Project Title

Secure Web Server Setup and Monitoring on AWS using CLI & CloudFormation

---

Objective

To build a secure, scalable, and monitored web server infrastructure on AWS using **CloudFormation** for provisioning and **AWS CLI** for monitoring. This includes setting up a VPC, public/private subnets, EC2 instance, internet gateway, security group, CloudTrail logging, and S3 storage for logs.

Part 1: Infrastructure Setup (via CloudFormation)

Resources Provisioned

- **VPC**
    - CIDR: 10.0.0.0/16
    - DNS support: Enabled
    - DNS hostname: Enabled

- **Subnets**
    - Public Subnet: 10.0.1.0/24 (AZ-a, public IP enabled)
    - Private Subnet: 10.0.2.0/24 (AZ-b, no public IP)

- **Internet Gateway**
    - Attached to the VPC for external internet access.

- **Route Table**
    - Associated with the public subnet to route internet traffic.

- **Security Group**
    - Ingress rules:
        - SSH (Port 22) from anywhere 0.0.0.0/0
        - HTTP (Port 80) from anywhere 0.0.0.0/0

- **EC2 Instance**
    - Ubuntu
    - Type: t2.micro
    - Located in the public subnet
    - Apache server installed via **UserData** script
    - Displays a basic web page: *"Welcome to My Secure Web Server"*

	Stack name	Status	Created time ▾	Description
⬤	SecureWebServerStack	⊘ CREATE_COMPLETE	2025-04-29 22:31:49 UTC+0530	CloudFormation template to deploy a secure web server with monitoring

Welcome to My Secure Web Server

Part 2: Monitoring Setup (via AWS CLI)

Step 1: Create S3 Bucket for Logs

aws s3 mb s3://my-cloudtrail-logs-harshitha --region us-west-2

Step 2: Attach the Required Bucket Policy

Step 3: Create the CloudTrail Trail

```
C:\Users\Harshitha Basavaraju>aws cloudtrail create-trail --name MyTrail-server --s3-bucket-name myserver-2025 --is-mult
i-region-trail --enable-log-file-validation --region us-west-2
{
    "Name": "MyTrail-server",
    "S3BucketName": "myserver-2025",
    "IncludeGlobalServiceEvents": true,
    "IsMultiRegionTrail": true,
    "TrailARN": "arn:aws:cloudtrail:us-west-2:048575012724:trail/MyTrail-server",
    "LogFileValidationEnabled": true,
    "IsOrganizationTrail": false
}
```

Step 4: Start Logging

Step 5: Get CloudTrail Status

```
C:\Users\Harshitha Basavaraju>aws cloudtrail start-logging --name MyTrail-server --region us-west-2

C:\Users\Harshitha Basavaraju>aws cloudtrail get-trail-status --name MyTrail-server --region us-west-2
{
    "IsLogging": true,
    "StartLoggingTime": "2025-04-29T23:17:21.068000+05:30",
    "LatestDeliveryAttemptTime": "",
    "LatestNotificationAttemptTime": "",
    "LatestNotificationAttemptSucceeded": "",
    "LatestDeliveryAttemptSucceeded": "",
    "TimeLoggingStarted": "2025-04-29T17:47:21Z",
    "TimeLoggingStopped": ""
}
```

▢ **"IsLogging": true means it's working.**

▢ **Go to S3 Console**

▢ **Open your bucket (e.g., my-cloudtrail-logs-bucket)**

▢ **Browse to AWSLogs/**

Objects (1) ↻ | Copy S3 URI | | Copy URL | | ↓ Download | | Open ↗ | | Delete | | Actions ▼ | | Create folder | | ↑ Upload |

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory ↗ to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more ↗

| Q Find objects by prefix | | | ‹ 1 › | ⚙ |

☐	Name ▲	Type ▽	Last modified ▽	Size ▽	Storage class ▽
☐	🗋 AWSLogs/	Folder	-	-	-

☐		Name
☐	🗀	CloudTrail-Digest/
☐	🗀	CloudTrail/