

Project-503 : Blog Page Application (Django) deployed on AWS Application Load Balancer with Auto Scaling, S3, Relational Database Service(RDS), VPC's Components, Lambda, DynamoDB and Cloudfront with Route 53

Description

The Clarusway Blog Page Application aims to deploy blog application as a web application written Django Framework on AWS Cloud Infrastructure. This infrastructure has Application Load Balancer with Auto Scaling Group of Elastic Compute Cloud (EC2) Instances and Relational Database Service (RDS) on defined VPC. Also, The Cloudfront and Route 53 services are located in front of the architecture and manage the traffic in secure. User is able to upload pictures and videos on own blog page and these are kept on S3 Bucket. This architecture will be created by Firms DevOps Guy.

Problem Statement

- Your company has recently ended up a project that aims to serve as Blog web application on isolated VPC environment. You and your colleagues have started to work on the project. Your Developer team has developed the application and you are going to deploy the app in production environment.
- Application is coded by Clarusway Fullstack development team and given you as DevOps team. App allows users to write their own blog page to whom user registration data should be kept in separate MySQL database in AWS RDS service and pictures or videos should be kept in S3 bucket. The object list of S3 Bucket containing movies and videos is recorded on DynamoDB table.
- The web application will be deployed using Django framework.
- The Web Application should be accessible via web browser from anywhere in secure.
- You are requested to push your program to the project repository on the Github. You are going to pull it into the webservers in the production environment on AWS Cloud.

In the architecture, you can configure your infrastructure using the followings,

- The application stack should be created with new AWS resources.
- Specifications of VPC:
 - VPC has two AZs and every AZ has 1 public and 1 private subnets.
 - VPC has Internet Gateway
 - One of public subnets has NAT Instance.
 - You might create new instance as Bastion host on Public subnet or you can use NAT instance as Bastion host.
 - There should be managed private and public route tables.
 - Route tables should be arranged regarding of routing policies and subnet associations based on public and private subnets.
- You should create Application Load Balancer with Auto Scaling Group of Ubuntu 18.04 EC2 Instances within created VPC.
- You should create RDS instance within one of private subnets on created VPC and configure it on application.
- The Auto Scaling Group should use a Launch Template in order to launch instances needed and should be configured to;
 - use all Availability Zones on created VPC.
 - set desired capacity of instances to 2
 - set minimum size of instances to 2
 - set maximum size of instances to 4
 - set health check grace period to 90 seconds
 - set health check type to ELB
 - Scaling Policy --> Target Tracking Policy
 - Average CPU utilization (set Target Value %70)
 - seconds warm up before including in metric ---> 200
 - Set notification to your email address for launch, terminate, fail to launch, fail to terminate instance situations
- ALB configuration;

- Application Load Balancer should be placed within a security group which allows HTTP (80) and HTTPS (443) connections from anywhere.
- Certification should be created for secure connection (HTTPS)
 - To create certificate, AWS Certificate Manager can be utilized.
- ALB redirects to traffic from HTTP to HTTPS
- Target Group
 - Health Check Protocol is going to be HTTP
- The Launch Template should be configured to;
 - Prepare Django environment on EC2 instance based on Developer Notes,
 - Download the "clarusway_aws_capstone" folder from Github repository,
 - Install the requirements using requirements.txt in 'clarusway_aws_capstone' folder
 - Deploy the Django application on port 80.
 - Launch Template only allows HTTP (80) and HTTPS (443) ports coming from ALB Security Group and SSH (22) connections from anywhere.
 - EC2 Instances type can be configured as t2.micro.
 - Instance launched should be tagged Clarusway AWS Capstone Project
 - Since Django App needs to talk with S3, S3 full access role must be attached EC2s.
- For RDS Database Instance;
 - Instance type can be configured as db.t2.micro
 - Database engine can be MySQL with version of 8.0.20.
 - RDS endpoint should be addressed within settings file of blog application that is explained developer notes.
 - Please read carefully "Developer notes" to manage RDS sub settings.
- Cloudfront should be set as a cache server which points to Application Load Balance with following configurations;
 - The cloudfront distribution should communicate with ALB securely.
 - Origin Protocol policy can be selected as HTTPS only.
 - Viewer Protocol Policy can be selected as Redirect HTTP to HTTPS
- As cache behavior;
 - GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE methods should be allowed.
 - Forward Cookies must be selected All.
 - Newly created ACM Certificate should be used for securing connections. (You can use same certificate with ALB)
- Route 53
 - Connection must be secure (HTTPS).
 - Your hostname can be used to publish website.
 - Failover routing policy should be set while publishing application
 - Primary connection is going to be Cloudformation
 - Secondary connection is going to be a static website placed another S3 bucket. This S3 bucket has just basic static website that has a picture said "the page is under construction" given files within S3_static_Website folder
 - Healthcheck should check If Cloudfront is healthy or not.
- As S3 Bucket
 - First S3 Bucket
 - It should be created within the Region that you created VPC
 - Since development team doesn't prefer to expose traffic between S3 and EC2s on internet, Endpoint should be set on created VPC.
 - S3 Bucket name should be addressed within configuration file of blog application that is explained developer notes.
 - Second S3 Bucket

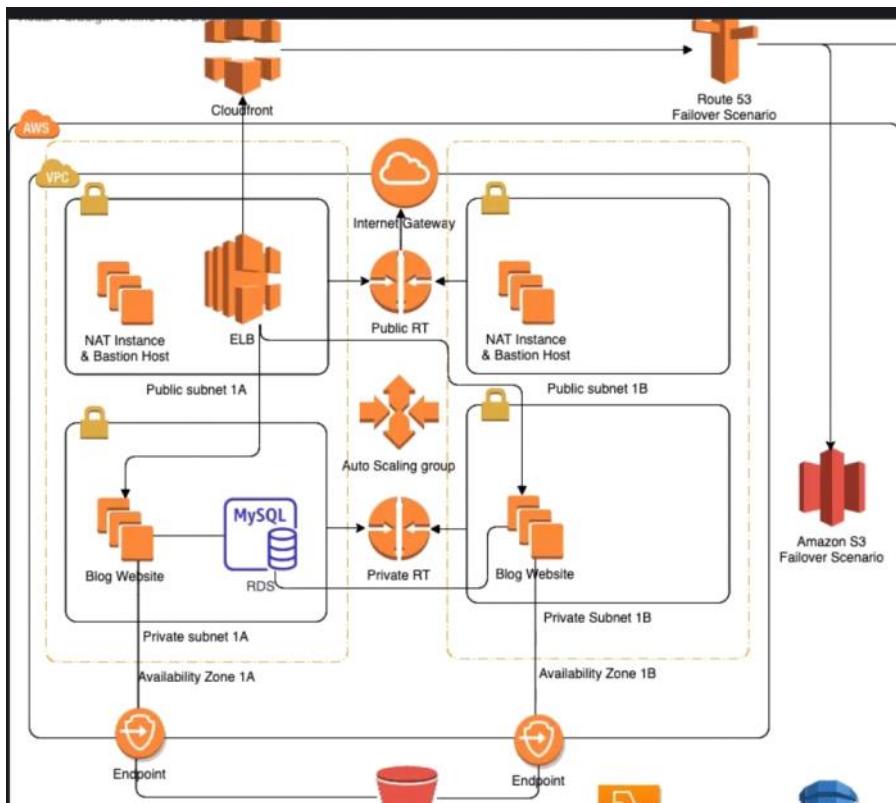
- This Bucket is going to be used for failover scenario. It has just a basic static website that has a picture said "the page is under construction"
- To write the objects of S3 on DynamoDB table
 - Lambda Function
 - Lambda function is going to be Python 3.8
 - Python Function can be found in github repo
 - S3 event is set as trigger
 - Since Lambda needs to talk S3 and DynamoDB and to run on created VPC, S3, DynamoDB full access policies and NetworkAdministrator policy must be attached it
 - S3 Event must be created first S3 Bucket to trigger Lambda function
 - DynamoDB Table
 - Create a DynamoDB table which has primary key that is id
 - Created DynamoDB table's name should be placed on Lambda function.

Project Skeleton

```
clarusway_blog_proj (folder)
|
|---Readme.md      # Given to the students (Definition of the
|   project)
|---src (folder)    # Given to the students (Django Application's )
|---requirements.txt # Given to the students (txt file)
|---lambda_function.py # Given to the students (python file)
|---developer_notes.txt # Given to the students (txt file)
```

Expected Outcome

From <[https://github.com/clarusway/clarusway-aws-8-21/tree/main/aws/projects/Project-503-Capstone-Project-Blog-Page-App-\(Django\)-on-AWS-Environment](https://github.com/clarusway/clarusway-aws-8-21/tree/main/aws/projects/Project-503-Capstone-Project-Blog-Page-App-(Django)-on-AWS-Environment)>



(Janko flask in gelmiş hall diyebiliriz bir frameworktir.)

Developerlar bir jango framworku ile block applicationu yazdilar. Blok sayfasi ile herkes kendi blogunu sayfاسini yazabiliyor. Fotograflarini ve videolarini paylasabiliyor.

Videolarini paylasacakları için bi login olunması ve bir yerde de user ve passwordların tutulması store edilmesi gerekiyor.

Store denilince aklimiza AWS de s3 geliyor. Developerlar s3 de tutulmasını istiyorlar. S3 obje tabanlı bir storage idi. Ne kadar cagirıllır ise o kadar ücretlendirmeye tabiydi.

Login datalarda database de tutulacak. Bunun içinde Mysql tercih edilmiş .

Bunun için Custom VPC kuracağız . Production ortamında da custom vpc kullanılması tercih ediliyor. Cunku VPC lerde Database gibi bazı makinalarımızın private subnetlerde kurulması gerekiyor ki bir bakıma bunlar bilerer firewall olarak nitelendiriliyor.

Custom VPC nin isterlerine bakalım;

- **2 adet Availability zonumuz var ve bu Availability Zon'un içerisinde bir private ve birde public subnetlerimiz olacak (Availability Zone : Bir region içerisinde bulunan, birbirlerine yakın konumlardırılmış, küçük sunucu tariqlerine verilen ismidir. Bir region içerisinde birden fazla availability zone bulunabilir ve her bir zone harf ile adlandırılır. Örneğin Oregon region'unda us-west-2a, us-west-2b ve us-west-2c olmak üzere üç adet AZ (availability-zone) bulunmaktadır.)**

Private ve public subnetler vpc içersine kurulan izole network çözümleridir.

- **Bi izole network içersine farklı resourcları koruma altına alabiliyoruz.**
- **Ortak bir subnet kumesini bir subnet gurubunda toplayabiliyorsunuz.**
- **Ayrıca farklı subnetlerde farklı replicalar bulundurarak failover durumlarında afet yangın olası tabii durumlarda mevcut subnetimize bir sey olması durumunda diğer subneti devreye sokabiliyoruz.**

Subnetler in kendi aralarında irtibati kurmaları için veya subnetlerin içerisindeki resourceların dış dunyaya ulaşmak istediklerinde, veya herhangi bir porta ulaşmak

Istediklerinde, Rote Tableti kullanırız. Route Tableler subnet içerisinde bir navigasyon cihazıdır. Rota Tableler içerisinde oluşturduğumuz Rule lar ile bir tarafa gitmesini veya hedefini sağlamasını sağlarız.

Özellikle de private Route Tablet yapılmasıının sebebi bir firewall yapılarak dış dünyadan ulaşamayacak bir hale getirmesini sağlamaktır.

Ayrıca videolar ve resimlerin s3 de saklanacağını ve dış dünyaya ya expoza olmasına istemedigimizi düşünürsek subnetler ile S3 bucket lar arasında da bir gateway endpoint kuracagız.

Ardından Jango web sitemiz bir EC2 lar grubu üzerinde tutulacak bunuda Autoscaling group sağlayacak. Bunun öncesi de bir Launch Template kuracagız ki L.Template ile Auto Scaling makinaların kurulumunu salayalım . Bizim istediğimiz desire kapasitede minimum ve max seviyede makinalar ayaga kalkacak . Burda bir Target Tracking Policy oluşturacagız.

Aynı zaman bu Ec2 lar ELB ye bağlı olacak ELB nin en önemli özelliği EC2 lardaki yoğunluga bakıp HealthCheck ler ile herhangi yoğunluk olması durumunda eşit olarak bu yere EC2 lar arasında dağıtmak. Hem Trafigi yayınıyor hem tek elden dağılımı sağlıyor. Hemde Dış dünyadan gelen User In her hangi bir aksama olmadan EC2 ya ulaşmasını sağlıyor.

ALB nin de önüne CloudFront koyacagız ki bu da bir cash hizmeti sunacak. Videolar ve fotoğraflar S3 den çekilecek her seferinde ücret ödememesi için bunu yapacaklar Cash hizmeti ile sağlanacak.

Production ortamında Cloudfront s3 un önüne de kurulabiliyor Eger burda tanımlamak istersek s3 u orjin olarak gösterecektir.

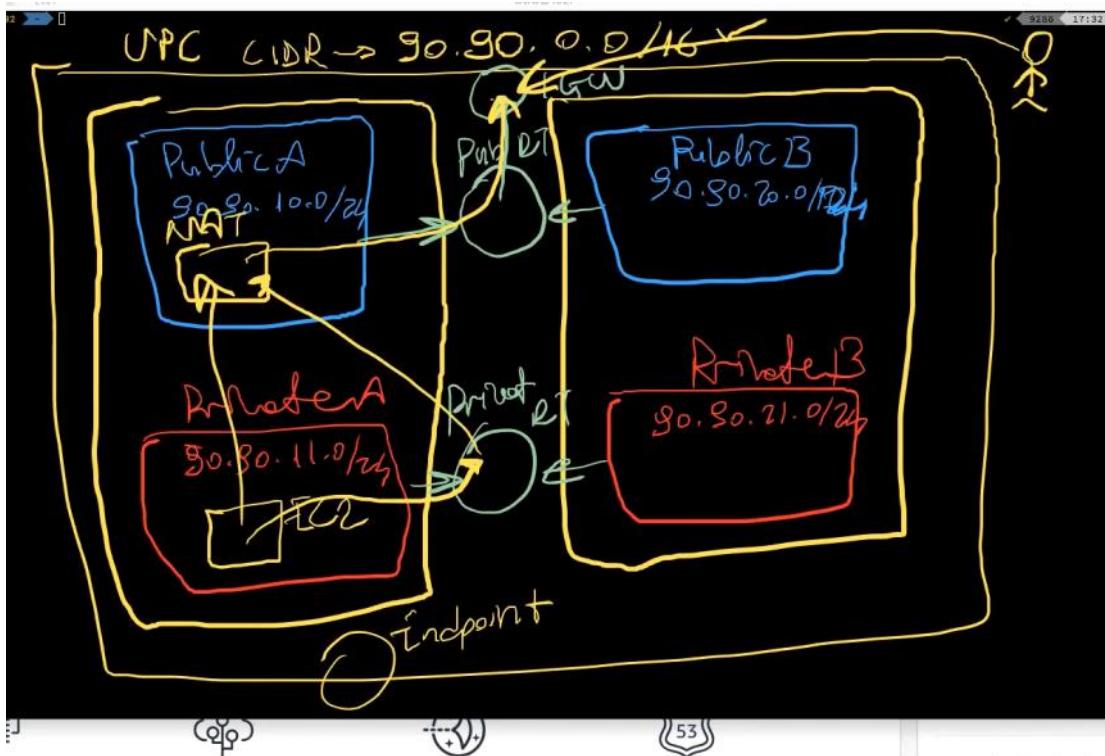
Developerlar kodunu kullanıcı karşısına çıkartmak için Route53 failover senaryosu ile karşımıza çıkacak.

Burada Failover senaryosu Route 53 olarak bir ister atanmış durumdadır. Route53 de iki adet ent pointi takip eder. Birisi static website olur. Degiride uniq olarak çalışan web sitesidir.basına herhangi bir durum gelmesi halinde secondary e trafigi yönlendirir.

Userlar bu haliyle karsılarına bir sey çıkarkı mevcut olarak bir sorunun olduğunu ve bu sorunun bir süre sonra çözülecegi gibi seyler içerebilir.

Birde Developerlere S3 un içeriğine konulan her seyi takip etmek istiyorlar. S3 e konan herhangi bir obje olduğunda , bir event olusacak bu event bir lambda function oluşturacak bu Lambda Function da Dynamodb içeriğine bilgileri yazdırılacak.

Dolayısıyla yazılan ve silinen bilgileri Dynamodb de grebilecegiz.



Konsolumuza geciyoruz :

Vpc de CIDR Bloklari vardır. Bz bunlari Private Ipler icin tanimliyoruz. Public oainları EC2 kendisi veriyor.

Tanimliyacagımız vpc de AWS 90.90.0.0/16 toplamda 65 bin ip tanimlayabilecegimiz BIR SINIRLAMA TANIYOR

Bir subneti private yada Public yapan disaruya acilmasidır.

Birde bunlara Private ve Public Rote tablet ayarlayacagız ki Routa tabletliere bir kural tanimlar ve dis dunnya ya acilmasini isterseniz Public istemez iseniz Private olurlar

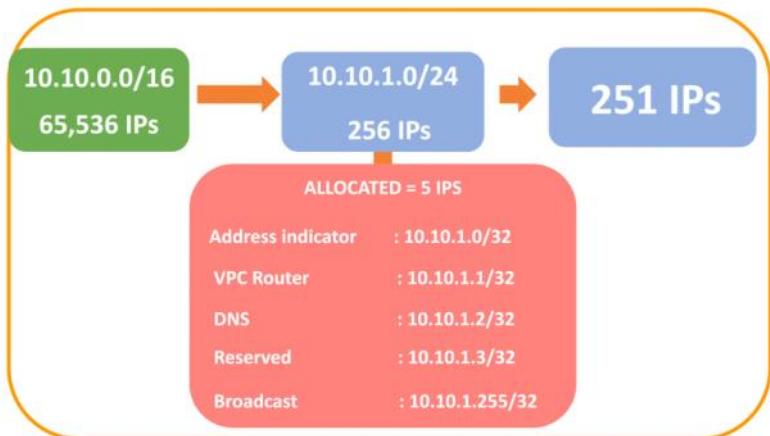
Ayrıca Bir de end Point ekleyecegiz s3 ler ve DYNAMODB Cloud Watch lar icin kullanılır ve burada s3 e irtibat saglamk icin kullanacagız.

Biz Internet Gate way aracılıyla Oncelikle Public Iplerimize giriş yapabiliyoruz. Ancak Private gecis yapmak icin Publicide kuracagımız Bustom Hostlar ile sibialma tahtalari ile Gecis yapacagız.

Ayrıca Icerdeki makinanın disaruya acilmasi icin ne yapmamız gerekiyor duerek bunun icinde Nat instance ve/yahut nat Gateway kurmamız gerekiyor Bastion Host olarak da goruluyor Ancak Nat Instance da dikkat edilmesi gereken konu http, HTTPS ve SSH anywhere olarak her yerden acmamız gerekiyor

Ayrıca birde Icerdeki makinanın disardaki ile görüşmesi icin ne yapmamız gerekiyor. Nat Instance veya/hut Nat Gateway kurmalz gerekiyor NatGateway AWS manage bir sistemdir. Yani biz kontrol etmiyoruk. Nat Instance ise özel bir instance tipidir. Public Subnete yerlestiririz. Private Instance da bulunan EC2 muz Private Ruta Table aracılıyla Nat Instance uzerinden dis dunya ile irtibat saglayabiliyoruz. Ayrıca Bastion Host olarak kullanılabiliyor ancak HTTP,HTTPS ve ssh In anywhere olarak her yöne acilmasi gerekiyor.

VPC CIDR



Inet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses
net-05335f428f973bc72	Available	vpc-0142f2295c4ac3c14 aws...	90.90.10.0/24	-	251

90.90.10.0 Network
 90.90.10.255 → Broadcast
 90.90.10.01 → VPC Router
 90.90.10.02 → DNS
 2^8 = 256 90.90.10.03 → Future

256 - 1 = 255 kullanılabilir 5 ntnesini AWS kendisine Reerverse eder.

İlk olarak VPC mizi yapmak için konsola gidiyoruz

```
# Project-503 : Blog Page Application (Django) deployed on AWS Application Load Balancer with Auto Scaling, S3, Relational Database Service(RDS), VPC's Components, DynamoDB and Cloudfront with Route 53 (STUDENT SOLUTION)
## Description
```

The Clarusway Blog Page Application aims to deploy blog application as a web application written Django Framework on AWS Cloud Infrastructure. This infrastructure has Application Load Balancer with Auto Scaling Group of Elastic Compute Cloud (EC2) Instances and Relational Database Service (RDS) on defined VPC. Also, The Cloudfront and Route 53 services are located in front of the architecture and manage the traffic in secure. User is able to upload pictures and videos on own blog page and these are kept on S3 Bucket. This architecture will be created by Firms DevOps Guy.

```
# Steps to Solution
```

```
### Step 1: Create dedicated VPC and whole components
```

```
### VPC
- Create VPC.
  create a vpc named `aws_capstone-`  

VPC` CIDR blok is `90.90.0.0/16`  

  no ipv6 CIDR block
  tenancy: default
- select `aws_capstone-`  

VPC` VPC, click `Actions` and `enable DNS hostnames` for the `aws_capstone-VPC`.
```

VPC settings

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

aws_capstone-VPC

IPv4 CIDR block [Info](#)
90.90.0.0/16

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

Tenancy [Info](#)
Default

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="aws_capstone-VPC"/>

Add new tag

You can add 49 more tags.

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

vpc ile birlikte route tablet in default olarak olustugunu
görebiliyoruz.

Route tables (5) [Info](#)

[Actions](#) [Create route table](#)

[Filter route tables](#)

	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC
<input type="checkbox"/>	-	rtb-062d4ec7095f88883	-	-	Yes	vpc-0c0a0da8de48dd91 aw...
<input type="checkbox"/>	clarus-private-rt	rtb-06ef049fb060b366	3 subnets	-	No	vpc-036f805ab0cb50ebd clar...
<input type="checkbox"/>	clarus-vpc-a-default-rtb	rtb-0c9e0ccc393f88236	-	-	Yes	vpc-036f805ab0cb50ebd clar...
<input type="checkbox"/>	clarus-public-rtb	rtb-02c42e5caa6d9aa41	3 subnets	-	No	vpc-036f805ab0cb50ebd clar...
<input type="checkbox"/>	default-rtb	rtb-00f263a33d166d2ee	-	-	Yes	vpc-05fe07f13680c6059 def...

Buna da public Routa tablet deyip bir taNE DE PRIVATE
OLUSTURabiliyoruz

Vpc icerisinde butun resource slarin bir birleri
ile ,konusmasini istiyorsak edit DNS Hostaname den ENABLE
YAPIYORUZ

Enable olmaz is e bu vpc icerrisine bir DNS atanmaz ve bir
bir leri ile konusmalari zora gider.

Your VPCs (1/3) [Info](#)

[Actions](#) [Create VPC](#)

[Filter VPCs](#)

Name	VPC ID	Status	IPv4 CIDR	IPv6 CIDR (Network border group)	IPv6	Actions
clarus-vpc-a	vpc-0fd961581569ac54	Available	10.70.0/16	-	-	Actions Edit Delete
default-vpc	vpc-f52d11bf	Available	172.31.0/16	-	-	Actions Edit Delete
aws_capstone-VPC	vpc-0142f2295e4ac3c14	Available	90.90.0/16	-	-	Actions Edit Delete

Simdid e subnet olusturacagiz

```
## Subnets
- Create Subnets
  - Create a public subnet named `aws_capstone-public-subnet-1A` under the vpc aws_capstone-VPC in AZ us-east-1a with 90.90.10.0/24
  - Create a private subnet named `aws_capstone-private-subnet-1A` under the vpc aws_capstone-VPC in AZ us-east-1a with 90.90.11.0/24
  - Create a public subnet named `aws_capstone-public-subnet-1B` under the vpc aws_capstone-VPC in AZ us-east-1b with 90.90.20.0/24
  - Create a private subnet named `aws_capstone-private-subnet-1B` under the vpc aws_capstone-VPC in AZ us-east-1b with 90.90.21.0/24
  - Set `auto-assign IP` up for public subnets. Select each public subnet and click Modify "auto-
```

assign IP settings and select "Enable auto-assign public IPv4 address"

VPC > Subnets > Create subnet

Create subnet Info

VPC

VPC ID
Create subnets in this VPC.
vpc-0c0a0da8de48dda91 (aws_capstone-VPC)

Associated VPC CIDRs
IPv4 CIDRs
90.90.0.0/16

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.
my-subnet-01

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.
No preference

IPv4 CIDR block Info
Q 10.0.0.0/24

▼ Tags - optional

Vpc Id olarak daha önce oluşturduğumuz vpc yi seçiyoruz.

vpc-0c0a0da8de48dda91 (aws_capstone-VPC)

Associated VPC CIDRs
IPv4 CIDRs
90.90.0.0/16

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.
aws_capstone-public-subnet-1A

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 CIDR block Info
Q 90.90.10.0/24 X

▼ Tags - optional

Key Value - optional
Q Name Q aws_capstone-public-subnet-1A X Remove

Add new tag You can add 49 more tags.

Remove

Add new subnet

Cancel **Create subnet**

You have successfully created 1 subnet: subnet-0e6c5deb9d406fe4

Subnets (4) Info						
<input type="checkbox"/>	Name	Subnet ID	State	VPC	Actions	
<input type="checkbox"/>	aws_capstone-public-subnet-1A	subnet-0b2fd9cdd64a3050e	Available	vpc-0c0a0da	View details	Create subnet
<input type="checkbox"/>	aws_capstone-private-subnet-1B	subnet-0e6c5deb9d406fe4	Available	vpc-0c0a0da	Edit IPv4 CIDR	Edit network ACL association
<input type="checkbox"/>	aws_capstone-private-subnet-1A	subnet-086733fa3f0fe391	Available	vpc-0c0a0da	Edit route table association	Share subnet
<input type="checkbox"/>	aws_capstone-public-subnet-1B	subnet-05085a0d50bc30d03	Available	vpc-0c0a0da	Manage tags	Delete subnet

Public Subnetler Icin Public Ip atanmasi gerekiyor. Bunu bizde kontroledebiliyoruz Bunun Icin Public Ipleri Actions bölümunden Modify deyip daha sonra enable ediyoruz.

You have successfully created 1 subnet: subnet-01e80641d4d2ade38

Subnets (1/4) Info						
<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR
<input checked="" type="checkbox"/>	aws_capstone-public-subnet-1A	subnet-0533f428f973bc72	Available	vpc-0142f2295c4ac3c14 aws...	90.90.10.0/24	-

Actions

- [View details](#)
- [Create flow log](#)
- [Modify auto-assign IP settings](#)
- [Edit IPv4 CIDR](#)
- [Edit network ACL association](#)
- [Edit route table association](#)
- [Share subnet](#)
- [Manage tags](#)
- [Delete subnet](#)

Subnetleri Private ve Public Yapmak Icin Route Tabletleri de duzenleyecegiz

Public routa Tabletleri Public yapmak Icin Interne Gate Way tanimlayacagiz

```
## Internet Gateway
- Click Internet gateway section on left hand side. Create an internet gateway named `aws_capstone-IGW` and create.
```

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.

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
<input type="text" value="Name"/>	<input type="text" value="aws_capstone-IGW"/>
Remove	
Add new tag	

You can add 49 more tags.

[Cancel](#) [Create internet gateway](#)

```
- ATTACH the internet gateway `aws_capstone-IGW` to the newly created VPC `aws_capstone-VPC`. Go to VPC and select newly created VPC and click action on ---> Attach to VPC ---> Select `aws_capstone-VPC` VPC.
```

Internet Gateway olusturduk ancak bunu attach etmemiz gerekiyor su an Detach olarak gözüküyor

Her bir VPC ye Ancak bir InternetGateWay Attach edilebiliyor.

The screenshot shows the AWS VPC Internet Gateways page. A specific Internet Gateway, 'igw-09d145959771e07c9 / aws_capstone-IGW', is selected. The 'Details' tab is active, displaying the Internet gateway ID (igw-09d145959771e07c9), state (Detached), VPC ID (-), and owner (046402772087). The 'Actions' menu includes options like 'Attach to VPC', 'Detach from VPC', 'Manage tags', and 'Delete'. Below the details, the 'Tags' section shows a single tag 'Name: aws_capstone-IGW'. A search bar for tags is also present.

Son olarak Route Tabletlerimize Internet Gate Way I ekleiyoruz.

The screenshot shows the AWS Route Tables page. A specific route table, 'rtb-062d4ee7095f88883', is selected. The 'Edit routes' section shows two routes: one to 'local' target and another to 'igw-07d971ec6c334d84e' target, both marked as Active. The 'Status' column indicates 'Active' for both. The 'Propagated' column shows 'No' for both. A 'Remove' button is available for the second route. A 'Save changes' button is at the bottom right. Other buttons include 'Add route' and 'Preview'.

Ve ardindan Private Routa Tabletler ile Private Subnetler, Public leri Public olan ile Associations edecegiz

The screenshot shows the AWS VPC Route Tables page. It lists six route tables: 'aws_capstone_Private_route_tablet', 'aws_capstone_Public_route_tablet', 'clarus-private-rt', 'clarus-public-rtb', 'clarus-vpc-a-default-rtb', and 'default-rtb'. The 'aws_capstone_Private_route_tablet' is selected, indicated by a checked checkbox. The 'Actions' menu for this table includes options like 'View details', 'Set main route table', 'Edit subnet associations', 'Edit edge associations', 'Edit route propagation', 'Edit routes', 'Manage tags', and 'Delete route table'. The 'Explicit subnet associations' column shows '-' for most tables except 'aws_capstone_Private_route_tablet' which has '3 subnets'.

ss

Ve simdi de endpoint olusturacagiz. Ent pointleri Private Subnetler icin tanimlayacagiz.

Vpc olarak kendi vpc mizi seciyoruz

Ardindan hangi Route Tabletleri sececegimiz karsimiza gelyor

A VPC endpoint enables you to securely connect your VPC to another service.

There are three types of VPC endpoints – Interface endpoints, Gateway Load Balancer endpoints, and gateway endpoints. Interface endpoints and Gateway Load Balancer endpoints are powered by AWS PrivateLink, and use an elastic network interface (ENI) as an entry point for traffic destined to the service. Interface endpoints are typically accessed using the public or private DNS name associated with the service, while gateway endpoints and Gateway Load Balancer endpoints serve as a target for a route in your route table for traffic destined for the service.

Service category

- AWS services
- Find service by name
- Your AWS Marketplace services

Service Name com.amazonaws.us-east-1.s3 

Service Name	Owner	Type
<input checked="" type="radio"/> com.amazonaws.us-east-1.s3	amazon	Gateway
<input type="radio"/> com.amazonaws.us-east-1.s3	amazon	Interface

VPC* vpc-f52d178f   

Configure route tables A rule with destination `pl-63a5400a` (`com.amazonaws.us-east-1.s3`) and a target with this endpoint's ID (e.g. `vpc-12345678`) will be added to the route tables you select below.

Subnets associated with selected route tables will be able to access this endpoint.

Subnets associated with selected route tables will be able to access this endpoint.

Route Table ID	Main	Associated With
<input type="checkbox"/> rtb-062d4ee7095f88883	Yes	2 subnets
<input checked="" type="checkbox"/> rtb-0a255a53c4f03b31e	No	2 subnets

Warning

When you use an endpoint, the source IP addresses from your instances in your affected subnets for accessing the AWS service in the same region will be private IP addresses, not public IP addresses. Existing connections from your affected subnets to the AWS service that use public IP addresses may be dropped. Ensure that you don't have critical tasks running when you create or modify an endpoint.

Policy*

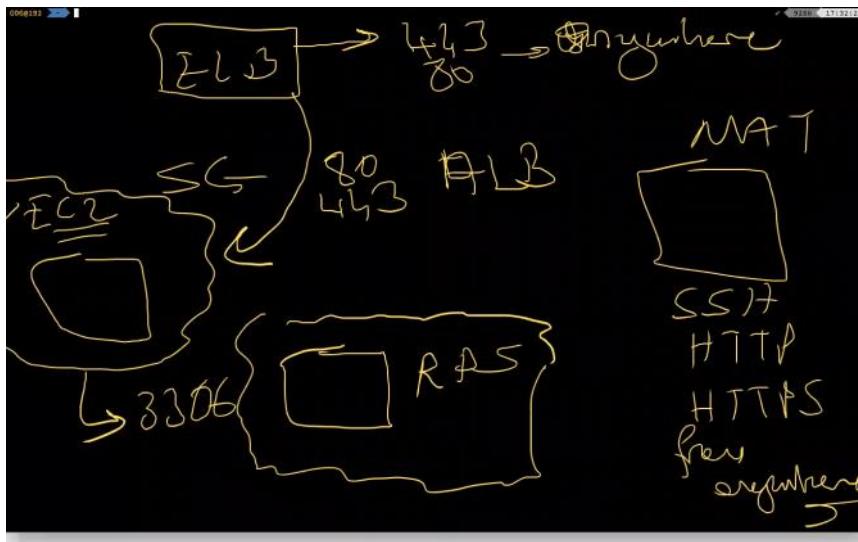
- Full Access - Allow access by any user or service within the VPC using credentials from any Amazon Web Services accounts to any resources in this Amazon Web Services service. All policies — IAM user policies, VPC endpoint policies, and Amazon Web Services service-specific policies (e.g. Amazon S3 bucket policies, any S3 ACL policies) — must grant the necessary permissions for access to succeed.
- Custom

Use the policy creation tool to generate a policy, then paste the generated policy below.

```
{ "Statement": [ { "Action": "sns:Publish", "Effect": "Allow", "Resource": "arn:aws:sns:us-east-1:123456789012:MyTopic", "Principal": "arn:aws:lambda:us-east-1:123456789012:function:MyFunction" } ] }
```

Ve simdi de security Gruplarimizi olusturacagiz. Ve daha sonra olusturdugumuz makinalarda kolay bir sekilde sececegiz.

**Rds e her makinani ulasmasini istemiyoruz sadece
application unumuzun oldugu EC2 nun ulasmasini istiyoruz**



- ELB dis dunya ile irtibat sagladigi icin ona 443 ve 80 portundan her yere yani any where olarak aciyoruz
- Ancak Ec2 ya sadece ELB uzerinden ulasilmasini istedigimiz icin EC2 icin olusturdugumuz Sec Grupta 80 ve 443 portundan sadece EC2 yu belirtecegiz
- RDS sadece EC2 dan ulasilmasini istedigimiz icin RDS e 3306 portundan sadece EC2 yu tanimliyoruz.
- Nat instance dis dunyadan her istegi teki Private icin yerine getiren oldugu icin burda any where ile http HTTPS I Tnimliyoruz

Step 2: Create Security Groups (ALB ---> EC2 ---> RDS)

1. ALB Security Group

Name : aws_capstone_ALB_Sec_Group
 Description : ALB Security Group allows traffic HTTP and HTTPS ports from anywhere
 Inbound Rules
 VPC : AWS_Capstone_VPC
 HTTP(80) ----> anywhere
 HTTPS (443) ----> anywhere

Basic details

Security group name : aws_capstone_EC2_Sec_Group
 Name cannot be edited after creation.
 Description : EC2 Security Groups only allows traffic coming from aws_capstone_ALB_Sec_Group Security
 VPC : vpc-0142f229564ac3c14 (aws_capstone-VPC)

Inbound rules		Outbound rules	
Type	Protocol	Port range	Source
HTTP	TCP	80	aws_capstone_ALB_Sec_Group
Add rule		Description - optional	
		0.0.0.0/0	

2. EC2 Security Groups

Name : aws_capstone_EC2_Sec_Group
 Description : EC2 Security Groups only allows traffic coming from aws_capstone_ALB_Sec_Group Security Groups for HTTP and HTTPS ports. In addition, ssh port is allowed from anywhere
 VPC : AWS_Capstone_VPC
 Inbound Rules
 HTTP(80) ----> aws_capstone_ALB_Sec_Group
 HTTPS (443) ----> aws_capstone_ALB_Sec_Group
 ssh ----> anywhere

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, enter a name and description, and then choose a VPC.

Basic details

Security group name Info

aws_capstone_ALB_Sec_Group

Name cannot be edited after creation.

Description Info

ALB Security Group allows traffic HTTP and HTTPS ports from anywhere

VPC Info

vpc-f52d178f (default-vpc)



vpc-0fdf631581569ac34 (clarus-vpc-a)

10.70.0.0/16

vpc-f52d178f (default-vpc)

172.31.0.0/16

vpc-0142f2295c4ac3c14 (aws_capstone-VPC)

90.90.0.0/16

Add rule

Outbound rules Info

Bu su anlama geliyor 80 ve 443 portu ile attach ettigimiz
 (her ALB nin) makinenin bu vpc ye ulasabilecegini
 belirtiyoruz.

3. RDS Security Groups

Name : aws_capstone_RDS_Sec_Group

Description : EC2 Security Groups only allows traffic coming from aws_capstone_EC2

_Sec_Group Security Groups for MySQL/Aurora port.

VPC : AWS_Capstone_VPC

Inbound Rules

MySQL/Aurora(3306) ----> aws_capstone_EC2_Sec_Group

Sadece EC2 kardan geleni kabul edecek

Inbound rules Info

Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Source <small>Info</small>	Description - option
MySQL/Aurora	TCP	3306	Custom	<input type="text" value="sg"/> X Security Groups
				aws_capstone_EC2_Sec_Group sg-0360174d5fdbab3ff2

Outbound rules Info

Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Destination <small>Info</small>	Description - option
				<input type="text" value="sg"/> X Security Groups
				aws_capstone_ALB_Sec_Group sg-0b9feaa077d1564a
				default sg-0bfef2bb9c60bc7ac

4. NAT Instance Security Group

Name : aws_capstone_NAT_Sec_Group

Description : ALB Security Group allows traffic HTTP and HTTPS and SSH ports from anywhere

Inbound Rules

VPC : AWS_Capstone_VPC

HTTP(80) ----> anywhere

HTTPS (443) ----> anywhere

SSH (22) ----> anywhere

Step 3: Create RDS

Custom VPC lerde RDS kurmadan önce bu RDS lerin hangi VPC de calismasini istiyorsak o sekilde bir Subnet Group olusturuyuz

First we create a subnet group for our custom VPC. Click `s ubnet Groups` on the left hand menu and click `create DB Su bnet Group`

```
```text
Name : aws_capstone_RDS_Subnet_Group
Description : aws capstone RDS Subnet Group
VPC : aws_capstone_VPC
Add Subnets
Availability Zones : Select 2 AZ in aws_capstone_VPC
Subnets : Select 2 Private Subnets in these subn
ets
```

```

Description: aws capstone RDS Subnet Group

VPC: aws_capstone-VPC (vpc-0142f295c4ac3c14)

Add subnets:

Availability Zones: Choose an availability zone

Subnets:

| Select subnets |
|--|
| us-east-1a |
| <input checked="" type="checkbox"/> subnet-01e80641d4d2ade39 (90.90.21.0/24) |
| <input type="checkbox"/> subnet-09996662f9dd3a13 (90.90.20.0/24) |
| us-east-1b |
| <input type="checkbox"/> subnet-05335f428f973bc72 (90.90.10.0/24) |
| <input checked="" type="checkbox"/> subnet-0db543e282ef89b1 (90.90.11.0/24) |

CIDR block:

| us-east-1a | us-east-1b |
|---------------|---------------|
| 90.90.21.0/24 | 90.90.20.0/24 |

- Go to the RDS console and click `create database` button

```
```text
Choose a database creation method : Standard Create
Engine Options : Mysql
```

```

Choose a database creation method Info

Standard create
You set all of the configuration options, including ones for availability, security, backups, and maintenance.

Easy create
Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

Engine options

Engine type Info

Amazon Aurora

MySQL

MariaDB

PostgreSQL

Oracle

Microsoft SQL Server

Edition

```
Version : 8.0.20
Templates : Free Tier
Settings :
- DB instance identifier : aws-capstone-RDS
- Master username : admin
- Password : Clarusway1234
DB Instance Class : Burstable classes (includes t classes) ---> db.t2.micro
Storage : 20 GB and enable autoscaling (up to 40GB)

```

Settings

DB instance identifier [Info](#)

Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AV Region.

aws-capstone-RDS

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

▼ Credentials Settings

Master username [Info](#)

Type a login ID for the master user of your DB instance.

admin

1 to 16 alphanumeric characters. First character must be a letter

Auto generate a password

Amazon RDS can generate a password for you, or you can specify your own password

Master password [Info](#)

Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), '(single quote)', "(double quote)" and ; (at sign).

Confirm password [Info](#)

DB instance class

DB instance class [Info](#)

Choose a DB instance class that meets your processing needs and resource requirements. The DB instance class settings below are

Connectivity:

| | | |
|------------------------|---|---|
| VPC | : | aws_capstone_VPC |
| Subnet Group | : | aws_capstone_RDS_Subnet_Group |
| P Public Access | : | No |
| VPC Security Groups | : | Choose existing ---> aws_capstone_RDS_Sec_Group |

Storage

Storage type [Info](#)

General Purpose (SSD)

Allocated storage

20 GiB

(Minimum: 20 GiB, Maximum: 16,384 GiB) Higher allocated storage [may improve](#) IOPS performance.

Storage autoscaling [Info](#)

Provides dynamic scaling support for your database's storage based on your application's needs.

Enable storage autoscaling

Enabling this feature will allow the storage to increase once the specified threshold is exceeded.

Maximum storage threshold [Info](#)

Charges will apply when your database autoscales to the specified threshold

40 GiB

(Minimum: 21 GiB, Maximum: 16,384 GiB)

Availability & durability

Storage kismini RDS'in kapasitesi max kac arttirabiliyor
max olarak 16,384 GiB yapabiliyor

Connectivity



Virtual private cloud (VPC) [Info](#)

VPC that defines the virtual networking environment for this DB instance.

aws_capstone-VPC (vpc-0142f2295c4ac3c14)

Only VPCs with a corresponding DB subnet group are listed.

After a database is created, you can't change the VPC selection.

Subnet group [Info](#)

DB subnet group that defines which subnets and IP ranges the DB instance can use in the VPC you selected.

aws_capstone_rds_subnet_group

Public access [Info](#)

Yes

Amazon EC2 instances and devices outside the VPC can connect to your database. Choose one or more VPC security groups that specify which EC2 instances and devices inside the VPC can connect to the database.

No

RDS will not assign a public IP address to the database. Only Amazon EC2 instances and devices inside the VPC can connect to your database.

VPC security group

Choose a VPC security group to allow access to your database. Ensure that the security group rules allow the appropriate incoming traffic.

Choose existing

Choose existing VPC security groups

Create new

Create new VPC security group

Existing VPC security groups

Choose VPC security groups

Public acces no diyoruz VPC nin disindan verilen bir izindir.

Availability Zone : No preference

Additional Configuration : Database port ---> 3306

Database authentication ---> Password authentication

Additional Configuration:

- Initial Database Name : database1
- Backup ---> Enable automatic backups
- Backup retention period ---> 7 days
- Select Backup Window ---> Select 03:00 (am) Duration

1 hour

- Maintenance window : Select window ---> 04:00(am) Duration:1 hour

create instance

...

Log flow

The following service-linked role is used for publishing logs to CloudWatch Logs.

RDS service-linked role

Ensure that general, slow query, and audit logs are turned on. Error logs are enabled by default. [Learn more](#)

Maintenance

Auto minor version upgrade [Info](#)

Enable auto minor version upgrade

Enabling auto minor version upgrade will automatically upgrade to new minor versions as they are released. The automatic upgrades occur during the maintenance window for the database.

Maintenance window [Info](#)

Select the period you want pending modifications or maintenance applied to the database by Amazon RDS.

Select window

No preference

Start day: Tuesday, Start time: 05:00 UTC, Duration: 0.5 hours

Deletion protection

Enable deletion protection

Protects the database from being deleted accidentally. While this option is enabled, you can't delete the database.

Estimated monthly costs

The Amazon RDS Free Tier is available to you for 12 months. Each calendar month, the free tier will allow you to use the Amazon RDS resources listed below for free:

- * 750 hrs of Amazon RDS in a Single-AZ db.t2.micro instance.

Enable deletion dersek silmek icin bir kac basamli bir sart getiri protection
ortanminda bu öneiri.

Iki bucket icin olusturacagiz bir failover icin digerri resim ve metinleri saklamak icin olusturacagiz

Step 4: Create two S3 Buckets and set one of these as static website.

Go to the S3 Consol and lets create two buckets.

1. Blog Website's S3 Bucket

- Click Create Bucket

```text

Bucket Name : awscapstones3<YOUR NAME>blog-----uniq dikkat  
edilmesi gereken  
Region : N.Virginia

The screenshot shows the AWS S3 'Create Bucket' wizard. In the first step, 'General configuration', the bucket name is set to 'awscapstones3serdarblog' and the region is 'US East (N. Virginia) us-east-1'. In the second step, 'Block Public Access settings for this bucket', the 'Block all public access' checkbox is unchecked, and a note says 'Other Settings are keep them as are'. The 'create bucket' button is visible at the bottom.

**Block all public access** : Unchecked  
Other Settings are keep them as are  
create bucket

**2. S3 Bucket for failover scenario**

- Click Create Bucket

```text

Bucket Name : www.<YOUR DNS NAME>

Region : N.Virginia

Block all public access : Unchecked

Please keep other settings as are

```create bucket

- Selects created `www.<YOUR DNS NAME>` bucket ---> Properties ---> Static website hosting

```text

Static website hosting : Enable

Hosting Type : Host a static website

Index document : index.html

save changes

```

- Select `www.<YOUR DNS NAME>` bucket ---> select Upload and upload `index.html` and `sorry.jpg` files from given folder---> Permissions ---> Grant public-read access ---> Checked warning message

Amazon S3 > www.clarunway.us > Upload

### Upload

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more [\[?\]](#)

Drag and drop files and folders you want to upload here, or choose Add files, or Add folders.

Files and folders (2 Total, 88.1 KB)		Remove	Add files	Add folder
All files and folders in this table will be uploaded.				
<input type="text"/> Find by name < 1 >				
Name	Folder	Type	Size	
index.html	-	text/html	199.0 B	
sorry.jpg	-	image/jpeg	87.9 KB	

**Destination**

Destination  
s3://www.clarunway.us

▶ Destination details Bucket settings that impact new objects stored in the specified destination.

Ayrıca static web site olarak kullanmak için de

**Ayrıca WWW. Ve DNS name ile oluşturduğumuz subnette Acces Control sekmesini Grant Public olarak açıyoruz upload ettigimiz file in dış dünyadan okunmasını sağlıyoruz.**

▼ Permissions

Grant public access and access to other AWS accounts.

#### Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. [Learn more \[?\]](#)

① AWS recommends using S3 bucket policies or IAM policies for access control. [Learn more \[?\]](#)

Access control list (ACL)

Choose from predefined ACLs

Specify individual ACL permissions

Predefined ACLs

Private (recommended) Only the object owner will have read and write access.

Grant public-read access Anyone in the world will be able to access the specified objects. The object owner will have read and write access. [Learn more \[?\]](#)

**⚠️ Granting public-read access is not recommended**  
Anyone in the world will be able to access the specified objects. [Learn more \[?\]](#)

I understand the risk of granting public-read access to the specified objects.

Not secure | devops-ramazan-kaya.com.tr-website-us-east-1.amazonaws.com

### FAILOVER SCENARIO



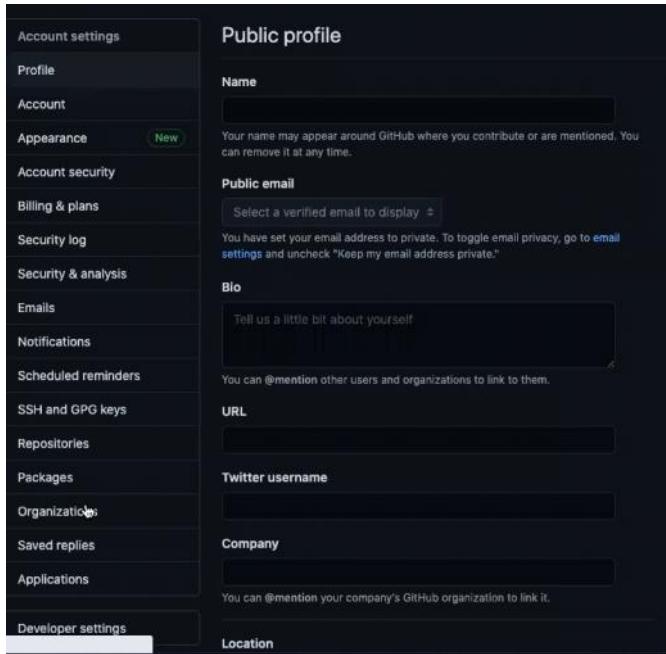
```
Step 5: Copy files downloaded or cloned from `Clarunway_` project` repo on Github
```

#### Git hub dan

S3 ler ayarlandı RDS ayarlandı ve şimdi Githubda bulunan private repomuzu clonlamamışık daha önce şimdi de git commit - m ve git push komutları ile ile lokalde bulunan dosyalarımızı git hub dosyamiza gönderdik.

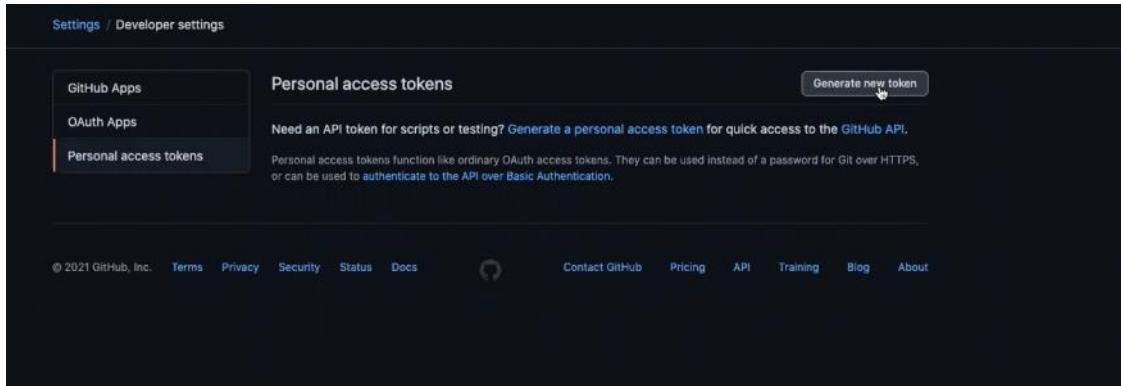
Simdi de git hub hesabımız dan **TOKEN** alacağız;

**Avatar----Setting-----Developer settings--Personel Access tokens----**



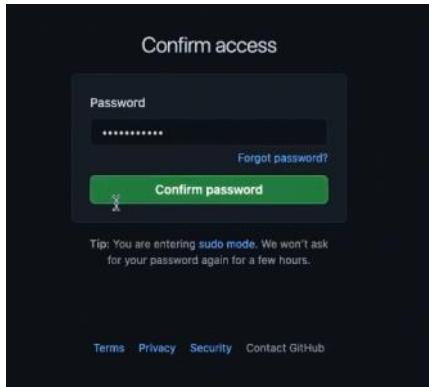
The screenshot shows the 'Public profile' section of the GitHub account settings. On the left, a sidebar lists various settings categories: Account settings, Profile, Account, Appearance (with a 'New' badge), Account security, Billing & plans, Security log, Security & analysis, Emails, Notifications, Scheduled reminders, SSH and GPG keys, Repositories, Packages, Organizations, Saved replies, Applications, and Developer settings. The 'Developer settings' category is highlighted with a yellow border. The main content area is titled 'Public profile' and contains fields for 'Name', 'Public email', 'Bio', 'URL', 'Twitter username', 'Company', and 'Location'. Each field has a descriptive placeholder text below it.

[View Generate new token](#)

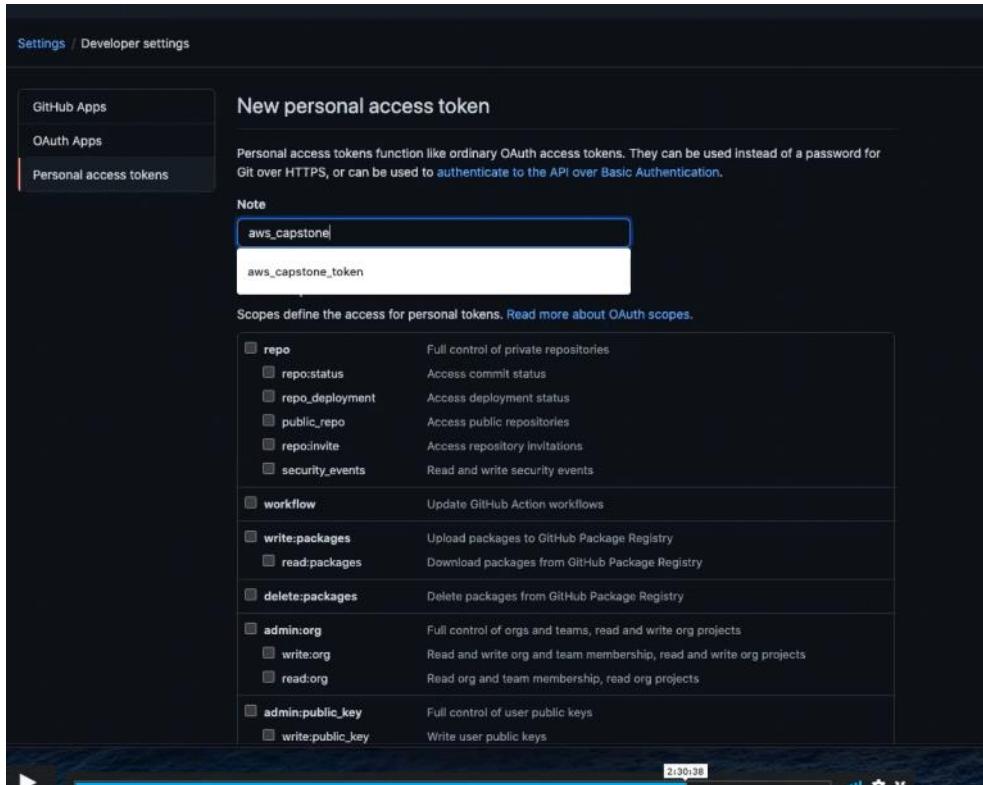


The screenshot shows the 'Personal access tokens' section under the 'Developer settings' tab. The sidebar on the left shows 'GitHub Apps', 'OAuth Apps', and 'Personal access tokens' (which is selected and highlighted with a yellow border). The main content area is titled 'Personal access tokens' and includes a 'Generate new token' button. Below the button, there is a note about generating an API token for scripts or testing. A detailed description explains that personal access tokens function like OAuth access tokens and can be used instead of a password for Git over HTTPS or for API authentication.

Enter the password



The screenshot shows a 'Confirm access' dialog box. It features a 'Password' input field with masked text, a 'Forgot password?' link, and a large green 'Confirm password' button. Below the dialog, a tip message states: 'Tip: You are entering sudo mode. We won't ask for your password again for a few hours.' At the bottom of the page, there are links for Terms, Privacy, Security, and Contact GitHub.



Ve Token hesabimiz olustu

```

#!/bin/bash
1 apt-get update -y
2 apt-get install git -y
3 apt-get install python3 -y
4 cd /home/ubuntu/
5 TOKEN="ghp_5zkSIFjvUL08Jk3Acu5s9GGN8d7Nh039nYHF"
6 git clone https://$TOKEN@github.com/Kaya-Ramazan/my-aws-capstone-project.git
7 cd /home/ubuntu/my-aws-capstone-project
8 apt install python3-pip -y
9 apt-get install python3.7-dev libmysqlclient-dev -y
10 pip3 install -r requirements.txt
11 cd /home/ubuntu/my-aws-capstone-project/src
12 python3 manage.py collectstatic --noinput
13 python3 manage.py makemigrations
14 python3 manage.py migrate
15 python3 manage.py runserver 0.0.0.0:80
16

```

User data da egerkli degisklikleri yaptik

Son dört komut Jangoyu calistiriyor.

```

Step 8: Write RDS database endpoint and S3 Bucket name in settings file given by Clarusway Fullstack Developer team
and push your application into your own public repo on GitHub
Please follow and apply the instructions in the developer_notes.txt.
```
- Movie and picture files are kept on S3 bucket named aws_c

```

```

apstone_S3
-<name>_Blog as object. You should create an S3 bucket and
write name of it on "/src/cblog/settings.py" file as AWS_ST
ORAGE_BUCKET_NAME variable. In addition, you must assign re
gion of S3 as AWS_S3_REGION_NAME variable
- Users credentials and blog contents are going to be kept
on RDS database. To connect EC2 to RDS, following variables
must be assigned on "/src/cblog/settings.py" file after yo
u create RDS;
    a. Database name - "NAME" variable
    b. Database endpoint - "HOST" variables
    c. Port - "PORT"
    d. PASSWORD variable must be written on "/src/.env" fil
e not to be exposed with settings file
```

```

- Please check if this userdata is working or not. to do th  
is create new instance in public subnet and show to student  
s that it is working

#### **## Step 9: Create NAT Instance in Public Subnet**

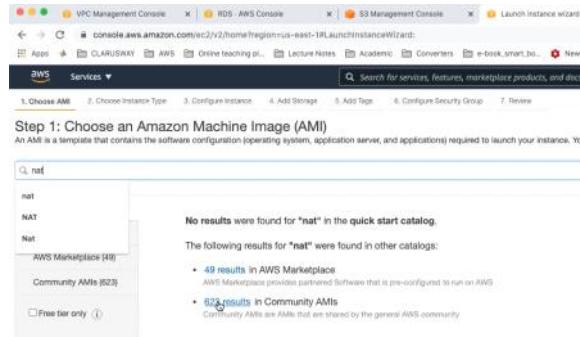
Public Subnette Nat instance olusturacagiz. Nat  
instance olusturmamizin sebebi Auto scaling  
olusturacagiz ki bunun icin öncelikle bir Launch  
Template olusturacaktik . AutoScalin EC2 olusturacak  
ve Ec2 larda Data cekmek isteyenler onun icin Nat  
instance ihtiyac var.

To launch NAT instance, go to the EC2 console and click the  
create button.

```text

write "NAT" into the filter box

```
select NAT Instance `amzn-ami-vpc-nat-
hvm-2018.03.0.20181116-x86_64-ebs`
```



```

Instance Type: t2.micro
Configure Instance Details
- Network : aws_capstone_VPC
- Subnet  : aws_capstone-public-
subnet-1A (Please select one of your Public Subnets)
- Other features keep them as are
Storage ---> Keep it as is
Tags: Key: Name   Value: AWS Capstone NAT Instance
Configure Security Group
- Select an existing security group: aws_capstone_NAT_S
ec_Group
Review and select our own pem key
```

```

!!!IMPORTANT!!!
- select newly created NAT instance and enable stop source/
destination check
- go to private route table and write a rule

```

Destination : 0.0.0.0/0
Target : instance ---> Select NAT Instance
Save
```

```

Public Subnetlerde olusturacagiz

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot Instances to take advantage of t

| | | |
|-----------------------|--|---------------------------------------|
| Number of instances | 1 | Launch into Auto Scaling Group |
| Purchasing option | <input type="checkbox"/> Request Spot instances | |
| Network | vpc-0142f2295c4ac3c14 aws_capstone-VPC | <input type="button"/> Create new VPC |
| Subnet | ✓ subnet-01e80641d4d2d8e39 aws_capstone-private-subnet-1B us-east-1b
subnet-099966862f9dd3a13 aws_capstone-public-subnet-1B us-east-1b
subnet-05335f4281973bc72 aws_capstone-public-subnet-1A us-east-1a
subnet-0bdb543e282ef89b1 aws_capstone-private-subnet-1A us-east-1a | |
| Auto-assign Public IP | <input checked="" type="checkbox"/> | |
| Placement group | <input type="checkbox"/> Add instance to placement group | |
| Capacity Reservation | Open | |
| Domain join directory | No directory | |
| IAM role | None | |

Nat instance olusturduktan sonra Actions -->Change Source/destination check
edecegiz ----stop edecegiz

Daha sonra Private Rote Table'lere bir Raute Table eklememiz gerekiyor.
Private
Makinalrdas dunyaya gitmek istediklerinde bi istegi nat instance
aktarmasini sagla diyoruzz.

Simdi de Launch Template olusturacagiz Launch Template tanimlamak icin EC2
ile konusabilmesi icin 2 alternatif var bunlardan ilki boto3 ile oluyor. Veyahut
bu ulasmayi iam Role tanimlayarak da yapabiliyoruz.

Full access yetkisi verecek bir IAM Role tanimlayacagiz ki bunun ile

Ilk olarak EC2 seciyoruz

Select type of trusted entity



Allows AWS services to perform actions on your behalf. Learn more

Choose a use case

Common use cases

EC2

Allows EC2 instances to call AWS services on your behalf.

Lambda

Allows Lambda functions to call AWS services on your behalf.

Or select a service to view its use cases

| | | | | |
|-------------|------------|---------|------------------|----------|
| API Gateway | CodeBuild | EMR | IoT SiteWise | RDS |
| AWS Lambda | CloudFront | Fargate | IoT Things Graph | Redshift |

Step 10: Create Launch Template and IAM role for it

Go to the IAM role console click role on the right hand menu than create role

```
```text
trusted entity : EC2 as ---> click Next:Permission
Policy : AmazonS3FullAccess policy
Tags : No tags
Role Name : aws_capstone_EC2_S3_Full_Access
Description : For EC2, S3 Full Access Role
```

```

Create role

Attach permissions policies

Choose one or more policies to attach to your new role.

Create policy

Filter policies ▾

| Policy name ▾ |
|--|
| <input type="checkbox"/> AmazonDMSRedshiftS3Role |
| <input checked="" type="checkbox"/> AmazonS3FullAccess |
| <input type="checkbox"/> AmazonS3OutpostsFullAccess |
| <input type="checkbox"/> AmazonS3OutpostsReadOnlyAccess |
| <input type="checkbox"/> AmazonS3ReadOnlyAccess |
| <input type="checkbox"/> IVSRecordToS3 |
| <input type="checkbox"/> QuickSightAccessForS3StorageManagementAnalyticsReadOnly |
| <input type="checkbox"/> s3_allow_policy |

Rol Create edildikten sonra Launch Template olusturacagiz;

```
```- create launch template
```

Delete Launch Template Request Succeeded

EC2 > Launch templates > Create launch template

## Create launch template

Creating a launch template allows you to create a saved instance configuration that can be reused, shared and launch later time. Templates can have multiple versions.

### Launch template name and description

Launch template name - required

aws\_capstone\_launch\_template

Must be unique to this account. Max 128 chars. No spaces or special characters like '&', '<', '@'.

Template version description

A prod webserver for MyApp

Max 255 chars

Auto Scaling guidance [Info](#)

Select this if you intend to use this template with EC2 Auto Scaling

Provide guidance to help me set up a template that I can use with EC2 Auto Scaling

► Template tags

► Source template

### Launch template contents

To create Launch Template, go to the EC2 console and select 'Launch Template' on the left hand menu. Tab the Create Launch Template button.

```
```bash
Launch template name : aws_capstone_launch_template
Template version description : Blog Web Page version
1
Amazon machine image (AMI) : Ubuntu 18.04
Instance Type : t2.micro
Key Pair : mykey.pem
Network Platform : VPC
```

AMI
Ubuntu Server 18.04 LTS (HVM), SSD Volume Type
ami-0747bdcab34c712a Catalog Quick Start virtualization: hvm architecture: 64-bit (x86)

Instance type [Info](#)

Instance type

Don't include in launch template

Compare instance types

t1.micro
Family: t1 1 vCPU 0.612 GB Memory
On-Demand Linux pricing: 0.02 USD per Hour
On-Demand Windows pricing: 0.02 USD per Hour

Free tier eligible

t2.nano
Family: t2 1 vCPU 0.5 GB Memory
On-Demand Linux pricing: 0.0058 USD per Hour
On-Demand Windows pricing: 0.0081 USD per Hour

Free tier eligible

t2.micro
Family: t2 1 vCPU 1 GB Memory On-Demand Linux pricing: 0.0116 USD per Hour
On-Demand Windows pricing: 0.0162 USD per Hour

Free tier eligible

t2.small
Family: t2 2 vCPU 2 GB Memory On-Demand Linux pricing: 0.023 USD per Hour
On-Demand Windows pricing: 0.032 USD per Hour

Free tier eligible

t2.medium
Family: t2 2 vCPU 4 GB Memory On-Demand Linux pricing: 0.0464 USD per Hour
On-Demand Windows pricing: 0.0644 USD per Hour

Free tier eligible

t2.large
Family: t2 2 vCPU 8 GB Memory On-Demand Linux pricing: 0.0928 USD per Hour
On-Demand Windows pricing: 0.1208 USD per Hour

Free tier eligible

```
Security Groups : aws_capstone_EC2
_sec_group : keep it as is
Storage (Volumes) : Key: Name Value: aw
Resource tags : Key: Name Value: aw
s_capstone_web_server
Advance Details:
  - IAM instance profile : aws_capstone_EC2_S3
  Full Access : Enable
  - Termination protection : Enable
```

▼ Network settings

Networking platform [Info](#)

Virtual Private Cloud (VPC)
Launch into a virtual network in your own logically isolated area within the AWS cloud

EC2-Classic
Launch into a single flat network that you share with other customers.

Security groups [Info](#)

Select security groups

Security Group	Description	SG ID
aws_capstone_EC2_Sec_Group	VPC: vpc-0142f2295c4ac3c14	sg-0360174d6fdb3ff2
aws_capstone_ALB_Sec_Group	VPC: vpc-0142f2295c4ac3c14	sg-0b9feeaa077d1364a
aws_capstone_RDS_Sec_Group	VPC: vpc-0142f2295c4ac3c14	sg-0de2ae839b36b26ae
aws_capstone_NAT_Sec_Group	VPC: vpc-0142f2295c4ac3c14	sg-0de41985e420e842a

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from be accessible from the instance.

[Add new volume](#)

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance

▼ Resource tags [Info](#)

Key [Info](#) Value [Info](#) Resource types [Info](#)

Key	Value	Type
<input type="text" value="Name"/>	<input type="text" value="aws_capstone_w"/>	<input type="text" value="Select resource types"/>
<input type="text" value="Instances"/>		

[Add tag](#)

49 remaining (Up to 50 tags maximum)

▼ Network interfaces [Info](#)

Purchasing option [Info](#)
 Request Spot Instances
 Request Spot Instances at the Spot price, capped at the On-Demand price

IAM Instance profile [Info](#)

Don't include in launch template

Specify a custom value...

Don't include in launch template

Admin
 arn:aws:iam::046402772087:instance-profile/Admin

ansible_dynamic_inv
 arn:aws:iam::046402772087:instance-profile/ansible_dynamic_inv

aws-elasticbeanstalk-ec2-role
 arn:aws:iam::046402772087:instance-profile/aws-elasticbeanstalk-ec2-role

aws_capstone_EC2_S3_Full_Access
 arn:aws:iam::046402772087:instance-profile/aws_capstone_EC2_S3_Full_Access

call-ec2-ecr-full-access
 arn:aws:iam::046402772087:instance-profile/call-ec2-ecr-full-access

Call-Jenkins-JenkinsServerEC2Profile-1A152LCKK0G7
 arn:aws:iam::046402772087:instance-profile/Call-Jenkins-JenkinsServerEC2Profile-1A152LCKK0G7

call-rke-role-cohort1
 arn:aws:iam::046402772087:instance-profile/call-rke-role-cohort1

Elastic Inference [Info](#)

Add Elastic Inference accelerators

- User Data

```
#!/bin/bash
apt-get update -y
apt-get install git -y
apt-get install python3 -y
cd /home/ubuntu/
TOKEN="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"
git clone https://$TOKEN@github.com/Kaya-Ramazan/my-aws-capstone-project.git
cd /home/ubuntu/my-aws-capstone-project
apt install python3-pip -y
apt-get install python3.7-dev default-libmysqlclient-dev -y
pip3 install -r requirements.txt
cd /home/ubuntu/my-aws-capstone-project/src
python3 manage.py collectstatic --noinput
python3 manage.py makemigrations
python3 manage.py migrate
python3 manage.py runserver 0.0.0.0:80
```

Metadata version [Info](#)
 Don't include in launch template

Metadata response hop limit [Info](#)
 Don't include in launch template

User data [Info](#)

```
#!/bin/bash
apt-get update -y
apt-get install git -y
```

User data has already been base64 encoded

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

Production Ortamında en basit bir site adahil secur bir baglansti yapmak ister.
 Browserlar sec baglanti var ise

HTTP den yayin Yapmazlar daha secure olan HTTPS den yayin yaparlar increp etmek icin sertifikalari kullanirlar

Step 11: Create certification for secure connection

Go to the certification manager console and click `request a certificate` button. Select `Request a public certificate`

', then `request a certificate` ---> `*.` --> DNS validation --> No tag --> Review --> click confirm and request button. Then it takes a while to be activated

Yeni alamak için;

Certificates

Select validation method

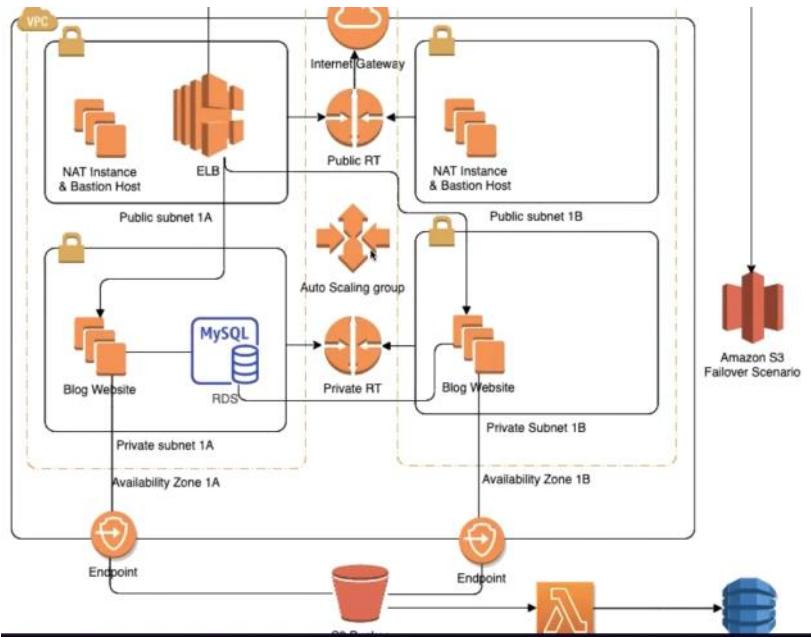
Choose how AWS Certificate Manager (ACM) validates your certificate by using DNS or by sending email to the contact addresses of the domain.

DNS validation

Choose this option if you have or can obtain permission to modify your DNS settings.

Email validation

Choose this option if you do not have permission or cannot modify your DNS settings.



Simdiye kadar yaptıklarımızı özetler isek ;

- Vpc leri kurduk
- Availability zonalar ve Subnetleri ayarladık
- internetGateway baglandı
- Public Subnetleri Asocate ettik
- RDS kurduk
- Endpointimizi verdik

Step 12: Create ALB and Target Group

Go to the Load Balancer section on the left hand side menu of EC2 console. Click `create Load Balancer` button and select Application Load Balancer

```
```text
Name : awscapstoneALB
Schema : internet-facing
```

```

Step 1: Configure Load Balancer

To configure your load balancer, provide a name, select a scheme, specify one or more listeners, and select

Name : awscapstoneALB
 Scheme : internet-facing
 internal
 IP address type : IPv4

Listeners

Listeners : HTTPS, HTTP

Listeners
 A listener is a process that checks for connection requests, using the protocol and port that you configured.

| Load Balancer Protocol | Load Balancer Port |
|------------------------|--------------------|
| HTTP | 80 |
| HTTPS (Secure HTTP) | 443 |
| Add listener | |

Availability Zones :
 - VPC : aws_capstone_VPC
 - **Availability zones:**
 1. aws_capstone-public-subnet-1A
 2. aws_capstone-public-subnet-1B

Availability Zones

Specify the Availability Zones to enable for your load balancer. The load balancer routes traffic to the targets in these Availability Zones on the balancer.

VPC (i) vpc-0142f2295c4ac3c14 (90.90.0.0/16) | aws_capstone-VPC ♦

Availability Zones us-east-1a Select a subnet
 subnet-05335f428f973bc72 (aws_capstone-public-subnet-1A)
 us-east-1b subnet-0bdb543e282ef89b1 (aws_capstone-private-subnet-1A)

Public e yerlestiriyoruz cunku yayanin yapacak

Step 2 - Configure Security Settings

Certificate type --> Choose a certificate from ACM (recommended)

- Certificate name : "*.clarusway.us" certificate
- Security policy : keep it as is

1. Configure Load Balancer 2. Configure Security Settings 3. Configure Security Groups 4. Configure Routing 5. Register Targets 6. Review

Step 2: Configure Security Settings

Select default certificate

AWS Certificate Manager (ACM) is the preferred tool to provision and store server certificates. If you previously stored a server certificate using IAM, you can deploy it to your load balancer. Learn more about ACM

Certificate type Choose a certificate from ACM (recommended)
 Upload a certificate from ACM (recommended)
 Choose a certificate from IAM
 Upload a certificate to IAM

Request a new certificate from ACM
AWS Certificate Manager makes it easy to provision, manage, deploy, and renew SSL Certificates on AWS

Certificate name clarusway.us (arn:aws:acm:us-east-1:046402772067:certificate/0e06d5)

Select Security Policy

Security policy ELBSecurityPolicy-2016-08

Step 3 - Configure Security Groups : aws_capstone_ALB_Sec_group

Step 3: Configure Security Groups

A security group is a set of firewall rules that control the traffic to your load balancer. On this page, you can add rules to allow specific traffic to reach your load balancer. For more information, see Security groups.

Assign a security group Create a new security group
 Select an existing security group

| Security Group ID | Name | Description |
|---|----------------------------|---|
| <input checked="" type="checkbox"/> sg-0b9feea077d1364a | aws_capstone_ALB_Sec_Group | ALB Security Group allows traffic HTTP and HTTPS ports from anywhere |
| <input type="checkbox"/> sg-0360174d6fdb3ff2 | aws_capstone_EC2_Sec_Group | EC2 Security Groups only allows traffic coming from aws_capstone_ALB_Sec_Group Security Group |
| <input type="checkbox"/> sg-0de419856420b842a | aws_capstone_NAT_Sec_Group | NAT Security Group allows traffic HTTP and HTTPS and SSH ports from anywhere |
| <input type="checkbox"/> sg-0de2ae839b36b26ae | aws_capstone_RDS_Sec_Group | EC2 Security Groups only allows traffic coming from aws_capstone_EC2_Sec_Group Security Group |
| <input type="checkbox"/> sg-0bfef2bb9c60bc7ac | default | default VPC security group |

Step 4 - Configure Routing

- Target group : New target group
- Name : awscapstoneTargetGroup
- Target Type : Instance
- Protocol : HTTP
- Port : 80

Step 4: Configure Routing

Your load balancer routes requests to the targets in this target group using the protocol and port that you specify here. It also performs health checks on the targets using these settings. The target group you specify in this step will apply to all of the listeners configured on this load balancer. You can change the target group or add listeners after the load balancer is created.

Target group

Target group New target group
Name awscapstoneTargetGroup
Target type Instance
 IP
 Lambda function

Protocol HTTP HTTP2
Port 80 443

Protocol version HTTP1.1 Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.
 HTTP2 Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.
 gRPC Send requests to targets using gRPC. Supported when the request protocol is gRPC.

Health checks

Protocol HTTP TCP
Path /



Instance nerede calisiyorsa o portta calistirmamiz gerekiyor

- Protocol version : HTTP1
- Health Check :
- Protocol : HTTP
- Path : /
- Port : traffic port
- Healthy threshold : 5 ----- ard ardigina 3 saglik sinyalini olarak muhurluyor
- Unhealthy threshold : 2-----ard ardigina 2 kez

```

gönderdi ve cevap alamadı sagıksız olarak nitelendiriyor
  - Timeout      : 5 -----sinyali gönderdikten
sonra bekleme süresi
  - Interval     : 20
  - Success Code : 200 ----- herhangi problem yok
demejdir.

```

Health checks

Protocol: HTTP
Path: /

Advanced health check settings

Port: traffic port
Healthy threshold: 5
Unhealthy threshold: 2
Timeout: 5 seconds
Interval: 30 seconds
Success codes: 200

Step 5 - Register Targets

without register any target click Next: Review

...

- click create
To redirect traffic from HTTP to HTTPS, go to the ALB console and select Listeners sub-section.

```text

select HTTP: 80 rule --> click edit  
- Default action(s)  
- Remove existing rule and create new rule which is  
 - Redirect to HTTPS 443  
 - Original host, path, query  
 - 301 - permanently moved

...

Lets go ahead and look at our ALB DNS --> it going to say "it is not safe", however, it will be fixed after settings of Route 53

Load balanceri oluşturduktan sonra yayını 80 portundan gelen yayını mevcutta Target Guruba gönderiyor iken Biz Önce 443 HTTPS e göndermesini ve sonrasında Target guruba gitmemisini istiyorduk. Bu şekilde daha secure olacaktı.

| Listener ID                           | Security policy           | SSL Certificate                                    | Rules                                                                                   |
|---------------------------------------|---------------------------|----------------------------------------------------|-----------------------------------------------------------------------------------------|
| HTTP: 80<br>arn:...d1af6e0105-        | N/A                       | N/A                                                | Default: forwarding to awscapstoneTargetGroup<br><a href="#">View/edit rules</a>        |
| HTTPS: 443<br>arn:...01e4c8c08ab8dddf | ELBSecurityPolicy-2016-08 | Default: 0e08d98e-f585-4773-93fd-8a83ab26bdd (ACM) | Default: forwarding to awscapstoneTargetGroup<br><a href="#">View/edit certificates</a> |

Bunun için 80 bağlantısını tıklayıp edit diyoruz.

**awscapstoneALB | HTTP : 80**

Listeners belonging to Application Load Balancers check for connection requests u are routed. Once you have created your listener, you can create and manage additk

**ARN**  
arn:aws:elasticloadbalancing:us-east-1:046402772087:listener/app/awscapstoneAl

**Protocol : port**  
Select the protocol for connections from the client to your load balancer, and enter a port

HTTP : 80

**Default action(s)**  
Indicate how this listener will route traffic that is not otherwise routed by a another rule.

1. Forward to awscapstoneTargetGroup: 1 (100%)  
Group-level stickiness: Off

+ Add action

Ardından default olan Forwardı siliyoruz.

**awscapstoneALB | HTTP : 80**

Listeners belonging to Application Load Balancers check for connection requests u are routed. Once you have created your listener, you can create and manage additc

**ARN**  
arn:aws:elasticloadbalancing:us-east-1:046402772087:listener/app/awscapstoneAl

**Protocol : port**  
Select the protocol for connections from the client to your load balancer, and enter a port

HTTP : 80

**Default action(s)**  
Indicate how this listener will route traffic that is not otherwise routed by a another rule.

+ Add action  
Forward to...  
Redirect to...  
Return fixed response...

Note: Additional actions are available for HTTPS listeners.

Ve Redirection ekliyoruz ve 443 secip tikliyoruz.

**awscapstoneALB | HTTP : 80**

Listeners belonging to Application Load Balancers check for connection requests using the protocol are routed. Once you have created your listener, you can create and manage additional routing rules

**ARN**  
arn:aws:elasticloadbalancing:us-east-1:046402772087:listener/app/awscapstoneALB/07ad59df1e

**Protocol : port**  
Select the protocol for connections from the client to your load balancer, and enter a port number from whic

HTTP : 80

**Default action(s)**  
Indicate how this listener will route traffic that is not otherwise routed by a another rule.

1. Redirect to...  
HTTPS : 443 Original value: #(port)  
Original host, path, query  
301 - Permanently moved  
Switch to full URL  
+ Add action

## Step 13: Create Autoscaling Group with Launch Tem plate

Go to the **Autoscaling Group** on the left hand side menu. Cli

ck create Autoscaling group.

- Choose launch template or configuration

```text  
Auto Scaling group name : aws_capstone_ASG
Launch Template : aws_capstone_launch_template
ate
````

EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1: Choose launch template or configuration [Info](#)  
Specify a launch template that contains settings common to all EC2 instances that are launched by this Auto Scaling group. If you currently use launch configurations, you might consider migrating to launch templates.

Step 2: Configure settings

Step 3: Configure advanced options

Step 4 (optional): Configure group size and scaling policies

Step 5 (optional): Add notifications

Step 6 (optional): Add tags

Step 7: Review

**Choose launch template or configuration**

Name: aws\_capstone\_ASG

Launch template: aws\_capstone\_launch\_template

Version: Default (1)

- Configure settings

```text  
Instance purchase options : Adhere to launch template
Network:
- VPC : aws-capstone-VPC
- Subnets : Private 1A and Private 1B
````

#### Instance purchase options [Info](#)

Use the launch template to create a uniform configuration among all of the instances in the group. Or define options to accommodate a wide variety of requirements, such as launching Spot and On-Demand Instances.

- Adhere to launch template  
The launch template determines the purchase option (On-Demand or Spot) and instance type.
- Combine purchase options and instance types  
Specify how much On-Demand and Spot capacity to launch and multiple instance types (optional). This choice is most helpful for optimizing the scale and cost for a fleet of instances.

#### Network [Info](#)

For most applications, you can use multiple Availability Zones and let EC2 Auto Scaling balance your instances across the zones. The default VPC and default subnets are suitable for getting started quickly.

VPC: vpc-0142f2295c4ac5c14 (aws\_capstone-VPC) 90.90.0.0/16

Create a VPC [\[ \]](#)

Subnets:

Select subnets us-east-1a | subnet-0bdb543e282ef89b1 (aws\_capstone-private-subnet-1A) 90.90.11.0/24 us-east-1b | subnet-01e80641d4d2ade39

- Configure advanced options

```text  
- Load balancing : Attach to an existing load balancer
- Choose from your load balancer target groups : awscapstoneTargetGroup
````

#### 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 awscapstoneTargetGroup | HTTP Application Load Balancer: awscapstoneALB

```
- Health Checks
 - Health Check Type : ELB
 - Health check grace period : 300
```

#### Health checks - optional

Health check type [Info](#)  
EC2 Auto Scaling automatically replaces instances that fail health checks. If you enabled load balancing, you can enable ELB health checks in addition to the EC2 health checks that are always enabled.

EC2     ELB

Health check grace period  
The amount of time until EC2 Auto Scaling performs the first health check on new instances after they are [put](#) into service.

300 seconds

```
- Configure group size and scaling policies
```

```
```text
```

Group size

- Desired capacity : 2
- Minimum capacity : 2
- Maximum capacity : 4

Scaling policies

- [Target tracking scaling policy](#)
 - Scaling policy name : Target Tracking Policy
 - Metric Type : Average CPU utilization
 - Target value : 70

```
- Add notifications
```

```
```text
```

#### Create new Notification

- Notification1
  - Send a notification to : aws-capstone-SNS
  - With these recipients : serdar@clarusway.com
  - event type : select all

Choose whether to use a scaling policy to dynamically resize your Auto Scaling group to meet changes in demand. [Info](#)

[Target tracking scaling policy](#)  
Choose a desired outcome and leave it to the scaling policy to add and remove capacity as needed to achieve that outcome.

[None](#)

Scaling policy name

Target Tracking Policy

Metric type

Average CPU utilization

Target value

70

Instances need

300 seconds warm up before including in metric

Disable scale in to create only a scale-out policy

#### Instance scale-in protection - optional

##### Instance scale-in protection

If protect from scale in is enabled, newly launched instances will be protected from scale in by default.

Enable instance scale-in protection

[Cancel](#) [Previous](#) [Skip to review](#) [Next](#)

**Target Training Policy Ec2 instance olusmasi veya hutch  
Terminate ettilirmesi icin belirtildir.**

**CPU Utilazition ortalama Cpu kullanimi bizim belirledigimiz  
degere ulasirsa yeni bir instance kuracak altinda kalirsa  
mevcudu koruyacaktir.**

<!-- WARNING!!! Sometimes your EC2 has a problem after you  
create autoscaling group, If you need to look inside one of

```

your instance to make sure where the problem is, please fo
llow these steps...
```
bash
eval "$(ssh-agent)" (your local)
ssh-add <pem-key> (your local )
ssh -A ec2-
user@<Public IP or DNS name of NAT instance> (your local)
ssh ubuntu@<Public IP or DNS name of private instance> (NA
T instance)
You are in the private EC2 instance
```
-->

```

▲ Not secure awscapstonealb-289774884.us-east-1.elb.amazonaws.com



Your connection is not private

Attackers might be trying to steal your information from [awscapstonealb-289774884.us-east-1.elb.amazonaws.com](http://awscapstonealb-289774884.us-east-1.elb.amazonaws.com) (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR\_CERT\_COMMON\_NAME\_INVALID

[Advanced](#)

[Back to safety](#)



Load balancer in DNS name ini alip Consola yapistirinca karsimiza cikan ekran  
da sol alt kism da ADVANCE tikliyoruz

Hala not secure gözükmesinin sebebi biz sertifikalari Host Name icin  
tanimladik Road Balancer in cikarttigi adres icin degil Dolayisiyla bunu oraya  
yönkendirmemiz gerekiyor

Azciyan sayfada ilk oalrak Register edecegiz ve kendimizde bir Mail ve sifre  
belirleyip sisteme girecegiz

larusway Blog Home About

## Blog Post

Title\*

Content\*

Image\*

No file chosen

Category\*

Status\*

Ve daha sonra

Post updated!!

# Clarusway Blog



## My Working Room

hard working It

 0  1  0

Posted 1 minute ago.

## ## Step 14: Create Cloudfront in front of ALB

**Go to the cloudfront menu and click start**  
**- Origin Settings**

**Load balancer in Domain Name ini isretliyoruz**

```
```text
Origin Domain Name      : aws-capstone-
ALB-1947210493.us-east-2.elb.amazonaws.com
Origin Path             : Leave empty (this means, define for root '/')
```

```

|           |   |              |
|-----------|---|--------------|
| Protocol  | : | Match Viewer |
| HTTP Port | : | 80           |
| HTTPS     | : | 443          |

|                             |                                                                                                                                         |                         |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| Origin Domain Name          | awscapstoneALB-1737831641.us-east-1                                                                                                     | <a href="#">i</a>       |
| Origin Path                 |                                                                                                                                         | <a href="#">i</a>       |
| Enable Origin Shield        | <input checked="" type="radio"/> Yes<br><input type="radio"/> No                                                                        | <a href="#">i</a>       |
| Origin ID                   | ELB-awscapstoneALB-1737831641                                                                                                           | <a href="#">i</a>       |
| Minimum Origin SSL Protocol | <input type="radio"/> TLSv1.2<br><input type="radio"/> TLSv1.1<br><input checked="" type="radio"/> TLSv1<br><input type="radio"/> SSLv3 | <a href="#">i</a>       |
| Origin Protocol Policy      | <input type="radio"/> HTTP Only<br><input type="radio"/> HTTPS Only<br><input checked="" type="radio"/> Match Viewer                    | <a href="#">i</a>       |
| Origin Connection Attempts  | 3                                                                                                                                       | <a href="#">i</a>       |
| Origin Connection Timeout   | 10                                                                                                                                      | <a href="#">i</a>       |
| Origin Response Timeout     | 30                                                                                                                                      | <a href="#">i</a>       |
| Origin Keep-alive Timeout   | 5                                                                                                                                       | <a href="#">i</a>       |
| HTTP Port                   | 80                                                                                                                                      | <a href="#">i</a>       |
| HTTPS Port                  | 443                                                                                                                                     | <a href="#">i</a>       |
| Origin Custom Headers       | Header Name                                                                                                                             | Value <a href="#">i</a> |
| <input type="text"/>        |                                                                                                                                         |                         |

#### Default Cache Behavior Settings

Path Pattern Default (\*) [i](#)

```
Minimum Origin SSL Protocol : Keep it as is
Name : Keep it as is
Add custom header : No header
Enable Origin Shield : No
Additional settings : Keep it as is
```

```

Default Cache Behavior Settings

```
```
text
Path pattern : Default
t (*)
Compress objects automatically : Yes
Viewer Protocol Policy : Redirect
ct HTTP to HTTPS
Allowed HTTP Methods : GET, H
EAD, OPTIONS, PUT, POST, PATCH, DELETE
Cached HTTP Methods : Select
OPTIONS
Cache key and origin requests
- Use legacy cache settings
```

|                                         |                                                                                                                                                              |                   |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| Path Pattern                            | Default (*)                                                                                                                                                  | <a href="#">i</a> |
| Viewer Protocol Policy                  | <input type="radio"/> HTTP and HTTPS<br><input checked="" type="radio"/> Redirect HTTP to HTTPS<br><input type="radio"/> HTTPS Only                          | <a href="#">i</a> |
| Allowed HTTP Methods                    | <input type="radio"/> GET, HEAD<br><input type="radio"/> GET, HEAD, OPTIONS<br><input checked="" type="radio"/> GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE | <a href="#">i</a> |
| Field-level Encryption Config           | <input type="button"/>                                                                                                                                       | <a href="#">i</a> |
| Cached HTTP Methods                     | GET, HEAD (Cached by default)<br><input checked="" type="checkbox"/> OPTIONS                                                                                 | <a href="#">i</a> |
| Cache and origin request settings       | <input type="radio"/> Use a cache policy and origin request policy<br><input checked="" type="radio"/> Use legacy cache settings                             | <a href="#">i</a> |
| Cache Based on Selected Request Headers | Whitelist <a href="#">i</a>                                                                                                                                  | <a href="#">i</a> |
| Learn More                              |                                                                                                                                                              |                   |

|                                                                                                                                                                                                                                                                                      |                   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| Whitelist Headers                                                                                                                                                                                                                                                                    | <a href="#">i</a> |
| <input type="text"/> Filter headers or enter a custom header <a href="#">Add Custom &gt;&gt;</a> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> Accept<br/>Accept-Charset<br/>Accept-Datetime<br/>Accept-Encoding<br/>Accept-Language<br/>Authorization </div> |                   |
| To use AWS ELB DNS named Origins, you must forward the Host or All headers. <a href="#">Learn more</a> .                                                                                                                                                                             |                   |

Object Caching  Use Origin Cache Headers  
 Customize [i](#)

**Headerlarda neleri cashlemesini istiyorsak onlari secebiliyoruz**

Headers : Include the following headers

Add Header

- Accept
- Accept-Charset
- Accept-Datetime
- Accept-Encoding
- Accept-Language
- Authorization
- Cloudfront-Forwarded-Proto
- Host
- Origin
- Referer

Forward Cookies : All

Query String Forwarding and Caching : All

Other stuff : Keep them as are

``

Object Caching

Use Origin Cache Headers

Customize

[Learn More](#)

Minimum TTL

Maximum TTL

Default TTL

Forward Cookies

Query String Forwarding and Caching

Smooth Streaming  Yes  No

Restrict Viewer Access (Use Signed URLs or Signed Cookies)  Yes  No

Compress Objects Automatically  Yes  No

[Learn More](#)

Edge Function Associations

| Edge Function                         | CloudFront Event                      | Function                              |
|---------------------------------------|---------------------------------------|---------------------------------------|
| <input type="button" value="Create"/> | <input type="button" value="Create"/> | <input type="button" value="Create"/> |

- Distribution Settings

```text

Price Class : Use all edge locations (best performance)

Alternate Domain Names : www.clarusway.us

SSL Certificate : Custom SSL Certificate (example.com) ---> Select your certificate created before

Other stuff : Keep them as are

````

Lambda@Edge

[Learn More](#)

Enable Real-time Logs  Yes  No

#### Distribution Settings

Price Class

AWS WAF Web ACL

Alternate Domain Names (CNAMEs)

SSL Certificate  Default CloudFront Certificate (\*.cloudfront.net)

Choose this option if you want your users to use HTTPS or HTTP to access your content with the CloudFront domain name <https://d111111abcedf8.cloudfront.net/logo.jpg>.  
Important: If you choose this option, CloudFront requires that browsers or devices support TLSv1 or later to access your content.

Custom SSL Certificate (example.com):

Choose this option if you want your users to access your content by using an alternate domain name, such as <https://www.clarusway.us>. You can use a certificate stored in AWS Certificate Manager (ACM) in the US East (N. Virginia) Region, or you can use a certificate stored in IAM.

[Learn more about using custom SSL/TLS certificates with CloudFront.](#)

[Learn more about using ACM.](#)

Aynı zaman bu Ec2 lar ELB ye bağlı olacak ELB nin en önemli özellikle EC2 lardaki yoğunluga bakıp HealthCheck ler ile herhangi yoğunluk olması durumunda eşit olarak bu

**yuklu EC2 lar arasında dağıtmak. Hem Trafigi yayınıyor hem tek ilden dağılımı sağlıyor. Hemde Dis dünyadan gelen User In her hangi bir aksama olmadan EC2 ya ulaşmasını sağlıyor.**

**ALB nin de önune bir CloudFront koyacagız ki bu da br cash hizmeti sunacak. Videolar ve fotoğraflar S3 den çekilecek her seferinde ücret ödenmemesi için bunu yapacaklar Cash hizmeti ile sağlanacak.**

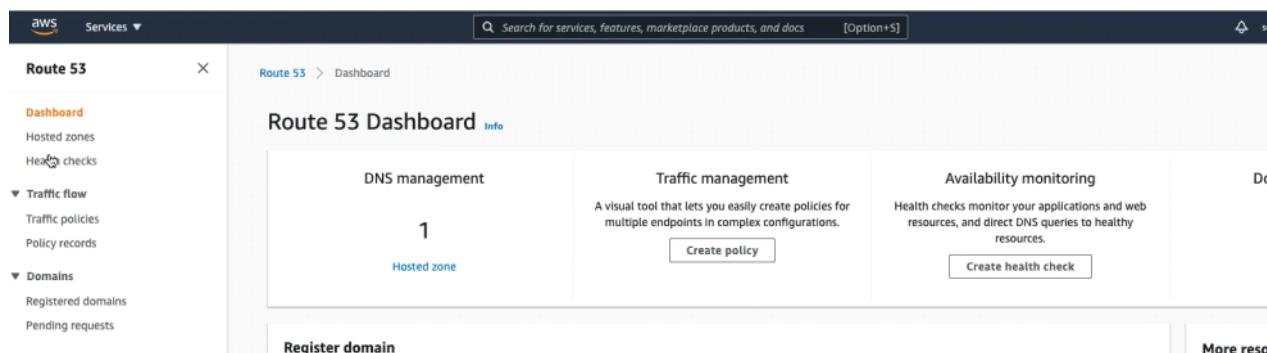
**Production ortamında Cloudfront s3 un önune de kurulabiliyor Eger burda tanımlamak istersek s3 u orjin olarak gösterecektir.**

**Developerler kodunu kullanıcı karsısına cikartmak için Route53 failover senaryosu ile karsımıza cıkacak.**

**Burada Failover senaryosu Route 53 olarak bir ister atanmış durumdadır. Route53 de iki adet ent pointı takip eder. Birisi static website olur. Degiride uniq olarak caallsan web sitemizdir.basına herhangi bir durum gelmesi halinde secondary e trafigi yönlendirir.**

**Userlar bu haliyle karsılarına bir sey cıkarı mevcut olarak bir sorunun olduğunu ve bu sorunun bir sure sonra çözülecegi gibi seyler icerebilir.**

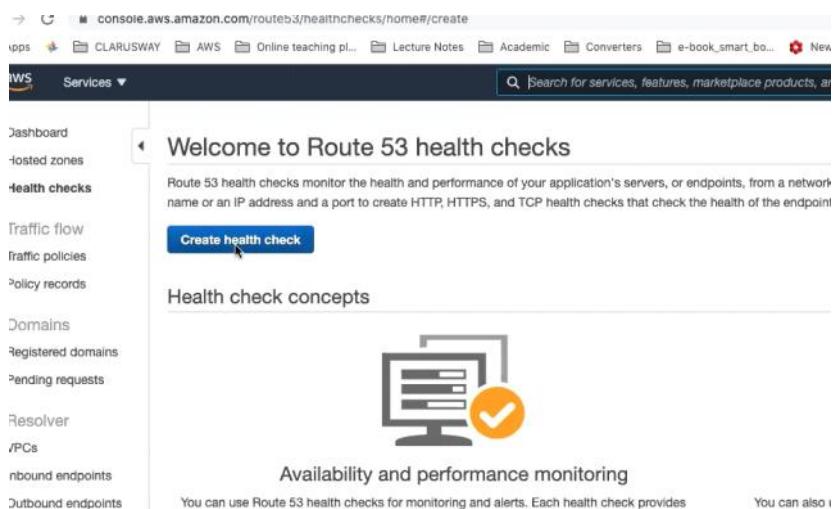
Simdide Route53 e gidecegiz Failover senaryosunu olusturmak icin.



The screenshot shows the AWS Route 53 dashboard. On the left, there's a sidebar with options like Dashboard, Hosted zones, Health checks, Traffic flow, Domains, and Register domain. The main area is titled "Route 53 Dashboard" and contains three sections: "DNS management" (1 Hosted zone), "Traffic management", and "Availability monitoring". Each section has a "Create policy" or "Create health check" button.

**## Step 15: Create Route 53 with Failover settings**

**Come to the Route53 console and select Health checks on the left hand menu. Click create health check**



The screenshot shows the "Welcome to Route 53 health checks" page. It features a "Create health check" button and a "Health check concepts" section with an icon of a computer monitor with a checkmark. Below this is a section titled "Availability and performance monitoring" with the text: "You can use Route 53 health checks for monitoring and alerts. Each health check provides You can also..."

```

Configure health check
```text
Name : aws capstone health check
What to monitor : Endpoint
Specify endpoint by : Domain Name
```

```

Best practices to optimize Lambda@Edge with CloudFront. [Learn more](#)

**Important:** On March 23, 2021, CloudFront will begin migrating the Certificate Authority for the \*.cloudfront.net certificate. For more information, refer to the [AWS Documentation](#).

## CloudFront Distributions

| Create Distribution |                |                               |           |                  |                 |  |
|---------------------|----------------|-------------------------------|-----------|------------------|-----------------|--|
| Viewing :           |                | Any Delivery Method           | Any State | Actions          |                 |  |
| Delivery Method     | ID             | Domain Name                   | Comment   | Origin           | CNAMEs          |  |
| Web                 | E37YJ8L1Q4R6V8 | d30l021hm3ex15.cloudfront.net | -         | awscapstoneALB-1 | www.claruswa... |  |

CloudFront taki Domain Name alip buraya kopyaliyoruz.

```

Protocol : HTTP
Domain Name : Write cloudfont domain name
Port : 80
Path : leave it blank
Other stuff : Keep them as are
```

```

The screenshot shows the AWS Route 53 Dashboard. It includes sections for DNS management (1 Hosted zone), Traffic management (Create policy), Availability monitoring (1 Health check), and Domain registration (1 Domain). There are also sections for Register domain, Notifications, and Service health.

- Click **Hosted zones** on the left hand menu
- click your Hosted zone : <YOUR DNS NAME>
- Create Failover scenario
- Click **Create Record**
- Select **Failover** ---> Click Next

clarusway.us [Info](#)

[Hosted zone details](#) [Edit hosted zone](#)

[Records \(4\)](#) [DNSSEC signing](#) [Hosted zone tags \(0\)](#)

Records (4) [Info](#)
Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.

<input type="checkbox"/>	Record name	Type	Routin...	Differ...	Value/Route traffic to
<input type="checkbox"/>	clarusway.us	NS	Simple	-	ns-435.awsdns-54.com. ns-1415.awsdns-48.org. ns-861.awsdns-43.net. ns-1648.awsdns-14.co.uk.
<input type="checkbox"/>	clarusway.us	SOA	Simple	-	ns-435.awsdns-54.com. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400
<input type="checkbox"/>	_35c2c6a1969f121d13c875477...	CNAME	Simple	-	_64d4256ba727964ee9dd657a42016674.zxlnyslw.acm-validations.aws.
<input type="checkbox"/>	_4f75946af91639a9da4632cf...	CNAME	Simple	-	_9810a47cc0708ff712ded78ecd990c4.wggjkgmgrm.acm-validations.aws.

Route 53 > Hosted zones > clarusway.us > Create record

Step 1 [Choose routing policy Info](#)

The routing policy determines how Amazon Route 53 responds to queries.

Step 2 [Configuring records](#)

Routing policy [Switch to quick create](#)

Simple routing Use if you're routing traffic to just one endpoint, such as a website.

Weighted Use when you have multiple resources that do the same job, and you want to specify the proportion of requests to each resource. For example, two or more EC2 instances.

Geolocation Use when you want to route traffic based on the location of your users.

Latency Use when you have resources in different locations and you want to route traffic to the Region that provides the best latency.

Failover Use to route traffic to a resource when it's healthy, and route traffic to a different resource when the first resource is unhealthy.

Multivalue answer Use when you want Route 53 to return multiple answers with up to eight randomly selected at random.

[Cancel](#) [Next Step](#)

```
```text
Configure records
Record name : www.<YOUR DNS NAME>
Record Type : A - Routes traffic to an IPv4 address and some AWS resources
TTL

```

Record name [Info](#)  
To route traffic to a subdomain, enter the subdomain name. For example, to route traffic to blog.example.com, enter blog. If you leave this field blank, the default record name is the name of the domain.

clarusway.us

Valid characters: a-z, 0-9, ! # \$ % & ^ \_ \* , - / ; < = > ? @ [ \ ] ^ \_ ` { } , ~

Record type [Info](#)  
The DNS type of the record determines the format of the value that Route 53 returns in response to DNS queries.

A - Routes traffic to an IPv4 address and some AWS resources

Choose when routing traffic to AWS resources for EC2, API Gateway, Amazon VPC, CloudFront, Elastic Beanstalk, ELB, or S3. For example: 192.0.2.44.

TTL (seconds) [Info](#)  
The amount of time, in seconds, that DNS resolvers and web browsers cache the settings in this record. ("TTL" means "time to live.")

300

1m  1h  1d

Recommended values: 60 to 172800 (two days)

Failover records to add to clarusway.us [Info](#)  
Use to route traffic to a resource when the resource is healthy, or to a different resource when the first resource is unhealthy.

[Edit](#) [Delete](#) [Define failover record](#)

Record ID	Failover record type	Value/Route traffic to	Health check

Define failover records to this list, then choose [Create records](#).

```
```text
: 300
---> First we'll create a primary record for cloudfront
Failover record to add to your DNS ---> Define failover record
Value/Route traffic to : Alias to cloudfront distribution
                        - Select created cloudfront DNS
Failover record type   : Primary
Health check          : aws capstone health check
Record ID              : Cloudfront as Primary Record

```

Define failover record

specify where you want to route internet traffic.

Alias to CloudFront distribution : US East (N. Virginia)

Failover record type : Primary

Health check : aws capstone health check

Evaluate target health : No

Record ID : this record was created for cloudfront and it is a primary one

Define failover record

----> Second we'll create secondary record for S3
 Failover another record to add to your DNS ---> Define failover record
 Value/Route traffic to : Alias to S3 website endpoint
 - Select Region
 - Your created bucket name emerge
 s ---> Select it
 Failover record type : Secondary
 Health check : No health check
 Record ID : S3 Bucket for Secondary record type
 -->
 - click create records

Define failover record

Value/Route traffic to : US East (N. Virginia) [us-east-1]

Failover record type : Secondary

Health check - optional : Choose health check

Evaluate target health : Yes

Record ID : This record is the secondary one

Define failover record

Artık sitemiz yayın yapmaya başladı ve secure bir yayındır.
 CloudFront ile oluşturduğumuz yayı su anda secure bir bagalantı

Clarusway Blog



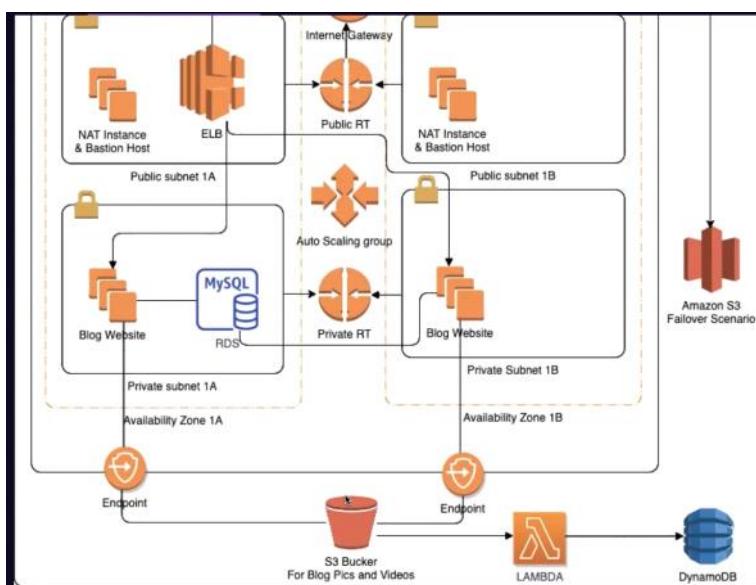
My Working Room

hard working it

0 1 0

Posted 19 hours, 42 minutes ago.

Simdi secure bir baglanti yapmis oldulk



Developerlar s3 de atilan objelerin takibini yapmak icin DYNAMODB de liste haliunde bunun takibini yapmak istiyor lar

Step 16: Create DynamoDB Table

Go to the Dynamo Db table and click create table button

- Create DynamoDB table

```text

```
Name : awscapstoneDynamo
Primary key : id
Other Stuff : Keep them as are
click create
```

#### Create DynamoDB table

Tutorial ?

DynamoDB is a schema-less database that only requires a table name and primary key. The table's primary key is made up of one or two attributes that uniquely identify items, partition the data, and sort data within each partition.

|                                       |                   |
|---------------------------------------|-------------------|
| Table name*                           | awscapstoneDynamo |
| Primary key*                          | Partition key     |
| id String                             |                   |
| <input type="checkbox"/> Add sort key |                   |

#### Table settings

Default settings provide the fastest way to get started with your table. You can modify these default settings now or after your table has been created.

Use default settings

- No secondary indexes.
- Auto Scaling capacity set to 70% target utilization, at minimum capacity of 5 reads and 5 writes.
- Encryption at Rest with DEFAULT encryption type.

+ Add tags NEW

Additional charges may apply if you exceed the AWS Free Tier levels for CloudWatch or Simple Notification Service. Advanced alarm settings are available in the CloudWatch management console.

Cancel **Create**

## ## Step 17-18: Create Lambda function

Lambda Fonksiyonunun s3 e ulasmasi lazim yani konusmasi lazim ayrica Dynamodb ile konususyor olamsi a+lazim ayrica Network alt yapisinda irtibatalanmasi gerekiyor

Before we create our Lambda function, **we should create IAM role** that we'll use for Lambda function. Go to the IAM console and select role on the left hand menu, then create role button

```text

Select Lambda as trusted entity ----> click Next:Permission

Choose: - LambdaS3fullaccess,
- Network Administrator
- DynamoDBFullAccess

Create role

1 2 3 4

Attach permissions policies

Choose one or more policies to attach to your new role.

| Filter policies | | Q Search | Showing 8 results |
|-------------------------------------|--|------------------------|-------------------|
| | Policy name | Used as | |
| <input checked="" type="checkbox"/> | AmazonDynamoDBFullAccess | None | |
| <input type="checkbox"/> | AmazonDynamoDBReadOnlyAccess | None | |
| <input type="checkbox"/> | AWSApplicationAutoScalingDynamoDBTablePolicy | Permissions policy (1) | |
| <input type="checkbox"/> | AWSLambdaDynamoDBExecutionRole | None | |
| <input type="checkbox"/> | AWSLambdaInvocation-DynamoDB | None | |
| <input type="checkbox"/> | DynamoDBCloudWatchContributorInsightsServiceRolePolicy | None | |
| <input type="checkbox"/> | DynamoDBKinesisReplicationServiceRolePolicy | None | |
| <input type="checkbox"/> | DynamoDBReplicationServiceRolePolicy | None | |

Set permissions boundary

No tags

Role Name : **aws_capstone_lambda_Role**
Role description : This role give a permission to lambda to reach S3 and DynamoDB on custom VPC

then, go to the Lambda Console and click **create function**

- Basic Information

```text

**Create function** info

Choose one of the following options to create your function.

Author from scratch      Start with a simple Hello World example.

Use a blueprint      Build a Lambda application from sample code and configuration presets for common use cases.

Container image      Select a container image to deploy for your function.

Browse serverless      Deploy a sample Lamb Serverless Application

**Basic information**

Function name  
Enter a name that describes the purpose of your function.  
**aws\_capstone\_lambda\_function**

Use only letters, numbers, hyphens, or underscores with no spaces.

Runtime info  
Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.  
**Python 3.8**

Permissions info  
By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this default role later when adding triggers.

Change default execution role

Advanced settings

## Permissions [Info](#)

By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs.

### ▼ Change default execution role

#### Execution role

Choose a role that defines the permissions of your function. To create a custom role, go to

- Create a new role with basic Lambda permissions
- Use an existing role
- Create a new role from AWS policy templates

#### Existing role

Choose an existing role that you've created to be used with this Lambda function. The role

```
Function Name : awscapsitonelambdafunction
Runtime : Python 3.8
Create IAM role : S3 full access policy
Advance Setting: Network
 - VPC : aws-capstone-VPC
 - Subnets : Select all subnets
 - Security Group: Select default security Group
```

```

- Now we'll go to the S3 bucket belongs our website and create an event to trigger our Lambda function.

Code signing configuration - optional [Info](#)
To enable code signing, choose a configuration that defines the signature validation policy and the signing profiles that are permitted to sign code.
Choose a code signing configuration ARN

Network
To provide network access for your Lambda function, specify a virtual private cloud (VPC), VPC subnets, and VPC security groups. VPC configuration is optional unless your user permissions require you to configure a VPC.

VPC - optional [Info](#)
Choose a VPC for your function to access.
vpc-0142f2295c4ac3c14 (90.90.0.0/16)

Subnets
Select the VPC subnets for Lambda to use to set up your VPC configuration.
Choose subnets

subnet-01e80641d4d2ade39 (90.90.21.0/24) us-east-1b X	subnet-05335f428f973bc72 (90.90.10.0/24) us-east-1a X	subnet-099966662f9dd3a13 (90.90.20.0/24) us-east-1b X
Name: aws_capstone-private-subnet-1B	Name: aws_capstone-public-subnet-1A	Name: aws_capstone-public-subnet-1B

subnet-0bdb543e282ef89b1 (90.90.11.0/24) us-east-1a X
Name: aws_capstone-private-subnet-1A

Security groups
Choose the VPC security groups for Lambda to use to set up your VPC configuration. The table below shows the inbound and outbound rules for the security groups that you choose.

Choose security groups

sg-0befef2bb9c60bc7ac (default) X
default VPC security group

Inbound rules Outbound rules

Ve simdi de s3 de event olusturacagiz; bu s3 bucket imiizin altina ne dosya atilisra bir event olsuturmasini isteyecegiz

Amazon S3 > awscapstones3ramazanblog > media/ > blog/ > 1/

1/

[Copy S3 URI](#)

Objects Properties

Objects (1)

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](#)

[Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

Find objects by prefix

< 1 >

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	Calisma_ortamı.jpeg	jpeg	August 27, 2021, 20:13:30 (UTC+03:00)	129.6 KB	Standard

Bucketimizin----- Properties kismina tiklayip daha sonra----- event notifications kismina tiklayacagiz

Evevt Notifications S3 un bucktin altinda her hangi bir sey olusstugu takdirde onu event olusturur

Ve bu event i Lambda functiona tanitacagiz

Step 17-18: Create S3 Event and set it as trigger for Lambda Function

Go to the S3 console and select the S3 bucket named `awscapstonec3<name>blog`.

- Go to the properties menu ---> Go to the Event notifications part

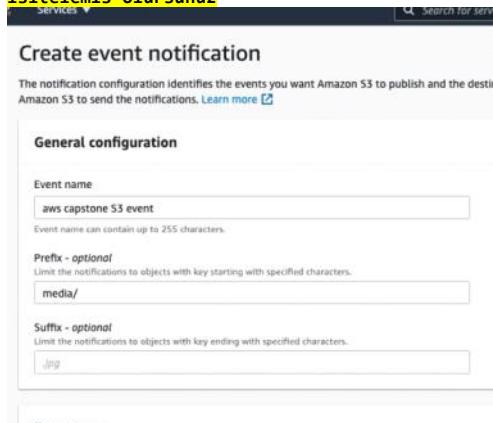
- Click **create event notification** for creating object

``text

Event Name : aws capstone S3 event

Prefix : media/

Egerki Suffix kismina jpeg belirtirseniz sadece jpegleri Isitelemis olursunuz



Create event notification

The notification configuration identifies the events you want Amazon S3 to publish and the destination Amazon S3 to send the notifications. [Learn more](#)

General configuration

Event name

aws capstone S3 event

Event name can contain up to 255 characters.

Prefix - optional

Limit the notifications to objects with key starting with specified characters.

media/

Suffix - optional

Limit the notifications to objects with key ending with specified characters.

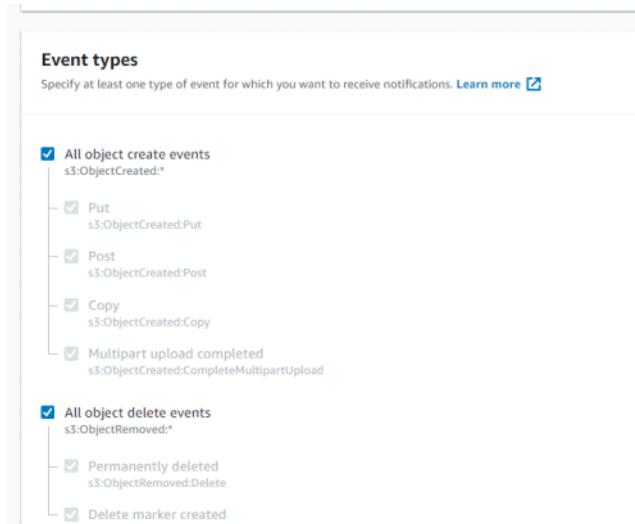
.jpg

Select :
- All object create events

Destination : Lambda Function

Specify Lambda function : Choose from your Lambda functions

Lambda function : awscapstonelambdafunction
click save



Event types
Specify at least one type of event for which you want to receive notifications. [Learn more](#)

All object create events
s3:ObjectCreated:
 Put
s3:ObjectCreated:Put
 Post
s3:ObjectCreated:Post
 Copy
s3:ObjectCreated:Copy
 Multipart upload completed
s3:ObjectCreated:CompleteMultipartUpload

All object delete events
s3:ObjectRemoved:
 Permanently deleted
s3:ObjectRemoved:Delete
 Delete marker created

```

```text
```
- After create an event go to the `awscapstonelambdafunction` lambda Function and click add trigger on the top left hand side.
- For defining trigger for creating objects

```

The screenshot shows the AWS Lambda console interface. At the top, there's a navigation bar with 'Lambda > Functions > awscapstonelambdafunction'. Below it is a title bar 'awscapstonelambdafunction'. Underneath is a 'Function overview' section with tabs for 'Info', 'Code', 'Test', 'Monitor', 'Configuration', 'Aliases', and 'Versions'. The 'Code' tab is active. In the main content area, there's a Lambda icon labeled 'awscapstonelambdafunction', a 'Layers' section showing '(0)', and a large 'Add trigger' button. Below this, there's a code editor with tabs for 'File', 'Edit', 'Find', 'View', 'Go', 'Tools', 'Window', 'Test', 'Deploy', and 'Changes deployed' (which is highlighted). The code editor shows a single file named 'lambda_function.py' under a folder 'awscapstonelambdafunction'. The code itself is partially visible.

```

```text
Trigger configuration : S3
Bucket : awscapstonec3<name>blog
Event type : All object create events
Check the warning message and click add ---- sometimes it says overlapping situation. When it occurs, try refresh page and create a new trigger or remove the s3 event and recreate again. then again create a trigger for lambda function
```

```

The screenshot shows the 'Add trigger' configuration page. At the top, there's a navigation bar with 'Lambda > Add trigger'. Below it is a title bar 'Add trigger'. Underneath is a 'Trigger configuration' section with a 'S3' icon. A note says 'Please select the S3 bucket that serves as the event source. The bucket must be in the same region as the function.' Below this is a dropdown menu with a search bar containing 'Q | awscapstonec3serdarblog'. Other options in the dropdown include 'cf-template-awscapstonec3serdarblog-1', 'cf-templates-5mfgdye7649f-sa-east-1', 'cf-templates-5mfgdye7649f-us-east-1', 'cf-templates-5mfgdye7649f-us-east-2', 'cf-templates-5mfgdye7649f-us-west-2', 'clarusway.broadcast.kc', 'clarusway.cors.broadcast.kc', 'clarusway.destination.lambda.osvaldo', 'clarusway.lambda.images', 'clarusway.lambda.images-resized', 'clarusway.source.lambda.osvaldo', and 'djangoserdarrrr-encryption-service'. At the bottom of the page is a 'Next Step' button.

Hata verebiliyor eger hata verir ise lamda function s una gidip silip tekrar Trigger edecegiz

▼ Function overview [Info](#)

 awscapstonelambdafunction
 Layers (0)

Description

Last modified 3 minutes ago

Function ARN arn:aws:lambda:us-east-1:046402772087:function:awscapstonelambdafunction

[+ Add destination](#)

[+ Add trigger](#)

Code | Test | Monitor | **Configuration** | Aliases | Versions

General configuration

Triggers

Permissions

Destinations

Environment variables

Tags

VPC

Monitoring and operations tools

Triggers (1)

Trigger

 S3: awscapstones3serdarblog arn:aws:s3::awscapstones3serdarblog

Bucket: s3/awscapstones3serdarblog Event type: ObjectCreated Notification name: 511a6d64-9786-433c-9679-c63d5d0e78e9

- For defining trigger for **deleting objects**
``bash
Trigger configuration : S3
Bucket : awscapstonec3<name>blog
Event type : All object delete events
Check the warning message and click add ---> sometimes it says overlapping situation. When it occurs, try refresh page and create a new trigger or remove the s3 event and recreate again. then again create a trigger for lambda function
``

Lambda > Add trigger

Add trigger

Trigger configuration

 S3 aws storage

Bucket
Please select the S3 bucket that serves as the event source. The bucket must be in the same region as the function.

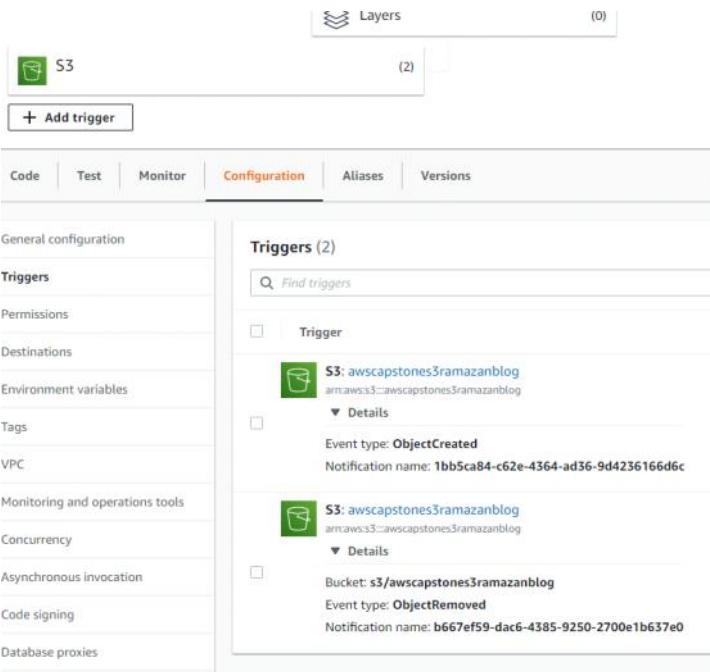
Event type
Select the events that you want to have trigger the Lambda function. You can optionally set up a prefix or suffix for an event, individual events cannot have multiple configurations with overlapping prefixes or suffixes that could match key.

Prefix - optional
Enter a single optional prefix to limit the notifications to objects with keys that start with matching characters.

Suffix - optional
Enter a single optional suffix to limit the notifications to objects with keys that end with matching characters.

Lambda will add the necessary permissions for Amazon S3 to invoke your Lambda function from this trigger. [Learn more about the Lambda permissions model.](#)

[Describe invocation](#)



- Go to the code part and select `lambda_function.py` ---> remove default code and paste a code on below. If you give DynamoDB a different name, please make sure to change it into the code.

```

```python
import json
import boto3
def lambda_handler(event, context):
 s3 = boto3.client("s3")

 if event:
 print("Event: ", event)
 filename = str(event['Records'][0]['s3']['object']['key'])
 timestamp = str(event['Records'][0]['eventTime'])
 event_name = str(event['Records'][0]['eventName']).split(':')[0][6:]

 filename1 = filename.split('/')
 filename2 = filename1[-1]

 dynamo_db = boto3.resource('dynamodb')
 dynamoTable = dynamo_db.Table('awscapstoneDynamo')

 dynamoTable.put_item(Item = {
 'id': filename2,
 'timestamp': timestamp,
 'Event': event_name,
 })
```

```

- Click deploy and all set. go to the website and add a new post with photo, then control if their record is written on DynamoDB.
- WE ALL SET
- Congratulations!! You have finished your AWS Capstone Project

1/

Objects (2)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in this bucket.

| <input type="checkbox"/> | Name | Type | Last modified |
|--------------------------|----------------------|------|--------------------------|
| <input type="checkbox"/> | Calisma_ortamı.jpeg | jpeg | August 27, 2021, 20:13:3 |
| <input type="checkbox"/> | Cloud_sistemleri.png | png | August 28, 2021, 23:09:4 |

Clarusway Blog Home About

Post created successfully!

Clarusway Blog



My Working Room

hard working it

Posted 1 day, 2 hours ago.



jds

Pizza as a Service

Order → Take & Binge → Pizza Delivered → Delivery

kaya

The New Project is ...

Posted 0 minutes ago.

Yeni yükledigimiz nesnenin geldigini görebiliyoruz

Project-503 : Blog Page Application (Django) deployed on AWS
Application Load Balancer with Auto Scaling, S3, Relational Database Service(RDS), VPC's Components, Lambda, DynamoDB and Cloudfront with Route 53

Description

The Clarusway Blog Page Application aims to deploy blog application as a web application written Django Framework on AWS Cloud Infrastructure. This infrastructure has Application Load Balancer with Auto Scaling Group of Elastic Compute Cloud (EC2) Instances and Relational Database Service (RDS) on defined VPC. Also, The Cloudfront and Route 53 services are located in front of the architecture and manage the traffic in secure. User is able to upload pictures and videos on own blog page and these are kept on S3 Bucket. This architecture will be created by Firms DevOps Guy.

Problem Statement

- Your company has recently ended up a project that aims to serve as Blog web application on isolated VPC environment. You and your colleagues have started to work on the project. Your Developer team has developed the application and you are going to deploy the app in production environment.
- Application is coded by Clarusway Fullstack development team and given you as DevOps team. App allows users to write their own blog page to whom user registration data should be kept in separate MySQL database in AWS RDS service and pictures or videos should be kept in S3 bucket. The object list of S3 Bucket containing movies and videos is recorded on DynamoDB table.
- The web application will be deployed using Django framework.
- The Web Application should be accessible via web browser from anywhere in secure.
- You are requested to push your program to the project repository on the Github. You are going to pull it into the web servers in the production environment on AWS Cloud.

In the architecture, you can configure your infrastructure using the followings,

- The application stack should be created with new AWS resources.
- Specifications of VPC:
 - VPC has two AZs and every AZ has 1 public and 1 private subnets.
 - VPC has Internet Gateway
 - One of public subnets has NAT Instance.
 - You might create new instance as Bastion host on Public subnet or you can use NAT instance as Bastion host.
 - There should be managed private and public route tables.
 - Route tables should be arranged regarding of routing policies and subnet associations based on public and private subnets.
- You should create Application Load Balancer with Auto Scaling Group of Ubuntu 18.04 EC2 Instances within created VPC.
- You should create RDS instance within one of private subnets on created VPC and configure it on application.
- The Auto Scaling Group should use a Launch Template in order to launch instances needed and should be configured to;
 - use all Availability Zones on created VPC.
 - set desired capacity of instances to 2
 - set minimum size of instances to 2
 - set maximum size of instances to 4
 - set health check grace period to 90 seconds
 - set health check type to ELB
 - Scaling Policy --> Target Tracking Policy
 - Average CPU utilization (set Target Value %70)
 - seconds warm up before including in metric ---> 200
 - Set notification to your email address for launch, terminate, fail to launch, fail to terminate instance situations
- ALB configuration;

- Application Load Balancer should be placed within a security group which allows HTTP (80) and HTTPS (443) connections from anywhere.
- Certification should be created for secure connection (HTTPS)
 - To create certificate, AWS Certificate Manager can be utilized.
- ALB redirects to traffic from HTTP to HTTPS
- Target Group
 - Health Check Protocol is going to be HTTP
- The Launch Template should be configured to;
 - Prepare Django environment on EC2 instance based on Developer Notes,
 - Download the "clarusway_aws_capstone" folder from Github repository,
 - Install the requirements using requirements.txt in 'clarusway_aws_capstone' folder
 - Deploy the Django application on port 80.
 - Launch Template only allows HTTP (80) and HTTPS (443) ports coming from ALB Security Group and SSH (22) connections from anywhere.
 - EC2 Instances type can be configured as t2.micro.
 - Instance launched should be tagged Clarusway AWS Capstone Project
 - Since Django App needs to talk with S3, S3 full access role must be attached EC2s.
- For RDS Database Instance;
 - Instance type can be configured as db.t2.micro
 - Database engine can be MySQL with version of 8.0.20.
 - RDS endpoint should be addressed within settings file of blog application that is explained developer notes.
 - Please read carefully "Developer notes" to manage RDS sub settings.
- Cloudfront should be set as a cache server which points to Application Load Balance with following configurations;
 - The cloudfront distribution should communicate with ALB securely.
 - Origin Protocol policy can be selected as HTTPS only.
 - Viewer Protocol Policy can be selected as Redirect HTTP to HTTPS
- As cache behavior;
 - GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE methods should be allowed.
 - Forward Cookies must be selected All.
 - Newly created ACM Certificate should be used for securing connections. (You can use same certificate with ALB)
- Route 53
 - Connection must be secure (HTTPS).
 - Your hostname can be used to publish website.
 - Failover routing policy should be set while publishing application
 - Primary connection is going to be Cloudformation
 - Secondary connection is going to be a static website placed another S3 bucket. This S3 bucket has just basic static website that has a picture said "the page is under construction" given files within S3_static_Website folder
 - Healthcheck should check If Cloudfront is healthy or not.
- As S3 Bucket
 - First S3 Bucket
 - It should be created within the Region that you created VPC
 - Since development team doesn't prefer to expose traffic between S3 and EC2s on internet, Endpoint should be set on created VPC.
 - S3 Bucket name should be addressed within

configuration file of blog application that is explained developer notes.

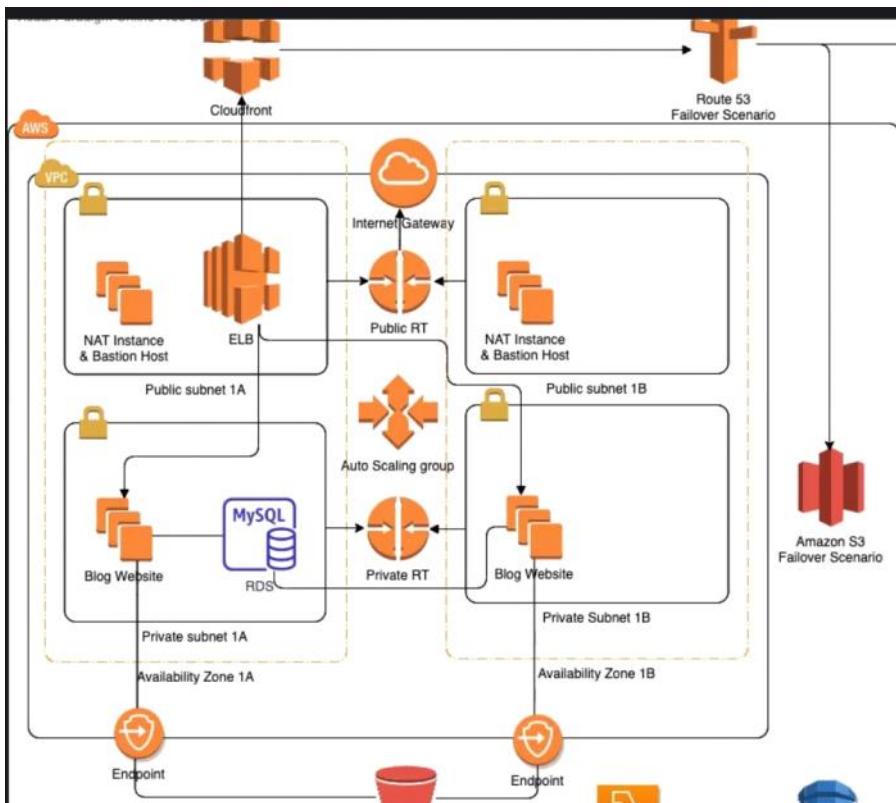
- Second S3 Bucket
 - This Bucket is going to be used for failover scenario. It has just a basic static website that has a picture said "the page is under construction"
- To write the objects of S3 on DynamoDB table
 - Lambda Function
 - Lambda function is going to be Python 3.8
 - Python Function can be found in github repo
 - S3 event is set as trigger
 - Since Lambda needs to talk S3 and DynamoDB and to run on created VPC, S3, DynamoDB full access policies and NetworkAdministrator policy must be attached it
 - S3 Event must be created first S3 Bucket to trigger Lambda function
 - DynamoDB Table
 - Create a DynamoDB table which has primary key that is id
 - Created DynamoDB table's name should be placed on Lambda function.

Project Skeleton

```
clarusway_blog_proj (folder)
|---Readme.md      # Given to the students (Definition of
the project)
|---src (folder)    # Given to the students (Django
Application's )
|---requirements.txt # Given to the students (txt file)
|---lambda_function.py # Given to the students (python
file)
|---developer_notes.txt # Given to the students (txt file)
```

Expected Outcome

From <[https://github.com/clarusway/clarusway-aws-8-21/tree/main/aws/projects/Project-503-Capstone-Project-Blog-Page-App-\(Django\)-on-AWS-Environment](https://github.com/clarusway/clarusway-aws-8-21/tree/main/aws/projects/Project-503-Capstone-Project-Blog-Page-App-(Django)-on-AWS-Environment)>



(Jango flask in gelimis hall diyebiliriz bir frameworktur.)

Developerlar bir Jango frameworku ile block applicationu yazdilar. Blok sayfasi ile herkes kendi blogunu sayfasini yazabiliyor. Fotograflarini ve videolarini paylasabiliyor.

Videolarini paylasacakları için bi login olunması ve bir yerde de user ve passwordlerin tutulması store edilmesi gerekiyor.

Store denilince akılimiza AWS de s3 geliyor.
Developerlar s3 de tutulmasını istiyorlar. S3 obje tabanlı bir storeage iddir. Ne kadar çağrırlı ise o kadar ücretlendirmeye tabiydi.

Login datalarda database de tutulacak. Bunun içinde Mysql tercih edilmiş .

Bunun için Custom VPC kuracagız . Production ortamında da custom vpc kullanılması tercih ediliyor. Cunku VPC lerde Database gibi bazı makinalarımızın private subnetlerde kurulması gerekiyor ki bir bakıma bunlar bilerer firewall olarak nitelendiriliyor.

Custom VPC nin isterlerine bakalım;

- 2 adet Availability zonumuz var ve bu Availability Zon'un içerisinde bir private ve birde public subnetlerimiz olacak (Availability Zone : Bir region içerisinde bulunan, birbirlerine yakın konumlandırılmış, küçük sunucu tarişalarına verilen isimdir. Bir region içerisinde birden fazla availability zone bulunabilir ve her bir zone harf ile adlandırılır. Örneğin Oregon region'unda us-west-2a, us-west-2b ve us-west-2c olmak üzere üç adet AZ (availability-zone) bulunmaktadır .
- From <<https://www.mobihanem.com/aws-dersleri-aws-nedir/>>)

Private ve public subnetler vpc icerisine kurulan izole network çözümleridir.

- Bi izole network icerisine farklı resourcları koruma altına alabiliyoruz.
- Ortak bir subnet kumesini bir subnet gurubunda toplayabiliyorsunuz.
- Ayrıca farklı subnetlerde farklı replicalar bulundurarak failover durumlarda afet yangın olası tabi durumlarda mevcut subnetimize bir sey olmasi durumunda diger subneti devreye

sokabiliyoruz.

**Subnetler in kendi aralarında irtibati kurmaları için
veyahut subnetlerin içerisindeki resourceların dış
dunyaya ulaşmak istediklerinde, veya herhangi bir
porta ulaşmak istediklerinde, Route Tablelerini
kullanırız. Route Tableler subnet içerisinde bir
navigasyon cihazıdır. Route Tablelerin içerisinde
oluşturduğumuz Rule lar ile bir tarafta gitmesini
veyahut da gitmemesini sağlarız.**

**Özellikle de private Route Table yapımının
sebebi bir firewall yapılarak dış dunyadan
ulaşılamayacak bir hale getirmesini sağlamaktır.**

**Ayrıca videolar ve resimlerin s3 de saklanacağını ve
dış dunyaya exposet olmamasını istediğimizi
dusunsek subnetler ile S3 bucket lar arasında da
bir gateway end point kuracağız**

**Ardından Jango web sitesi bir EC2 lar grubu
üzerinde tutulacak bunuda Autoscaling group
saglayacak. Bunun öncesi de bir Launch Template
kuracağız ki L .Template ile Auto Scalinge
makinaların kurulumunu salayalım . Bizim istediğimiz
desire kapasitede minimum ve max seviyede
makinalar ayaga kalkacak . Burda bir Target Tracking
Policy oluşturacağız.**

**Aynı zaman bu EC2 lar ELB ye bağlı olacak ELB nin
en önemli özelliği EC2 lardaki yoğunluga bakıp
HealthCheck ler ile herhangi yoğunluk olması
durumunda esit olarak bu yarısı EC2 lar arasında
dagıtımak. Hem Trafığı yayılıyor hem tek elden
dagılımlı saglıyor. Hemde Dis dunyadan gelen User In
herhangi bir aksama olmadan EC2 ya ulaşmasını
saglıyor.**

**ALB nin de önüne bir CloudFront koymuş olacak ELB
bir cash hizmeti sunacak. Videolar ve fotoğraflar S3
den çekilecek her seferinde ücret ödenmemesi için
bunu yapacaklar Cash hizmeti ile sağlanacak.**

**Production ortamında Cloudfront s3 un önüne de
kuruluyor. Eğer burda tanımlamak istersek s3 u
orjin olarak gösterecektir.**

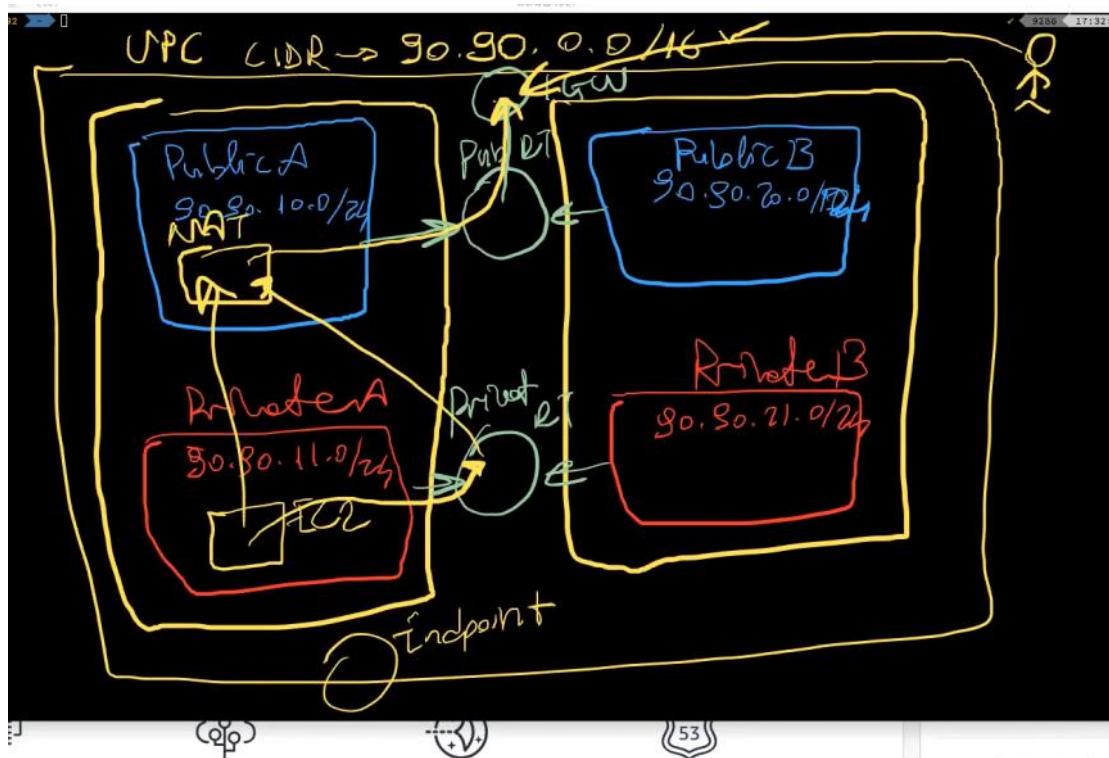
**Developerlar kodunu kullanıcı karşısına çıkartmak
için Route53 failover senaryosu ile karsımıza
çıkaracak.**

**Burada Failover senaryosu Route 53 olarak bir
içeride atanmış durumdadır. Route53 de İki adet ent
pointı takip eder. Birisi static website olur. Degiride
uniq olarak caaşsan web sitesidir. basına herhangi
bir durum gelmesi halinde secondary e trafıgi
yönlenendirir.**

**Userlar bu haliyle karsılarına bir sey çıkardı mevcut
olarak bir sorunun olduğunu ve bu sorunun bir süre
sonra çözülecegi gibi seyler içerebilir.**

**Birde Developerlar S3 un içerisinde konulan her seyi
takip etmek istiyorlar. S3 e konan herhangi bir obje
oldugunda , bir event olusacak bu event bir lambda
function oluşturacak bu Lambda Function da
Dynamodb içerisinde bilgileri yazdıracak.**

**Dolayısıyla yazılan ve silinen bilgileri Dynamodb de
gerekli olarak kaydedilecektir.**



Konsolumuza geciyoruz :

Vpc de CIDR Blokları vardır. Bz bunları Private Ipler için tanımlıyor. Public olsalar EC2 kendisi veriyor.

Tanımlıacamız vpc de AWS 90.90.0.0/16 toplamda
65 bin ip tanımlayabileceğimiz BIR SINIRLAMA

TANIYOR

Bir subneti private yada Public yapan dışarıya
acılmasıdır.

Birde bunlara Private ve Public Route tablet
ayarlayacağız ki Routa tabletlerde bir kural tanımlar
ve dış dünya ya acımasını isterseniz Public İstemez
iseniz Private olurlar

Ayrıca Bir de end Point ekleyeceğiz S3 ler ve
DYNAMODB Cloud Watch lar için kullanılır ve burada
s3 e irtibat sağlamak için kullanacağız.

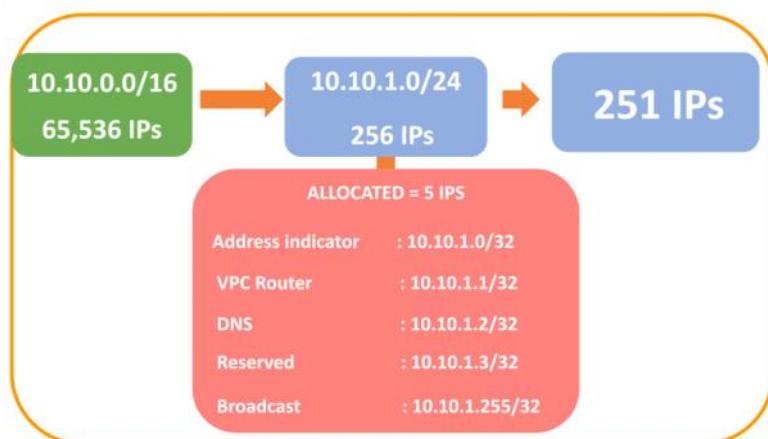
Bz Internet Gate way aracılığıyla Öncelikle Public
Iplerimize giriş yapabiliyoruz. Ancak Private geçiş
yapmak için Publicde kuracağımız Bastion Hostlar
ile siblama tahtaları ile Geçiş yapacağız.

Ayrıca icerdeki makinanın dışarıya acılması için ne
yapmamız gerekiyordu dersek bunun içinde Nat
Instance veya Nat Gateway kurmalız gerekiyor
Bastion Host olarak da görülmüyor Ancak Nat Instance
da dikkat edilmesi gereken konu http, HTTPS ve SSH
anywhere olarak her yerden açmamız gerekiyor

Ayrıca birde icerdeki makinanın dışardaki ile
görüşmesi için ne yapmamız gerekiyor; Nat
Instance veya Nat Gateway kurmalız gerekiyor
NatGateway AWS manage bir sistemdir. Yani biz
kontrol etmiyoruz. Nat Instance ise özel bir
Instance tipidir. Public Subnete yerleştiririz. Private
Instance da bulunan EC2 muz Private Route Table
aracılığıyla Nat Instance üzerinden dış dünya ile
irtibat saglayabiliyoruz. Ayrıca Bastion Host olarakta

kullanılabilir ancak HTTP, HTTPS ve ssh in anywhere olarak her yöne açılması gerekiyor.

VPC CIDR



| inet ID | State | VPC | IPv4 CIDR | IPv6 CIDR | Available IPv4 addresses |
|-----------------------|-----------|--------------------------------|---------------|-----------|--------------------------|
| net-05335f428f975bc72 | Available | vpc-0142f2295c4ac3c14 aws... | 90.90.10.0/24 | - | 251 |

Handwritten notes on the table:

- 90.90.10.0 → Network
- 90.90.10.255 → Broadcast
- 90.90.10.01 → VPC Router
- 90.90.10.02 → DNS
- 90.90.10.03 → Future

Calculation: $32 - 24 = 8$
 $2^8 = 256$

256 - 1 = 255 kullanılabılır 5 ntnesini AWS kendisine reverse eder.

İlk olarak VPC mizi yapmak için konsola gidiyoruz

```
# Project-503 : Blog Page Application (Django) deployed on A
WS Application Load Balancer with Auto Scaling, S3, Relational Database Service(RDS), VPC's Components, DynamoDB and CloudFront with Route 53 (STUDENT_SOLUTION)
## Description
```

The Clarusway Blog Page Application aims to deploy blog application as a web application written Django Framework on AWS Cloud Infrastructure. This infrastructure has Application Load Balancer with Auto Scaling Group of Elastic Compute Cloud (EC2) Instances and Relational Database Service (RDS) on defined VPC. Also, The Cloudfront and Route 53 services are located in front of the architecture and manage the traffic in secure. User is able to upload pictures and videos on own blog page and these are kept on S3 Bucket. This architecture will be created by Firms DevOps Guy.

```
# Steps to Solution
```

```
### Step 1: Create dedicated VPC and whole components
```

```
### VPC
- Create VPC.
  - create a vpc named `aws_capstone-`  

  VPC` CIDR blok is `90.90.0.0/16`  

  no ipv6 CIDR block
```

```

tenancy: default
- select `aws_capstone-
VPC` VPC, click `Actions` and `enable DNS hostnames`
for the `aws_capstone-VPC`.

```

VPC settings

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

aws_capstone-VPC

IPv4 CIDR block [Info](#)
90.90.0.0/16

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

Tenancy [Info](#)
Default

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="aws_capstone-VPC"/> |

Add new tag

You can add 49 more tags.

Create VPC

vpc ile birlikte route tablet in default olarak olustugunu gorebiliyoruz.

| Route tables (5) Info | | | | | | | |
|---------------------------------------|-------------------------|------------------------|-----------------------------|-------------------|------|---------------------------------|----------------------|
| | Name | Route table ID | Explicit subnet associat... | Edge associations | Main | VPC | Actions |
| <input type="checkbox"/> | - | rtb-062d4ee7095f88883 | - | - | Yes | vpc-0c0a0da8de48bdda91 aw... | Edit |
| <input type="checkbox"/> | clarus-private-rt | rtb-06ef049fb0f060b366 | 3 subnets | - | No | vpc-056f805ab0cb50ebd clar... | Edit |
| <input type="checkbox"/> | clarus-vpc-a-default... | rtb-0c9e0ecc393f88236 | - | - | Yes | vpc-036f805ab0cb50ebd clar... | Edit |
| <input type="checkbox"/> | clarus-public-rtb | rtb-02c42e5caa6d9aa41 | 3 subnets | - | No | vpc-036f805ab0cb50ebd clar... | Edit |
| <input type="checkbox"/> | default-rtb | rtb-00f263a33d166d2ee | - | - | Yes | vpc-05fd077f13680c6059 def... | Edit |

Buna da public Routa tablet deyip bir taNE DE PRIVATE OLUSTurabiliriz

Vpc icerisinde butun resource slarin bir birleri ile ,konusmasini istiyororsak edit DNS Hostaname den
ENABLE YAPIMIZ GEREKLİ

Enable olmaz is e bu vpc icerrisine bir DNS atanmaz ve bir bir leri ile konusmalari zora girer.

| Your VPCs (1 / 3) Info | | | | | | | |
|--|------------------|----------------------|--|-------------|----------------------------------|------|-------------------------|
| Actions Create VPC | | | | | | | |
| <input type="checkbox"/> | Name | VPC ID | Status | IPv4 CIDR | IPv6 CIDR (Network border group) | IPV6 | Actions |
| <input type="checkbox"/> | clarus-vpc-a | vpc-0f9631581569ac54 | <input checked="" type="radio"/> Available | 10.70.0/16 | - | - | Edit |
| <input type="checkbox"/> | default-rtb | vpc-f12a17bf | <input checked="" type="radio"/> Available | 172.31.0/16 | - | - | Edit |
| <input checked="" type="checkbox"/> | aws_capstone-VPC | vpc-0142722954ac3c14 | <input checked="" type="radio"/> Available | 90.90.0/16 | - | - | Edit |

Simdi de subnet olusturacagiz

```

## Subnets
- Create Subnets
  - Create a public subnet named `aws_capstone-
public-subnet-1A` under the vpc aws_capstone-
VPC in AZ us-east-1a with 90.90.10.0/24
  - Create a private subnet named `aws_capstone-
-private-subnet-1A` under the vpc aws_capstone-
VPC in AZ us-east-1a with 90.90.11.0/24
  - Create a public subnet named `aws_capstone-
public-subnet-1B` under the vpc aws_capstone-
VPC in AZ us-east-1b with 90.90.20.0/24
  - Create a private subnet named `aws_capstone-

```

-private-subnet-1B` under the vpc aws_capstone-
VPC in AZ us-east-1b with 90.90.21.0/24
- Set `auto-
assign IP up for public subnets. **Select each public**
subnets and click Modify "auto-
assign IP settings" and select "Enable auto-
assign public IPv4 address"

VPC > Subnets > Create subnet

Create subnet Info

VPC

VPC ID
Create subnets in this VPC.
 ▾

Associated VPC CIDRs
IPv4 CIDRs
90.90.0.0/16

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.
 ▾
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.
 ▾

IPv4 CIDR block Info
 ▾
▼ Tags - optional

Vpc Id olarak daha önce oluşturduğumuz vpc yi seçiyoruz.

vpc-0c0a0da8de48dda91 (aws_capstone-VPC) ▾

Associated VPC CIDRs
IPv4 CIDRs
90.90.0.0/16

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.
 ▾
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.
 ▾

IPv4 CIDR block Info
 ▾
▼ Tags - optional

| Key | Value - optional |
|-------------------------------------|---|
| <input type="text" value="Name"/> X | <input type="text" value="aws_capstone-public-subnet-1A"/> X Remove |

Add new tag
You can add 49 more tags.

Remove

Add new subnet

Cancel Create subnet

You have successfully created 1 subnet: subnet-0e6c5debf9d406fe4

| Subnets (4) Info | | | | | |
|---|--------------------------|---|-------------|-------------------------------|--|
| | | Actions | | Create subnet | |
| <input type="checkbox"/> Filter subnets | | <input type="text" value="search: capstone"/> Clear filters | | | |
| Name | Subnet ID | State | VPC | | |
| aws_capstone-public-subnet-1A | subnet-0b2fd9cdd64a3050e | Available | vpc-0c0a0da | | |
| aws_capstone-private-subnet-1B | subnet-0e6c5debf9d406fe4 | Available | vpc-0c0a0da | | |
| aws_capstone-private-subnet-1A | subnet-0867333fa3f0fe391 | Available | vpc-0c0a0da | | |
| aws_capstone-public-subnet-1B | subnet-05085a0d50bc30d03 | Available | vpc-0c0a0da | | |

Public Subnetler Icin Public Ip atanmasi gereklidir.
Bunu bize kontroledebiliyoruz Bunun Icin Public Ipleri Actions bolumunden Modify deyip daha sonra enable ediyoruz.

You have successfully created 1 subnet: subnet-01eb0641d4d2ade39

| Subnets (1/4) Info | | | | | |
|---|---------------------------------|---|---------------------------------------|-------------------------------|-----------|
| | | Actions | | Create subnet | |
| <input type="checkbox"/> Filter subnets | | <input type="text" value="search: aws_capstone"/> Clear filters | | | |
| Name | Subnet ID | State | VPC | IPv4 CIDR | IPv6 CIDR |
| aws_capstone-private-subnet-1A | subnet-06db543e282ef861 | Available | vpc-0142f2295a4ac3c14 aws... | 90.90.11.0/24 | - |
| aws_capstone-private-subnet-1B | subnet-01eb0641d4d2ade39 | Available | vpc-0142f2295a4ac3c14 aws... | 90.90.21.0/24 | - |
| aws_capstone-public-subnet-1A | subnet-05335f42ff7fbcc72 | Available | vpc-0142f2295a4ac3c14 aws... | 90.90.10.0/24 | - |

Subnetleri Private ve Public Yapmak Icin Route Tableleri de duzenleyecegiz

Public routa Tabletleri Public yapmak Icin Internet Gateway tanimlayacagiz

```
## Internet Gateway
- Click Internet gateway section on left hand side
e. Create an internet gateway named `aws_capstone-IGW` and create
```

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.

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 |
| <input type="text" value="Name"/> | <input type="text" value="aws_capstone-IGW"/> |
| Remove | |
| Add new tag | |

You can add 49 more tags.

[Cancel](#) [Create internet gateway](#)

```
- ATTACH the internet gateway `aws_capstone-IGW` to the newly created VPC `aws_capstone-VPC`. Go to VPC and select newly created VPC and click action ---> Attach to VPC ---> Select `aws_capstone-VPC` VPC
```

Internet Gateway olusturduk ancak bunu attach etmemiz gereklidir su an Detach olarak gözüküyor

Her bir VPC ye Ancak bir InternetGateWay Attach edilebiliyor.

Son olarak Route Tablelerimize Internet Gate Way I ekliyoruz.

Ve ardindan Private Routa Tabletlere Private Subnetleri, Public leri Public olan ile Associations edecegiz

ss

Ve simdi de endpoint olusturacagiz. Ent pointler! Private Subnetler icin tanimlayacagiz.

Vpc olarak kendi vpc mizi secyorum

Ardindan hangi Rote Tabletlere sececegimiz karsimiza geliyor

A VPC endpoint enables you to securely connect your VPC to another service. There are three types of VPC endpoints – Interface endpoints, Gateway Load Balancer endpoints, and gateway endpoints. Interface endpoints and Gateway Load Balancer endpoints are powered by AWS PrivateLink, and use an elastic network interface (ENI) as an entry point for traffic destined to the service. Interface endpoints are typically accessed using the public or private DNS name associated with the service, while gateway endpoints and Gateway Load Balancer endpoints serve as a target for a route in your route table for traffic destined for the service.

Service category

- AWS services
- Find service by name
- Your AWS Marketplace services

Service Name com.amazonaws.us-east-1.s3 

| Search: s3  Add filter  | | |
|---|--------|-----------|
| Service Name | Owner | Type |
| com.amazonaws.us-east-1.s3 | amazon | Gateway |
| com.amazonaws.us-east-1.s3 | amazon | Interface |

VPC* vpc-f52d178f   

Configure route tables A rule with destination `pl-63a5400a` (`com.amazonaws.us-east-1.s3`) and a target with this endpoints' ID (e.g. `vpce-12345678`) will be added to the route tables you select below.

Subnets associated with selected route tables will be able to access this endpoint.

Subnets associated with selected route tables will be able to access this endpoint.

| Route Table ID | Main | Associated With |
|---|------|-----------------|
| <input type="checkbox"/> rtb-062d4ee7095f86883 | Yes | 2 subnets |
| <input checked="" type="checkbox"/> rtb-0a955a53c4f03b31e | No | 2 subnets |

Warning When you use an endpoint, the source IP addresses from your instances in your affected subnets for accessing the AWS service in the same region will be private IP addresses, not public IP addresses. Existing connections from your affected subnets to the AWS service that use public IP addresses may be dropped. Ensure that you don't have critical tasks running when you create or modify an endpoint.

Policy*

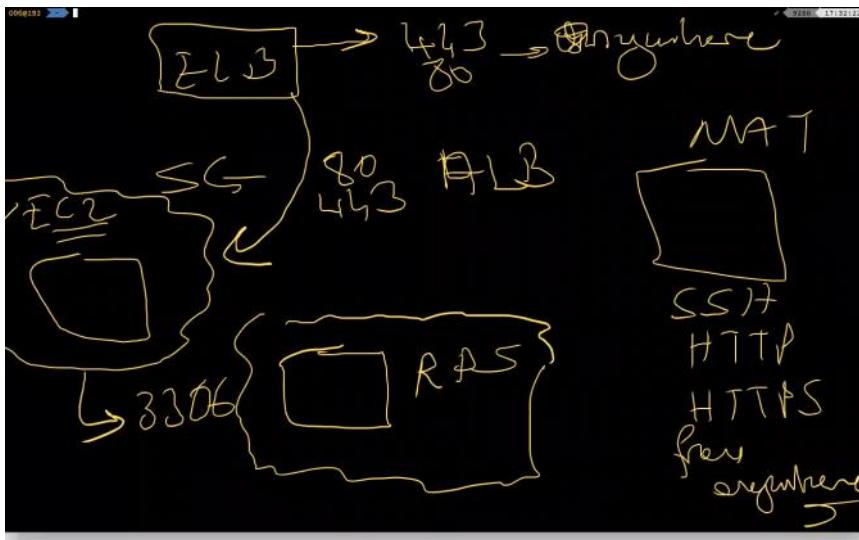
- Full Access - Allow access by any user or service within the VPC using credentials from any Amazon Web Services accounts to any resources in this Amazon Web Services service. All policies — IAM user policies, VPC endpoint policies, and Amazon Web Services service-specific policies (e.g. Amazon S3 bucket policies, any S3 ACL policies) — must grant the necessary permissions for access to succeed.
- Custom

Use the policy creation tool to generate a policy, then paste the generated policy below.

```
{
  "Statement": [
    {
      "Action": "...",
      "Effect": "Allow",
      "Resource": "...",
      "Principal": ...
    }
  ]
}
```

Ve simdi de security Grouplarimizi olusturacagiz. Ve daha sonra olusturdugumuz makinalarda kolay bir sekilde sececegiz.

Rds e her makinani ulasmasini istemiyoruz sadece application unumuzun oldugu EC2 nun ulasmasini istiyoruz



- ELB dis dunya ile irtibat sagladigi icin ona 443 ve 80 portundan her yere yani anywhere olarak aciyoruz
- Ancak Ec2 ya sadece ELB uzerinden ulasilmasini istedigimiz icin EC2 icin olusturdugumuz Sec Grupta 80 ve 443 portundan sadece EC2 yu belirtecegiz
- RDS sadece EC2 dan ulasilmasini istedigimiz icin RDS e 3306 portundan sadece EC2 yu tanimliyoruz.
- Nat instance dis dunyadan her istegi ic teki Private icin yerine getiren oldugu icin burda any where ile http HTTPS I Tanimliyoruz

Step 2: Create Security Groups (ALB ---> EC2 ---> RDS)

1. ALB Security Group

Name : aws_capstone_ALB_Sec_Group
 Description : ALB Security Group allows traffic H
 TTP and HTTPS ports from anywhere
 Inbound Rules
 VPC : AWS_Capstone_VPC
 HTTP(80) ----> anywhere
 HTTPS (443) ----> anywhere

Basic details

Security group name [Info](#)
 aws_capstone_EC2_Sec_Group
 Name cannot be edited after creation.
 Description [Info](#)
 EC2 Security Groups only allows traffic coming from aws_capstone_ALB_Sec_Group Security
 VPC [Info](#)
 vpc-0142f2295c4ac3c14 [aws_capstone-VPC]

| Inbound rules Info | Protocol Info | Port range Info | Source Info | Description - optional Info |
|------------------------------------|--------------------------------------|---------------------------------------|---------------------------------------|--|
| Type Info
HTTP | Protocol Info
TCP | Port range Info
80 | Source Info
Custom | Security Groups
aws_capstone_ALB_Sec_Group sg-09feef07d70f544a
aws_capstone_ALB_Sec_Group sg-09feef07d70f544a
default sg-0bh199ff0e070f544a
Description - optional
sg |
| Add rule | | | | |

| Outbound rules Info | Type Info | Protocol Info | Port range Info | Destination Info | Description - optional Info |
|--|--------------------------------------|--|--|-------------------------------------|---|
| Type Info
All traffic | Protocol Info
All | Port range Info
All | Destination Info
Custom | Description - optional
0.0.0.0/0 | |

2. EC2 Security Groups

Name : aws_capstone_EC2_Sec_Group
 Description : EC2 Security Groups only allows traffic coming from aws_capstone_ALB_Sec_Group Security Groups for HTTP and HTTPS ports. In addition, ssh port is allowed from anywhere
 VPC : AWS_Capstone_VPC
 Inbound Rules
 HTTP(80) ----> aws_capstone_ALB_Sec_Group
 HTTPS (443) ----> aws_capstone_ALB_Sec_Group
 ssh ----> anywhere



Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, enter a name and description, and then choose a VPC.

Basic details

Security group name Info

Name cannot be edited after creation.

Description Info

VPC Info



(default)

Outbound rules Info

Bu su anlama geliyor 80 ve 443 portu ile attach ettigimiz (her ALB nin) makininen bu vpc ye ulasabilecegini belirtiyoruz.

3. RDS Security Groups

Name : aws_capstone_RDS_Sec_Group
 Description : EC2 Security Groups only allows traffic coming from aws_capstone_EC2_Sec_Group Security Groups for MySQL/Aurora port.
 VPC : AWS_Capstone_VPC
 Inbound Rules
 MySQL/Aurora(3306) ----> aws_capstone_EC2_Sec_Group

Sadece EC2 kardan geleni kabul edecek

Inbound rules Info

| Type <small>Info</small> | Protocol <small>Info</small> | Port range <small>Info</small> | Source <small>Info</small> | Description - optional |
|--------------------------|------------------------------|--------------------------------|----------------------------|-------------------------------------|
| MySQL/Aurora | TCP | 3306 | Custom | <input type="text" value="Q sg"/> X |
| Add rule | | | | |

Outbound rules Info

| Type <small>Info</small> | Protocol <small>Info</small> | Port range <small>Info</small> | Destination <small>Info</small> | Description - optional |
|--------------------------|------------------------------|--------------------------------|---------------------------------|------------------------|
| | | | | |
| | | | | |
| | | | | |

4. NAT Instance Security Group

Name : aws_capstone_NAT_Sec_Group
 Description : ALB Security Group allows traffic HTTP and HTTPS and SSH ports from anywhere
 Inbound Rules
 VPC : AWS_Capstone_VPC
 HTTP(80) ----> anywhere
 HTTPS (443) ----> anywhere
 SSH (22) ----> anywhere

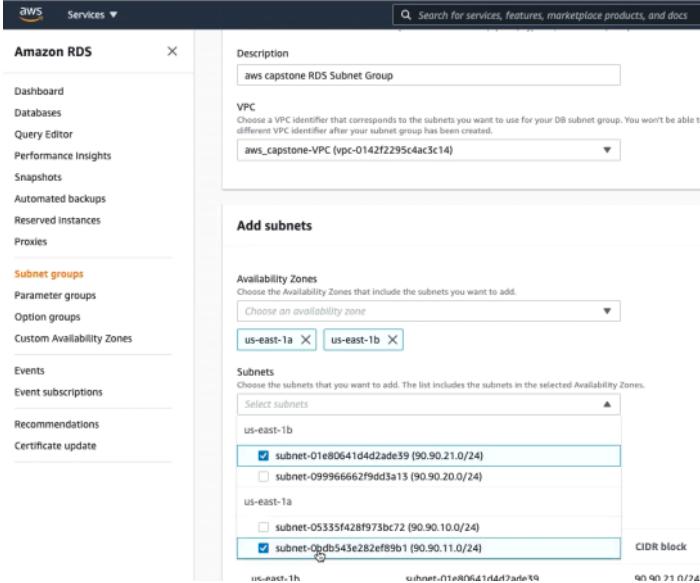
Step 3: Create RDS

Custom VPC lerde RDS kurmadan önce bu RDS lerin hangi VPC de calismasini istiyorsak o sekilde bir Subnet Group olusturuuz

```

First we create a subnet group for our custom VPC. Click `subnet Groups` on the left hand menu and click `create DB Subnet Group`
```text
Name : aws_capstone_RDS_Subnet_Group
Description : aws capstone RDS Subnet Group
VPC : aws_capstone_VPC
Add Subnets
Availability Zones : Select 2 AZ in aws_capstone_VPC
Subnets : Select 2 Private Subnets in these subnets
```

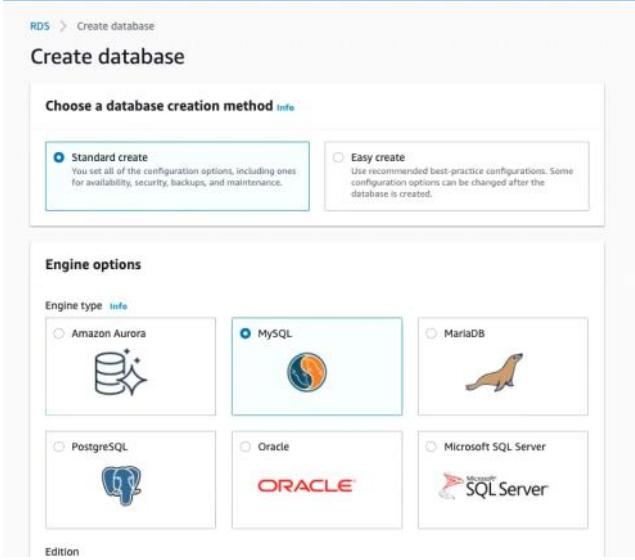
```



```

- Go to the RDS console and click `create database` button
```text
Choose a database creation method : Standard Create
Engine Options : MySQL
```

```



```

Version : 8.0.20
Templates : Free Tier
Settings :
  - DB instance identifier : aws-capstone-RDS
  - Master username : admin
  - Password : Clarusway1234
DB Instance Class : Burstable classes (includes t classes) ---> db.t2.micro
Storage : 20 GB and enable autoscaling(up to 40GB)
```

```

## Settings

### DB instance identifier [Info](#)

Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

aws-capstone-RDS

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

### ▼ Credentials Settings

#### Master username [Info](#)

Type a login ID for the master user of your DB instance.

admin

1 to 16 alphanumeric characters. First character must be a letter

#### Auto generate a password

Amazon RDS can generate a password for you, or you can specify your own password

#### Master password [Info](#)

Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), {single quote}, "double quote) and : (at sign).

#### Confirm password [Info](#)

## DB instance class

### DB instance class [Info](#)

Choose a DB instance class that meets your compute resource and memory requirements. The DB instance class controls how much

### Connectivity:

VPC : aws\_capstone\_VPC  
Subnet Group : aws\_capstone\_RDS\_Subnet  
t\_Group  
Public Access : No  
VPC Security Groups : Choose existing ---> a  
ws\_capstone\_RDS\_Sec\_Group

## Storage

### Storage type [Info](#)

General Purpose (SSD)

### Allocated storage

20 GiB

(Minimum: 20 GiB, Maximum: 16,384 GiB) Higher allocated storage may improve IOPS performance.

### Storage aut-scaling [Info](#)

Provides dynamic scaling support for your database's storage based on your application's needs.

#### Enable storage aut-scaling

Enabling this feature will allow the storage to increase once the specified threshold is exceeded.

### Maximum storage threshold [Info](#)

Changes will apply when your database autoscals to the specified threshold

40 GiB

(Minimum: 21 GiB, Maximum: 16,384 GiB)

## Availability & durability

Storage kismini RDS'in kapasitesi max kaç artırmaktadır max olarak 16,384 GiB yapabiliyor

## Connectivity

Virtual private cloud (VPC) [Info](#)  
VPC that defines the virtual networking environment for this DB instance.

aws\_capstone-VPC (vpc-0142f2295c4ac3c14)

Only VPCs with a corresponding DB subnet group are listed.

After a database is created, you can't change the VPC selection.

Subnet group [Info](#)  
DB subnet group that defines which subnets and IP ranges the DB instance can use in the VPC you selected.

aws\_capstone\_rds\_subnet\_group

Public access [Info](#)

Yes  
Amazon EC2 instances and devices outside the VPC can connect to your database. Choose one or more VPC security groups that specify which EC2 instances and devices inside the VPC can connect to the database.

No  
RDS will not assign a public IP address to the database. Only Amazon EC2 instances and devices inside the VPC can connect to your database.

VPC security group  
Choose a VPC security group to allow access to your database. Ensure that the security group rules allow the appropriate incoming traffic.

Choose existing  
Choose existing VPC security groups

Create new  
Create new VPC security group

Existing VPC security groups

Choose VPC security groups

Public acces no diyoruz VPC nin disindan verilen bir izindir.

Availability Zone : No preference  
Additional Configuration : Database port ---> 330  
6  
Database authentication ---> Password authentication  
Additional Configuration:  
- Initial Database Name : database1  
- Backup ---> Enable automatic backups  
- Backup retention period ---> 7 days  
- Select Backup Window ---> Select 03:00 (am) Duration 1 hour  
- Maintenance window : Select window ---> 04:00(am) Duration:1 hour  
create instance  
...

The following service-linked role is used for publishing logs to CloudWatch Logs.

RDS service-linked role

Ensure that general, slow query, and audit logs are turned on. Error logs are enabled by default. [Learn more](#)

## Maintenance

Auto minor version upgrade [Info](#)

Enable auto minor version upgrade

Enabling auto minor version upgrade will automatically upgrade to new minor versions as they are released. The automatic upgrades occur during the maintenance window for the database.

Maintenance window [Info](#)

Select the period you want pending modifications or maintenance applied to the database by Amazon RDS.

Select window

No preference

Start day      Start time      Duration  
Tuesday      05 : 00 UTC      0.5 hours

## Deletion protection

Enable deletion protection

Protects the database from being deleted accidentally. While this option is enabled, you can't delete the database.

## Estimated monthly costs

The Amazon RDS Free Tier is available to you for 12 months. Each calendar month, the free tier will allow you to use the Amazon RDS resources listed below for free:

- 750 hrs of Amazon RDS in a Single-AZ db.t2.micro Instance.

Enable deleion dersek silmek icin bir kac basamli bir sart getiri protection ortanminda bu öneriir.

Iki bucket icin olusturacagiz bir failover icin digerri resim ve metinleri saklamak icin olusturacagiz

### Step 4: Create two S3 Buckets and set one of them

e as static website.

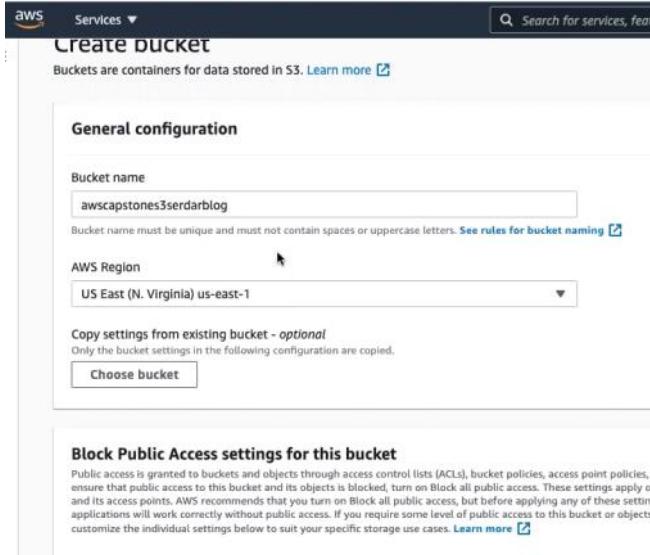
Go to the S3 Consol and lets create two buckets.

#### 1. Blog Website's S3 Bucket

- Click Create Bucket

```text

Bucket Name : awscapstones3<YOUR NAME>blog-----unique
dikkat edilmesi gereken
Region : N.Virginia



Block all public access : Unchecked

Other Settings are keep them as are
create bucket

```

#### 2. S3 Bucket for failover scenario

- Click Create Bucket

```text

Bucket Name : www.<YOUR DNS NAME>

Region : N.Virginia

Block all public access : Unchecked
Please keep other settings as are

```

- create bucket

- Selects created `www.<YOUR DNS NAME>` bucket ---> Properties ---> Static website hosting

```text

Static website hosting : Enable

Hosting Type : Host a static website

Index document : index.html

save changes

```

- Select `www.<YOUR DNS NAME>` bucket ---> select Upload and upload `index.html` and `sorry.jpg` files from given folder---> Permissions ---> Grant public-read access ---> Checked warning message

Amazon S3 > www.clarusway.us > Upload

### Upload

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose Add files, or Add folders.

Files and folders (2 Total, 88.1 KB)		Remove	Add files	Add folder
All files and folders in this table will be uploaded.				
<input type="text"/> Find by name	Name	Folder	Type	Size
<input type="checkbox"/>	index.html	-	text/html	199.0 B
<input type="checkbox"/>	sorry.jpg	-	image/jpeg	87.9 KB

**Destination**

Destination  
s3://www.clarusway.us

**Destination details**  
Bucket settings that impact new objects stored in the specified destination.

Ayrıca static web site olarak kullanmak için de

**Ayrıca WWW. Ve DNS name ile oluşturduğumuz subnette Access Control sekmesini Grant Public olarak açıyoruz upload ettiğimiz file in dis dညan okunmasını saglıyoruz**

**▼ Permissions**  
Grant public access and access to other AWS accounts.

**Access control list (ACL)**  
Grant basic read/write permissions to other AWS accounts. [Learn more](#)

**① AWS recommends using S3 bucket policies or IAM policies for access control. [Learn more](#)**

Access control list (ACL)  
 Choose from predefined ACLs  
 Specify individual ACL permissions

Predefined ACLs  
 Private (recommended)  
 Only the object owner will have read and write access.  
 Grant public-read access  
 Anyone in the world will be able to access the specified objects. The object owner will have read and write access. [Learn more](#)

**⚠️ Granting public-read access is not recommended**  
 Anyone in the world will be able to access the specified objects. [Learn more](#)

I understand the risk of granting public-read access to the specified objects.

bit secure | devops-ramazan-kaya.com:s3-website-us-east-1.amazonaws.com

### FAILOVER SCENARIO



```
Step 5: Copy files downloaded or cloned from `Clarusway_project` repo on Github
```

Git hub dan  
 S3 ler ayarlandı RDS ayarlandı ve simdi Githubda bulunan private repomuzu clonlamistik daha önce simdi de git commit - m ve git push komutları ile lokalde bulunan dosyalarımızı git hub dosyamiza gönderdik.

Simdi de git hub hesabımız dan **TOKEN** alacağız;

Avatar----Setting-----Developer settings--Personel Access tokens----

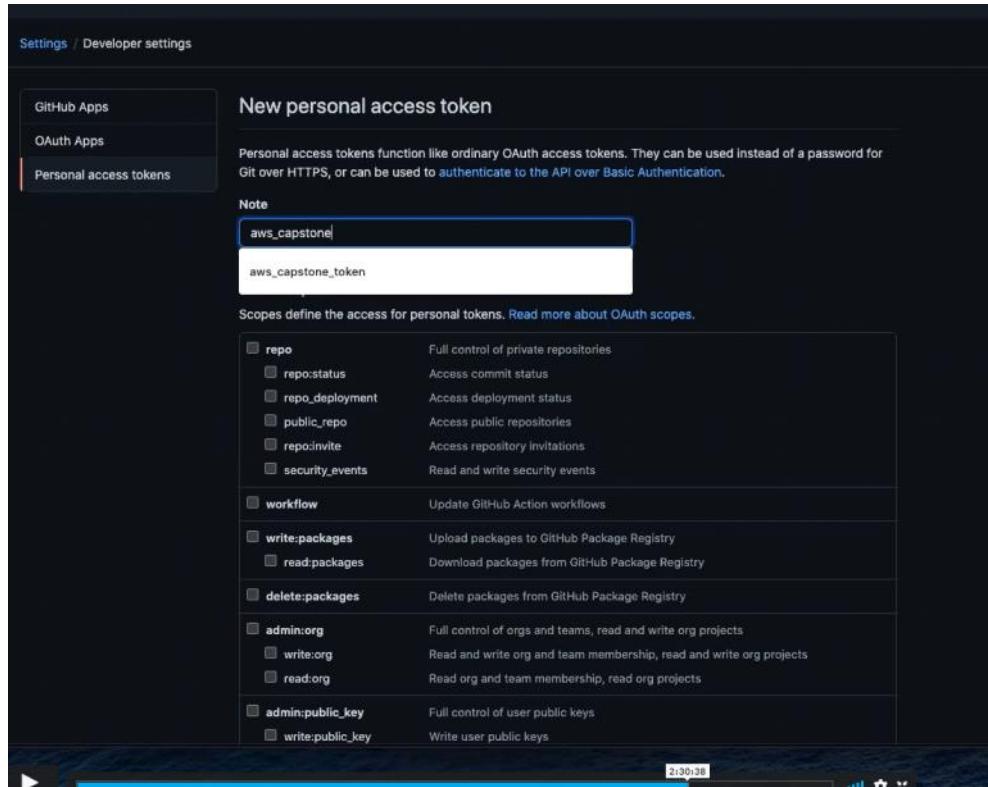
The screenshot shows the 'Public profile' section of the GitHub account settings. On the left, a sidebar lists various settings categories: Account settings, Profile, Account, Appearance (New), Account security, Billing & plans, Security log, Security & analysis, Emails, Notifications, Scheduled reminders, SSH and GPG keys, Repositories, Packages, Organizations, Saved replies, Applications, and Developer settings. The 'Developer settings' option is highlighted with a yellow box. The main content area is titled 'Public profile' and contains fields for 'Name', 'Public email', 'Bio', 'URL', 'Twitter username', 'Company', and 'Location'. Each field has a descriptive placeholder text below it.

Ve Generate new token

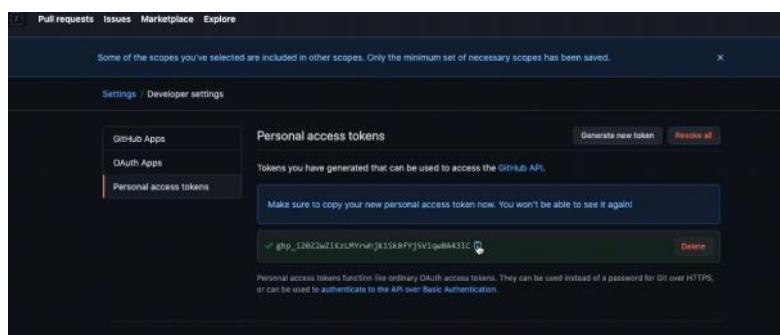
The screenshot shows the 'Personal access tokens' section under 'Developer settings'. The sidebar on the left shows 'GitHub Apps', 'OAuth Apps', and 'Personal access tokens' (which is selected and highlighted with a yellow box). The main content area is titled 'Personal access tokens' and includes a 'Generate new token' button. A note says: 'Need an API token for scripts or testing? Generate a personal access token for quick access to the GitHub API.' Below that, another note says: 'Personal access tokens function like ordinary OAuth access tokens. They can be used instead of a password for Git over HTTPS, or can be used to authenticate to the API over Basic Authentication.' At the bottom, there are links for 'Contact GitHub', 'Pricing', 'API', 'Training', 'Blog', and 'About'.

Enter the password

The screenshot shows the 'Confirm access' page. It features a password input field with the placeholder 'Password' and a redacted password entry. Below the input is a 'Forgot password?' link. A large green 'Confirm password' button is centered at the bottom. A tip message at the bottom states: 'Tip: You are entering sudo mode. We won't ask for your password again for a few hours.' At the very bottom, there are links for 'Terms', 'Privacy', 'Security', and 'Contact GitHub'.



Ve Token hesabimiz olustu



```
↓ Readme_solution_student (1).md ↗ settings.py ↗ userdata.sh X ↗ .env ↗ storage
☰ userdata.sh
1 #!/bin/bash
2 apt-get update -y
3 apt-get install git -y
4 apt-get install python3 -y
5 cd /home/ubuntu/
6 TOKEN="ghp_5zkS1FjvUL08Jk3Acu5s9GGN8d7NHo39nYHF"
7 git clone https://$TOKEN@github.com/Kaya-Ramazan/my-aws-capstone-project.git
8 cd /home/ubuntu/my-aws-capstone-project
9 apt install python3-pip -y
10 apt-get install python3.7-dev libmysqlclient-dev -y
11 pip3 install -r requirements.txt
12 cd /home/ubuntu/my-aws-capstone-project/src
13 python3 manage.py collectstatic --noinput
14 python3 manage.py makemigrations
15 python3 manage.py migrate
16 python3 manage.py runserver 0.0.0.0:80
```

User data da egerkli degisklikleri yaptik

Son dört komut Jangoyu calistiriyor.

```
Step 8: Write RDS database endpoint and S3 Bucket
name in settings file given by Clarusway Fullstack Developer team and push your application into your own public repo on Github
Please follow and apply the instructions in the developer_notes.txt.
```text
- Movie and picture files are kept on S3 bucket named
```

```

aws_capstone_S3
<name>_Blog as object. You should create an S3 bucket and write name of it on "/src/cblog/settings.py" file as AWS_STORAGE_BUCKET_NAME variable. In addition, you must assign region of S3 as AWS_S3_REGION_NAME variable
- Users credentials and blog contents are going to be kept on RDS database. To connect EC2 to RDS, following variables must be assigned on "/src/cblog/settings.py" file after you create RDS;
  a. Database name - "NAME" variable
  b. Database endpoint - "HOST" variables
  c. Port - "PORT"
  d. PASSWORD variable must be written on "/src/.env" file not to be exposed with settings file
```

```

- Please check if this userdata is working or not. to do this create new instance in public subnet and show to students that it is working

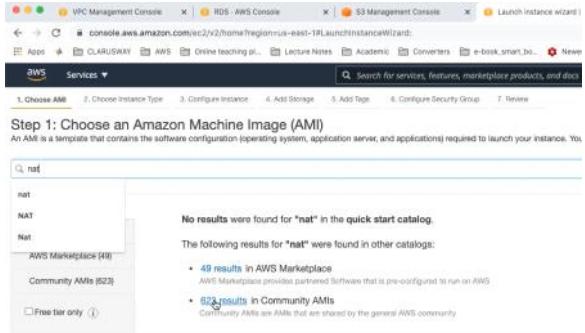
#### ## Step 9: Create NAT Instance in Public Subnet

Public Subnette Nat instance olusturacagiz. Nat instance olusturmamizin sebebi Auto scaling olusturacagiz ki bunun icin öncelikle bir Launch Template olusturacaktik . AutoScalin EC2 olusturacak ve Ec2 larda Data cekmek isteyeceler onun icin Nat instance ihtiyaci var.

To launch NAT instance, go to the EC2 console and click the create button.

```

```text
write "NAT" into the filter box
select NAT Instance `amzn-ami-vpc-nat-hvm-2018.03.0.20181116-x86_64-ebs`
```



```

Instance Type: t2.micro
Configure Instance Details
  - Network : aws_capstone_VPC
  - Subnet : aws_capstone-public-subnet-1A (Please select one of your Public Subnets)
    - Other features keep them as are
Storage ---> Keep it as is
Tags: Key: Name      Value: AWS Capstone NAT Instance
Configure Security Group
  - Select an existing security group: aws_capstone_NAT_Sec_Group
Review and select our own pem key
```

```

**!!!IMPORTANT!!!**

- select newly created NAT instance and enable stop source/destination check
- go to private route table and write a rule

```

Destination : 0.0.0.0/0
Target : instance ---> Select NAT Instance
Save
```

```

Public Subnetlerde olusturacagiz

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of lower prices, or use Auto Scaling to automatically manage the number of instances based on demand.

Number of Instances	1	Launch into Auto Scaling Group
Purchasing option	<input type="checkbox"/> Request Spot Instances	
Network	vpc-0142f2295c4ec3c14 aws_capstone-VPC	
Subnet	<input checked="" type="checkbox"/> subnet-01e80641d4d2ade39 aws_capstone-private-subnet-1B us-east-1a <input checked="" type="checkbox"/> subnet-099966662f9dd3a13 aws_capstone-public-subnet-1B us-east-1b <input type="checkbox"/> subnet-05335f428973bc72 aws_capstone-public-subnet-1A us-east-1a <input type="checkbox"/> subnet-0bb5b543e282ef89b1 aws_capstone-private-subnet-1A us-east-1a	
Auto-assign Public IP	<input type="checkbox"/>	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	Open	
Domain join directory	No directory	
IAM role	None	

Nat instance olusturduktan sonra Actions ---Change Source destination Check edecegiz ---stop edecegiz

Instances (1/1) Info

Filter instances

Instance state: running X Clear filters

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
AW5 Capstone NAT Instance	i-0d8242f6da16449db	Running	t2.micro	Initializing	No alarms	-	-

Actions ▾

- Connect
- View details
- Manage instance state
- Instance settings
- Networking
- Security
- Image and templates
- Dissociate Elastic IP address
- Monitor and troubleshoot
- Change Source/destination check
- Stop
- Start
- Reboot
- Terminate
- Launch Instances

Daha sonra Private Rote Table'lere bir Raute Table eklememiz

gerekiyor. Private

Makinalrd da dis dunyaya gitmek istediklerinde bi istegi nat instance aktarmasini sagla diyoruzz.

VPC Management Console | RDS - AWS Console | S3 Management Console | Instances | EC2 Management | aws_capstone_tr/settings.s | Options

Route tables | rtb-0c58971831b4e084b | Edit routes

Edit routes

Destination	Target	Status	Propagated
pl-63a5400a	vpce-07b8cb6e715d4d45e	Active	No
90.90.0.0/16	local	Active	No
0.0.0.0/0	i-0d8242f6da16449db (AW5 Capstone NAT Instance)	-	No

Add route

Simdi de Launch Template olusturacagiz Launch Template tanimlamak icin EC2 ile konusabilmesi icin 2 alternatif var bunlardan ilki boto3 ile oluyor. Veyahut bu ulasmayi iam Role tanimlayarak da yapabiliyoruz.

Full access yetkisi verecek bir IAM Role tanimlayacagiz ki bunun ile

Ilk olarak EC2 seciyoruz

Select type of trusted entity



Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose a use case

Common use cases

EC2

Allows EC2 Instances to call AWS services on your behalf.

Lambda

Allows Lambda functions to call AWS services on your behalf.

Or select a service to view its use cases

API Gateway	CodeBuild	EMR	IoT SiteWise	RDS
AWS Lambda	CloudFront	FMS	IoT Things Graph	Redshift

Step 10: Create Launch Template and IAM role for it

Go to the IAM role console click role on the right hand menu than create role

```
```text
trusted entity : EC2 as ---> click Next:Permission
Policy : AmazonS3FullAccess policy
Tags : No tags
Role Name : aws_capstone_EC2_S3_Full_Access
Description : For EC2, S3 Full Access Role
```

## Create role

### Attach permissions policies

Choose one or more policies to attach to your new role.

Rol Create edildikten sonra Launch Template olusturacagiz;

```
```
- create launch template
```

Services ▾

>Delete Launch Template Request Succeeded

EC2 > Launch templates > Create launch template

Create launch template

Creating a launch template allows you to create a saved instance configuration that can be reused, shared and launched later time. Templates can have multiple versions.

Launch template name and description

Launch template name - required

aws_capstone_launch_template

Must be unique to this account. Max 128 chars. No spaces or special characters like '&', '*', '@'.

Template version description

A prod webserver for MyApp

Max 255 chars

Auto Scaling guidance [Info](#)

Select this if you intend to use this template with EC2 Auto Scaling

Provide guidance to help me set up a template that I can use with EC2 Auto Scaling

► Template tags
► Source template

Launch template contents

To create Launch Template, go to the EC2 console and select 'Launch Template' on the left hand menu. Tab to the Create Launch Template button.

```
```bash
Launch template name : aws_capstone_launch_template
Template version description : Blog Web Page version 1
Amazon machine image (AMI) : Ubuntu 18.04
Instance Type : t2.micro
Key Pair : mykey.pem
Network Platform : VPC
```

console.aws.amazon.com/ec2/v2/home?region=us-east-1#CreateTemplate:

AMI

Ubuntu Server 18.04 LTS (HVM), SSD Volume Type  
ami-0747bdabd34c12a  
Catalog: Quick Start virtualization: hvm architecture: 64-bit (x86)

▼ Instance type [Info](#)

Instance type

Don't include in launch template

Free tier eligible

t1.micro Family: t1 1 vCPU 0.612 GB Memory  
On-Demand Linux pricing: 0.02 USD per Hour  
On-Demand Windows pricing: 0.02 USD per Hour

t2.nano Family: t2 1 vCPU 0.5 GiB Memory  
On-Demand Linux pricing: 0.0058 USD per Hour  
On-Demand Windows pricing: 0.0081 USD per Hour

t2.micro Family: t2 1 vCPU 1 GiB Memory  
On-Demand Linux pricing: 0.0116 USD per Hour  
On-Demand Windows pricing: 0.0162 USD per Hour

t2.small Family: t2 2 vCPU 2 GiB Memory  
On-Demand Linux pricing: 0.023 USD per Hour  
On-Demand Windows pricing: 0.032 USD per Hour

t2.medium Family: t2 2 vCPU 4 GiB Memory  
On-Demand Linux pricing: 0.0464 USD per Hour  
On-Demand Windows pricing: 0.0644 USD per Hour

t2.large Family: t2 2 vCPU 8 GiB Memory  
On-Demand Linux pricing: 0.0928 USD per Hour  
On-Demand Windows pricing: 0.1208 USD per Hour

Create new key pair

```
Security Groups : aws_capstone_EC
2_sec_group
Storage (Volumes)
Resource tags : Key: Name Val
 ue: aws_capstone_web_server
Advance Details:
 - IAM instance profile : aws_capstone_EC
 2_S3_Full_Access
 - Termination protection : Enable
```

### ▼ Network settings

Networking platform [Info](#)

**Virtual Private Cloud (VPC)**  
Launch into a virtual network in your own logically isolated area within the AWS cloud.

**EC2-Classic**  
Launch into a single flat network that you share with other customers.

Security groups [Info](#)

Select security groups	
<input type="checkbox"/> <a href="#">aws_cap</a>	X
Specify a custom value...	C
<a href="#">aws_capstone_EC2_Sec_Group</a> VPC: vpc-0142f2295c4ac3c14	sg-0360174d6fdb3ff2
<a href="#">aws_capstone_ALB_Sec_Group</a> VPC: vpc-0142f2295c4ac3c14	sg-0b9feaaa077d1364a
<a href="#">aws_capstone_RDS_Sec_Group</a> VPC: vpc-0142f2295c4ac3c14	sg-0de2ae839b36b26ae
<a href="#">aws_capstone_NAT_Sec_Group</a> VPC: vpc-0142f2295c4ac3c14	sg-0de41985e420e842a

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance.

[Add new volume](#)

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance.

### ▼ Resource tags [Info](#)

Key <a href="#">Info</a>	Value <a href="#">Info</a>	Resource types <a href="#">Info</a>
<input type="text"/> Name X	<input type="text"/> aws_capstone_w X	<input type="text"/> Select resource types X
<a href="#">Instances</a> X		
<a href="#">Add tag</a>		

49 remaining (Up to 50 tags maximum)

### ▼ Network interfaces [Info](#)

Apps CLARUSWAY AWS Online teaching pl... Lecture Notes Academic |

aws Services ▾ Search for s

template.

Add network Interface

**Advanced details** Info

Purchasing option [Info](#)

Request Spot Instances

Request Spot Instances at the Spot price, capped at the On-Demand price

IAM Instance profile [Info](#)

Don't include in launch template

Q |

Specify a custom value...

Don't include in launch template

Admin  
arn:aws:iam::046402772087:instance-profile/Admin

ansible\_dynamic\_inv  
arn:aws:iam::046402772087:instance-profile/ansible\_dynamic\_inv

aws-elasticbeanstalk-ec2-role  
arn:aws:iam::046402772087:instance-profile/aws-elasticbeanstalk-ec2-role

aws\_capstone\_EC2\_S3\_Full\_Access  
arn:aws:iam::046402772087:instance-profile/aws\_capstone\_EC2\_S3\_Full\_Access

call-ec2-ecr-full-access  
arn:aws:iam::046402772087:instance-profile/call-ec2-ecr-full-access

Call-Jenkins-JenkinsServerEC2Profile-1A152LCKK0G7  
arn:aws:iam::046402772087:instance-profile/Call-Jenkins-JenkinsServerEC2Profile-1A152LCKK0G7

call-rke-role-cohort1  
arn:aws:iam::046402772087:instance-profile/call-rke-role-cohort1

Elastic Inference [Info](#)

Add Elastic Inference accelerators

**User Data**

```
#!/bin/bash
apt-get update -y
apt-get install git -y
apt-get install python3 -y
cd /home/ubuntu/
TOKEN="ghp_5zkSIFjVUL08Jk3Acu5s9GGN8d7NHo39nYHF"
git clone https://$TOKEN@github.com/Kaya-Ramazan/my-
aws-capstone-project.git
cd /home/ubuntu/my-aws-capstone-project
apt install python3-pip -y
apt-get install python3.7-dev default-libmysqlclient-
dev -y
pip3 install -r requirements.txt
cd /home/ubuntu/my-aws-capstone-project/src
python3 manage.py collectstatic --noinput
python3 manage.py makemigrations
python3 manage.py migrate
python3 manage.py runserver 0.0.0.0:80
```

Metadata version [Info](#)

Don't include in launch template

Metadata response hop limit [Info](#)

Don't include in launch template

User data [Info](#)

```
#!/bin/bash
apt-get update -y
apt-get install git -y
```

User data has already been base64 encoded

Cancel **Create launch template**

Production Ortaminda en basit bir site adahil secur bir baglansti yapmak ister. Browserlar sec baglanti var ise

HTTP den yayin Yaptazlar daha secure olan HTTPS den yayin yaparlar incip etmek icin sertifikalari kullanirlar

**## Step 11: Create certification for secure connection**

Go to the certification manager console and click 're

quest a certificate` button. Select `Request a public certificate`, then `request a certificate` ---> `\*.< YOUR DNS NAME>` ---> DNS validation ---> No tag ---> Review ---> click confirm and request button. Then it takes a while to be activated.

The screenshot shows the AWS Services search interface with the query "certificate manager". The results list includes "Certificate Manager" under "Services (10)", which is highlighted. Other services listed include Secrets Manager, Incident Manager, and Systems Manager. Below the main search results, there is a section titled "Features" with "See all 23 results".

[Yeni alamak için;](#)

## Certificates

The screenshot shows the AWS Certificate Manager console. At the top, there are buttons for "Request a certificate" and "Import a certificate". Below that is a table with columns "Name" and "Domain name", showing one entry for "\*.clarusway.us". Under the "Status" section, it says "Status Issued" and "Detailed status The certificate was issued a". Further down, there is a "Request a certificate" form with steps 1-5. Step 1 is "Add domain names" with a sub-step "Add domain name" and a text input field containing "clarusway.us". Step 2 is "Select validation method" with two options: "DNS validation" (selected) and "Email validation".

## Select validation method

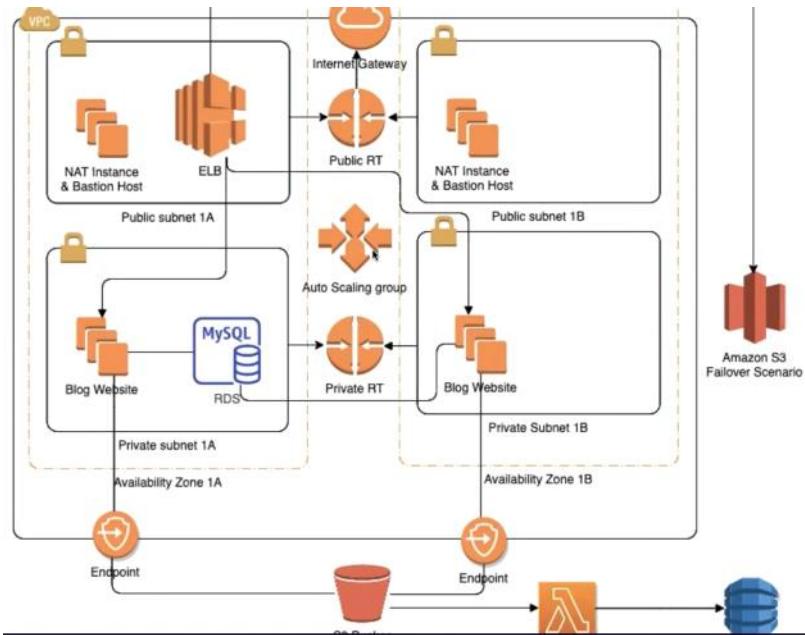
Choose how AWS Certificate Manager (ACM) validates your certificate by using DNS or by sending email to the contact addresses of the domain.

### DNS validation

Choose this option if you have or can obtain permission to:

### Email validation

Choose this option if you do not have permission or cannot:



Simdiye kadar yaptıklarımızı özetler ısek ;

- Vpc leri kurduk
- Availability zonalar ve Subnetleri ayarladık
- internetGateway baglandı
- Public Subnetleri Asocate ettik
- RDS kurduk
- Endointimizi verdik

#### ## Step 12: Create ALB and Target Group

**Go to the Load Balancer section** on the left hand side menu of EC2 console. Click `create Load Balancer` button and select Application Load Balancer

```
```text
Name : awscapstoneALB
Schema : internet-facing
```



Step 1: Configure Load Balancer

To configure your load balancer, provide a name, select a scheme, specify one or more listeners, and selec

Name	: awscapstoneALB
Scheme	<input checked="" type="radio"/> internet-facing <input type="radio"/> internal
IP address type	: IPv4

Listeners

Listeners : HTTPS, HTTP

Listeners
A listener is a process that checks for connection requests, using the protocol and port that you configured.

Load Balancer Protocol	Load Balancer Port
HTTP	80
HTTPS (Secure HTTP)	443
Add listener	

Availability Zones :
 - VPC : aws_capstone_VPC
 - **Availability zones:**
 1. aws_capstone-public-subnet-1A
 2. aws_capstone-public-subnet-1B

Availability Zones

Specify the Availability Zones to enable for your load balancer. The load balancer routes traffic to the targets in these Availability Zones only.

VPC: vpc-0142f2295c4ac3c14 (90.90.0.0/16) | aws_capstone-VPC
 Availability Zones: us-east-1a ✓ Select a subnet
 subnet-0533bf42bf973bc72 (aws_capstone-public-subnet-1A)
 subnet-0bdb543e282ef89b1 (aws_capstone-private-subnet-1A)

Public e yerlestiriyoruz cunku yayin yapacak

Step 2 - Configure Security Settings

Certificate type ---> Choose a certificate from ACM (recommended)

- Certificate name : "*.clarusway.us" certificate
- Security policy : keep it as is

1. Configure Load Balancer 2. Configure Security Settings 3. Configure Security Groups 4. Configure Routing 5. Register Targets 6. Review
Step 2: Configure Security Settings
 Select default certificate
 AWS Certificate Manager (ACM) is the preferred tool to provision and store server certificates. If you previously stored a server certificate using IAM, you can deploy it to your load balancer. Learn more about ACM
 Certificate type: Choose a certificate from ACM (recommended)
 Upload a certificate to ACM (recommended)
 Choose a certificate from IAM
 Upload a certificate to IAM
 Certificate name: clarusway.us [arn:aws:acm:us-east-1:046402772087:certificate/0e0bd5]

Select Security Policy
 Security policy: ELBSecurityPolicy-2016-08

Step 3 - Configure Security Groups : aws_capstone_ALB_Sec_group

Step 3: Configure Security Groups

A security group is a set of firewall rules that control the traffic to your load balancer. On this page, you can add rules to allow specific traffic to reach your load balancer. If

Assign a security group: Create a new security group Select an existing security group

Security Group ID	Name	Description
<input checked="" type="checkbox"/> sg-0b9feea077d1364a	aws_capstone_ALB_Sec_Group	ALB Security Group allows traffic HTTP and HTTPS ports from anywhere
<input type="checkbox"/> sg-0360174d6fd3ff2	aws_capstone_EC2_Sec_Group	EC2 Security Groups only allows traffic coming from aws_capstone_ALB_Sec_Group Sec
<input type="checkbox"/> sg-0de41985e420e842a	aws_capstone_NAT_Sec_Group	NAT Security Group allows traffic HTTP and HTTPS and SSH ports from anywhere
<input type="checkbox"/> sg-0de2ae839b36b26ae	aws_capstone_RDS_Sec_Group	EC2 Security Groups only allows traffic coming from aws_capstone_EC2_Sec_Group Sec
<input type="checkbox"/> sg-0bfe2bb9c60bc7ac	default	default VPC security group

Step 4 - Configure Routing

- Target group : New target group
- Name : awscapstoneTargetGroup
- Target Type : Instance
- Protocol : HTTP
- Port : 80

Step 4: Configure Routing
 Your load balancer routes requests to the targets in this target group using the protocol and port that you specify here. It also performs health checks on the targets using these settings. The target group you specify in this step will apply to all of the listeners configured on this load balancer. You can change or add listeners after the load balancer is created.

Target group
 Target group: New target group
 Name: awscapstoneTargetGroup
 Target type: Instance
 Protocol: HTTP
 Port: 80
 Protocol version: HTTP/1.1
 Health checks
 Protocol: HTTP
 Path: /

Hand-drawn diagram: A red circle labeled "ELB" is at the top, connected by arrows to three separate boxes labeled "EC2". Each EC2 box has a blue circle with the number "80" inside, representing the port number.

Instance nerede calisiyorsa o portta calistirmamiz gerekiyor

- Protocol version : HTTP1
- Health Check :
- Protocol : HTTP
- Path : /
- Port : traffic port
- Healthy threshold : 5 ----- ardi ardina gonderilen 3 saglik sinyalinde sagliklin olarak

muhurluyor
 - Unhealthy threshold : 2-----ard ardina 2 kez gonderdi ve cevap alamadi sagliksz olarak nitelendiriyor
 - Timeout : 5 -----sinyali gönderdikten sonra bekleme suresi
 - Interval : 20
 - Success Code : 200 ----- herhangi problem yok demejtir.

Health checks

Protocol: HTTP
 Path: /

Advanced health check settings

Port: traffic port
 override

Healthy threshold: 5
 Unhealthy threshold: 2
 Timeout: 5 seconds
 Interval: 30 seconds
 Success codes: 200

Step 5 - Register Targets

without register any target click Next: Review

- click create
 To redirect traffic from HTTP to HTTPS, go to the ALB console and select Listeners sub-section.

```
```text
select HTTP: 80 rule --> click edit
- Default action(s)
- Remove existing rule and create new rule which is
 - Redirect to HTTPS 443
 - Original host, path, query
 - 301 - permanently moved
```

```

Lets go ahead and look at our ALB DNS --> it going to say "it is not safe", however, it will be fixed after settings of Route 53

Load balanceri olusturduktan sonra yayini 80 portundan gelen yayini mevcutta Target Guruba gonderiyor iken Biz Once 443 HTTPS e gondermesini ve sonmrasinda Target guruba gitmrisni istiyorduk. Bu sekilde daha secure olacakti.

The screenshot shows the AWS Lambda Load Balancer configuration page. At the top, there's a search bar and a table with one row for 'awscapstoneALB'. The table columns include Name, DNS name, State, VPC ID, Availability Zones, and Type. The 'Listeners' tab is selected in the navigation bar below. Under the 'Listeners' tab, there's a table showing two listeners: 'HTTP : 80' and 'HTTPS : 443'. Both listeners have their 'Forwarding' rules set to point to the 'awscapstoneTargetGroup'. A note at the bottom of the listener section states: 'A listener checks for connection requests using its configured protocol and port, and the load balancer uses the listener rules to route requests to targets. You can add, remove, or update listeners and lists'.

Bunun icin 80 baglantisini tiklayip edit diyoruz.



View/edit listener. Each listener must include one action of type forward, redirect, fo

awscapstoneALB | HTTP : 80

Listeners belonging to Application Load Balancers check for connection requests u are routed. Once you have created your listener, you can create and manage addit

ARN
 arn:aws:elasticloadbalancing:us-east-1:046402772087:listener/app/awscapstoneAl

awscapstoneALB | HTTP : 80

Listeners belonging to Application Load Balancers check for connection requests u are routed. Once you have created your listener, you can create and manage additk

ARN
arn:aws:elasticloadbalancing:us-east-1:046402772087:listener/app/awscapstoneAl

Protocol : port
Select the protocol for connections from the client to your load balancer, and enter a port

HTTP : 80

Default action(s)
Indicate how this listener will route traffic that is not otherwise routed by another rule.

1. Forward to
awscapstoneTargetGroup: 1 (100%)
Group-level stickiness: Off

+ Add action

Ardindan default olan Forwardi siliyoruz

awscapstoneALB | HTTP : 80

Listeners belonging to Application Load Balancers check for connection requests u are routed. Once you have created your listener, you can create and manage additc

ARN
arn:aws:elasticloadbalancing:us-east-1:046402772087:listener/app/awscapstoneAl

Protocol : port
Select the protocol for connections from the client to your load balancer, and enter a port

HTTP : 80

Default action(s)
Indicate how this listener will route traffic that is not otherwise routed by another rule.

+ Add action

Forward to...
Redirect to...
Return fixed response...

Note: Additional actions are available for HTTPS listeners.

Ve Redirection ekliyoruz ve 443 secip tikliyoruz.

awscapstoneALB | HTTP : 80

Listeners belonging to Application Load Balancers check for connection requests using the protocol are routed. Once you have created your listener, you can create and manage additional routing rules

ARN
arn:aws:elasticloadbalancing:us-east-1:046402772087:listener/app/awscapstoneALB/07ad59d5f51e

Protocol : port
Select the protocol for connections from the client to your load balancer, and enter a port number from which

HTTP : 80

Default action(s)
Indicate how this listener will route traffic that is not otherwise routed by another rule.

1. Redirect to...
HTTPS : 443 Original value: #(port)
Original host, path, query
301 - Permanently moved
Switch to full URL

+ Add action

Step 13: Create AutoScaling Group with Launch Template

Go to the AutoScaling Group on the left hand side men

u. Click create Autoscaling group.

- Choose launch template or configuration

```
```text
Auto Scaling group name : aws_capstone_ASG
Launch Template : aws_capstone_launch
template
```

```

EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1
Choose launch template or configuration

Step 2
Configure settings

Step 3 (optional)
Configure advanced options

Step 4 (optional)
Configure group size and scaling policies

Step 5 (optional)
Add notifications

Step 6 (optional)
Add tags

Step 7
Review

Choose launch template or configuration Info

Specify a launch template that contains settings common to all EC2 instances that are launched by this Auto Scaling group. If you currently use launch configurations, you might consider migrating to launch templates.

Name

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

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

Launch template Info **Switch to launch configuration**

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.
aws_capstone_launch_template

Create a launch template Info

Version
Default (1)

- Configure settings

```
```text
Instance purchase options : Adhere to launch te
mplate
Network
 - VPC : aws-capstone-VPC
 - Subnets : Private 1A and Priv
ate 1B
```

```

Instance purchase options Info

Use the launch template to create a uniform configuration among all of the instances in the group. Or define options to accommodate a wide variety of requirements, such as launching Spot and On-Demand Instances.

Adhere to launch template
The launch template determines the purchase option (On-Demand or Spot) and instance type.

Combine purchase options and instance types
Specify how much On-Demand and Spot capacity to launch and multiple instance types (optional). This choice is most helpful for optimizing the scale and cost for a fleet of instances.

Network Info

For most applications, you can use multiple Availability Zones and let EC2 Auto Scaling balance your instances across the zones. The default VPC and default subnets are suitable for getting started quickly.

VPC
vpc-0142f2295c4ac3c14 (aws_capstone-VPC) 90.90.0.0/16

Create a VPC Info

Subnets

| | |
|--|---|
| us-east-1a subnet-0bdb543e282ef89b1
(aws_capstone-private-subnet-1A)
90.90.11.0/24 | X |
| us-east-1b subnet-01e80641d4d2ade39 | X |

- Configure advanced options

```
```text
- Load balancing : Att
ach to an existing load balancer
- Choose from your load balancer target groups : aws
capstoneTargetGroup
```

```

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 ▾ C

Q |

awscapstoneTargetGroup | HTTP
Application Load Balancer: awscapstoneALB

```
- Health Checks
  - Health Check Type      : ELB
  - Health check grace period : 300
```

```

#### Health checks - optional

**Health check type** [Info](#)  
 EC2 Auto Scaling automatically replaces instances that fail health checks. If you enabled load balancing, you can enable ELB health checks in addition to the EC2 health checks that are always enabled.

EC2     ELB

**Health check grace period**  
 The amount of time until EC2 Auto Scaling performs the first health check on new instances after they are ~~put~~ into service.

300 seconds

```
- Configure group size and scaling policies
```
text

```

Group size

- Desired capacity : 2
- Minimum capacity : 2
- Maximum capacity : 4

Scaling policies

```
- Target tracking scaling policy
  - Scaling policy name      : Target Tracking
Policy
  - Metric Type              : Average CPU uti
lization
  - Target value             : 70
```

```

**Add notifications**

```
```
text
Create new Notification
- Notification1
  - Send a notification to   : aws-capstone-
SNS
  - with these recipients    : serdar@claruswa
y.com
  - event type                : select all
```

```

Choose whether to use a scaling policy to dynamically resize your Auto Scaling group to meet changes in demand. [Info](#)

<input checked="" type="radio"/> Target tracking scaling policy Choose a desired outcome and leave it to the scaling policy to add and remove capacity as needed to achieve that outcome.	<input type="radio"/> None
Scaling policy name <input type="text" value="Target Tracking Policy"/>	
Metric type <input type="text" value="Average CPU utilization"/>	
Target value <input type="text" value="70"/>	
Instances need <input type="text" value="300"/> seconds warm up before including in metric	
<input type="checkbox"/> Disable scale in to create only a scale-out policy	

**Instance scale-in protection - optional**

Instance scale-in protection  
If protect from scale in is enabled, newly launched instances will be protected from scale in by default.  
 Enable Instance scale-in protection

[Cancel](#) [Previous](#) [Skip to review](#) [Next](#)

Target Training Policy Ec2 instance olusmasi veya hukmet ettilmesi icin belirtilir.

CPU Utilazition ortalama Cpu kullanimi bizim belirledigimiz degere ulasirsa yeni bir instance kuracak altinda kalirsa mevcudu koruyacaktir.

```
<!-- WARNING!!! Sometimes your EC2 has a problem after you create autoscaling group, If you need to look inside one of your instance to make sure where the problem is, please follow these steps...-->
```

```
```bash
eval "$(ssh-agent)" (your local)
ssh-add <pem-key> (your local )
ssh -A ec2-
user@<Public IP or DNS name of NAT instance> (your local)
ssh ubuntu@<Public IP or DNS name of private instance> (NAT instance)
You are in the private EC2 instance
```
-->
```

⚠ Not secure | [awscapstonealb-289774884.us-east-1.elb.amazonaws.com](https://awscapstonealb-289774884.us-east-1.elb.amazonaws.com)



Your connection is not private

Attackers might be trying to steal your information from [awscapstonealb-289774884.us-east-1.elb.amazonaws.com](https://awscapstonealb-289774884.us-east-1.elb.amazonaws.com) (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR\_CERT\_COMMON\_NAME\_INVALID

[Advanced](#)

[Back to safety](#)



Load balancer in DNS name ini alip Consola yapistirinka karsimiza cikan ekran da sol alt kism da ADVANCE tikliyoruz  
Hala not secure gözükmesinin sebebi biz sertifikalari Host Name icin tanimladik Road Balancer in cikarttigi adres icin degil Dolayisiyla bunu oraya yöndirirmemiz gerekiyor

Azciyan sayfada ilk oalrak Register edegez ve kendimizle bir Mail ve

sifre belirleyip sisteme girecegiz



### Blog Post

Title\*  
My Working Room

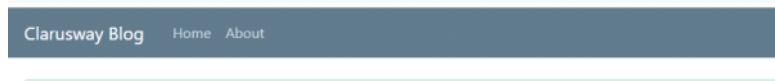
Content\*  
hard working It

Image\*  
 No file chosen

Category\*  
Entertainment

Status\*  
Published

Ve daha sonra



## Clarusway Blog



**My Working Room**  
hard working It  
0 0 1 1 0 0  
Posted 1 minute ago.

## Step 14: Create Cloudfront in front of ALB

Go to the cloudfront menu and click start  
- Origin Settings

Load balancer in Domain Name ini isretliyoruz

```
```text
Origin Domain Name      : aws-capstone-
ALB-1947210493.us-east-2.elb.amazonaws.com
Origin Path            : Leave empty (this means
, define for root '')
```



Step 1: Select delivery method
Step 2: Create distribution

Create Distribution

Origin Settings

Origin Domain Name: clarusway.lambda.images-resized.s3.amazonaws.com

Origin Path: djangoserdarr-encryption-service.s3.amazonaws.com

Step 1: Select delivery method
Step 2: Create distribution

Create Distribution

Origin Settings

Origin Domain Name	<input type="text"/>	
Origin Path	<input type="text"/>	
Origin ID	<input type="text"/>	
Origin Custom Headers	<ul style="list-style-type: none"> — <i>Elastic Load Balancers</i> — awscapstoneALB-1737831641.us-east-1.x — <i>MediaPackage Origins</i> — Failed to List your origins — <i>MediaStore Containers</i> — No Origins Available 	
Default Cache Behavior Settings		
Path Pattern	Default (*)	
Viewer Protocol Policy	<input checked="" type="radio"/> HTTP and HTTPS <input type="radio"/> Redirect HTTP to HTTPS	

Protocol : Match Viewer
 HTTP Port : 80
 HTTPS : 443

Origin Domain Name	<input type="text"/> awscapstoneALB-1737831641.us-east-1.x	
Origin Path	<input type="text"/>	
Enable Origin Shield	<input type="radio"/> Yes <input checked="" type="radio"/> No	
Origin ID	<input type="text"/> ELB-awscapstoneALB-1737831641	
Minimum Origin SSL Protocol	<input type="radio"/> TLSv1.2 <input type="radio"/> TLSv1.1 <input checked="" type="radio"/> TLSv1 <input type="radio"/> SSLv3	
Origin Protocol Policy	<input type="radio"/> HTTP Only <input type="radio"/> HTTPS Only <input checked="" type="radio"/> Match Viewer	
Origin Connection Attempts	<input type="text"/> 3	
Origin Connection Timeout	<input type="text"/> 10	
Origin Response Timeout	<input type="text"/> 30	
Origin Keep-alive Timeout	<input type="text"/> 5	
HTTP Port	<input type="text"/> 80	
HTTPS Port	<input type="text"/> 443	
Origin Custom Headers	Header Name	Value
	<input type="text"/>	<input type="text"/>

Default Cache Behavior Settings

Path Pattern	Default (*)	

```
Minimum Origin SSL Protocol : Keep it as is
Name : Keep it as is
Add custom header : No header
Enable Origin Shield : No
Additional settings : Keep it as is
```

```

### Default Cache Behavior Settings

```
```text
Path pattern : D
default (*) : Y
Compress objects automatically : Y
Viewer Protocol Policy : R
redirect HTTP to HTTPS
Allowed HTTP Methods : G
ET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE : S
Cached HTTP Methods : S
select OPTIONS
Cache key and origin requests
- Use legacy cache settings
```

```

|                                         |                                                                                                                                                              |  |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| Path Pattern                            | Default (*)                                                                                                                                                  |  |
| Viewer Protocol Policy                  | <input type="radio"/> HTTP and HTTPS<br><input checked="" type="radio"/> Redirect HTTP to HTTPS<br><input type="radio"/> HTTPS Only                          |  |
| Allowed HTTP Methods                    | <input type="radio"/> GET, HEAD<br><input type="radio"/> GET, HEAD, OPTIONS<br><input checked="" type="radio"/> GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE |  |
| Field-level Encryption Config           | <input type="button" value=""/>                                                                                                                              |  |
| Cached HTTP Methods                     | GET, HEAD (Cached by default)<br><input checked="" type="checkbox"/> OPTIONS                                                                                 |  |
| Cache and origin request settings       | <input type="radio"/> Use a cache policy and origin request policy<br><input checked="" type="radio"/> Use legacy cache settings                             |  |
| Cache Based on Selected Request Headers | <input type="button" value="Whitelist"/>                                                                                                                     |  |
|                                         | <a href="#">Learn More</a>                                                                                                                                   |  |

|                                                                                                                                                                                                                                  |                                                                                               |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| <b>Whitelist Headers</b>                                                                                                                                                                                                         |                                                                                               |
| <input type="text" value="Filter headers or enter a custom header"/><br><input type="button" value="Add Custom &gt;&gt;"/><br>Accept<br>Accept-Charset<br>Accept-Datetime<br>Accept-Encoding<br>Accept-Language<br>Authorization | <input type="button" value="Add &gt;&gt;"/><br><input type="button" value="&lt;&lt; Remove"/> |
| Host                                                                                                                                                                                                                             |                                                                                               |
| <small>To use AWS ELB DNS named Origins, you must forward the Host or All headers. <a href="#">Learn more</a>.</small>                                                                                                           |                                                                                               |

Object Caching  Use Origin Cache Headers

### Headerlarda neleri cashlemesini istiyorsak onlari secebiliyoruz

Headers : Include the following headers

Add Header

- Accept
- Accept-Charset
- Accept-Datetime
- Accept-Encoding
- Accept-Language
- Authorization
- Cloudfront-Forwarded-Proto
- Host
- Origin
- Referrer

Forward Cookies : All

Query String Forwarding and Caching : All

Other stuff : Keep them as are  
 ...

Object Caching  Use Origin Cache Headers

[Learn More](#)

Minimum TTL : 0

Maximum TTL : 31536000

Default TTL : 86400

Forward Cookies : All

Query String Forwarding and Caching : Forward all, cache based on all

Smooth Streaming : No

Restrict Viewer Access : No  
(Use Signed URLs or Signed Cookies)

Compress Objects Automatically : Yes

[Learn More](#)

Edge Function Associations

Edge Function

CloudFront Event

Function

- Distribution Settings  
 ...  
 Price Class : Use all edge locations (best performance)  
 Alternate Domain Names : [www.clarusway.us](http://www.clarusway.us)  
 SSL Certificate : Custom SSL Certificate (example.com) ---> Select your certificate created before  
 Other stuff : Keep them as are  
 ...

Distribution Settings

Enable Real-time Logs  Yes  No

Price Class  Use All Edge Locations (Best Performance)

AWS WAF Web ACL  None

Alternate Domain Names (CNAMEs)  www.clarusway.us

SSL Certificate  Default CloudFront Certificate (\*.cloudfront.net)  
Choose this option if you want your users to use HTTPS or HTTP to access your content with the CloudFront domain name https://d111111abcdef8.cloudfront.net/logo.jpg.  
Important: If you choose this option, CloudFront requires that browsers or devices support TLSv1 or later to access your content.

Custom SSL Certificate (example.com):  
Choose this option if you want your users to access your content by using an alternate domain name, such as https://www.yourdomain.com. You can use a certificate stored in AWS Certificate Manager (ACM) in the US East (N. Virginia) Region, or you can use a certificate stored in IAM.

Request or Import a Certificate with ACM

Learn more about using custom SSL/TLS certificates with CloudFront.  
Learn more about using ACM.

**Aynı zaman bu Ec2 lar ELB ye bağlı olacak ELB nin en önemli özelliği EC2 lardaki yoğunluga bakıp HelatCheck ler ile herhangi yoğunluk olması durumunda esit olarak bu yuku EC2 lar arasında dağıtmak. Hem Trafigi yayınıyor hem tek eilden dağılımlı sağlıyor. Hemde Dis dünyadan gelen User In her hangi bir aksama olmadan EC2 ya ulaşılmasını sağlıyor.**

**ALB nin de öünde bir CloudFront koyacagız ki bu da br cash hizmeti sunacak. Videolar ve fotoğraflar S3 den cekilecek her seferinde ücret ödenmemesi için bunu yapacaklar Cash hizmeti ile sağlanacak.**

**Production ortamında Cloudfront s3 un öünde de kurulabiliyor Eger burda tanımlamak istersen s3 u orjin olarak gösterecektir.**

**Developerler kodunu kullanıcı karşısına çıkartmak için Route53 failover senaryosu ile karşımıza çıkacak.**

**Burada Failover senaryosu Route 53 olarak bir ister atanmış durumdadır. Route53 de İki adet ent pointi takip eder. Birisi static website olur. Degiride uniq olarak caaşsan web sistemizdir.basına herhangi bir durum gelmesi halinde secondary e trafigi yönlendirir.**

**Userlar bu hallyle karsılarına bir sey çıkarkı mevcut olarak bir sorunun olduğunu ve bu sorunun bir sure sonra çözüleceği gibi seyler içerebilir.**

Simdide Rote53 e gidecegiz Failover senaryosunu olusturmak için.

AWS Services ▾

Route 53 > Dashboard

### Route 53 Dashboard Info

|                                                                |                                                                                                                                                                    |                                                                                                                                                                                  |
|----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DNS management</b><br>1 Hosted zone                         | <b>Traffic management</b><br>A visual tool that lets you easily create policies for multiple endpoints in complex configurations.<br><a href="#">Create policy</a> | <b>Availability monitoring</b><br>Health checks monitor your applications and web resources, and direct DNS queries to healthy resources.<br><a href="#">Create health check</a> |
| <a href="#">Register domain</a> <a href="#">More resources</a> |                                                                                                                                                                    |                                                                                                                                                                                  |

## Step 15: Create Route 53 with Failover settings

Come to the Route53 console and select Health checks on the left hand menu. Click create health check

console.aws.amazon.com/route53/healthchecks/home#/create

CLARUSWAY AWS Online teaching pl... Lecture Notes Academic Converters e-book\_smart\_bo... New

Services ▾

### Welcome to Route 53 health checks

Route 53 health checks monitor the health and performance of your application's servers, or endpoints, from a network name or an IP address and a port to create HTTP, HTTPS, and TCP health checks that check the health of the endpoint

[Create health check](#)

Health check concepts



Availability and performance monitoring

You can use Route 53 health checks for monitoring and alerts. Each health check provides You can also i

Configure health check

```
```text
Name : aws capstone health check
What to monitor : Endpoint
Specify endpoint by : Domain Name
```

Best practices to optimize Lambda@Edge with CloudFront. [Learn more](#)

Important: On March 23, 2021, CloudFront will begin migrating the Certificate Authority for the *.cloudfront.net certificate. For more information, refer to the AWS

CloudFront Distributions

Create Distribution Distribution Settings Delete Enable Disable

Viewing : Any Delivery Method Any State

Delivery Method	ID	Domain Name	Comment	Origin	CNAMEs
Web	E3YJ8L1Q4R6V8	d30t021hm3ex15.cloudfront.net	-	awscapstoneALB-1	www.claruswa...

CloudFront taki Domain Name alip buraya kopyaliyoruz.

```
Protocol : HTTP
Domain Name : Write cloudfront domain name
Port : 80
Path : leave it blank
Other stuff : Keep them as are
```

Route 53 > Dashboard

Route 53 Dashboard Info

Route 53 Dashboard

DNS management	Traffic management	Availability monitoring	Domain registral
1 Hosted zone	A visual tool that lets you easily create policies for multiple endpoints in complex configurations. Create policy	1 Health check	1 Domain

Register domain

Find and register an available domain, or transfer your existing domains to Route 53.

Enter a domain name [Check](#)

Each label (each part between dots) can be up to 65 characters long and must start with a-z or 0-9. Maximum length: 255 characters, including dots. Valid characters: a-z, 0-9, and - (hyphen).

Notifications

Find notifications [Check](#)

Resource	Status	Last update
----------	--------	-------------

More resources

- Documentation
- API reference
- FAQs
- Forum - DNS and health checks
- Forum - Domain name registration
- Request a limit increase

Service health

- Click **Hosted zones** on the left hand menu
- click your Hosted zone : <YOUR DNS NAME>
- Create Failover scenario
- Click **Create Record**
- Select Failover ---> Click Next

clarusway.us

[Delete zone](#) [Test record](#) [Configure query logging](#) [Edit hosted zone](#)

Hosted zone details

[Records \(4\)](#) [DNSSEC signing](#) [Hosted zone tags \(0\)](#)

Records (4)

Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.

<input type="checkbox"/> Record name	Type	Routin...	Differ...	Value/Route traffic to
clarusway.us	NS	Simple	-	ns-435.awsdns-54.com. ns-1415.awsdns-48.org. ns-861.awsdns-43.net. ns-1648.awsdns-14.co.uk.
clarusway.us	SOA	Simple	-	ns-435.awsdns-54.com. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400
_53c2c6a1969f121d13c875477...	CNAME	Simple	-	_64d4256ba727964ee9dd657a42016674.zxlnyiswt.acm-validations.aws.
_4f75946af91639a9da4632cf...	CNAME	Simple	-	_9810a47cc0708f712ded78ecde990c4.wggjkgigrm.acm-validations.aws.

Route 53 > Hosted zones > clarusway.us > Create record

Step 1: Choose routing policy [Info](#)

The routing policy determines how Amazon Route 53 responds to queries.

Step 2: Configure records

Choose routing policy

Routing policy

- Simple routing Use when you have multiple resources that do the same job, and you want to specify which goes to each resource. For example, two web servers.
- Weighted Use when you have multiple resources that do the same job, and you want to specify the weight for each resource. For example, two web servers.
- Geolocation Use when you want to route traffic based on the location of your users.
- Failover Use to route traffic to a resource that is healthy, and then automatically fail over to a different resource when the first resource is unhealthy.
- Multivalue answer Use when you want Route 53 to return multiple answers. For example, if you want to return up to eight healthy records selected at random.

[Switch to quick create](#)

[Cancel](#) [Next Step](#)

```
```text
Configure records
Record name : www.<YOUR DNS NAME>
Record Type : A - Routes traffic to an IP
v4 address and some AWS resources
TTL
```

```

Record name [Info](#)
 To route traffic to a subdomain, enter the subdomain name. For example, to route traffic to blog.example.com, enter blog. If you leave this field blank, the default record name is the name of the domain.

www [clarusway.us](#)
 Valid characters: a-z, 0-9, ! * # \$ % & " { } ^ _ - / ; < = > ? @ [\] ^ _ { } . ~

Record type [Info](#)
 The DNS type of the record determines the format of the value that Route 53 returns in response to DNS queries.

A – Routes traffic to an IPv4 address and some AWS resources [▼](#)
 Choose when routing traffic to AWS resources for EC2, API Gateway, Amazon VPC, CloudFront, Elastic Load Balancer, ELB, or S3. For example: 192.0.2.44.

TTL (seconds) [Info](#)
 The amount of time, in seconds, that DNS resolvers and web browsers cache the settings in this record. ("TTL" means "time to live.")

300

Recommended values: 60 to 172800 (two days)

Failover records to add to clarusway.us [Info](#)
 Use to route traffic to a resource when the resource is healthy, or to a different resource when the first resource is unhealthy.

[Edit](#) [Delete](#) [Define failover record](#)

| Record ID | Failover record type | Value/Route traffic to | Health check |
|-----------|----------------------|------------------------|--------------|
| | | | |

Define failover records to this list, then choose [Create records](#).

```
: 300
---> First we'll create a primary record for cloudfront
Failover record to add to your DNS ---> Define failover record
Value/Route traffic to : Alias to cloudfront distribution
                         - Select created cloudfront
DNS
Failover record type   : Primary
Health check          : aws capstone health check
Record ID              : Cloudfont as Primary Record
```

clarusway.us

Define failover record

specify where you want to route internet traffic.

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

d30t021hm3ex15.cloudfront.net [X](#)

Failover record type
 Choose Primary to route traffic to the specified resource by default or Secondary to route traffic to the specified resource when the primary resource is unavailable. You can create only one failover record of each type.

Primary [▼](#)

Health check
 Choose the health check that you want Route 53 to use to determine whether this record set is healthy. You can create a health check in the [health check console](#).

aws capstone health check [▼](#)

Evaluate target health
 Select Yes if you want Route 53 to use this record to respond to DNS queries only if the specified AWS resource is healthy.

No

Record ID
 Enter a unique description that differentiates this record from other records with the same name and type.

this record was created for cloudfont and it is a primary one

[Cancel](#) [Define failover record](#)

[Cancel](#) [Previous](#) [Create records](#)

```
--> Second we'll create secondary record for S3
Failover another record to add to your DNS ---> Define failover record
Value/Route traffic to : Alias to S3 website endpoint
                         - Select Region
                         - Your created bucket name
emerges ---> Select it
Failover record type   : Secondary
Health check          : No health check
Record ID              : S3 Bucket for Secondary record type
```
- click create records
```

**Define failover record**

**Value/Route traffic to**  
The option that you choose determines how Route 53 responds to DNS queries. For most options, you specify where you want to route internet traffic.

Alias to S3 website endpoint  
US East (N. Virginia) [us-east-1]  
s3-website-us-east-1.amazonaws.com

**Failover record type**  
Choose Primary to route traffic to the specified resource by default or Secondary to route traffic to the specified resource when the primary resource is unavailable. You can create only one failover record of each type.

Secondary

**Health check - optional**  
Choose the health check that you want Route 53 to use to determine whether this record set is healthy. You can create a health check in the [health check console](#).

Choose health check

**Evaluate target health**  
Select Yes if you want Route 53 to use this record to respond to DNS queries only if the specified AWS resource is healthy.

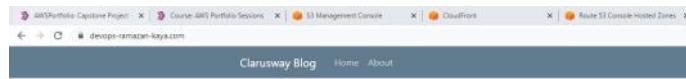
Yes

**Record ID**  
Enter a unique description that differentiates this record from other records with the same name and type.

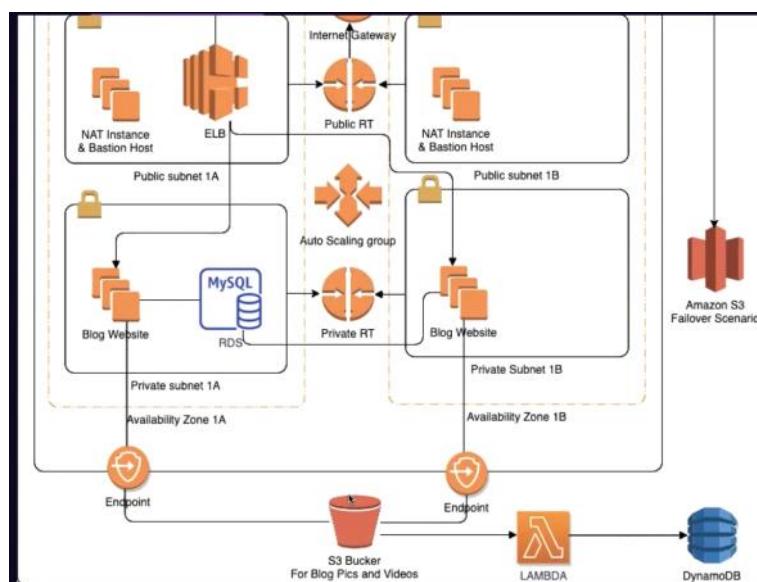
This record is the secondary one

Cancel Define failover record

Artık sitemiz yayın yapmaya başladı ve secure bir yayındır.  
Clou'dFront ile oluşturduğumuz yayısu anda secure bir bagaalantı



Simdi secure bir bağlantı yapmış oldulk



Developerlar s3 de atılan objelerin takibini yapmak için DYNAMODB  
de liste haliunde bunun takibini yapmak istiyorlar

#### # Step 16: Create DynamoDB Table

Go to the Dynamo Db table and click create table butt  
on

- Create DynamoDB table

```text

```
Name : awscapstoneDynamo  
Primary key : id  
Other Stuff : Keep them as are  
click create
```

Create DynamoDB table

DynamoDB is a schema-less database that only requires a table name and primary key. The table's primary key is made up of one or two attributes that uniquely identify items, partition the data, and sort data within each partition.

Table name* awscapstoneDynamo

Primary key* Partition key

id String

Add sort key

Table settings

Default settings provide the fastest way to get started with your table. You can modify these default settings now or after your table has been created.

Use default settings

- No secondary indexes.
- Auto Scaling capacity set to 70% target utilization, at minimum capacity of 5 reads and 5 writes.
- Encryption at Rest with DEFAULT encryption type.

+ Add tags NEW!

Additional charges may apply if you exceed the AWS Free Tier levels for CloudWatch or Simple Notification Service. Advanced alarm settings are available in the CloudWatch management console.

Cancel Create

Step 17-18: Create Lambda function

Lambda Fonksiyonunun s3 e ulaşması lazım yani
konusması lazım ayrıca Dynamodb ile konuşuyor olamış
a+lazım ayrıca Network altyapısında irtibatalanması
gerekliyor

Before we create our Lambda function, **we should create an IAM role** that we'll use for Lambda function. Go to the IAM console and select role on the left hand menu, then create role button

```text

Select Lambda as trusted entity ---> click Next:Permission

Choose:  
- LambdaS3FullAccess,  
- Network Administrator  
- DynamoDBFullAccess

#### Create role

1 2 3 4

##### Attach permissions policies

Choose one or more policies to attach to your new role.

Create policy

Filter policies ▾ Q Search Showing 8 results

|                                     | Policy name                                            | Used as                |
|-------------------------------------|--------------------------------------------------------|------------------------|
| <input checked="" type="checkbox"/> | AmazonDynamoDBFullAccess                               | None                   |
| <input type="checkbox"/>            | AmazonDynamoDBReadOnlyAccess                           | None                   |
| <input type="checkbox"/>            | AWSApplicationAutoscalingDynamoDBTablePolicy           | Permissions policy (1) |
| <input type="checkbox"/>            | AWSLambdaDynamoDBExecutionRole                         | None                   |
| <input type="checkbox"/>            | AWSLambdaInvocation-DynamoDB                           | None                   |
| <input type="checkbox"/>            | DynamoDBCloudWatchContributorInsightsServiceRolePolicy | None                   |
| <input type="checkbox"/>            | DynamoDBKinesisReplicationServiceRolePolicy            | None                   |
| <input type="checkbox"/>            | DynamoDBReplicationServiceRolePolicy                   | None                   |

Get recommended by AWS

No tags

Role Name : aws\_capstone\_lambda\_Role

Role description : This role give a permission to

lambda to reach S3 and DynamoDB on custom VPC

```

then, go to the Lambda Console and click **create function**

- Basic Information

```text

**Create function** Info

Choose one of the following options to create your function.

Author from scratch  
Start with a simple Hello World example.

Use a blueprint  
Build a Lambda application from sample code and configuration presets for common use cases.

Container image  
Select a container image to deploy for your function.

Browse serverless  
Deploy a sample Lambda Serverless Application

**Basic information**

**Function name**  
Enter a name that describes the purpose of your function.  
**awscapsitonelambdafunction**

**Runtime** Info  
Choose the language to use when writing your functions. Note that the console code editor supports only Node.js, Python, and Ruby.  
**Python 3.8**

**Permissions** Info  
By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this default role later when adding triggers.

**Change default execution role** Info

**Advanced settings**

## Permissions Info

By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs.

### ▼ Change default execution role

#### Execution role

Choose a role that defines the permissions of your function. To create a custom role, go to

- Create a new role with basic Lambda permissions  
 Use an existing role  
 Create a new role from AWS policy templates

#### Existing role

Choose an existing role that you've created to be used with this Lambda function. The role

**Function Name** : awscapsitonelambdafunction  
**Runtime** : **Python 3.8**  
**Create IAM role** : S3 full access policy  
**Advance Setting:**  
**Network** :  
- **VPC** : aws-capstone-VPC  
- **Subnets** : Select **all** subnets  
- **Security Group** : Select default security Gro

up

```  
- Now we'll go to the S3 bucket belongs our website and create an event to trigger our Lambda function.

Code signing configuration - optional Info
To enable code signing, choose a configuration that defines the signature validation policy and the signing profiles that are permitted to sign code.

Choose a code signing configuration ARN

Network
To provide network access for your Lambda function, specify a virtual private cloud (VPC), VPC subnets, and VPC security groups. VPC configuration is optional unless your user permissions require you to configure a VPC.

VPC - optional Info
Choose a VPC for your function to access.

vpc-0142f2295c4ac3c14 (90.90.0.0/16)

Subnets
Select the VPC subnets for Lambda to use to set up your VPC configuration.

Choose subnets

subnet-01e80641d4d2ade39 (90.90.21.0/24) us-east-1b X
Name: aws_capstone-private-subnet-1B

subnet-05335f428f973bc72 (90.90.10.0/24) us-east-1a X
Name: aws_capstone-public-subnet-1A

subnet-099966662f9dd3a13 (90.90.20.0/24) us-east-1b X
Name: aws_capstone-public-subnet-1B

subnet-0bdb543e282ef89b1 (90.90.11.0/24) us-east-1a X
Name: aws_capstone-private-subnet-1A

Security groups
Choose the VPC security groups for Lambda to use to set up your VPC configuration. The table below shows the inbound and outbound rules for the security groups that you choose.

Choose security groups

sg-0bef2bb9c60bc7ac (default) X
default VPC security group

Inbound rules **Outbound rules**

Ve simdi de s3 de event olusturacagiz; bu s3 bucket iniizin altina ne

dosya atilrsa bir event olusturmasini isteyecegiz

The screenshot shows the Amazon S3 console interface. At the top, the path is listed as 'Amazon S3 > awscapstones3ramazanblog > media/ > blog/ > 1/'. Below this, there is a header with tabs for 'Objects' (which is selected) and 'Properties'. A large '1/' is displayed above the object list. On the right side of the header, there is a 'Copy S...' button. The main area is titled 'Objects (1)' and contains a table with one item. The table columns are 'Name', 'Type', 'Last modified', 'Size', and 'Storage class'. The item listed is 'Calisma_ortamı.jpeg', which is a 'jpeg' file last modified on August 27, 2021, at 20:13:30 (UTC+03:00), with a size of 129.6 KB and a storage class of Standard. Below the table is a search bar with the placeholder 'Find objects by prefix'.

**Bucketimizin----- Properties kismina tiklayip daha somra-----
event notifications kismina tiklayacagiz**

Event Notifications S3 un bucktin altinda her hangi bir sey olusstugu
taktirde onu event olusturur

Ve bu event i Lambda functiona tanitacagiz

Step 17-18: Create S3 Event and set it as trigger for Lambda Function

Go to the S3 console and select the S3 bucket named `awscapstonec3<name>blog` .
- Go to the properties menu ---> Go to the Event notifications part
- Click create event notification for creating object
```text  
Event Name : aws capstone S3 event  
Prefix : media/

**Egerki Suffix kismina jpeg belirtirseniz sadece  
jpegleri Isitelemis olursunuz**

The screenshot shows the 'Create event notification' configuration page. At the top, it says 'Create event notification'. Below that, a note states: 'The notification configuration identifies the events you want Amazon S3 to publish and the destination Amazon S3 to send the notifications. [Learn more](#)'.

**General configuration**

Event name: aws capstone S3 event  
Event name can contain up to 255 characters.

Prefix - optional: media/

Suffix - optional: jpg

Select :  
- All object create events  
Destination : Lambda Function  
Specify Lambda function : Choose from your Lambda functions  
Lambda function : awscapstonelambdafunction  
click save

**Event types**

Specify at least one type of event for which you want to receive notifications. [Learn more](#)

- All object create events
  - Put
    - s3:ObjectCreated:Put
  - Post
    - s3:ObjectCreated:Post
  - Copy
    - s3:ObjectCreated:Copy
  - Multipart upload completed
    - s3:ObjectCreated:CompleteMultipartUpload
- All object delete events
  - Permanently deleted
    - s3:ObjectRemoved:Delete
  - Delete marker created

```
```text
```
- After create an event go to the `awscapstonelambdafunction` lambda Function and click add trigger on the top left hand side.
- For defining trigger for creating objects
```

Lambda > Functions > awscapstonelambdafunction

### awscapstonelambdafunction

▼ Function overview [Info](#)

 awscapstonelambdafunction  
 Layers (0)  
[+ Add trigger](#)

[Code](#) | [Test](#) | [Monitor](#) | [Configuration](#) | [Aliases](#) | [Versions](#)

**Code source** [Info](#)

File Edit Find View Go Tools Window [Test](#) Deploy Changes deployed

Go to Anything (⌘ P)  

environment  awscapstonelambd   
 lambda\_function.py

```
```text
Trigger configuration : S3
Bucket : awscapstonec3<name>blog
Event type : All object create events
Check the warning message and click add ---> sometime
it says overlapping situation. When it occurs, try
refresh page and create a new trigger or remove the s
3 event and recreate again. then again create a trigg
er for lambda function
```

```

## Add trigger

### Trigger configuration

S3

aws storage

**Bucket**

Please select the S3 bucket that serves as the event source. The bucket must be in the same region as the function.

Q |

awscapstones3serdarblog

cf-template awscapstones3serdarblog\_itral-1

cf-templates-5mfgdye7649f-sa-east-1

cf-templates-5mfgdye7649f-us-east-1

cf-templates-5mfgdye7649f-us-east-2

cf-templates-5mfgdye7649f-us-west-2

clarusway.broadcast.kc

clarusway.cors.broadcast.kc

clarusway.destination.lambda.osvaldo

clarusway.lambda.images

clarusway.lambda.images-resized

clarusway.source.lambda.osvaldo

djangoserdarr-encryption-service

Hata verebiliyor eger hata verir ise lamda function s una gidip silip tekarar Trigger edecegiz

**Function overview** Info

awscapstonelambdafunction

Layers (0)

S3

+ Add trigger

+ Add destination

Description -

Last modified 3 minutes ago

Function ARN arn:aws:lambda:us-east-1:046402772087:function:awscapstonelambdafunction

Code Test Monitor Configuration Aliases Versions

General configuration

**Triggers**

Triggers (1)

Find triggers

Trigger

S3: awscapstones3serdarblog

arn:aws:s3:::awscapstones3serdarblog

Details

Bucket: s3/awscapstones3serdarblog

Event type: ObjectCreated

Notification name: 511a6d64-9786-433c-9679-c63d5d0e78e9

Enable Disable Fix errors Delete Add trigger

- For defining trigger for **deleting objects**

```
```bash
Trigger configuration : S3
Bucket : awscapstonec3<name>blog
Event type : All object delete events
Check the warning message and click add ---> sometimes it says overlapping situation. When it occurs, try refresh page and create a new trigger or remove the old event and recreate again. then again create a trigger for lambda function
```

```

Lambda > Add trigger

## Add trigger

### Trigger configuration

**S3** aws storage

**Bucket**  
Please select the S3 bucket that serves as the event source. The bucket must be in the same region as the function.

awschapstones3ramazanblog

**Event type**  
Select the events that you want to have trigger the Lambda function. You can optionally set up a prefix or suffix for an event type. Each bucket, individual events cannot have multiple configurations with overlapping prefixes or suffixes that could match key.

All object delete events

**Prefix - optional**  
Enter a single optional prefix to limit the notifications to objects with keys that start with matching characters.  
e.g. images/

**Suffix - optional**  
Enter a single optional suffix to limit the notifications to objects with keys that end with matching characters.  
e.g. .jpg

Lambda will add the necessary permissions for Amazon S3 to invoke your Lambda function from this trigger. [more](#) about the Lambda permissions model.

**Amazon Lambda**   (0)

**S3** (2)

**+ Add trigger**

**Code** **Test** **Monitor** **Configuration** **Aliases** **Versions**

**General configuration**

**Triggers** **Triggers (2)**

- Trigger**
  - S3: awscapstones3ramazanblog**  
arn:aws:s3:::awscapstones3ramazanblog
  - Details**
- Event type: ObjectCreated**  
Notification name: 1bb5ca84-c62e-4364-ad36-9d4236166d6c
- S3: awscapstones3ramazanblog**  
arn:aws:s3:::awscapstones3ramazanblog
- Details**
- Bucket: s3:awscapstones3ramazanblog**  
Event type: ObjectRemoved  
Notification name: b667ef59-dac6-4385-9250-2700e1b637e0

- Go to the code part and select `lambda_function.py` -  
--> remove default code and paste a code on below. If you give DynamoDB a different name, please make sure to change it into the code.

```
```python
import json
import boto3
def lambda_handler(event, context):
    s3 = boto3.client("s3")

    if event:
        print("Event: ", event)
        filename = str(event['Records'][0]['s3']['object']['key'])
        timestamp = str(event['Records'][0]['eventTime'])
        event_name = str(event['Records'][0]['eventName']).split(':')[0][6:]

        filename1 = filename.split('/')
        filename2 = filename1[-1]

        dynamo_db = boto3.resource('dynamodb')
        dynamoTable = dynamo_db.Table('awscapstoneDynamo')

        dynamoTable.put_item(Item = {
            'id': filename2,
            'name': event_name,
            'timestamp': timestamp
        })
```

```

```

 'timestamp': timestamp,
 'Event': event_name,
 })
```
return "Lammda success"
```
- Click deploy and all set. go to the website and add a new post with photo, then control if their record is written on DynamoDB.
- WE ALL SET
- Congratulations!! You have finished your AWS Capstone Project

```

Amazon S3 > awscapstones3ramazanblog > media/ > blog/ > 1/

1/

**Objects (2)**

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in this bucket.

| <input type="checkbox"/> | Name                 | Type | Last modified            |
|--------------------------|----------------------|------|--------------------------|
| <input type="checkbox"/> | Calisma_ortamı.jpeg  | jpeg | August 27, 2021, 20:13:3 |
| <input type="checkbox"/> | Cloud_sistemleri.png | png  | August 28, 2021, 23:09:4 |

Clarusway Blog Home About

Post created succesfully!

## Clarusway Blog

**My Working Room**

hard working It

Posted 1 day, 2 hours ago.

**kaya**

The New Project is ...

Posted 0 minutes ago.

Yeni yukledigimiz nesnenin geldigini gorebiliyoruz