbda24152ab17dd - data-tier

Inbound rules (2)

Name	Security group rule ID	Type	Protocol	Port
-	sgr-001bf2149052af3c3	MySQL/Aurora	TCP	3306
-	sgr-016b7ab591bbac01d	MySQL/Aurora	TCP	3306

Step 10: Launch the Bastion Host instance

Deploy an Amazon Linux 2023 instance named bastion Host using the t2.micro instance type to minimize costs. Generate a new key pair named 123.pem for secure access. Select the public subnet in the Project VPC and assign the bastion-host security group.

Step 11: Subnet Group in RDS

In Amazon RDS, create a subnet group named dev-db-subnet-group.

Select the private subnets across the two availability zones in your VPC to host the database securely.

Availability zone	Subnet name	Subnet ID	CIDR block
us-east-1a	project-subnet-private1-us-east-1a	subnet-0f3e2be500a2caeb1	10.0.128.0/20
us-east-1b	project-subnet-private2-us-east-1b	subnet-0c309402158ca4335	10.0.144.0/20

Step 12: Data Base creation in RDS

Launch a multi-AZ MySQL database instance named dev-db-instance using the dev/test template. Set the username as admin and password as admin123. Attach the Data Tier security group and use the previously created subnet group.

The screenshot shows the AWS RDS console for the 'dev-db-instance'. The instance is identified as 'dev-db-instance' and is currently 'Available'. It runs the 'MySQL Community' engine and is located in the 'us-east-1a' region. The connectivity & security tab is active, displaying the endpoint ('dev-db-instance.ctua4qsuyy6i.us-east-1.rds.amazonaws.com'), port (3306), and associated VPC and security group information.

Step 13: Add the identity using the key file and Checking the Data

Base connection using Bastion Host

Using the key file 123.pem, securely connect to

the bastion-host. From there, test the connection to the RDS database to ensure accessibility.

```
root@ip-10-0-1-15:~# C:\Users\204c1>cd downloads
C:\Users\204c1\Downloads>ssh -N -L 3307:dev-db-instance.ctua4qsuyy6i.us-east-1.rds.amazonaws.com:3306 ec2-user@ec2-52-90-31-18.compute-1.amazonaws.com
Identity added: 3-tier-architech.pem (3-tier-architech.pem)

C:\Users\204c1\Downloads>ssh -A ec2-user@ec2-52-90-31-18.compute-1.amazonaws.com
# Amazon Linux 2023
# https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@ip-10-0-1-15 ~]$ sudo su -
[root@ip-10-0-1-15 ~]# ssh ec2-user@ec2-54-174-170-149.compute-1.amazonaws.com
The authenticity of host 'ec2-54-174-170-149.compute-1.amazonaws.com (10.0.26.67)' can't be established.
ED25519 key fingerprint is SHA256:PaELzuM9wdCgMCdqBqBu6UL3glsHwrdrlDRx0lUvk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-54-174-170-149.compute-1.amazonaws.com' (ED25519) to the list of known hosts.

[root@ip-10-0-1-15 ~]#
```

Step 14: Install MYSQL and adding first connection(rds-dev-db-admin)

Install MySQL Workbench on your local machine. Configure a connection named rds-dev-db-admin to the RDS instance on port 3307 using the admin credentials. Test the connection, and if successful, execute initial queries from a GitHub repository.

The screenshot shows the MySQL Workbench interface. In the top tab bar, there are three tabs: 'rds-dev-db-admin', 'rds-dev-db-admin', and 'rds-dev-db-admin'. The 'Query 1' tab is active, displaying the following SQL code:

```

1 -- Create Database and User
2 CREATE DATABASE react_node_app;
3 CREATE USER 'appuser'@'%' IDENTIFIED BY 'admin123';
4 GRANT ALL PRIVILEGES ON react_node_app.* TO 'appuser'@'%';
5 FLUSH PRIVILEGES;

```

In the bottom right corner of the window, the date and time are shown as '29-12-2024 21:11'.

Step 15: Adding the rds-dev-db-appuser connection in Workbench

Add another connection named rds-dev-db-appuser in MySQL

Workbench. Use the same port and credentials to run additional queries provided in the repository.

The screenshot shows the MySQL Workbench interface with a new connection named 'rds-dev-db-appuser'. The 'react_node_app' database is selected in the Navigator. The 'SQL File 1' tab is active, displaying the following SQL code:

```

1 USE react_node_app;
2 -- Create Tables
3 CREATE TABLE `author` (
4     `id` int NOT NULL AUTO_INCREMENT,
5     `name` varchar(255) NOT NULL,
6     `birthday` date NOT NULL,
7     `bio` text NOT NULL,
8     `createdat` date NOT NULL,
9     `updatedat` date NOT NULL,
10    PRIMARY KEY (`id`)
11 ) ENGINE=InnoDB AUTO_INCREMENT=8 DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_0900_ai_ci;
12
13 CREATE TABLE `book` (
14     `id` int NOT NULL AUTO_INCREMENT,

```

The 'Output' pane shows the execution results for each query, indicating successful execution with 0 rows affected. The date and time in the bottom right corner are '29-12-2024 21:35'.

Step 16: Creating Launch Template for Presentation Tier

Create a launch template named Presentation-Tier-It with Amazon Linux

2 as the AMI and t2.micro as the instance type. Attach the Presentation Tier EC2 security group and include user data from the GitHub repository.

User data - optional

```
#!/bin/bash
# Update the package list and install NGINX
sudo yum update -y
sudo yum install nginx -y

# Start and enable NGINX
sudo systemctl start nginx
sudo systemctl enable nginx

# Fetch metadata token (IMDSv2)
TOKEN=$(curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600")

# Fetch instance details using IMDSv2

```

User data has already been base64 encoded

Summary

Software Image (AMI)
Amazon Linux 2023.6.2...[read more](#)
ami-01816d07b1128cd2d

Virtual server type (instance type)
t2.micro

Firewall (security group)
Presentation-tier-ec2

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month.

[Cancel](#) [Create template version](#)

Step 17: Creating Target Group for Presentation Tier

Create a target group named Presentation Tier Target Group for instance targets with a health check path of /health.

Details

Target type Instance	Protocol : Port HTTP: 80	Protocol version HTTP1	VPC vpc-0759059a111bf23ab	
IP address type IPv4	Load balancer presenation-tier-alb			
2 Total targets	2 Healthy	0 Unhealthy	0 Unused	0 Initial
0 Anomalous				

Distribution of targets by Availability Zone (AZ)
Select values in this table to see corresponding filters applied to the Registered targets table below.

Targets **Monitoring** **Health checks** **Attributes** **Tags**

Step 18: Creating Load Balancer for Presentation Tier

Create an internet-facing ALB named Presentation-Tier-ALB in public

subnets. Assign the Presentation Tier ALB security group.

Details

Load balancer type Application	Status Active	VPC vpc-0759059a111bf23ab	Load balancer IP address type IPv4
Scheme Internet-facing	Hosted zone Z35SXDOTRQ7X7K	Availability Zones subnet-05f31d98b155a6059 us-east-1b (use1-az4) subnet-015e6d57c13e90ad1 us-east-1a (use1-az2)	Date created January 6, 2025, 11:33 (UTC+05:30)

Listeners and rules (1) [Info](#)

A listener checks for connection requests on its configured protocol and port. Traffic received by the listener is routed according to the default action and any additional actions defined.

Listeners and rules (1) [Info](#)

Manage rules Manage listener Add listener

Step 19: Creating Auto Scaling Group for Presentation Tier

Create an ASG named Presentation-Tier-ASG with desired capacity 2, minimum 2, and maximum 4. Enable health checks and monitoring.

The screenshot shows the AWS Auto Scaling group details page for 'applicatoin-tier-asg'. The left sidebar includes sections for Elastic Block Store, Network & Security, Load Balancing, and Auto Scaling. The main content area displays the 'Capacity overview' section with desired capacity of 2, scaling limits of 2-4, and a status of '-'.

Capacity overview

Desired capacity	Scaling limits (Min - Max)	Desired capacity type	Status
2	2 - 4	Units (number of instances)	-

Date created
Mon Jan 06 2025 12:09:30 GMT+0530 (India Standard Time)

Launch template

Launch template	AMI ID	Instance type	Owner
lt-058f383f6fb419b87 application-tier-lt	ami-01816d07b1128cd2d	t2.micro	arn:aws:iam::605134464260:root
Version	Security groups	Security group IDs	Create time
4	-	sg-008109c2dd5489c5f	Mon Jan 06 2025 15:47:40

Step 20: Creating Launch Template for Application Tier

Create Application-Tier-lt with user data customized for the RDS endpoint.

The screenshot shows the AWS Launch templates page for 'application-tier-lt'. The left sidebar includes sections for Dashboard, EC2 Global View, Events, Instances, Images, and Elastic Block Store. The main content area displays the 'Launch template details' section with a launch template ID of 'lt-058f383f6fb419b87', a name of 'application-tier-lt', and a default version of 1.

Launch template details

Launch template ID	Launch template name	Default version	Owner
lt-058f383f6fb419b87	application-tier-lt	1	arn:aws:iam::605134464260:root

Launch template version details

Version	Description	Date created	Created by
1 (Default)	version 2	2025-01-06T06:31:16.000Z	arn:aws:iam::605134464260:root
Instance details		Resource tags	Network interfaces
AMI ID	Instance type	Availability Zone	Key pair name
ami-01816d07b1128cd2d	t2.micro	-	123
Security groups		Tags	
-		sg-008109c2dd5489c5f	

The screenshot shows the AWS CloudShell interface. On the left, a terminal window displays a shell script for EC2 user data:

```

echo "LOG_DIR=$LOG_DIR" >> "$ENV_FILE"
echo "DB_HOST="`dev-db-instance.ctua4qsuyy6i.us-east-1.rds.amazonaws.com`" >> "$ENV_FILE"
echo "DB_PORT=3306" >> "$ENV_FILE"
echo "DB_USER=root" >> "$ENV_FILE"
echo "DB_PASSWORD=admin123" >> "$ENV_FILE" # Replace with actual password
echo "DB_NAME=react_node_app" >> "$ENV_FILE"
# Install Node.js dependencies as ec2-user
sudo -u ec2-user npm install
# Start the application using PM2 as ec2-user
sudo -u ec2-user npm run serve
# Ensure PM2 restarts on reboot as ec2-user
sudo -u ec2-user pm2 startup systemd
sudo -u ec2-user pm2 save

```

A note below the script says: "User data has already been base64 encoded".

Summary

- Software Image (AMI)**: Amazon Linux 2023 AMI 2023.6.2... [read more](#)
- Virtual server type (instance type)**: t2.micro
- Firewall (security group)**: application-tier-ec2
- Storage (volumes)**: 1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month.

Create template version

Step 21: Creating Target Group for Application Tier

Create Application Tier Target Group with port 3200 and health check

path /health.

The screenshot shows the AWS CloudShell interface. On the left, a terminal window displays the creation of a target group named "application-tier-sg":

```

arn:aws:elasticloadbalancing:us-east-1:605134464260:targetgroup/application-tier-sg/bc73714e916ea6b1

```

Details

Target type Instance	Protocol : Port HTTP: 3200	Protocol version HTTP1	VPC vpc-0759059a111bf23ab	
IP address type IPv4	Load balancer application-tier-alb			
2 Total targets	2 Healthy	0 Unhealthy	0 Unused	0 Initial
0 Anomalous				

Distribution of targets by Availability Zone (AZ)

Targets | Monitoring | Health checks | Attributes | Tags

Step 22: Creating Load Balancer for Application Tier

Deploy an internal ALB named Application-Tier-ALB in private

subnets.

Step 23: Creating Auto Scaling Group for Application Tier

Configure an ASG named Application-Tier-ASG with a desired capacity

of 3.

Step 24: Checking the Backend connection

Connect the bastion host through command prompt and connect to the application tier instance. Check the logs if obtained then the backend is connected.

```

[ec2-user@ip-10-0-159-59 ~]$ pm2 logs
[TAILING] Tailing last 15 lines for [all] processes (change the value with --lines option)
/home/ec2-user/.pm2/pm2.log last 15 lines:
PM2    | 2025-01-05T19:34:11: PM2 log: PM2 version      : 5.4.3
PM2    | 2025-01-05T19:34:11: PM2 log: Node.js version   : 18.20.5
PM2    | 2025-01-05T19:34:11: PM2 log: Current arch     : x64
PM2    | 2025-01-05T19:34:11: PM2 log: PM2 home        : /home/ec2-user/.pm2
PM2    | 2025-01-05T19:34:11: PM2 log: PM2 PID file       : /home/ec2-user/.pm2/pm2.pid
PM2    | 2025-01-05T19:34:11: PM2 log: RPC socket file    : /home/ec2-user/.pm2/rpc.sock
PM2    | 2025-01-05T19:34:11: PM2 log: BUS socket file    : /home/ec2-user/.pm2/pub.sock
PM2    | 2025-01-05T19:34:11: PM2 log: Application log path : /home/ec2-user/.pm2/logs
PM2    | 2025-01-05T19:34:11: PM2 log: Worker Interval    : 30000
PM2    | 2025-01-05T19:34:11: PM2 log: Process dump file  : /home/ec2-user/.pm2/dump.pm2
PM2    | 2025-01-05T19:34:11: PM2 log: Concurrent actions  : 2
PM2    | 2025-01-05T19:34:11: PM2 log: SIGTERM timeout    : 1600
PM2    | 2025-01-05T19:34:11: PM2 log: =====
PM2    | 2025-01-05T19:34:11: PM2 log: App [server:0] starting in -fork mode-
PM2    | 2025-01-05T19:34:11: PM2 log: App [server:0] online

/home/ec2-user/.pm2/logs/server-error.log last 15 lines:
/home/ec2-user/.pm2/logs/server-out.log last 15 lines:
0|server | Server is running on port http://localhost:3200
0|server | 2025-01-05 19:34:12 [INFO]: Connected to MySQL Database

```

Step 25: Modifying Presentation Tier Launch template

Select the Presentation-Tier-It and modify it by changing the version as 2.

Go to the user data and make the changes and update. Replace the domain name with our actual domain name and the application tier DNS name.

User data - optional

```

TOKEN=$(curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"
# Fetch instance details using IMDSv2
INSTANCE_ID=$(curl -H "X-aws-ec2-metadata-token: $TOKEN"
"http://169.254.169.254/latest/meta-data/instance-id")
AVAILABILITY_ZONE=$(curl -H "X-aws-ec2-metadata-token: $TOKEN"
"http://169.254.169.254/latest/meta-data/placement/availability-zone")
PUBLIC_IP=$(curl -H "X-aws-ec2-metadata-token: $TOKEN"
"http://169.254.169.254/latest/meta-data/public-ipv4")

# Create a simple HTML page displaying instance details
sudo bash -c "cat > /usr/share/nginx/html/index.html <<EOF
<h1>Instance Details</h1>
<p><b>Instance ID:</b> $INSTANCE_ID</p>

```

User data has already been base64 encoded

Summary

Software Image (AMI)
Amazon Linux 2023 AMI 2023.6.2... [read more](#)
ami-01816d07b1128cd2d

Virtual server type (instance type)
t2.micro

Firewall (security group)
Presentation-tier-ec2

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month.

[Cancel](#) [Create template version](#)



Step 26: Modifying Presentation Tier Auto Scaling group

Select the Presentation-Tier-ASG and edit the desired quantity as 2 with a minimum and maximum of 2 and 2. Name the template version as 2.

The screenshot shows the AWS EC2 Auto Scaling group details page for 'presenation-tier-asg'. The 'Capacity overview' section displays the desired capacity as 2, scaling limits from 2 to 2, and the desired capacity type as 'Units (number of instances)'. The 'Launch template' section shows the launch template name as 'lt-Oad18cb2164c3992b', AMI ID as 'ami-01816d07b1128cd2d', instance type as 't2.micro', and owner as 'arn:aws:iam::605134464260:root'. The 'Details' tab is selected, showing the date created as Mon Jan 06 2025 11:36:12 GMT+0530 (India Standard Time). Other tabs include Integrations - new, Automatic scaling, Instance management, Instance refresh, Activity, and Monitoring.

Step 27: Integrating application with Cloud Watch

Connect to the application tier EC2 instances and check the logs. We can see the books and authors.

```
2025-01-02 12:13:48 [INFO]: Connected to MySQL Database
Broadcast message from root@localhost (Thu 2025-01-02 12:58:19 UTC):
2025-01-02 12:58:21 [INFO]: Books count: 8
The system will power off now!authorsController [GET]
2025-01-02 12:58:26 [INFO]: Authors count: 6
Connection to 10.0.156.7 closed normally: 8
[ec2-user@ip-10-0-11-78 ~]$ client_loop: send disconnect: Connection reset by peer.
authorId: 4
C:\Users\ASUS>cd ..
```

Step 28: IAM Role

Create the IAM role using EC2 and giving the roles as "CloudWatchLogsFullAccess" and "CloudWatchAgentServicePolicy". Give the name to this role as "EC2InstanceRoleForCloudWatchlogs"

Identity and Access Management (IAM)

Permissions

Permissions policies (2)

Policy name	Type	Attached entities
CloudWatchAgentServerPolicy	AWS managed	1
CloudWatchLogsFullAccess	AWS managed	1

Step 29: Cloud Watch Log Group

Go to the Cloud watch log group services in the aws and create a log group

named as backend-node-app-logs. We can see the logs such as book created or deleted etc..

Log group details

Log streams (0)

Step 30: Modifying Application Tier Launch template

Create a modified version for the application launch template named as version 2. Attach the IAM role that we created in the advanced details and enable the cloud watch monitoring and update the user data script.

The screenshot shows the 'Modify template (Create new version)' page for an EC2 launch template. On the left, there's a code editor containing the CloudWatch Agent configuration file:

```
# Step 1: Install CloudWatch Agent
sudo yum install -y amazon-cloudwatch-agent

# Step 2: Create the CloudWatch Agent configuration file
sudo tee /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-
agent.json > /dev/null <>EOL
{
  "logs": {
    "logs_collected": {
      "files": {
        "collect_list": [
          {
            "file_path": "/home/ec2-user/react-node-mysql-app/backend/logs/*.*",
            "log_group_name": "backend-node-app-logs",
            "log_stream_name": "{instance_id}"
          }
        ]
      }
    }
  }
}
```

On the right, the 'Summary' section includes:

- Software Image (AMI)**: Amazon Linux 2023 AMI 2023.6.2... [read more](#)
- Virtual server type (instance type)**: t2.micro
- Firewall (security group)**: application-tier-ec2
- Storage (volumes)**: 1 volume(s) - 8 GiB
- A callout box for the **Free tier** (in your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month).

At the bottom are 'Cancel' and 'Create template version' buttons.



Step 31: Modifying Application Tier Auto Scaling Group

Update the version of the application tier auto scaling group and name it as

version 2.

The screenshot shows the 'Edit Auto Scaling group | EC2' page. The left sidebar lists various AWS services. The main area displays the 'Launch template' configuration for the 'application-tier-asg' group:

- Launch template**: application-tier-lt
- Version**: 2
- Description**: version 2
- AMI ID**: ami-01816d07b1128cd2d
- Key pair name**:
- Launch template**: application-tier-lt
- Security groups**: -
- Instance type**: t2.micro
- Request Spot Instances**: No

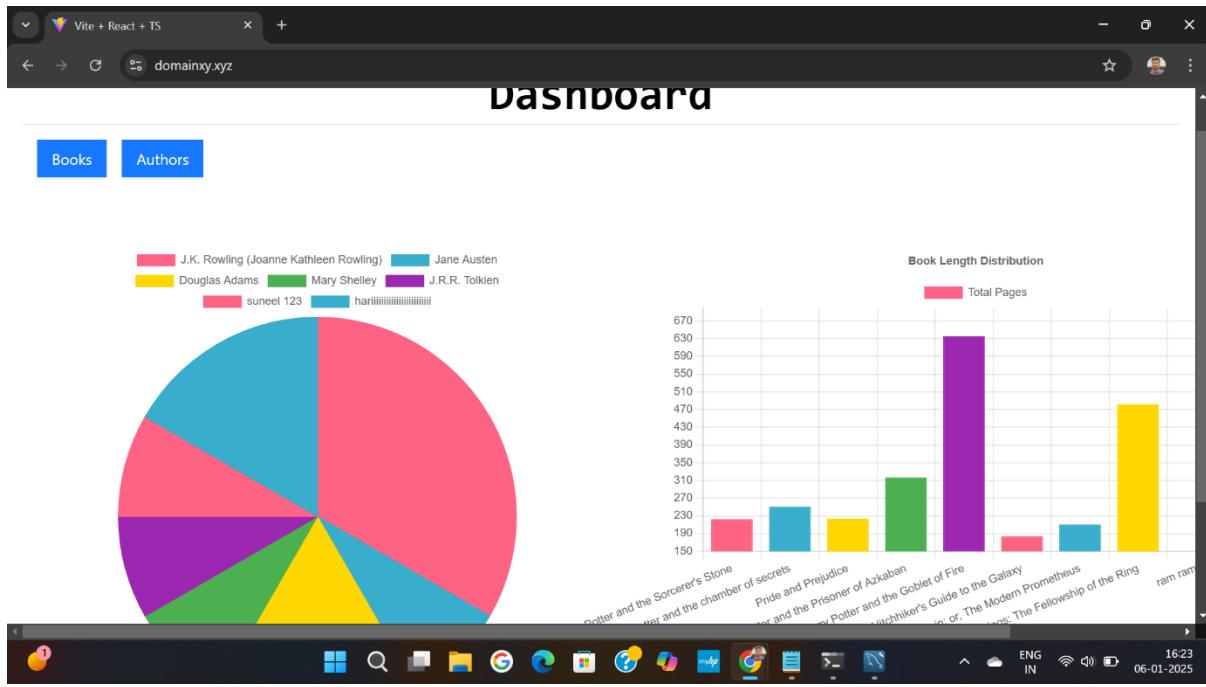
At the bottom are 'CloudShell' and 'Feedback' buttons.

Step 32: Accessing the Application

To access the application delete the instances and wait for the new

instances. After the new instances are created, access the application.

"Hooray we can access the application and to verify it check the cloud watch logs".



Vite + React + TS domainxyz/books

MANAGE BOOKS

[Dashboard](#) [+ Add Book](#)

ID	Title	Description	Release Date	Author	Created Date	Updated Date	Actions
1	Harry Potter and the Sorcerer's Stone	On his birthday, Harry Potter discovers that he is the son of two well-known wizards, from whom he has inherited magical powers. He must attend a famous school of magic and sorcery, where he establishes a friendship with two young men who will become his companions on his adventure. During his first year at Hogwarts, he discovers that a malevolent and powerful wizard named Voldemort is in search of a philosopher's stone that prolongs the life of its owner.	1997-07-26T00:00:00.000Z	J.K. Rowling (Joanne Kathleen Rowling)	2024-05-29T00:00:00.000Z	2024-05-29T00:00:00.000Z	
3	Harry Potter and the chamber of secrets	Harry Potter and the sophomores investigate a malevolent threat to their Hogwarts classmates, a menacing beast that hides within the castle.	1998-07-02T00:00:00.000Z	J.K. Rowling (Joanne Kathleen Rowling)	2024-05-29T00:00:00.000Z	2024-05-29T00:00:00.000Z	
2	Pride and Prejudice	An English novel of manners by Jane Austen, first published in 1813. The story centres on the relationships among the Bennet	1813-01-18T00:00:00.000Z	Jane Austen	2024-05-29T00:00:00.000Z	2024-05-29T00:00:00.000Z	

17:35 07-01-2025

The screenshot shows a table with the following data:

ID	Author	Birthday	Description	Created Date	Updated Date	Actions
1	J.K. Rowling (Joanne Kathleen Rowling)	1965-07-31T00:00:00.000Z	J.K. Rowling is a British author best known for writing the Harry Potter fantasy series. The series has won multiple awards and sold over 500 million copies, becoming the best-selling book series in history. Rowling has also written other novels, including The Casual Vacancy and the Cormoran Strike crime series under the pen name Robert Galbraith.	2024-05-29T00:00:00.000Z	2024-05-29T00:00:00.000Z	
3	Jane Austen	1775-12-16T00:00:00.000Z	Jane Austen was an English novelist known for her wit, social commentary, and romantic stories. Her six major novels, which explore themes of love, marriage, and money, have earned her a place as one of the greatest writers in the English language.	2024-05-29T00:00:00.000Z	2024-05-29T00:00:00.000Z	
4	Harper Lee	1960-07-11T00:00:00.000Z	Harper Lee was an American novelist best known for her Pulitzer Prize-winning novel To Kill a Mockingbird. The novel explores themes of racial injustice and the importance of compassion. Lee published a sequel, Go Set a Watchman, in 2015.	2024-05-29T00:00:00.000Z	2024-05-29T00:00:00.000Z	

Step 33: Cloud Front Distribution

Create a cloud front distribution with name as Presentation-Tier-ALB and select the HTTP and Redirect to HTTP and do not enable the WAF. Now select the regions and add our domain names (in our case domainxy.xy.xyz & www.domainxy.xy.xyz) and attach the certificate that is obtained from AWS certificate manager.

The screenshot shows the CloudFront console with the following details:

- Distributions**: Policies, Functions, Static IPs, VPC origins, What's new.
- Telemetry**: Monitoring, Alarms, Logs.
- Reports & analytics**: Cache statistics, Popular objects, Top referrers, Usage, Viewers.
- General Tab Details**:
 - Distribution domain name**: d100docjbrkjpt.cloudfront.net
 - ARN**: arn:aws:cloudfront::605134464260:distribution/E34N7YBPUCJQVZ
 - Last modified**: January 6, 2025 at 10:27:18 AM UTC
- General Tab Settings**:
 - Description**: -
 - Alternate domain names**: www.domainxy.xy, domainxy.xy
 - Custom SSL certificate**: [domainxy.xy](#)
 - Supported HTTP versions**: HTTP/2, HTTP/1.1, HTTP/1.0
 - Security policy**: TLSv1.2_2021
 - Standard logging**: Off
 - Cookie logging**: Off
 - Default root object**: -

Step 34: DNS Records for Cloud Front in Route 53

In the Route 53 , open the hosted zone that we created and add the record

alias and select the first distribution i.e.domainxy.xyz

Route 53 > Hosted zones > domainxy.xyz > Create record

Create record [Info](#)

Quick create record

Record name [Info](#) www.domainxy.xyz

Record type [Info](#) A – Routes traffic to an IPv4 address and some AWS resources

Route traffic to [Info](#) Alias to CloudFront distribution

US East (N. Virginia)

An alias to a CloudFront distribution and another record in the same hosted zone are global and available only in US East (N. Virginia).

d100docjbrkjpt.cloudfront.net

Routing policy [Info](#) Simple routing

Evaluate target health No

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

Step 35: DNS Records for Cloud Front in Route 53

In the Route 53 , open the hosted zone that we created and add the record

alias and select the second distribution i.e. www.domainxy.xyz

Route 53 > Hosted zones > domainxy.xyz

Records (1/6) [Info](#)

Route 53

Hosted zones

Health checks

Profiles [New](#)

IP-based routing

Traffic flow

Domains

Resolver

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

Alias	Value/Route traffic to	TTL (s...)	Health ...	Evalu...
No	ns-302.awsdns-37.com. ns-1015.awsdns-62.net. ns-2014.awsdns-59.co.uk. ns-1250.awsdns-28.org.	172800	-	-
No	ns-302.awsdns-37.com. awsd...	900	-	-
No	_fce16f506ca07955a6935b...	300	-	-
No	_93d1ce9dc91f1447ae0717...	300	-	-
Yes	d100docjbrkjpt.cloudfront.net.	-	-	No
Yes	d100docjbrkjpt.cloudfront.net.	-	-	No

Record name domainxy.xyz

Record type NS – Name servers for a hosted zone

Alias

Value [Info](#)

ns-302.awsdns-37.com.
ns-1015.awsdns-62.net.
ns-2014.awsdns-59.co.uk.
ns-1250.awsdns-28.org.

TTL (seconds) [Info](#) 900 1m 1h 1d

Routing policy [Info](#) Simple routing

Cancel Save

"AFTER THAT WE CAN SUCCESSFULLY ACCESS

THE APPLICATION AND BASED ON OUR

REQUIREMENT WE CAN ADD OR DELETE THE
AUTHORS AND BOOKS."