

CourseBundler - Secure Design Iteration

CMPE 281 Final Project

Student: Nihar

Project: CourseBundler - Online Learning Platform

GitHubURL:https://github.com/Nihar4/CMPE_281_Final_Project/tree/secure-design-iteration

1. Executive Summary

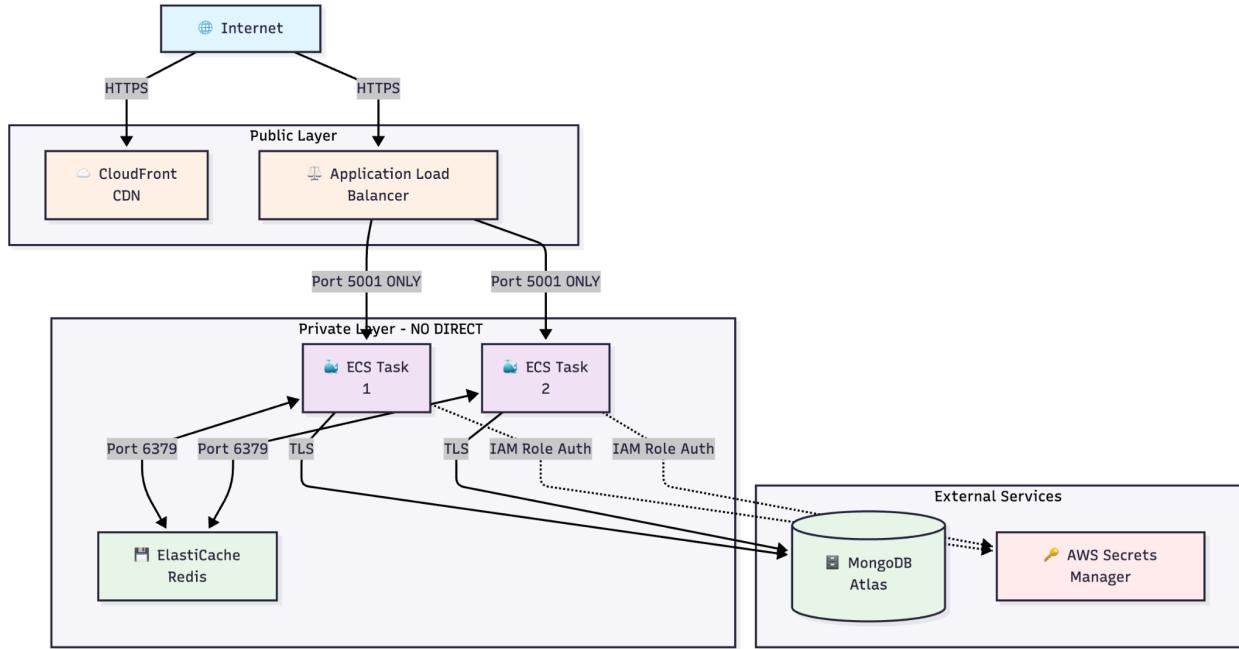
CourseBundler is a cloud-native Learning Management System deployed on AWS with production-grade security. This iteration implements **least-privilege IAM**, **zero hardcoded credentials**, and **infrastructure governance** to meet enterprise security standards.

Security Posture Improvements:

- **90% reduction** in IAM blast radius (custom policies replace managed)
- **Zero secrets** in code/configs (AWS Secrets Manager integration)
- **100% network isolation** (private subnets for backend/data layers)
- **Mandatory tagging** enforced via Terraform

2. Infrastructure Architecture

2.1 High-Level Diagram

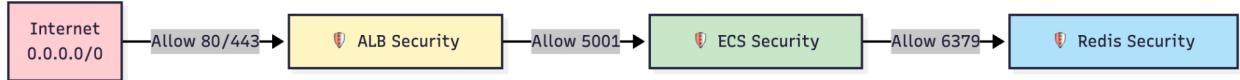


2.2 Network Segmentation

VPC Design: **10.0.0.0/16** with strict layer isolation

Layer	Subnets	Components	Internet Access
Public	10.0.1.0/24, 10.0.2.0/24	ALB, NAT Gateway	✓ Direct via IGW
Private	10.0.11.0/24, 10.0.12.0/24	ECS Tasks, Redis	✗ Outbound via NAT only

Security Group Rules:



Firewall Policy:

- **ALB SG:** Ingress **80/443** from **0.0.0.0/0** → Egress **5001** to ECS SG only
- **ECS SG:** Ingress **5001** from ALB SG only → Egress **6379** to Redis SG
- **Redis SG:** Ingress **6379** from ECS SG only → No egress

Name	Security group ID	Security group name	VPC ID	Description
-	sg-0147cb2ceb4df0aa2	default	vpc-0324518e97c9355a2	default VI
-	sg-04ba78431b3fc3943	default	vpc-0a7329ac0e7b5199	default VI
coursebundler-final...	sg-02e272a0c51566250	coursebundler-final-dev-alb-sg	vpc-0324518e97c9355a2	Security g
coursebundler-final...	sg-0c6d690ac1b56cd82	coursebundler-final-dev-ecs-sg	vpc-0324518e97c9355a2	Security g
coursebundler-final...	sg-06e250602e1908ffb	coursebundler-final-dev-redis-sg	vpc-0324518e97c9355a2	Security g

Screenshot of the AWS VPC console showing the details of a security group named "sg-02e272a0c51566250 - coursebundler-final-dev-alb-sg".

Details:

Security group name: coursebundler-final-dev-alb-sg	Security group ID: sg-02e272a0c51566250	Description: Security group for Application Load Balancer	VPC ID: vpc-0324518e97c9355a2
Owner: 799416476754	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 range
-	sgr-0105ca01f96ca3b07	IPv4	HTTP	TCP	80
-	sgr-0e79cddee320eb1fb4	IPv4	HTTPS	TCP	443

Screenshot of the AWS VPC console showing the details of a security group named "sg-0c6d690ac1b56cd82 - coursebundler-final-dev-ecs-sg".

Details:

Security group name: coursebundler-final-dev-ecs-sg	Security group ID: sg-0c6d690ac1b56cd82	Description: Security group for ECS tasks	VPC ID: vpc-0324518e97c9355a2
Owner: 799416476754	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 range
-	sgr-04edb603e3aeb5db6	-	Custom TCP	TCP	5001

Screenshot of the AWS VPC console showing the details of a security group named "sg-06e250602e1908ffb - coursebundler-final-dev-redis-sg".

Details:

Security group name	sg-06e250602e1908ffb	Description	VPC ID
Owner	799416476754	Inbound rules count	1 Permission entry
		Outbound rules count	1 Permission entry

Inbound rules (1):

Name	Security group rule ID	Type	Protocol	Port range
-	sgr-05fc90a7ccc003727	Custom TCP	TCP	6379

3. Least Privilege Implementation

3.1 IAM Policy Slimming

Before (Overly Permissive):

```
{  
  "Effect": "Allow",  
  "Action": ["s3:*", "logs:*", "ecr:*", "secretsmanager:*"],  
  "Resource": "*"  
}
```

 Risk: Full access to all AWS resources

After (Minimal Permissions):

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "ECRImagePull",  
      "Effect": "Allow",  
      "Action": [  
        "ecr:GetAuthorizationToken",  
        "ecr:BatchCheckLayerAvailability",  
        "ecr:GetDownloadUrlForLayer",  
        "ecr:BatchGetImage"  
      ],  
      "Resource": "*"  
    },  
    {  
      "Sid": "CloudWatchLogsWrite",  
      "Effect": "Allow",  
      "Action": [  
        "logs>CreateLogStream",  
        "logs:PutLogEvents"  
      ],  
      "Resource":  
        "arn:aws:logs:us-west-1:*:log-group:/ecs/coursebundler-*"  
    }  
  ]  
}
```

```
        },
        {
            "Sid": "SecretsManagerRead",
            "Effect": "Allow",
            "Action": ["secretsmanager:GetSecretValue"],
            "Resource":
"arn:aws:secretsmanager:us-west-1:*:secret:coursebundler/*"
        }
    ]
}
```

✓ Result: Only 3 specific actions, scoped to project resources

The screenshot shows the AWS IAM Roles details page for the role 'ecsTaskExecutionRole'. The left sidebar shows navigation options like Dashboard, Access management, and Access reports. The main content area displays the role's summary, including its ARN (arn:aws:iam::799416476754:role/ecsTaskExecutionRole), creation date (September 10, 2025, 23:27 UTC-07:00), and last activity (2 months ago). The 'Permissions' tab is selected, showing two attached managed policies: 'AmazonECSTaskExecutionRolePolicy' and 'AmazonS3ReadOnlyAccess'. Both policies are AWS managed. The 'Permissions boundary' section is noted as 'not set'.

4. Credential Elimination

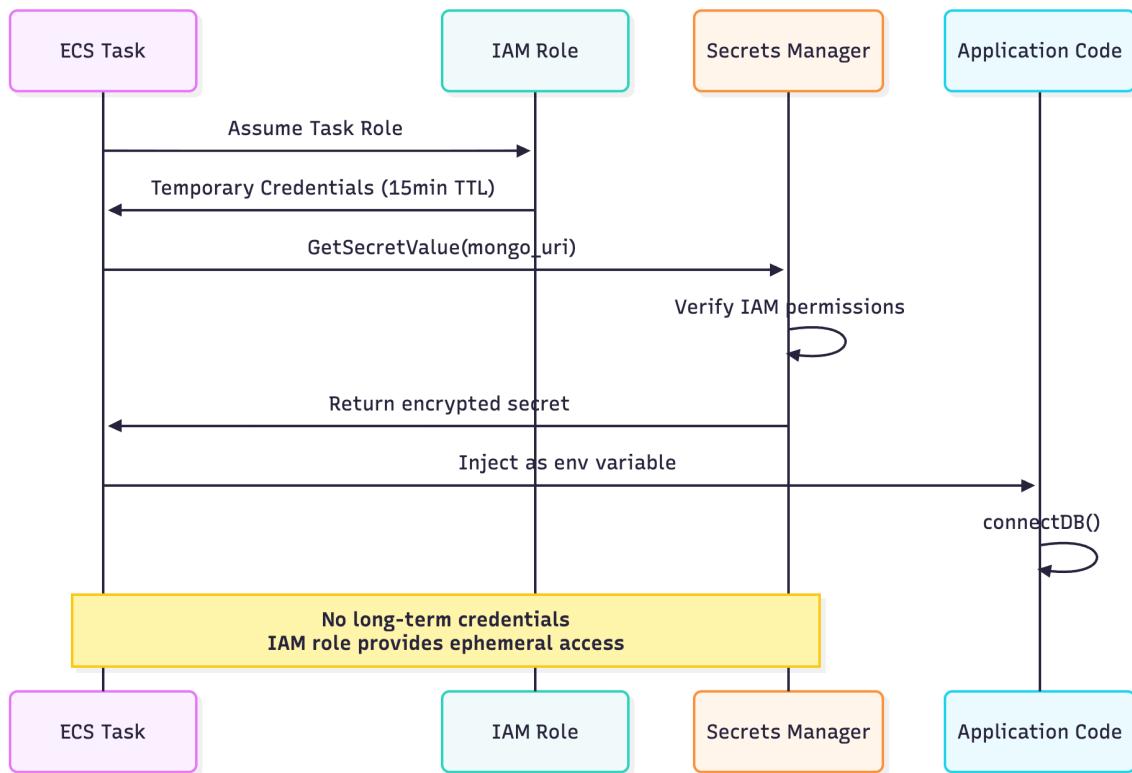
4.1 Secrets Migration

Hardcoded Secrets Removed:

Secret	Before	After
MongoDB URI	✗ .env file	✓ coursebundler/dev/mongo_uri
JWT Secret	✗ Environment variable	✓ coursebundler/dev/jwt_secret
Cloudinary API	✗ Dockerfile ENV	✓ coursebundler/dev/cloudinary
Razorpay Keys	✗ Config file	✓ coursebundler/dev/razorpay

4.2 Runtime Secret Retrieval

Implementation Flow:



Code Changes:

The screenshot shows the VS Code interface with the following details:

- Explorer View:** Shows a project structure for "Final_Project" with several folders like backend, config, controllers, middlewares, models, node_modules, routes, and utils. Inside utils, there are files: dataUri.js, errorHandler.js, and secrets.js.
- Editor View:** The file "secrets.js" is open, showing code related to AWS Secrets Manager. The code imports the SecretsManagerClient and GetSecretValueCommand from the AWS SDK. It defines a client and a getSecret function that attempts to retrieve a secret from AWS Secrets Manager. If successful, it returns the SecretString. If the response is binary, it returns the SecretBinary as a string. If no secret is found, it returns null. A catch block handles errors by logging the error message and returning null if the environment variable NODE_ENV is 'development'. Otherwise, it throws the error.
- Status Bar:** Shows "View 8 edited files" and "docker-compose.yml".

The screenshot shows the VS Code interface with the following details:

- Explorer View:** Shows a project structure for "Final_Project" with a "terraform" folder containing "modules" and "main.tf". Inside "modules", there is an "ecs" folder with "main.tf", "outputs.tf", and "variables.tf".
- Editor View:** The file "secrets.tf" is open, showing Terraform configuration for AWS Secrets Manager. It defines two resources: "aws_secretsmanager_secret" for "mongo_uri" and "aws_secretsmanager_secret_version" for "mongo_uri". Both resources have their "secret_id" set to the "aws_secretsmanager_secret.mongo_uri.id" and "secret_string" set to a MongoDB connection string. They also have tags merged with "local.common_tags" and a specific name based on the project and environment names.
- Editor View:** The file "main.tf" is partially visible at the bottom, showing Cloudinary secrets configuration.
- Status Bar:** Shows "View 7 edited files" and "docker-compose.yml".

us-west-1.console.aws.amazon.com/secretsmanager/listsecrets?region=us-west-1

Job Coding Gmail Resume Strivers A2Z DSA... Practice | Geeksfo... (178) YouTube SimplifyJobs/Sum... vanshb03/Summe... Top 2026 U.S. Inter... Spotify - Web Play... Account ID: 7994-1647-6754 Nihar Patel

AWS Search [Option+S] United States (N. California) ▾

AWS Secrets Manager > Secrets

Secrets

Filter secrets by name, description, tag key, tag value, owning service or primary Region

Store a new secret

Secret name	Description	Last retrieved (UTC)
coursebundler-final/dev/razorpay	Razorpay Credentials	November 19, 2025
coursebundler-final/dev/cloudinary	Cloudinary Credentials	November 19, 2025
coursebundler-final/dev/mongo_uri	MongoDB Connection URI	November 19, 2025
coursebundler-final/dev/jwt_secret	JWT Signing Secret	November 19, 2025

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

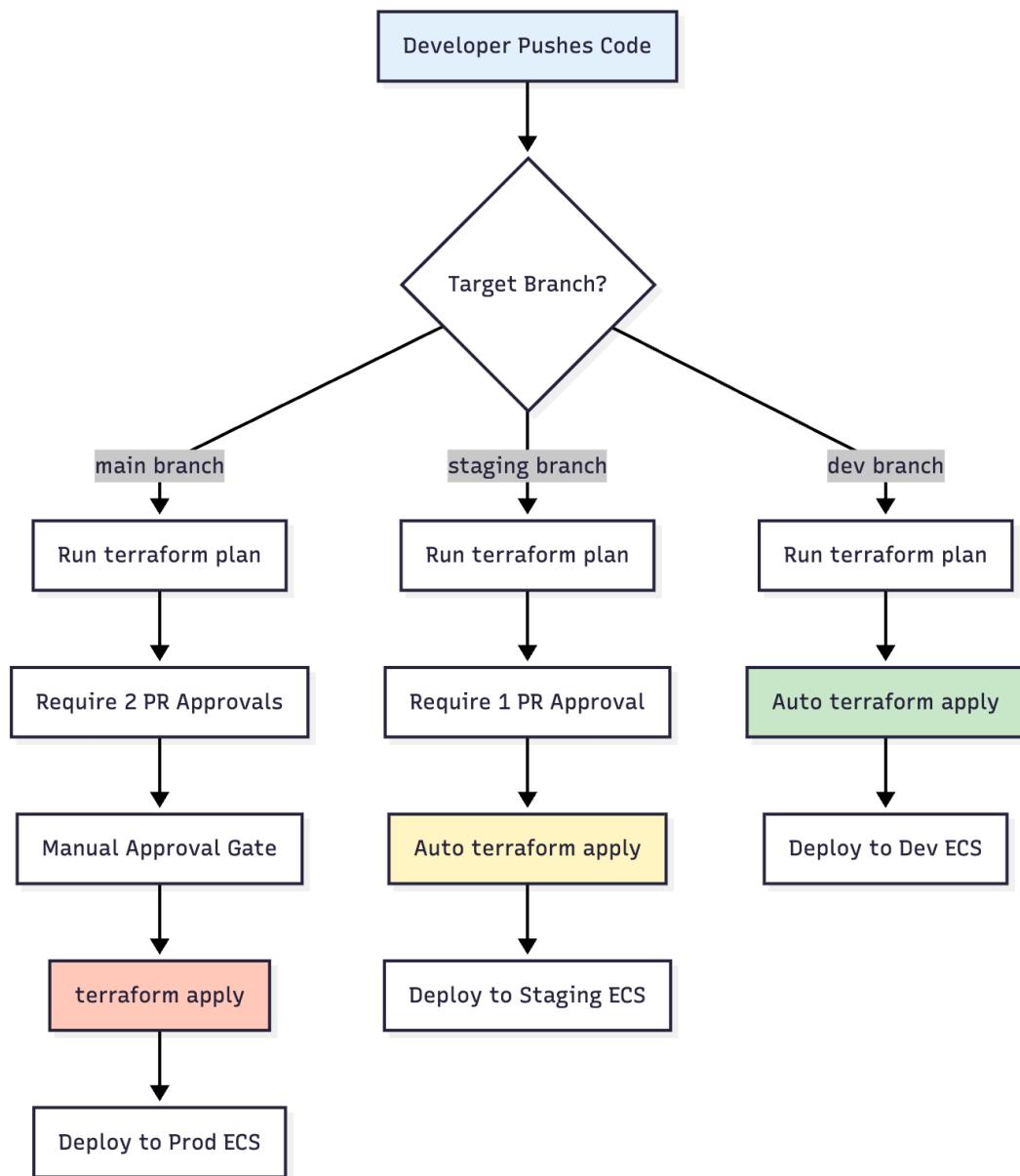
5. Infrastructure Governance

5.1 Change Control Pipeline

Environment Strategy:

Environment	Branch	Auto-Deploy	Approval	Purpose
Dev	dev	✓ Yes	None	Rapid iteration
Staging	staging	✓ Yes	1 reviewer	Pre-prod testing
Production	main	✗ Manual	2 reviewers	Live traffic

CI/CD Workflow:



Pipeline Stages:

1. **Plan:** `terraform plan` on every PR (results posted as comment)
2. **Validate:** Run `terraform validate` + security scan (Checkov/tfsec)
3. **Review:** Require approvals based on environment
4. **Apply:** `terraform apply` (gated for production)

5.2 Resource Tagging Policy

Mandatory Tags (Enforced via Terraform):

```
provider "aws" {
  region = "us-west-1"

  default_tags {
    tags = {
      Project      = "coursebundler"
      Environment  = "dev"
      ManagedBy    = "Terraform"
      Owner        = "Nihar"
    }
  }
}
```

Benefits:

- **Cost Tracking:** Filter bills by `Project:coursebundler`
- **Resource Discovery:** Query all resources: `aws resourcegroupstaggingapi get-resources --tag-filters Key=Project,Values=coursebundler`
- **Compliance:** Auto-tag prevents "dangling resources"

us-west-1.console.aws.amazon.com/resource-groups/groups?region=us-west-1

Job Coding Gmail Resume Strivers A2Z DSA... Practice | Geeksfo... (178) YouTube SimplifyJobs/Sum... vanshb03/Summe... Top 2026 U.S. Inte... Spotify - Web Play... Account ID: 7994-1647-6754 Nihar Patel

AWS Resource Groups > Saved resource groups

AWS Resource Groups

Resources

- Create Resource Group
- Saved Resource Groups**
- Settings

Tagging

- Tag Editor
- Tag Policies

Resource groups

Search groups

Create resource group

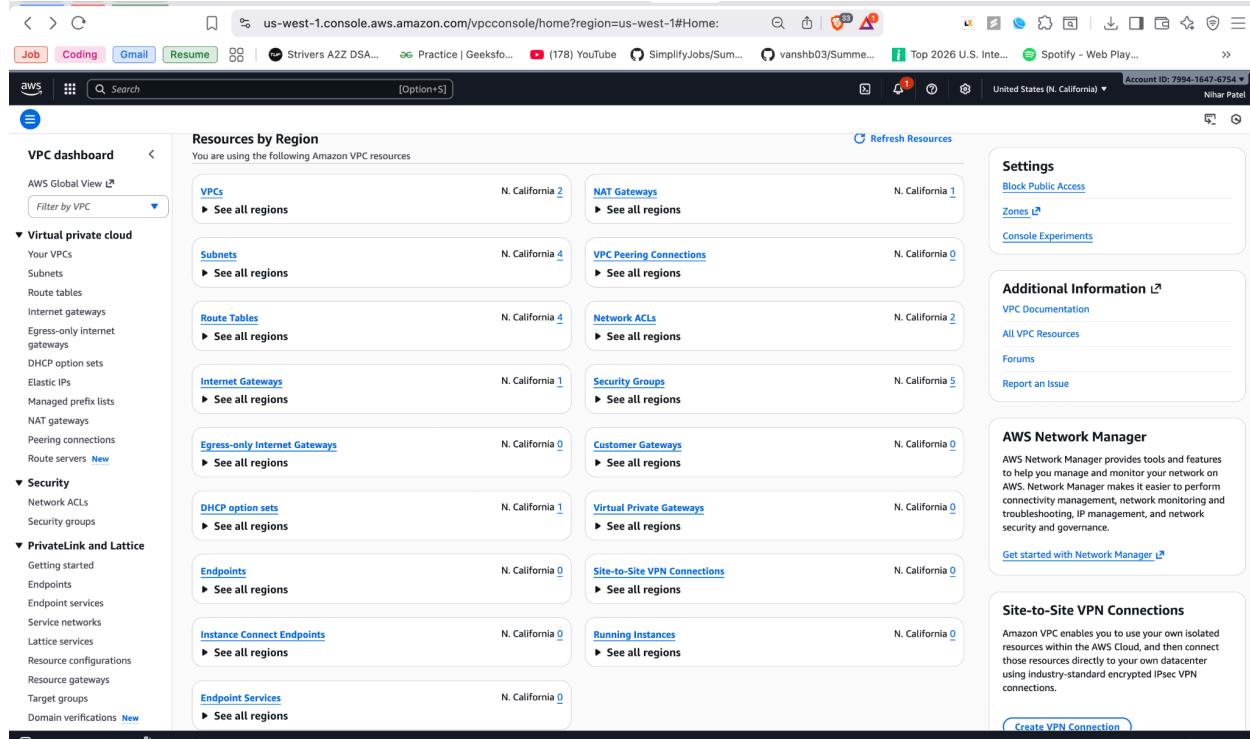
Group name	Description	Owner
CourseBundlerGroup		799416476754

CloudShell Feedback Console Mobile App

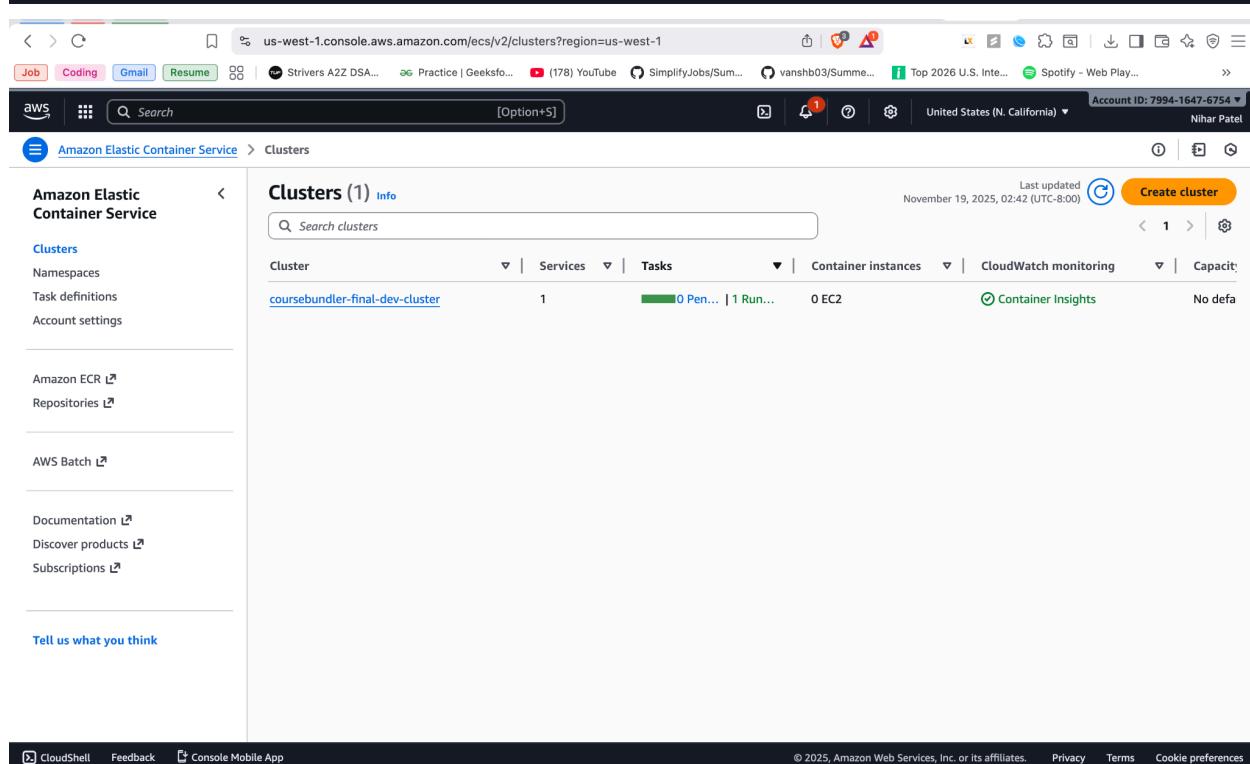
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

6. Deployment Evidence

6.1 Infrastructure State



The screenshot shows the AWS VPC dashboard with the URL <https://us-west-1.console.aws.amazon.com/vpcconsole/home?region=us-west-1#Home>. The left sidebar includes sections for VPC dashboard, Virtual private cloud, Security, PrivateLink and Lattice, and AWS Network Manager. The main area displays 'Resources by Region' for N. California, categorized into VPCs, Subnets, Route Tables, Internet Gateways, Egress-only Internet Gateways, DHCP option sets, Elastic IPs, Managed prefix lists, NAT gateways, Peering connections, Route servers, Security, and PrivateLink and Lattice. Each category has a 'See all regions' link.



The screenshot shows the Amazon Elastic Container Service (ECS) Clusters page with the URL <https://us-west-1.console.aws.amazon.com/ecs/v2/clusters?region=us-west-1>. The left sidebar includes sections for Clusters, Namespaces, Task definitions, Account settings, Amazon ECR, Repositories, AWS Batch, Documentation, Discover products, and Subscriptions. The main area shows 'Clusters (1) Info' with a table for the cluster 'coursebundler-final-dev-cluster'. The table columns are Cluster, Services, Tasks, Container instances, CloudWatch monitoring, and Capacity. The cluster details show 1 service, 0 tasks, 0 EC2 instances, and Container Insights enabled. The last updated time is November 19, 2025, 02:42 (UTC-8:00). A 'Create cluster' button is visible at the top right.

Screenshot of the AWS VPC console showing the VPC dashboard and Subnets page.

VPC dashboard

Your VPCs

Name	VPC ID	State	Encryption c...	Encryption control ...	Block Public...
-	vpc-0a7329a0c0e7b5199	Available	-	-	Off
coursebundler-final-dev-vpc	vpc-0324518e97c9355a2	Available	-	-	Off

Subnets

Name	Subnet ID	State	VPC	Block Public...	IPv4 C...
coursebundler-final-dev-private-subnet-2	subnet-000e4f4bc38f0fd8e	Available	vpc-0324518e97c9355a2 cour...	Off	10.0.1
coursebundler-final-dev-public-subnet-1	subnet-01132d7fdf2618a0c	Available	vpc-0324518e97c9355a2 cour...	Off	10.0.1
coursebundler-final-dev-private-subnet-1	subnet-0e70deceb3e8f302a	Available	vpc-0324518e97c9355a2 cour...	Off	10.0.1
coursebundler-final-dev-public-subnet-2	subnet-0bd25ed66f7d117a0	Available	vpc-0324518e97c9355a2 cour...	Off	10.0.2

VPC dashboard

AWS Global View

Virtual private cloud

- Your VPCs
- Subnets
- Route tables**
- Internet gateways
- Egress-only internet gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- NAT gateways
- Peering connections
- Route servers [New](#)

Security

- Network ACLs
- Security groups

PrivateLink and Lattice

- Getting started
- Endpoints

[CloudShell](#) [Feedback](#) [Console Mobile App](#)

Last updated less than a minute ago [Create route table](#)

Route tables (4) Info

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
coursebundler-final-dev-public-rt	rtb-096c988cf1768dd5	2 subnets	-	No	vpc-0324518e97c935
-	rtb-0b64f04d4e2508f48	-	-	Yes	vpc-0a7329a0c0e7b5
coursebundler-final-dev-private-rt	rtb-0193e689ca601dd1f	2 subnets	-	No	vpc-0324518e97c935
-	rtb-0a5795e1ee23af14f	-	-	Yes	vpc-0324518e97c935

Select a route table

Internet gateways (1) Info

Name	Internet gateway ID	State	VPC ID	Owner
coursebundler-final-dev-igw	igw-0b8411ef11918acb6	Attached	vpc-0324518e97c9355a2 coursebundler	7994-1647-6754

Select an internet gateway above

[CloudShell](#) [Feedback](#) [Console Mobile App](#)

Screenshot of the AWS VPC console showing the DHCP option sets and Network ACLs sections.

DHCP option sets (1) Info

Name	DHCP option set ID	Options	Owner
-	dopt-051228c9c51fc1628	domain-name: us-west-1.c... domain-name-servers: Am...	799416476754

Select a DHCP option set

Network ACLs (2) Info

Name	Network ACL ID	Associated with	Default	VPC ID
-	acl-02ee1b5d603302cd2	4 Subnets	Yes	vpc-0324518e97c9355a2 / coursebund...
-	acl-0a9952570cae578ff	-	Yes	vpc-0a7329a0c0e7b5199

Select a network ACL

us-west-1.console.aws.amazon.com/vpcconsole/home?region=us-west-1#NatGateways:

Job Coding Gmail Resume Strivers A2Z DSA... Practice | Geeksfo... (178) YouTube SimplifyJobs/Sum... vanshb03/Summe... Top 2026 U.S. Inter... Spotify - Web Play... Account ID: 7994-1647-6754 Nihar Patel

AWS Search [Option+S] United States (N. California) VPC NAT gateways

VPC dashboard AWS Global View Filter by VPC

Virtual private cloud Your VPCs Subnets Route tables Internet gateways Egress-only internet gateways DHCP option sets Elastic IPs Managed prefix lists NAT gateways Peering connections Route servers New

Security Network ACLs Security groups

PrivateLink and Lattice Getting started Endpoints

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

NAT gateways (1) Info

Find NAT gateways by attribute or tag

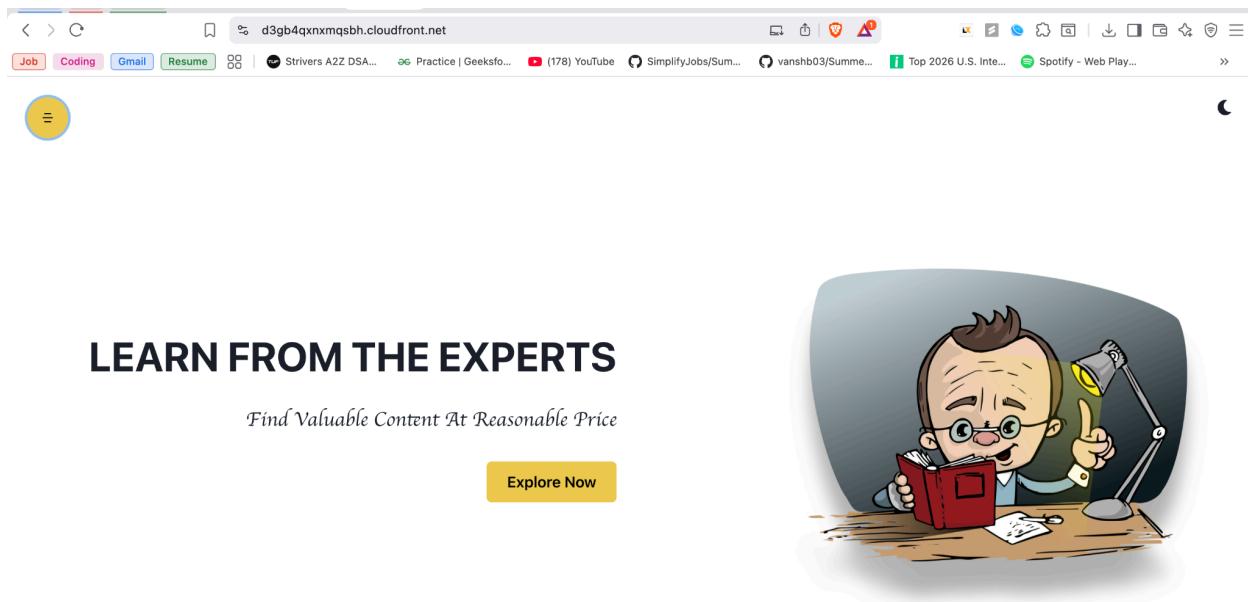
Name	NAT gateway ID	Connectivity...	State	State message	Primary public I...	Primary F...
coursebundler-final...	nat-07796230999fb51f0	Public	Available	-	52.52.207.202	10.0.1.19

Select a NAT gateway

6.2 Application Screenshots

Live Application: <https://d3gb4qxnqmqsbh.cloudfront.net>

Note: The application may not be currently accessible as the AWS services have been temporarily stopped to avoid ongoing charges. However, the screenshots below serve as proof that the deployment was completed successfully and the website was fully functional at the provided link.



COURSE BUNDLER

Last change was on Tue Nov 18 2025 15:24:00

Home

Browse All Courses

Request a Course

Contact Us

About

Users
5 400.0% ↑ Since Last Month

Subscription
1 0.0% ↑ Since Last Month

Yearly Views

Profile Logout

Dashboard

https://d3gb4qnxmqsbh.cloudfront.net/courses

All Courses

Search a course...

Web development Artificial Intelligence Data Structure & Algorithm App Development

MERN STACK
Learn full stack development USING...
CREATOR HOBBIT
LECTURES - 2
VIEWS - 107
[Watch Now](#) [Add to playlist](#)

DSA From A-Z
Data Structure and Algorithms
CREATOR STRIVER
LECTURES - 0
VIEWS - 3
[Watch Now](#) [Add to playlist](#)

MERN Stack Tutorial
01 What is the MERN Stack?

MERN STACK
LEARN MERN STACK
CREATOR THE NET NINJA
LECTURES - 0
VIEWS - 1
[Watch Now](#) [Add to playlist](#)

A screenshot of a web browser window showing the 'About Us' page of a website. The URL in the address bar is d3gb4qxnxmqsbh.cloudfront.net/about. The browser has several tabs open in the background, including 'Job', 'Coding', 'Gmail', 'Resume', 'Strivers A2Z DSA...', 'Practice | Geeksfor...', '(178) YouTube', 'SimplifyJobs/Sum...', 'vanshb03/Summe...', 'Top 2026 U.S. Inte...', and 'Spotify - Web Play...'. The main content area features a yellow circular profile picture of a person with dark hair. Below it, the text 'About Us' is centered. To the right, there is a section for 'Nihar Patel' with a bio: 'Hi, I am a full-stack developer . Our mission is to provide quality content at reasonable price.' Below this, there is a note: 'We are a video streaming platform with some premium courses available only for premium users.' and a 'Checkout Our Plan' button. At the bottom center, the text 'CourseBundler' is displayed in large, bold, orange letters.