

CCT College Dublin

Assessment Cover Page

Module Title:	Cloud Services
Assessment Title:	Designing and Implementing a Proof-of-Concept Cloud Solution Based on a Client's Needs
Lecturer Name:	Michael Weiss
Student Full Name:	Muhammad Sajjad Haider
Student Number:	2021384
Assessment Due Date:	Sunday 8th December
Date of Submission:	Sunday 8th December

Table of Contents

TASK 1: Medi-Advice company (Needs Solutions)	3
Current Infrastructure and Its Flaws:	3
Recommended AWS solution:	3
Architecture Design Proposal:	4
Auto-Setup of Servers and Availability:	4
Cost Optimization:	5
Conclusion:	5
TASK2: Architecture diagram (Solution Medi-Advice needs)	6
TASK 3a) Anti-patterns of Medi-Advice	7
1) Single Point of Failure (SPOF) in Database Architecture:	7
Problem (Anti-Pattern):	7
Impacts:	7
Solution:	7
2) Lack of Elasticity and Manual Scaling Issue:	8
Problem (Anti-Pattern):	8
Impact:	8
Solution:	8
TASK 3b) Six Pillars of the AWS Well-Architected Framework	9

1) Excellence in Operations:.....	9
2) Security:	9
3) Dependability:.....	9
4) Performance Efficiency:.....	10
5) Cost Optimization:	10
6) Ecological Responsibility:.....	10
TASK 4a) VPC & its components	11
Public Subnets:.....	11
Private Subnets:	11
Blocks of CIDR:	11
Gateway to the Internet (IGW):	11
NAT Instances and NAT Gateways:.....	11
NAT Instances:	12
Security Groups:.....	12
TASK 4(b) Use of FileZilla, Linux Server & MediAdviceVPC	12
TASK 5: Content Delivery Network (CDN)	17
1)Essential System element is the usage of Edge Sites for Worldwide Distribution:	17
2) Caching of Content:.....	17
3) Decreased Latency:	17
4) Enhanced Scalability:.....	18
5) Enhanced Delivery of Content:.....	18
CH-TASK 1: Edge Location content caching of the Medi-Advice brochures	19
CH-TASK 2: Medi-advice-private-network (VPC), ALB with ASG:	22
Practical Work:.....	22
Load-Balancer integration with Auto-scaler benefits:	31
Improved Availability and Reliability:.....	31
Cost effectiveness and system growth:	31
Prevention of Information Leakage and Compliance:.....	31
Reduced Manual Efforts:.....	31
CH-TASK 3: AWS Cloud Formation (Infrastructure as code)	32
A1: Deployment of VPC using AWS CloudFormation template:.....	32
A2: Linux EC2 instance in new VPC:.....	36
B1: Advantage of using CloudFormation to create VPC:.....	38
B2: Supporting Example for CloudFormation:	38
References:	39

TASK 1: Medi-Advice company (Needs | Solutions)

Convert client needs into a proposed technical solution.

Current Infrastructure and Its Flaws:

The current infrastructure is hosted in a data center based in Dublin, Ireland, on Microsoft Windows servers. It consists of:

- Two web servers
- Two application servers
- One database server

Defined weaknesses:

- One Point of Failure
- Manual Scaling
- Performance Issues
- Lack of Disaster Recovery
- Non-elastic Infrastructure
- Issues in Content Delivery

Recommended AWS solution:

Availability Zones and AWS Regions Medi-Advice should leverage AWS regions and Availability Zones (AZs) to ensure disaster recovery, fault tolerance, and high availability.

Specifically:

- The production environment should be in the EU (Ireland) region.
- For the North American user base, the US-East (North Virginia) area should be used. Resources need to be spread across at least two Availability Zones within a location to ensure redundancy and high availability. Essential AWS Services Needed.

Architecture Design Proposal:

Web Tier:

- Elastic load balancer (ALB) distributes traffic across multiple EC2 instances in two regions, North Virginia and Ireland.
- Auto Scaling changes the count of EC2 instances based on real-time traffic.

Tier of Application:

- Application logic is hosted in EC2 instances, which are attached to the RDS database.
- Document processing operations that are initiated by uploads to S3 are automated via AWS Lambda.

Tier of the Database:

- Database availability is guaranteed across two availability zones when Amazon RDS is deployed using Multi-AZ.
- From North America, Read Replicas offer quick access to the database.

Level of Storage:

- Images and documents are stored on S3.
- S3 Glacier is utilized for long-term, reasonably priced storage.

Delivery of Content:

- It allows the enhancement of accessibility to brochures and other resources all over the world by caching static content at edge sites.

Disaster Recovery:

- The cross-region load balancing feature in Route 53 guarantees service continuity and failover between the US and EU.

(Dong et al., 2018).

Auto-Setup of Servers and Availability:

The EC2 instance auto-scaling groups guarantee that the infrastructure can adjust automatically to traffic, both during periods of high traffic and periods of low traffic.

CloudWatch Alarms immediately deploy new instances in order to save money or terminate unused ones based on the failure or heavy load of EC2 instances.

Cost Optimization:

EC2 Reserved Instances significantly reduce costs if used for the base load of database and application servers. S3 Intelligent-Tiering and S3 Glacier will automatically move infrequently accessed data to lower-cost storage, optimizing storage costs.

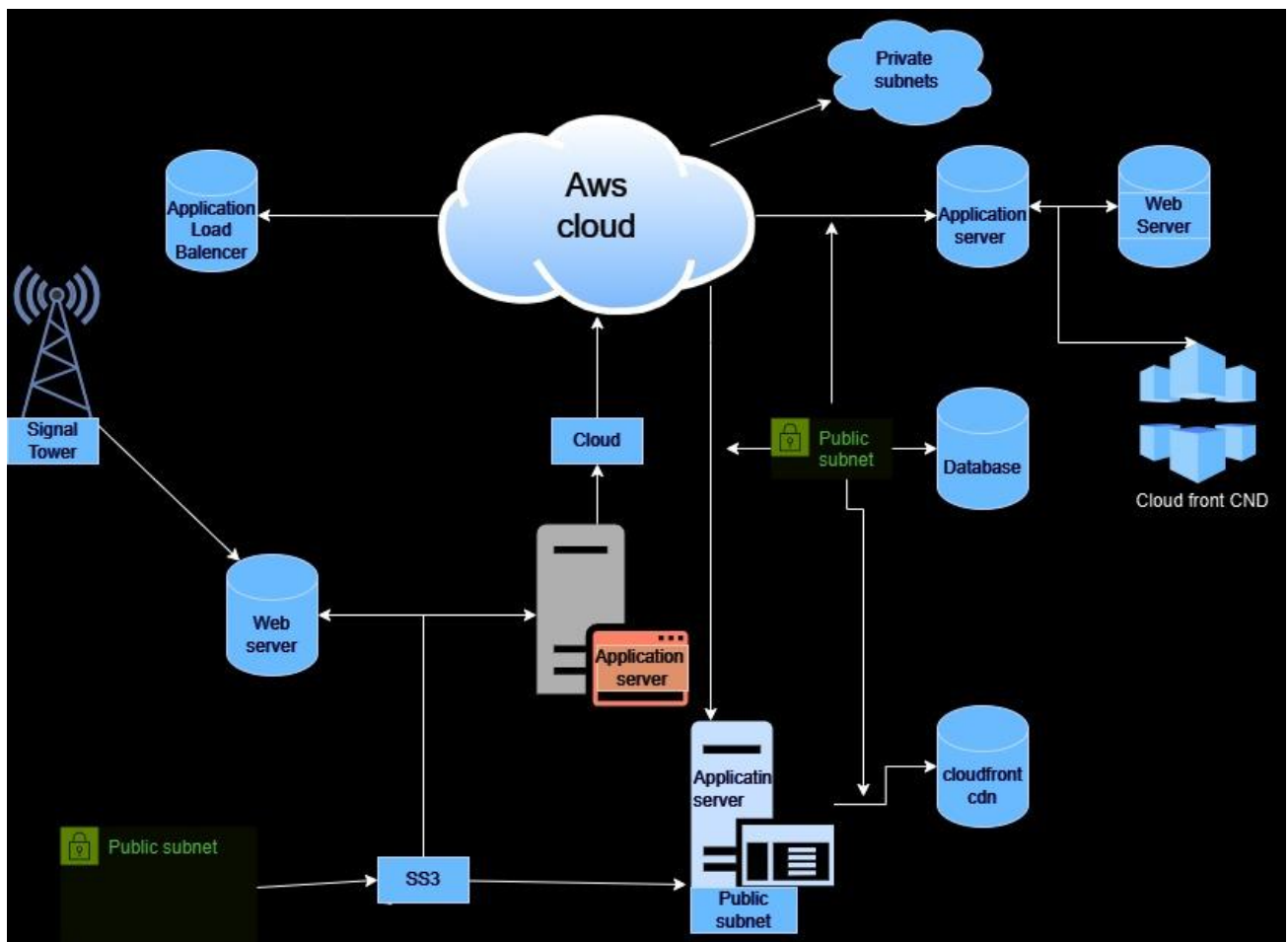
Conclusion:

The proposed AWS solution addresses all the requirements Medi-Advice has for a secure, scalable, and highly available infrastructure. We can ensure that the application runs well on a global scale, scales dynamically, and is resilient to regional failures by using AWS services such as EC2, RDS, CloudFront, and Lambda. Moreover, the implementation of a content distribution network and automation of document processing would greatly improve user experience and operational efficiency. Moreover, the architecture ensures that Medi-Advice can scale down to reduce costs and scale up in light of growing demand. In addition to addressing the client's needs, this solution positions Medi-Advice for eventual growth and expansion.

(elmoallistair, 2020).

TASK2: Architecture diagram (Solution Medi-Advice needs)

- The architecture ensures fault tolerance, high availability, and scalability, addressing Medi-Advice's challenges like single points of failure, manual scaling, and disaster recovery.
- It incorporates best practices by separating tiers (web, application, database) and isolating private resources.
- The inclusion of CloudFront addresses global accessibility issues for brochures and other static content.



- This diagram effectively meets the technical requirements stated in the assignment.

TASK 3a) Anti-patterns of Medi-Advice

While applied to the context of infrastructure design, anti-pattern has more negative connotations, denoting mere recurrent inefficient approaches that, in most cases, result in increased costs or diminished performance and complexity. Describe here two anti-patterns observed in Medi-Advice's current application structure and then explain, how the presented AWS solution eradicates them.

Some of the Anti-Patterns identified in Medi-Advice's current infrastructure are as follows;

1) Single Point of Failure (SPOF) in Database Architecture:

Problem (Anti-Pattern):

Medi-Advice currently relies on a single database server to manage their application data. This creates a single point of failure for the entire system. If the database server goes down, the entire application becomes unusable, resulting in significant service outages and downtime. This is an anti-pattern because it fails to provide the necessary fault tolerance and high availability for critical business operations.

Impacts:

- Doctors and patients cannot access records.
- Application downtime disrupts business continuity.
- Recovery from failure is slow and manual, increasing operational overhead.

(Amazon Web Services, 2018).

Solution:

In an attempt to overcome this problem, the proposed solution employs the use of Amazon RDS with Multi-AZ Deployment. This arrangement makes certain the database is mirrored across different Availability Zones (AZs) to give an instant failover in case of a problem in a particular zone.

High Availability:

Multi-AZ deployment means if for any reason, the primary database is not available, there will be a solution and the application will be served the replica without interruption.

2) Lack of Elasticity and Manual Scaling Issue:

Problem (Anti-Pattern):

At the present time Medi-Advice employs manual scaling to increase the number of machines that are used in response to the changing conditions. This is evidenced by delays, inefficiency and overprovisioning.

Impact:

- Slow response to sudden traffic increase that results in a poor performance like time out errors or slow page rendering.
- Over investing in certain regions at sometimes h increases infrastructure cost disproportionately.

(AWS, 2019).

Solution:

AWS Elastic Load Balancer known as ALB and AWS Auto Scaling are adopted in the proposed strategy.

Elasticity:

Due to auto scaling, infrastructure can easily scale in or out according to the intensity of traffic. It eliminates situations of under and over provision and ensures optimum use of resources.

Cost Efficiency:

Medi-Advice does not have to pay for more computing capability than is necessary because intelligent resource scaling reduces costs of those related.

TASK 3b) Six Pillars of the AWS Well-Architected Framework

An explanation of how each pillar can be used to maximize Medi-Advice's infrastructure is provided below:

1) Excellence in Operations:

Optimal Techniques:

Sustained the operations of recurring activities and monitor the state of the system. For continuous monitoring and alerting that we are assured that any issues will be detected and resolved on time, use Amazon CloudWatch.

Optimization:

Decrease the need for human intervention and the general operational cost by automatically managing volume with CloudWatch Alarms and using AWS Lambda for document processing.

2) Security:

Best Practices:

Implement least privilege through AWS IAM, and for critical assets, you should allow the Multi-Factor Authentication.

Optimization:

Run Security Hub to triage security policies every now and then and subsequently encrypt sensitive data that is stored in Amazon S3. AWS WAF and Shield should be adopted for web application security to protect application flow.

3) Dependability:

Best Practices:

Ensure systems availability and redundancy by following Failure Design thru Multi-AZ and Multi-Region configurations.

Optimization:

For availability zones contingency utilize Cross-Region Replication and for databases availability utilize Amazon RDS Multi-AZ. For web and application servers safe guard performance under different loads, you need to apply auto scaling. (New Relic, 2021).

4) Performance Efficiency:

Best Practices:

Select resources necessary for the task, monitor results and adjust resources if it's needed.

Optimization:

To increase performance at the international level, use CloudFront to help to cache and deliver content to the clients and obtain EC2 Auto Scaling to transform the capacity on the basis of requirement. For breaking the traffic, utilize an elastic load balancer (ALB).

5) Cost Optimization:

Best Practices:

Identify wastage in the usage of the resources, choose a right model of pricing and remove unnecessary resources.

Optimization:

For EC2, save money on the instance cost by subscribing to AWS RI or AWS Savings Plans to cut-on the long-term cost. For more cost-effective storage of the data and for data that is rarely accessed, use S3 Glacier. Minimize operation cost through auto scaling in order to ensure that servers are not over provisioned, yet provisioned enough to meet load demands.

(vsi_clear_admin, 2022).

6) Ecological Responsibility:

Best Practices:

Design services that will achieve highest service levels while demand the least input resources.

Optimization:

To reduce server supposedly hence the efficient use of serverless services like AWS Lambda for processing tasks. Choose the right EC2 instance types with the help of AWS Compute Optimizer.

TASK 4a) VPC & its components

A conceptually separate region of the AWS cloud where you can place AWS resources: A Virtual Private Cloud (VPC) enables you to launch AWS resources in a virtual network of your selection. It gives you full control of the network environment; specification of the subnets, route tables, IP address range, and security.

Public Subnets:

Subnets running on direct internet connection are referred to as public subnets. Resources placed in public subnets can start using the internet after connecting it via an Internet Gateway.

Private Subnets:

These subnets are for handling operational data such as user informations or back-end included databases and Application servers and does not have access to the public internet.

(Spiceworks, n.d.).

Blocks of CIDR:

The private IP addresses that you are allowed to select in your VPC are determined by CIDR blocks. An example is the CIDR block like 10.0.0.0/16, where we may be given an amount of range that could accommodate 65,536 IP numbers.

Every CIDR blocks helps in the division of the distribution of IP address in relation to the subnets in the VPC. (T, 2023).

Gateway to the Internet (IGW):

An Internet gateway provides access to the Internet for traffic originating from resources in public subnets. This makes it possible for the VPC and the internet to communicate with each other in both ways. The IGW provides the ability for any resource located on a public subnet, let it be a web server, to have access to the internet.

NAT Instances and NAT Gateways:

A managed service termed as NAT (Network Address Translation) gateway allow resources in the private subnets to send traffic out to the internet without letting incoming traffic get through to them.

NAT Instances:

An EC2 instance which has been configured to perform NAT duties. It works like the NAT Gateway but needs more attention since it is a self-serviced service.

Security Groups:

Security Groups act in a manner that of instance-level security appliances that control traffic flow. Since instances are stateful, when letting incoming traffic to an instance, this also immediately allows outgoing traffic. Alternatively, they are used to control traffic flow in and out of the EC2 instances.

(Shalom, 2018).

TASK 4(b) Use of FileZilla, Linux Server & MediAdviceVPC

- Firstly, Set the name of new VPC as MediAdviceVPC.

[VPC](#) > [Your VPCs](#) > [Create VPC](#)

Create VPC [Info](#)

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances, Amazon S3 buckets, and Amazon ElastiCache instances.

VPC settings

Resources to create [Info](#)
Create only the VPC resource or the VPC and other networking resources.

☐ VPC only ☒ VPC and more

Name tag auto-generation [Info](#)
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

☒ Auto-generate
MediAdviceVPC

IPv4 CIDR block [Info](#)
Determine the starting IP and the size of your VPC using CIDR notation.

10.0.0.0/16 65,536 IPs
CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)

☒ No IPv6 CIDR block
☐ Amazon-provided IPv6 CIDR block

Tenancy [Info](#)

Default

Number of Availability Zones (AZs) [Info](#)
Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

1 2 3

- VPC has created successfully.

Create VPC workflow

✓ Success

▼ Details

- ✓ Create VPC: [vpc-05154a14f867f8d97](#)
- ✓ Enable DNS hostnames
- ✓ Enable DNS resolution
- ✓ Verifying VPC creation: [vpc-05154a14f867f8d97](#)
- ✓ Create S3 endpoint: [vpce-082131603832502c4](#)
- ✓ Create subnet: [subnet-0149df157b078af22](#)
- ✓ Create subnet: [subnet-0aa2a94d6c4ba4c10](#)
- ✓ Create subnet: [subnet-0efc2d512cefa3aa4](#)
- ✓ Create subnet: [subnet-0f625e74163047086](#)
- ✓ Create internet gateway: [igw-0371222b8b3480e20](#)
- ✓ Attach internet gateway to the VPC
- ✓ Create route table: [rtb-03298d067287af6c6](#)
- ✓ Create route
- ✓ Associate route table
- ✓ Associate route table
- ✓ Create route table: [rtb-074c22084f92501b0](#)
- ✓ Associate route table
- ✓ Create route table: [rtb-0c6f5c71899e12231](#)
- ✓ Associate route table
- ✓ Verifying route table creation
- ✓ Associate S3 endpoint with private subnet route tables: [vpce-082131603832502c4](#)

[View VPC](#)

- Created new Linux instance with the name Medi-Advice-server.

Name and tags [Info](#)

Name

Medi-Advice-server [Add additional tags](#)

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

🔍 Search our full catalog including 1000s of application and OS images

Recents **Quick Start**

 aws	 Mac	 ubuntu	 Microsoft	 Red Hat	 SUSE	 Browse more AMIs Including AMIs from AWS, Marketplace and the Community
---------	---------	------------	---------------	-------------	----------	--

Amazon Machine Image (AMI)

- Created new .pem key pair for this instance and named as Year4-key-pem.

Create key pair ✕

Key pair name
Key pairs allow you to connect to your instance securely.

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

☒ **RSA**
RSA encrypted private and public key pair

☐ **ED25519**
ED25519 encrypted private and public key pair

Private key file format

☒ **.pem**
For use with OpenSSH

☐ **.ppk**
For use with PuTTY

Warning: When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. [Learn more](#)

[Cancel](#) [Create key pair](#)

- In Network settings, selected the MediAdviceVPC which has created above with the public subnet.
- Also created new security group Medi-Advice-ca2-sg for this particular instance.

Network settings [Info](#)

VPC - required [Info](#)

10.0.0.0/16

Subnet [Info](#)

VPC: vpc-05154a14f867f8d97
Availability Zone: us-east-1a
IP addresses available: 4091
Zone type: Availability Zone
CIDR: 10.0.0.0/20

Auto-assign public IP [Info](#)

Firewall (security groups) [Info](#)

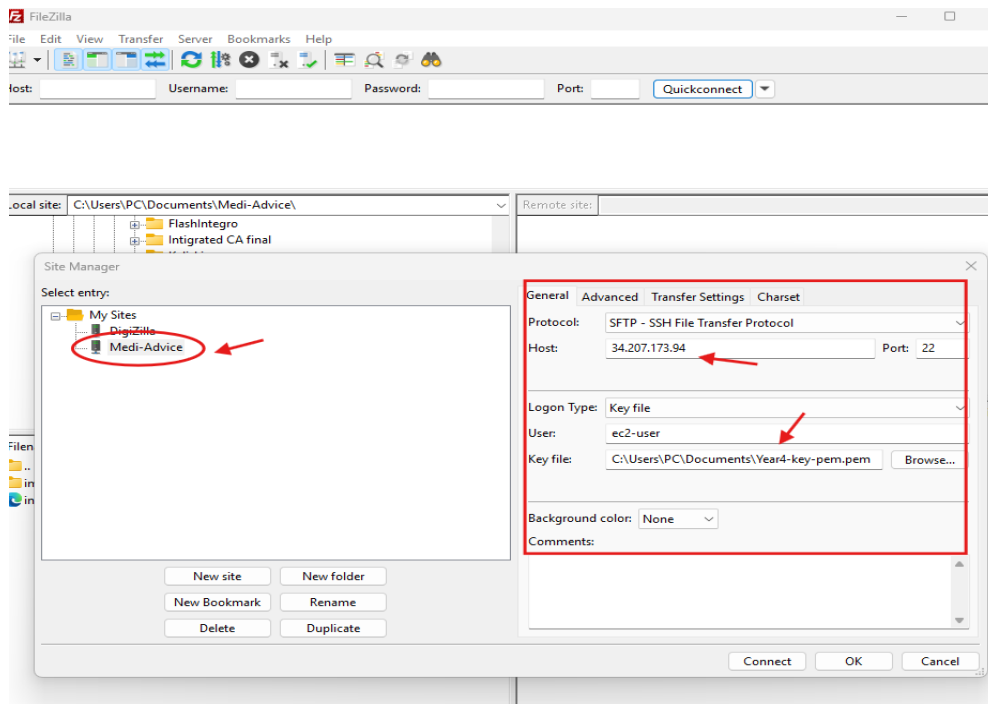
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ **Create security group** ☐ **Select existing security group**

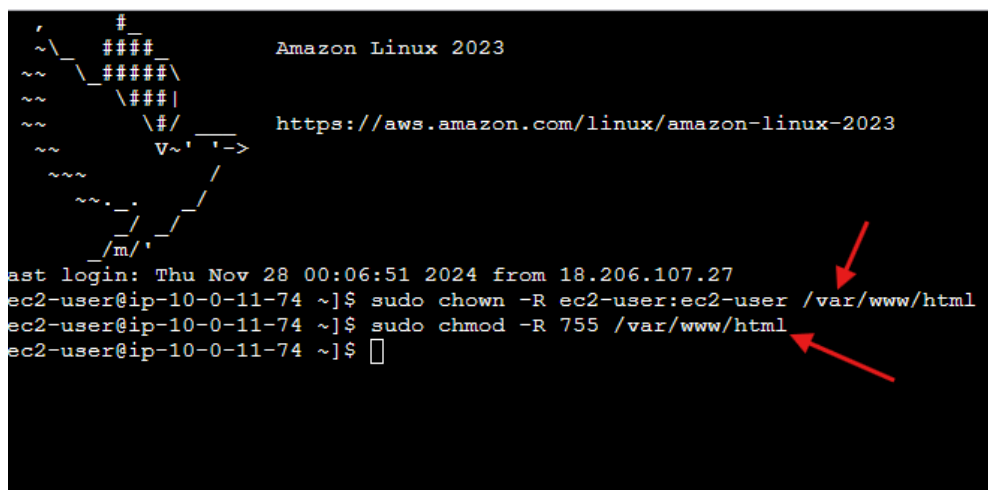
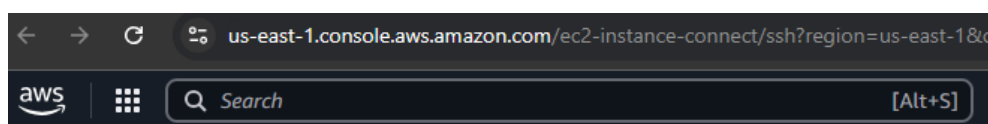
Security group name - required

Description - required [Info](#)

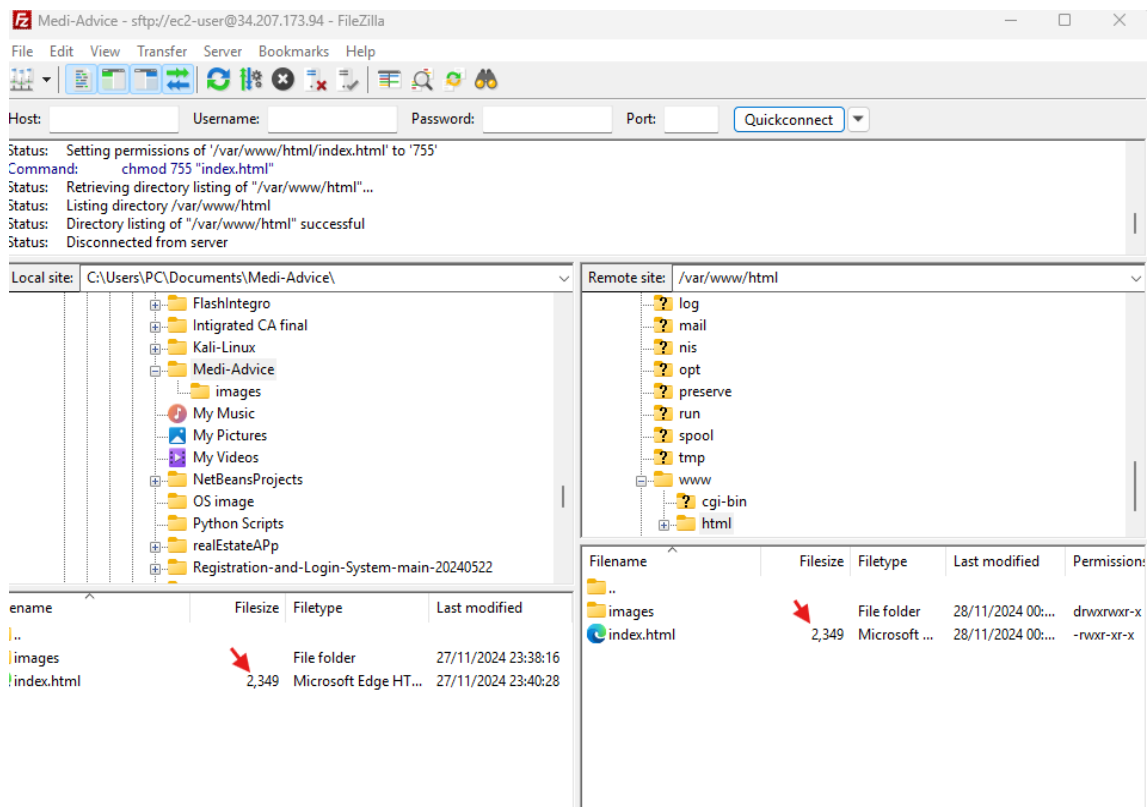
- Used FileZilla software to access the Medi-Advice Linux server created above.
- In FileZilla, go to file and navigate Site Manager.
- In Site Manager, selected SSH protocol with the public IP address of Linux instance as Host and used Port 22 for connection.
- Logged on the client site by using key file which is used to create the instance above.



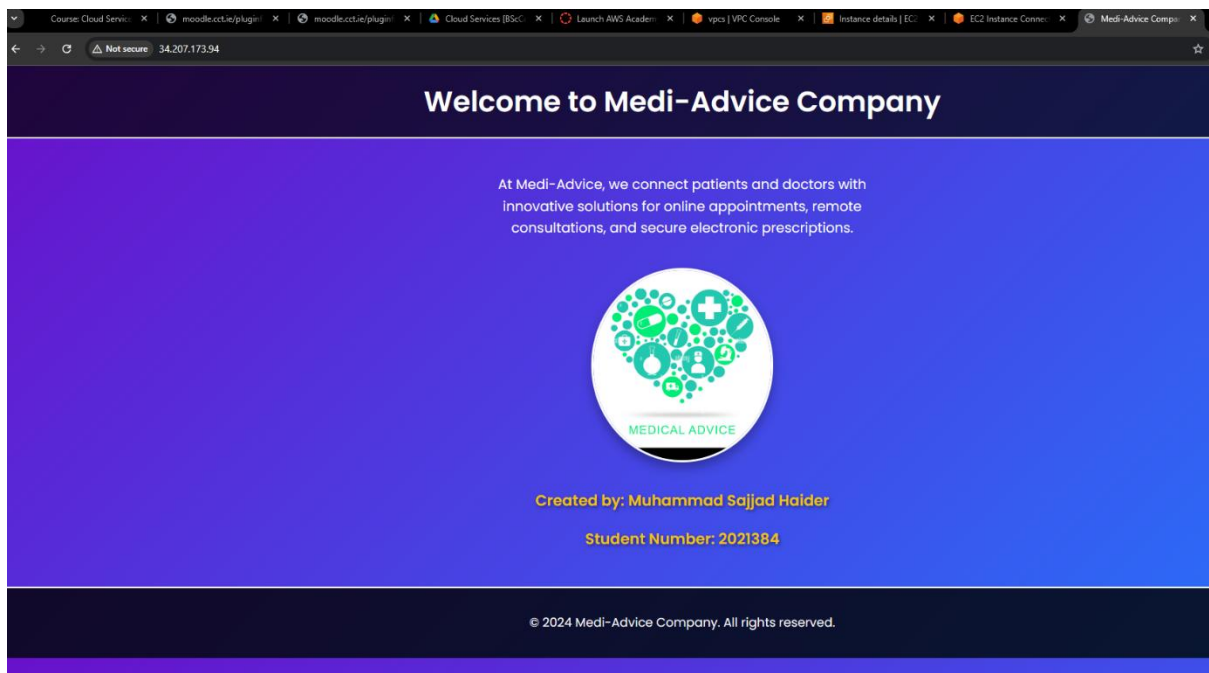
- Connect the Linux instance with EC2 connect and applied the permission commands for the FileZilla to allowed the uploading of Medi-Advice website in Linux server.



- The Medi-Advice website has uploaded on the Linux server successfully.



- Copied and pasted the public IP address of Medi-Advice Linux server in browser and searched, Medi-Advice website worked success.



TASK 5: Content Delivery Network (CDN)

Utilizing Guide on AWS CloudFront CDN to Enhance Availability of Sales Brochures.

In order to enhance the rapid dissemination for their global clients, Medi-Advice's new sales brochure may be cached and distributed to many edge locations around the globe through AWS CloudFront, a CDN. CloudFront reduces client latency and improves content delivery by serving material from the nearest edge location to the end user.

The Functionalist Approach to Understanding How Content Delivery Is Accelerated by AWS CloudFront CDN.

(Google Cloud, n.d.).

1) Essential System element is the usage of Edge Sites for Worldwide Distribution:

CloudFront has an enhanced expansive worldwide network location; such locations are well placed. When a customer wants to download the sales brochure, the material is fed from the nearest edge location possibly an EC2 instance or AWS S3 rather than directly from the source. (loriver.io, 2024).

2) Caching of Content:

The material is only cached at the edge location for the first time after a particular user request for the sales brochure. While the first time a user might request the brochure could involve having to go to a remote server or origin, later requests by other users in the area will require retrieving from this cached content which of course takes much less time for the retrieval process.

3) Decreased Latency:

Since the data between the user and the server takes less time in round-trip, using edge locations of CloudFront is beneficial. For example, to reduce latency by nearly all possible extent, a customer from North America will be served content by CDN edge server from United States rather than the origin server located in Ireland.

4) Enhanced Scalability:

Actually, dealing with such high levels of traffic loads is achieved quite transparently via CloudFront. CloudFront will distribute the load amongst the several edge locations in case there is high traffic demand for the brochure and this will ensure that the server is never overburden and at the same time the brochure will always be available to the customers.

(www.harperdb.io, n.d.).

5) Enhanced Delivery of Content:

To ensure that content delivery is both fast and secure, CloudFront is implemented with additional features to support such as SSL and compression.

Benefit of Medi-Advice CloudFront CDN Use.

Quicker loading times:

Faster loading is a gain for users when the sales brochure is served from the nearest edge point this benefits the user constantly. Foreign customers possibly located far from the main server should take extra precautions in this respect.

Economic Effectiveness:

- Technique EXPERIMENT
- Reliability and approachability
- High and increased availability
- Delivery Scalability

(STL Partners, 2024).

CH-TASK 1: Edge Location content caching of the Medi-Advice brochures

- Firstly, created S3 bucket with name medi-advice-brochure-384.

Create bucket [Info](#)

Buckets are containers for data stored in S3.

General configuration

AWS Region
US East (N. Virginia) us-east-1

Bucket type [Info](#)

☒ **General purpose**
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

☐ **Directory**
Recommended for low-latency use cases, which provides faster performance.

Bucket name [Info](#)

medi-advice-brochure-384

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

- Unblock the all-public access in bucket setting.

Edit Block public access (bucket settings) [Info](#)

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☒ **Block all public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

☐ **Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

☐ **Block public access to buckets and objects granted through any access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.

☐ **Block public access to buckets and objects granted through new public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

☐ **Block public and cross-account access to buckets and objects through any public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

[Cancel](#) [Save changes](#)

- Gave scrip in bucket policy for public access to read the bucket object with the bucket ARN.

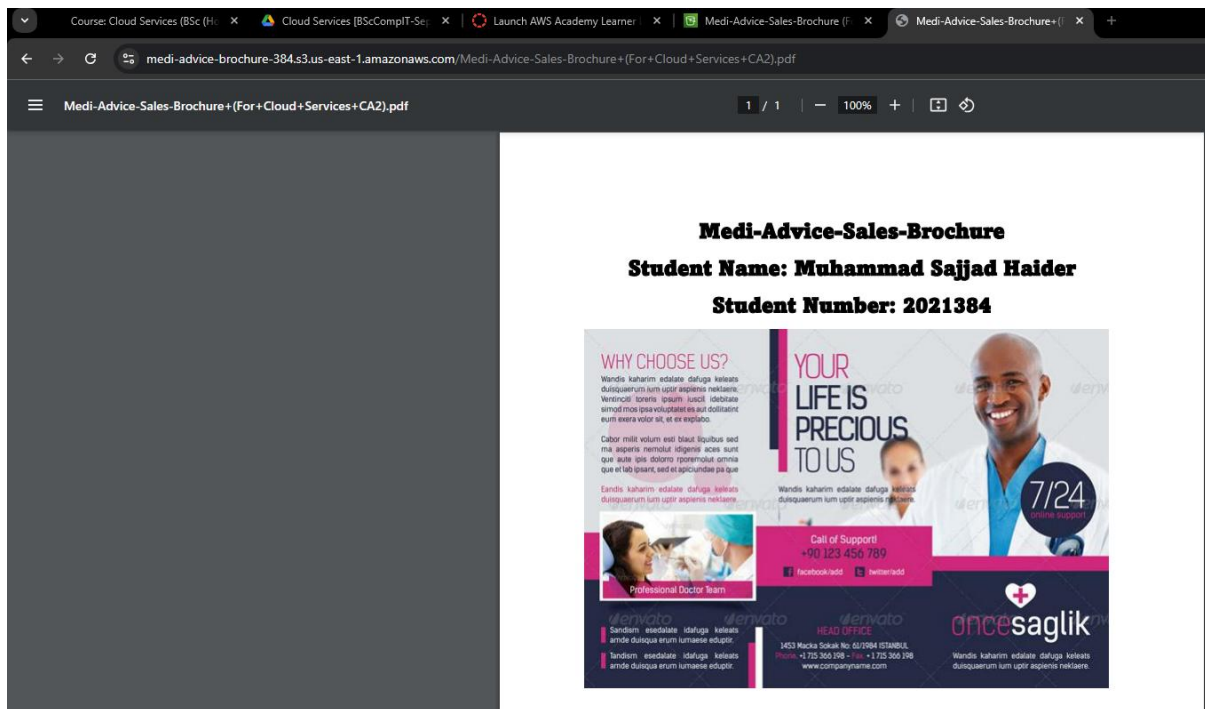
The bucket policy, written in JSON, provides access to the objects stored in the bucket

Bucket ARN
`arn:aws:s3:::medi-advice-brochure-384`

Policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "PublicReadGetObject",  
6       "Effect": "Allow",  
7       "Principal": "*",  
8       "Action": ["s3:GetObject"],  
9       "Resource": ["arn:aws:s3:::medi-advice-brochure-384/*"]  
10    }  
11  ]  
12 }
```

- Copy and pasted the DNS name of medi-advice-brochure-384 bucket in browser and searched it, showed the Medi-Advice-Sales-Brochure with my name and student number.



- In the AWS services, search for CloudFront.
- Click Create Distribution.
- Under Origin domain, paste the S3 bucket URL for the brochure.

Create distribution

Origin

Origin domain
Choose an AWS origin, or enter your origin's domain name. [Learn more](#)

medi-advice-brochure-384.s3.us-east-1.amazonaws.com

Enter a valid DNS domain name, such as an S3 bucket, HTTP server, or VPC origin ID.

Origin path - optional
Enter a URL path to append to the origin domain name for origin requests.

Enter the origin path

Name
Enter a name for this origin.

medi-advice-brochure-384.s3.us-east-1.amazonaws.com

Origin access | Info

☒ Public
Bucket must allow public access.

☐ Origin access control settings (recommended)
Bucket can restrict access to only CloudFront.

☐ Legacy access identities
Use a CloudFront origin access identity (OAI) to access the S3 bucket.

Add custom header - optional
CloudFront includes this header in all requests that it sends to your origin.

[Add header](#)

Enable Origin Shield
Origin shield is an additional caching layer that can help reduce the load on your origin and help protect its availability.

☒ No

☐ Yes

- Set the Viewer Protocol Policy to "Redirect HTTP to HTTPS."

Viewer

Viewer protocol policy

- ☐ HTTP and HTTPS
☒ Redirect HTTP to HTTPS
☐ HTTPS only

Allowed HTTP methods

- For Cache Policy, tried to create new cache policy.
- Set name as MediAdviceCachePolicy and hit create.
- Unfortunately, I got error as a student, I wasn't authorized for this to perform as seen in shots below:

Create cache policy

Details

Name
Enter a name for the cache policy.

Description - optional
Enter a description for the cache policy.

TTL settings [Info](#)

Minimum TTL Minimum time to live in seconds. <input type="text" value="1"/>	Maximum TTL Maximum time to live in seconds. <input type="text" value="31536000"/>	Default TTL Default time to live in seconds. <input type="text" value="86400"/>
--	---	--

Cache key settings [Info](#)

Headers
Choose which headers to include in the cache key.

Query strings
Choose which query strings to include in the cache key.

Cookies
Choose which cookies to include in the cache key.

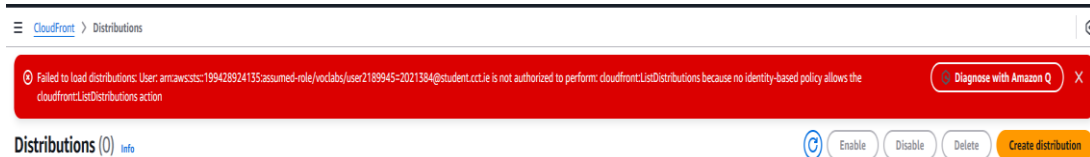
Compression support [Info](#)

☒ Gzip
☒ Brotli

User: am:aws:sts::199428924135:assumed-role/voclabs/user2189946-2021384@student.cct.ie is not authorized to perform: cloudfront:CreateCachePolicy on resource: arn:aws:cloudfront::199428924135:cache-policy/* because no identity-based policy allows the cloudfront:CreateCachePolicy action

[Diagnose with Amazon Q](#)

[Cancel](#) [Create](#)



- But I studied the whole procedure of its deployment as stated below:
- Leave other settings as default and click Create Distribution
- It might take a few minutes for the distribution to deploy.
- Once completed, you'll see a domain name.
- Copy and paste the CloudFront domain name in browser and searched it.
- The brochure should be displayed from the CloudFront edge location.

CH-TASK 2: Medi-advice-private-network (VPC), ALB with ASG:

Practical Work:

- Created VPC by using VPC only option.
- Set name as medi-advice-private-network.

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create [Info](#)
Create only the VPC resource or the VPC and other networking resources.

☒ VPC only ☐ VPC and more

Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify.

IPv4 CIDR block [Info](#)
☒ IPv4 CIDR manual input
☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)
☒ No IPv6 CIDR block
☐ IPAM-allocated IPv6 CIDR block
☐ Amazon-provided IPv6 CIDR block
☐ IPv6 CIDR owned by me

Tenancy [Info](#)

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	value - optional	
<input type="text" value="Name"/>	<input type="text" value="medi-advice-private-network"/>	<input type="button" value="Remove tag"/>

- Created two new public and two new private subnets manually in this VPC.
- Set in US East (N. Virginia) / us-east-1a and us-east-1b two availability zone with network 10.0.0.0/16.

VPC ID
Create subnets in this VPC.

vpc-04d2a3127678cc67f (medi-advice-private-network)

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
Public-Subnet-1
The name can be up to 256 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US East (N. Virginia) / us-east-1a

IPv4 VPC CIDR block [Info](#)
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/16

IPv4 subnet CIDR block
10.0.1.0/24 256 IPs

▼ **Tags - optional**

Key	Value - optional	
Q Name	Public-Subnet-1	Remove

Create subnets in this VPC.

vpc-04d2a3127678cc67f (medi-advice-private-network)

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
Private-Subnet-1
The name can be up to 256 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US East (N. Virginia) / us-east-1a

IPv4 VPC CIDR block [Info](#)
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/16

IPv4 subnet CIDR block
10.0.2.0/24 256 IPs

▼ **Tags - optional**

Key	Value - optional	
Q Name	Private-Subnet-1	Remove

Create subnets in this VPC.

vpc-04d2a3127678cc67f (medi-advice-private-network)

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
Public-Subnet-2
The name can be up to 256 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US East (N. Virginia) / us-east-1b

IPv4 VPC CIDR block [Info](#)
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/16

IPv4 subnet CIDR block
10.0.3.0/24 256 IPs

▼ **Tags - optional**

Key	Value - optional	
Q Name	Public-Subnet-2	Remove

Create subnets in this VPC.

vpc-04d2a3127678cc67f (medi-advice-private-network)

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
Private-Sunet-2
The name can be up to 256 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US East (N. Virginia) / us-east-1b

IPv4 VPC CIDR block [Info](#)
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/16

IPv4 subnet CIDR block
10.0.4.0/24 256 IPs

▼ **Tags - optional**

Key	Value - optional	
Q Name	Private-Sunet-2	Remove

- Enable auto-assign public IPv4 addresses for public subnets in setting.

VPC > Subnets > subnet-0d0be58a1a2084939 > Edit subnet settings

Edit subnet settings [Info](#)

Subnet

Subnet ID	Name
subnet-0d0be58a1a2084939	Public-Subnet-1

Auto-assign IP settings [Info](#)

Enable AWS to automatically assign a public IPv4 or IPv6 address to a new primary network interface for an instance in this subnet.

☒ **Enable auto-assign public IPv4 address [Info](#)**

☐ **Enable auto-assign customer-owned IPv4 address [Info](#)**

Option disabled because no customer owned pools found.

- Created New Internet Gateway with name medi-advice-igw.

VPC > Internet gateways > Create internet gateway

Create internet gateway [Info](#)

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag

Creates a tag with a key of 'Name' and a value that you specify.

medi-advice-igw

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional	
Name	medi-advice-igw	Remove

Add new tag

You can add 49 more tags.

Cancel **Create internet gateway**

- Attached Internet Gateway with medi-advice-private-network VPC.

VPC > Internet gateways > Attach to VPC (igw-0e6da66ef736a1d1a)

Attach to VPC (igw-0e6da66ef736a1d1a) [Info](#)

VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs

Attach the internet gateway to this VPC.

vpc-04d2a3127678cc67f

Use: "vpc-04d2a3127678cc67f"

vpc-04d2a3127678cc67f - medi-advice-private-network

Cancel **Attach internet gateway**

- Navigate route tables in VPC, created a public route with name medi-advice-public-rt and attached the medi-advice-private-network VPC.

VPC > Route tables > Create route table

Create route table [Info](#)

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - optional
Create a tag with a key of 'Name' and a value that you specify.

medi-advice-public-rt

VPC
The VPC to use for this route table.

vpc-04d2a3127678cc67f (medi-advice-private-network)

Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key: Name Value - optional: medi-advice-public-rt

[Add new tag](#)

You can add 49 more tags.

Cancel [Create route table](#)

- Associated the public subnets only with this route table.

VPC > Route tables > rtb-0a643d03286592296 > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/4)

Filter subnet associations

	Name	Subnet ID	IP
<input checked="" type="checkbox"/>	Public-Subnet-1	subnet-0d0be58a1a2084939	10.0.0.0/16
<input checked="" type="checkbox"/>	Public-Subnet-2	subnet-067949c101c4646ce	10.0.0.0/16
<input type="checkbox"/>	Private-Subnet-1	subnet-003e848ebde257e39	10.0.0.0/16
<input type="checkbox"/>	Private-Subnet-2	subnet-05c11bf19a4a3035a	10.0.0.0/16

Selected subnets

subnet-0d0be58a1a2084939 / Public-Subnet-1

subnet-067949c101c4646ce / Public-Subnet-2

- Add route in edit routes setting, routed it with medi-advice-igw Internet gateway.

VPC > Route tables > rtb-0a643d03286592296 > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	Internet Gateway	-	No

[Add route](#)

igw-0e6da66ef736a1d1a (medi-advice-igw)

Cancel [Preview](#) [Save](#)

- Created a private route table with name medi-advice-private-rt and attached the medi-advice-private-network VPC as did above for public route.
- Associated the private subnets only with this route table.

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/4)

Filter subnet associations

	Name	Subnet ID	IPv4 CIDR
<input type="checkbox"/>	Public-Subnet-1	subnet-0d0be58a1a2084939	10.0.1.0/24
<input type="checkbox"/>	Public-Subnet-2	subnet-067949c101c4646ce	10.0.3.0/24
<input checked="" type="checkbox"/>	Private-Subnet-1	subnet-003e848ebde257e39	10.0.2.0/24
<input checked="" type="checkbox"/>	Private-Subnet-2	subnet-05c11bf19a4a3035a	10.0.4.0/24

Selected subnets

subnet-003e848ebde257e39 / Private-Subnet-1 X subnet-05c11bf19a4a3035a / Private-Subnet-2 X

- Created new Linux-instance with name Private-instance-384.

Name and tags

Name: Private-instance-384 Add additional tags

Application and OS Images (Amazon Machine Image)

An AMI is a template that contains the software configuration (operating system, application server, and applications) to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Recents Quick Start

Amazon Linux
aws

macOS
Mac

Ubuntu
ubuntu

Windows
Microsoft

Red Hat
Red Hat

SUSE Linux
SUSE

Browse more
Including AMI
AWS, Marketpl
the Comm

- User data will display Welcome page with my student number 2021384.

User data - optional

Upload a file with your user data or enter it in the field.

Choose file

```

sudo yum update -y
sudo yum install httpd -y
sudo systemctl start httpd
sudo systemctl enable httpd
echo "<h1>Welcome to Medi-Advice-2021384</h1>" | sudo tee
/var/www/html/index.html

```

- Created new Application Load Balancer with name medi-advice-alb-384.

► How Application Load Balancers work

Basic configuration

Load balancer name
Name must be unique within your AWS account and can't be changed after the load balancer is created.

medi-advice-alb-384

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Scheme | Info
Scheme can't be changed after the load balancer is created.

☒ **Internet-facing**

- Serves internet-facing traffic.
- Has public IP addresses.
- DNS name is publicly resolvable.
- Requires a public subnet.

☐ **Internal**

- Serves internal traffic.
- Has private IP addresses.
- DNS name is not publicly resolvable.
- Compatible with the IPv4 and Dualstack IP address types.

Load balancer IP address type | Info
Select the front-end IP address type to assign to the load balancer. The VPC and subnets mapped to this load balancer must include the selected IP address types. Public

☒ **IPv4**
Includes only IPv4 addresses.

☐ **Dualstack**
Includes IPv4 and IPv6 addresses.

☐ **Dualstack without public IPv4**
Includes a public IPv6 address, and private IPv4 and IPv6 addresses. Compatible with internet-facing load balancers only.

- Selected medi-advice-private-network VPC with public subnets in Network.

Network mapping

The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

VPC | Info
The load balancer will exist and scale within the selected VPC. The selected VPC is also where the load balancer targets must be hosted unless routing to a VPC for your targets, view [target groups](#). For a new VPC, [create a VPC](#).

medi-advice-private-network
vpc-04d2a3127678cc67f
IPv4 VPC CIDR: 10.0.0.0/16

Mappings | Info
Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability Zones available for selection.

Availability Zones

☒ **us-east-1a (use1-az6)**

Subnet

subnet-0d0be58a1a2084939
IPv4 subnet CIDR: 10.0.1.0/24

Public-Subnet-1

IPv4 address
Assigned by AWS

☒ **us-east-1b (use1-az1)**

Subnet

subnet-067949c101c4646ce
IPv4 subnet CIDR: 10.0.3.0/24

Public-Subnet-2

IPv4 address
Assigned by AWS

- Created a new target group with name medi-advice-tg-384 with HTTP 80.

Target group name

medi-advice-tg-384

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Protocol : Port
Choose a protocol for your target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now include mitigation options once your target group is created. This choice cannot be changed after creation

HTTP

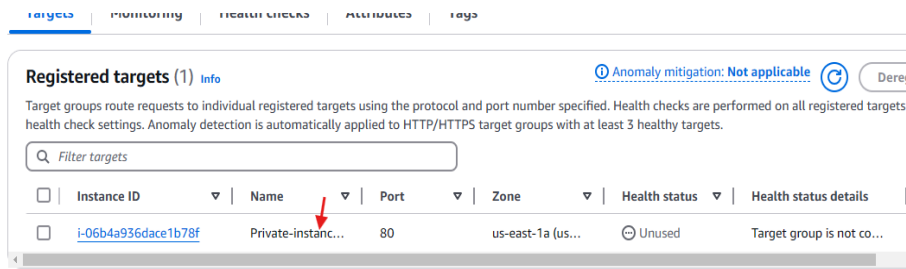
80

1-65535

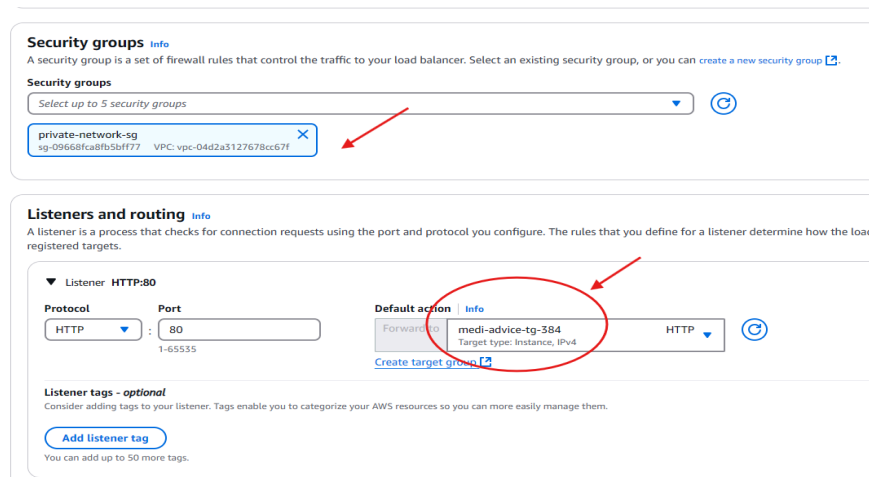
IP address type
Only targets with the indicated IP address type can be registered to this target group.

☒ **IPv4**
Each instance has a default network interface (eth0) that is assigned the primary private IPv4 address. The

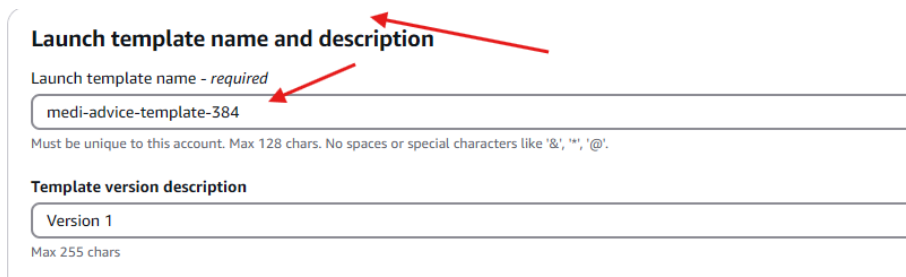
- Add private-instance-384 Linux server as registered in target group.



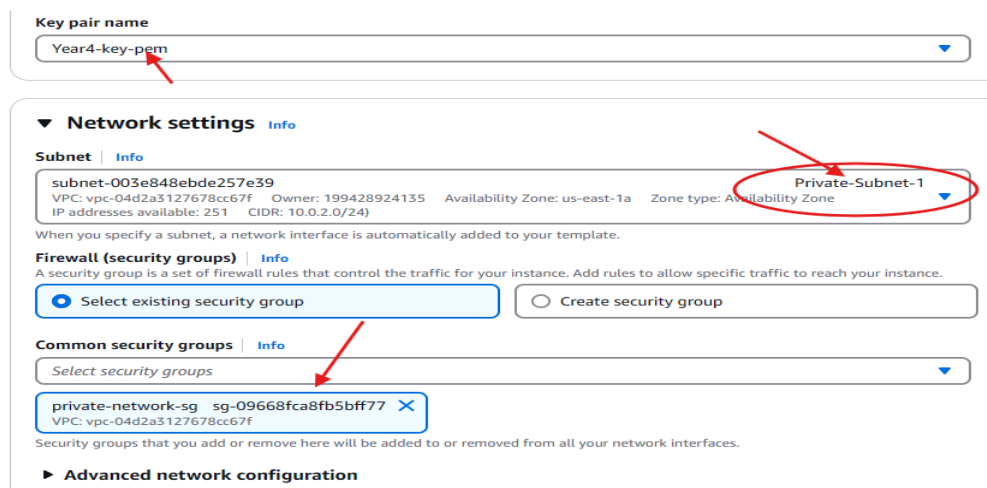
- Go back in ALB, Attached the newly created security group (private-network-sg) and target group (medi-advice-tg-384) by editing.



- Created Launch template with name medi-advice-template-384.



- Selected Private-Subnet-1 for Launch template with private-network-sg.



- Created Auto scaling group with name medi-advice-asg-384.
- Attached above created medi-advice-template-384.

Choose launch template [Info](#)

Specify a launch template that contains settings common to all EC2 instances that are launched by this Auto Scaling group.

Name

Auto Scaling group name
Enter a name to identify the group.

medi-advice-asg-384

Must be unique to this account in the current Region and no more than 255 characters.

Launch template [Info](#)

For accounts created after May 31, 2023, the EC2 console only supports creating Auto Scaling groups with launch templates. Creating Auto Scaling groups with launch configurations is not recommended but still available via the CLI and API until December 31, 2023.

Launch template
Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.

medi-advice-template-384

[Create a launch template](#)

Version

Default (1)

- Attached medi-advice-private-network VPC with Private subnets only.

Network [Info](#)

For most applications, you can use multiple Availability Zones and let EC2 Auto Scaling balance your instances across them. For applications that require high availability, you can use multiple Availability Zones and let EC2 Auto Scaling balance your instances across them. For applications that require high availability, you can use multiple Availability Zones and let EC2 Auto Scaling balance your instances across them.

VPC
Choose the VPC that defines the virtual network for your Auto Scaling group.

vpc-04d2a3127678cc67f (medi-advice-private-network)
10.0.0.0/16

[Create a VPC](#)

Availability Zones and subnets
Define which Availability Zones and subnets your Auto Scaling group can use in the chosen VPC.

Select Availability Zones and subnets

us-east-1a | subnet-003e848ebde257e39 (Private-Subnet-1)
10.0.2.0/24

us-east-1b | subnet-05c11bf19a4a3035a (Private-Subnet-2)
10.0.4.0/24

[Create a subnet](#)

- Attached ALB, configured above with target group (medi-advice-tg-384).

Load balancing [Info](#)

Use the options below to attach your Auto Scaling group to an existing load balancer, or to a new load balancer that you create.

☐ No load balancer
Traffic to your Auto Scaling group will not be fronted by a load balancer.

☒ Attach to an existing load balancer
Choose from your existing load balancers.

☐ Attach to a new load balancer
Quickly create a basic load balancer and attach it to your Auto Scaling group.

Attach to an existing load balancer
Select the load balancers that you want to attach to your Auto Scaling group.

☒ Choose from your load balancer target groups
This option allows you to attach Application, Network, or Gateway Load Balancers.

☐ Choose from Classic Load Balancers

Existing load balancer target groups
Only instance target groups that belong to the same VPC as your Auto Scaling group are available for selection.

Select target groups

medi-advice-tg-384 | HTTP
Application Load Balancer: medi-advice-alb-384

- Set scaling capacities, desired 3, min 2 and max 5.

Configure group size and scaling - optional [Info](#)

Define your group's desired capacity and scaling limits. You can optionally add automatic

Group size [Info](#)

Set the initial size of the Auto Scaling group. After creating the group, you can change automatic scaling.

Desired capacity type

Choose the unit of measurement for the desired capacity value. vCPUs and Memory(GiB) are only s instance attributes.

Units (number of instances)

Desired capacity

Specify your group size.

3

Scaling [Info](#)

You can resize your Auto Scaling group manually or automatically to meet changes in

Scaling limits

Set limits on how much your desired capacity can be increased or decreased.

Min desired capacity

2

Equal or less than desired capacity

Max desired capacity

5

Equal or greater than desired capacity

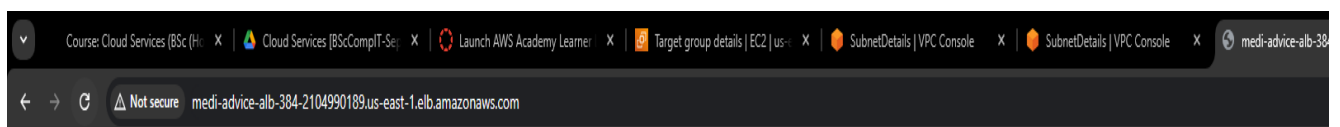
- Instances are automatically launching again after termination, indicating the successful working of auto scaling group.

Instances (3/18) [Info](#)

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

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input type="checkbox"/>		i-00bb751a1c50b6c17	Terminated	t2.micro	-	View alarms	us-east-1b
<input checked="" type="checkbox"/>		i-07b6ec9b6791dab18	Running	t2.micro	2/2 checks passed	View alarms	us-east-1b
<input type="checkbox"/>		i-016a430ae2a1f3914	Terminated	t2.micro	-	View alarms	us-east-1b
<input type="checkbox"/>		i-0bdf8cca55d72295e	Terminated	t2.micro	-	View alarms	us-east-1b
<input checked="" type="checkbox"/>		i-0ae71d9e19c75a3ae	Running	t2.micro	2/2 checks passed	View alarms	us-east-1b
<input type="checkbox"/>		i-0b16a15404e0f596f	Terminated	t2.micro	-	View alarms	us-east-1b
<input type="checkbox"/>		i-00c7bc8a823864131	Terminated	t2.micro	-	View alarms	us-east-1b
<input type="checkbox"/>		i-0b67bcf3f4e13d05	Terminated	t2.micro	-	View alarms	us-east-1b
<input type="checkbox"/>		i-08f51c2cb08b9e203	Terminated	t2.micro	-	View alarms	us-east-1b
<input type="checkbox"/>		i-0acc864c388b6a6f1	Terminated	t2.micro	-	View alarms	us-east-1b
<input type="checkbox"/>		i-0141c2ad3951cd8fd	Terminated	t2.micro	-	View alarms	us-east-1a
<input type="checkbox"/>		i-0864ae0af8d3418af	Terminated	t2.micro	-	View alarms	us-east-1a
<input type="checkbox"/>		i-01a58139cc1844a0d	Terminated	t2.micro	-	View alarms	us-east-1a
<input checked="" type="checkbox"/>		i-0398dc16ad700afaa	Running	t2.micro	2/2 checks passed	View alarms	us-east-1a

- Copy the DNS name of ALB and searched on browser.
- Showed the Welcome page with my student number 2021384.
- It distributed the traffic through instances by refreshing again and again.



Welcome to Medi-Advice 2021384 ip-10-0-1-230.ec2.internal

Load-Balancer integration with Auto-scaler benefits:

For a healthcare company like Medi-Advice, merging an Auto Scaling Group together with a Load Balancer brings a lot of anticipated benefits in terms of application's availability, performance, and use of resources in a cost-effective manner.

Improved Availability and Reliability:

A Load Balancer ensures that the expected traffic is satisfactorily served and, in the case of a server losing connectivity, it intelligently routes traffic to other available servers - ever helping to keep the desired application up and running. This is very crucial in the context of health services in which the existence of the application is critical to patients.

Cost effectiveness and system growth:

When there is a drop in traffic Auto Scaling reduces the number of servers, whereas, during peak traffic it increases the number of servers. In this manner, application performance is maintained while the number of servers is increased whenever it is required or minimized when usage is lower, resulting in decreased expenses. In this way, Medi-Advice will be able to use the required resources within a specified time and no more which is economically sound.

Prevention of Information Leakage and Compliance:

Encryption can be made much stronger through the addition of Load Balancers because they perform SSL/TLS, so fewer certificates need to be processed and back-end servers require less computation power. This is very important in the healthcare industry since patients' personal information must be safeguarded.

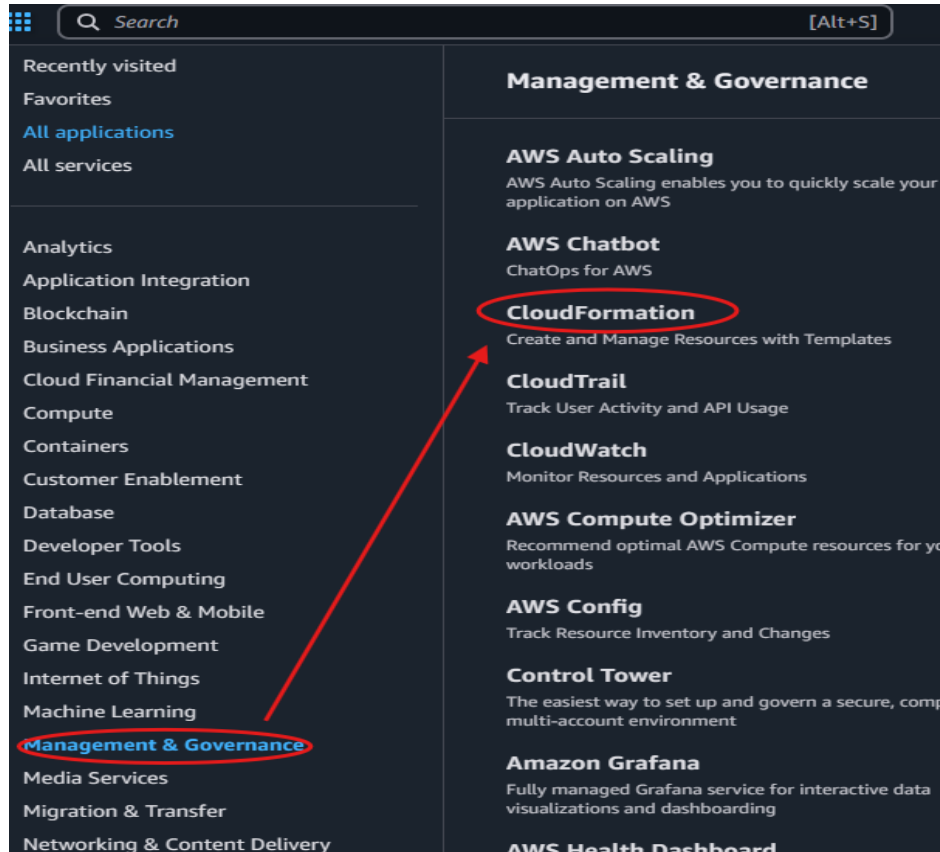
Reduced Manual Efforts:

Combining Load Balancers with Auto Scaling lessens human supervision and inputs. Instead, it streamlines the maintenance of the desired volume of servers and traffic distribution, allowing IT staff to focus on strategic initiatives rather than routine maintenance.

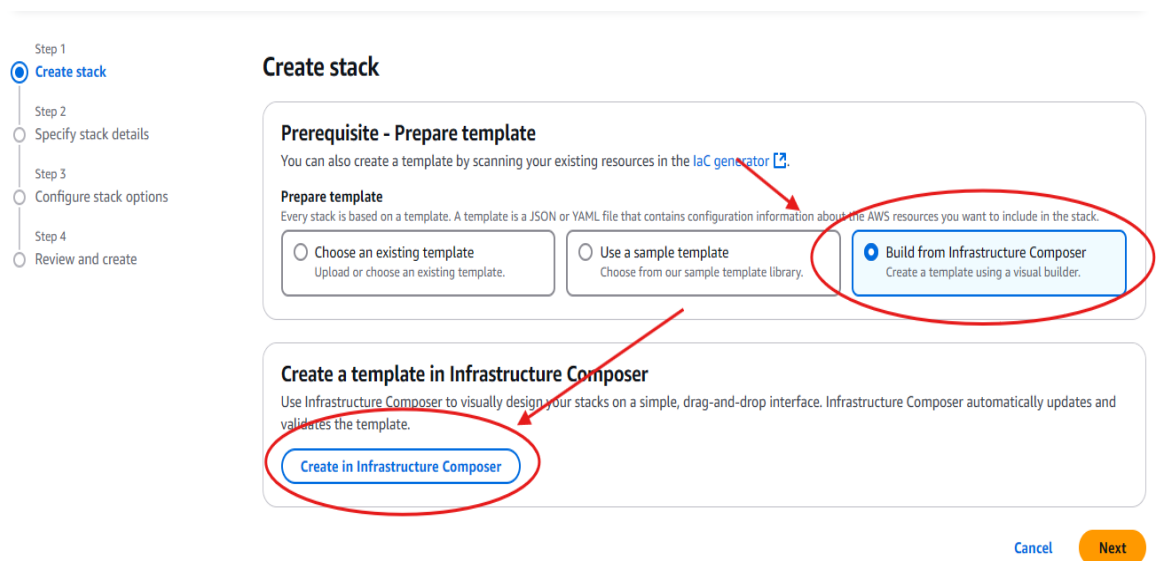
CH-TASK 3: AWS Cloud Formation (Infrastructure as code)

A1: Deployment of VPC using AWS CloudFormation template:

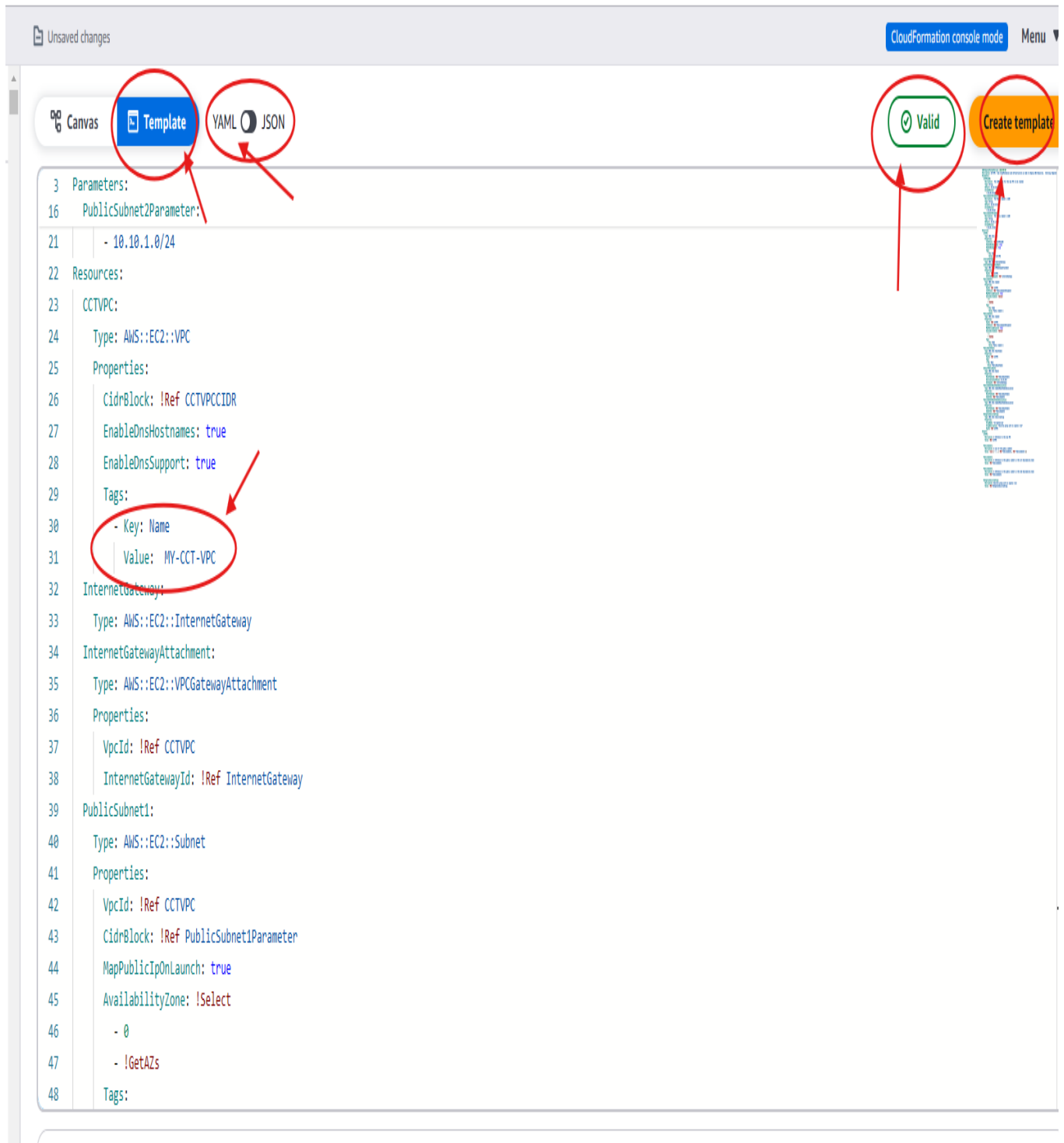
- Navigate CloudFormation from Management & Governance services.



- Create stack, selected 'Build from Infrastructure Composer' option.
- Open blue highlighted below option of create as shown in shot below with red circle.



- Selected Template option with YAML code.
- Gave YAML code for creating the new VPC with name MY-CCT-VPC.
- Checked Validity of code and hit create template.



- Set stack name as My-yaml-vpc.
- Left the other settings default, review and create.

Step 1
● Create stack

Step 2
● Specify stack details

Step 3
○ Configure stack options

Step 4
○ Review and create

Specify stack details

Provide a stack name

Stack name

My-yaml-vpc

Stack name must be 1 to 128 characters, start with a letter, and only contain alphanumeric characters. Character count: 11/128.

- It can be seen that My-yaml-vpc stack is successfully created.

Stacks (3)

Filter by stack name

Filter status: Active

View nested

Stack name	Status	Created time	Description
My-yaml-vpc	CREATE_COMPLETE	2024-11-29 23:17:55 UTC+0000	CCT-VPC - Use CloudFormation and Infrastructure as Code to Deploy AWS Resources. Starting template with VPC.
JSON-cloudformation-vpc	ROLLBACK_COMPLETE	2024-11-29 23:08:06 UTC+0000	-
c134587a3413854l7761777t1w199428924135	CREATE_COMPLETE	2024-09-28 11:33:57 UTC+0100	associate Learner Lab template (academy)

- Navigate VPC from services and verified that the new MY-CCT-VPC has successfully created and showed.

Virtual private cloud

Your VPCs (1/4)

Name	VPC ID	State	Block Public...	IPv4 CIDR	IPv6 CIDR	DHCP option set	Main route ta
-	vpc-03a413d600aa12a2	Available	Off	172.31.0.0/16	-	dopt-007e990ab4ad4c...	rtb-047dc36a
MediAdviceVPC-vpc	vpc-05154a14f867f8d97	Available	Off	10.0.0.0/16	-	dopt-007e990ab4ad4c...	rtb-0a4eaf26f
medi-advice-private-network	vpc-04d2a3127678cc67f	Available	Off	10.0.0.0/16	-	dopt-007e990ab4ad4c...	rtb-01b79603
MY-CCT-VPC	vpc-058ae3ae047e0a553	Available	Off	10.10.0.0/16	-	dopt-007e990ab4ad4c...	rtb-05262bac

Code Explanation:

Parameters:

- CCTVPCCIDR is CIDR block for the VPC.
- PublicSubnet1Parameter and PublicSubnet2Parameter are CIDR blocks for public subnets.

Resources:

- VPC (CCTVPC) with the specified CIDR block.
- Internet Gateway for internet access.
- InternetGatewayAttachment to attach the Internet Gateway with VPC.
- Creates two public subnets across different Availability Zones with public IP mapping enabled.
- Creates a route table for the public subnets.
- Adds a default route to the Internet Gateway in the route table.
- Associates each public subnet with the public route table.
- Creates a security group with no ingress rules.

Outputs:

- References to the created VPC, public subnets, and the security group.
- Outputs are helpful for accessing resource IDs after stack creation.

A2: Linux EC2 instance in new VPC:

- Created a new Linux-instance with name my-cloudformation-instance.

EC2 > Instances > Launch an instance

Name and tags [Info](#)

Name
my-cloudformation-instance [Add additional tags](#)

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Recents **Quick Start**

Amazon Linux [aws](#) macOS [Mac](#) Ubuntu [ubuntu](#) Windows [Microsoft](#) Red Hat [Red Hat](#) SUSE Linux [SUSE](#)

[Browse more AMIs](#)
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

- Selected MY-CCT-VPC which is created above through CloudFormation.

▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-058ae3ea047e8a553 (MY-CCT-VPC)
10.10.0.0/16

Search

vpc-03a413fd600aa12a2 (default)
172.31.0.0/16

vpc-05154a14f867f8d97 (MediAdviceVPC-vpc)
10.0.0.0/16

vpc-04d2a3127678cc67f (medi-advice-private-network)
10.0.0.0/16

vpc-058ae3ea047e8a553 (MY-CCT-VPC)
10.10.0.0/16

[Create new subnet](#)

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance

☒ Create security group ☐ Select existing security group

- User data to display html page.

User data - optional | [Info](#)
Upload a file with your user data or enter it in the field.

[Choose file](#)

```
#!/bin/bash
yum update -y
yum install httpd -y
service httpd start
chkconfig httpd on
cd /var/www/html
echo "<html><h1> This is Cloudformation VPC - Server $(hostname -f) </h1>
</html>" > index.html
```

- New instance has created successfully inside MY-CCT-VPC.

	Name	Instance ID	Instance state	Instance type	Status check
<input checked="" type="checkbox"/>	my-cloudformation-inst...	i-094fer067811614e9	Running	t2.micro	2/2 checks passed
<input type="checkbox"/>		i-06ca4c3185b4d2914	Terminated	t2.micro	-

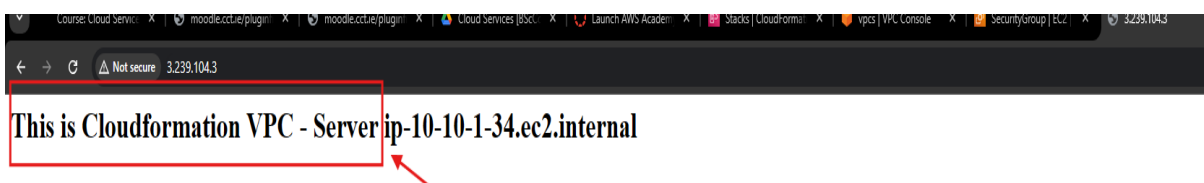
- Added HTTP and HTTPS rule in security group which used for instance.

Edit inbound rules | [Info](#)
Inbound rules control the incoming traffic that's allowed to reach the instance.

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sgr-03029a9ebee7b8812	HTTP	TCP	80	Cu...	
sgr-09c0a2df010140673	HTTPS	TCP	443	Cu...	
sgr-0e0dff99ae5a411f9	SSH	TCP	22	Cu...	

[Add rule](#)

- Linux-server is running successfully.



B1: Advantage of using CloudFormation to create VPC:

Well, there are a number of benefits that come available through setting up a custom VPC using AWS CloudFormation: In terms of automation and repeatability, namely.

In code, define your infrastructure, and CloudFormation makes it even easier for you to deploy, manage, and maintain a standardized VPC across your different environments. A similar configuration in many AWS accounts or regions in a twinkling of an eye without typing the settings manually again after as soon as you define them in a CloudFormation template JSON or YAML format. By adopting this method, the assurance of deploying the infrastructure in the right manner every time is achieved while in the process reducing the time and effort required to put up this infrastructure and also reducing the impact that human element would have on the entire process. Version control is also accomplished easily, and the changes in infrastructure can be monitored and administered more effectively over a given period.

(Reliability Pillar AWS Well-Architected Framework, n.d.)

B2: Supporting Example for CloudFormation:

Suppose one of the production environments of a total production system of a company really fails critically. Using CloudFormation, if this tool were not there, it would mean going through a recovery procedure whereby even the VPC and subnets, EC2 instances, security groups and so on were all configured from the scratch by way of a very time-consuming process. It may take longer time and may be rife with a number of errors and non-re-usable.

However, CloudFormation holds all of the definitions in a single template of as-code infrastructure. Failure to the same can be easily rectified as the CloudFormation template is just used to load the same infrastructure again in just a few minutes. This reduces recover time and offers highly replicative and consistent environment for the deployment.

(Amazon Web Services, n.d.)

References:

- AWS (2019). Amazon Relational Database Service (RDS) – AWS. [online] Amazon Web Services, Inc. Available at: <https://aws.amazon.com/rds/>.
- Cloud Academy. (n.d.). Cloud Training That Drives Digital Transformation. [online] Available at: <https://cloudacademy.com/>.
- Cloud Computing News. (n.d.). Cloud Tech News | Cloud Computing News, Analysis & Events. [online] Available at: <https://www.cloudcomputing-news.net/>.
- searchaws.techtarget.com. (n.d.). Amazon Web Services (AWS) news and technology information – SearchAWS.com. [online] Available at: <https://searchaws.techtarget.com/>.
- InformationWeek. (n.d.). Cloud Computing & IT Infrastructure News | page 1 of 683. [online] Available at: <https://www.informationweek.com/cloud>.
- www.tutorialspoint.com. (n.d.). Cloud Computing Tutorial. [online] Available at: https://www.tutorialspoint.com/cloud_computing/.
- Amazon Web Services. (2020). Why Deployment Requirements are Important When Making Architectural Choices | Amazon Web Services. [online] Available at: <https://aws.amazon.com/blogs/architecture/why-deployment-requirements-are-important-when-making-architectural-choices/> [Accessed 3 Dec. 2024].
- docs.aws.amazon.com. (n.d.). Appendix: 21 CFR 11 Controls – Shared Responsibility for use with AWS services - GxP Systems on AWS. [online] Available at: <https://docs.aws.amazon.com/whitepapers/latest/gxp-systems-on-aws/appendix-21-cfr-11-controls-shared-responsibility-for-use-with-aws-services.html>.
- The (2011). The difference between best practices and common sense? [online] Software Engineering Stack Exchange. Available at: <https://softwareengineering.stackexchange.com/questions/95482/the-difference-between-best-practices-and-common-sense> [Accessed 3 Dec. 2024].
- Reliability Pillar AWS Well-Architected Framework. (n.d.). Available at: <https://docs.aws.amazon.com/wellarchitected/latest/reliability-pillar/wellarchitected-reliability-pillar.pdf>.
- Amazon Web Services (2023). What Is Amazon VPC? - Amazon Virtual Private Cloud. [online] Amazon.com. Available at: <https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html>.
- STL Partners. (2024). Edge content delivery: The most mature edge computing use case today. [online] Available at: <https://stlpartners.com/articles/edge-computing/edge-content-delivery-the-most-mature-edge-computing-use-case-today/> [Accessed 3 Dec. 2024].
- HashiCorp (n.d.). What is infrastructure as code and why is it important? [online] HashiCorp. Available at: <https://www.hashicorp.com/resources/what-is-infrastructure-as-code>.
- AWS (2019). Disaster Recovery. [online] Amazon Web Services, Inc. Available at: <https://aws.amazon.com/disaster-recovery/>.
- AWS (2017). AWS CloudFormation - Infrastructure as Code & AWS Resource Provisioning. [online] Amazon Web Services, Inc. Available at: <https://aws.amazon.com/cloudformation/>