**ALTYAPI OLUŞTURMA**

**Proje:** Çok bölgeye dağılan bir VPC altyapısı oluşturarak ölçeklenebilir ve güvenli bir uygulama dağıtımı 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 şablonda 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*

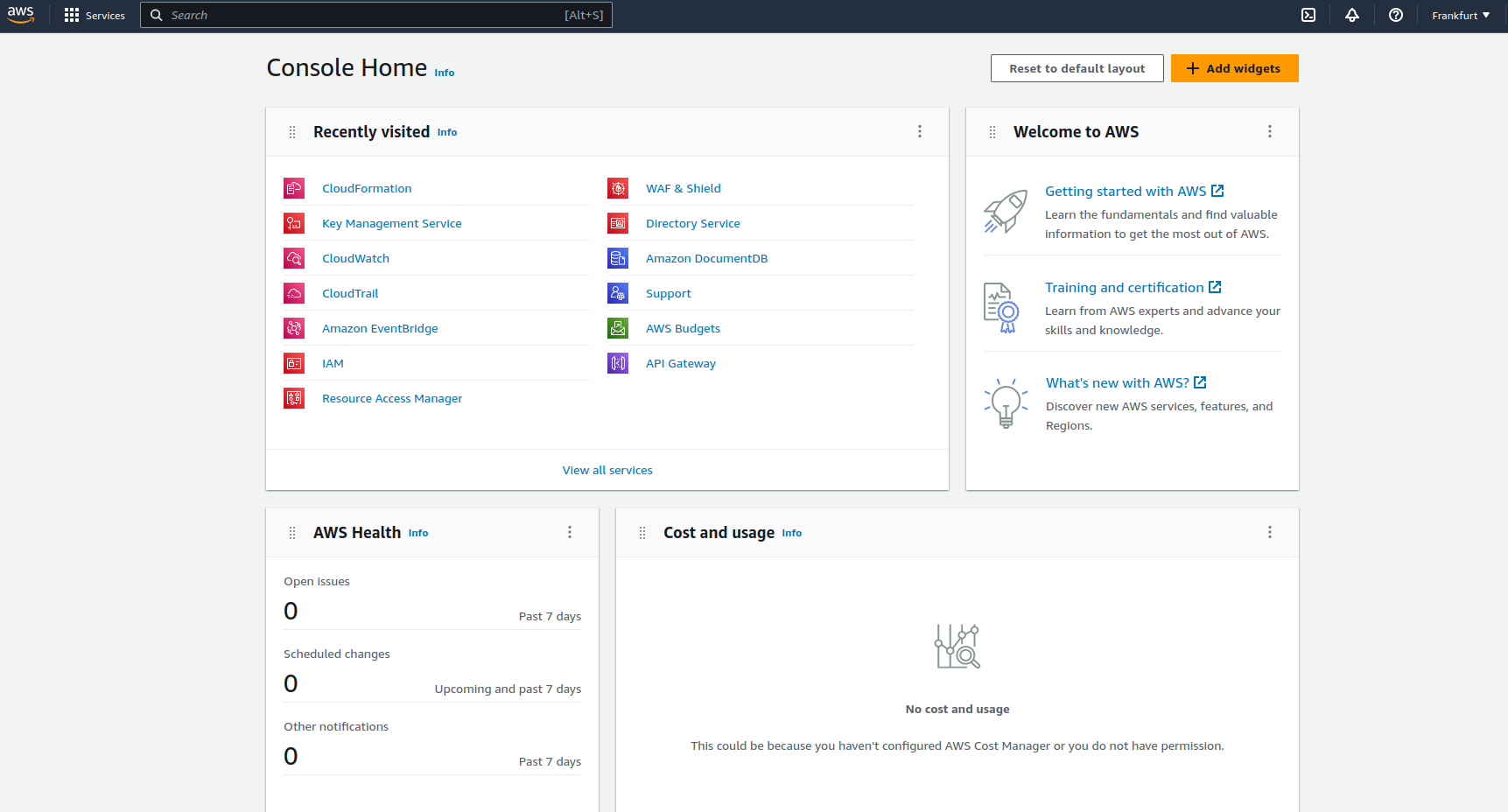
*Type: String*

*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 yapılabildiği, genel bir yönetim arayüzüdür. Cloudformation ve Management Console temel olarak aynı amaca hizmet eder: AWS hizmetlerini kolayca kullanılmasına olanak tanımak.

**AWS Management Console**

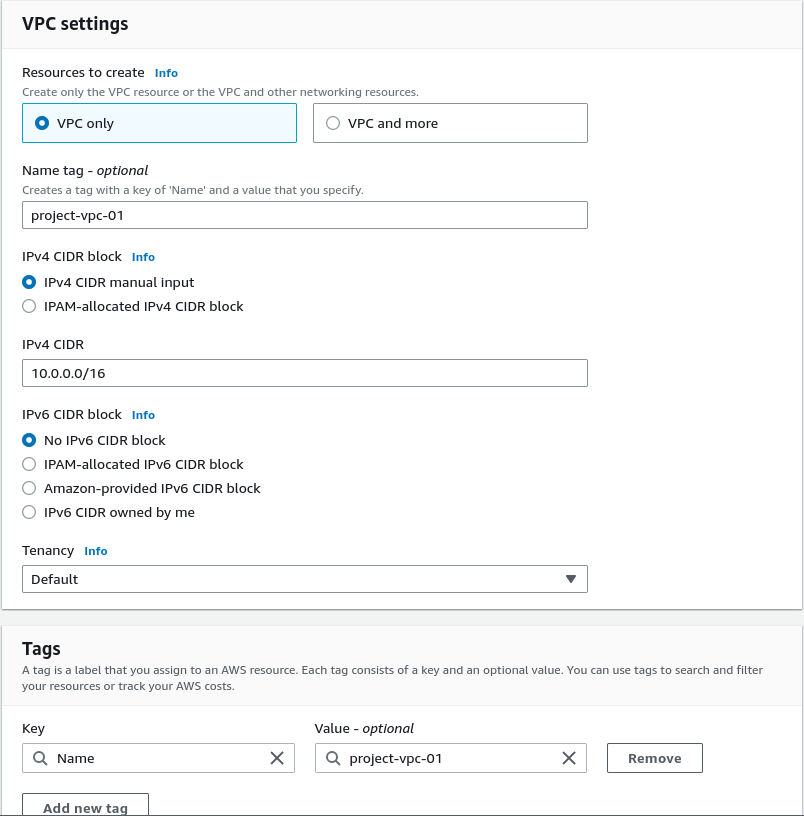
**AWS Virtual Private Cloud Oluşturma**

Virtual Private Cloud kullanıcıların; sanal ağlar, subnetler oluşturabilmesine, ağ güvenlik ayarlarının oluşturulmasına, kısaca barındırılan kaynakların yapılandırılmasını ve güvenliğini kontrol altına almak için oluşturulmuş bir kaynaktır.

VPC, aşağıdaki bileşenlerden oluşmaktadır:

1. Subnetler:
   * Public Subnetler: Her bir bölgede birer adet public subnet bulunmaktadır. Public subnetler, internete doğrudan erişim sağlamak için kullanılır.
   * Private Subnetler: Her bir bölgede birer adet private subnet bulunmaktadır. Private subnetler, içerideki kaynakların güvenliğini sağlamak için kullanılır ve internete doğrudan erişime izin vermez.
2. Internet Gateway:
   * VPC, varsayılan bir internet gateway kullanarak public subnetlerden internete erişimi sağlar. Bu sayede, public subnetlerdeki kaynaklar internete çıkabilir ve dışarıdan gelen isteklere cevap verebilir.
3. NAT Gateway:
   * Her bir bölgede birer adet NAT gateway bulunmaktadır. NAT gateway'ler, private subnetlerdeki kaynakların internete erişmesini sağlar. Bu sayede, private subnetlerdeki kaynaklar güncellemeleri indirebilir, hizmetlere bağlanabilir ve dışarıya çıkabilir. Ancak, dışarıdan doğrudan erişim almadıkları için daha güvenli bir ortam sunarlar.
4. Route Ayarları:
   * Public subnetler için, varsayılan bir route oluşturulur ve internet gateway'e yönlendirilir. Böylece, public subnetlerdeki kaynaklar doğrudan internete erişebilir.
   * Private subnetler için, NAT gateway'ler için varsayılan route oluşturulur. Bu sayede, private subnetlerdeki kaynaklar internete NAT gateway üzerinden erişebilir.

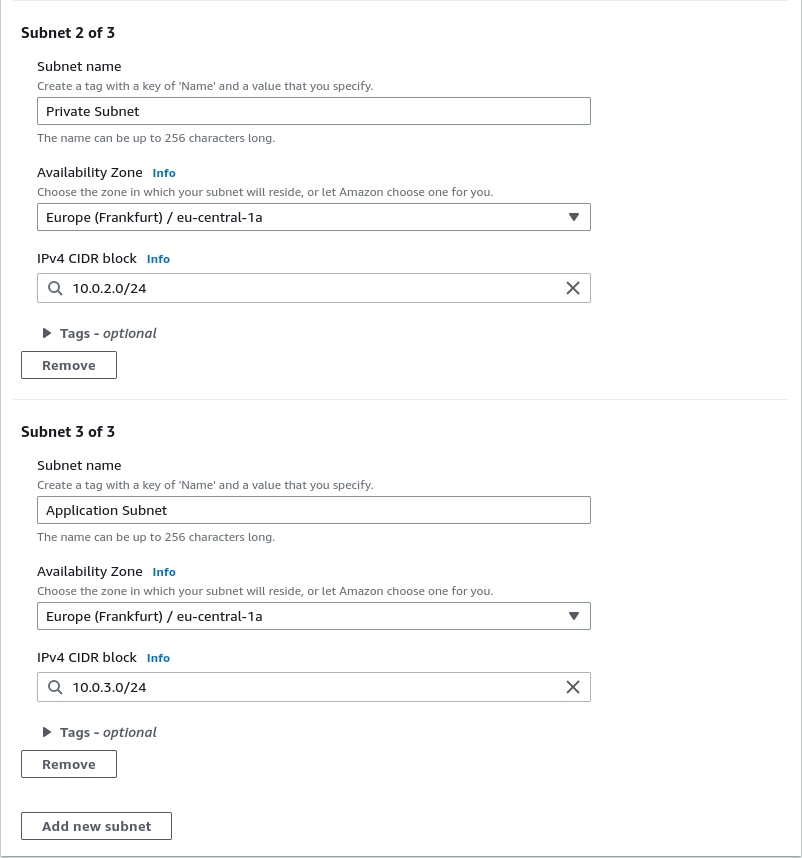
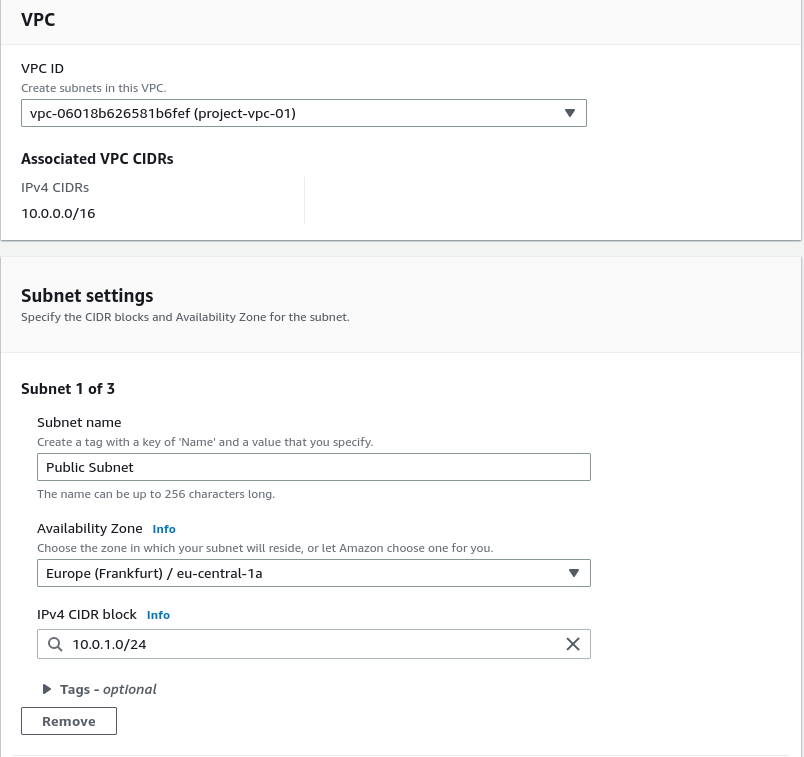
Management Console üzerinde arama kutucuğuna VPC yazılarak kaynağa erişim sağlanır. Dashboard sekmesinde sol üstte bulunan “***Create VPC***” seçeneği seçilerek yeni bir VPC oluşturmak için ilk adım atılır.



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.

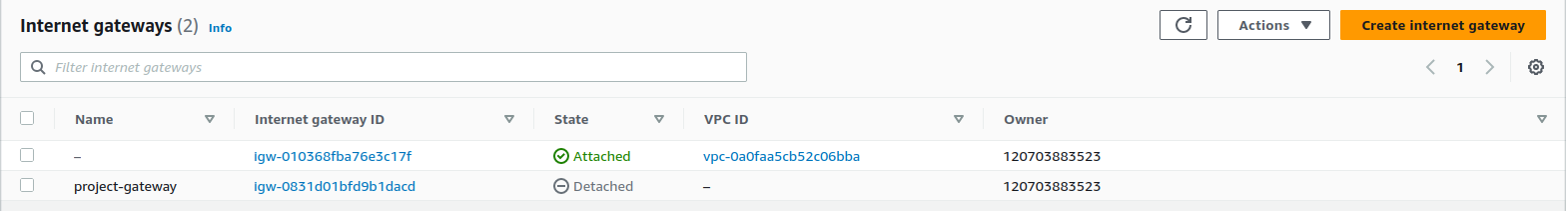
VPC sekmesinden Subnet oluşturulabilir. Uygulamalar için /24, private subnet için için /24 ve public subnet için /24 lük IP adresleri tanımlanmıştır.

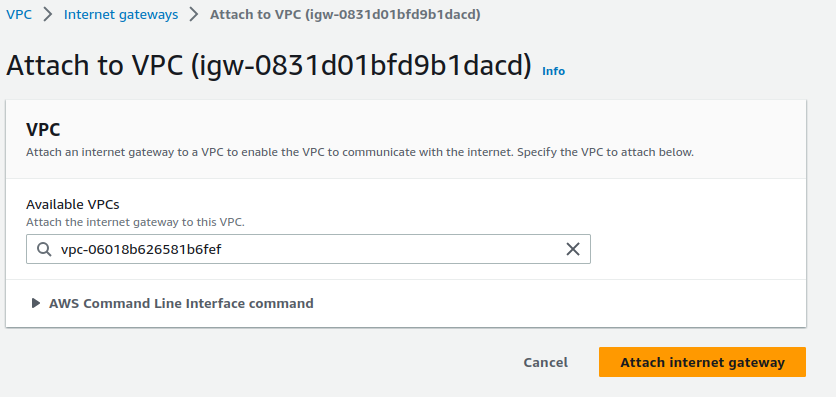
****

**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.



****

**Amazon Elastic Compute Cloud (EC2)**

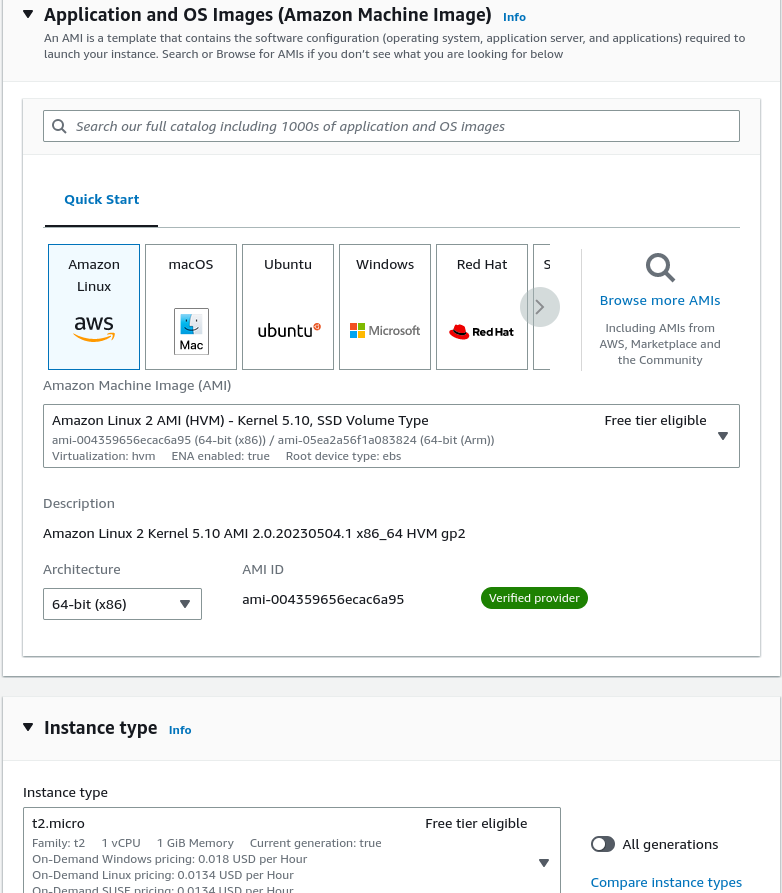
Amazon EC2 bulut ortamda sanal sunucular oluşturmaya imkan tanır. Bulutta güvenli yeniden boyutlandırılabilen işlem kapasitesi sağlar.

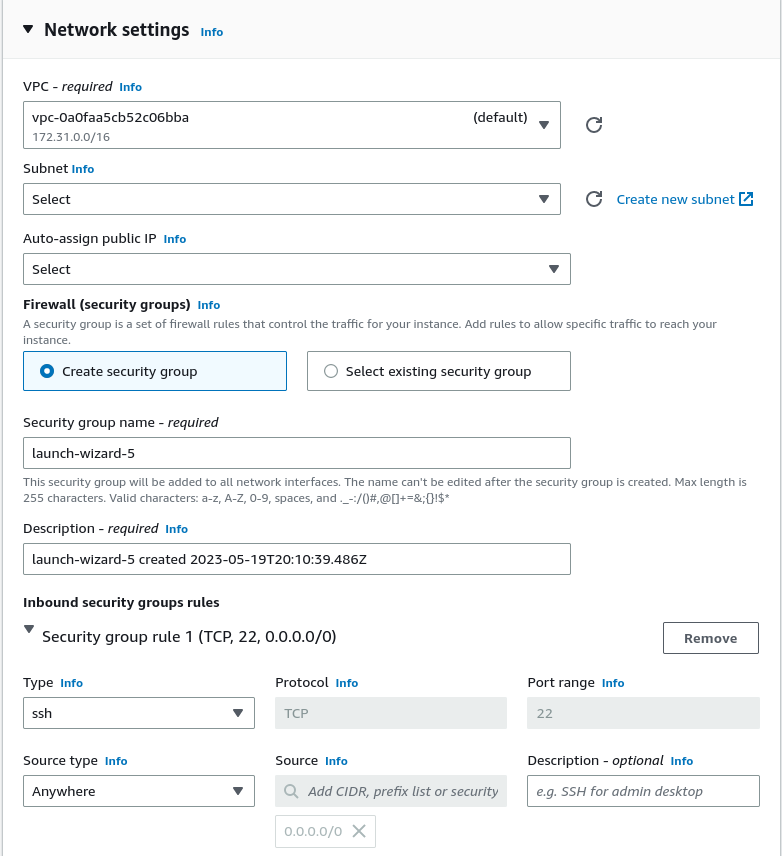
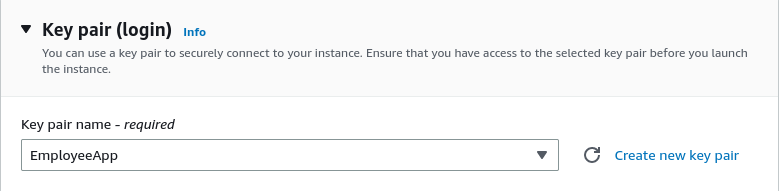
**Amazon EC2 (Elastic Compute Cloud) aşağıdaki bileşenlerden oluşur:**

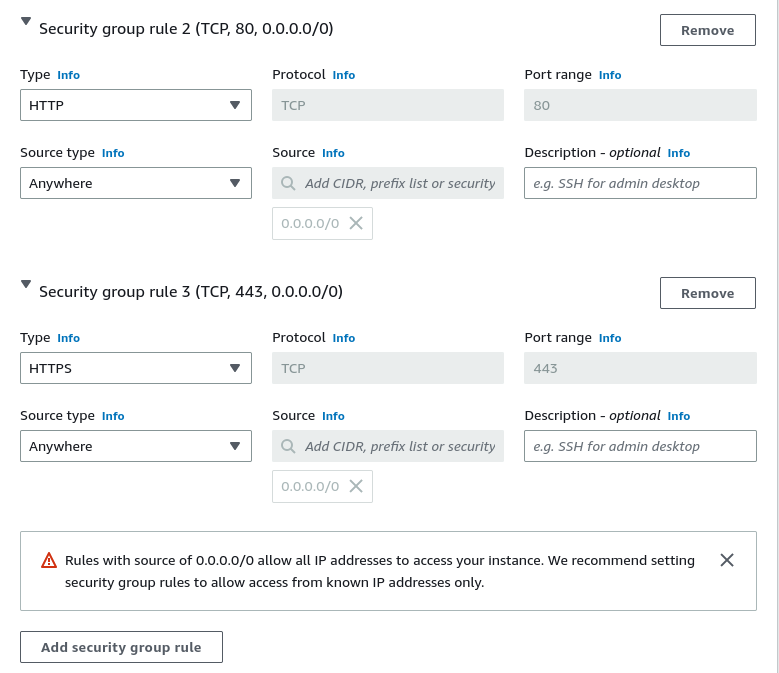
1. Instance:
   * EC2'nin temel bileşeni olan instance, sanal bir sunucudur. Bir instance, iş yüklerinizi barındırmak ve yönetmek için kullanabilen bir bilgisayardır. İşletim sistemine, kaynaklara ve yapılandırmaya sahip bir örnektir.
2. Amazon Machine Image (AMI):
   * AMI'lar, instance'ların temelini 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 ağdır. VPC, subnet'ler, route tabloları, ağ 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.

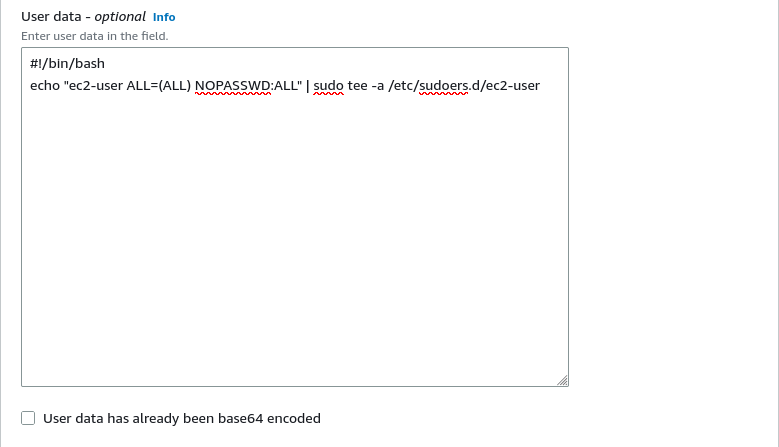
EC2 instance oluşturmak için uygun olanların seçilmesi gereklidir.

* 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 kullanıcılağından ötürü Disable olarak seçilmiştir.
* Uygulamaya SSH ile bağlantı sağlamak için key pair oluşturulmuştur.





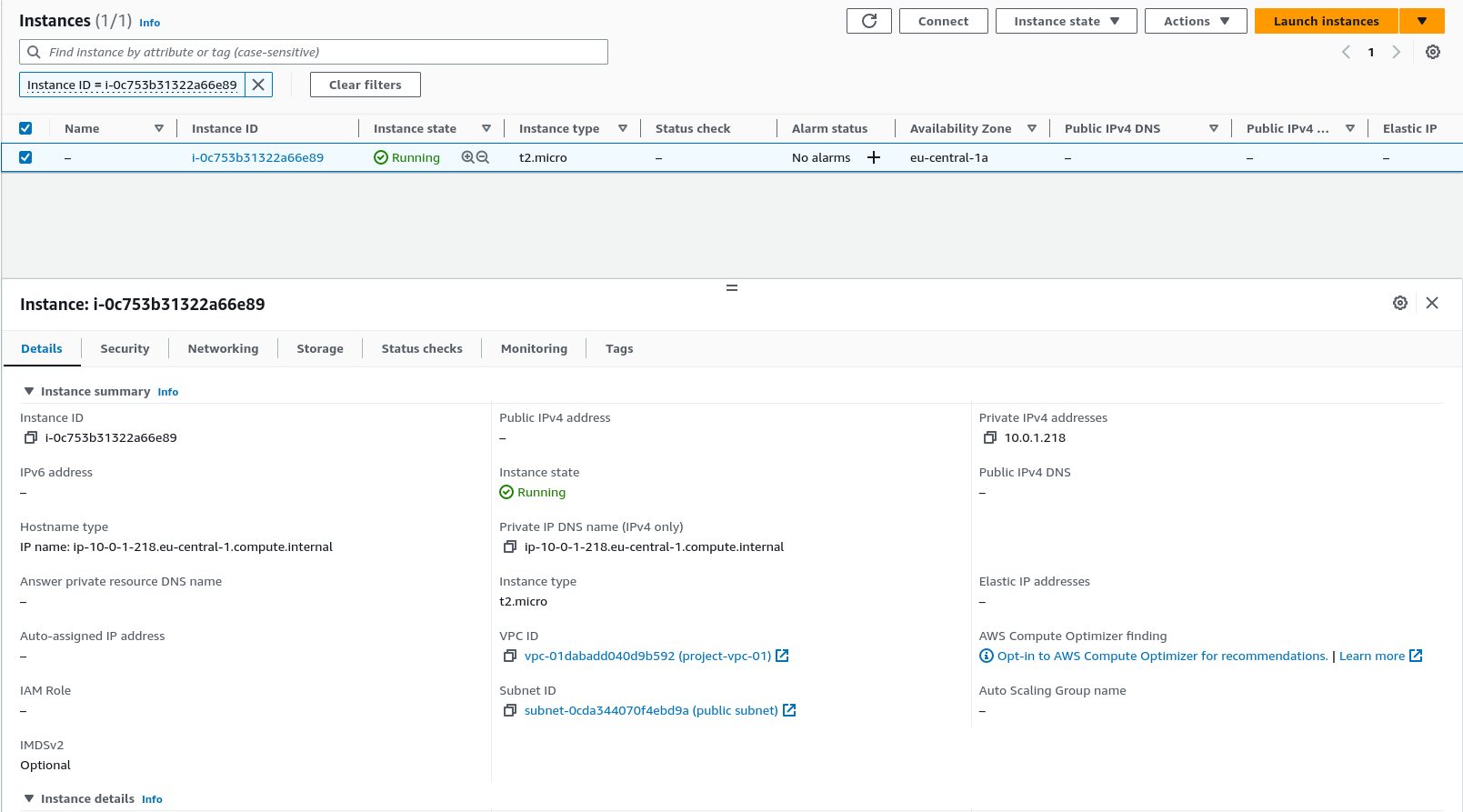
****

****

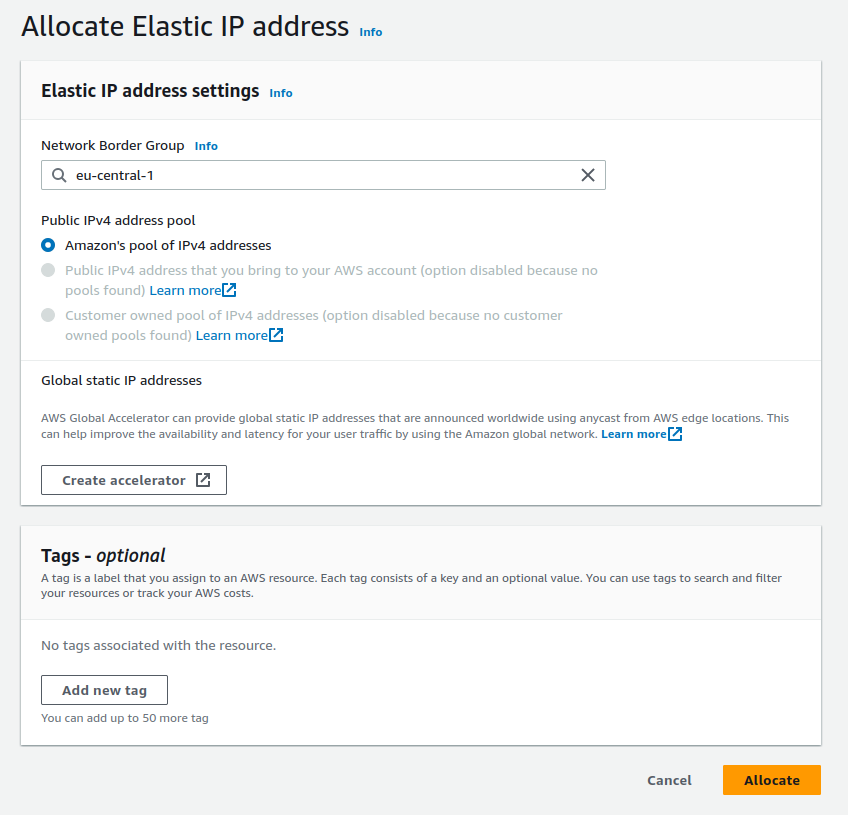
**Uygulama içerisine Yazılacak Kod Satırı**

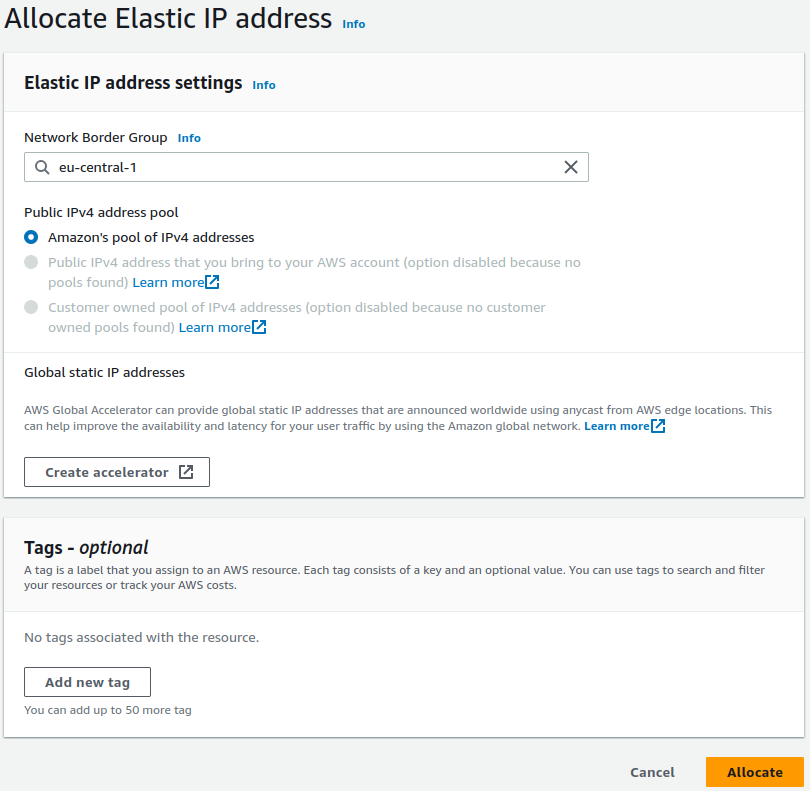
*#!/bin/bash echo "ec2-user ALL=(ALL) NOPASSWD:ALL" | sudo tee -a /etc/sudoers.d/ec2-user*

Bu komut ssh ile bağlantıda bütün kullanıcılar için parola istemeksizin sadece key pair ile girişi sağlamaya izin verir ve ec2-user için root yetkilerinin yapılandırılmasına olanak sağlar.

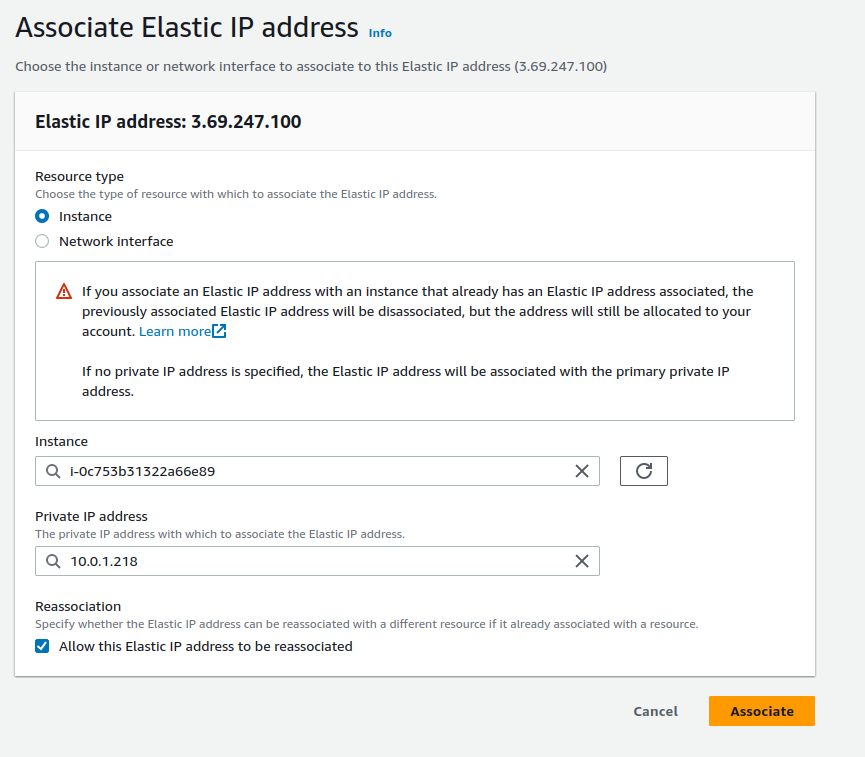


Göründüğü üzere instance’e herhangi bir public IP adresi atanmamış. Public IP adresi tanımlaması yapmak için yeni bir Elastic IP adresi oluşturulması gerekmektedir.

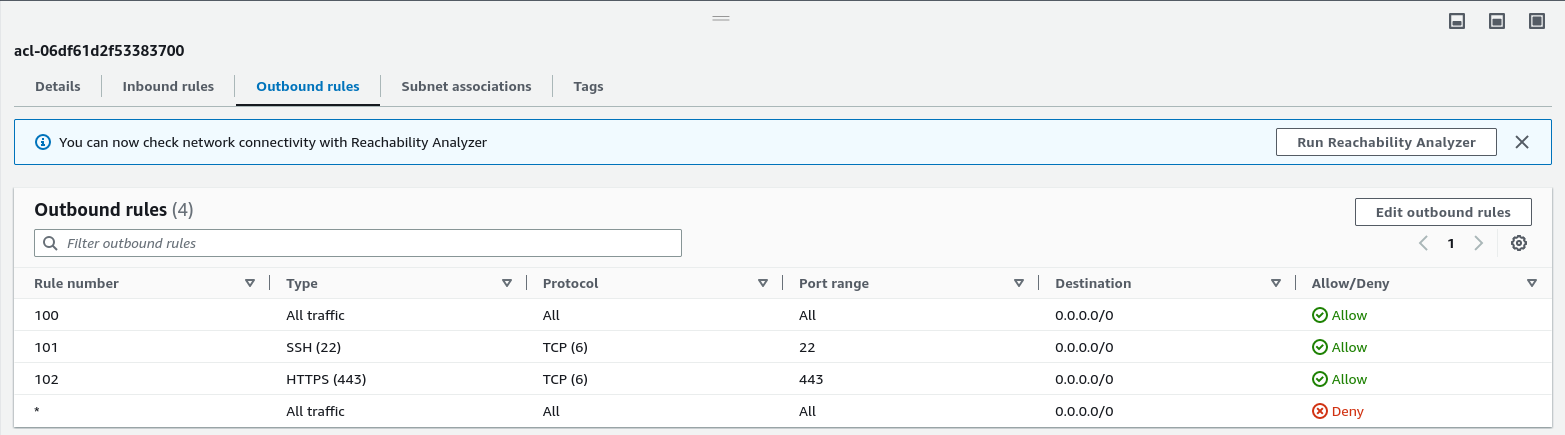
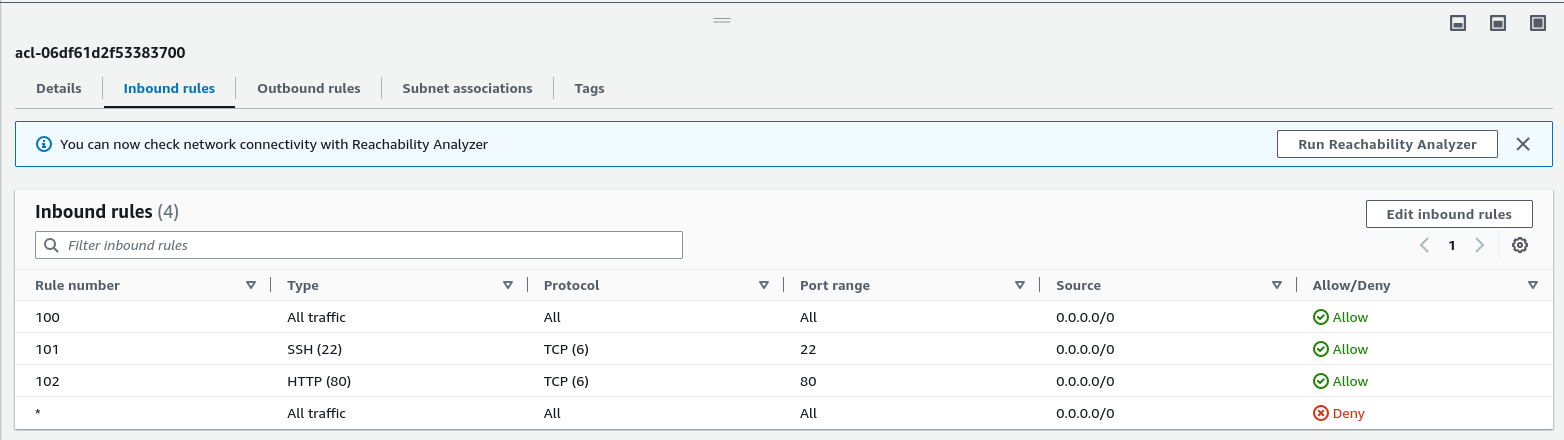




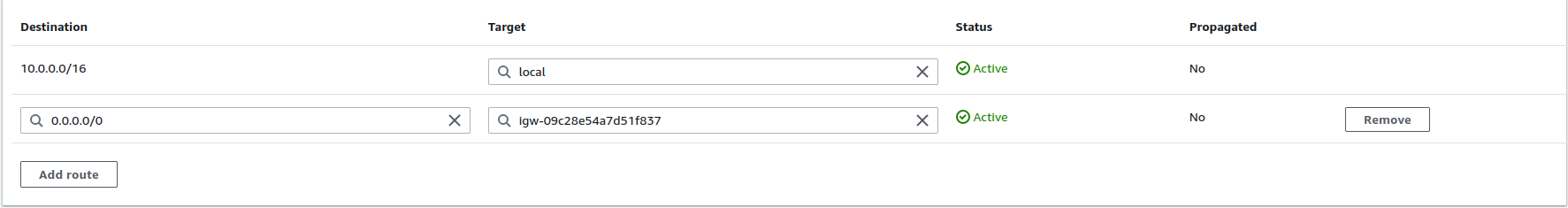
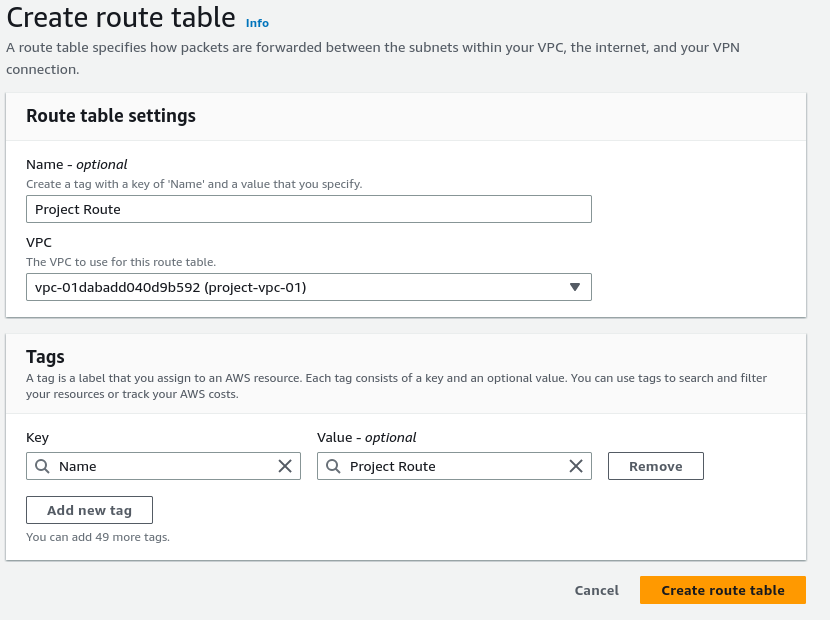
Allocate seçildikten sonra Amazon public IP atamasını gerçekleştirir. Oluşturulan Elastic IP adress seçeneğinde Actions seçeneği altında bulunan “*Associate* [*Elastic IP address*](https://eu-central-1.console.aws.amazon.com/ec2/home?region=eu-central-1)” seçeneği seçilir. İstenen uygulama instance’ı için instance seçilir ve public IP adresinin uygulama instance’ına ataması yapılabilir.



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.



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.

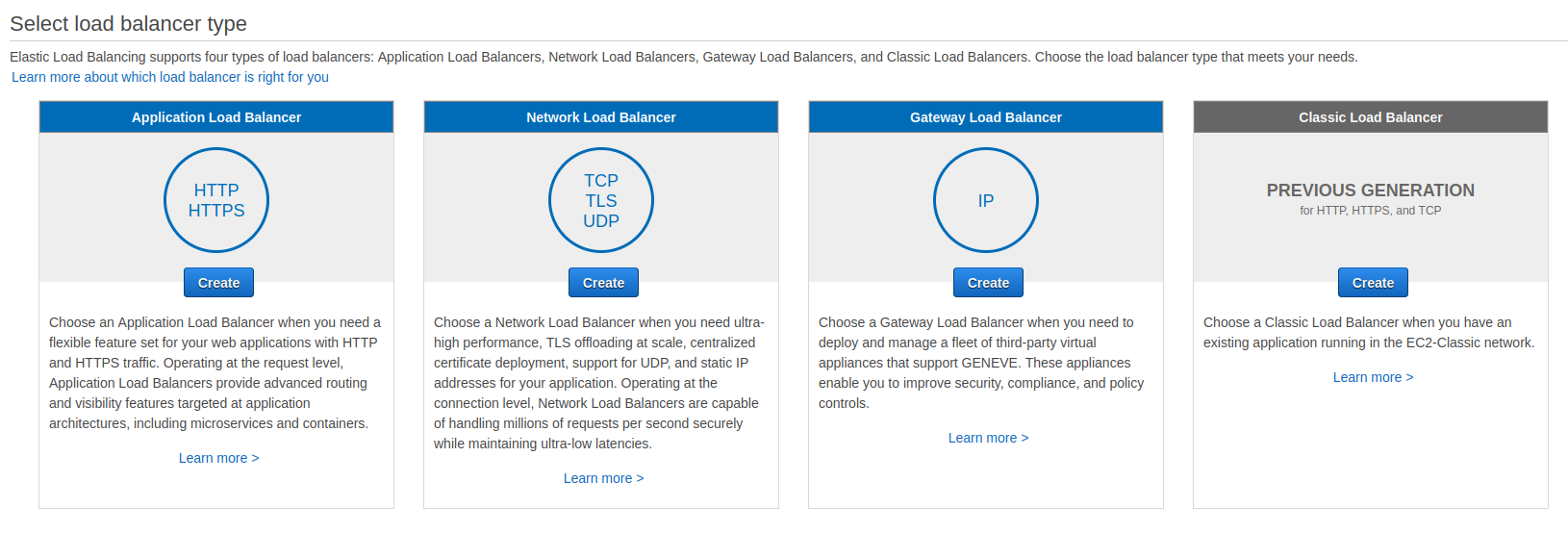


İşlemler tamamlandıktan sonra SSH ile IP adresine bağlantı sağlanabilir. Gerekli yapılandırmalar yapıldıktan sonra HTTP servisi ile HTTP portuna bağlantı gerçekleştirilir.

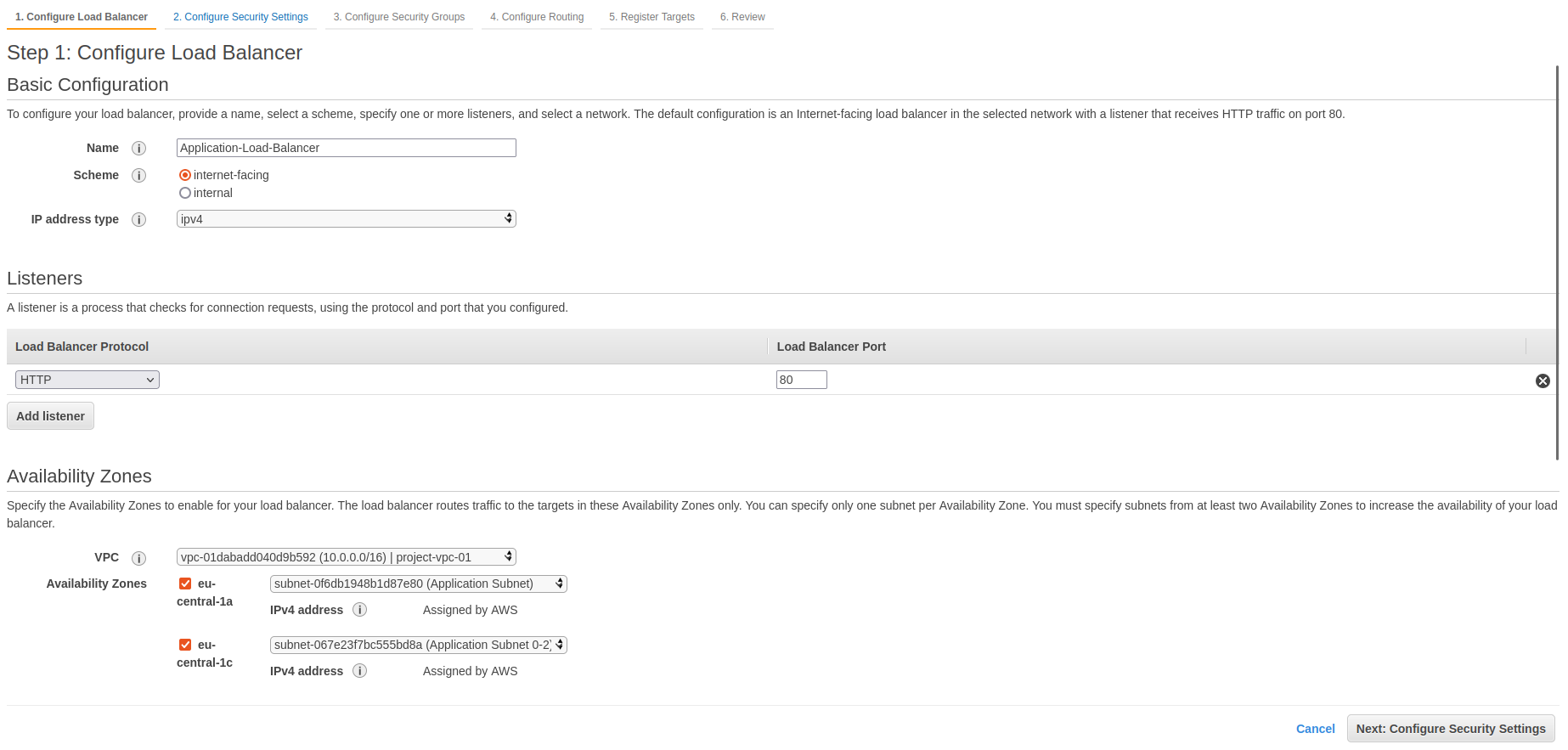
**Amazon Elastic Load Balancer (ELB)**

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 arttırılmasını, kesintiye uğrayan bir servisin trafiğinin farklı olan sağlıklı servislere aktarılmasını ve daha bir çok olumlu yönleri vardır.

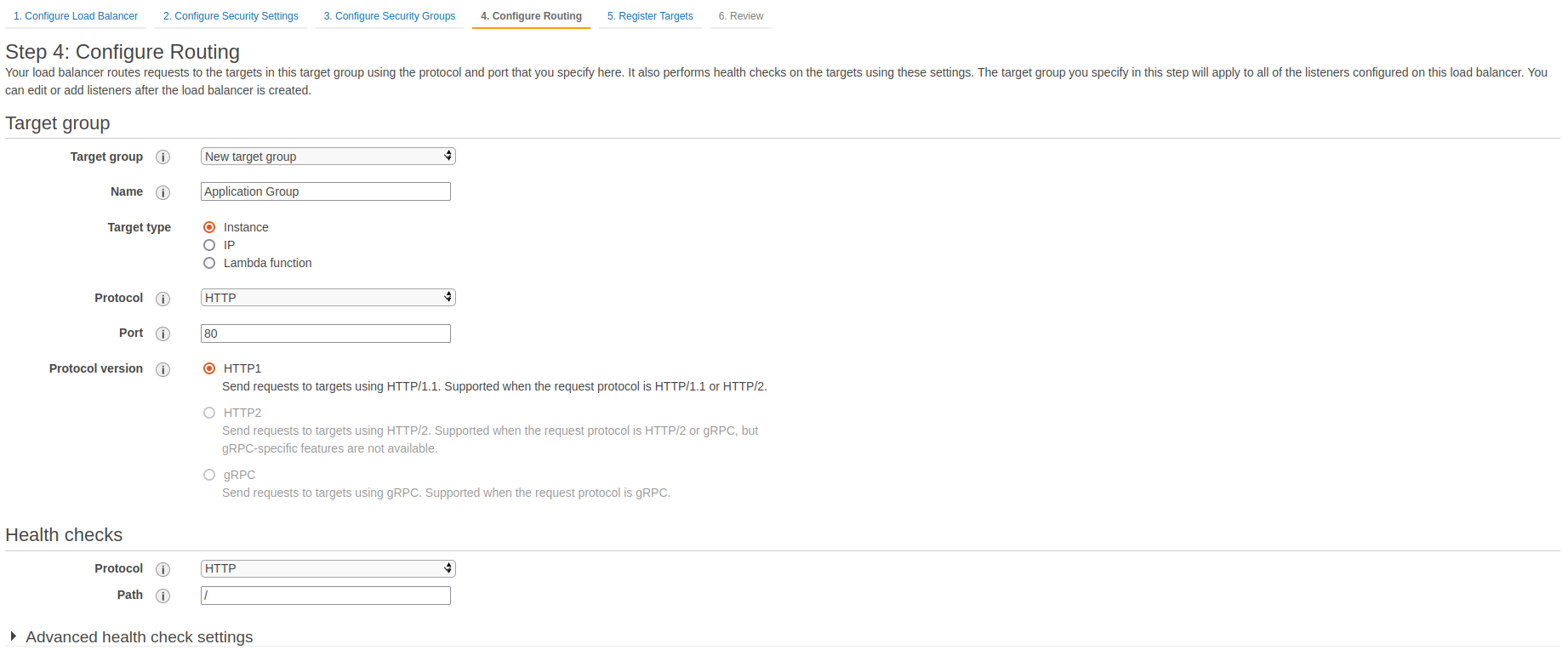
Elastic Load Balancer eklemek için EC2 içerisinde bulunan Load Balancers seçeneği seçildikten sonra create load balancer seçeneği seçilir. Uygulama HTTP ve HTTPS servislerini kullandığı için “*Application Load Balancer*” seçilerek işlemlere deam edilir.



Bu işlemlerde önce farklı bir Availability Zone için subnet eklenmesi gereklidir. Çünkü Load Balancer gelen isteği farklı availability zonelarda dağıtması gerekecektir. 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.



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.

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.

