



Faculty of Mathematical, Physical and
Natural Sciences of Tunis

Faculté des Sciences Mathématiques,
Physiques et Naturelles de Tunis

كلية العلوم للرياضيات
والفيزياء والطبيعتين بتونس

AWS Project



Realized by : Oussama Maaroufi

Plan :

I. Introduction

II. Steps :

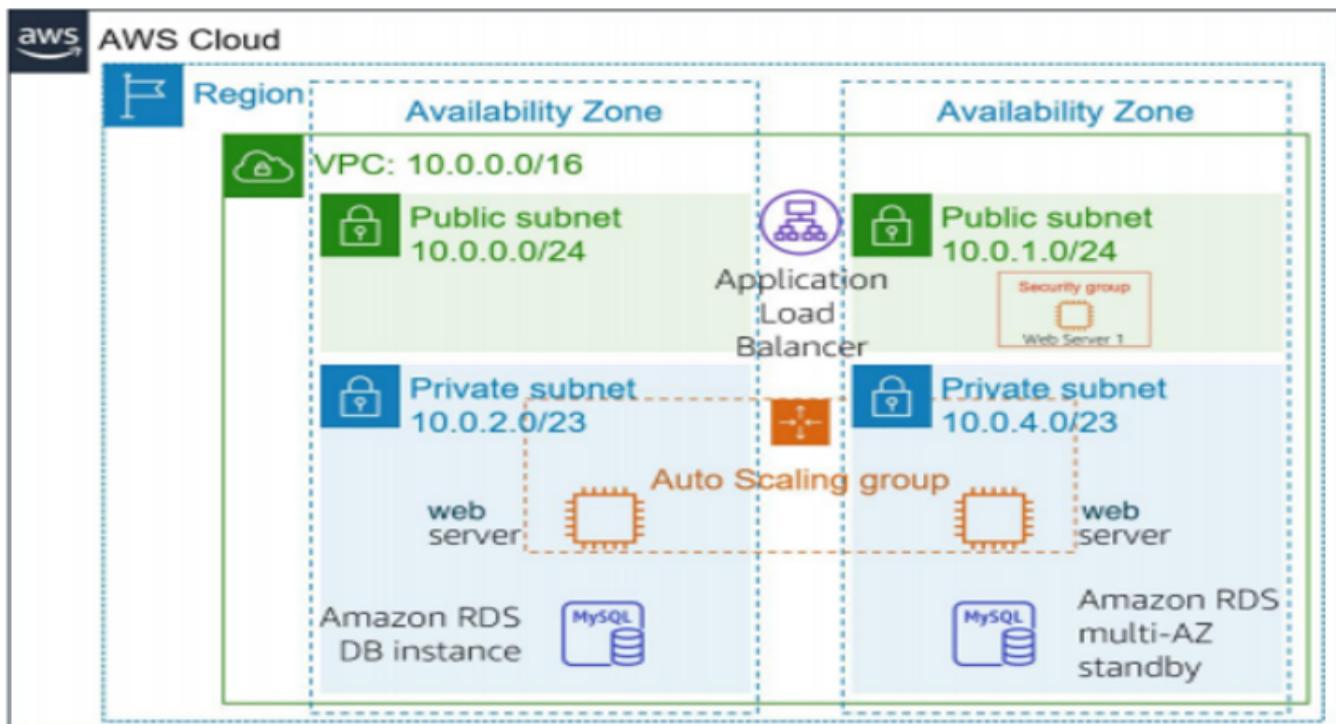
- i. Create the VPC for our project
- ii. Create Public/Private Subnets:
- iii. Overview about Route Table
- iv. Create and Attach Internet Gateway
- v. Create a Route Table for the public subnets
- vi. Create NAT Gateways
- vii. Create Security Groups
- viii. Create a LoadBalancer
- ix. Create an autoscaling group
- x. Create Database Instance RDS - MYSQL
- xi. Deploy A React App In EC2 Instance
- xii. Create Machine Bastion

III. Conclusion

I. Introduction

High availability (HA) is the elimination of single points of failure to enable applications to continue to operate even if one of the IT components it depends on, such as a server, fails . So in this project we decided to create a height-available architecture using AWS services such as EC2, RDS , Auto Scaling Group Application Load Balancer ,Vpc etc .

The Architecture that we want to build is shown below



II. Steps

Step 1: Create the VPC for our project

Firstly from the management console, we verify the region that we are currently in and where we want to launch this VPC. We are currently in the **us-east-1** northern Virginia region.

Navigate to VPC in the AWS console. Click “Create VPC.” Choose “VPC only” and we enter an optional name tag. Name tags are useful to help keep our projects organized. We choose the IPv4 CIDR block. I have chosen to manually enter a CIDR block of 10.0.0.0/16. Adjust tenancy and tags as desired, then click “Create VPC.”

VPC > Your VPCs > Create VPC

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

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.
my-vpc

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	Remove
<input type="text" value="Name"/> X	<input type="text" value="my-vpc"/> X	Remove
Add new tag		
You can add 49 more tags.		

Cancel Create VPC

✓ You successfully created vpc-0f36022490de29f6d / my-vpc X

VPC > Your VPCs > vpc-0f36022490de29f6d

vpc-0f36022490de29f6d / my-vpc

Actions ▾

Details		Info	
VPC ID vpc-0f36022490de29f6d	State Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-057e99d94cf322a88	Main route table rtb-01d8a5ef1fac61e21	Main network ACL acl-042635045392119d
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool -	IPv6 CIDR (Network border group) -
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups Failed to load rule groups	Owner ID 278484320774	

CIDRs Flow logs Tags

CIDRs		Info	
Address type	CIDR	Network Border Group	Status
IPv4	10.0.0.0/16	-	Associated

Step 2: Create Public/Private Subnets

Now let's create two public subnets with the following CIDR blocks: **10.0.0.0/24**, **10.0.1.0/24**. These will be created within two different availability zones and two private subnets with following CIDR Blocks: **10.0.2.0/23**, **10.0.4.0/23**.

By creating multiple subnets across multiple availability zones, we increase **reliability** and **availability**. In the VPC console, on the left side menu, select “Subnets,” then click the orange “Create subnet” button. We want to create subnets within the VPC that we created in Step 1, so we choose that VPC from the drop down menu.

Create subnet [Info](#)

VPC

VPC ID

Create subnets in this VPC.



Associated VPC CIDRs

IPv4 CIDRs

10.0.0.0/16

We are able to create all four subnets at the same time, and they will be created within the VPC above. Enter the names of the new subnets and their IPv4 CIDR block information. Choose a different availability zone for each subnet.

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 4

Subnet name

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

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.



IPv4 CIDR block [Info](#)



▼ Tags - optional

Key

Value - optional

You can add 49 more tags.

Subnet 2 of 4

Subnet name

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

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.



IPv4 CIDR block [Info](#)



▼ Tags - optional

Key



Value - optional



You can add 49 more tags.

Subnet 3 of 4

Subnet name

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

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.



IPv4 CIDR block [Info](#)



▼ Tags - optional

Key



Value - optional



You can add 49 more tags.

Subnet 4 of 4

Subnet name

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

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.



IPv4 CIDR block Info



▼ Tags - optional

Key

Value - optional



You can add 49 more tags.

⌚ You have successfully created 4 subnets: subnet-018529334702628c5, subnet-0dde70a44df6605ec, subnet-077e8589a9c78622d, subnet-02d379562ed92c18f 

Subnets (4) Info



<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addr...	
<input type="checkbox"/>	public-subnet1	subnet-018529334702628c5		vpc-0f36022490de29f...	10.0.0.0/24	-	251	
<input type="checkbox"/>	private-subnet1	subnet-077e8589a9c78622d		vpc-0f36022490de29f...	10.0.2.0/23	-	507	
<input type="checkbox"/>	public-subnet2	subnet-0dde70a44df6...		vpc-0f36022490de29f...	10.0.1.0/24	-	251	
<input type="checkbox"/>	private-subnet2	subnet-02d379562ed...		vpc-0f36022490de29f...	10.0.4.0/23	-	507	

Select a subnet

Step 3: Overview about Route Table

When we create a VPC it automatically comes with a main (or default) route table that is responsible for directing network traffic. We can create a custom route table if desired, and associate subnets to the custom route table. If we do not manually associate the subnets to a custom route table, they will be automatically associated to the main route table. Routes in the table have both a destination and a target.

The target is typically the internet gateway that is associated with our VPC for public subnets and local for private subnets. For the example above, if we select “Route tables” from the left side menu in the VPC console, we will see my default route table with the VPC we created previously. The default Route Table :

The screenshot shows the AWS VPC Route Tables page. At the top, there is a search bar with the value "vpc-0f36022490de29f6d" and a "Clear filters" button. Below the search bar is a table with the following columns: Name, Route table ID, Explicit subnet a..., Edge associati..., Main, VPC, and Owner ID. There is one row selected, showing "rtb-01d8a5ef1fac61e21" as the Route table ID, "vpc-0f36022490de29f6d" as the VPC, and "Yes" as the Main status. The table has a header row with sorting icons and a "Create route table" button at the top right.

Below the table, a modal window titled "rtb-01d8a5ef1fac61e21" is open, showing the "Routes" tab. It contains a table with columns: Destination, Target, Status, and Propagated. One row is listed: "10.0.0.0/16" with "local" as the target, "Active" as the status, and "No" as the propagated status. Other tabs in the modal include "Details", "Subnet associations", "Edge associations", "Route propagation", and "Tags".

If we click on “Subnet associations,” we can see that the four subnets we created within the VPC are automatically associated with this default route table, which has a local target.

The screenshot shows the "Subnet associations" tab for the route table "rtb-01d8a5ef1fac61e21". The tab bar includes "Details", "Routes", "Subnet associations" (which is active), "Edge associations", "Route propagation", and "Tags". Below the tab bar, a section titled "Explicit subnet associations (0)" is shown. A note says "No subnet associations" and "You do not have any subnet associations." There is a "Edit subnet associations" button at the top right of this section.

Subnets without explicit associations (4)			
The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:			
Edit subnet associations			
<input type="text" value="Find subnet association"/> < 1 > @			
Subnet ID	IPv4 CIDR	IPv6 CIDR	
subnet-018529334702628c5 / public-subnet1	10.0.0.0/24	-	
subnet-077e8589a9c78622d / private-subnet1	10.0.2.0/23	-	
subnet-0dde70a44df6605ec / public-subnet2	10.0.1.0/24	-	
subnet-02d379562ed92c18f / private-subnet2	10.0.4.0/23	-	

As we see above the default route table only contains one route with target locale and that means that there is no internet traffic available which indicates that our subnets are private by default .

So what we need to do is create another route table with a route that has an internet gateway as its target and associate public subnets to it and keep private subnets associated to main route table ., But first let's Create an Internet gateway and attach it to our VPC .

Step 4 : Create and Attach Internet Gateway

In order to allow resources in your VPC to communicate with the internet, you must create and attach an internet gateway. To do this, navigate to “Internet gateways” on the left side menu in the VPC console. Then select “Create internet gateway.”

VPC > Internet gateways > Create internet gateway

Create internet gateway Info

An internet gateway is a virtual router 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
Creates a tag with a key of 'Name' and a value that you specify.

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.

Key	Value - optional	
<input type="text" value="Name"/>	<input type="text" value="Project-IGW"/>	<input type="button" value="Remove"/>
<input type="button" value="Add new tag"/>		

You can add 49 more tags.

The following internet gateway was created: igw-08a3115a4d65df7ca - Project-IGW. You can now attach to a VPC to enable the VPC to communicate with the internet.

Attach to a VPC

VPC > Internet gateways > igw-08a3115a4d65df7ca / Project-IGW

Actions ▾

Details [Info](#)

Internet gateway ID igw-08a3115a4d65df7ca	State Detached	VPC ID -	Owner 278484320774
--	-------------------	-------------	-----------------------

Tags

Manage tags

Key	Value
Name	Project-IGW

After we created an internet gateway, we need to attach it to the VPC we want to use. We will attach it to the VPC we created earlier. Click the “Attach to a VPC” button, then use the down arrow to select the VPC we created earlier. Click “Attach internet gateway.”

VPC > Internet gateways > Attach to VPC (igw-08a3115a4d65df7ca)

Attach to VPC (igw-08a3115a4d65df7ca) [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.

 X

▶ AWS Command Line Interface command

Cancel Attach internet gateway

Internet gateway igw-08a3115a4d65df7ca successfully attached to vpc-0f36022490de29f6d

VPC > Internet gateways > igw-08a3115a4d65df7ca

igw-08a3115a4d65df7ca / Project-IGW

Actions ▾

Details	Info
---------	------

Internet gateway ID: igw-08a3115a4d65df7ca State: Attached VPC ID: vpc-0f36022490de29f6d | my-vpc Owner: 278484320774

Tags

Key	Value
Name	Project-IGW

Manage tags < 1 > ⚙

After attaching the internet gateway to our VPC, I should be able to see it listed under “Internet Gateways”.

Internet gateway igw-08a3115a4d65df7ca successfully attached to vpc-0f36022490de29f6d

Internet gateways (2) Info

Filter internet gateways

Name	Internet gateway ID	State	VPC ID	Owner
-	igw-019dc6676d9eb7ef9	Attached	vpc-0070a31bcad985080	278484320774
Project-IGW	igw-08a3115a4d65df7ca	Attached	vpc-0f36022490de29f6d m...	278484320774

and now we are ready to create the Route Table

Step 5 : Create a Route Table for the public subnets

On the VPC console menu select *route table* and *create route table*. Name the route table and select our custom VPC to place it in.

VPC > Route tables > Create route table

Create route table Info

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. <input type="text" value="publicRT"/>
VPC The VPC to use for this route table. <input type="text" value="vpc-0f36022490de29f6d (my-vpc)"/>

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	Remove
<input type="text" value="Name"/> X	<input type="text" value="publicRT"/> X	Remove

Add new tag

You can add 49 more tags.

Cancel Create route table

Route table rtb-095c0433efcb2947c | publicRT was created successfully. X

VPC > Route tables > rtb-095c0433efcb2947c

rtb-095c0433efcb2947c / publicRT

Actions ▾

ⓘ You can now check network connectivity with Reachability Analyzer Run Reachability Analyzer X

Details	Info
Route table ID rtb-095c0433efcb2947c	Main No
VPC vpc-0f36022490de29f6d my-vpc	Owner ID 278484320774
	Explicit subnet associations -
	Edge associations -

Now that we have created our public route table we need to create a **Public Route** for it. Select our Public route table and select the *routes tab*, then select *edit routes*.

Select *add route* For the destination select **0.0.0.0/0**. The destination of our public route will be to the public internet.

Under *target* select Internet gateway and select our custom **internet gateway** that we created earlier, save these changes.

Routes	Subnet associations	Edge associations	Route propagation	Tags
Routes (1)				
<input type="text" value="Filter routes"/> Both				
Destination	Target	Status	Propagated	
10.0.0.0/16	local	Active	No	

VPC > Route tables > rtb-095c0433efcb2947c > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-08a3115a4d65df7ca (Project-IGW)	-	No

Add route Cancel

Routes	Subnet associations	Edge associations	Route propagation	Tags
Routes (2)				
<input type="text" value="Filter routes"/> Both				
Destination	Target	Status	Propagated	
0.0.0.0/0	igw-08a3115a4d65df7ca	Active	No	
10.0.0.0/16	local	Active	No	

Now we will associate our route table with our public subnets.

Select *subnet associations* and then *edit subnet associations*. Select two public subnets and *save associations*.

VPC > Route tables > rtb-095c0433efcb2947c > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/4)						
	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID	
<input checked="" type="checkbox"/>	public-subnet1	subnet-018529334702628c5	10.0.0.0/24	-	Main (rtb-01d8a5ef1fac61e21)	
<input type="checkbox"/>	private-subnet1	subnet-077e8589a9c78622d	10.0.2.0/23	-	Main (rtb-01d8a5ef1fac61e21)	
<input checked="" type="checkbox"/>	public-subnet2	subnet-Odde70a44df6605ec	10.0.1.0/24	-	Main (rtb-01d8a5ef1fac61e21)	
<input type="checkbox"/>	private-subnet2	subnet-02d379562ed92c18f	10.0.4.0/23	-	Main (rtb-01d8a5ef1fac61e21)	

Selected subnets

subnet-018529334702628c5 / public-subnet1 subnet-Odde70a44df6605ec / public-subnet2

Cancel

You have successfully updated subnet associations for rtb-095c0433efcb2947c / publicRT.

Route table ID rtb-095c0433efcb2947c	Main No	Explicit subnet associations 2 subnets	Edge associations -
VPC vpc-0f36022490de29f6d my-vpc	Owner ID 278484320774		

Routes Subnet associations Edge associations Route propagation Tags

Explicit subnet associations (2)

Explicit subnet associations (2)			
Edit subnet associations			
Find subnet association		< 1 > ⚙	
Subnet ID	IPv4 CIDR	IPv6 CIDR	
subnet-018529334702628c5 / public-subnet1	10.0.0.0/24	-	
subnet-0dde70a44df6605ec / public-subnet2	10.0.1.0/24	-	

so now we have associated our public subnets to newly created Route Table and for private subnets they remain associated with the main Route Table as it's displayed below .

Route tables (1/2) Info

Filter route tables

search: vpc-0f36022490de29f6d X Clear filters

Name	Route table ID	Explicit subnet a...	Edge associ...	Main	VPC	Owner ID
publicRT	rtb-095c0433efcb...	2 subnets	-	No	vpc-0f36022490de29f...	278484320774
-	rtb-01d8a5ef1fac6...	-	-	Yes	vpc-0f36022490de29f...	278484320774

No subnet associations
You do not have any subnet associations.

Subnets without explicit associations (2)

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Subnets without explicit associations (2)			
Edit subnet associations			
Find subnet association			
Subnet ID	IPv4 CIDR	IPv6 CIDR	
subnet-077e8589a9c78622d / private-subnet1	10.0.2.0/23	-	
subnet-02d379562ed92c18f / private-subnet2	10.0.4.0/23	-	

Step 6 : Create NAT Gateways

we need to create Nat Gateway and modify Main Route Table to allow patching and updating to our Ec2 instances that are launched in the private subnets

Create NAT gateway Info

A highly available, managed Network Address Translation (NAT) service that instances in private subnets can use to connect to services in other VPCs, on-premises networks, or the internet.

NAT gateway settings

Name - optional

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

Project-NAT-GW

The name can be up to 256 characters long.

Subnet

Select a subnet in which to create the NAT gateway.

subnet-018529334702628c5 (public-subnet1)



Connectivity type

Select a connectivity type for the NAT gateway.

Public

Private

Elastic IP allocation ID Info

Assign an Elastic IP address to the NAT gateway.

Select an Elastic IP



Allocate Elastic IP

As we see we Need to Allocate an Elastic Ip for our Nat Gateway

Elastic IP allocation ID Info

Assign an Elastic IP address to the NAT gateway.

eipalloc-0ad5ab56496661064



Allocate Elastic IP

NAT gateway nat-055389c17ffdd4f4d | Project-NAT-GW was created successfully.

VPC > NAT gateways > nat-055389c17ffdd4f4d

nat-055389c17ffdd4f4d / Project-NAT-GW

[Delete](#)

Details		Info	
NAT gateway ID nat-055389c17ffdd4f4d	Connectivity type Public	State Pending	State message -
NAT gateway ARN arnawssec2us-east-1:278484320774:natgateway/nat-055389c17ffdd4f4d	Elastic IP address -	Primary private IPv4 address -	Network Interface ID -
VPC vpc-0f36022490de29f6d / my-vpc	Subnet subnet-018529334702628c5 / public-subnet1	Created Monday, December 26, 2022 at 23:01:46 GMT+1	Deleted -

Now we Need to update the main route table which has private subnets associated with it by adding a new route with target nat gateway when the destination is the internet .

Choose the main route table and select edit routes

Route tables (1/2) [Info](#)

[Filter route tables](#)

search: vpc-0f36022490de29f6d [X](#) [Clear filters](#)

Name	Route table ID	Explicit subnet a...	Edge associ...	Main	VPC	Owner ID
publicRT	rtb-095c0433efcb...	2 subnets	-	No	vpc-0f36022490de29f...	278484320774
-	rtb-01d8a5ef1fac6...	-	-	Yes	vpc-0f36022490de29f...	278484320774

add a route with destination internet and target nat gateway

VPC > Route tables > rtb-01d8a5ef1fac61e21 > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	<input type="text" value="local"/> X Active	No	
0.0.0.0/0	<input type="text" value="nat-055389c17ffdd4f4d"/> X -	No	Remove
Add route			

[Cancel](#) [Preview](#) [Save changes](#)

Step 7 : Create Security Groups

The security group will be attached to the Application load balancer. The security group needs to allow inbound HTTP and HTTPS traffic from 0.0.0.0/0 the public internet .

EC2 > Security Groups > Create security group

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info
ALB-SG
Name cannot be edited after creation.

Description Info
Security Group for Application Load Balancer

VPC Info
Q vpc-0f36022490de29f6d

Inbound rules Info

Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Source <small>Info</small>	Description - optional <small>Info</small>
HTTP	TCP	80	Anywhere... ▾ 0.0.0.0/0 X	
HTTPS	TCP	443	Anywhere... ▾ 0.0.0.0/0 X	

Add rule

Outbound rules Info

Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Destination <small>Info</small>	Description - optional <small>Info</small>
All traffic	All	All	Custom ▾ 0.0.0.0/0 X	

Add rule

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.

Key	Value - optional
Q Name	Q ALB-SG X Remove

Add new tag
You can add up to 49 more tags

Cancel Create security group

⌚ Security group (sg-04fe1ee3376da2239 | ALB-SG) was created successfully X

EC2 > Security Groups > sg-04fe1ee3376da2239 - ALB-SG

sg-04fe1ee3376da2239 - ALB-SG Actions ▾

Details

Security group name ALB-SG	Security group ID sg-04fe1ee3376da2239	Description Security Group for Application Load Balancer	VPC ID vpc-0f36022490de29f6d
Owner 278484320774	Inbound rules count 2 Permission entries	Outbound rules count 1 Permission entry	

We need also to create a security group for instances that have our web app running on it .

Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [Info](#)
Web-App-SG
Name cannot be edited after creation.

Description [Info](#)
Security Group to allow traffic only from ALB-SG

VPC [Info](#)
vpc-0f36022490de29f6d

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info
HTTP	TCP	80	Custom	sg-04fe1ee3376da2239 X
HTTPS	TCP	443	Custom	sg-04fe1ee3376da2239 X

[Add rule](#)

Outbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Destination Info	Description - optional Info
All traffic	All	All	Custom	0.0.0.0/0 X

[Add rule](#)

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.

Key	Value - optional
Q Name	Web-App-SG X Remove

[Add new tag](#)
You can add up to 49 more tags

[Cancel](#) [Create security group](#)

EC2 > Security Groups > sg-0b0fdbbeae61fff60 - Web-App-SG [Actions](#)

sg-0b0fdbbeae61fff60 - Web-App-SG

Details

Security group name Web-App-SG	Security group ID sg-0b0fdbbeae61fff60	Description Security Group to allow traffic only from ALB-SG	VPC ID vpc-0f36022490de29f6d
Owner 278484320774	Inbound rules count 2 Permission entries	Outbound rules count 1 Permission entry	

Also we need to create a security for db instance to allow only the traffic coming from Web-App-SG the security group of our web app .

EC2 > Security Groups > Create security group

Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [Info](#)
Mysql-SG
Name cannot be edited after creation.

Description [Info](#)
Allow access only from Security group that contain web app

VPC [Info](#)
vpc-0f36022490de29f6d

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info
MySQL/Aurora	TCP	3306	Custom	sg-0b0fbdbae61fff60 X

Add rule

Success message: Security group (sg-0ac438cc3b566b317 | Mysql-SG) was created successfully [Details](#)

EC2 > Security Groups > sg-0ac438cc3b566b317 - Mysql-SG [Actions ▾](#)

Details

Security group name Mysql-SG	Security group ID sg-0ac438cc3b566b317	Description Allow access only from Security group that contain web app	VPC ID vpc-0f36022490de29f6d
Owner 278484320774	Inbound rules count 1 Permission entry	Outbound rules count 0 Permission entries	

Step 8 : Create a LoadBalancer

Application Load Balancers distributes incoming application traffic across multiple targets, such as EC2 instances, in multiple Availability Zones. This increases the availability of your application.

From the EC2 Dashboard, left side menu, scroll down and click *Load Balancers*, *Create Load Balancer*.

EC2 > Load balancers

Load balancers

Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

Name	DNS name	State	VPC ID	Availability Zones	Type	Created At
No load balancers						
You don't have any load balancers in us-east-1						
Create load balancer						

Name our ALB. Select *Internet facing*. Select *IPv4*. Select your VPC. Then We select each Subnet that We want the ALB to distribute the load between.

Load balancer types

<p>Application Load Balancer Info</p> <p>Choose an Application Load Balancer when you need a flexible feature set for your 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> <p>Create</p>	<p>Network Load Balancer Info</p> <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 applications. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.</p> <p>Create</p>	<p>Gateway Load Balancer Info</p> <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> <p>Create</p>
<p>► Classic Load Balancer - previous generation</p> <p>Close</p>		

Choose the type Application load balancer and we make the Load Balancer span in two subnets

The screenshot shows the 'Network mapping' section of the AWS CloudFormation template editor. It includes fields for selecting a VPC (my-vpc) and defining mappings for two Availability Zones (us-east-1a and us-east-1b), each associated with a specific subnet and IPv4 settings.

VPC | [Info](#)
Select the virtual private cloud (VPC) for your targets. Only VPCs with an internet gateway are enabled for selection. The selected VPC cannot be changed after the load balancer is created. To confirm the VPC for your targets, view your [target groups](#).

Mappings | [Info](#)
Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability Zones that are not supported by the load balancer or the VPC are not available for selection.

Subnet
subnet-018529334702628c5 public-subnet1

IPv4 settings
Assigned by AWS

Subnet
subnet-Odde70a44df6605ec public-subnet2

IPv4 settings
Assigned by AWS

Select the security group for our load balancer to allow inbound traffic coming from the internet because our LB is internet facing not internal LB .

The screenshot shows the 'Security groups' section of the AWS CloudFormation template editor. It lists the selected security group (ALB-SG) and provides options to select up to 5 security groups or create a new one.

Security groups | [Info](#)
A security group is a set of firewall rules that control the traffic to your load balancer.

Security groups
Select up to 5 security groups
Create new security group

ALB-SG sg-0fe1ee3376da2239 X
VPC: vpc-0f36022490de29f6d

Scroll down and under *Listeners and routers* select *HTTP, port 80*, we do not yet have a Target Group, so we will create one from here.

Each target group is used to route requests to one or more registered targets. When we create each listener rule, we specify a target group and conditions

Click *create target group*.

Choose your target type as *instances* and name your target group.

The screenshot shows the 'Listeners and routing' configuration for a load balancer. It displays a single listener named 'Listener HTTP:80' with the following settings:

- Protocol:** HTTP
- Port:** 80
- Default action:** Forward to 'Select a target group'
- Create target group:** A blue link.

Below the listener settings, there is a section for 'Listener tags - optional' with a note about adding tags for categorization. There is also a 'Add listener tag' button and a note that you can add up to 50 more tags.

Specify group details

Your load balancer routes requests to the targets in a target group and performs health checks on the targets.

Basic configuration

Settings in this section cannot be changed after the target group is created.

Choose a target type

Instances

- Supports load balancing to instances within a specific VPC.
- Facilitates the use of [Amazon EC2 Auto Scaling](#) to manage and scale your EC2 capacity.

IP addresses

- Supports load balancing to VPC and on-premises resources.
- Facilitates routing to multiple IP addresses and network interfaces on the same instance.
- Offers flexibility with microservice based architectures, simplifying inter-application communication.
- Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.

Lambda function

- Facilitates routing to a single Lambda function.
- Accessible to Application Load Balancers only.

Application Load Balancer

- Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
- Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.

Give our target group a name and set the protocol to HTTP port 80.

Select our VPC, select protocol version HTTP1 and click next.

Target group name

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Protocol **Port**

HTTP	:	80
------	---	----

VPC
Select the VPC with the instances that you want to include in the target group.

vpc-0f36022490de29f6d
IPv4: 10.0.0.0/16

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.

Register targets

This is an optional step to create a target group. However, to ensure that your load balancer routes traffic to this target group you must register your targets.

Available instances (0)

Instance ID	Name	State	Security groups	Zone	Subnet ID
No Available Instances					

Ports for the selected instances
Ports for routing traffic to the selected instances.

1-65535 (separate multiple ports with commas)

Review targets

Targets (0)

All	Q Filter resources by property or value	Remove all pending						
Remove	Health status	Instance ID	Name	Port	State	Security groups	Zone	Subnet ID
No instances added yet								
Specify instances above, or leave the group empty if you prefer to add targets later.								

0 pending

Cancel Previous Create target group

then click the button Create target group .

Now turn back to the screen to continue configuring our load balancer .

Listeners and routing Info

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

▼ Listener HTTP:80

Protocol	Port	Default action	Info
HTTP	: 80	Forward to ALB-TG	HTTP
Target type: Instance, IPv4			
Create target group			

Listener tags - optional
Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.

[Add listener tag](#)
You can add up to 50 more tags.

[Add listener](#)

as we see our load balancer is created successfully as shown below

EC2 > Load balancers

Load balancers (1)
Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

<input type="checkbox"/>	Name	DNS name	State	VPC ID	Availability Zones	Type	Created At
<input type="checkbox"/>	Project-ALB	Project-ALB-1792821405.us-east-1.elb.amazonaws.com	Provisioning	vpc-0f36022490de29f6d	2 Availability Zones	application	December 26, 2022, 15:37 (UTC+01:00)

[Actions](#) [Create load balancer](#)

Step 9 : Create an autoscaling group

To help your instances adjust in response to demand, you have the option to create an auto scaling group. This can be done in the EC2 console via “Auto scaling groups” on the left side menu. When creating the auto scaling group, you must first choose a launch template, which is a saved instance configuration that includes an AMI, instance type, key pair, security group, and any user data that you want to be executed upon launch of the instance. If you don’t already have a launch template, you should create a new one prior to creating the auto scaling group. The launch template creation is a bit lengthy, but starts with selecting “Launch Templates” on the left side menu in the EC2 console.

First let’s create a launch template :

Click the orange “**Create launch template**” button and get started by choosing a launch template name and selecting an AMI. Below I have selected an Amazon Linux 2 AMI with 64 bit architecture.

The screenshot shows the 'Create launch template' wizard in the AWS EC2 console. The top navigation bar shows 'EC2 > Launch templates > Create launch template'. The main title is 'Create launch template'. A sub-instruction says '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.' The first step is 'Launch template name and description'. It has a 'Launch template name - required' field containing 'Project-LT', a note that it must be unique to the account and max 128 chars, and a 'Template version description' field containing 'project launch template' with a note of max 255 chars. The second step is 'Auto Scaling guidance'. It has an 'Info' link, a note to select it if using with Auto Scaling, and a checked checkbox for 'Provide guidance to help me set up a template that I can use with EC2 Auto Scaling'. The third step is partially visible with 'Template tags' and 'Source template' options.

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*

Project-LT

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

Template version description

project launch template

Max 255 chars

Auto Scaling guidance [Info](#)

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](#)

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.

▼ Application and OS Images (Amazon Machine Image) - required [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

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

Quick Start



Amazon
Linux



macOS



Ubuntu



Windows



Red Hat



[Browse more AMIs](#)

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type Free tier eligible

ami-0b5eea76982371e91 (64-bit (x86)) / ami-03a45a5ac837f33b7 (64-bit (Arm))

Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2 Kernel 5.10 AMI 2.0.20221210.1 x86_64 HVM gp2

Architecture

AMI ID

64-bit (x86)

ami-0b5eea76982371e91

Verified provider

Next, I've selected a t2.micro instance type, a key pair (you can create a new key pair if you don't already have one), and I've selected the security group I created earlier. Because this launch template will be used for an auto scaling group, we do not need to include a subnet here.

▼ Instance type [Info](#)

[Advanced](#)

Instance type

t2.micro

Free tier eligible

Family: t2 1 vCPU 1 GiB Memory

On-Demand Linux pricing: 0.0116 USD per Hour

On-Demand Windows pricing: 0.0162 USD per Hour

[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

project-KP ▼

[Create new key pair](#)

▼ Network settings [Info](#)

Subnet [Info](#)

Don't include in launch template ▼

[Create new subnet](#)

When you specify a subnet, a network interface is automatically added to your template.

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.

Select existing security group Create security group

Common security groups [Info](#)

Select security groups ▼

[Compare security group rules](#)

Web-App-SG sg-0b0fbdbeae61fff60 X
VPC: vpc-0f36022490de29f6d

Security groups that you add or remove here will be added to or removed from all your network interfaces.

Select “Enable” under “Auto-assign public IP.” The next sections are “Storage (volumes)” and “Resource tags” and we have chosen not to change any of those default settings.

▼ Storage (volumes) [Info](#)

EBS Volumes [Hide details](#)

- ▶ Volume 1 (AMI Root) (8 GiB, EBS, General purpose SSD (gp2))
AMI Volumes are not included in the template unless modified

[Add new volume](#)

▼ Resource tags [Info](#)

No resource tags are currently included in this template. Add a resource tag to include it in the launch template.

[Add tag](#)
50 remaining (Up to 50 tags maximum)

► Advanced details [Info](#)

▼ Advanced network configuration

Network interface 1

Device index Info 0	Network Interface Info New interface	Description Info Remove
Subnet Info Don't include in launch template Not applicable for EC2 Auto Scaling	Security groups Info Select security groups	Auto-assign public IP Info Enable
Show all selected (1)		
Primary IP Info Not applicable for EC2 Auto Scaling	Secondary IP Info Don't include in launch tem...	IPv6 IPs Info Don't include in launch tem...
Not applicable for EC2 Auto Scaling		
IPv4 Prefixes Info Don't include in launch tem...	IPv6 Prefixes Info Don't include in launch tem...	Delete on termination Info Don't include in launch tem...
The selected instance type does not support IPv4 prefixes.		
Elastic Fabric Adapter Info <input checked="" type="checkbox"/> Enable EFA is only compatible with certain instance types.	Network card index Info Don't include in launch tem...	The selected instance type does not support multiple network cards.
Add network interface		

In the advanced section we add a user_data script that will allow us to deploy our express backend after installing all the necessary dependencies .

User data [Info](#)

```
#!/bin/bash -ex
# output user data logs into a separate file for debugging
# exec > >(tee /var/log/user-data.log|logger -t user-data -s 2>/dev/console) 2>&1
# download nvm
curl -o- https://raw.githubusercontent.com/nvm-sh/nvm/v0.39.2/install.sh | bash
# source nvm
chmod +x ~/.nvm/nvm.sh
source ~/.bashrc

# install node

nvm install 16
nvm use 16

#upgrade yum
```

User data has already been base64 encoded

This is the complete script

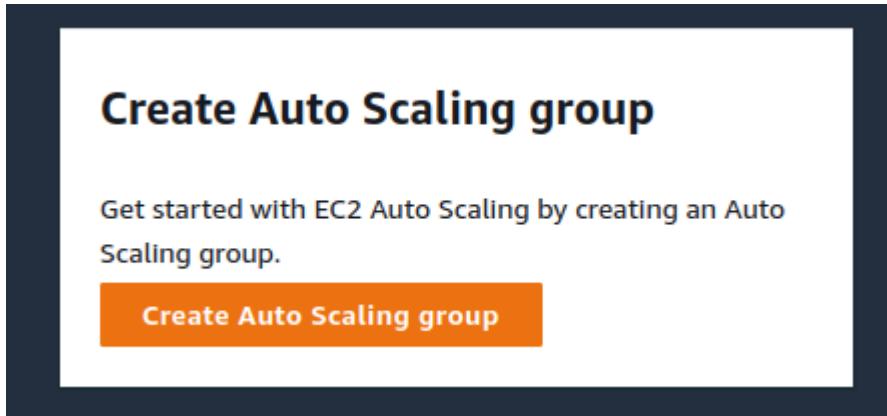
```
#!/bin/bash
# download nvm
curl -o- https://raw.githubusercontent.com/nvm-sh/nvm/v0.39.2/install.sh | bash
# source nvm
chmod +x ~/.nvm/nvm.sh
source ~/.bashrc

export NVM_DIR="$HOME/.nvm"
[ -s "$NVM_DIR/nvm.sh" ] && \. "$NVM_DIR/nvm.sh"
[ -s "$NVM_DIR/bash_completion" ] && \. "$NVM_DIR/bash_completion"
# install node
nvm install 16
nvm use 16
#upgrade yum
sudo yum upgrade
#install git
sudo yum install git -y
cd /home/ec2-user
# get source code from github
git clone https://github.com/OussamaMaroufi/Express-Backend.git
#get in server dir
cd Express-Backend
#give permission
sudo chmod -R 777 .
#install node module
npm install
# start the app
npm run dev > app.out.log 2> app.err.log < /dev/null &
# to redirect traffic comes to port 80 into port 3001
sudo iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 3001
```

When we finish configuring the launch template, click “Create launch template.”

Launch templates (2) <small>Info</small>							<small>Create</small>	Actions ▾	<small>Create launch template</small>
Launch template ID	Launch template name	Default version	Latest version	Create time	Created by				
lt-0102780104334b34b	Project-LT	1	1	2022-12-26T15:38:40.000Z	arn:aws:sts::278484320774:a ssumed-role/voclabs /user2181130=maaroufi.ousss ama@etudiant-fst.utm.tn				
lt-02b593b12ac4ef46a	My-LT	1	2	2022-12-24T16:40:51.000Z	arn:aws:sts::278484320774:a ssumed-role/voclabs /user2181130=maaroufi.ousss ama@etudiant-fst.utm.tn				

Now we are ready to create the Auto Scaling Group. On the EC2 dashboard we scroll down and select *auto scaling groups*, *create auto scaling groups*.



Give our auto scaling group a name and select the launch template we just created. Scroll down and *click next*.

EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1 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.

Step 2 Choose instance launch options

Step 3 (optional) Configure advanced options

Step 4 (optional)

Choose launch template or configuration Info

Name

Auto Scaling group name
Enter a name to identify the group.

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.

Project-LT ▼ C

[Create a launch template](#) 

Select our custom VPC and subnets. *Click next.*

Choose instance launch options [Info](#)

Choose the VPC network environment that your instances are launched into, and customize the instance types and purchase options.

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
Choose the VPC that defines the virtual network for your Auto Scaling group.

vpc-0f36022490de29f6d (my-vpc) ▼ C

[Create a VPC](#) 

Availability Zones and subnets
Define which Availability Zones and subnets your Auto Scaling group can use in the chosen VPC.

Select Availability Zones and subnets ▼ C

us-east-1a | subnet-077e8589a9c78622d X
(private-subnet1)
10.0.2.0/23

us-east-1b | subnet-02d379562ed92c18f X
(private-subnet2)
10.0.4.0/23

[Create a subnet](#) 

click next.

Select *Attach to existing load balancer* and the target group that we have already created, under health check type select *ELB*, select *next*.

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 ▾ ✖ C

ALB-TG | HTTP X
Application Load Balancer: Project-ALB

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

We will instruct our Auto Scaling Group to always ensure we have a minimum of two instances running at a time. Configure the following scaling policy.

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
2

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

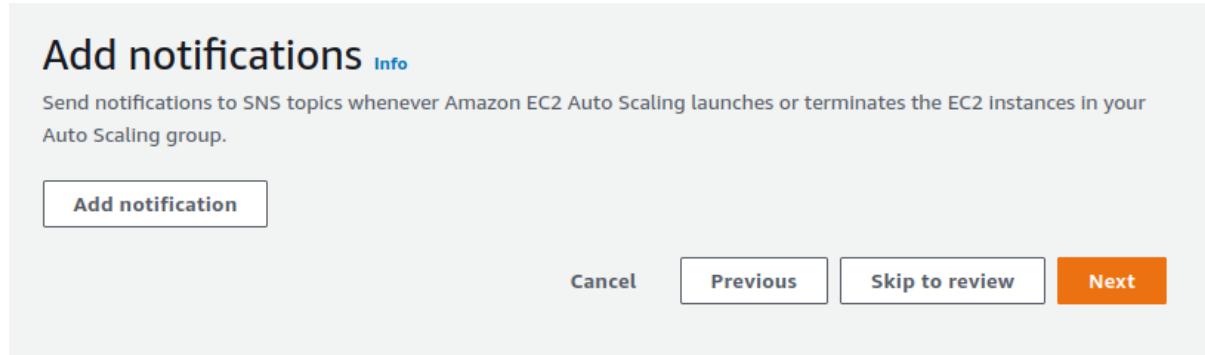
Metric type
 ▾

Target value

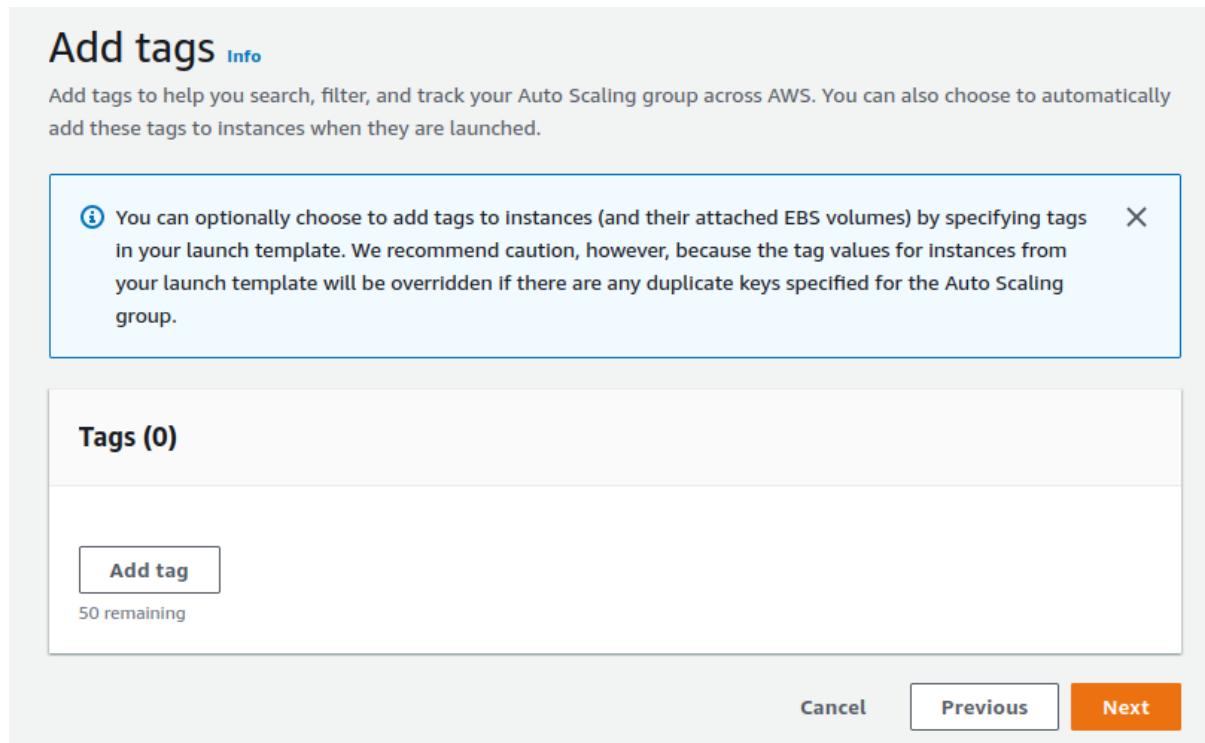
Instances need
 seconds warm up before including in metric

Disable scale in to create only a scale-out policy

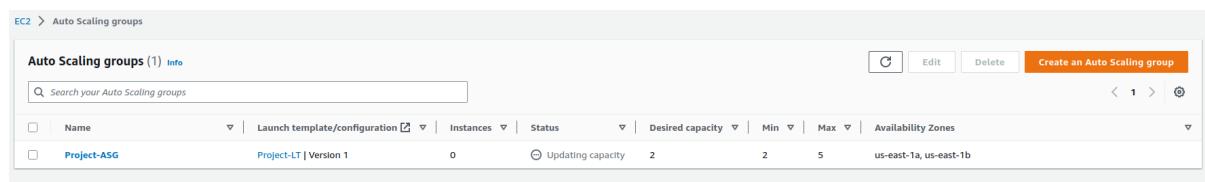
click Next we don't need to add Notification to our autoscaling group for now .



click Next



the click create auto scaling group



if we check the activity history we see that our instances are successfully launched

The screenshot shows the 'Activity history' section for the 'Auto Scaling group: Project-ASG'. It lists two entries:

Status	Description	Cause	Start time	End time
Successful	Launching a new EC2 instance: i-025425e68d7fafa86	At 2022-12-28T22:02:09Z a user request created an AutoScalingGroup changing the desired capacity from 0 to 2. At 2022-12-28T22:02:12Z an instance was started in response to a difference between desired and actual capacity, increasing the capacity from 0 to 2.	2022 December 28, 11:02:14 PM +01:00	2022 December 28, 11:02:46 PM +01:00
Successful	Launching a new EC2 instance: i-026456f4bdc6a41b4	At 2022-12-28T22:02:09Z a user request created an AutoScalingGroup changing the desired capacity from 0 to 2. At 2022-12-28T22:02:12Z an instance was started in response to a difference between desired and actual capacity, increasing the capacity from 0 to 2.	2022 December 28, 11:02:14 PM +01:00	2022 December 28, 11:02:46 PM +01:00

Step 10 : Create Database Instance RDS - MYSQL

First, set up the MySQL database by creating subnet groups for this database. Navigate to RDS > Subnet Groups > Create DB subnet group.

“A DB subnet group is a collection of subnets (typically private) that you create for a VPC and that you then designate for your DB instances.”

The screenshot shows the 'Create DB subnet group' wizard. The steps are: RDS > Subnet groups > Create DB subnet group.

Create DB subnet group

To create a new subnet group, give it a name and a description, and choose an existing VPC. You will then be able to add subnets related to that VPC.

Subnet group details

Name
You won't be able to modify the name after your subnet group has been created.

Must contain from 1 to 255 characters. Alphanumeric characters, spaces, hyphens, underscores, and periods are allowed.

Description

VPC
Choose a VPC identifier that corresponds to the subnets you want to use for your DB subnet group. You won't be able to choose a different VPC identifier after your subnet group has been created.

Add subnets

Availability Zones

Choose the Availability Zones that include the subnets you want to add.

Choose an availability zone ▾

us-east-1a X

us-east-1b X

Subnets

Choose the subnets that you want to add. The list includes the subnets in the selected Availability Zones.

Select subnets ▾

us-east-1a

subnet-018529334702628c5 (10.0.0.0/24)

subnet-077e8589a9c78622d (10.0.2.0/23)

us-east-1b

subnet-0dde70a44df6605ec (10.0.1.0/24)

subnet-02d379562ed92c18f (10.0.4.0/23)

CIDR block

us-east-1a

subnet-077e8589a9c78622d

10.0.2.0/23

us-east-1b

subnet-02d379562ed92c18f

10.0.4.0/23

Cancel

Create

Next, we navigate back to the RDS dashboard to create the MySQL database. We are using a Standard create with MySQL selected as the engine option.

RDS > Create database

Create database

Choose a database creation method Info

Standard create
You set all of the configuration options, including ones for availability, security, backups, and maintenance.

Easy create
Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

Select Mysql Engine

Engine options

Engine type Info

Amazon Aurora 

MySQL 

MariaDB 

PostgreSQL 

Oracle 

Microsoft SQL Server 

Edition

MySQL Community

Engine Version

MySQL 8.0.28

We are using a free-tier template. This is important to avoid accruing costs. We also needed to generate a password in the Credentials Settings.

Templates

Choose a sample template to meet your use case.

- Production**
Use defaults for high availability and fast, consistent performance.
- Dev/Test**
This instance is intended for development use outside of a production environment.
- Free tier**
Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS. [Info](#)

▼ Credentials Settings

Master username [Info](#)
Type a login ID for the master user of your DB instance.

1 to 16 alphanumeric characters. First character must be a letter.

Manage master credentials in AWS Secrets Manager
Manage master user credentials in Secrets Manager. RDS can generate a password for you and manage it throughout its lifecycle.

Auto generate a password
Amazon RDS can generate a password for you, or you can specify your own password.

Master password [Info](#)

Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), '(single quote), "(double quote) and @ (at sign).

Confirm master password [Info](#)

For instance Configuration, We are using db.t2.micro also we uncheck the box labeled “Enable storage autoscaling” .

Instance configuration

The DB instance configuration options below are limited to those supported by the engine that you selected above.

DB instance class [Info](#)

- Standard classes (includes m classes)
- Memory optimized classes (includes r and x classes)
- Burstable classes (includes t classes)**

db.t2.micro ▼

1 vCPUs 1 GiB RAM Not EBS Optimized

Include previous generation classes

Storage

Storage type [Info](#)

General Purpose SSD (gp2) ▼

Baseline performance determined by volume size

Allocated storage

40 GiB ▼

The minimum value is 20 GiB and the maximum value is 6,144 GiB

Storage autoscaling [Info](#)

Provides dynamic scaling support for your database's storage based on your application's needs.

Enable storage autoscaling
Enabling this feature will allow the storage to increase after the specified threshold is exceeded.

Connectivity Info



Compute resource

Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings so that the compute resource can connect to this database.

Don't connect to an EC2 compute resource

Don't set up a connection to a compute resource for this database. You can manually set up a connection to a compute resource later.

Connect to an EC2 compute resource

Set up a connection to an EC2 compute resource for this database.

Network type Info

To use dual-stack mode, make sure that you associate an IPv6 CIDR block with a subnet in the VPC you specify.

IPv4

Your resources can communicate only over the IPv4 addressing protocol.

Dual-stack mode

Your resources can communicate over IPv4, IPv6, or both.

Virtual private cloud (VPC) Info

Choose the VPC. The VPC defines the virtual networking environment for this DB instance.

my-vpc (vpc-0f36022490de29f6d)



Only VPCs with a corresponding DB subnet group are listed.

setup the security group for our db instance :

VPC security group (firewall) Info

Choose one or more VPC security groups to allow access to your database. Make sure that the security group rules allow the appropriate incoming traffic.

Choose existing

Choose existing VPC security groups

Create new

Create new VPC security group

Existing VPC security groups

Choose one or more options



Mysql-SG

Databases									<input type="checkbox"/> Group resources	<input type="button" value="C"/>	<input type="button" value="Modify"/>	<input type="button" value="Actions ▾"/>	<input type="button" value="Restore from S3"/>	<input type="button" value="Create database"/>
									<input type="button" value="Filter by databases"/>	< 1 >				<input type="button" value=""/>
	DB identifier	Role	Engine	Region & AZ	Size	Status	CPU	Current activity						
<input type="radio"/>	project-database	Instance	MySQL Community	-	db.t2.micro	<input type="button" value="Creating"/>	-	-						

And Now our db instance is Ready as shown below

Databases									<input type="checkbox"/> Group resources	<input type="button" value="C"/>	<input type="button" value="Modify"/>	<input type="button" value="Actions ▾"/>	<input type="button" value="Restore from S3"/>	<input type="button" value="Create database"/>
									<input type="button" value="Filter by databases"/>	< 1 >				<input type="button" value=""/>
	DB identifier	Role	Engine	Region & AZ	Size	Status	CPU	Current activity						
<input type="radio"/>	project-database	Instance	MySQL Community	us-east-1b	db.t2.micro	<input type="button" value="Available"/>	-	-						

Now let's convert the db instance to Multi-AZ and that will create a standby instance that will be helpful in case of disaster recovery .

Databases									<input type="checkbox"/> Group resources	<input type="button" value="C"/>	<input type="button" value="Modify"/>	<input type="button" value="Actions ▾"/>	<input type="button" value="Restore from S3"/>	<input type="button" value="Create database"/>
									<input type="button" value="Filter by databases"/>	< 1 >				<input type="button" value=""/>
	DB identifier	Role	Engine	Region & AZ										
<input type="radio"/>	project-database	Instance	MySQL Community	us-east-1b										

Convert to Multi-AZ DB instance deployment?

Create a standby replica in a different Availability Zone. A Multi-AZ DB instance deployment provides data redundancy and minimizes latency spikes during system backups. Additional charges apply. [Learn more](#)

Schedule database modification

Apply during the next scheduled maintenance window
Current maintenance window: December 28, 2022 05:32 - 06:02 UTC+1

Apply immediately

The modifications in this request and any pending modifications will be asynchronously applied as soon as possible, regardless of the maintenance window setting for this database instance.



Potential performance impact when converting to Multi-AZ

Your DB instance might experience a significant performance impact during and after converting to a Multi-AZ DB instance deployment. We don't recommend this conversion on a production DB instance. To avoid the performance impact, you can create a read replica of the DB instance, convert the read replica to a Multi-AZ DB instance deployment, and promote the read replica. [Learn more](#)

And now db-instance become deployed in Multi-AZ :

Databases		Group resources		Actions	Restore from S3	Create database				
		Region & AZ		Size	Status	CPU	Current activity	Maintenance	VPC	Multi-AZ
Community	us-east-1b	db.t2.micro	Available	4.24%	0 Connections	none	vpc-0f36022490de29f6d	Yes		

Connect to our db instance from an Ec2 instance launched in (Wec-App-SG) and have mysql client Already installed on it Then Create a database (crudgames) and table (games)

```
No packages marked for update
[ec2-user@ip-10-0-0-173 ~]$ sudo yum install mysql
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
Resolving Dependencies
--> Running transaction check
--> Package mariadb.x86_64 1:5.5.68-1.amzn2 will be installed
--> Finished Dependency Resolution

Dependencies Resolved
```

```
[ec2-user@ip-10-0-0-173 ~]$ sudo mysql -h project-database.chtzczkph8w4.us-east-1.rds.amazonaws.com -P 3306 -u oussama -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 231
Server version: 8.0.28 Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

```
MySQL [(none)]> create database crudgames;
Query OK, 1 row affected (0.05 sec)
```

```
MySQL [(none)]> show databases
-> ;
+-----+
| Database |
+-----+
| crudgames |
| information_schema |
| mysql |
| performance_schema |
| sys |
+-----+
5 rows in set (0.00 sec)
```

Create Table games :

```
MySQL [(none)]> use crudgames
Database changed
MySQL [crudgames]> create table games(
-> idgames int not null AUTO_INCREMENT,
-> name varchar(255),
-> cost varchar(255),
-> category varchar(255),
-> PRIMARY KEY(idgames))
-> ;
Query OK, 0 rows affected (0.16 sec)

MySQL [crudgames]>
```

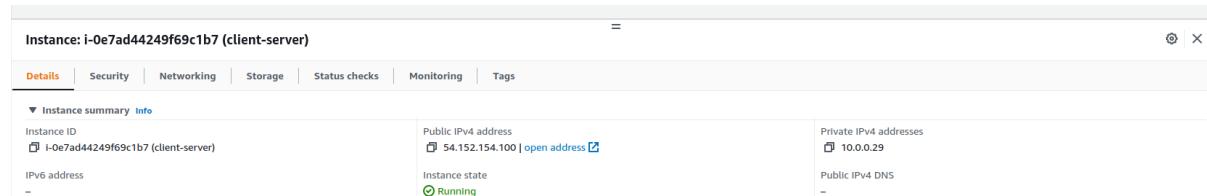
```
MySQL [crudgames]> SHOW TABLES;
+-----+
| Tables_in_crudgames |
+-----+
| games |
+-----+
1 row in set (0.00 sec)

MySQL [crudgames]>
```

Step 11 : Deploy A React App In EC2 Instance

We deploy the react app in order to interact with our database and perform some crud operations on it .

1 launch an EC2 instance to deploy the React App



then we run that script to pull the project from github repository and run the build

```
#!/bin/bash
# download nvm
curl -o- https://raw.githubusercontent.com/nvm-sh/nvm/v0.39.2/install.sh | bash
# source nvm
chmod +x ~/.nvm/nvm.sh
source ~/.bashrc
export NVM_DIR="$HOME/.nvm"
[ -s "$NVM_DIR/nvm.sh" ] && \. "$NVM_DIR/nvm.sh"
[ -s "$NVM_DIR/bash_completion" ] && \. "$NVM_DIR/bash_completion"
# install node
nvm install 16
nvm use 16
#upgrade yum
sudo yum upgrade
#install git
sudo yum install git -y
cd /home/ec2-user
# get source code from github
git clone https://github.com/OussamaMaroufi/client-tier.git
#get in server dir
cd client-tier
#give permission
sudo chmod -R 777 .
#install node module
npm install
# start the app
# npm run dev > appl.out.log 2> appl.err.log < /dev/null &
#build the app
npm run build > appl.out.log 2> appl.err.log < /dev/null &
# to redirect traffic comes to port 80 into port 3001
sudo iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 3000
```

we run this bash script to install nginx server

```
#!/bin/bash
sudo yum update -y
sudo amazon-linux-extras install nginx1 -y
sudo systemctl enable nginx
sudo systemctl start nginx
```

add this configuration in /etc/nginx/conf.d

```
server {
    listen 80;
    listen [::]:80;
    root /home/ec2-user/app-deploy/dist;
    location / {
        try_files $uri /index.html;
    }
}
```

```
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
[ec2-user@ip-10-0-0-29 conf.d]$ sudo service nginx reload
Redirecting to /bin/systemctl reload nginx.service
[ec2-user@ip-10-0-0-29 conf.d]$
```

our app is deployed successfully

Game Shop
Add a Game

Title	Cost	Category	Add
App1	\$2.22	Cat1	Edit Delete
App2	\$3.22	44	Edit Delete

Now we should create an Elastic Ip and attach it to our client-server

Elastic IP address allocated successfully.
Elastic IP address 3.225.203.34

Associate this Elastic IP address [X](#)

Elastic IP addresses (1/1)

Name	Allocated IPv4 address	Type	Allocation ID	Reverse DNS record	Associated instance	Private IP address
–	3.225.203.34	Public IP	eipalloc-09cfbae9b5a...	–	–	–

After we allocate an Elastic IP we Need to associate it to the instance running our frontend tier .

Associate Elastic IP address

Choose the instance or network interface to associate to this Elastic IP address (3.225.203.34)

Elastic IP address: 3.225.203.34

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

Instance

i-016d3154e51592a74



Private IP address

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

Choose a private IP address

Reassociation

Specify whether the Elastic IP address can be reassigned to a different resource if it's already associated with a resource.

Allow this Elastic IP address to be reassigned

Cancel

Associate

and now our application is available on <http://3.225.203.34>

Step 12 : Create Machine Bastion

1 - create a security group for bastion machine

The screenshot shows the AWS Lambda console interface. At the top, there's a search bar labeled "Search our full catalog including 1000s of application and OS images". Below it, there are two tabs: "Recents" and "Quick Start", with "Quick Start" being the active tab. Under "Quick Start", there are several cards for different operating systems: Amazon Linux (AMI), macOS, Ubuntu, Windows, Red Hat, and SUSE. To the right of these cards is a search icon and a link to "Browse more AMIs". Below this section, a detailed card for the "Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type" is displayed. The card includes the AMI ID "ami-0b5eea76982371e91 (64-bit (x86)) / ami-03a45a5ac837f33b7 (64-bit (Arm))", and information about its compatibility with "Free tier eligible", "Virtualization: hvm", "ENAv2 enabled: true", and "Root device type: ebs".

▼ 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*

project-KP ▼

[Create new key pair](#)

▼ Network settings [Info](#)

VPC - *required* [Info](#)

vpc-0f36022490de29f6d (my-vpc) ▼

10.0.0.0/16 C

[Create new VPC](#)

Subnet [Info](#)

subnet-018529334702628c5 public-subnet1 ▼

Subnet ID: subnet-018529334702628c5
VPC: vpc-0f36022490de29f6d Owner: 278484320774 Availability Zone: us-east-1a IP addresses available: 247 CIDR: 10.0.0.0/24

[Create new subnet](#)

Auto-assign public IP [Info](#)

Enable ▼

We allow ssh access from everywhere to the bastion machine .

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*

bastion-SG

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 created 2022-12-29T00:07:30.907Z

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

Description - *optional* [Info](#)

e.g. SSH for admin desktop

0.0.0.0/0 X

2 - Edit Web-App-SG to allow ssh traffic from bastion-SG

The screenshot shows the 'Edit inbound rules' page for the security group 'sg-0b0fbdbae61ffff60 - Web-App-SG'. The left sidebar lists 'Inbound rules' with three entries: 'sgr-0ec0e9a9f5eaef9f' (HTTP, port 80), 'sgr-0c4f82d8c5c50433c' (HTTPS, port 443), and a new rule starting with '-' (SSH, port 22). The right panel displays a table for defining the source of the rule. The 'Source' dropdown is set to 'Custom' and shows a list of CIDR blocks and security groups. Under 'CIDR blocks', options like '0.0.0.0/0', '::/0', and '::/16' are listed. Under 'Security Groups', 'bastion-SG | sg-08ddf649d224c470a' and 'Web-App-SG |' are listed. A search bar and a 'Delete' button are also present. At the bottom, there are 'Cancel', 'Preview changes', and a prominent orange 'Save rules' button.

III. Conclusion

OK that's it! After setting up a VPC, subnets, route table, security group, and internet gateway,nat gateway,, you then created a Launch Template with specific AMI, instance type, key pair, security group, and user data. We then created an Auto Scale group using the Launch Template, and applied an Application Load Balancer. Our business application is now ready to meet the demands of its users .

Références :

- <https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html>
- <https://docs.aws.amazon.com/autoscaling/ec2/userguide/auto-scaling-groups.html>
- <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html>
- https://docs.amazonaws.cn/en_us/AmazonRDS/latest/UserGuide/Welcome.html
- https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html
- <https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html>