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

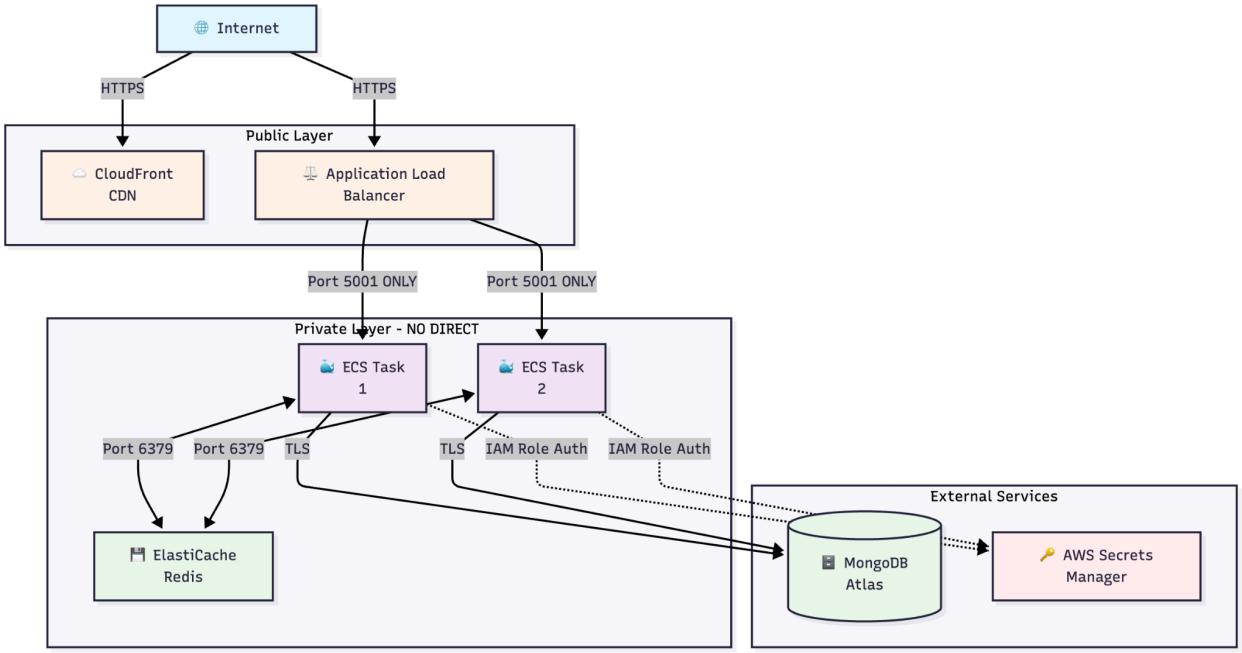
CourseBundler is a cloud-native Learning Management System deployed on AWS with production-grade security. This iteration implements **least-privilege IAM**, **zero hardcoded credentials**, and **infrastructure governance** to meet enterprise security standards.

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

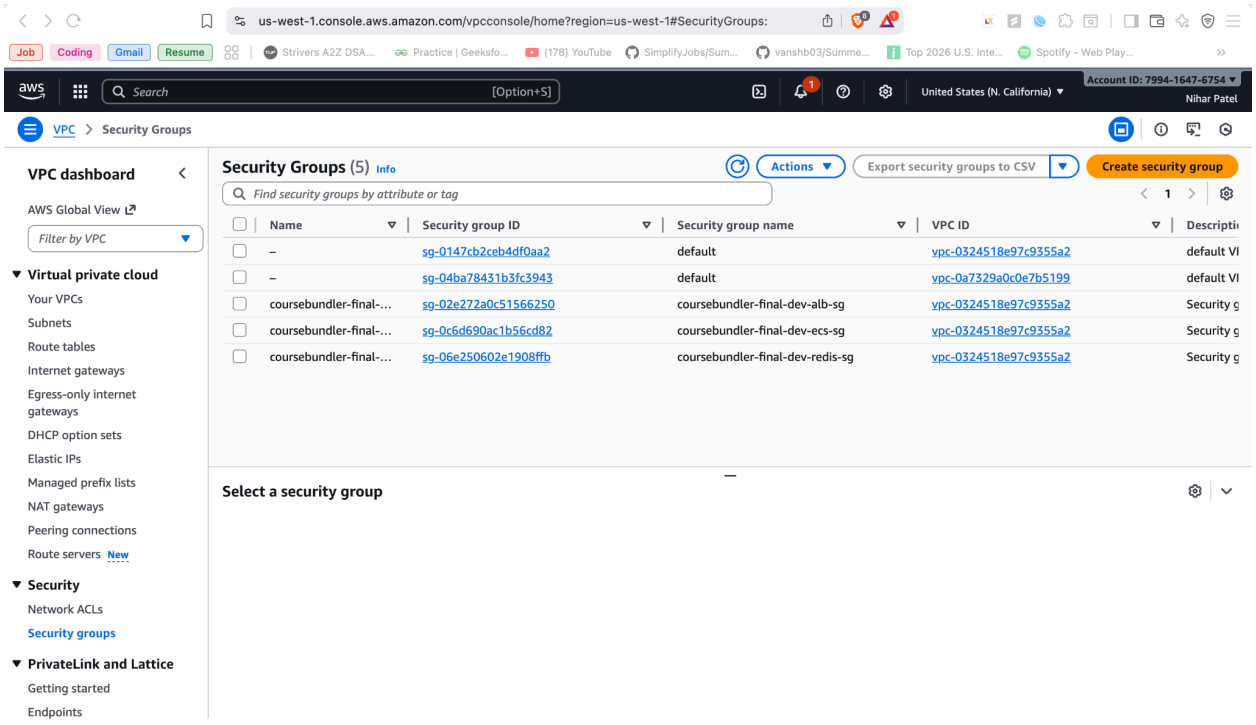
VPC Design: `10.0.0.0/16` with strict layer isolation

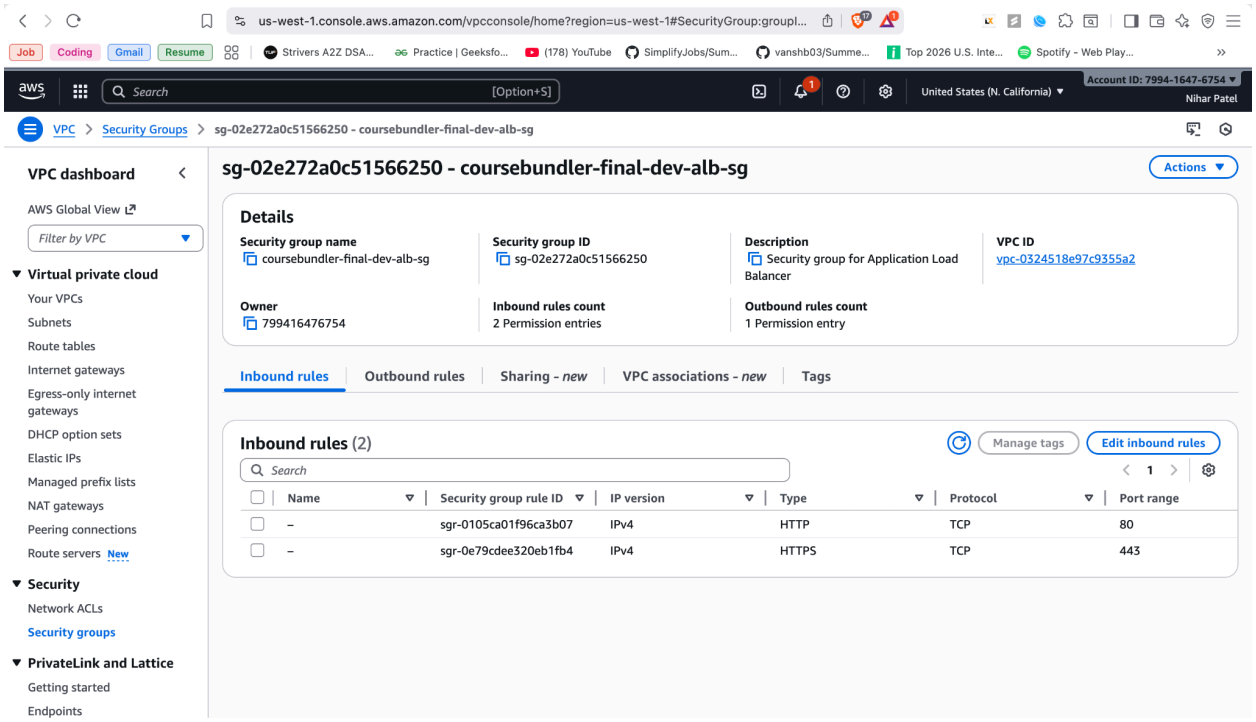
Layer	Subnets	Components	Internet Access
Public	`10.0.1.0/24`, `10.0.2.0/24`	ALB, NAT Gateway	✅ Direct via IGW
Private	`10.0.11.0/24`, `10.0.12.0/24`	ECS Tasks, Redis	❌ Outbound via NAT only

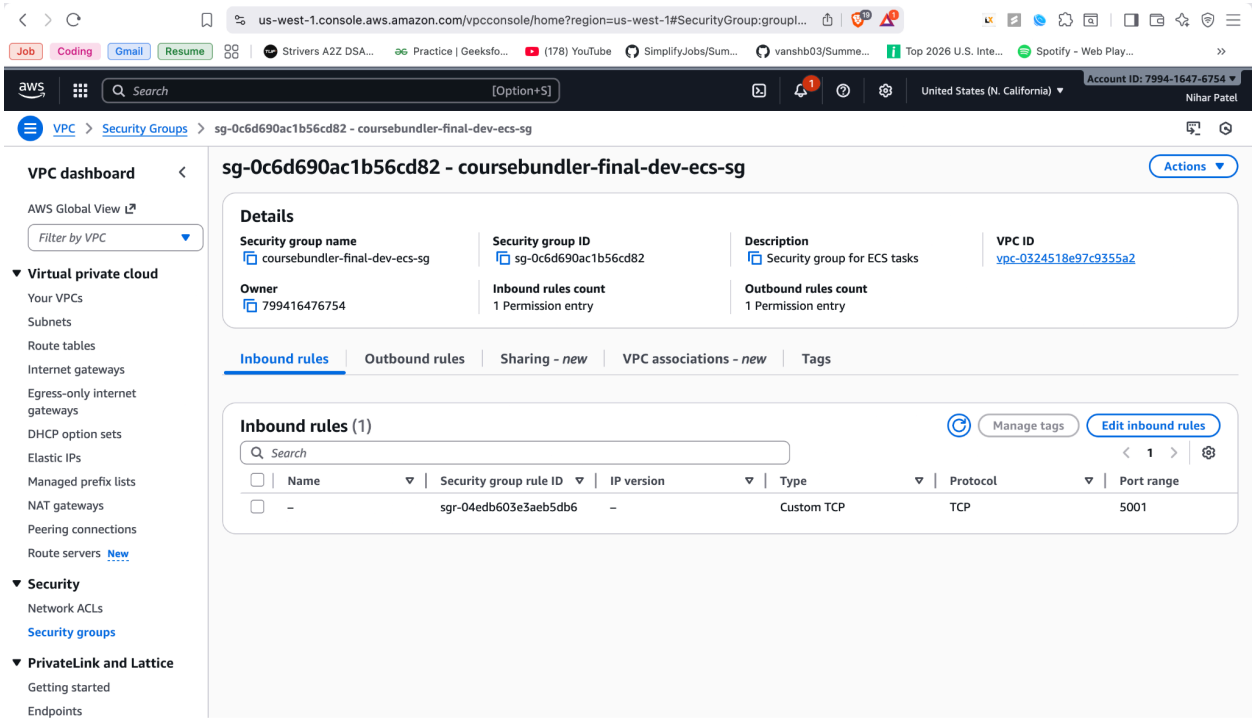
Security Group Rules:

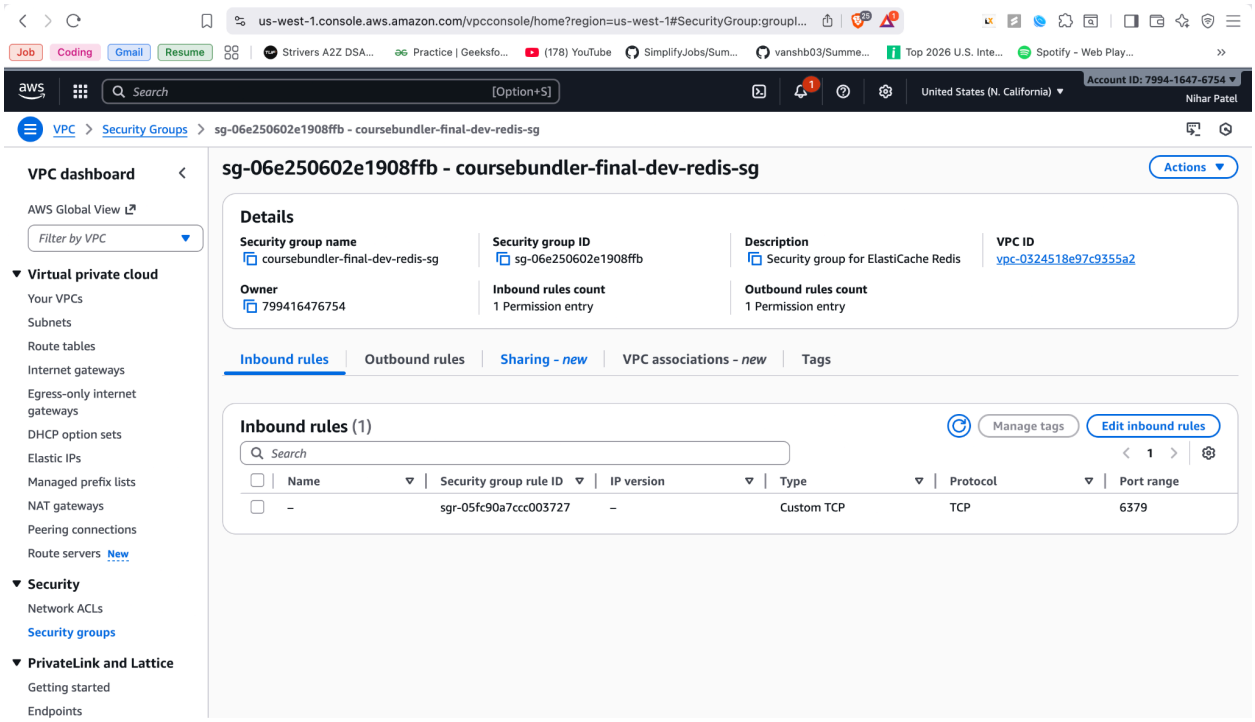
Firewall Policy:

- **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




us-west-1.console.aws.amazon.com/vpcconsole/home?region=us-west-1#SecurityGroup:groupI...
Search
[Option+S]
United States (N. California)
Account ID: 7994-1647-6754
Nihar Patel
VPC > Security Groups > sg-02e272a0c51566250 - coursebundler-final-dev-alb-sg
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
sg-02e272a0c51566250 - coursebundler-final-dev-alb-sg
Actions
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
Outbound rules
Sharing - new
VPC associations - new
Tags
Inbound rules (2)
Manage tags
Edit inbound rules
Search
Name
Security group rule ID
IP version
Type
Protocol
Port range
– sgr-0105ca01f96ca3b07 IPv4 HTTP TCP 80
– sgr-0e79cdee320eb1fb4 IPv4 HTTPS TCP 443


us-west-1.console.aws.amazon.com/vpcconsole/home?region=us-west-1#SecurityGroup:groupI...
Search
[Option+S]
United States (N. California)
Account ID: 7994-1647-6754
Nihar Patel
VPC > Security Groups > sg-0c6d690ac1b56cd82 - coursebundler-final-dev-ecs-sg
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
sg-0c6d690ac1b56cd82 - coursebundler-final-dev-ecs-sg
Actions
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
Outbound rules
Sharing - new
VPC associations - new
Tags
Inbound rules (1)
Manage tags
Edit inbound rules
Search
Name
Security group rule ID
IP version
Type
Protocol
Port range
– sgr-04edb603e3aeb5db6 – Custom TCP TCP 5001


us-west-1.console.aws.amazon.com/vpcconsole/home?region=us-west-1#SecurityGroup:groupI...
Job
Coding
Gmail
Resume
Strivers A2Z DSA...
Practice | Geeksfo...
(178) YouTube
SimplifyJobs/Sum...
vanshb03/Summe...
Top 2026 U.S. Inte...
Spotify - Web Play...
aws
Search
[Option+S]
United States (N. California)
Account ID: 7994-1647-6754
Nihar Patel
VPC
Security Groups
sg-06e250602e1908ffb - coursebundler-final-dev-redis-sg
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
sg-06e250602e1908ffb - coursebundler-final-dev-redis-sg
Actions
Details
Security group name
coursebundler-final-dev-redis-sg
Security group ID
sg-06e250602e1908ffb
Description
Security group for ElastiCache Redis
VPC ID
vpc-0324518e97c9355a2
Owner
799416476754
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)
Manage tags
Edit inbound rules
Search
1
Name
Security group rule ID
IP version
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": "*"
}
```

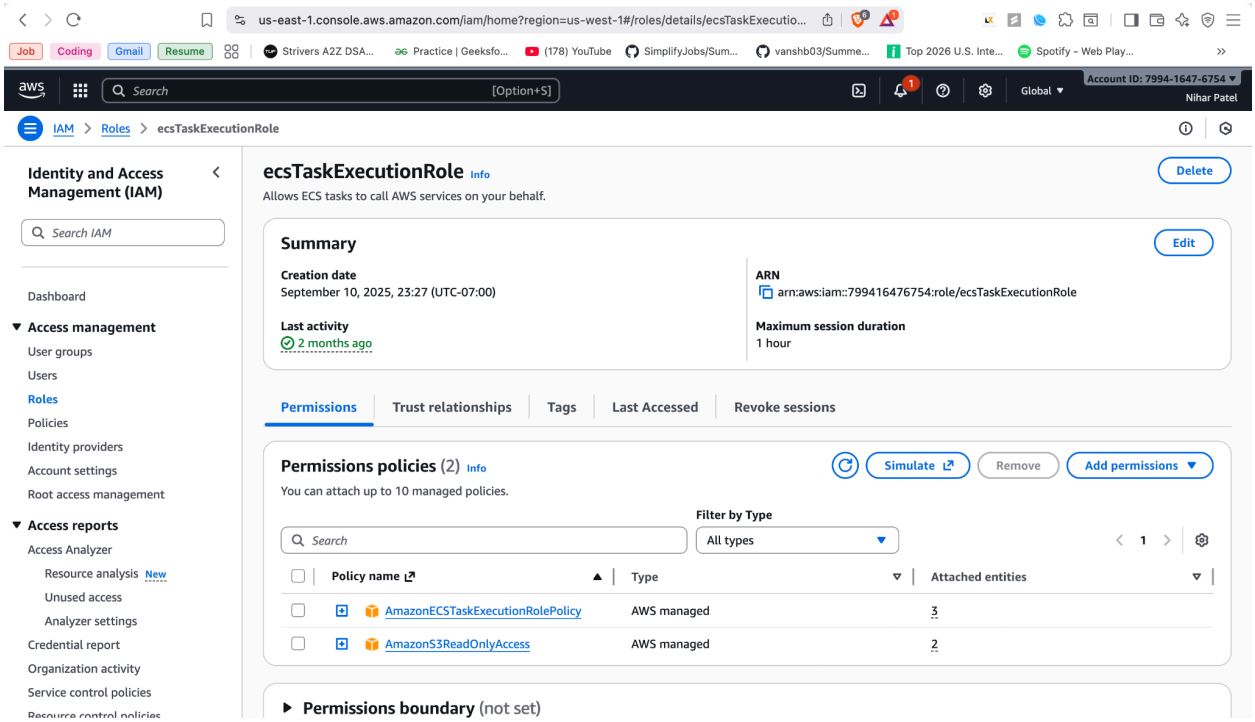
❌ **Risk:** Full access to all AWS resources

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



4. Credential Elimination

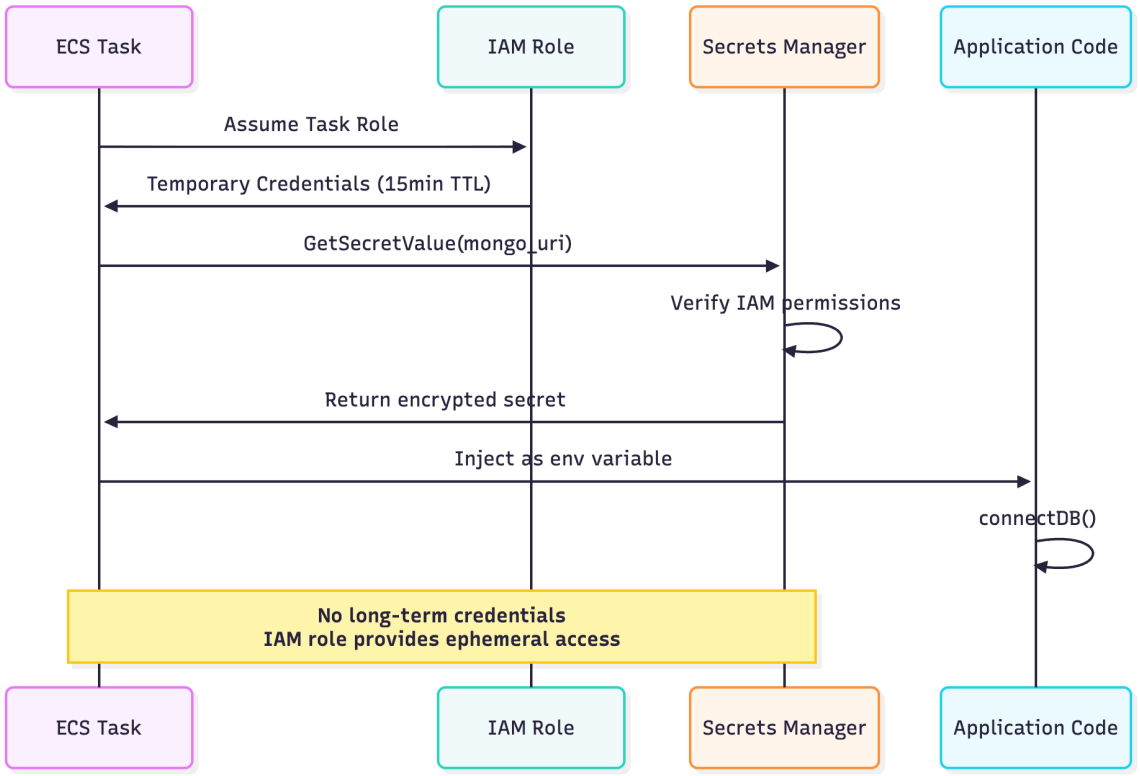
4.1 Secrets Migration

Hardcoded Secrets Removed:

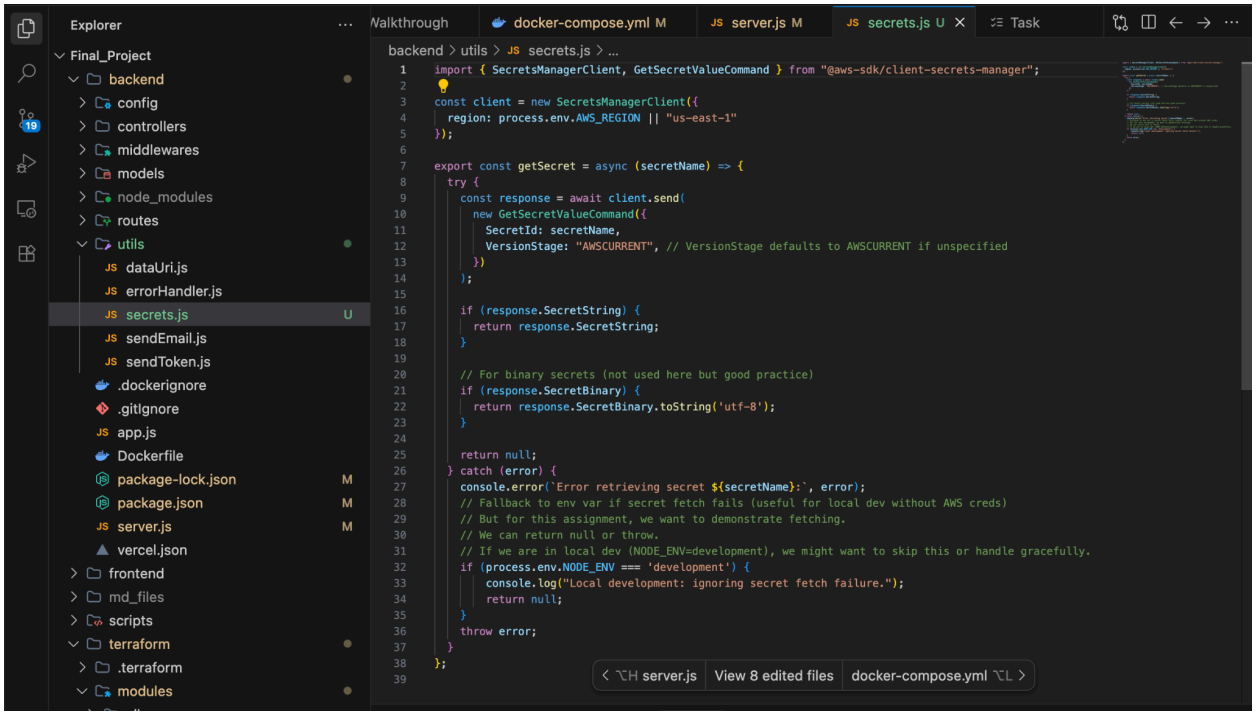
Secret	Before	After
MongoDB URI	❌ `.env` file	✅ `coursebundler/dev/mongo_uri`
JWT Secret	❌ Environment variable	✅ `coursebundler/dev/jwt_secret`
Cloudinary API	❌ Dockerfile ENV	✅ `coursebundler/dev/cloudinary`
Razorpay Keys	❌ Config file	✅ `coursebundler/dev/razorpay`

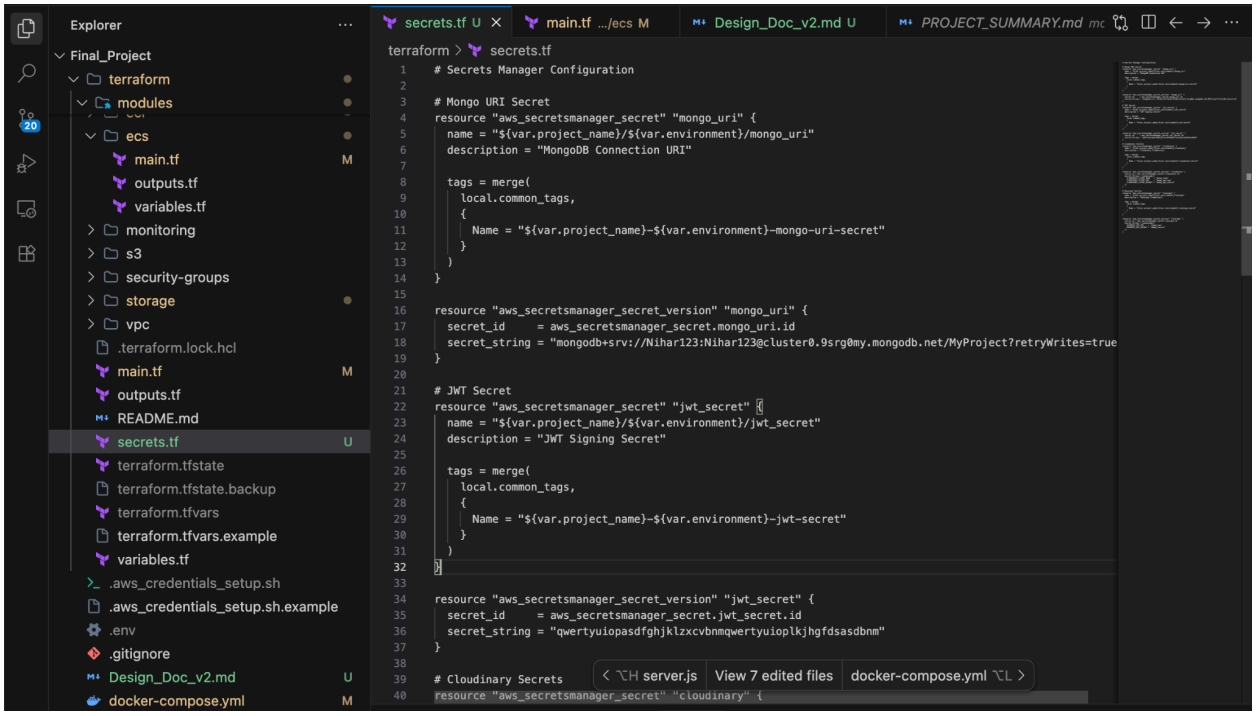
4.2 Runtime Secret Retrieval

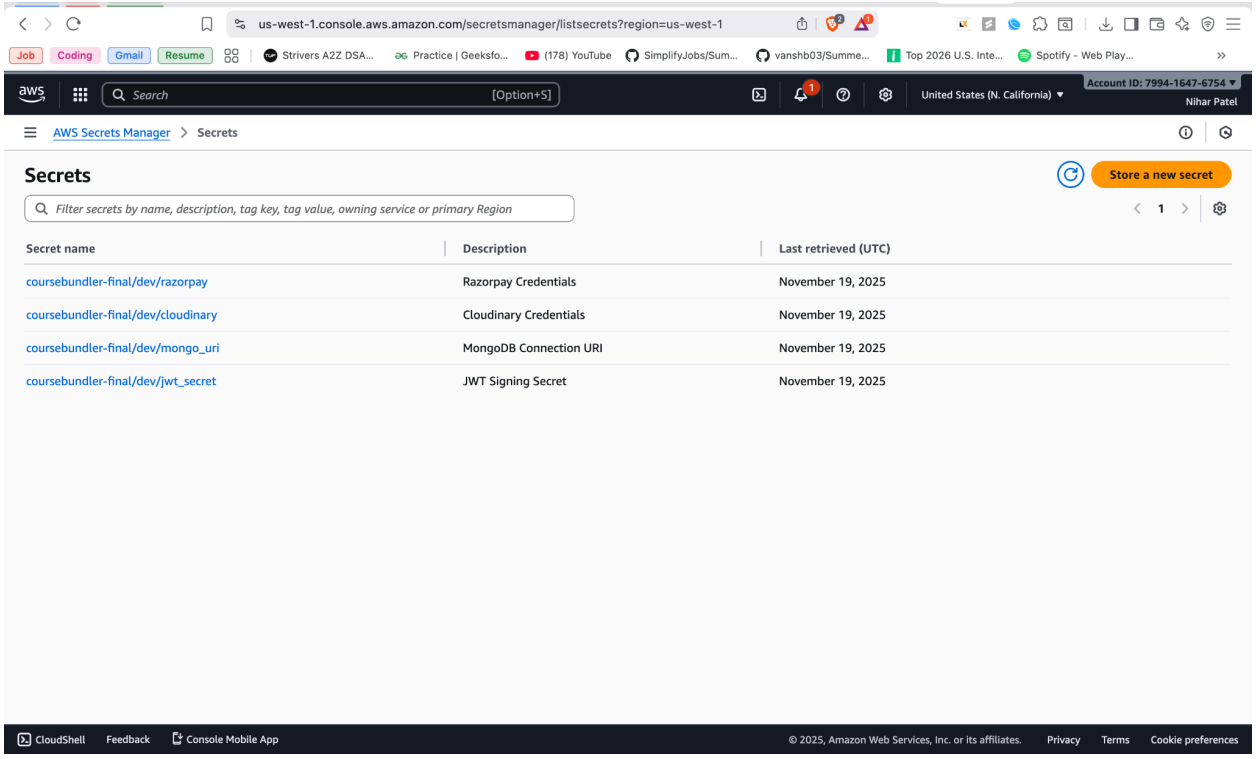
Implementation Flow:



Code Changes:






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. Inte...
Spotify - Web Play...
aws
Search
[Option+S]
United States (N. California)
Account ID: 7994-1647-6754
Nihar Patel
AWS Secrets Manager
Secrets
Secrets
Store a new secret
Filter secrets by name, description, tag key, tag value, owning service or primary Region
1
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

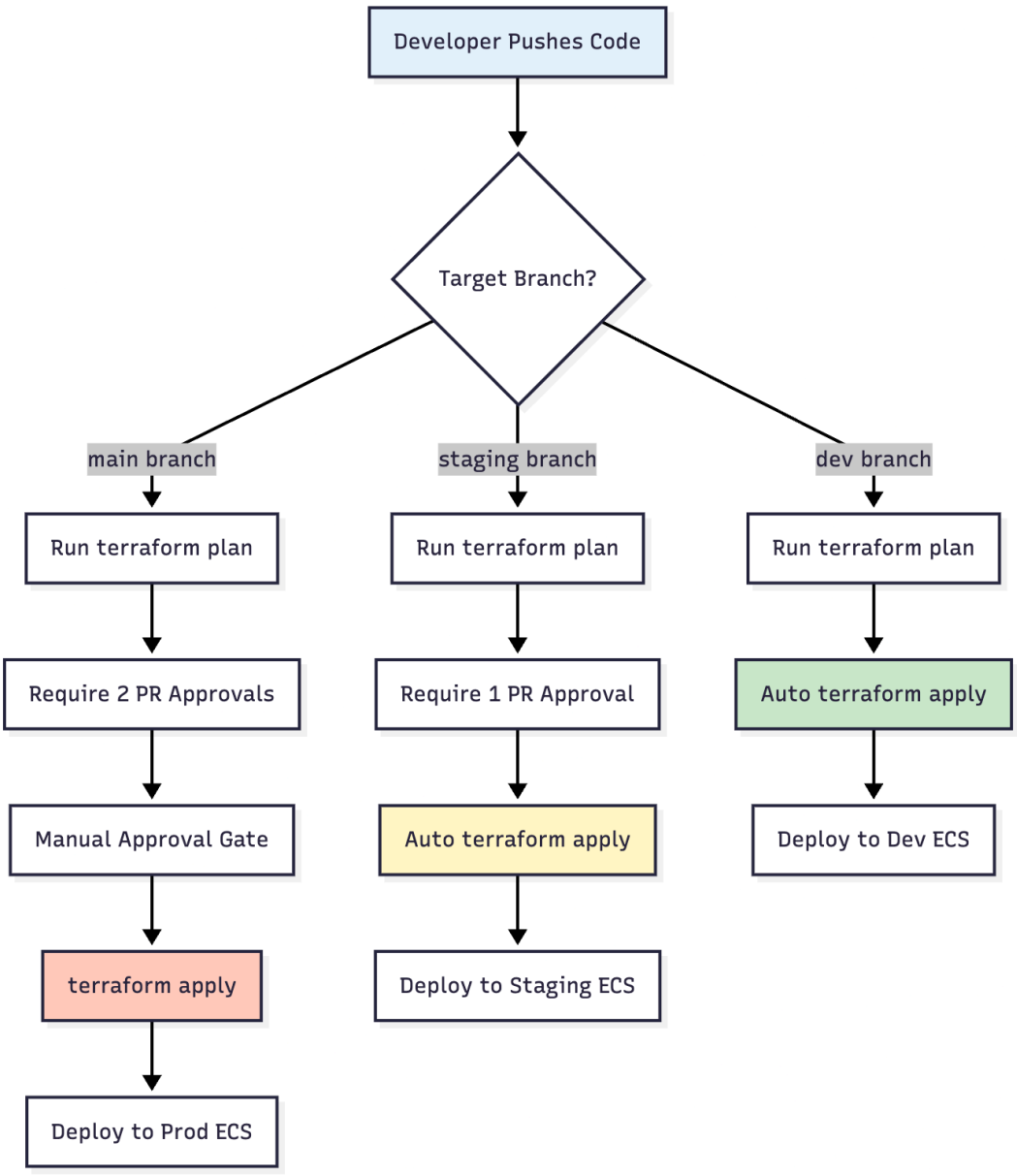
5. Infrastructure Governance

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

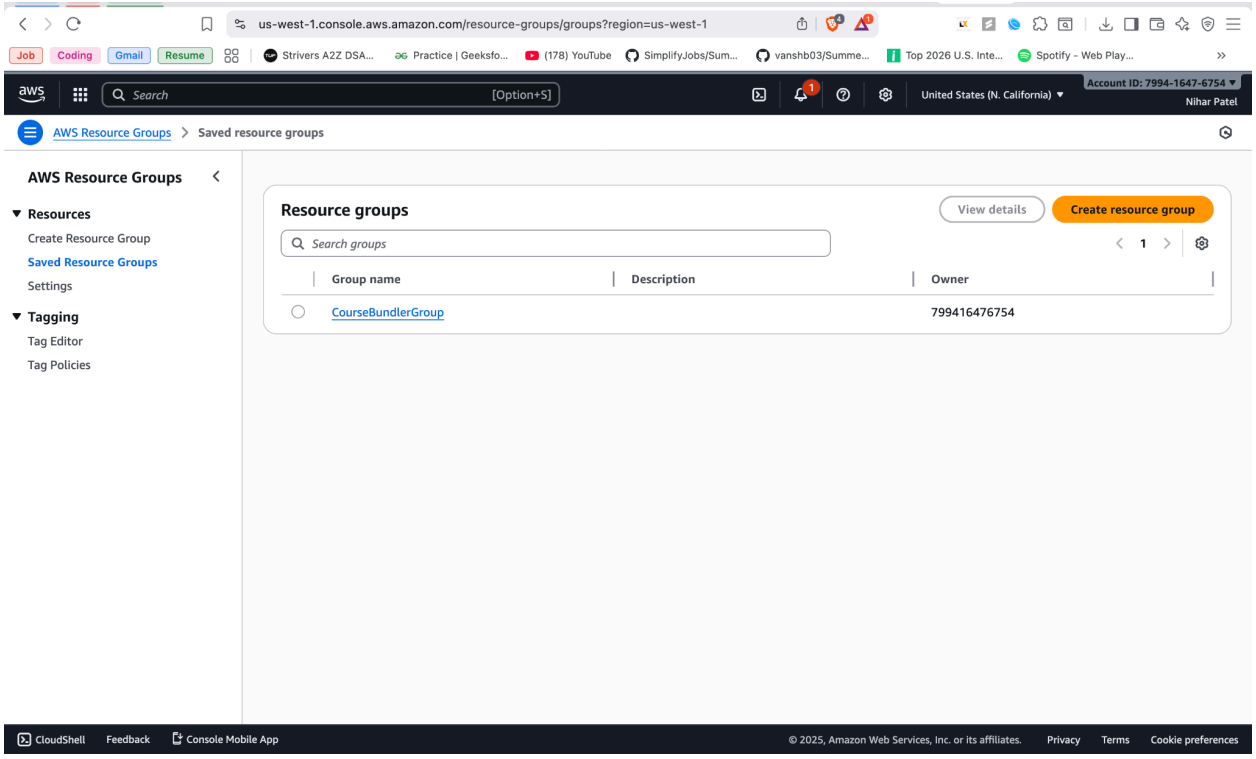
Mandatory Tags (Enforced via Terraform):

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

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

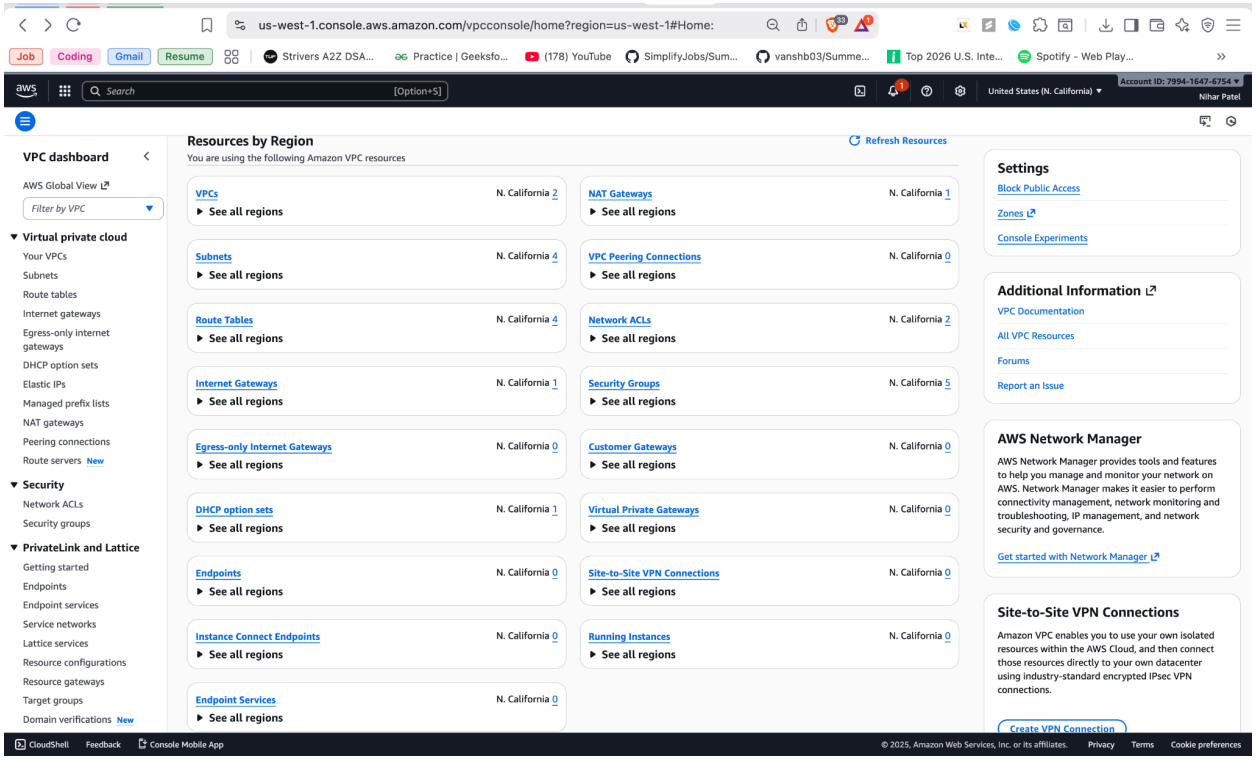
Benefits:

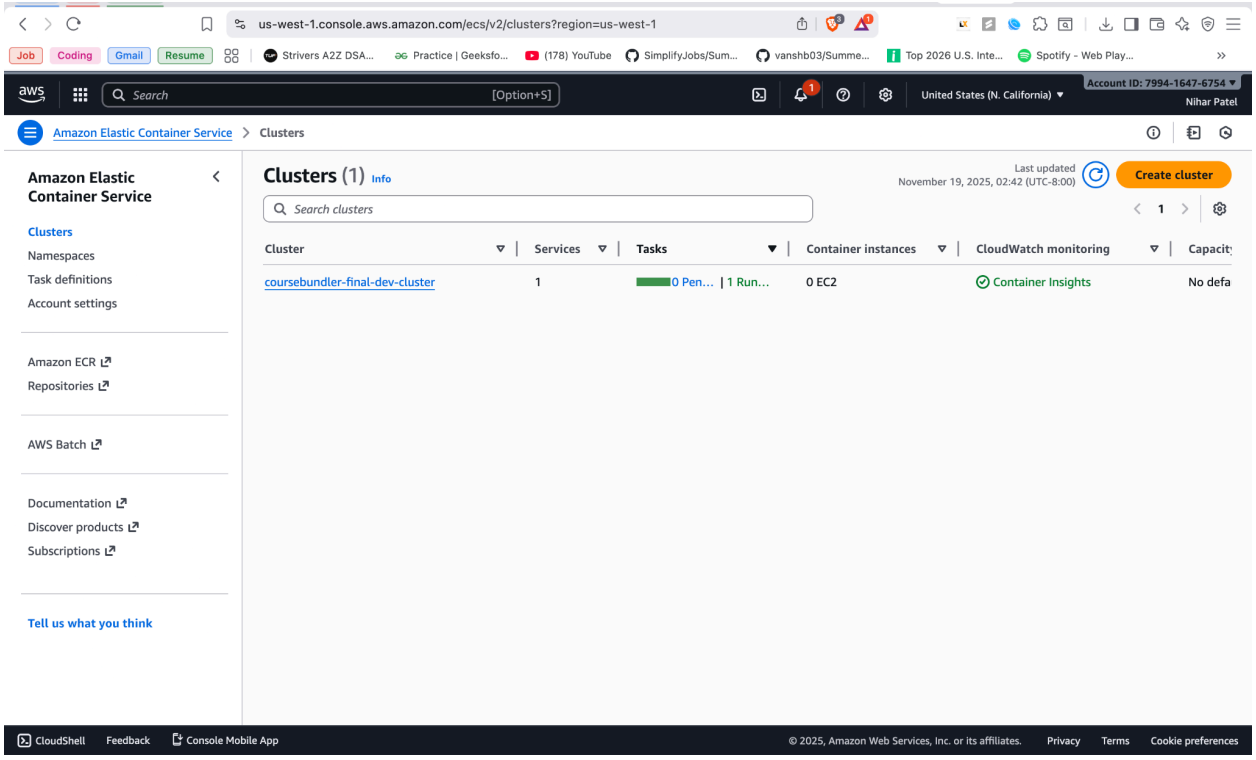
- ✅ **Cost Tracking:** Filter bills by `Project:coursebundler`
- ✅ **Resource Discovery:** Query all resources: `aws resourcegroupstaggingapi get-resources --tag-filters Key=Project,Values=coursebundler`
- ✅ **Compliance:** Auto-tag prevents "dangling resources"

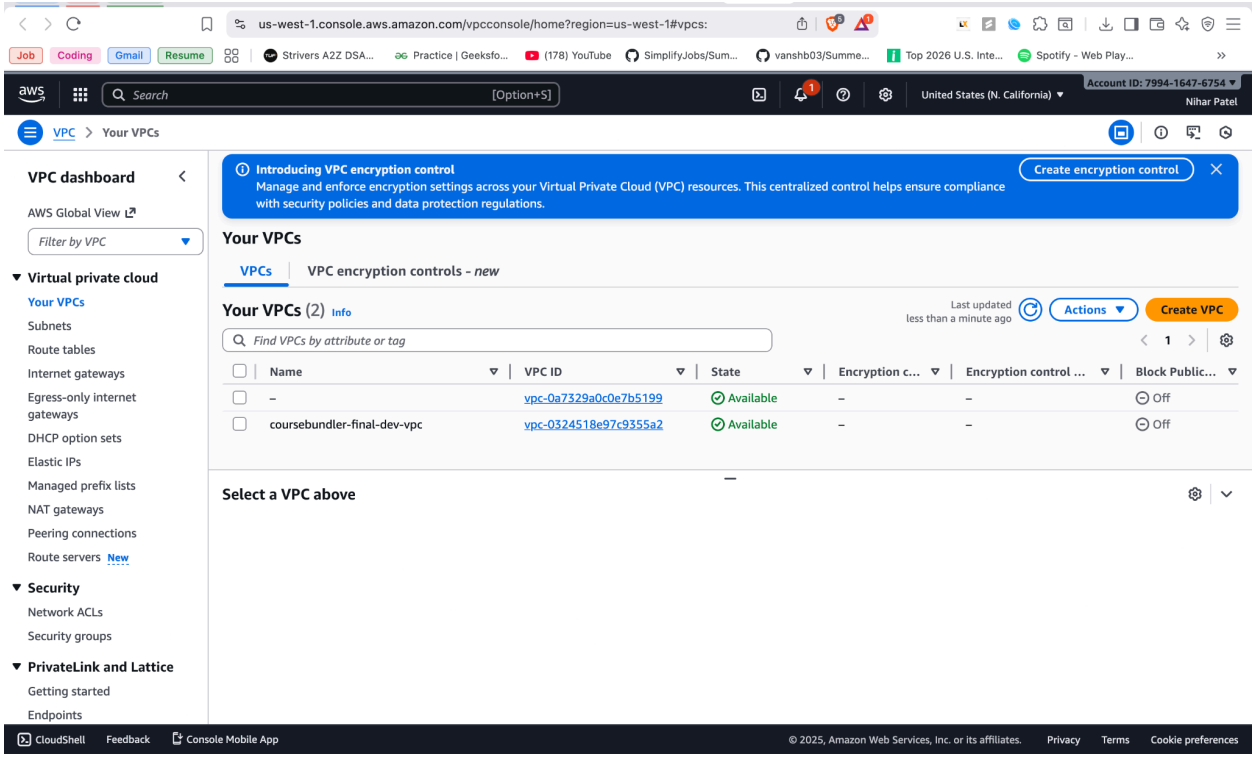

us-west-1.console.aws.amazon.com/resource-groups/groups?region=us-west-1
Job
Coding
Gmail
Resume
Strivers A2Z DSA...
Practice | Geeksfo...
(178) YouTube
SimplifyJobs/Sum...
vanshb03/Summe...
Top 2026 U.S. Inte...
Spotify - Web Play...
aws
Search
[Option+S]
United States (N. California)
Account ID: 7994-1647-6754
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
View details
Create resource group
Search groups
1
Group name
Description
Owner
CourseBundlerGroup
799416476754
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

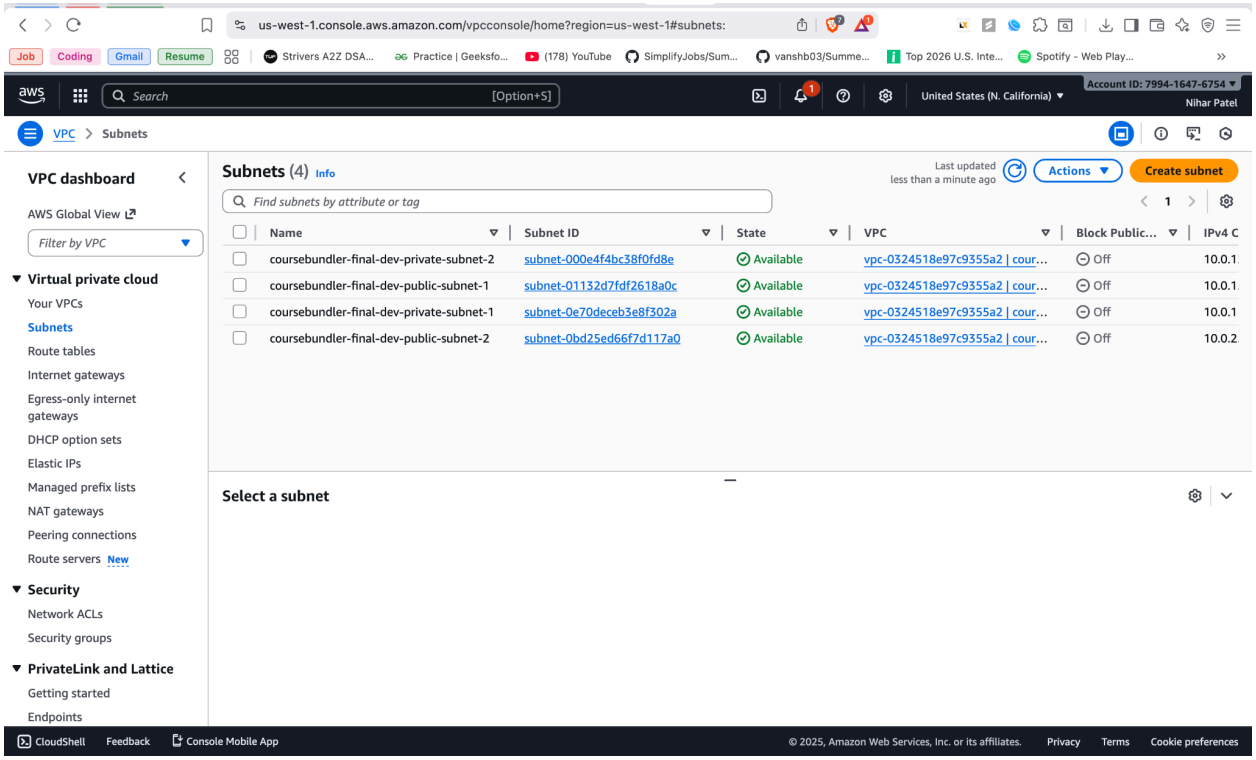
6. Deployment Evidence

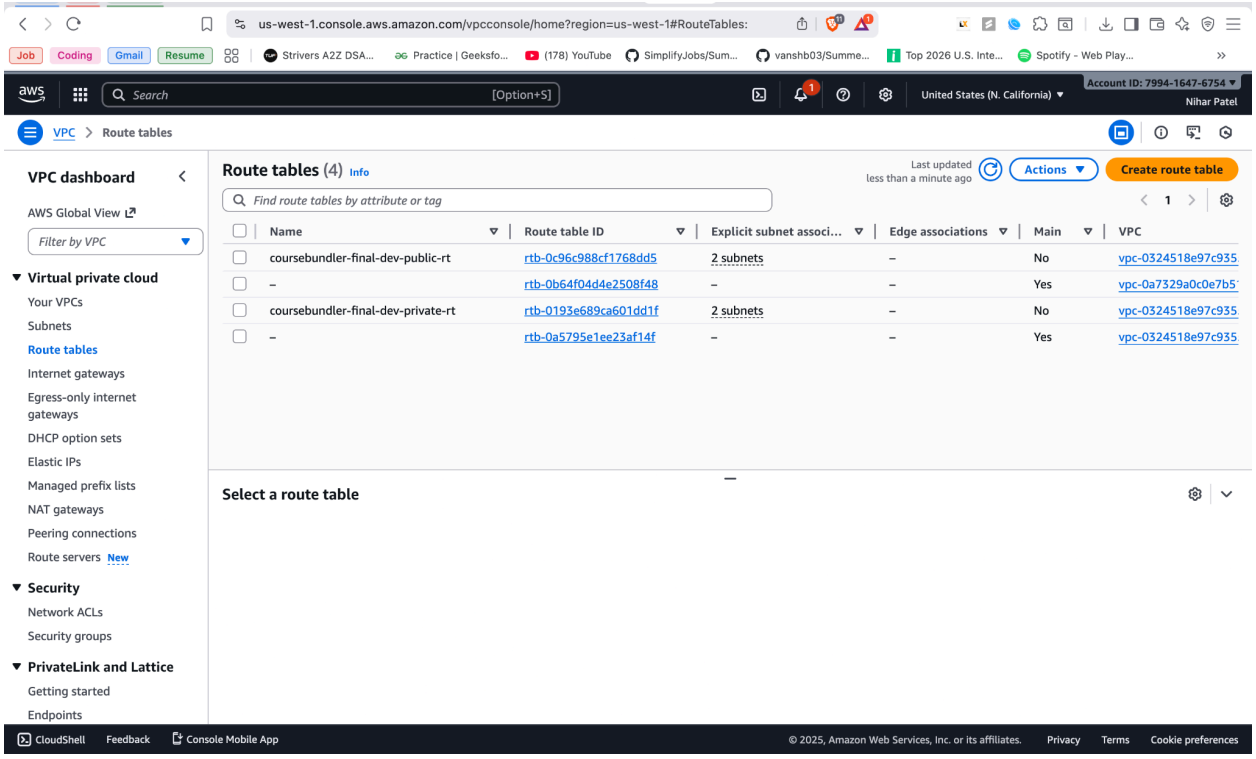
6.1 Infrastructure State

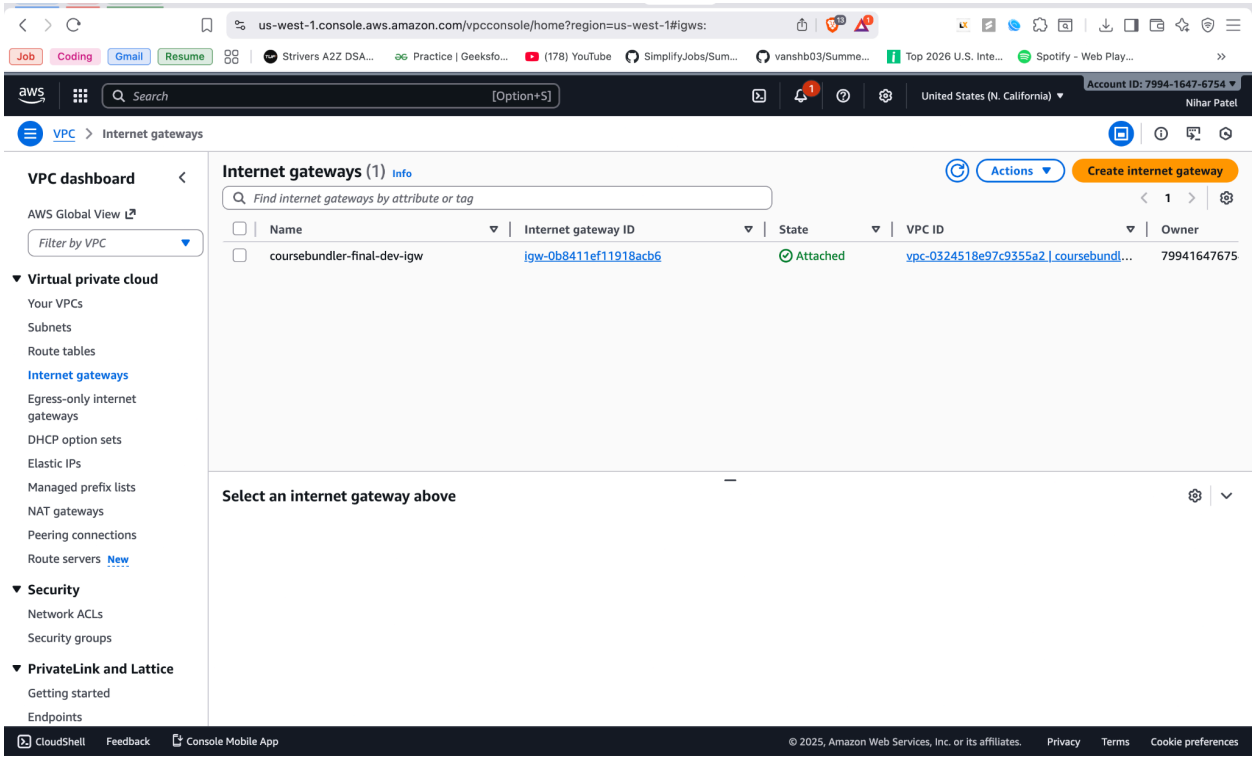


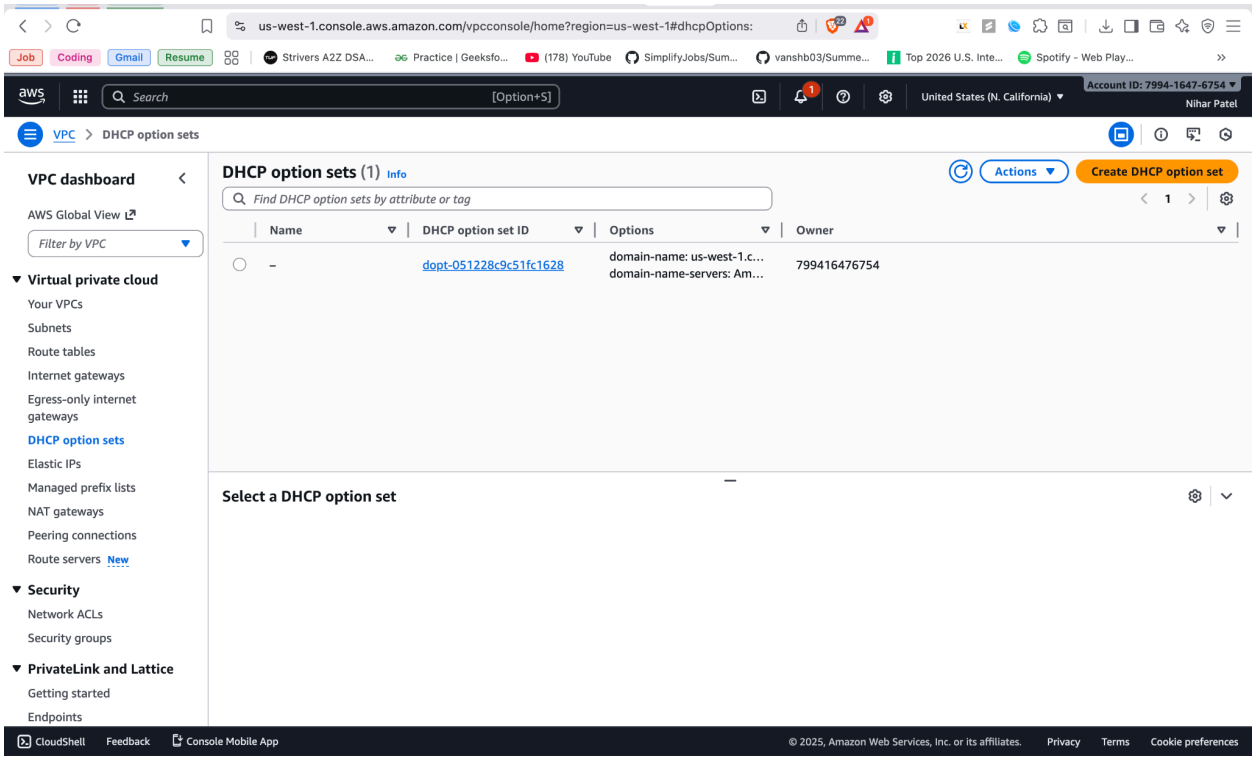


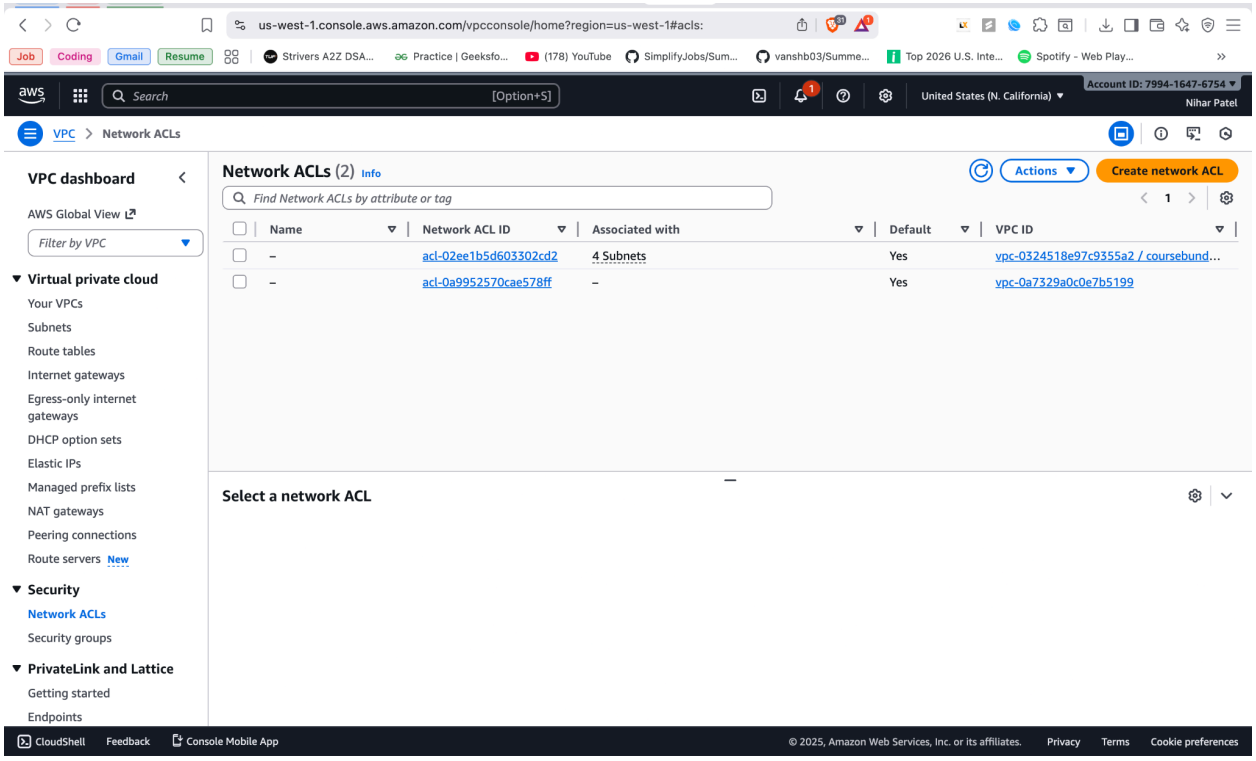

us-west-1.console.aws.amazon.com/vpcconsole/home?region=us-west-1#vpcs:
Search [Option+S]
United States (N. California)
Account ID: 7994-1647-6754
Nihar Patel
VPC > Your VPCs
VPC dashboard
AWS Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only 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
Introducing VPC encryption control
Manage and enforce encryption settings across your Virtual Private Cloud (VPC) resources. This centralized control helps ensure compliance with security policies and data protection regulations.
Create encryption control
Your VPCs
VPCs
VPC encryption controls - new
Your VPCs (2) Info
Last updated less than a minute ago
Actions
Create VPC
Find VPCs by attribute or tag
Name
VPC ID
State
Encryption c...
Encryption control ...
Block Public...
– vpc-0a7329a0c0e7b5199 Available – – Off
coursebundler-final-dev-vpc vpc-0324518e97c9355a2 Available – – Off
Select a VPC above
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

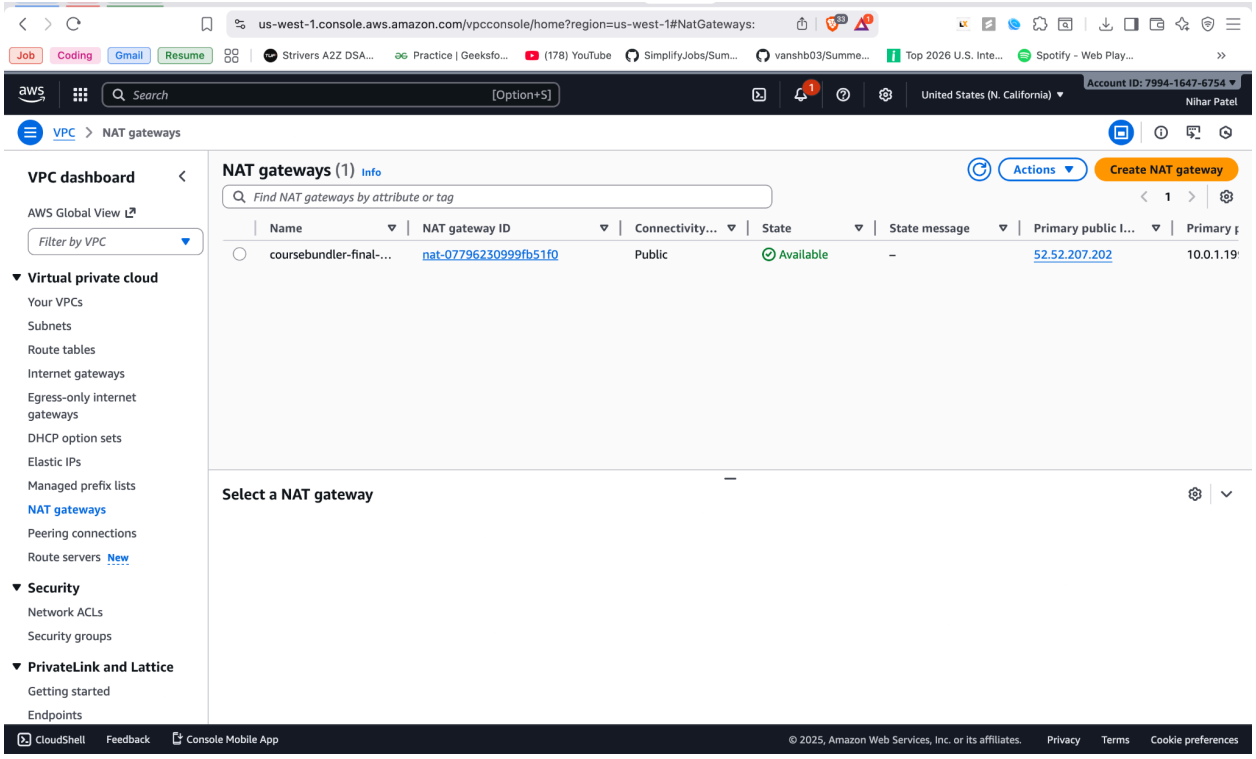

us-west-1.console.aws.amazon.com/vpcconsole/home?region=us-west-1#subnets:
Search [Option+S]
United States (N. California)
Account ID: 7994-1647-6754
Nihar Patel
VPC > Subnets
VPC dashboard
AWS Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only 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
Subnets (4) Info
Last updated less than a minute ago
Actions
Create subnet
Find subnets by attribute or tag
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.
Select a subnet
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


us-west-1.console.aws.amazon.com/vpcconsole/home?region=us-west-1#RouteTables:
Search [Option+S]
United States (N. California)
Account ID: 7994-1647-6754
Nihar Patel
VPC > Route tables
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
Route tables (4) Info
Last updated less than a minute ago
Actions
Create route table
Find route tables by attribute or tag
Name
Route table ID
Explicit subnet associ...
Edge associations
Main
VPC
coursebundler-final-dev-public-rt
rtb-0c96c988cf1768dd5
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
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


us-west-1.console.aws.amazon.com/vpcconsole/home?region=us-west-1#igws:
Search [Option+S]
United States (N. California)
Account ID: 7994-1647-6754
Nihar Patel
VPC > Internet 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
Internet gateways (1) Info
Actions
Create internet gateway
Find internet gateways by attribute or tag
Name
Internet gateway ID
State
VPC ID
Owner
coursebundler-final-dev-igw
igw-0b8411ef11918acb6
Attached
vpc-0324518e97c9355a2 | coursebundl...
79941647675
Select an internet gateway above
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


us-west-1.console.aws.amazon.com/vpcconsole/home?region=us-west-1#dhcpOptions:
Search [Option+S]
United States (N. California)
Account ID: 7994-1647-6754
Nihar Patel
VPC > DHCP option sets
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
DHCP option sets (1) Info
Find DHCP option sets by attribute or tag
Actions
Create DHCP option set
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
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

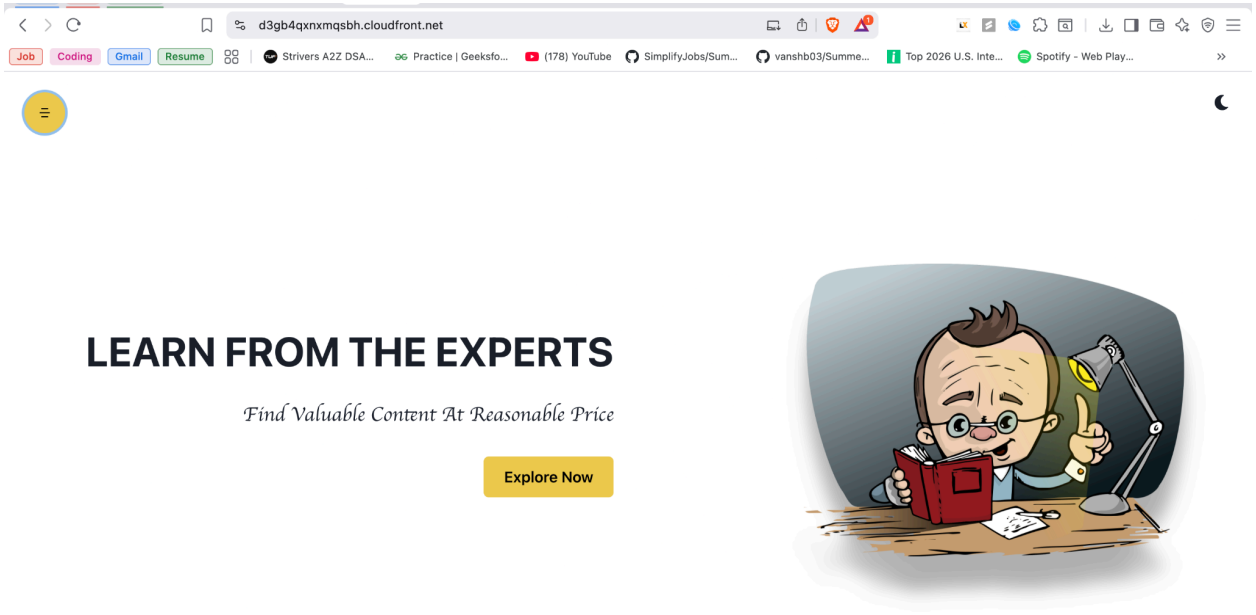

us-west-1.console.aws.amazon.com/vpcconsole/home?region=us-west-1#acls:
Search [Option+S]
United States (N. California)
Account ID: 7994-1647-6754
Nihar Patel
VPC > Network ACLs
VPC dashboard
AWS Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only 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
Network ACLs (2) Info
Find Network ACLs by attribute or tag
Actions
Create network ACL
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
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

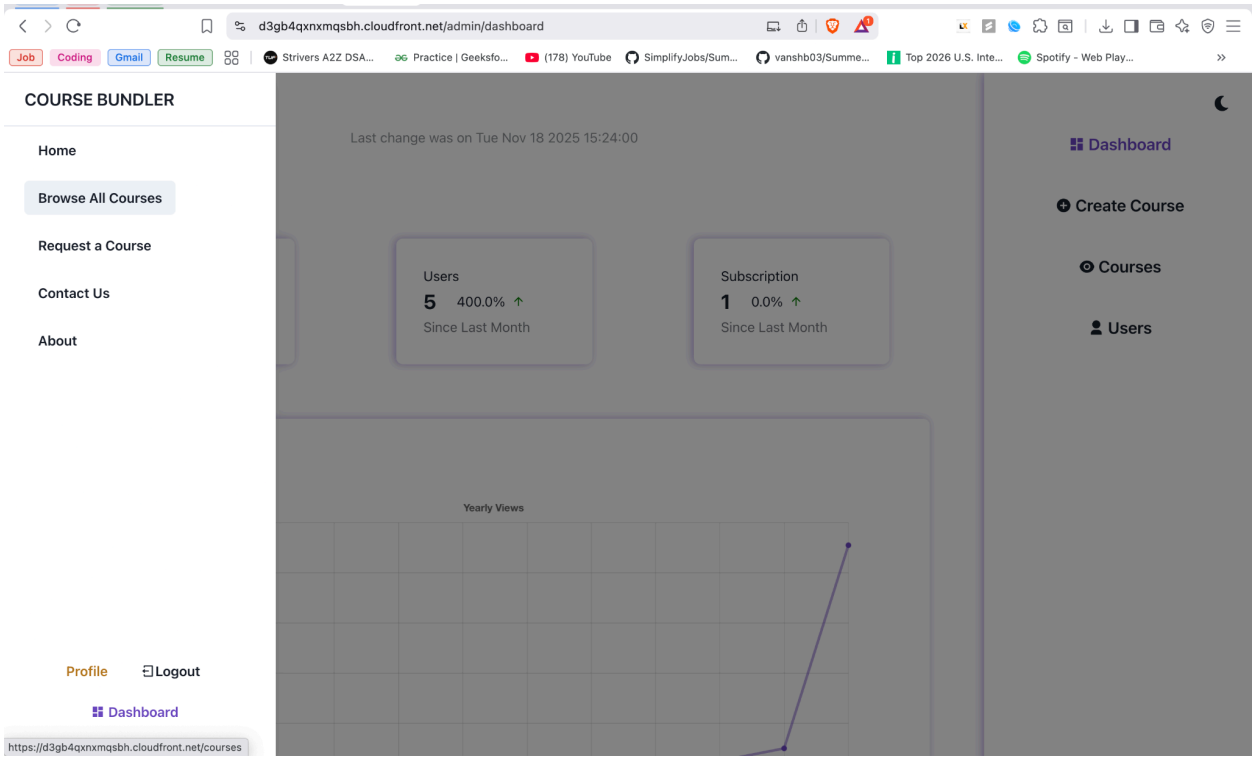

us-west-1.console.aws.amazon.com/vpcconsole/home?region=us-west-1#NatGateways:
Job
Coding
Gmail
Resume
Strivers A2Z DSA...
Practice | Geeksfo...
(178) YouTube
SimplifyJobs/Sum...
vanshb03/Summe...
Top 2026 U.S. Inte...
Spotify - Web Play...
aws
Search
[Option+S]
United States (N. California)
Account ID: 7994-1647-6754
Nihar Patel
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
NAT gateways (1) Info
Find NAT gateways by attribute or tag
Actions
Create NAT gateway
Name
NAT gateway ID
Connectivity...
State
State message
Primary public I...
Primary
coursebundler-final-...
nat-07796230999fb51f0
Public
Available
–
52.52.207.202
10.0.1.19
Select a NAT gateway
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

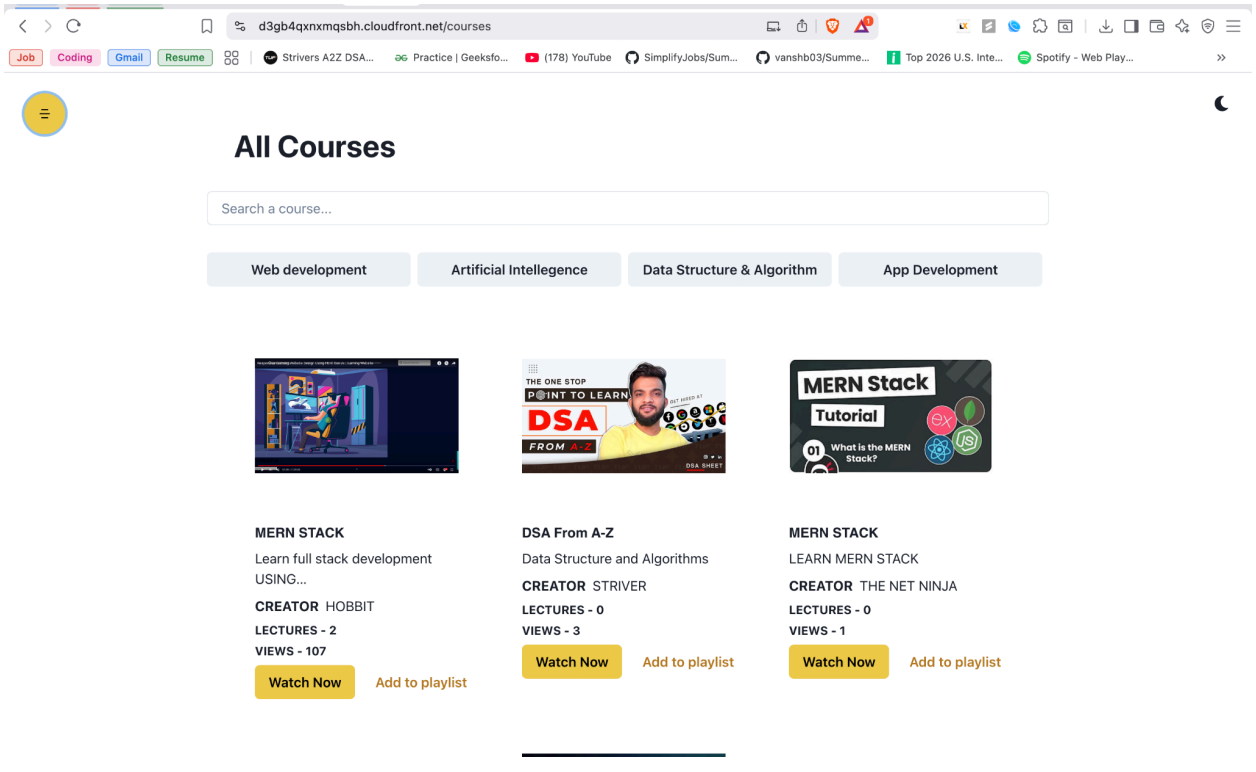
6.2 Application Screenshots

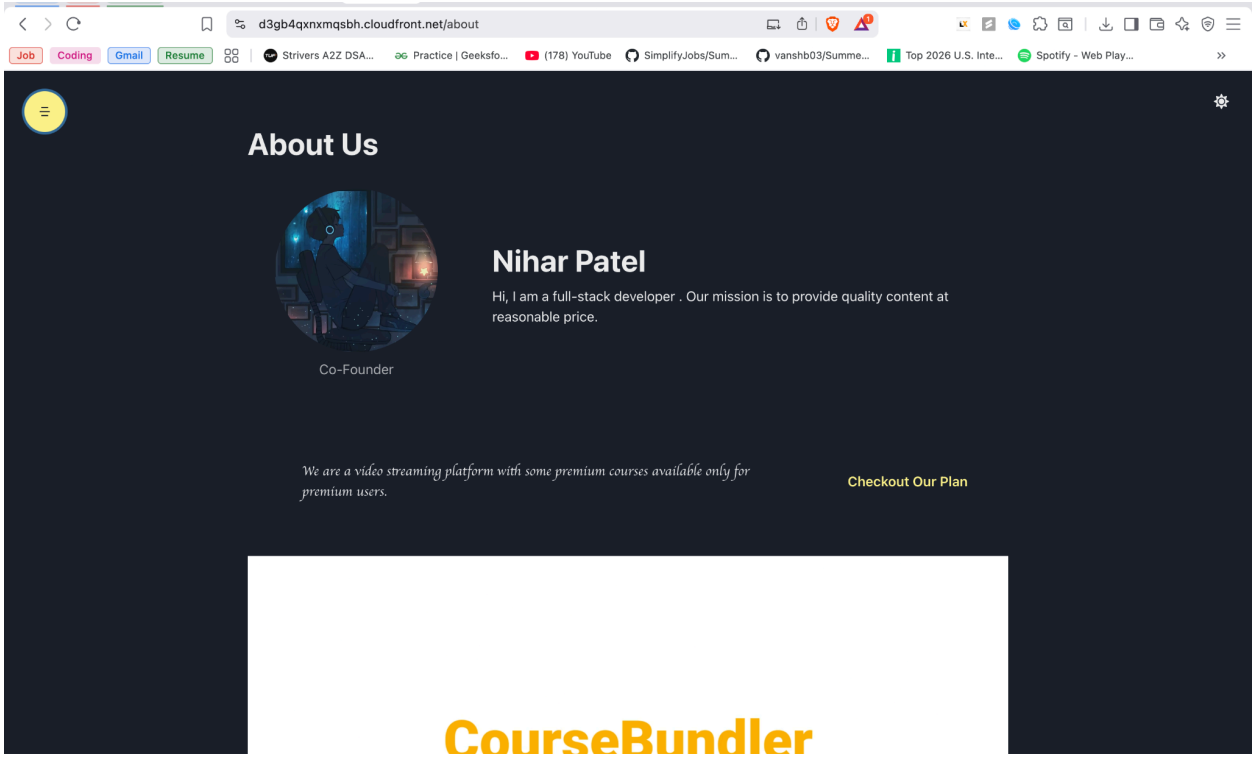
Live Application: https://d3gb4qxnxmqsbh.cloudfront.net

> **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.




d3gb4qxnxmqsbh.cloudfront.net/admin/dashboard
COURSE BUNDLER
Home
Browse All Courses
Request a Course
Contact Us
About
Profile
Logout
Dashboard
https://d3gb4qxnxmqsbh.cloudfront.net/courses
Last change was on Tue Nov 18 2025 15:24:00
Users
5 400.0%
Since Last Month
Subscription
1 0.0%
Since Last Month
Yearly Views
Dashboard
Create Course
Courses
Users


d3gb4qxnxmqsbh.cloudfront.net/courses
All Courses
Search a course...
Web development
Artificial Intellegence
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
LEARN MERN STACK
CREATOR THE NET NINJA
LECTURES - 0
VIEWS - 1
Watch Now
Add to playlist


d3gb4qxnxmqsbh.cloudfront.net/about
Job
Coding
Gmail
Resume
Strivers A2Z DSA...
Practice | Geeksfo...
(178) YouTube
SimplifyJobs/Sum...
vanshb03/Summe...
Top 2026 U.S. Inte...
Spotify - Web Play...
About Us
Nihar Patel
Hi, I am a full-stack developer . Our mission is to provide quality content at reasonable price.
Co-Founder
We are a video streaming platform with some premium courses available only for premium users.
Checkout Our Plan
CourseBundler