



# AWS GAME DAY 2023

## NIVEL INICIAL

## DIVERTITE, JUGÁ Y APRENDÉ HACIENDO

**Sponsor**



Haciendo foco en:

- EC2
- VPC
- AutoScaling
- ELB/ALB



*Unicorn.Rentals*

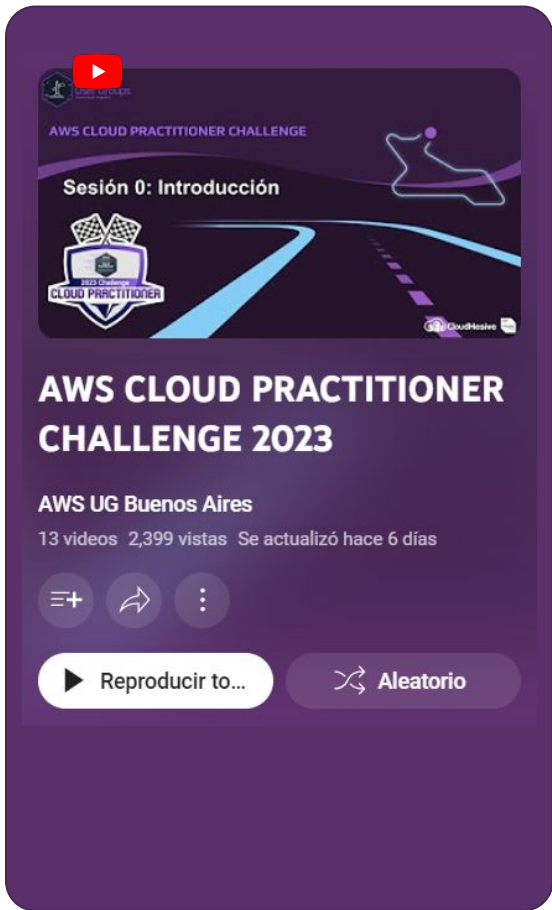
- CloudFront
- ElastiCache
- S3
- CloudWatch
- ECS/Fargate





- Sesión 1 "IAM"
- Sesión 2 "VPC"
- Sesión 3 "EC2"
- Sesión 4 "AWS Elastic Load Balancers y Auto Scaling"
- Sesión 5 "Storage (EBS, EFS, S3) + Monitoring/Log"
- Sesión 6 "Cloudfront+Route 53"

- Sesión 7 "Databases"
- Sesión 8 "Serverless"
- Sesión 9 "Security & Compliance"
- Sesión 10 "Billing & Support"
- Sesión 11 "TIPS"



# 1. Building a Custom VPC from Scratch in AWS



## Networking

Internet GtW ~vs.~ Nat Gateway  
Nat Instance ~vs.~ Nat Gateway  
Nat Instance ~vs.~ Bastion  
Nat Instance ~ Disabling source/destination checks

Route Table Public ~> Path to ~ Internet Gateway  
Route Table Private ~> Path to ~ Nat Gateway

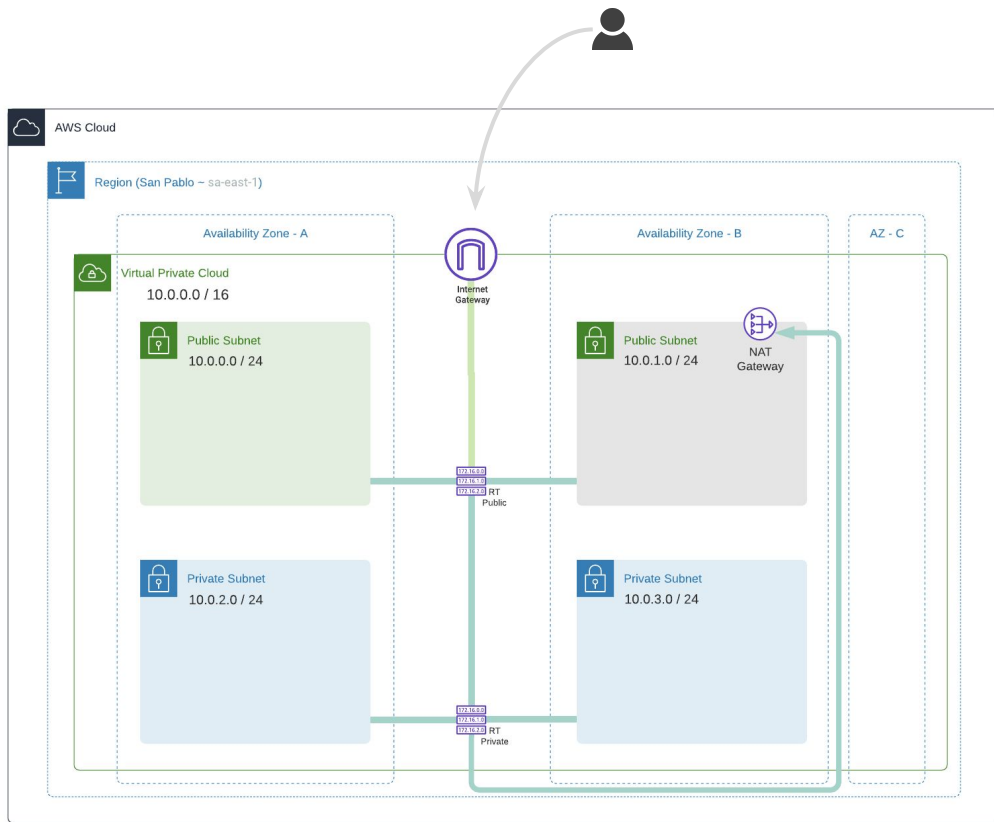
Security Group ~Stateful ~ (allow)  
NACL ~ Stateless ~ (allow & deny)

Security Group, NACL Default - Allow All  
Security Group, NACL Custom - Deny All

ICMP, Ephemeral Ports

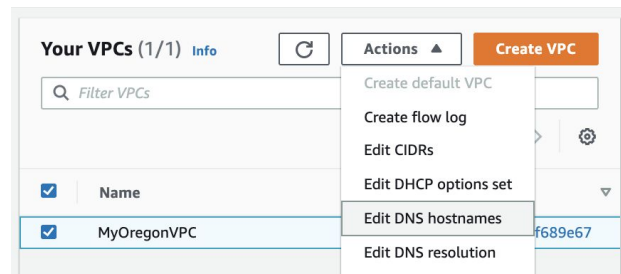
# 1. Building a Custom VPC from Scratch in AWS

## Redes y Ruteo



RT-Public    10.0.0.0 / 16    →    local  
                 0.0.0.0 / 0    →    igw-

RT-Private    10.0.0.0 / 16    →    local  
                 0.0.0.0 / 0    →    ngw-



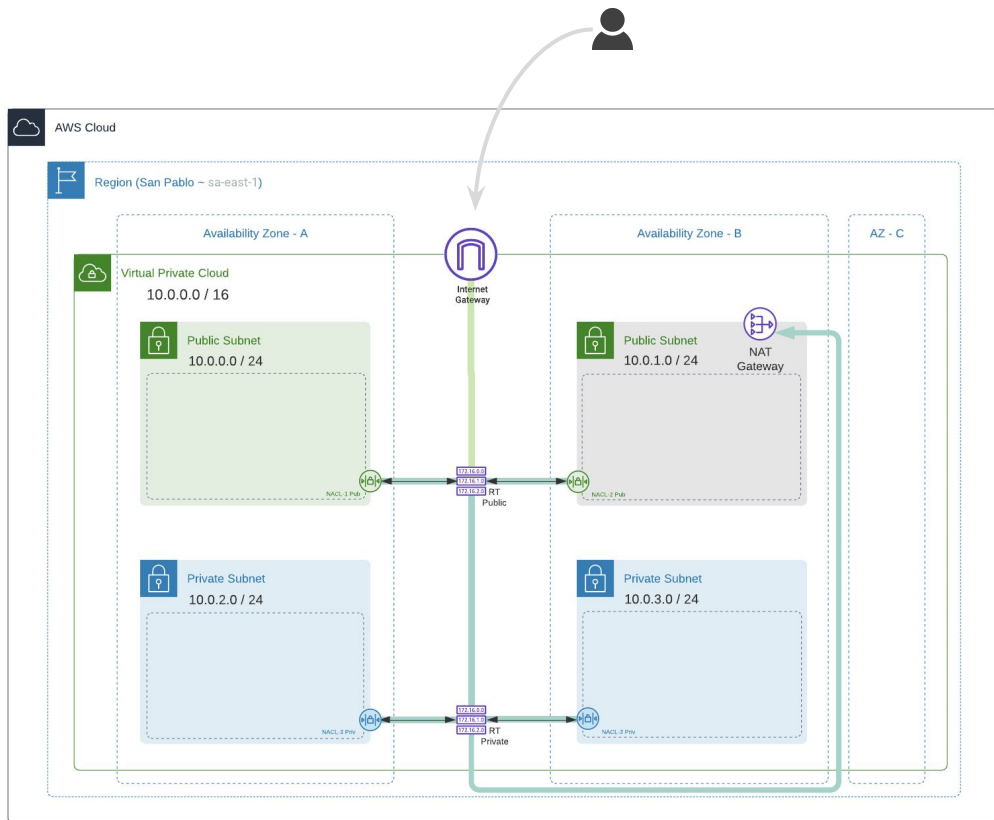
### Auto-assign IPv4 [Info](#)

☒ Enable auto-assign public IPv4 address

RT-Public    0.0.0.0 / 0    →    igw-  
RT-Public    10.0.0.0 / 16    →    local  
RT-Private    0.0.0.0 / 0    →    nat-  
RT-Private    10.0.0.0 / 16    →    local

# 1. Building a Custom VPC from Scratch in AWS

## Seguridad - “Física”



RT-Public    10.0.0.0 / 16    →    local  
                 0.0.0.0 / 0    →    igw-

RT-Private    10.0.0.0 / 16    →    local  
                 0.0.0.0 / 0    →    ngw-

### Caso de USO: Internet - Web Server - BD

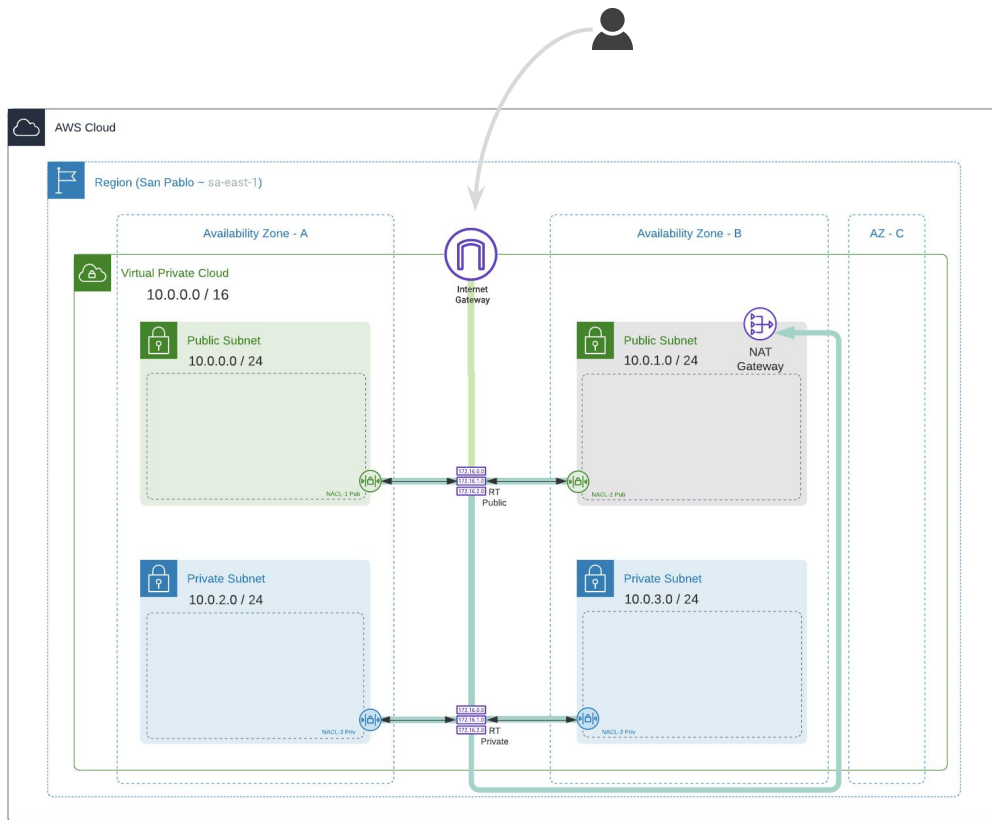
NACL-Public-A		Inbound rules			
Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	HTTP (80)	TCP (6)	80	0.0.0.0/0	Allow
200	SSH (22)	TCP (6)	22	181.164.85.20/32	Allow
300	Custom TCP	TCP (6)	1024 - 65535	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny
Outbound rules					
Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

NACL-Private		Inbound rules			
Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	MySQL/Aurora (3306)	TCP (6)	3306	10.0.0.0/24	Allow
200	SSH (22)	TCP (6)	22	10.0.0.243/32	Allow
300	Custom TCP	TCP (6)	1024 - 65535	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny
Outbound rules					
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

[ephemeral ports](#)

# 1. Building a Custom VPC from Scratch in AWS

## Seguridad - “Física”



RT-Public 10.0.0.0 / 16 → local  
0.0.0.0 / 0 → igw-

RT-Private 10.0.0.0 / 16 → local  
0.0.0.0 / 0 → ngw-

## Caso de USO: Update SW. Privado por Nat Gwy

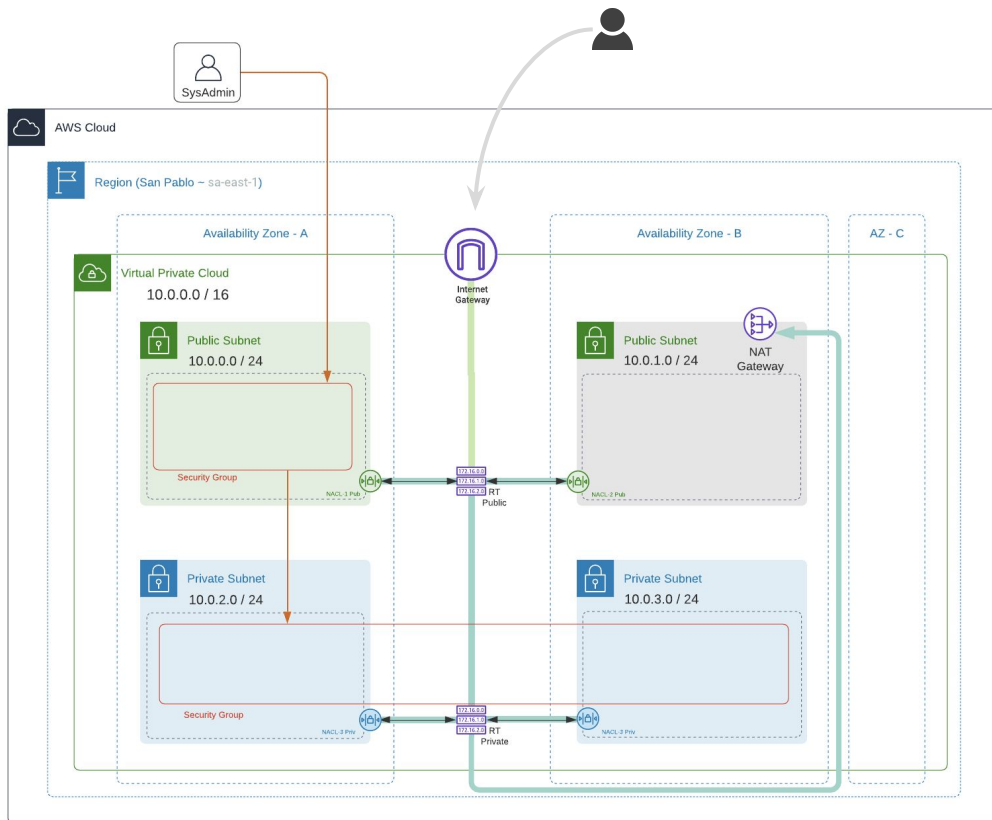
NACL-Public-B					
Inbound rules					
Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	HTTP (80)	TCP (6)	80	10.0.2.0/24	Allow
200	HTTPS (443)	TCP (6)	443	10.0.2.0/24	Allow
300	Custom TCP	TCP (6)	1024 - 65535	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny
Outbound rules					
Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	HTTP (80)	TCP (6)	80	0.0.0.0/0	Allow
200	HTTPS (443)	TCP (6)	443	0.0.0.0/0	Allow
300	Custom TCP	TCP (6)	1024 - 65535	10.0.2.0/24	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

NACL-Private					
Inbound rules					
Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	MySQL/Aurora (3306)	TCP (6)	3306	10.0.0.0/24	Allow
200	SSH (22)	TCP (6)	22	10.0.0.243/32	Allow
300	Custom TCP	TCP (6)	1024 - 65535	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny
Outbound rules					
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny



# 1. Building a Custom VPC from Scratch in AWS

## Seguridad - “Lógica”



RT-Public 10.0.0.0 / 16 → local  
0.0.0.0 / 0 → igw-

RT-Private 10.0.0.0 / 16 → local  
0.0.0.0 / 0 → ngw-

WebDMZ-SG				
Inbound rules				
Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	0.0.0.0/0	-
SSH	TCP	22	181.164.85.20/32	-
Custom TCP	TCP	1024 - 65535	0.0.0.0/0	User-Data Setup (yum update, git clone)
Outbound rules				
Type	Protocol	Port range	Destination	
All TCP	TCP	0 - 65535	0.0.0.0/0	

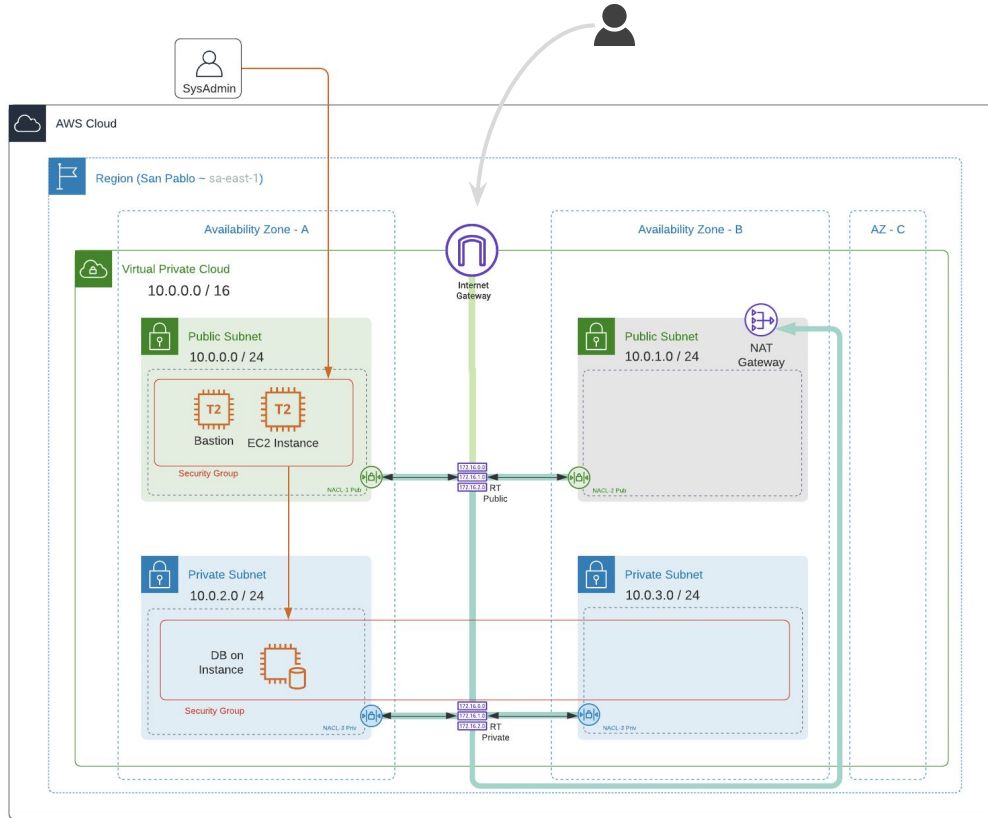
MyDB-SG			
Inbound rules			
Type	Protocol	Port range	Source
SSH	TCP	22	sg- (WebDMZ-SG)
MySQL/Aurora	TCP	3306	sg- (WebDMZ-SG)
Outbound rules			
Type	Protocol	Port range	Destination
All traffic	All	All	0.0.0.0/0

3306 | desde SG-1  
22 | desde SG-1



# 1. Building a Custom VPC from Scratch in AWS

## Despliegue



RT-Public 10.0.0.0 / 16 → local  
0.0.0.0 / 0 → igw-

RT-Private 10.0.0.0 / 16 → local  
0.0.0.0 / 0 → ngw-

## EC2 Web

```
#!/bin/bash
yum update -y
yum install httpd -y
yum install git -y
yum install php -y
service httpd start
chkconfig httpd on

#-----
echo "Hello Static Site!" > /var/www/html/index.html

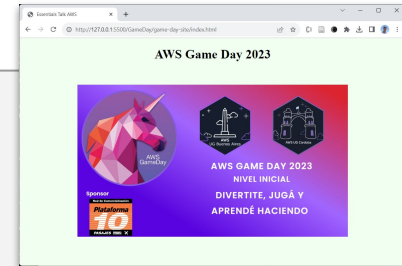
#-----
echo "<?php echo '<p>Hello PHP World</p>'; ?>" > /var/www/html/index.php

#-----
# Static web Site

git clone https://github.com/Pabloin/AWS-Essentials.git

cp -r AWS-Essentials/GameDay/game-day-site/* /var/www/html/
```

user\_data\_gameday.sh





Muchos Éxitos!!!

