Oluşturduğumuz VPC yi silmiyoruz.

Introduction to VPC 
What is VPC? 
loud, 
egion 
LAR 
VPC 
Auto 
Scaling 
ELB 
RDS 
Amazon Virtual Private 
Cloud (Amazon VPC) is a 
logically isolated area of the 
AWS cloud where you can 
launch AWS resources in a 
virtual network that you 
define. 
EBS 

VPC izole edilmiş bir mantıksal alandır. Resource larımızı public internetten ve kendi resource larımızdan izole ediyoruz. Hepimizin konsolda bir defaut VPC si var. Ürettiğimiz bütün kaynaklar aynı enviorenment de duruyor. Biri içeri bir sızarsa her şeye ulaşabilir.

Best practice olarak her proje için ayrı VPC oluşturulur. Default VPC denemeler veya günlük işler için kullanılır.

Non-VPC resorcelar da var; DynomoDB ve S3

AWS 
Amzon S3 

Aslında bizim VPC altındaki resource umuz DynamoDB veya S3 e bağlanmak için VPC den çıkıp internet üzerinden bağlanır. Ancak ilerede göreceğimiz gibi burada VPC kullanacağız.

VPC regionaldır. Basic Componentler:

VPC Basic Components 
• VPC Region (AZ) 
• VPC Subnets 
• VPC CIDR 
Internet Gateway 
Route Table 
• 
Security Group and Network ACL 

Region,VPC, 
AWS 
Region 
PC 
AZ 
Subnet 
CLARUSWAY 
WAV TO REIWENT YOURSELF 
AZ and Subnets 
AW 
Region 
Availability Zone I-A 
Public Subnei IA 
RDS 
Private Subnet IA 
Availability Zone I-B 
Public Subnet 1B 
111b 
Private Subnet 1B 

VPC ler bir region içerisindedir. VPC leri de subnetlere bölüyoruz. Region altında hiyerarşik AZ olduğu gibi.

VPC bir region içerisinde yer aldığı gibi subnetler de VPC nin içinde bulunduğu regionların AZ sinde yer alır. VPC region-based Subnet de AZ-based tir.

VPC de neden subnet create ediyoruz? S3 te bucket ı neden create ediyorduk? Bir şey depolamak için oluşturuyorduk Süpermarketteki market arabası gibi. Subnetsiz VPC olmaz.

VPC CDR 
1 
10.0.o.0 16 
10.0.0.0/16= 65,536 IPs in Range 
10.0.1.0/24=256 IPS in Range 
10.0.1.0/32= 
1 IP in Range 
Block Size 
CDR 
refers to Classless Inter-Domain Routing. 
• It is a set of Internet protocol (IP) standards that is used to create unique 
identifiers for networks. 
• As the Size Block/Netmask (/16,24,32) increases, the number of IP 
located in CIDR Block decreases. 

CIDR Kapalı devre iletişim sağlayan bir IP bloğu gibi düşünülebilir. CIDR bloklar Subnet masklar kullanılarak oluşturuluyor. Temelde 3 tane seçebileceğimiz CIDR bloğu var.

16 subnetmask bloğunu gösterir.

Subnet 24 kullanıldığında host yetersiz olabilir. 20 kullanılması daha iyidir.

C dc-editor.org/rfc/rfc1918 
G traslate - Google' m 
RFC 1918 
o 
Clarusway-de+n AWS-Plans-Slides... Amazon Web Serv... E Clarusway LLC 
Address Allocation tor Private Internets February 1996 
3. Private Address Space 
The Internet Assigned Numbers Authority (IANA) has reserved the 
following three blocks of the I p address space for private internets: 
10.0.0.0 
172.16.o.o 
192.168.0.0 
10.255.255.255 (10/8 prefix) 
172.31.255.255 (172.16t12 prefix) 
192.168.255.255 (192.168/16 prefix) 

Biz genelde 172.16.0.0 bloğunu kullanırız.

VPC CDR 
VP 
Subnets 
10.7.0.0/16= 65,536 IPs in Range 
la 
1b 
lc 
10.7.1.0/24=256 IPS in Range. 
10.7.2.0/24=256 IPS in Range 
10.7.3.0/24= 256 IPS in Range 
esource 
11[) 
10.0.1.1/32 
10.0.1.2/32 
RDS 

CIDR bloğu bize bir demet dolusu IP hediye ediyor. Bu IP leri instance lara veriyoruz.

VPC CDR 
10.10.0.0/16 
65,536 IPs 
10.10.1.0/24 
251 IPs 
256 IPs 
ALLOCATED = 5 IPS 
Address indicator 
VPC Router (AWS) 
DNS (AWS) 
Reserved (AWS) 
Broadcast 
: 10.10.1.0/32 
: 10.10.1.1/32 
: 10.10.1.2/32 
: 10.10.1.3/32 
: 10.10.1.255/32 

10.10.1.0/24 subnet içinde 256 tane IP var ancak 5 tanesi reservedir.

10.10.1.0/32 Address inticator,

10.10.1.1/32 VPC Router (AWS)

10.10.1.2/32 DNS (AWS)

10.10.1.3/32 Reserved (AWS)

10.10.1.255/32 Broadcast

Diğer bir component Inernet Gateway dir. VPC içindeki instance ların dışarıyla olan bağantısını sağlayan componenttir. Instance ları internete bağlarken, ssh ile de instance lara ulaşmayı sağlar. NAT görevi de görür. NAT translate yapar, dışarıyla bağlantı yaparken public IP (isim ile hitap edilmesini), içeride bağlantı yaparken (lakap ile hitap) private IP kullanılmasını sağlar.

Diğer bir component Route Table dır.

Internet Gateway i kullanabilmemiz için Router a yazmamız lazım. Internet Gateway vize, Route Table pasaport gibidir. Vizeyi pasaporta yazdırman lazım.

Route Table lar Subnet-based componenttir. Birkaç subneti route table a bağlayarak subnet içerisindeki instance lar da bu pasaportu kullanmış olurlar. Yani instance lar RT yi doğrudan kullanamaz. Hangi subnete bağlıysa, o subnet in bağlı oldu RT kurallarına tabidirler.

VPC içerisinde dışarıya çıkışla ilgili herhangi bir component create edeceksek Route Table a yazılması gerekir.

Security Group Componenti

SECGRP aslında bir VPC componentidir. Host-based bir firewall dır. Yakın koruma gibi.

Bir de Network Access Control List vardır. Biz bugüne kadar hep default olanı kullandık. Network ACL de bir firewall dır. Subnet-based dir. Yani subnet in önünde yer alır. EC2 subnet içinde olduğu için subnet kuralına tabidir ancak daha önce Network ACL kontrolüne tabidir. Çünkü Network ACL subnetin önündedir.

Network ACL subnet-based olduğu için kapsadığı bütün resource lara da etki eder. Bir değişiklik yaparken dikkatli olmak gerekir.

Network ACL stateless tır yani bir haberleşme yoktur. Giriş kapısı ile çıkış kapısı arasında bir konuşma olmaz. SECGRP ta outbound u all yapınca giren çıkabiliyordu. Network ACL böyle çalışmaz. İçeri girerken kontrol eder, çıkarken de kontrol eder. Yani girişteki nöbetçi ile çıkıştaki nöbetçi arasında bağlantı yoktur. SECGRP lar ise statefuldur. Yani inabound da olan bir değişiklik otomatik olarak outbound a yansıtılır.

SECGRP ta bir kural yazdığımızda bu allow demekti. Ancak Network ACL de bir kural allow ya da deny olabilir.

SECGRP ta allow deny diye bir seçenek yoktu.

Bu kurallar da yukarıdan aşağı sırasıyla bakar. SSH ile bağlantı yapılacak önce 100 e bakıyor, 80 için, sonra 200 e bakıyor kendisi için ama deny. Bağlantı yapamaz.

3306 bağlantısı sırasıyla baktı 100 ve 200 ona göre değil. \* hiçbirine uymuyorsa bana gel demek. Oraya bakıyor All trafic deny. bağlantı yapamaz.

Internal Phone Number Range: 
1-2-3..........100 
Intemal Phone 
Network 
Department: Finance:10-19 
Internal Phone Number Range: 
1-2-3... 
Manager 210 
0532-324-54-43) 
532-324-54-46) 
Vice-manager:ll 
Department IT:20-29 
Developer: 20 (m) 
VIP 
Database: 21 
Deoartment Supply:30-39 
Manager :30 
( 532-324-54-78) 
Department Marketing:40-4 
....100 
Finance:10-19 
IT :20-29 
Supply:30-39 
Marketing:40-49 
Manager: 40 
Employee 41: 
TESLE 
( 532-324-54-57) 
532-324-54-81) 

TESLE diye bir firmamız var. Şirket içinde mantıksal departmanlar kurduk. Çalışanlar için ileride iletişimi yerel telefon şebekesi üzerinden yapmak istiyorum. Masaüstü telefonlarda dahili telefon şebekesi. Bunun için bir tane dahili telefon santrali almamız gerekiyor ve 1 den 100 e kadar numara barındırıyor bu santral. 1 Ahmet in 5 Mehmet in gibi.

Bu numaraları dağıtmak için departmanlara bölüyoruz. 1-10 arasını elimizde tuttuk. 10-19 u finans departmanına, 20-29 u IT dep, 30-39 u Supply departmanına gibi.

Departmanlar içerisinde de bu numaralar çalışanlara veriliyor. Finans departmanındaki birisi Marketing dep müdürnü arayacaksa 40 ı çeviriyor. Öte yandan 42 numarasına baktığımızda onun da marketingde çalıştığını anlayabiliyoruz.

Ancak bu numaralar sadece içeride geçerli. Dışarıdan kimse 42 yi arayarak ulaşamaz. Ya da bu dahili telefonlarla dışarıyı arayamıyorlar. Dışarı görşümeler için herkese cep telefonu numarası veriyoruz. Public.

Ancak IT departmanındaki bilgiler hassas olduğu için onlara cep telefonu verilmiyor, onlar başka departmanlar üzerinden dışarıya ulaşabiliyor.

Internal Phone Number Range: 
1-2-3-4-5.... 100 
Intemal Phone 
Network 
Department: Finance:10-19 
Manager 210 
Vice-manager:ll 
Department IT:20-29 
Developer: 20 (m) 
Database: 21 
Deoartment Supply:30-39 
Manager 
Department Marketing:40-4 
Manager: 40 
imployee 41: 
TESLA 
0532-324-54-43) 
532-324-54-46) 
VIP 
32-324-54-78) 
532-324-54-57) 
532-324-54-81) 
vpc 
Public IP :3.4.9.0/32 
Private IP: 10.7.1.1/32 
Public IP 
Private IP: 10.7.2.1/32 
CIDR 
10.7.0.0/16 
SUBNET CIDR 
10.7.1.0/24 
Private 
10.7.2.0/24 
10.7.3.0/24 
10.7.4.0/24 
Account 

Dahili telefon santrali VPC dir. Santral de 1-100 arası numara vardır. Bu CIDR bloğudur. private IP address havuzudur. Departmanlar VPC altındaki subnetlerdir. Subnet teki amaç da aynı amaca hizmet eden resource ları gruplamaktır.

10.7.3.0/24 gibi IP lerden de hangi subnet olduğunu olduğunu anlayabiliyoruz. Dışarıyla irtibat public IP address ile kurulur. Dışarıyla irtibat kuramayan IT departmanı da private subnettir.

VPC CIDR Bock 
Labeling 
10.7.0.0/16 = 65000 IP = 65000 
Internal Communication 

VPC CIDR Bloğu bir etiketlemedir ve dahili iletişimi sağlar.

How is it possible to use the same CIDR block for all of us? 
HOSPITAL 
SSN:01-A-2345-4563 
SSN:02-C-98756H64 
vpc 1 
VPC 2=House 2 

Bugün hepimiz aynı private IP bloğunu kullanacağız. Ancak farklı VPC lerde olacağımız için karışıklık ve çakışma olmaz.

VPC konsolu açıyoruz.

(VPC i silip yeni default VPC create edebiliriz.)

Actions A 
create vpc 
IPv6 CIDR 
V 
No VPCs found in t 
Create default VPC 
Create flow log 
Edit VPC settings 
Edit CIDRs 
Manage middlebox routes 
Manage tags 
Delete vpc 

Şimdi handson dayız.

Create VPC diyoruz.

VPC and more dersek bizim için subnetlerle hazır kuruyor. Biz bugün önce VPC yi kendimiz kurup içini kendimiz dolduracaz.

VPC settings 
Resources to create Info 
Cæate mly the V PC the VPC and retwking 
O VPC only 
C) VPC and more 
Name tag - optional 
tag with of and a value that sp.æify. 
clarus-VPC-a 
block Info 
O CIDR manual input 
C) IPAM-a110cated block 
CIDR 
10_7.0.0/16 
Info 
O No IPv6 CIDR block 
C) IPAM-a110cated CIDR block 
C) Amazon-provided CIDR block 
C) CIDR owned by me 
Tenancy Info 
Default 

Isim verdik, 10.7.0.0/16 CIDR bloğunu girdik. IPv& istemiyoruz. Tag Name key ile verilmiş durumda.

Create diyoruz.

Default VPC nin CIDR bloğu 172 li:



Elimizde bir flow chart olmalı

Create VPC 
Create IGW 
IGW Action Menu: 
Attach IGW to VPC 
Set the VPC Route Table: 
VPC Action Menu: 
Edit DNS Hostname 
Name tag: clarus-vpc-a 
IPv4 CDR block: 10.7.0.0/16 
Name Default Route Table: default-labvpc 

Oluşturacağımız yapı da şu şekilde olacak:

Cloud 
Region 
Ro te 
Ta le 
10.10.1.0,'24 
:010.020/24 
Ro te 
Tab 
vpc=clarus-vpc- 
Availability Zone I-a 
Public Subnet la 
10.7.1.0/24 
10.7.2.0/24 
Private Subnet la 
Region : N.Virginia 
.7.0.0/16 
Availability Zone I-b 
Public Subnet 1b 
10.7.4.0/24 
10.7.5.0/24 
Private Subnet 1b 
Internet Gateway 
Availability Zone I-c 
Public Subnet Ic 
10.7.7.0/24 
10.7.8.0(24 
Private Subnet lc 

6 subnet oluşturacaz. Her AZ de bir public bir private subnet oluşturacaz. Internet Gateway imiz ve Route table lar oluşturacaz.

Sol taraftaki menüden Internet Gateway i tıklıyoruz.

Default VPC imize bağlı bir internet gateway var. Her VPC için bir internet gateway olmalı. Yeni VPC miz için bir igw oluşturuyoruz:

Create internet gateway Info 
An internet gateway is a virtual anter 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 
tag with of and a value that sp«ify 
clarus-igw 
Tags - optional 
A tag is a Label that æsign to an AWS tag of and 
track AWS 
n optimEl Ym_l en tags to 
Value - optional 
Q clarus-igw 
Q Name 
Add new tag 
Gn add 49 
X 
x 
Cancel 
Remove 
Create internet gateway 

VPC imize attach ediyoruz. Actions tan.

Internet gateways 
Attach to V 
Attach to VPC (igw 
vpc 
-Obb519b763757dd04) 
Attach an gat—,' to VPC to VPC to witl Sp.æify VPC to attach 
Available VPCs 
Attach the gat—,' to this VPC 
Q vpc-Of10b2E959b7b42941 
AWS Command Line Interface command 
Cancel 
Attach internet gateway 

CLI komutlarını da alttaki sekme gösteriyor.

IGW yi kurduk ama yetiyor mu? Hayır çünkü vizeyi pasaporta işlememiz gerekiyor. Sol taraftdan route tables a tıklıyoruz.

VPC miz için default olarak gelen bir route table var. Buna clarus-default ismi veriyoruz:

Name 
default 
Route table ID 
rtb-og1d4A372SbbcccOa 
rtb-0011b4dOc577cf77S 
Explicit subnet associat... 
Edge associations 
Main 
vpc-Of10b28959b7b4294 1 cla.. 
vpc-oc9174f10af407a4d I 

Default VPC nin default RT sine bakalım:

Routes (2) 
Q Filter routes 
Destination 
000.0/0 
172.31.0.0/16 
Target 
igw-07993a8354cdd8720 
local 
Propagated 
@Active 
@Active 

Dışarı çıkmak için destionation anywhere hedef igw diyor.

vpc 
1010.0.0/16 
Cloud 
Region 
Local 
Int 
Gat 
Domestk 
1000 1 
to 10020,'za 
Route 
Tables 
PASSPORT 
DIS 1 

Ancak clarus-default RT sinde igw yok:

poJe6edoud 
s meus 
CROB 
56 el 
9 L/OOTOL 
uoneuusaa 
saancu 
soJno.' upa 
uone5edo•d 
suoneposse a6pa 
suoneposse Jauqns 
sou noH 

Edit routes diyerek public route ekleeycez.

Edit routes 
Destination 
10.7_0.0/16 
Q 0.0.0_0/0 
Add route 
X 
Target 
Q local 
Q igw-Obb519b763757dd041 
X 
Status 
@Active 

Ekleyip save changes diyoruz. Igw vizemizi RT pasaportumuza yazdırdık.

Routes 
Routes (2) 
Subnet associations 
Edge associations 
Target 
Route propagation 
Tags 
Edit routes 
Q Filter routes 
Destination 
0.0.0_0/0 
10.7.0.0/16 
goth 
Status 
@ Active 
@ Active 
Propagated 
igw-Obb519b763757dd04 
Ojcal 

RT ler subnetleri yönetir. Biz hiçbir şey yapmazsak bütün subnetler default RT ye bağlanır.

Şimdi VPC Action menu den Edit DNS Hostname yapacaz.

VPC imizi seçip Actions tan Edit VPC settings diyoruz.

Enable DNS Hostnames i tick leyip save ediyoruz.

DNS settings 
Enable DNS resolution Info 
Enable DNS hostnames Info 

Public ve private DNS leri de versin diye bunu editledik.

VPC imiz kabaca hazır oldu.

Şimdi Subnetleri oluşturacağız:

Sol menüden subnets i açıyoruz.

Önümüze çıkanlar default VPC mizin subnetleri. Subnetler 20 ile bitiyor. Bu ne demek her subnet içind 4096-5 tane IP verebiliyoruz.

IPV4 CIDR 
172.31.0.0/20 
172.51.32.0/20 
172.31.80.0/20 
172.51.64.0/20 
172.51.4&0/20 
16.0/20 
IP-v6 CIDR 
Available IPv4 addresses 
4091 
40 1 
4091 
4091 
4091 
4091 

Create Subnet diyoruz bize hangi VPC içinde create edeceğimizi soruyor:

IPV4 CIDR 
172.31.0.0/20 
172.51.32.0/20 
172.31.80.0/20 
172.51.64.0/20 
172.51.4&0/20 
16.0/20 
IP-v6 CIDR 
Available IPv4 addresses 
4091 
40 1 
4091 
4091 
4091 
4091 

Subnet isimlerini handson dan alıyoruz:

Subnet settings 
CIDR kÆiLability Zme 
Subnet I Of I 
Subnet name 
Cæate with of and a »ecify_ 
clarus-azl a-public-subnet 
The up to 256 
Availability Zone Info 
Chm the which will ræide, let fw 
US East (N. Virginia) / us-east-la 
block Info 
Q 10.7.1.0/24 
Tags - optional 
Q Name 
Add new tag 
add 49 
Remove 
X 
Value - optional 
Q clarus-azla-public-subnet 
x 
Remove 

Us-east-1a da public subnet imizin CIDR bloğunu 10.7.2.0/24 olarak belirledik. Create subnet diyoruz.

Public oluşturduk şimdi private oluşturacaz.

Subnet settings 
CIDR kÆiLability Zme 
Subnet I of I 
Subnet name 
Cæate with of and a WIue »ecify_ 
clarus-azl a-private-subnet 
The up to 256 
Availability Zone Info 
Chm the which will ræide, let fw 
US East (N. Virginia) / us-east-la 
block Info 
Q 10.7.20/24 
Tags - optional 
Q Name 
Add new tag 
add 49 
Remove 
X 
Value - optional 
Q clarus-azla-private-subnet 
x 
Remove 

CIDR bloğunda 3 ü atladık 4 e geçtik çünkü bu AZ de başka subnet ileride lazım olabilir 3 ü kullanabiliriz.

İkinci subnetleri us-east-1b AZ de private ve public olarak oluşturuyoruz.

CIDR bloğunda 6 yı es geçtik. Bu AZ de reserve etmiş gibi.

Üçüncü subnetleri de us-east-1c AZ de private ve public oluşturduk.

wuqns 
Iou e) 
aauqns mau ppv 

Add new subnet diyerek subnetleri alt alta oluşturabiliriz.

6 tane subnet imizi oluşturduk.

U 
Name 
clarus-azla-public-. 
clarus-azl b-public-._. 
clarus-azl b-private. 
clarus-azlc-public-_ 
clarus-azl 
clarus-azlc-private_ 
Subnet ID 
subnet-Oa220c1bcb51agc2d 
subnet-04ag916440a4eg56g 
subnet-03dc071d7cf73c3a6 
subnet-Od37f338c24gb65c6 
subnet-03aabog9ed35asa19 
subnet-02g251327a683b6S6 
State 
@Available 
@Available 
@Available 
@Available 
@Available 
@Available 
vpc-Of10b28959b7b4294 1 cla.._ 
vpc-Of10b28959b7b4294 1 cla.._ 
vpc-Of10b28959b7b4294 1 cla.._ 
vpc-Of10b28959b7b4294 1 cla.._ 
vpc-Of10b28959b7b4294 1 cla.._ 
vpc-Of10b28959b7b4294 1 cla.._ 
CIDR 
10.7.1.0/24 
10.7.4.0/24 
10.7.5.0/24 
10.7.7.0/24 
10.720/24 
10.780/24 
IPv6 CIDR 
Available 

Private yazınca private olmaz subnet. Route Table dan configure etmemiz gerekir. Bütün subnetlerimize igw si olan Route table ı default olarak atadı.

Route Tables a gidio Subnet association a gidiyoruz:

Explicit subnet associations (O) 
Q Find subnet association 
Subnet ID 
Edit subnet associations 
CIDR 
No subnet associations 
You do not have any subnet associations. 
CIDR 

Explicit olarak bu rt yi bir subnete bağlamamışız (özellikle)

Subnets without explicit associations (6) 
The follcwing not ev!icitly with tablæ and aæ with table 
Edit subnet associations 
Q Find subnet association 
Subnet ID 
subnet-04ag916440a4eg56g / clarus-azlb-public-subnet 
subnet-Oa220c I bcb51agc2d / clarus-azla-public-subnet 
subnet-03dc071d7cf73c3a6 / clarus-azl b-private-subnct 
subnet-Od37f338c24gb65c6 / clarus-azlc-public-subnct 
subnet-03aabog9ed35a5a19 / clarus-azla-private-subnet 
subnet-02g251327a683b6S6 / clarus-azlc-private-subnct 
CIDR 
10_7.4.0/24 
10_7.1.0/24 
10_7.5.0/24 
10_7.7.0/24 
10_7.2.0/24 
10_7.8.0/24 
CIDR 

Without explicit (implicitly) olarak yani default olarak bütün bu VPC deki bütün subnetler bu rt ye bağlanmış. Bizim default RT miz de igw mevcut yani bütün subnetler public.

1- All Subnets are associated with 
Default Route Table Implicitly 
Conclusion 
2- By default all subnets are 
PUBLIC a.Local 
b.OOOO/0 

Private RT açıp private Subnetlere assign edebiliriz. Ya da public RT ve privte RT olarak iki tane oluşturabiliriz.

6 Public 
PUBLIC RT 
PI lhlir Private 
Option-I 
DEFAULT RT 
PRIVATE RT 
PRrvATE 
PRtVATE 
Option-2 
DEFAULT RT 
PRIVATE RT 
PRIVATE 
PRIVATE 

Çünkü yeni oluşturduğumuz bir subnet direk default olarak public oluyor bu durumda.

Şimdi Create Route Table diyoruz:

Route table settings 
Name - optional 
Cæate tag with of a 
clarus-public 
The VPC to for this table 
a WIue *ecify_ 
vpc-0f1 Ob28959b7b4294 (clarus-vpc-a) 

Şimdi route edit leyecez. Public networke bağlanırken clarus igw yi kullansın diyoruz:

Edit routes 
Destination 
10.7_0.0/16 
Q 0.0.0_0/0 
Add route 
x 
Target 
Q local 
igw-Obb519b763757dd041 
Q 
X 
Status 
@Active 
Propagated 
Remove 

Edit subnet association diyoruz ve public subnetlerimizi ekliyoruz:

-suoneposse lauqns Aue aneu lou op noA 
suoneposse ON 
Hal) 
suoneposse lauqns 
01 aauqns 
uouoposso aauqns puy 
(0) suoyeposse u.!ldxa 
56 el 
Hal) 
uone5edo•d 
suoneposse a6pa 
suoneposse Jouqns 
s nn0H 

Available subnets 
(3/6) 
Q Filter subnet associations 
Name 
clarus-az I ID-public-subnet 
clarus-az la-public-subnet 
clarus-az I ID-private-subnet 
clarus-az I c-public-subnet 
clarus-az I a-private-subnet 
clarus-azlc-private-subnct 
Selected subnets 
> 
o 
Subnet ID 
subnet 
-04ag916440a4c8568 
subnet 
subnet 
-03dc071d7cf7Sc3a6 
subnet 
-Od37f338c249b65c6 
subnet- 
03aabog9ed35a5a1g 
subnet- 
029251327a683b656 
CIDR 
10.7.4_0/24 
10.7.1_0/24 
10.7.5_0/24 
10.7.7_0/24 
10.7.2_0/24 
10.7&0/24 
CIDR 
Route table ID 
Main (rtb-081d443723bbcecOa / claros-default) 
Main (rtb-OgId443723bbcecOa / claros-default) 
Main (rtb-081d443723bbcecOa / claros-default) 
Main (rtb-OgId443723bbcecOa / claros-default) 
Main (rtb-OgId443723bbcecOa / claros-default) 
Main (rtb-OgId443723bbcecOa / claros-default) 
subnet-Od37f33gc249b65c6 / clarus-azlc-public-subnet X 
subnet-Oa220cIbcb51age2d / clarus-azla-public-subnet X 
subnet-04a9916440a4eg568 / clarus-azlb-public-subnet X 
Cancel 
Save associations 

Save associations diyoruz.

Şimdi bu subnetler altında kuracağımız instance lara otomatik IP ataması için ayar yapmamız gerekiyor:

Public Route Table Steps 
Create a new Route Table 
for Public Subnets 
Associate 3 Public Subnets 
with Public Route Table 
Set Routes: 
a.Local 
b.OOOO/0 
Modify Auto-Assign IP 
Settings-Subnet Action 
Menu-Edit bnet setti@s 
Default Route Table of VPC — 
Public Subnet! 
Internet Connectivi 

Subnets e geliyoruz. Public subnet leri tek tek seçip Edit Subnet Settings diyoruz:

Subnets 
(1 / 6) Info 
Q Filter subnets 
Name 
clarus-azl b-public-__ 
clarus-azla-gublic-. 
Subnet ID 
subnet-04ag916440a4egs6g 
subnet-Oa220c1bcb51agc2d 
State 
@Available 
@Available 
vpc-Of10b28959b7b4294 1 cla.._ 
vpc-Of10b28959b7b4294 1 cla.._ 
View details 
Create flow log 
Edit subnet settings 
Edit IPv6 CIDRs 
CIDR 
Edit network ACL as 
10.7.4.0/24 
Edit route table ass( 
10.7.1.0/24 

Bu kutucuğu işaretliyoruz ve save diyoruz.

Auto-assign IP settings Info 
the IP to æquæt public in this 
Enable auto-assign public address Info 
• Enable auto-assign customer-owned IPv4 address Info 
Option no ms 

Üç public subnet için de bunları yaptık.

Şimdi yeni bir RT oluşturuyoruz bu private RT olacak.

Route table settings 
Name - optional 
Cæate with of a 
clarus-private-rt 
The VPC to for this table 
a WIue *ecify_ 
vpc-0f1 Ob28959b7b4294 (clarus-vpc-a) 
Tags 
A tag a Label that to an AWS tag of and an opti•MEl Ym_l tags to 
track AWS 
Q Name 
Add new tag 
add 49 
X 
Value - optional 
Q clarus-private-rt 
x 
Cancel 
Remove 
Create route table 

Private subnetlerimiz için association yapacaz:

Edit subnet associations 
Change which subnets are associated with this route table. 
Available subnets 
(3/6) 
Q Filter subnet associations 
Name 
clarus-azl ID-public-subnet 
clarus-azl a-public-subnet 
clarus-az I b-privatc-subnet 
clarus-az I c-public-subnet 
clarus-az I a-private-subnet 
clarus-az Ic-private-subnct 
> 
o 
Subnet ID 
subnet 
-04ag916440a4c856g 
subnet- 
oa220c1bcb51age2d 
subnet 
-03dc071d7cfBc3a6 
subnet 
-Od37f338c249b65c6 
subnet 
-03aabog9ed35a5a1g 
subnet 
-029251327a683b656 
CIDR 
10.740/24 
10.7_1.0/24 
10.7_5.0/24 
10.7_7.0/24 
10.720/24 
10.7_8.0/24 
CIDR 
Route table ID 
rtb-Oda21c4fae763gccO / claros-public 
rtb-Oda21c4fae763gceO / claros-public 
Main (rtbGId443723bbcecOa / claros-default-rt) 
rtb-Oda21c4fae763gccO / claros-public 
Main (rtbGId443723bbcecOa / claros-default-rt) 
Main (rtb-OgId443723bbcecOa / claros-default-rt) 

Peki burada publicleri de seçersek nolur? Diğer taraftan düşürür bu tarafa ekler. Bir subnet iki farklı route table a assoicate edilemez. Son koyduğumuz kural geçerli olur.

Şu an VPC yi kurduk.

Launching an Instance 
Create in Public Subnet 
VPC CIDR Pool 
Public IP 
(Auto Assign IP ) 
AWS IP POOL 
Create in Private Subnet 
vpc CIDR Pool 

Biz public subnet te bir EC2 ayağa kaldırırsak o subnete ait CIDR dan bir private IP verecek ve bir de public IP verecek.

Private subnet içinde EC2 ayağa kaldırırsak o subnete ait CIDT bloğundan bir private IP verecek ancak public IP vermeyecek.

EC2 konsoluna gidip test ediyoruz:

EC2 launch ederken VPC imizi kendimiz seçiyoruz:

Network settings 
V PC - required Info 
vpc-Of10b2g959b7b42g4 (clarus-vpc-a) 
107.0.o/1E 
S u b net Info 
WC: .4x-of10b28959b7ba29a 
Availability a IP 251 
Auto-assign public IP Info 
Enable 
c 
clarus-azl a-public-su bnet 
CIDR: loml 0/24) 
Create new subnet 

AZ 1a seçiyoruz. Auto-assign public IP Enable durumda. Bu ne demekti? Public IP otomatik olarak verecek. Bunu enable etmesek napardık? Elastic IP alıp atayabilirdik.

Public IP si:

Public IPv4 address 
92.54.21&1011 open address 
Instance state 
@ Running 

Private IP si:

Private IPv4 addresses 
0 10.7.1.109 

Private IP başkaları ile aynı olabilir ancak farklı VPC ler altında olduğu için bir çakışma olmaz. Public in aynı olma ihtimali yok.

Bir de private subnet te instance kaldıralım. Auto-assign public IP Disable:

Network settings 
V PC - required Ho 
vpc-Of10b2g959b7b4294 (clarus-vpc-a) 
107.0.o/1E 
S u b net Info 
subnet-03dc071d7cf73c3a6 
c 
clarus-azlb-private-subnet 
WC: vpc-of10b28959b7ba29a 
Availability umast-l b IP 251 CDR: 10.7.50/24) 
Auto-assign public IP Info 
Disable 
Firewall (security groups) Info 
Create new subnet 

Private instance da public IP vermedi:

Public IPv4 address 
Instance state 
@ Running 
Private IP DNS name (IPv4 only) 
iP-10-7-2-153.eQ.internal 
Private IPv4 addresses 
0 10.7.2.153 
public IPV4 DNS 

VPC create ederken VPC and more diyerek create etmek ödevimiz olacak. Ancak aşağıdaki iki değer None olacak:

NAT gateways ($) Info 
Choose the number of Availability Zones (AZs) in which to create NAT gateways. 
Note that there is a charge for each NAT gateway 
None 
VPC endpoints Info 
In 1 AZ 
1 per AZ 
Endpoints can help reduce NAT gateway charges and improve security by 
accessing SI directly from the VPC. By default, full access policy is used. You can 
customize this policy at any time. 
None 
Gatewa 