

ALTYAPI OLUŖTURMA

Proje: Çok bölgeye dağılan bir VPC altyapısı oluşturarak ölçeklenebilir ve güvenli bir uygulama dağıtımını sağlamak.

Proje Açıklaması: AWS Management Console kullanılarak çok bölgeye dağılmış bir VPC altyapısı oluşturulacak, EC2 örnekleri Auto Scaling grubuna eklenerek yük dengeleme sağlanacak ve güvenlik duvarı kuralları yapılandırılacak.

Projenin Temel Adımları:

AWS Cloudformation veya AWS Management Console kullanarak çok bölgeye yayılan bir Virtual Private Cloud (VPC) atyapısının oluşturulması.

Her bölge için Amazon EC2 instance oluşturulması ve bu instancelerin bir Auto Scaling grubuna eklenmesi.

Elastic Load Balancer (ELB) kullanarak trafik dağıtımının yapılandırılması ve güvenlik duvarı (Security Group) kurallarının yapılandırılması.

AWS Route 53 ile alan adı yönetiminin yapılandırılması ve trafik yönlendirilmesinin gerçekleştirilmesi.

Proje İçin Kullanılacak Amazon Hizmetleri

- **AWS Management Console**
- **Amazon EC2**
- **Auto Scaling**
- **Elastic Load Balancer (ELB)**
- **AWS Route 53**

AWS CloudFormation: Cloudformation: Şablon dosyası kullanarak, bir şirketin iç ağda yapabildikleri işlemleri cloudda yapmasına izin verir. Şirket içindeki kullanıcı yönetiminin sağlanması, veritabanlarını, sunucuları ve diğer kaynakları oluşturmasını sağlar. Kullanıcı izinleri, sunucu özellikleri (boyut, işletim sistemi, güvenlik ayarları vb.), veritabanı kaynaklarını oluşturmak için gerekli olan şablonları hazırlayıp cloudformationa yüklenerek, cloudformationın bu uygulamaları gerekli şekilde otomatik yapılandırılmasını, güncellenebilmesini ve yönetimini sağlar. İstenen şablon hazırlandıktan sonra zip halinde cloudformationa yüklenip ve cloudformation şablonunda istenilen özellikleri otomatik olarak oluşturulması sağlanır.

Örnek Cloudformation Şablonu:

Description: This template deploys a VPC, with a pair of public and private subnets spread across two Availability Zones. It deploys an internet gateway, with a default route on the public subnets. It deploys a pair of NAT gateways (one in each AZ), and default routes for them in the private subnets.

Parameters:

EnvironmentName:

Description: An environment name that is prefixed to resource names

Type: String

VpcCIDR:

Description: Please enter the IP range (CIDR notation) for this VPC

Type: String

Default: 10.192.0.0/16

PublicSubnet1CIDR:

Description: Please enter the IP range (CIDR notation) for the public subnet in the first Availability Zone

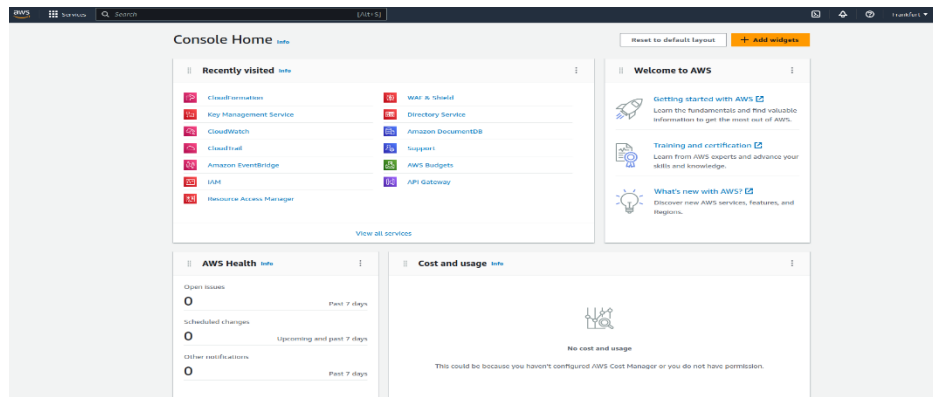
Type: String

Default: 10.192.10.0/24

Şablon, iki kullanılabilir bölgeye yayılmış bir çift public ve private subnet (alt ağ) içeren bir VPC oluşturur. Public subnetlerde varsayılan bir internet geçidi (internet gateway) ve ilgili route (yönlendirme) ayarları oluşturulur. Private subnetlerde ise her bir bölgede birer adet NAT geçidi (NAT gateway) oluşturulur ve bu geçitlerin ilgili route ayarları yapılır.

Bu kod parçacığı ayrıca, CloudFormation şablonu çalıştırılırken kullanıcıdan alınacak bazı parametreleri de tanımlar. “*EnvironmentName*” parametresi, kaynak isimlerine ön ek olarak eklenen bir ortam adını tanımlar. “*VpcCIDR*” parametresi ise VPC'nin IP aralığını (CIDR gösteriminde) belirler. “*PublicSubnet1CIDR*” parametresi ise ilk kullanılabilir bölgedeki public subnetin IP aralığını belirler.

AWS Management Console: AWS Management Console; Cloudformation gibi sunucu, veritabanı, kullanıcı yönetimi veya diğer kaynakların yönetimi (oluşturulması, güncellenmesi ve silinmesi gibi) işlemlerin GUI ile yapılabilirdiği, genel bir yönetim arayüzüdür. Cloudformation ve Management Console temel olarak aynı amaca hizmet eder: AWS hizmetlerini kolayca kullanılmasına olanak tanımak.



AWS Management Console

AWS Virtual Private Cloud Oluřturma

Virtual Private Cloud kullanıcıların; sanal aęlar, subnetler oluřturabilmesine, aę gvenlik ayarlarının oluřturulmasına, kısaca barındırılan kaynakların yapılandırılmasını ve gvenlięini kontrol altına almak iin oluřturulmuř bir kaynaktır.

VPC, ařaęıdaki bileřenlerden oluřmaktadır:

1. Subnetler:

- Public Subnetler: Her bir blgede birer adet public subnet bulunmaktadır. Public subnetler, internete doęrudan eriřim saęlamak iin kullanılır.
- Private Subnetler: Her bir blgede birer adet private subnet bulunmaktadır. Private subnetler, ierideki kaynakların gvenlięini saęlamak iin kullanılır ve internete doęrudan eriřime izin vermez.

2. Internet Gateway:

- VPC, varsayılan bir internet gateway kullanarak public subnetlerden internete eriřimi saęlar. Bu sayede, public subnetlerdeki kaynaklar internete ıkabilir ve dıřarıdan gelen isteklere cevap verebilir.

3. NAT Gateway:

- Her bir blgede birer adet NAT gateway bulunmaktadır. NAT gateway'ler, private subnetlerdeki kaynakların internete eriřmesini saęlar. Bu sayede, private subnetlerdeki kaynaklar gncellemeleri indirebilir, hizmetlere baęlanabilir ve dıřarıya ıkabilir. Ancak, dıřarıdan doęrudan eriřim almadıkları iin daha gvenli bir ortam sunarlar.

4. Route Ayarları:

- Public subnetler iin, varsayılan bir route oluřturulur ve internet gateway'e ynlendirilir. Bylece, public subnetlerdeki kaynaklar doęrudan internete eriřebilir.
- Private subnetler iin, NAT gateway'ler iin varsayılan route oluřturulur. Bu sayede, private subnetlerdeki kaynaklar internete NAT gateway zerinden eriřebilir.

Management Console zerinde arama kutucuęuna VPC yazılarak kaynaęa eriřim saęlanır. Dashboard sekmesinde sol stte bulunan **“Create VPC”** seeneęi seilerek yeni bir VPC oluřturmak iin ilk adım atılır.

VPC settings

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

☒ VPC only ☐ VPC and more

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

project-vpc-01

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

IPv4 CIDR
10.0.0.0/16

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

Tenancy [Info](#)
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	
Q Name	Q project-vpc-01	Remove

Add new tag

Tasarımda her bölge için farklı ayrı alt ağlar seçileceği için CIDR bloğu /16 olarak tanımlanmıştır. Subnetler bir şirketin alt ağlarıdır. Alt ağlarda; veritabanları, sunucular ve kullanıcılar gibi farklı kaynaklar barındırılabilir. VPC sekmesinden Subnet oluşturulabilir. Uygulamalar için /24, private subnet için için /24 ve public subnet için /24 lük IP adresleri tanımlanmıştır.

VPC

VPC ID
Create subnets in this VPC.

vpc-06018b626581b6fef (project-vpc-01) ▼

Associated VPC CIDRs

IPv4 CIDRs

10.0.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 3

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

Public Subnet

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.

Europe (Frankfurt) / eu-central-1a ▼

IPv4 CIDR block [Info](#)

Q 10.0.1.0/24 X

► Tags - optional

Remove

Subnet 2 of 3

Subnet name

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

Private Subnet

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.

Europe (Frankfurt) / eu-central-1a

IPv4 CIDR block [Info](#)

10.0.2.0/24

Tags - optional

Remove

Subnet 3 of 3

Subnet name

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

Application Subnet

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.

Europe (Frankfurt) / eu-central-1a

IPv4 CIDR block [Info](#)

10.0.3.0/24

Tags - optional

Remove

Add new subnet

Internet Gateway

Internet Gateway, VPC networklerinin internete bağlanmasını sağlayan Amazon Cloud hizmetidir. Uygulamaların dışarıdan bağlanması için internet gateway uygulama VPC'lerine bağlanması gerekmektedir.

VPC sekmesinde internet gateway seçilerek yeni bir internet gateway oluşturulur, oluşturulan gateway de "Actions" seçeneğinde "Attach to VPC" seçeneği seçilerek istenilen VPC sunucusu Internet Gateway'e bağlanılabilir.

Internet gateways (2) Info					
<input type="text" value="Filter internet gateways"/>					
<input type="checkbox"/>	Name	Internet gateway ID	State	VPC ID	Owner
<input type="checkbox"/>	-	igw-010368fba76e3c17f	Attached	vpc-0a0faa5cb52c06bba	120703883523
<input type="checkbox"/>	project-gateway	igw-0831d01bfd9b1dacd	Detached	-	120703883523

VPC > Internet gateways > Attach to VPC (igw-0831d01bfd9b1dacd)

Attach to VPC (igw-0831d01bfd9b1dacd) [Info](#)

VPC

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

Available VPCs

Attach the internet gateway to this VPC.

► AWS Command Line Interface command

Cancel

Attach internet gateway

Amazon Elastic Compute Cloud (EC2)

Amazon EC2 bulut ortamda sanal sunucular oluşturmaya imkan tanır. Bulutta güvenli yeniden boyutlandırılabilen işlem kapasitesi sağlar.

Amazon EC2 (Elastic Compute Cloud) aşağıdaki bileşenlerden oluşur:

1. Instance:

- EC2'nin temel bileşeni olan instance, sanal bir sunucudur. Bir instance, iş yüklerinizi barındırmak ve yönetmek için kullanabilen bir bilgisayardır. İşletim sistemine, kaynaklara ve yapılandırmaya sahip bir örnektir.

2. Amazon Machine Image (AMI):

- AMI'lar, instance'ların temelini oluşturan sanal makine görüntüleridir. Bir AMI, bir işletim sistemi, ön yüklü yazılımlar ve yapılandırmalar içerebilir.

3. Instance Türleri:

- EC2, farklı iş yükleri için çeşitli instance türleri sunar. Instance türleri, kaynakların (CPU, bellek, depolama vb.) boyutunu ve performans düzeyini belirler.

4. Security Groups (Güvenlik Grupları):

- EC2 instance'larınızın erişebileceği ağ kaynaklarını kontrol etmek için güvenlik grupları kullanılır. Güvenlik grupları, gelen ve giden trafiği belirli protokoller ve portlar üzerinden kontrol eder.

5. Elastic IP (Elastik IP):

- Elastik IP'ler, EC2 instance'larınıza kalıcı bir IP adresi sağlar. Normalde EC2 instance'lar, başladığında dinamik olarak atanan bir IP adresine sahiptir.

6. VPC (Virtual Private Cloud):

- VPC, EC2 instance'larınızı barındıracağınız özel bir sanal ağıdır. VPC, subnet'ler, route tabloları, ağ geçitleri, ağ ACL'leri ve diğer ağ bileşenlerini içerir.

7. EBS (Elastic Block Store):

- EBS, instance'larınız için blok depolama hizmetidir. EBS, verilerinizi kalıcı bir şekilde saklamanızı sağlar ve yüksek performanslı depolama seçenekleri sunar.

EC2 instance oluşturmak için uygun olanların seçilmesi gereklidir.

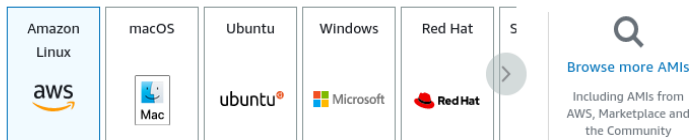
- Sunucu tipi (Amazon Linux – MacOS – Windows – Debian vb.)
- Instance Type: Örnekte seçilen t2.micro instance ı; t2 ailesine ait (t2 genel amaçlı kullanımı olan instance türüdür) ve micro işlemcileri içerir. Test/öğrenme ortamı için uygun olan türdür.
- Sunucunun kurulması için gerekli olan VPC'nin ve subnetin seçilmesi.
- Auto-Assigned Public IP: Dış ağdan erişilebilecek IP adresinin tanımlanması. Örnekte farklı Amazon dağıtımları kullanıcılarından ötürü Disable olarak seçilmiştir.
- Uygulamaya SSH ile bağlantı sağlamak için key pair oluşturulmuştur.

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

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

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

Quick Start



Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type Free tier eligible
ami-004359656ecac6a95 (64-bit (x86)) / ami-05ea2a56f1a083824 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2 Kernel 5.10 AMI 2.0.20230504.1 x86_64 HVM gp2

Architecture

64-bit (x86)

AMI ID

ami-004359656ecac6a95

Verified provider

▼ **Instance type** [Info](#)

Instance type

t2.micro

Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows pricing: 0.018 USD per Hour
On-Demand Linux pricing: 0.0134 USD per Hour
On-Demand SUSE pricing: 0.0134 USD per Hour

All generations

[Compare instance types](#)

▼ **Key pair (login)** [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

EmployeeApp



[Create new key pair](#)

▼ Network settings [Info](#)

VPC - *required* [Info](#)

vpc-0a0faa5cb52c06bba (default) 

Subnet [Info](#)

Select  [Create new subnet](#) 

Auto-assign public IP [Info](#)

Select ▼

Firewall (security groups) [Info](#)

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

☒ Create security group

☐ Select existing security group

Security group name - *required*

launch-wizard-5

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&,{}!\$*

Description - *required* [Info](#)

launch-wizard-5 created 2023-05-19T20:10:39.486Z

Inbound security groups rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0)

Remove

Type [Info](#)

ssh ▼

Protocol [Info](#)

TCP

Port range [Info](#)

22

Source type [Info](#)

Anywhere ▼

Source [Info](#)

 Add CIDR, prefix list or security

0.0.0.0/0 

Description - *optional* [Info](#)

e.g. SSH for admin desktop

▼ Security group rule 2 (TCP, 80, 0.0.0.0/0)

Remove

Type [Info](#)

HTTP ▼

Protocol [Info](#)

TCP

Port range [Info](#)


80

Source type [Info](#)

Anywhere ▼

Source [Info](#)

 Add CIDR, prefix list or security

0.0.0.0/0 

Description - *optional* [Info](#)

e.g. SSH for admin desktop

▼ Security group rule 3 (TCP, 443, 0.0.0.0/0)

Remove

Type [Info](#)

HTTPS ▼

Protocol [Info](#)

TCP

Port range [Info](#)

443

Source type [Info](#)

Anywhere ▼



Source [Info](#)

 Add CIDR, prefix list or security

0.0.0.0/0 

Description - *optional* [Info](#)

e.g. SSH for admin desktop

 Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only. 

Add security group rule

Allocate Elastic IP address [Info](#)

Elastic IP address settings [Info](#)

Network Border Group [Info](#)

Q eu-central-1 X

Public IPv4 address pool

- ☒ Amazon's pool of IPv4 addresses
- ☐ Public IPv4 address that you bring to your AWS account (option disabled because no pools found) [Learn more](#)
- ☐ Customer owned pool of IPv4 addresses (option disabled because no customer owned pools found) [Learn more](#)

Global static IP addresses

AWS Global Accelerator can provide global static IP addresses that are announced worldwide using anycast from AWS edge locations. This can help improve the availability and latency for your user traffic by using the Amazon global network. [Learn more](#)

Create accelerator [↗](#)

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.

No tags associated with the resource.

Add new tag

You can add up to 50 more tag

Cancel **Allocate**

Allocate seçildikten sonra Amazon public IP atamasını gerçekleştir. Oluşturulan Elastic IP adres seçeneğinde Actions seçeneği altında bulunan “Associate Elastic IP address” seçeneği seçilir. İstenen uygulama instance’ı için instance seçilir ve public IP adresinin uygulama instance’ına ataması yapılabilir.

Associate Elastic IP address [Info](#)

Choose the Instance or network Interface to associate to this Elastic IP address (3.69.247.100)

Elastic IP address: 3.69.247.100

Resource type

Choose the type of resource with which to associate the Elastic IP address.

- ☒ Instance
- ☐ Network Interface

⚠ If you associate an Elastic IP address with an instance that already has an Elastic IP address associated, the previously associated Elastic IP address will be disassociated, but the address will still be allocated to your account. [Learn more](#)

If no private IP address is specified, the Elastic IP address will be associated with the primary private IP address.

Instance

Q I-0c753b31322a66e89 X [↻](#)

Private IP address

The private IP address with which to associate the Elastic IP address.

Q 10.0.1.218 X

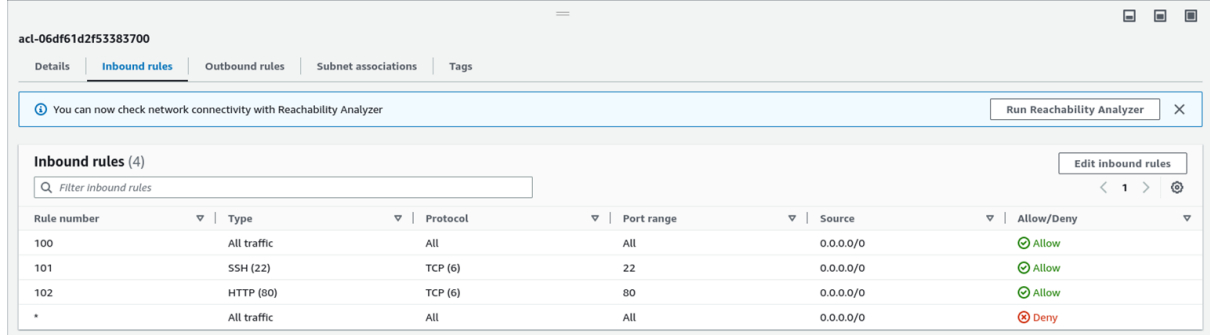
Reassociation

Specify whether the Elastic IP address can be reassociated with a different resource if it already associated with a resource.

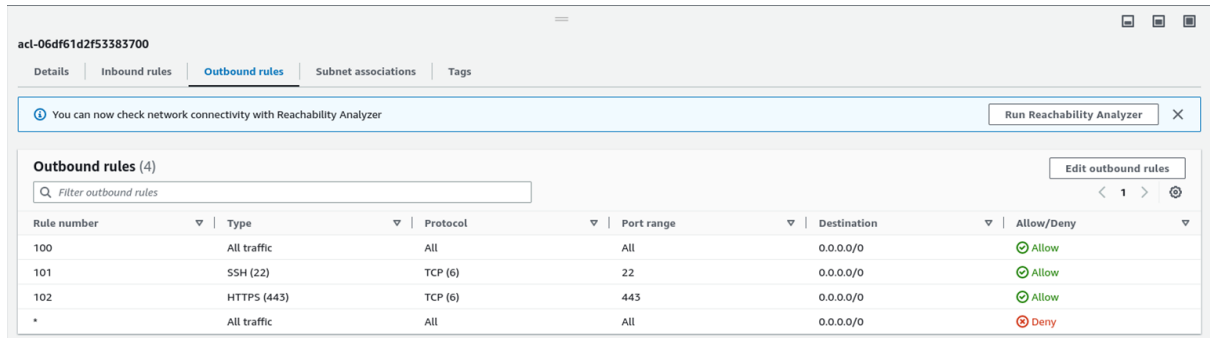
☒ Allow this Elastic IP address to be reassociated

Cancel **Associate**

Yapılan işlemler uygulandığı zaman SSH veya HTTP portlarına bağlantı sağlanamaz. Çünkü Network ACL (Access Control Lists) giden gelen bütün trafiği internete kapalı şekilde default olarak eklenir. Network ACL gelen istek ve giden yanıt, ağ trafiğini yönetmek için kullanılan güvenlik mekanizmasıdır. Network ACL sekmesinde Inbound ve Outbound kurallarına SSH ve HTTP kurallarının eklenmesi gerekmektedir.

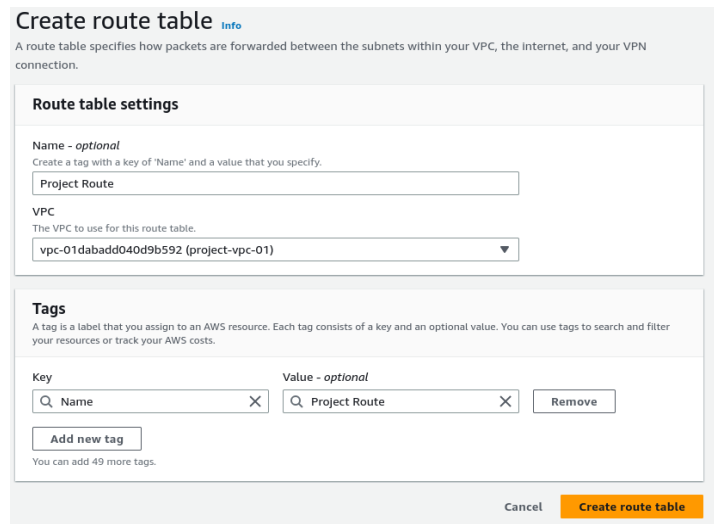


Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
101	SSH (22)	TCP (6)	22	0.0.0.0/0	Allow
102	HTTP (80)	TCP (6)	80	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny



Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
101	SSH (22)	TCP (6)	22	0.0.0.0/0	Allow
102	HTTPS (443)	TCP (6)	443	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Ardından istenilen VPC için Route tablosu eklenmelidir. Route tablosu internet üzerinden erişim için internet gateway'e izin verecektir. VPC için route tablosu oluşturduktan sonra edit route seçeneği seçilerek internet gateway için route oluşturulmalıdır. Destination parametresinin 0.0.0.0/0 olması internet üzerinden tüm IP adreslerinden hedefe erişim izni sağlanacağını temsil eder.



Create route table

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

Route table settings

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

VPC
The VPC to use for this route table.
vpc-01dabadd040d9b592 (project-vpc-01)

Tags

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

Key
Name

Value - optional
Project Route

Remove

Add new tag

You can add 49 more tags.

Cancel Create route table




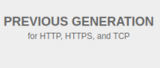
İşlemler tamamlandıktan sonra SSH ile IP adresine bağlantı sağlanabilir. Gerekli yapılandırmalar yapıldıktan sonra HTTP servisi ile HTTP portuna bağlantı gerçekleştirilir.

Amazon Elastic Load Balancer (ELB)

Amazon ELB gelen yüksek trafiği EC2 instanceleri arasında dağıtarak her bir instance'e eşit şekilde trafik gitmesini sağlayan bir yük dengeleyici hizmettir. Elastic Load Balancer; ölçeklenebilir bir performans sunarak uygulamaların otomatik olarak servislerinin azaltılması veya artırılmasını, kesintiye uğrayan bir servisin trafiğinin farklı olan sağlıklı servislere aktarılmasını ve daha birçok olumlu yönleri vardır. Elastic Load Balancer eklemek için EC2 içerisinde bulunan Load Balancers seçeneği seçildikten sonra create load balancer seçeneği seçilir. Uygulama HTTP ve HTTPS servislerini kullandığı için "Application Load Balancer" seçilerek işlemlere devam edilir.

Select load balancer type

Elastic Load Balancing supports four types of load balancers: Application Load Balancers, Network Load Balancers, Gateway Load Balancers, and Classic Load Balancers. Choose the load balancer type that meets your needs. [Learn more about which load balancer is right for you](#)

Application Load Balancer	Network Load Balancer	Gateway Load Balancer	Classic Load Balancer
 Create	 Create	 Create	 Create
<p>Choose an Application Load Balancer when you need a flexible feature set for your web applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers.</p> Learn more >	<p>Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your application. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.</p> Learn more >	<p>Choose a Gateway Load Balancer when you need to deploy and manage a fleet of third-party virtual appliances that support GENEVE. These appliances enable you to improve security, compliance, and policy controls.</p> Learn more >	<p>Choose a Classic Load Balancer when you have an existing application running in the EC2-Classical network.</p> Learn more >

Bu işlemlerde önce farklı bir Availability Zone için subnet eklenmesi gereklidir. Çünkü Load Balancer gelen isteği farklı availability zonelerde dağıtmayı gerektirecektir. Load balancer içerisinde bulunan gerekli alanlar doldurulur. Schema, uygulamaya dış ağdan mı erişilecek yoksa iç ağda mı olacağını temsil eder. Proje üzerinde dış ağdan erişilecek uygulama kullanılacağı için internet-facing seçeneği seçilmiştir. Gerekli alanlar seçildikten sonra altta bulunan Global Accelerator seçeneği aktif edilir. AWS Global Accelerator, trafik yönlendirmesini optimize etmek ve uygulamalarınıza gelen talepleri en yakın AWS kenar konumuna yönlendirmek için küresel ağ altyapısını kullanır.

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

Step 1: Configure Load Balancer

Basic Configuration

To configure your load balancer, provide a name, select a scheme, specify one or more listeners, and select a network. The default configuration is an internet-facing load balancer in the selected network with a listener that receives HTTP traffic on port 80.

Name (i) Application-Load-Balancer

Scheme (i) ☒ Internet-facing ☐ Internal

IP address type (i)

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

[Add listener](#)

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. You can specify only one subnet per Availability Zone. You must specify subnets from at least two Availability Zones to increase the availability of your load balancer.

VPC (i) vpc-01dabadd0409f5902 (10.0.0.0/16) | project-vpc-01

Availability Zones	Subnet	IPv4 address	Assigned by
<input checked="" type="checkbox"/> eu-central-1a	subnet-0f6db1348b1887e80 (Application Subnet)		Assigned by AWS
<input checked="" type="checkbox"/> eu-central-1c	subnet-067c2377c555b8bfa (Application Subnet 0-2)		Assigned by AWS

[Cancel](#) [Next: Configure Security Settings](#)

Configure Security Groups sayfasında uygulama için hazırlanan security group seçilerek devam edilir. "Configure Routing" (Yönlendirmeyi Yapılandır) sayfasında "Create a new target group" (Yeni bir hedef grubu oluştur) seçeneğini seçin ve hedef gruplarını yapılandırın.

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

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 edit or add listeners after the load balancer is created.

Target group

Target group ⓘ New target group ▾

Name ⓘ Application Group

Target type

☒ Instance

☐ IP

☐ Lambda function

Protocol ⓘ HTTP ▾

Port ⓘ 80

Protocol version ⓘ ☒ HTTP1

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 ▾

Path ⓘ /

➤ Advanced health check settings

Sayfa içerisinde bulunan target type hedefin türünü temsil eder. Instance: EC2 örnekleri hedef olarak belirlenebilir. Bu durumda, ALB trafiği belirtilen EC2 örneklerine dağıtır. IP Address: Belirli IP adreslerini hedef olarak belirleyebilirsiniz. ALB, belirtilen IP adreslerine trafiği yönlendirir. Lambda Function: Serverless işlevler (Lambda fonksiyonları) hedef olarak belirlenebilir. Bu durumda, ALB, gelen istekleri belirtilen Lambda fonksiyonlarına iletebilir.

"Register Targets" sayfasında yük dengeleyiciye yönlendirilecek EC2 instanceları seçilir ve kaydedilir.

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

Step 5: Register Targets

Register targets with your target group. If you register a target in an enabled Availability Zone, the load balancer starts routing requests to the targets as soon as the registration process completes and the target passes the initial health checks.

Registered targets

To deregister instances, select one or more registered instances and then click Remove.

Remove

<input type="checkbox"/>	Instance	Name	Port	State	Security groups	Zone
<input checked="" type="checkbox"/>	i-0c75b31322a66e89	Employee Application	80	running	launch-wizard-5	eu-central-1a

Instances

To register additional instances, select one or more running instances, specify a port, and then click Add. The default port is the port specified for the target group. If the instance is already registered on the specified port, you must specify a different port.

Add to registered on port 80

Search instances X

<input type="checkbox"/>	Instance	Name	State	Security groups	Zone	Subnet ID	Subnet CIDR
<input checked="" type="checkbox"/>	i-0c75b31322a66e89	Employee Application	running	launch-wizard-5	eu-central-1a	subnet-0cda3440704ebd9a	10.0.1.0/24