



AWS GAME DAY 2023

NIVEL INICIAL

DIVERTITE, JUGÁ Y APRENDÉ HACIENDO

Sponsor



Haciendo foco en:

- EC2
- VPC
- AutoScaling
- ELB/ALB



Unicorn.Rentals

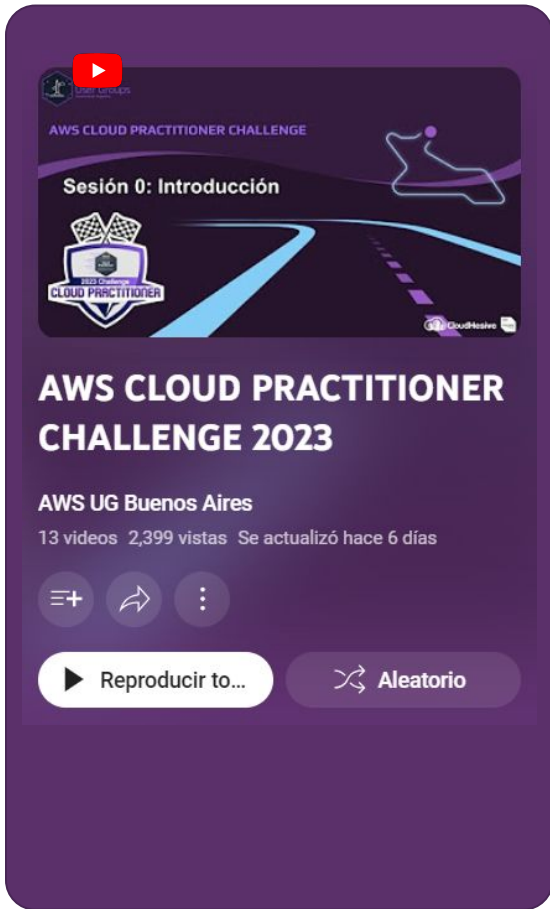
- CloudFront
- Elasticache
- S3
- CloudWatch
- ECS/Fargate





- 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"



VPC from Scratch



Unicorn.Rentals



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

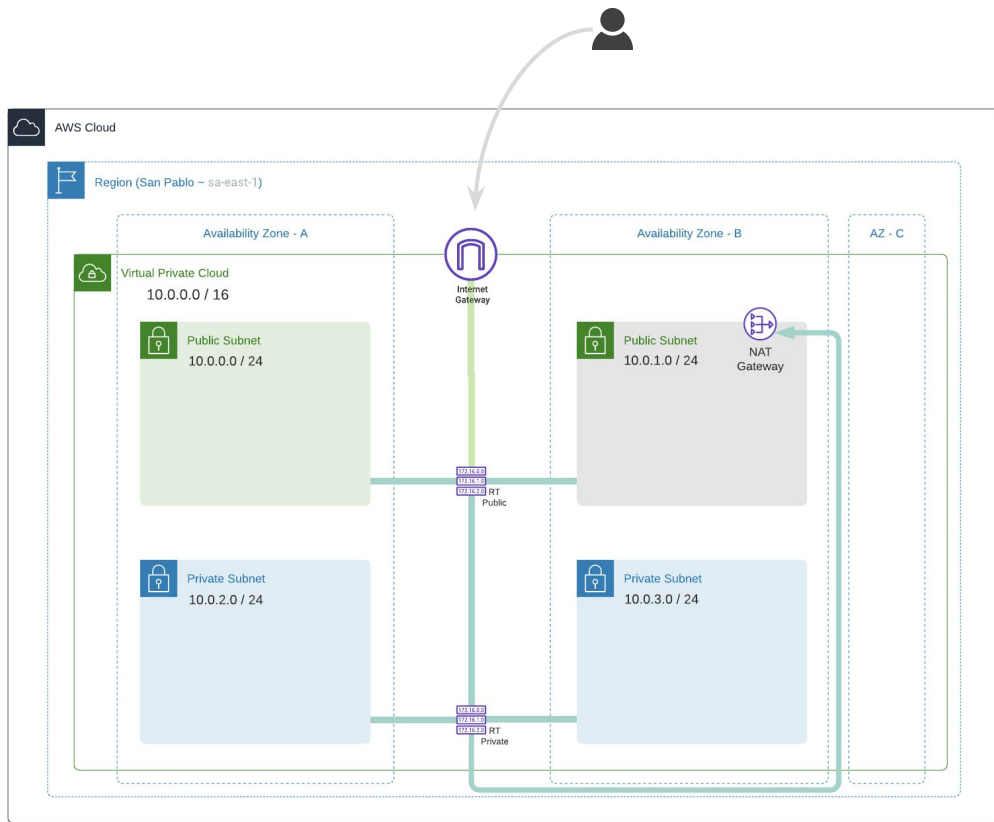
Security Group ~Stateful ~ (allow)
NACL ~ Stateless ~ (allow & deny)

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

ICMP, Ephemeral Ports

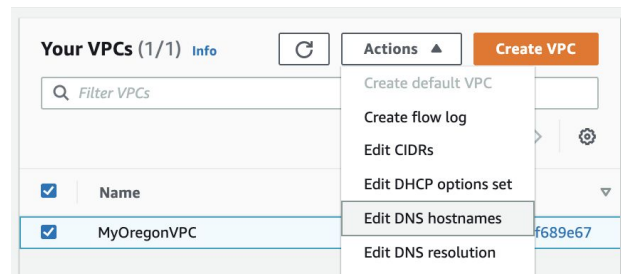
1. Building a Custom VPC from Scratch in AWS

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-



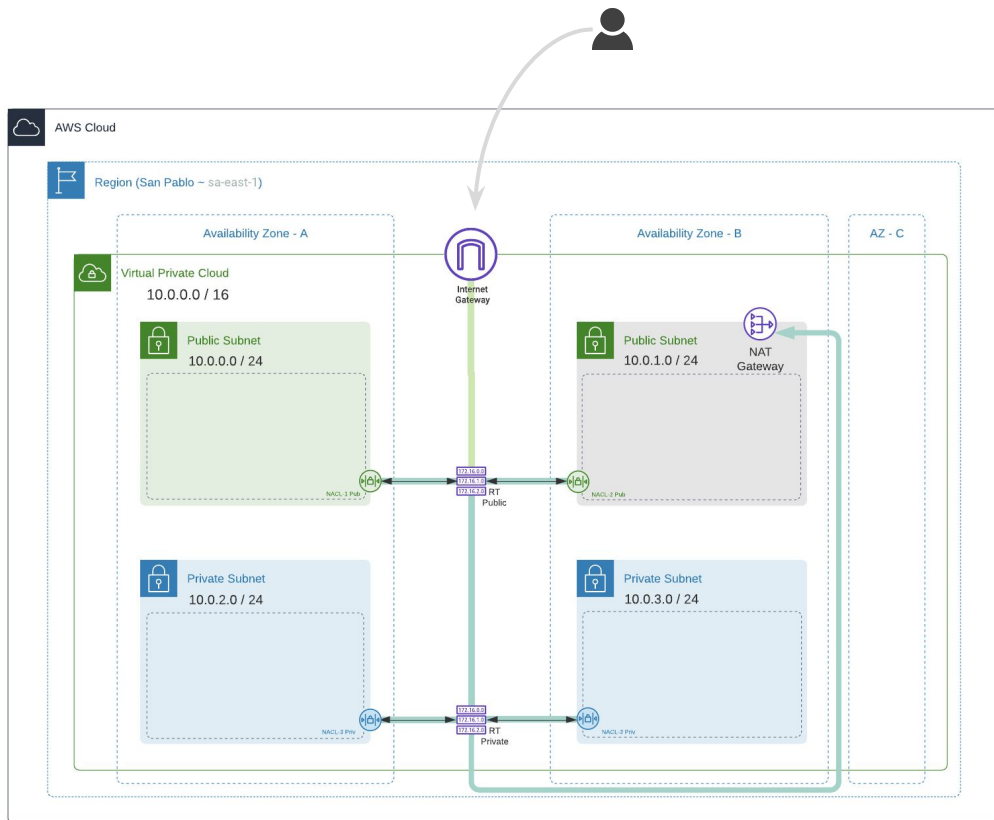
Auto-assign IPv4 [Info](#)

☒ 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

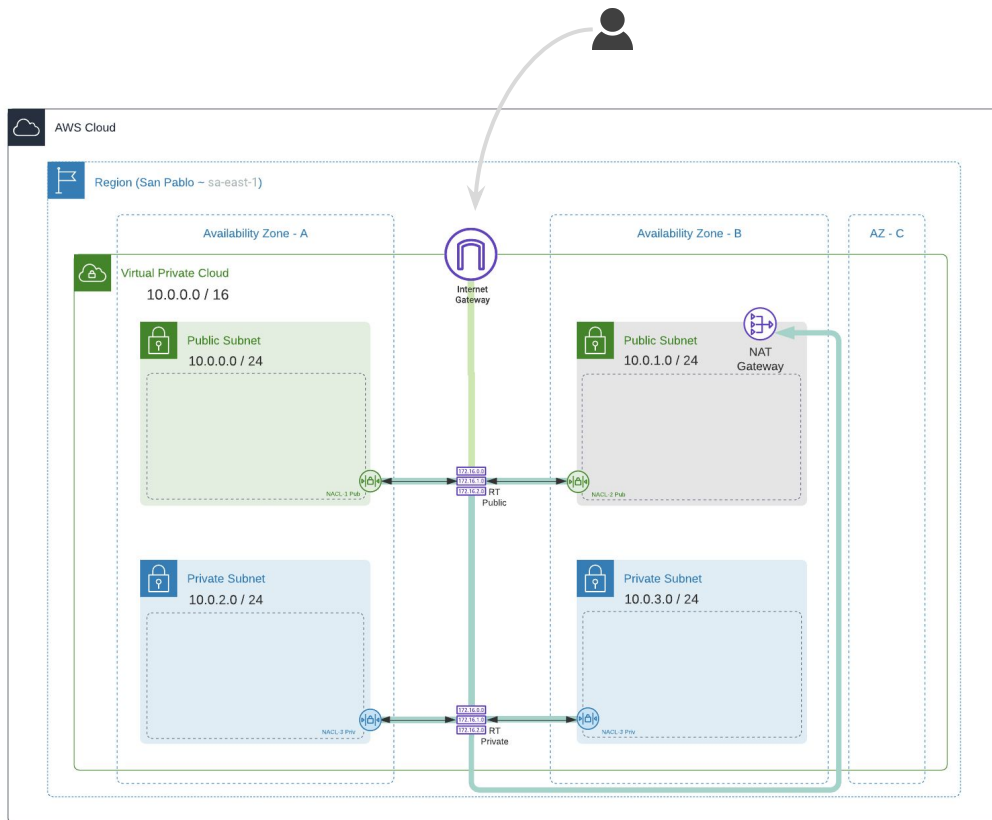
NACL-Public-A		Inbound rules			
Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	HTTP (80)	TCP (6)	80	0.0.0.0/0	 Allow
200	SSH (22)	TCP (6)	22	181.164.85.20/32	 Allow
300	Custom TCP	TCP (6)	1024 - 65535	0.0.0.0/0	 Allow
*	All traffic	All	All	0.0.0.0/0	 Deny
Outbound rules					
Rule number	Type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

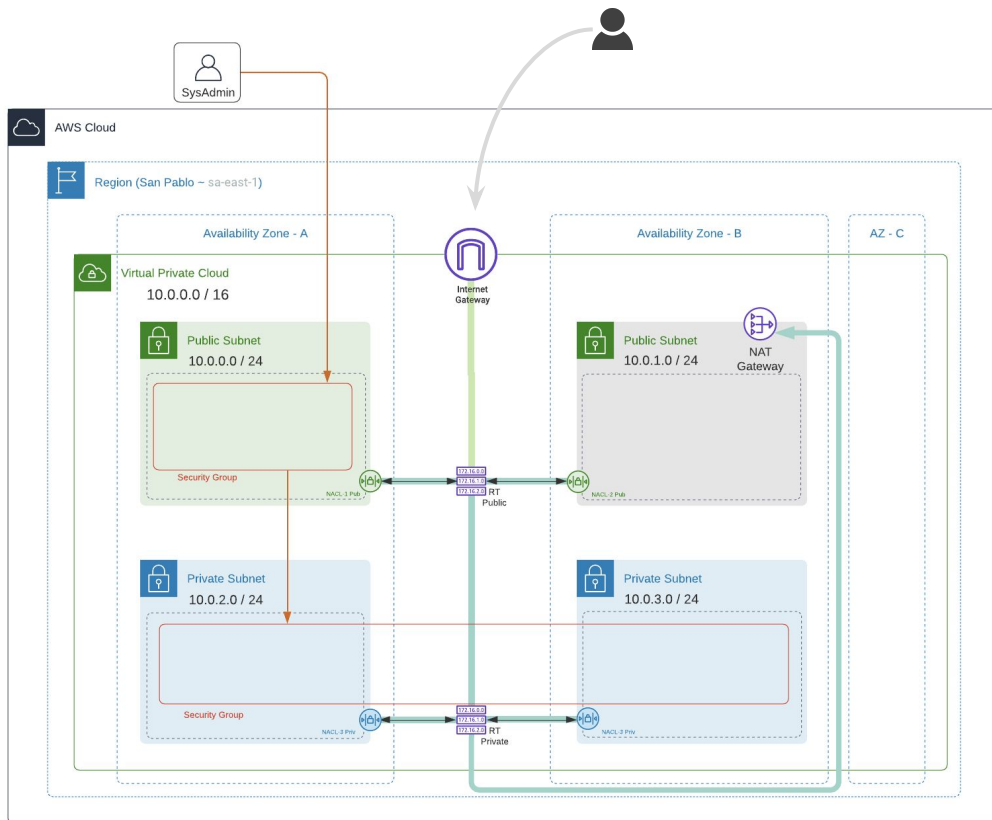
Caso de USO: Update SW. Privado por Nat Gwy

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-

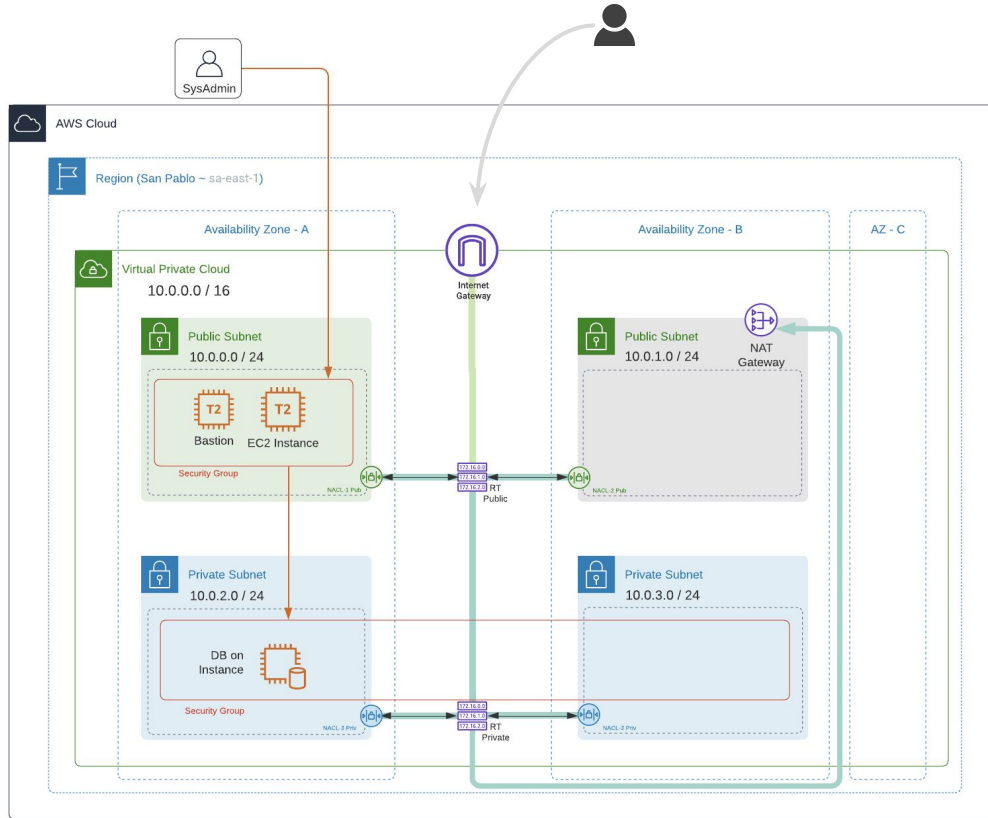
WebDMZ-SG				
Inbound rules				
Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	0.0.0.0/0	-
SSH	TCP	22	181.164.85.20/32	-
Custom TCP	TCP	1024 - 65535	0.0.0.0/0	User-Data Setup (yum update, git clone)
Outbound rules				
Type	Protocol	Port range	Destination	
All TCP	TCP	0 - 65535	0.0.0.0/0	

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

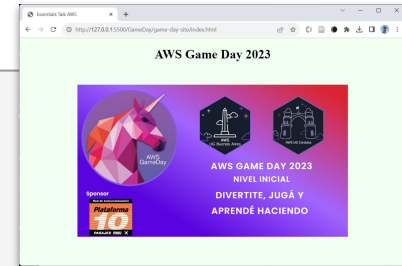
#-----
echo "<?php echo '<p>Hello PHP World</p>'; ?>" > /var/www/html/index.php

#-----
# 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





Unicorn.Rentals

ALB & ASG

Application Load Balancers
Auto Scaling Group

ALB - Target Group



aws

Services

Q

🔍

🔔

Oregon

Support

1. Configure Load Balancer

2. Configure Security Settings

3. Configure Security Groups

4. Configure Routing

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

ALB

Scheme

Internet-facing

Internal

IP address type

IPv4

Listeners

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

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

vpc-0de2d9601d863dccc5 (10.0.0.0/16) | lab-5

Availability Zones

us-west-2a

subnet-0ebffff0e3c68911c6 (lab-5 Subnet Public A)

IPv4 address

Assigned by AWS

us-west-2b

subnet-020d12c119078e011 (lab-5 Subnet Public B)

IPv4 address

Assigned by AWS

Cancel

Next: Configure Security Settings

aws

Services

Q

🔍

Search for services, features, marks (Optional)

Oregon

Support

1. Configure Load Balancer

2. Configure Security Settings

3. Configure Security Groups

Step 3: Configure Security Groups

A security group is a set of firewall rules that control the traffic to your load balancer. First, decide whether to create a new security group or select an existing one.

Assign a security group

Create a new security group

Select an existing security group

Security group name

ALB-SG

Description

ALB-SG

Type	Protocol	Port Range
HTTP	TCP	80

Add Rule

aws

Services

Q

🔍

🔔

cloud_user @ 2483-9375-4086

Oregon

Support

1. Configure Load Balancer

2. Configure Security Settings

3. Configure Security Groups

4. Configure Routing

5. Register Targets

Step 4: Configure Routing

Your load balancer routes requests to the targets in this target group using the protocol and port that you specify, and performs health checks on the targets using these health check settings. The target group you specify in this step will apply to all of the listeners configured on this load balancer; you can edit the listeners and add listeners after the load balancer is created.

Target group

Target group

New target group

Name

ALB-TG

Target type

Instance

IP

Lambda function

Protocol

HTTP

Port

80

Protocol version

HTTP1

HTTP2

gRPC

Send requests to targets using HTTP/1.1. Supported

Send requests to targets using HTTP/2. Supported

Send requests to targets using gRPC. Supported

Health checks

Protocol

HTTP

Path

/

Advanced health check settings

Port

traffic port

Override

Healthy threshold

2

Unhealthy threshold

2

Timeout

5

seconds

Interval

30

seconds

Success codes

200

Cancel

Previous

Next: Register Targets

aws

Services

Q

🔍

🔔

cloud_user @ 2483-9375-4086

Oregon

Support

1. Configure Load Balancer

2. Configure Security Settings

3. Configure Security Groups

4. Configure Routing

5. Register Targets

Step 5: Register Targets

Register targets with your target group. If you register a target in an enabled target group, requests to the targets as soon as the registration process completes and the target is healthy.

Registered targets

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

Remove

Instance

Name

Port

State

Security group

No instances available.

Load Balancer Creation Status

Successfully created load balancer

Load balancer ALB was successfully created.

Note: It might take a few minutes for your load balancer to be fully set up and ready to route traffic, and for the targets to complete the registration process and pass the initial health checks.

Suggested next steps

Discover other services that you can integrate with your load balancer. Visit the [Integrated services](#) tab within ALB.

Consider using [AWS Global Accelerator](#) to further improve the availability and performance of your application.

Launch Template



aws Services Oregon Support

EC2 launch templates

Streamline, simplify and standardize instance launches

Use launch templates to automate instance launches, simplify permission policies, and enforce best practices across your organization. Save launch parameters in managed services, including EC2 Auto Scaling, creating a new launch template version.

New launch template

Create launch template

Benefits and features

Streamline provisioning

Minimize steps to provision instances. With EC2 Auto Scaling, updates to a launch template can be automatically passed to an Auto Scaling group. [Learn more](#)

Governance

Ensure best practices are used across your organization. [Learn more](#)

Documentation

[Documentation](#)

[API reference](#)

aws Services cloud_user @ 2483-9375-4086 Oregon Support

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 at a later time. Templates can have multiple versions.

Launch template name and description

Launch template name - required

MyLT

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

Template version description

MyLT

Max 255 chars

Auto Scaling guidance

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

aws Services cloud_user @ 2483-9375-4086 Oregon Support

Launch template contents

Specify the details of your launch template below. Leaving a field blank will result in the field not being included in the launch template.

▼ **Amazon machine image (AMI) - required**

AMI - required

Amazon Linux 2 AMI (HVM, SSD Volume Type)

ami-0518bb0e75d3619ca

Catalog: Quick Start virtualization: hvm architecture: 64-bit (x86)

▼ **Instance type**

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory

Free tier eligible

▼ **Key pair (login)**

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

Key pair name

lab-vpc12-oregon-borrame

▼ **Network settings**

Networking platform

Virtual Private Cloud (VPC)

Launch into a virtual network in your own account, logically isolated area within the AWS cloud

EC2-Classical

Launch into a simple network that shares with other instances in the same VPC

Security groups

Select security groups

Web-DMZ-SG sg-084053d03351a111e

VPC: vpc-0de2d9601d863d0c5

▼ **Advanced details**

User data

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

cd /var/www/html
echo "Hello!" > index.html

git clone https://github.com/Pabloin/AWS-Essentials.git
unzip AWS-Essentials/c-site-glacier/lab-02/site-glacier-lab-02.zip
cp -r lab-02/site/* /var/www/html/
```

☐ User data has already been base64 encoded

Cancel Create launch template

EC2 > Launch templates > Create launch template

Success

Successfully created MyLT (lt-0e2e4b987e8239fb7)

► Actions log

Auto Scaling Group



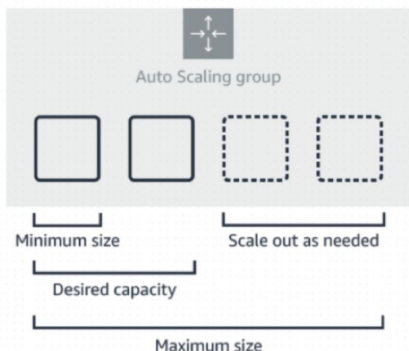
Amazon EC2 Auto Scaling helps maintain the availability of your applications

Create Auto Scaling group

Get started with EC2 Auto Scaling by creating an Auto Scaling group.

Create Auto Scaling group

How it works



aws Services Oregon Support

EC2 > ... > Create Auto Scaling group

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.

MyASG

Must be unique to 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.

Select a launch template

Search launch templates

MyLaunchTemplate

Cancel Next

aws Services cloud_user @ 1031-1549-1239 Oregon Support

Configure settings [info](#)

Configure the settings below. Depending on whether you chose a launch template, these settings may include options to help you make optimal use of EC2 resources.

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-073d17162ae8d04a2 (lab14)
10.0.0.0/16

Create a VPC

Subnets

Select subnets

us-west-2a | subnet-03548b4d31aecfb3 (lab14 Subnet Public A)
10.0.0.0/24

us-west-2b | subnet-0afd1a1f3ffe181e2 (lab14 Subnet Public B)
10.0.1.0/24

Create a subnet

Cancel Previous Skip to review Next

Auto Scaling Group



Configure advanced options [Info](#)

Choose a load balancer to distribute incoming traffic for your application across instances to make it more reliable and easily scalable. You can also set options that give you more control over health check replacements and monitoring.

Load balancing - optional [Info](#)

Use the options below to attach your Auto Scaling group to an existing load balancer, or to a new load balancer that you define.

☐ No load balancer

Traffic to your Auto Scaling group will not be fronted by a load balancer.

☒ Attach to an existing load balancer

Choose from your existing load balancers.

☐ Attach to a new load balancer

Quickly create a basic load balancer to attach to your Auto Scaling group.

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

MyTG | HTTP
Application Load Balancer: MyALB

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

Additional settings - optional

Monitoring [Info](#)

☐ Enable group metrics collection within CloudWatch

Cancel

Previous

Skip to review

Next

Configure group size and scaling policies [Info](#)

Set the desired, minimum, and maximum capacity of your Auto Scaling group. You can optionally add a scaling policy to dynamically scale the number of instances in the group.

Group size - optional [Info](#)

Specify the size of the Auto Scaling group by changing the desired capacity. You can also specify minimum and maximum capacity limits. Your desired capacity must be within the limit range.

Desired capacity

2

Minimum capacity

1

Maximum capacity

5

Scaling policies - optional

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

30

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



Muchos Éxitos!!!

