

Projet: AWS 3-tier-architecture

Introduction

Lors de la création d'une application basée sur le cloud, l'architecture et l'environnement sous-jacents sont tout aussi importants que l'application elle-même. De nombreuses considérations entrent en ligne de compte lorsqu'il s'agit de décider de l'architecture appropriée de votre application :

- **Évolutivité** : avec quelle facilité et/ou fréquence l'application doit-elle évoluer vers le haut ou vers le bas ? Quelle valeur accordez-vous au fait de ne pas avoir à micro-gérer et à surveiller en permanence l'utilisation des ressources ?
- **Disponibilité** : Dans quelle mesure votre application est-elle facilement disponible ? Quelle est l'importance de pouvoir passer de longues périodes sans défaillance ? En cas de défaillance d'une partie de votre application, quelle est la vulnérabilité du reste ?
- **Sécurité** : Quel est le niveau de sécurité de votre application ? Comment votre application gère-t-elle les autorisations de sécurité pour les différentes parties de votre application ? Si une attaque se produit dans une partie de votre application, quelle est la vulnérabilité du reste ?

L'architecture à trois niveaux d'AWS

Pourquoi une architecture à trois niveaux ? Cette forme d'architecture répond à tous les problèmes mentionnés ci-dessus. Elle offre une évolutivité, une disponibilité et une sécurité accrues en répartissant l'application sur plusieurs zones de disponibilité et en la séparant en trois couches qui remplissent des fonctions différentes, indépendantes les unes des autres. Si une zone de disponibilité tombe en panne pour une raison quelconque, l'application peut automatiquement transférer ses ressources vers une autre zone de disponibilité, sans affecter les autres niveaux de l'application. Chaque niveau dispose de son propre groupe de sécurité qui n'autorise que le trafic entrant/sortant nécessaire à l'exécution de tâches spécifiques.

- **Niveau Web/Présentation** : Il héberge les éléments de l'application orientés vers l'utilisateur, tels que les serveurs web et l'interface/frontale.
- **Niveau application** : Il héberge le code source de l'application et du backend nécessaire au traitement des données et à l'exécution des fonctions.
- **Niveau des données** : Il héberge et gère les données de l'application. C'est souvent là que sont stockées les bases de données.

Scénario

Une entreprise de commerce électronique en pleine croissance a récemment connu une augmentation significative de son trafic web, surtout pendant les périodes de soldes et de fêtes. L'infrastructure actuelle de l'entreprise est monolithique, hébergée sur un seul serveur, et ne peut plus répondre efficacement à la demande croissante. Cette situation entraîne des temps d'arrêt fréquents, une faible performance, et une mauvaise expérience utilisateur.

L'entreprise décide donc de migrer vers AWS et souhaite mettre en place une architecture en 3 niveaux (3-Tier Architecture) hautement disponible, résiliente, et capable de s'adapter à la croissance future.

Objectif

L'objectif est de concevoir et de mettre en œuvre une infrastructure en 3 niveaux sur AWS qui soit :

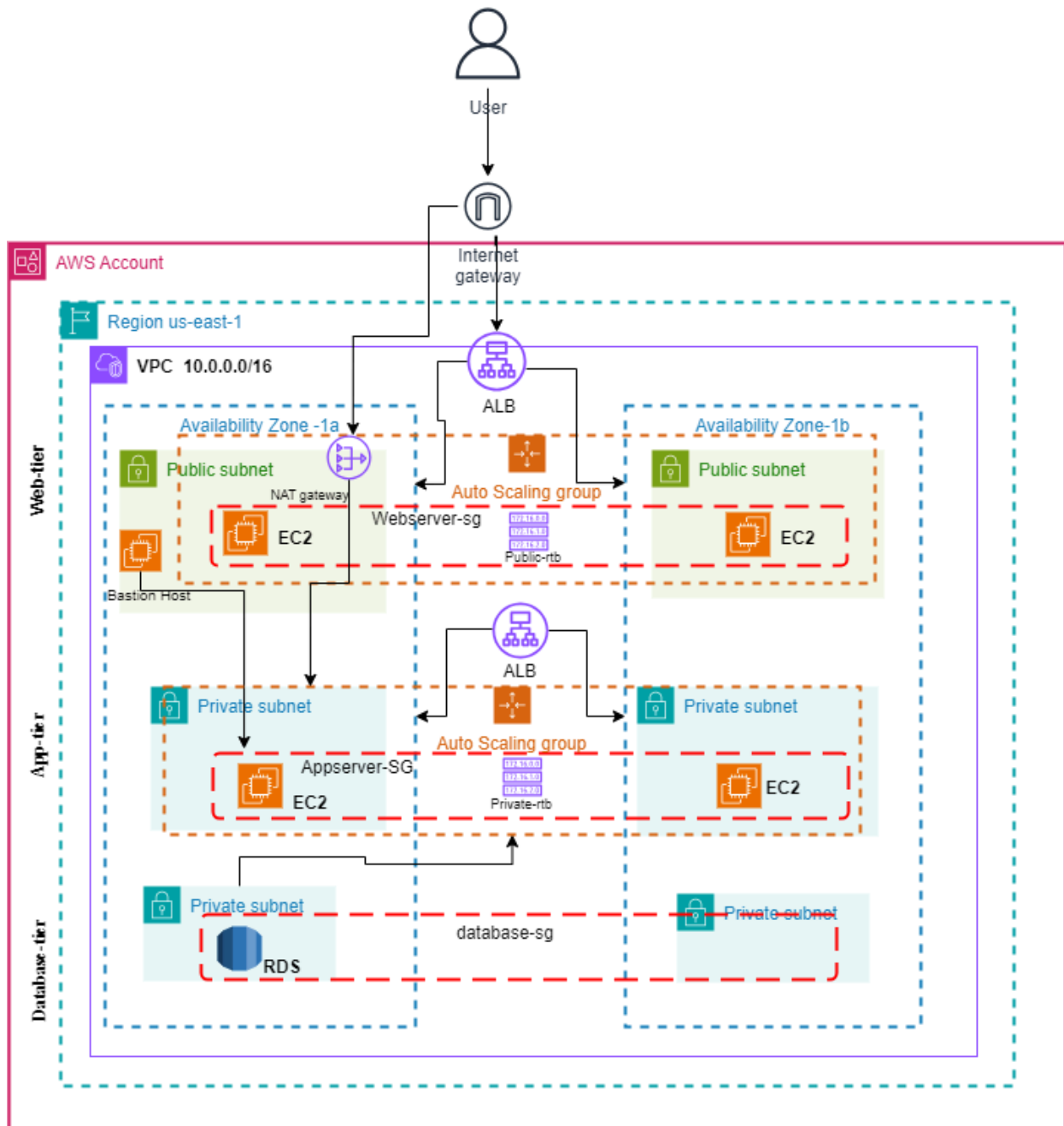
- **Hautement disponible** : L'application doit être accessible même en cas de panne d'un composant ou d'une région.
- **Résiliente** : L'application doit être capable de se remettre rapidement de toute perturbation.
- **Scalable** : L'infrastructure doit pouvoir évoluer automatiquement pour gérer les pics de trafic.
- **Sécurisée** : Les données doivent être protégées et les accès contrôlés.

Coûts: free tier

Temps estimé de réalisation: 3h

Architecture de solution

AWS 3-Tiers Architecture



Réalisation

Ce réseau de base comprend

- UN VPC.

- Deux (2) sous-réseaux publics répartis sur deux zones de disponibilité (Web Tier).
- Deux (2) sous-réseaux privés répartis sur deux zones de disponibilité (Application Tier).
- Deux (2) sous-réseaux privés répartis sur deux zones de disponibilité (niveau base de données).
- Une (1) table de routage publique qui connecte les sous-réseaux publics à une passerelle internet.
- Une (1) table de routage privée qui connectera les sous-réseaux privés de l'Application Tier à une passerelle NAT.

Dans la console VPC, créons un nouveau VPC. Nous sélectionnerons l'option '**VPC and more**' et nommerons notre projet '**Bootcamp-3tier**' avec un bloc CIDR de 10.0.0.0/16.

Pour augmenter la disponibilité de notre application **Bootcamp-3tier**, nous utiliserons deux AZ (us-east-1a et us-east-1b), deux sous-réseaux publics et quatre sous-réseaux privés (nous ajouterons une passerelle NAT plus tard lorsque nous serons prêts à construire le niveau Application).

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 auto-generation [Info](#)
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

☒ Auto-generate
Bootcamp-3tier

IPv4 CIDR block [Info](#)
Determine the starting IP and the size of your VPC using CIDR notation.

10.0.0.0/16 65 536 IPs
CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)
☒ No IPv6 CIDR block
☐ Amazon-provided IPv6 CIDR block

Preview

VPC [Show details](#)
Your AWS virtual network

Bootcamp-3tier-vpc

Subnets

us-east-1a
A Bc
A Bc
A Bc

us-east-1b
B Bc
B Bc
B Bc

Number of Availability Zones (AZs) [Info](#)

Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

1	2	3
---	---	---



► [Customize AZs](#)

Number of public subnets [Info](#)

The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0	2
---	---



Number of private subnets [Info](#)

The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

0	2	4
---	---	---



► [Customize subnets CIDR blocks](#)

NAT gateways (\$) [Info](#)

Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway

☒ None
 ☐ In 1 AZ
 ☐ 1 per AZ

VPC endpoints [Info](#)

Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

☒ None
 ☐ S3 Gateway

DNS options [Info](#)

☒ Enable DNS hostnames
☒ Enable DNS resolution

► **Additional tags**

Cancel

- **Activer l'attribution automatique de l'adresse IPv4**

Une fois que tous les actifs ont été créés, nous devons nous assurer d'activer l'attribution automatique d'une adresse IPv4 publique pour les DEUX sous-réseaux publics afin de pouvoir accéder à leurs ressources via l'internet.

Subnets (1/12) [Info](#)

Last updated 1 minute ago

Find resources by attribute or tag

	Name	Subnet ID	State	VPC
<input type="checkbox"/>	-	subnet-0096b215e0777d4a0	Available	vpc-
<input type="checkbox"/>	Bootcamp-3tier-subnet-private2-us-eas...	subnet-069dd609a594f8905	Available	vpc-
<input checked="" type="checkbox"/>	Bootcamp-3tier-subnet-public2-us-east...	subnet-0e3d5ab4aff815c75	Available	vpc-
<input type="checkbox"/>	Bootcamp-3tier-subnet-private4-us-eas...	subnet-0654ee8cc2f87d1ce	Available	vpc-
<input type="checkbox"/>	-	subnet-01c09607314c0bb4b	Available	vpc-


Actions

- View details
- Create flow log
- Edit subnet settings
- Edit IPv6 CIDRs
- Edit network ACL association
- Edit route table association
- Edit CIDR reservations
- Share subnet


Edit subnet settings [Info](#)

Subnet

Subnet ID

 subnet-0e3d5ab4aff815c75

Name

 Bootcamp-3tier-subnet-public2-us-east-1b

Auto-assign IP settings [Info](#)

Enable AWS to automatically assign a public IPv4 or IPv6 address to a new primary network interface for an instance in this subnet.

☒ Enable auto-assign public IPv4 address [Info](#)

☐ Enable auto-assign customer-owned IPv4 address [Info](#)
Option disabled because no customer owned pools found.

Resource-based name (RBN) settings [Info](#)

Specify the hostname type for EC2 instances in this subnet and optional RBN DNS query settings.

☐ Enable resource name DNS A record on launch [Info](#)

☐ Enable resource name DNS AAAA record on launch [Info](#)

Hostname type [Info](#)

☐ Resource name

☒ IP name

DNS64 settings

Enable DNS64 to allow IPv6-only services in Amazon VPC to communicate with IPv4-only services and networks.

☐ Enable DNS64 [Info](#)

Cancel

Save 

- **Définir la table de routage principale**

Lorsqu'un VPC est créé, il est livré avec une table de routage par défaut en tant que « table principale ». Cependant, nous voulons que notre table de routage publique serve de table principale, alors sélectionnez la table de routage publique dans le tableau de bord « Tables de routage » et définissez-la comme table principale dans le menu déroulant « Actions ».

VPC dashboard X

EC2 Global View

Filter by VPC ▾

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

YOUR VPCs (1/2) Info 6 minutes ago Actions ▾ **Create VPC**

Search

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR
-	vpc-058e2b9ce56adf840	Available	172.31.0.0/16	-
<input checked="" type="checkbox"/> Bootcamp-3tier-vpc	vpc-0bd9f4c4bbc08cedc	Available	10.0.0.0/16	-

VPC ID vpc-0bd9f4c4bbc08cedc	State Available	DNS hostnames Enabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-033adf0f50a8b88e6	Main route table rtb-09022adb70a40ab41	Main network ACL acl-0c6623d28f4d84d87
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool -	IPv6 CIDR (Network border group) -

Route tables (1/7) Info Last updated 10 minutes ago Actions ▴ **Create route table**

Find resources by attribute or tag

Name	Route table ID	Explicit subnet associ...
-	rtb-0ad87d293ec949d01	-
Bootcamp-3tier-rtb-private1-us-east-1a	rtb-0db87542c889a45f8	subnet-0a81fda8a2c32ee...
Bootcamp-3tier-rtb-private2-us-east-1b	rtb-0e1793e2ef6993ffc	subnet-069dd609a594f8...
<input checked="" type="checkbox"/> Bootcamp-3tier-rtb-public	rtb-014b1935204b7fb0e	2 subnets
-	rtb-09022adb70a40ab41	-

View details

Set main route table

Edit subnet associations

Edit edge associations

Edit route propagation

Edit routes

Manage tags

Delete route table

Set main route table X

Main route table controls the routing for all subnets that are not explicitly associated with any other route table. Are you sure you want to set this route table as the main route table?

- rtb-014b1935204b7fb0e / Bootcamp-3tier-rtb-public

To confirm setting, type set in the field.

set

Cancel **OK**

- Créer une passerelle NAT

Une passerelle NAT permet aux instances des sous-réseaux privés de se connecter aux ressources en dehors du VPC et de l'Internet (pour les services nécessaires tels que les correctifs ou les mises à jour de paquets).

La meilleure pratique consiste à maintenir une haute disponibilité et à déployer deux passerelles NAT dans nos sous-réseaux publics (une dans chaque AZ) ; cependant, pour l'instant, nous n'en déploierons qu'une seule.

Naviguez vers '**NAT Gateways**' et créez une nouvelle passerelle appelée public-NAT-1. Sélectionnez l'un des sous-réseaux publics, allouez une IP élastique et créez la passerelle.

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.

The name can be up to 256 characters long.

Subnet
Select a subnet in which to create the NAT gateway.

The name can be up to 256 characters long.

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.

The name can be up to 256 characters long.

[Allocate Elastic IP](#)

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	
<input type="text" value="Name"/>	<input type="text" value="my-nat-gateway"/>	Remove

[Add new tag](#)

You can add 49 more tags.

[Cancel](#) [Create NAT gateway](#)

- **Configurer les tables de routage privées**

Comme nous pouvons le voir, une table de routage a été créée par défaut pour chaque sous-réseau privé (4). Cependant, nous n'avons besoin que d'une seule table de routage privée (pour les sous-réseaux de l'Application Tier). C'est ici que des conventions de nommage claires peuvent énormément aider à éviter la confusion, alors naviguons vers nos tables de routage et nettoyons un peu les choses.

Sélectionnez l'une des tables de routage privées et modifiez le nom en quelque chose comme 'Bootcamp-webApp-rtb-private1'. Ce sera notre table de routage privée. Nous pouvons maintenant associer cette table aux quatre sous-réseaux privés (-subnet-private1, -subnet-private2, -subnet-private3, -subnet-private4).

The screenshot shows the AWS Management Console interface. At the top, a table lists route tables. A red arrow points to the first row, 'Bootcamp-3tier-WebApp-rtb-private1-us-east-1a', which is selected. Below the table, the details for this route table are shown, including tabs for 'Details', 'Routes', 'Subnet associations', 'Edge associations', 'Route propagation', and 'Tags'. The 'Subnet associations' tab is active, showing 'Explicit subnet associations (1)'. A red arrow points to the 'Edit subnet associations' button in the top right corner of this section.

Name	Route table ID	Explicit subnet associ...	Edge associations	Main
<input checked="" type="checkbox"/> Bootcamp-3tier-WebApp-rtb-private1-us-east-1a	rtb-0db87542c889a45f8	subnet-0a81fda8a2c32ee...	-	No
<input type="checkbox"/> Bootcamp-3tier-Apptier-rtb-private2-us-east-1a	rtb-0e1793e2ef6993ffc	subnet-069dd609a594f8...	-	No
<input type="checkbox"/> -	rtb-0ad87d293ec949d01	-	-	Yes
<input type="checkbox"/> Bootcamp-3tier-rtb-public	rtb-014b1935204b7fb0e	2 subnets	-	Yes
<input type="checkbox"/> -	rtb-0902adb70a40ab41	-	-	No
<input type="checkbox"/> Bootcamp-3tier-dbtier-rtb-private3-us-east-1a	rtb-0fd14e1ab70defb6e	subnet-07cbb254b1e6ce...	-	No

rtb-0db87542c889a45f8 / Bootcamp-3tier-WebApp-rtb-private1-us-east-1a

Details | Routes | **Subnet associations** | Edge associations | Route propagation | Tags

Explicit subnet associations (1)

Edit subnet associations

Les tables de routage supplémentaires sont inutiles, nous allons donc les supprimer. Si cela est fait correctement, il devrait y avoir un total de deux tables de routes, une avec deux sous-réseaux associés et une avec quatre sous-réseaux associés.

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (4/6)

Filter subnet associations

<input type="checkbox"/>	Name	Subnet ID	IPv4 CIDR
<input type="checkbox"/>	Bootcamp-3tier-subnet-public1-us-east-1a	subnet-0fcb798d7ab60ff13	10.0.0.0/20
<input checked="" type="checkbox"/>	Bootcamp-3tier-subnet-WebApp-private3-us-east-1a	subnet-07cbb254b1e6ce2f9	10.0.160.0/20
<input checked="" type="checkbox"/>	Bootcamp-3tier-subnet-WebApp-private1-us-east-1a	subnet-0a81fda8a2c32ee8b	10.0.128.0/20
<input checked="" type="checkbox"/>	Bootcamp-3tier-DB-subnet-private2-us-east-1b	subnet-069dd609a594f8905	10.0.144.0/20
<input type="checkbox"/>	Bootcamp-3tier-subnet-public2-us-east-1b	subnet-0e3d5ab4aff815c75	10.0.16.0/20
<input checked="" type="checkbox"/>	Bootcamp-3tier-DB-subnet-private4-us-east-1b	subnet-0654ee8cc2f87d1ce	10.0.176.0/20

- Edition de la route

<input checked="" type="checkbox"/>	Bootcamp-3tier-rtb-private1-us-east-1a	rtb-0db87542c889a45f8	4 subnets	-	No
<input type="checkbox"/>	Bootcamp-3tier-rtb-public	rtb-014b1935204b7fb0e	2 subnets	-	Yes

rtb-0db87542c889a45f8 / Bootcamp-3tier-rtb-private1-us-east-1a

Details Routes Subnet associations Edge associations Route propagation Tags

Routes (1) Both Edit routes

Filter routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

VPC > Route tables > [rtb-0db87542c889a45f8](#) > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
<input type="text" value="0.0.0.0/0"/>	<input type="text" value="local"/>		
	NAT Gateway		No
	<input type="text" value="nat-0e8f43c60b4a50319"/>		
<input type="button" value="Add route"/>			
<input type="button" value="Cancel"/> <input type="button" value="Preview"/> <input type="button" value="Save changes"/>			

- **Niveau 1 : Niveau Web (Frontend)**

Le niveau Web, également connu sous le nom de niveau « **Présentation** », est l'environnement dans lequel notre application sera livrée pour que les utilisateurs puissent interagir avec elle. Pour **BootcampApp**, c'est là que nous lancerons nos serveurs web qui hébergent le frontend de notre application.

Ce que nous allons construire :

- **Un modèle de lancement** de serveur web pour définir quel type d'instances EC2 qui sera provisionné pour l'application.
- **Un groupe de mise à l'échelle automatique (ASG)** qui provisionnera dynamiquement les instances EC2.
- **Un équilibreur de charge d'application (ALB)** pour aider à acheminer le trafic entrant vers les cibles appropriées.

1. Créer un modèle de lancement de serveur web

Il est temps de créer un modèle qui sera utilisé par notre ASG pour lancer dynamiquement des instances EC2 dans nos sous-réseaux publics.

- Dans la console EC2, naviguez vers « Launch templates » (modèles de lancement) dans le menu latéral « Instances ». Nous allons créer un nouveau modèle appelé « **bootcamp-webServer** » avec les dispositions suivantes :
 - AMI : Amazon 2 Linux
 - Type d'instance : t2.micro (1GB - Free Tier)
 - Une paire de clés nouvelle ou existante

Nous n'allons pas spécifier de sous-réseaux, mais nous allons créer un nouveau groupe de sécurité avec des règles SSH, HTTP et HTTPS entrantes. Assurez-vous que le VPC bootcamp-3tier approprié est sélectionné.

EC2 Dashboard

EC2 Global View


Events

Console-to-Code [Preview](#)

Instances

Instances

Instance Types

Launch Templates 

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity

Reservations [New](#)

Images

...


Compute

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 a template that can be used for on-demand launches and with managed services, including EC2 Auto Scaling and EC2 Fleet. Easily update your launch parameters by creating a new launch template version.

New launch template

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*

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

Template version description

Max 255 chars

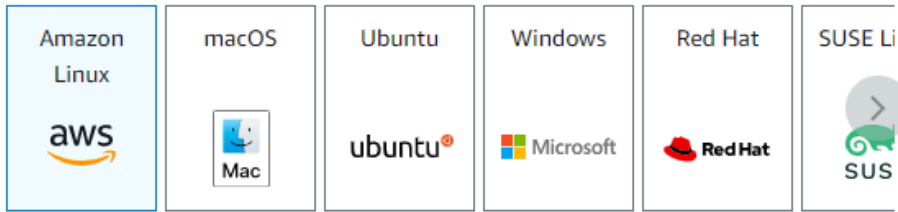
Auto Scaling guidance | [Info](#)

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

recently

Quick Start



Browse more AMIs

Including AMIs from
AWS, Marketplace and
the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI

Free tier eligible

ami-066784287e358dad1 (64-bit (x86), uefi-preferred) / ami-023508951a94f0c71 (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Architecture

Boot mode

AMI ID

64-bit (x86)



uefi-preferred

ami-066784287e358dad1

Verified provider

▼ 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

sourceDBKey



[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

Security group name - required

bootcamp-webserver-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](#)

bootcamp-webserver-sg

VPC [Info](#)

vpc-0bd9f4c4bbc08cedc (Bootcamp-3tier-vpc)
10.0.0.0/16

Inbound Security Group 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](#)

Custom

Source [Info](#)

Q Add CIDR, prefix list or security

0.0.0.0

Description - optional [Info](#)

e.g. SSH for admin desktop

User data - optional [Info](#)

Upload a file with your user data or enter it in the field.

Choose file

```
#!/bin/bash

sudo yum -y install httpd

sudo systemctl enable httpd
sudo systemctl start httpd

sudo echo '<!DOCTYPE html>

<html lang="en">
  <head>
    <meta charset="utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1"
```

☐ User data has already been base64 encoded

Software Image (AMI)

Amazon Linux 2023 AMI 2023.5.2...read more
ami-066784287e358dad1

Virtual server type (instance type)

-

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which

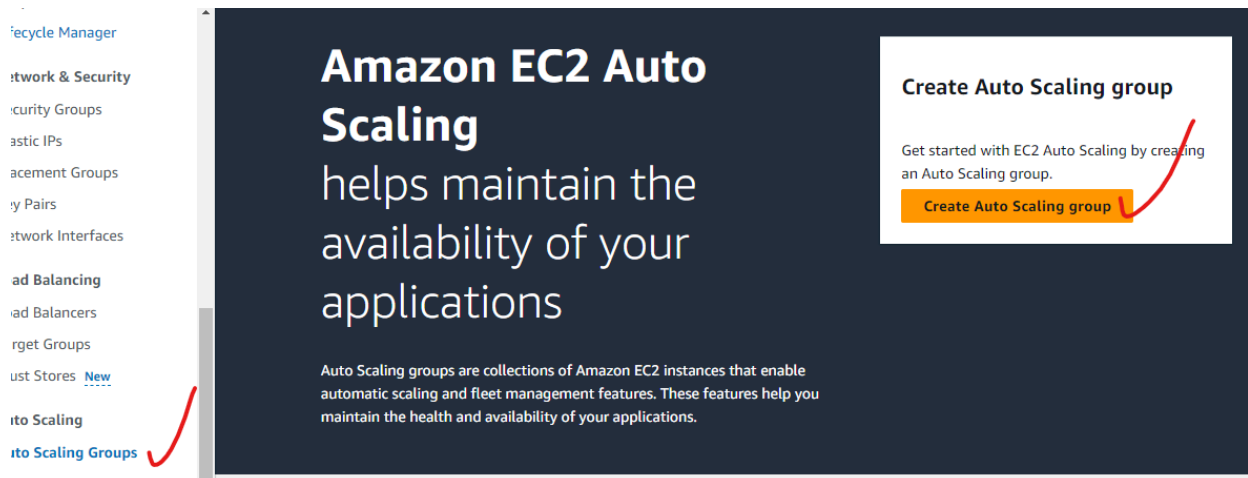
Cancel

Create launch template

2. Créer un groupe de mise à l'échelle automatique (ASG)

Pour assurer la haute disponibilité de l'application **Bootcamp-webApp** et limiter les points de défaillance uniques, nous allons créer un ASG qui fournira dynamiquement des instances EC2, selon les besoins, sur plusieurs AZ dans nos sous-réseaux publics.

- Naviguez vers la console ASG depuis le menu latéral et créez un nouveau groupe. L'ASG utilisera le modèle de lancement **Bootcamp-webserver** -template que nous avons configuré à l'étape précédente.
- Sélectionnez le **bootcamp-3tier** ainsi que les deux sous-réseaux publics.



Name

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

Bootcamp-ASG

Must be unique to this account in the current Region and no more than 255 characters.

Launch template [Info](#)

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.

bootcamp-webserver

[Create a launch template](#)

Instance type requirements [Info](#)

[Reset to launch template](#)

You can keep the same instance attributes or instance type from your launch template, or you can choose to override the launch template by specifying different instance attributes or manually adding instance types.

☒ Specify instance attributes

Provide your compute requirements. We fulfill your desired capacity with matching instance types based on your allocation strategy selection.

☐ Manually add instance types

Add one or more instance types. Any of the instance types may be launched to fulfill your desired capacity based on your allocation strategy selection.

Required instance attributes

Enter your compute requirements in virtual CPUs (vCPUs) and memory.

vCPUs

Enter the minimum and maximum number of vCPUs per instance.

minimum

maximum

☐ No minimum☐ No maximum

Memory (GiB)

Enter the minimum and maximum GiBs of memory per instance.

minimum

maximum

☐ No minimum☐ No maximum

Instance purchase options [Info](#)

Instances distribution

To run fault-tolerant workloads at low cost, define a percentage of instances that will be Spot Instances. Spot Instances are spare EC2 capacity that offer steep discounts compared to On-Demand prices that AWS can interrupt with a 2-minute notification.

% On-Demand

% Spot

☒ Include On-Demand base capacity

Specify how much On-Demand capacity the Auto Scaling group should have for its base portion before scaling by percentages. The maximum group size will be increased (but not decreased) to this value.

On-Demand Instances

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

vpc-0bd9f4c4bbc08cedc (Bootcamp-3tier-vpc) 10.0.0.0/16

[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

us-east-1a | subnet-0fcb798d7ab60ff13
(Bootcamp-3tier-subnet-public1-us-east-1a)
10.0.0.0/20

us-east-1b | subnet-0e3d5ab4aff815c75
(Bootcamp-3tier-subnet-public2-us-east-1b)
10.0.16.0/20

[Create a subnet](#)

Cancel Skip to review Previous **Next**

3. Équilibreur de charge d'application (ALB)

Nous aurons besoin d'un ALB pour distribuer le trafic HTTP entrant vers les cibles appropriées (nos EC2). L'ALB sera nommé 'bootcamp-ASG'. Nous voulons que cet ALB soit « tourné vers l'Internet », afin qu'il puisse écouter les requêtes HTTP/S.

Load balancing [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 a new load balancer

Define a new load balancer to create for attachment to this Auto Scaling group.

Load balancer type

Choose from the load balancer types offered below. Type selection cannot be changed after the load balancer is created. If you need a different type of load balancer than those offered here, visit the [Load Balancing console](#).

☒ Application Load Balancer
HTTP, HTTPS

☐ Network Load Balancer
TCP, UDP, TLS

Load balancer name

Name cannot be changed after the load balancer is created.

Bootcamp-ASG-1

Load balancer scheme

Scheme cannot be changed after the load balancer is created.

☐ Internal

☒ Internet-facing

Network mapping

Your new load balancer will be created using the same VPC and Availability Zone selections as your Auto Scaling group. You can select different subnets and add subnets from additional Availability Zones.

VPC

[vpc-0bd9f4c4bbc08cedc](#)

Bootcamp-3tier-vpc

Availability Zones and subnets

You must select a single subnet for each Availability Zone enabled. Only public subnets are available for selection to support DNS resolution.

☒ us-east-1a

subnet-0fcb798d7ab60ff13

☒ us-east-1b

subnet-0e3d5ab4aff815c75

Listeners and routing

If you require secure listeners, or multiple listeners, you can configure them from the [Load Balancing console](#) after your load balancer is created.

Protocol	Port	Default routing (forward to)
HTTP	80	Create a target group
		New target group name
		An instance target group with default settings will be created.
		Bootcamp-ASG-1

Tags - optional

Consider adding tags to your load balancer. Tags enable you to categorize your AWS resources so you can more easily manage them.

Add tag

50 remaining

EC2 health checks

[i](#) Always enabled

Additional health check types - optional

[Info](#)

☒ Turn on Elastic Load Balancing health checks Recommended

Elastic Load Balancing monitors whether instances are available to handle requests. When it reports an unhealthy instance, EC2 Auto Scaling can replace it on its next periodic check.

[i](#) EC2 Auto Scaling will start to detect and act on health checks performed by Elastic Load Balancing. ×
To avoid unexpected terminations, first verify the settings of these health checks in the [Load Balancer console](#)

☐ Turn on VPC Lattice health checks

VPC Lattice can monitor whether instances are available to handle requests. If it considers a target as failed a health check, EC2 Auto Scaling replaces it after its next periodic check.

☐ Turn on Amazon EBS health checks

EBS monitors whether an instance's root volume or attached volume stalls. When it reports an unhealthy volume, EC2 Auto Scaling can replace the instance on its next periodic health check.

Health check grace period [Info](#)

This time period delays the first health check until your instances finish initializing. It doesn't prevent an instance from terminating when placed into a non-running state.

300 seconds

Additional settings

Monitoring [Info](#)

☐ Enable group metrics collection within CloudWatch

Default instance warmup [Info](#)

The amount of time that CloudWatch metrics for new instances do not contribute to the group's aggregated instance metrics, as their usage data is not reliable yet.

☐ Enable default instance warmup

Cancel

Skip to review

Previous

Next

- **Taille du groupe**

Nous voulons définir un nombre minimum et maximum d'instances que l'ASG peut provisionner :

- Capacité souhaitée : 2
- Capacité minimale : 2
- Capacité maximale : 5

Group size [Info](#)

Set the initial size of the Auto Scaling group. After creating the group, you can change its size to meet demand, either manually or by using automatic scaling.

Desired capacity type

Choose the unit of measurement for the desired capacity value. vCPUs and Memory(GiB) are only supported for mixed instances groups configured with a set of instance attributes.

Units (number of instances) ▼

Desired capacity

Specify your group size.

2

Scaling [Info](#)

You can resize your Auto Scaling group manually or automatically to meet changes in demand.

Scaling limits

Set limits on how much your desired capacity can be increased or decreased.

Min desired capacity

Equal or less than desired capacity

Max desired capacity

Equal or greater than desired capacity

- Nous ajouterons également une politique de mise à l'échelle dynamique qui indique à l'ASG quand augmenter ou diminuer le nombre d'instances EC2. Pour cette version, nous surveillerons l'utilisation du CPU et créerons plus d'instances lorsque l'utilisation est supérieure à 50 % (n'hésitez pas à utiliser la métrique appropriée pour votre application).

Automatic scaling - *optional*

Choose whether to use a target tracking policy | [Info](#)

You can set up other metric-based scaling policies and scheduled scaling after creating your Auto Scaling group.



No scaling policies

Your Auto Scaling group will remain at its initial size and will not dynamically resize to meet demand.



Target tracking scaling policy

Choose a CloudWatch metric and target value and let the scaling policy adjust the desired capacity in proportion to the metric's value.

Scaling policy name

Metric type | [Info](#)

Monitored metric that determines if resource utilization is too low or high. If using EC2 metrics, consider enabling detailed monitoring for better scaling performance.

Target value

Instance warmup | [Info](#)

seconds

The screenshot shows the 'Launch configuration' step of the AWS Auto Scaling console. It features four tabs for scaling behavior: 'Mixed behavior' (selected), 'Prioritize availability', 'Control costs', and 'Flexible'. Under 'Mixed behavior', the 'No policy' option is selected. Below these tabs is the 'Instance scale-in protection' section, which includes a checkbox to 'Enable instance scale-in protection'. At the bottom, there are four buttons: 'Cancel', 'Skip to review', 'Previous', and 'Next' (highlighted in orange with a red checkmark).

Mixed behavior

- ☒ **No policy**
For rebalancing events, new instances will launch before terminating others. For all other events, instances terminate and launch at the same time.

Prioritize availability

- ☐ **Launch before terminating**
Launch new instances and wait for them to be ready before terminating others. This allows you to go above your desired capacity by a given percentage and may temporarily increase costs.

Control costs

- ☐ **Terminate and launch**
Terminate and launch instances at the same time. This allows you to go below your desired capacity by a given percentage and may temporarily reduce availability.

Flexible

- ☐ **Custom behavior**
Set custom values for the minimum and maximum amount of available capacity. This gives you greater flexibility in setting how far below and over your desired capacity EC2 Auto Scaling goes when replacing instances.

Instance scale-in protection

Scale-in protection prevents newly launched instances from being terminated by scaling activities. Make sure to remove scale-in protection for the group or individual instances when instances are ready to be terminated.

☐ Enable instance scale-in protection

Cancel Skip to review Previous **Next**

Faites nex, enfin review and create.

The screenshot shows the 'Add tags' step of the AWS Auto Scaling console. It has a title 'Step 6: Add tags' and an 'Edit' button. Below the title is a table with columns 'Key', 'Value', and 'Tag new instances'. The table is currently empty, with a 'No tags' message. At the bottom, there are three buttons: 'Cancel', 'Previous', and 'Create Auto Scaling group' (highlighted in orange with a red checkmark).

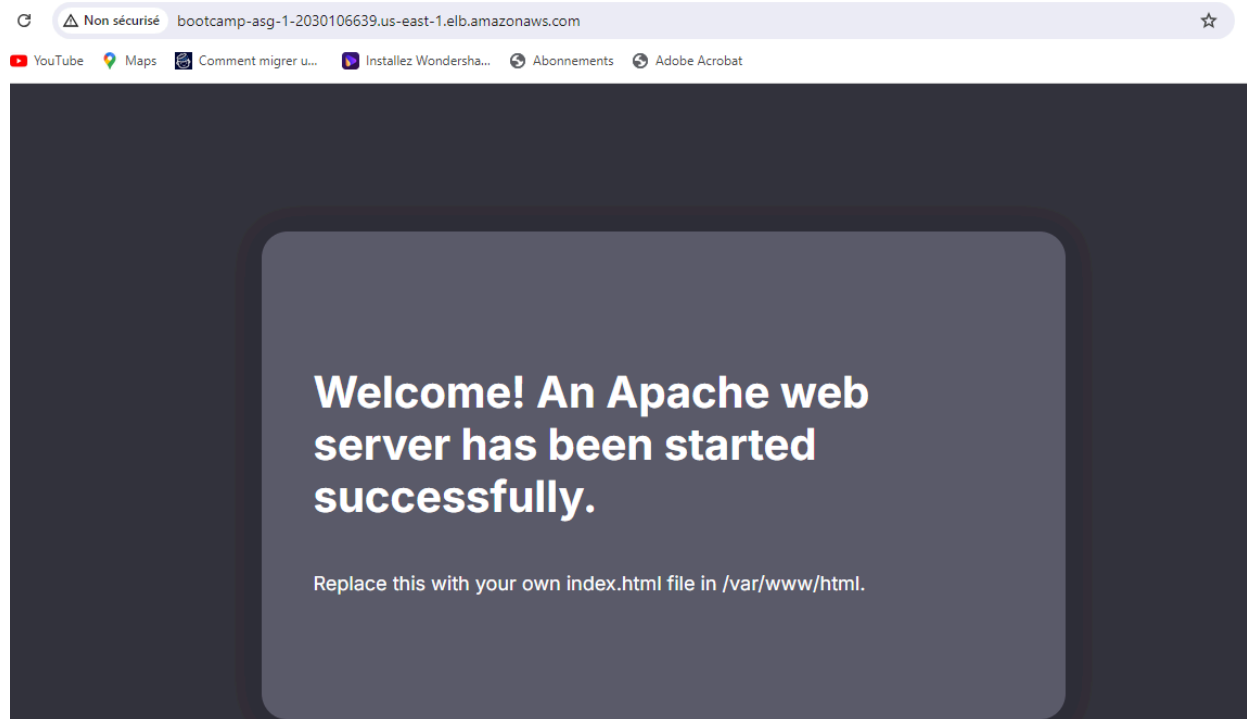
Step 6: Add tags Edit

Tags (0)

Key	Value	Tag new instances
No tags		

Cancel Previous **Create Auto Scaling group**

Pour voir si notre ALB achemine correctement le trafic, accédons à son DNS public. Nous devrions pouvoir accéder au site web que nous avons mis en place lors de la création de notre modèle de lancement EC2.



- **Niveau 2 : Niveau de l'application (backend)**

Le niveau d'application est essentiellement l'endroit où se trouve le cœur de notre application BootcampApp. C'est là que le code source et les opérations de base envoient/récupèrent les données vers/depuis les niveaux Web et Base de données.

La structure est très similaire à celle du niveau Web, mais avec quelques ajouts et considérations mineures.

Ce que nous allons construire :

- Un modèle de lancement pour définir le type d'instances EC2.
- Un groupe de mise à l'échelle automatique (ASG) pour provisionner dynamiquement les instances EC2.
- Un Application Load Balancer (ALB) pour acheminer le trafic depuis le niveau Web.
- Un hôte Bastion pour se connecter en toute sécurité à nos serveurs d'application.

1. Créer un modèle de lancement de serveur d'application

- Ce template définira le type d'instances EC2 que nos services backend utiliseront, donc créons un nouveau template appelé '**bootcam-appServer-template**'.

- Nous utiliserons les mêmes paramètres que le modèle `bootcamp-webServer-template` (Amazon 2 Linux, t2.micro-1GB, même paire de clés).
- Les paramètres de notre groupe de sécurité sont différents. N'oubliez pas qu'il s'agit d'un sous-réseau privé, où se trouve tout le code source de notre application. Nous devons prendre des précautions pour qu'il ne soit pas accessible de l'extérieur.
- Nous voulons autoriser ICMP-IPv4 depuis le **bootcamp-webServer-sg**, ce qui nous permet d'envoyer un ping au serveur d'application depuis notre serveur web.

[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*

bootcam-appServer-template ✓

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

Template version description

bootcam-appServer-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

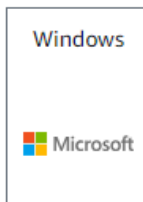
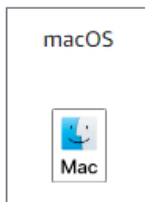
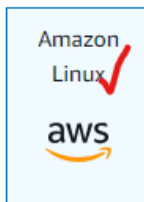
▼ Application and OS Images (Amazon Machine Image) - required [Info](#)

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

Recents

Quick Start



[Browse more AMIs](#)

Including AMIs from
AWS, Marketplace and
the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI

ami-066784287e358dad1 (64-bit (x86), uefi-preferred) / ami-023508951a94f0c71 (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible ▼

▼ Instance type [Info](#) | [Get advice](#)

Advanced

Instance type

t2.micro

Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour
On-Demand RHEL base pricing: 0.026 USD per Hour
On-Demand Linux base pricing: 0.0116 USD per Hour

☐ All generations

[Compare instance types](#)


Additional costs apply for AMIs with pre-installed software

▼ 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

sourceDBKey

 [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

Security group name - required

bootcamp-appserver-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

bootcamp-appserver-SG

VPC

Info

vpc-0bd9f4c4bbbc08cedc (Bootcamp-3tier-vpc)
10.0.0.0/16
▼

↻

- Nous voulons autoriser ICMP-IPv4 depuis le **bootcamp-webServer-sg**, ce qui nous permet d'envoyer un ping au serveur d'application depuis notre serveur web.

Inbound Security Group Rules

▼
Security group rule 1 (ICMP, All, sg-073c712ab063716b6)
Remove

Type

Info

All ICMP - IPv4

Protocol

Info

ICMP

Port range

Info

All

Source type

Info

Custom

Source

Info

Add CIDR, prefix list or security
sg-073c712ab063716b6
X

Description - optional

Info

e.g. SSH for admin desktop

Add security group rule

►
Advanced network configuration

Entrez dans détails avance, au niveau de user data, coller le script suivant:

```
#!/bin/bash
```

```
sudo yum install mysql -y
```

User data - optional | Info

Upload a file with your user data or enter it in the field.

Choose file

```
#!/bin/bash
sudo yum install mysql -y
```

☐ User data has already been base64 encoded

Software Image (AMI)
Amazon Linux 2023 AMI 2023.5.2...[read more](#)
ami-066784287e358dad1

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which

Cancel Create launch template

2. Créer un groupe de mise à l'échelle automatique (ASG)

Comme pour le niveau Web, nous allons créer un ASG à partir du modèle **bootcamp-appServer-template** appelé '**bootcamp-app-asg**'.

Assurez-vous de sélectionner le **bootcamp-3tier-vpc** et les 2 sous-réseaux privés (subnet-private1 et subnet-private2).

Nous

allons

maintenant

créer

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

bootcamp-app-ASG

Must be unique to this account in the current Region and no more than 255 characters.

Launch template [Info](#)

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.

bootcam-appServer-template

[Create a launch template](#)

Version

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-0bd9f4c4bbc08cedc (Bootcamp-3tier-vpc)
10.0.0.0/16

[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

us-east-1a | subnet-07cbb254b1e6ce2f9
(Bootcamp-3tier-subnet-WebApp-private3-us-east-1a)
10.0.160.0/20

us-east-1b | subnet-069dd609a5941e905
(Bootcamp-3tier-DB-subnet-private2-us-east-1b)
10.0.144.0/20

[Create a subnet](#)

Cancel

Skip to review

Previous

Next

3. Équilibreur de charge d'application (ALB)

Nous allons maintenant créer un autre ALB qui achemine le trafic du niveau Web vers le niveau Application. Nous le nommerons **'bootcamp-app-asg'**.

Cette fois-ci, nous voulons que l'ALB soit **'Internal'**, puisque nous routons le trafic depuis notre niveau Web, et non depuis l'Internet.

Configure advanced options - *optional* [Info](#)

Integrate your Auto Scaling group with other services to distribute network traffic across multiple servers using a load balancer or to establish service-to-service communications using VPC Lattice. You can also set options that give you more control over health check replacements and monitoring.

Load balancing [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 a new load balancer

Define a new load balancer to create for attachment to this Auto Scaling group.

Load balancer type

Choose from the load balancer types offered below. Type selection cannot be changed after the load balancer is created. If you need a different type of load balancer than those offered here, [visit the Load Balancing console](#).

☒ Application Load Balancer
HTTP, HTTPS

☐ Network Load Balancer
TCP, UDP, TLS

Load balancer name

Name cannot be changed after the load balancer is created.

bootcamp-app-ASG-1

Load balancer scheme

Scheme cannot be changed after the load balancer is created.

☒ Internal

☐ Internet-facing

Nous allons également créer un autre groupe cible qui ciblera nos instances EC2 appServer.

VPC

vpc-0bd9f4c4bbc08cedc [🔗](#)

Bootcamp-3tier-vpc

Availability Zones and subnets

You must select a single subnet for each Availability Zone enabled. Only public subnets are available for selection to support DNS resolution.

☒ us-east-1a

subnet-07cbb254b1e6ce2f9 ▼

☒ us-east-1b

subnet-069dd609a594f8905 ▼

Listeners and routing

If you require secure listeners, or multiple listeners, you can configure them from the [Load Balancing console](#) [🔗](#) after your load balancer is created.

Protocol

HTTP

Port

80

Default routing (forward to)

Create a target group ▼

New target group name

An instance target group with default settings will be created.

bootcamp-app-ASG-1

Tags - optional

Consider adding tags to your load balancer. Tags enable you to categorize your AWS resources so you can more easily manage them.

VPC Lattice integration options [Info](#)

To improve networking capabilities and scalability, integrate your Auto Scaling group with VPC Lattice. VPC Lattice facilitates communications between AWS services and helps you connect and manage your applications across compute services in AWS.

Select VPC Lattice service to attach



No VPC Lattice service

VPC Lattice will not manage your Auto Scaling group's network access and connectivity with other services.



Attach to VPC Lattice service

Incoming requests associated with specified VPC Lattice target groups will be routed to your Auto Scaling group.

[Create new VPC Lattice service](#)

Health checks

Health checks increase availability by replacing unhealthy instances. When you use multiple health checks, all are evaluated, and if at least one fails, instance replacement occurs.

EC2 health checks



Always enabled

Additional health check types - optional [Info](#)



Turn on Elastic Load Balancing health checks **Recommended**

Elastic Load Balancing monitors whether instances are available to handle requests. When it reports an unhealthy instance, EC2 Auto

Configure group size and scaling - optional [Info](#)

Define your group's desired capacity and scaling limits. You can optionally add automatic scaling to adjust the size of your group.

Group size [Info](#)

Set the initial size of the Auto Scaling group. After creating the group, you can change its size to meet demand, either manually or by using automatic scaling.

Desired capacity type

Choose the unit of measurement for the desired capacity value. vCPUs and Memory(GiB) are only supported for mixed instances groups configured with a set of instance attributes.

Units (number of instances)



Desired capacity

Specify your group size.

2

Scaling [Info](#)

You can resize your Auto Scaling group manually or automatically to meet changes in demand.

Scaling limits

Set limits on how much your desired capacity can be increased or decreased.

Min desired capacity

Equal or less than desired capacity

Max desired capacity

Equal or greater than desired capacity

Automatic scaling - optional

Choose whether to use a target tracking policy [Info](#)

You can set up other metric-based scaling policies and scheduled scaling after creating your Auto Scaling group.

☐ No scaling policies

Your Auto Scaling group will remain at its initial size and will not dynamically resize to meet demand.

☒ Target tracking scaling policy

Choose a CloudWatch metric and target value and let the scaling policy adjust the desired capacity in proportion to the metric's value.

Scaling policy name

Mixed behavior

☒ No policy

For rebalancing events, new instances will launch before terminating others. For all other events, instances terminate and launch at the same time.

Prioritize availability

☐ Launch before terminating

Launch new instances and wait for them to be ready before terminating others. This allows you to go above your desired capacity by a given percentage and may temporarily increase costs.

Control costs

☐ Terminate and launch

Terminate and launch instances at the same time. This allows you to go below your desired capacity by a given percentage and may temporarily reduce availability.

Flexible

☐ Custom behavior

Set custom values for the minimum and maximum amount of available capacity. This gives you greater flexibility in setting how far below and over your desired capacity EC2 Auto Scaling goes when replacing instances.

Instance scale-in protection

Scale-in protection prevents newly launched instances from being terminated by scaling activities. Make sure to remove scale-in protection for the group or individual instances when instances are ready to be terminated.

☐ Enable instance scale-in protection

Cancel

Skip to review

Previous

Next

valider le tout sur create

Tags (0)

Key	Value	Tag new instances
No tags		

Cancel Previous Create Auto Scaling group

Auto Scaling groups (2) [Info](#) ↻ Launch configurations Launch templates [↗](#) Actions ▼ Create Auto Scaling group

< 1 > ⚙

<input type="checkbox"/>	Name ▼	Launch template/configuration ↗ ▼	Instances ▼	Status ▼	Desired capacity ▼	Min ▼	Max ▼
<input type="checkbox"/>	bootcamp-app-ASG	bootcam-appServer-template Version D	2	-	2	2	5
<input type="checkbox"/>	bootcamp-ASG	bootcamp-launch-template Version Defi	3	-	2	2	5

C'est parfait ! Nous devrions voir deux instances EC2 supplémentaires fonctionner à partir de nos sous-réseaux privés.

- Confirmation de la connectivité depuis le niveau Web
- Nos serveurs d'application sont opérationnels. Vérifions la connectivité en envoyant un ping au serveur d'application depuis l'un des serveurs web.
- Connectez-vous en SSH à l'EC2 du serveur web et envoyez un ping à l'adresse IP privée de l'un des EC2 du serveur d'applications.
- Pour cela, nous allons faire un ping sur l'adresse IP privée du serveur d'application.

<input checked="" type="checkbox"/>	i-008308ba028c20b6e	Shutting-d...	t2.micro	2/2 checks passec	View
<input type="checkbox"/>	i-08088f9d8577d4610	Terminated	t2.micro	-	View
<input type="checkbox"/>	i-04136d5fa4ab7955a	Running	t2.micro	2/2 checks passec	View
<input type="checkbox"/>	i-000930386e4bfac3f	Terminated	t2.micro	-	View
<input type="checkbox"/>	i-03a7667a81952fd64	Running	t2.micro	2/2 checks passec	View

i-008308ba028c20b6e

[Details](#) | [Status and alarms](#) | [Monitoring](#) | [Security](#) | [Networking](#) | [Storage](#) | [Tags](#)

▼ Instance summary [Info](#)

Instance ID

i-008308ba028c20b6e

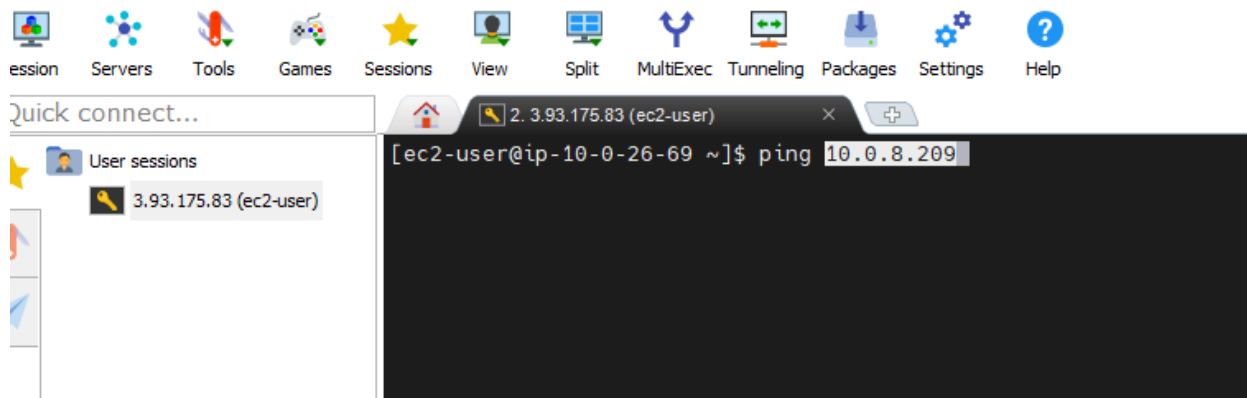
Public IPv4 address

-

✓ Private IPv4 address copied

Private IPv4 addresses
 10.0.8.209

Sur le shell du webserver, tapons **ping 10.0.163.238**



En cas de succès, vous devriez obtenir une réponse répétée comme celle-ci :

```
PING 10.0.163.238 (10.0.163.238) 56(84) bytes of data.  
64 bytes from 10.0.163.238: icmp_seq=1 ttl=127 time=2.33 ms  
64 bytes from 10.0.163.238: icmp_seq=2 ttl=127 time=0.903 ms  
64 bytes from 10.0.163.238: icmp_seq=3 ttl=127 time=0.912 ms  
64 bytes from 10.0.163.238: icmp_seq=4 ttl=127 time=0.868 ms  
64 bytes from 10.0.163.238: icmp_seq=5 ttl=127 time=0.995 ms  
64 bytes from 10.0.163.238: icmp_seq=6 ttl=127 time=0.908 ms  
64 bytes from 10.0.163.238: icmp_seq=7 ttl=127 time=0.881 ms  
64 bytes from 10.0.163.238: icmp_seq=8 ttl=127 time=0.974 ms  
64 bytes from 10.0.163.238: icmp_seq=9 ttl=127 time=0.869 ms  
64 bytes from 10.0.163.238: icmp_seq=10 ttl=127 time=0.913 ms  
64 bytes from 10.0.163.238: icmp_seq=11 ttl=127 time=0.947 ms  
64 bytes from 10.0.163.238: icmp_seq=12 ttl=127 time=0.908 ms  
64 bytes from 10.0.163.238: icmp_seq=13 ttl=127 time=0.918 ms  
64 bytes from 10.0.163.238: icmp_seq=14 ttl=127 time=0.732 ms  
64 bytes from 10.0.163.238: icmp_seq=15 ttl=127 time=0.866 ms  
64 bytes from 10.0.163.238: icmp_seq=16 ttl=127 time=0.865 ms  
64 bytes from 10.0.163.238: icmp_seq=17 ttl=127 time=0.926 ms  
64 bytes from 10.0.163.238: icmp_seq=18 ttl=127 time=0.927 ms  
64 bytes from 10.0.163.238: icmp_seq=19 ttl=127 time=0.921 ms  
64 bytes from 10.0.163.238: icmp_seq=20 ttl=127 time=0.844 ms
```

Woo ! Nous avons réussi à envoyer un ping au serveur de l'application et nous avons reçu une réponse !

4. Créer un hôte Bastion

Un **hôte bastion** est un serveur dédié utilisé pour accéder en toute sécurité à un réseau privé à partir d'un réseau public. Nous voulons protéger notre Application Tier des points d'accès extérieurs potentiels, nous allons donc créer une instance EC2 dans le Web Tier, en dehors de l'ASG. C'est le seul serveur qui sera utilisé comme passerelle vers nos serveurs d'applications.

- Dans la console EC2, lancez une nouvelle instance appelée « **bootcamp-bastionHost** ». Nous utiliserons les mêmes dispositions que précédemment (Amazon Linux2, t2.micro). Assurez-vous que le **bootcamp-3tier-vpc** est sélectionné, ainsi que l'un des sous-réseaux publics.

Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name

bootcamp-BastionHost ✓

[Add additional tags](#)

▼ Application and OS Images (Amazon Machine Image) [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

Recents

Quick Start



macOS



Ubuntu



Windows



Red Hat



SUSE Li



[Browse more AMIs](#)

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI

ami-066784287e358dad1 (64-bit (x86), uefi-preferred) / ami-023508951a94f0c71 (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs ✓

Free tier eligible ▼

▼ Instance type [Info](#) | [Get advice](#)

Instance type

t2.micro

Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour
On-Demand RHEL base pricing: 0.026 USD per Hour
On-Demand Linux base pricing: 0.0116 USD per Hour

☒ All generations

[Compare instance types](#)

Additional costs apply for AMIs with pre-installed software

▼ 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*

sourceDBKey

 [Create new key pair](#)

▼ Network settings [Info](#)

VPC - *required* | [Info](#)

vpc-0bd9f4c4bbc08cedc (Bootcamp-3tier-vpc)
10.0.0.0/16



Subnet | [Info](#)

subnet-0fcb798d7ab60ff13 Bootcamp-3tier-subnet-public1-us-east-1a
VPC: vpc-0bd9f4c4bbc08cedc Owner: 010928200112 Availability Zone: us-east-1a
Zone type: Availability Zone IP addresses available: 4087 CIDR: 10.0.0.0/20



[Create new subnet](#)

Auto-assign public IP | [Info](#)

Enable

Additional charges apply when outside of free tier allowance

Créez un nouveau groupe de sécurité appelé « **bootcamp-bastionHost-sg** » et autorisez uniquement SSH via My IP.

Inbound rules [Info](#)

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	
sg-08891037d6e2da48c	All ICMP - IPv4	ICMP	All	Cust...		Delete
-	SSH	TCP	22	Cust...	sg-0395ac0614f8675a	Delete

[Add rule](#)

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

- **Tester la connexion**

Voyons si nous pouvons nous connecter à notre serveur d'application via notre hôte bastion. Pour cela, rassurez-vous de recréer la clé dans votre serveur de bastion, comme sur l'image ci-dessous (étant connecté à mon serveur de bastion).

Quick connect...

/home/ec2-user/

Name

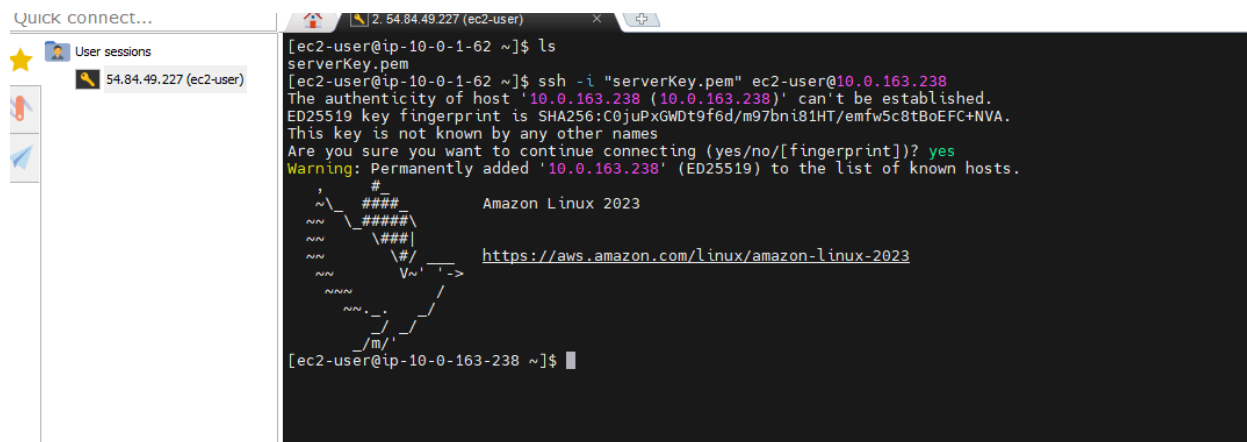
..
.ssh
.bash_history
.bash_logout
.bash_profile
.bashrc

2. 54.84.49.227 (ec2-user)

[ec2-user@ip-10-0-1-62 ~]\$ ls
[ec2-user@ip-10-0-1-62 ~]\$ touch serverKey.pem
[ec2-user@ip-10-0-1-62 ~]\$ ls
serverKey.pem
[ec2-user@ip-10-0-1-62 ~]\$ nano serverKey.pem
[ec2-user@ip-10-0-1-62 ~]\$ chmo 400 serverKey.pem
-bash: chmo: command not found
[ec2-user@ip-10-0-1-62 ~]\$ chmod 400 serverKey.pem
[ec2-user@ip-10-0-1-62 ~]\$

Une fois la paire de clés ajoutée à l'agent, connectez-vous en SSH à l'hôte Bastion.

Et puis SSH dans notre serveur d'application (rappelez-vous, nous avons besoin de l'adresse IPv4 privée)



Succès !

Nous avons réussi à construire l'architecture du niveau application pour notre application!

N'oubliez pas qu'il s'agit de la couche « backend », où se trouve notre code source et où les opérations backend envoient/récupèrent des données vers/depuis le niveau Web et le niveau Base de données.

Niveau 3 : Niveau base de données (stockage et récupération des données)

Nous y sommes presque ! Il est maintenant temps de construire le dernier niveau de notre architecture d'application **Bootcamp : la base de données**. Toute application a besoin d'un moyen de stocker des données importantes, telles que les informations de connexion des utilisateurs, les données de session, les transactions, le contenu de l'application, etc. Nos serveurs d'application doivent être en mesure de lire et d'écrire dans les bases de données afin d'effectuer les tâches nécessaires et de fournir un contenu/service adéquat au niveau Web et aux utilisateurs. Nous allons utiliser un service de base de données relationnelle (RDS) qui utilise MySQL.

Ce que nous allons construire :

- Un groupe de sécurité de la base de données qui autorise les requêtes mySQL sortantes et entrantes vers et depuis nos serveurs d'applications.
- Un groupe de sous-réseau DB pour s'assurer que la base de données est créée dans les sous-réseaux appropriés.
- Une base de données RDS avec MySql.

1. Créer un groupe de sécurité pour la base de données

Nos serveurs d'application ont besoin d'un moyen d'accéder à la base de données, alors commençons par créer un groupe de sécurité qui autorise le trafic entrant depuis les serveurs d'application.

Créons un nouveau groupe de sécurité appelé '**bootcamp-db-sg**'. Assurez-vous que le vpc bootcamp est sélectionné.

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

Basic details

Security group name Info

Name cannot be edited after creation.

Description Info

VPC Info

Nous devons maintenant ajouter des règles **entrantes ET sortantes** qui autorisent les requêtes MySQL vers et depuis les serveurs d'application sur le port 3306.

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>
MYSQL/Aurora	TCP	3306	Cust... Q sg-04901e88c0021808 sg-04901e88c0021808 3	<input type="text"/>

Add rule

Outbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Destination Info	Description - optional Info
All traffic	All	All	Cust... <input type="text" value="0.0.0.0/0"/>	<input type="text"/>
MySQL/Aurora	TCP	3306	Cust... <input type="text" value="sg-04901e88c00218083"/>	<input type="text"/>

Nous devrions faire de même pour le **bootcamp-appServer-sg**. Type **MYSQL/AURORA** et **source** c'est le groupe de sécurité de la base de données **bootcamp-db-sg**

sg-04901e88c00218083 - bootcamp-appserver-SG [Actions](#)

Details

Security group name bootcamp-appserver-SG	Security group ID sg-04901e88c00218083	Description bootcamp-appserver-SG	VPC ID vpc-0bd9f4c4bbc08cedc
Owner 010928200112	Inbound rules count 2 Permission entries	Outbound rules count 1 Permission entry	

[Inbound rules](#) | [Outbound rules](#) | [Tags](#)

Inbound rules (2)

< 1 >

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	
sgr-0b920ec9d71422647	SSH	TCP	22	Cust...	<input type="text"/>	<input type="button" value="Delete"/>
sgr-08891037d6e2da48c	All ICMP - IPv4	ICMP	All	Cust...	<input type="text"/>	<input type="button" value="Delete"/>
-	MySQL/Aurora	TCP	3306	Cust...	<input type="text"/>	<input type="button" value="Delete"/>

EC2 > Security Groups > sg-04901e88c00218083 - bootcamp-appserver-SG > Edit outbound rules

Edit outbound rules [Info](#)

Outbound rules control the outgoing traffic that's allowed to leave the instance.

Outbound rules [Info](#)

Security group rule ID	Type Info	Protocol Info	Port range Info	Destination Info	Description - optional Info	
sgr-0c82a8db7853e79eb	All traffic	All	All	Cust...	<input type="text"/>	<input type="button" value="Delete"/>
-	MySQL/Aurora	TCP	3306	Cust...	<input type="text"/>	<input type="button" value="Delete"/>

2. Créer un groupe de sous-réseaux DB

Dans la console RDS, sous le menu latéral '**Subnet groups**', créez un nouveau groupe de sous-réseaux appelé '**bootcamp-db-subnetGroup**'. Assurez-vous que le **bootcamp-vpc** est sélectionné.

Subnet groups

Parameter groups

Option groups

Custom engine versions

Zero-ETL integrations [New](#)

[RDS](#) > Subnet groups

Subnet groups (1)



Edit

Delete

Create DB subnet group

Filter by subnet group

< 1 > ⚙

<input type="checkbox"/>	Name	Description	Status	VPC
<input type="checkbox"/>	default	default	✔ Complete	vpc-058e2b9ce56adf840

[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.

bootcamp-db-subnetGroup

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

Description

bootcamp-db-subnetGroup

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.

Bootcamp-3tier-vpc (vpc-0bd9f4c4bbc08cedc)

Sélectionnez nos deux AZ (us-east-1 et us-east-2) et nos sous-réseaux privés (-subnet-private3 et -subnet-private4). Malheureusement, la liste déroulante de sélection ne fournit pas les noms des sous-réseaux, nous devons donc retourner à notre tableau de bord principal Subnets pour obtenir les bons identifiants.

Add subnets

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

Choose an availability zone ▼

us-east-1a ✕ us-east-1b ✕

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

Select subnets ▼

subnet-07cbb254b1e6ce2f9 (10.0.160.0/20) ✕

subnet-0654ee8cc2f87d1ce (10.0.176.0/20) ✕

For Multi-AZ DB clusters, you must select 3 subnets in 3 different Availability Zones.

Subnets selected (2)

Availability zone	Subnet ID	CIDR block
us-east-1a	subnet-07cbb254b1e6ce2f9	10.0.160.0/20
us-east-1b	subnet-0654ee8cc2f87d1ce	10.0.176.0/20

Cancel Create

3. Créer une base de données RDS

Sous la console RDS et le menu latéral « **Databases** », créez une nouvelle base de données avec un moteur MySQL.

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.

Engine options

Engine type [Info](#)

☐ Aurora (MySQL Compatible)



☐ Aurora (PostgreSQL Compatible)



☒ **MySQL**



☐ MariaDB



☐ PostgreSQL



☐ Oracle

ORACLE®

MySQL Community

Engine version [Info](#)

View the engine versions that support the following database features.

▼ Hide filters

☒ Show versions that support the Multi-AZ DB cluster [Info](#)

Create a Multi-AZ DB cluster with one primary DB instance and two readable standby DB instances. Multi-AZ DB clusters provide up to 2x faster transaction commit latency and automatic failover in typically under 35 seconds.

☐ Show versions that support the Amazon RDS Optimized Writes [Info](#)

Amazon RDS Optimized Writes improves write throughput by up to 2x at no additional cost.

Engine Version

MySQL 8.0.35

☐ Enable RDS Extended Support [Info](#)

Amazon RDS Extended Support is a [paid offering](#). By selecting this option, you consent to being charged for this offering if you are running your database major version past the RDS end of standard support date for that version. Check the end of standard support date for your major version in the [RDS for MySQL documentation](#).

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](#)

Settings

DB cluster identifier [Info](#)

Enter a name for your DB cluster. The name must be unique across all DB clusters owned by your AWS account in the current AWS Region.

The DB cluster identifier is case-insensitive, but is stored as all lowercase (as in "mydbcluster"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

▼ Credentials Settings

Master username [Info](#)

Type a login ID for the master user of your DB cluster.

1 to 16 alphanumeric characters. The first character must be a letter.

Master password [Info](#)

Password strength [Strong](#)

Minimum constraints: At least 8 printable ASCII characters. Can't contain any of the following symbols: / ' " @

Confirm master password [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.


Virtual private cloud (VPC) [Info](#)

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

Bootcamp-3tier-vpc (vpc-0bd9f4c4bbc08cedc)

7 Subnets, 3 Availability Zones

Only VPCs with a corresponding DB subnet group are listed.

 After a database is created, you can't change its VPC.

DB subnet group [Info](#)

Choose the DB subnet group. The DB subnet group defines which subnets and IP ranges the DB instance can use in the VPC that you selected.

bootcamp-db-subnetgroup

3 Subnets, 3 Availability Zones

Public access [Info](#)

☐ Yes

RDS assigns a public IP address to the database. Amazon EC2 instances and other resources outside of the VPC can connect to your database. Resources inside the VPC can also connect to the database. Choose one or more VPC security groups that specify which resources can connect to the database.

☒ No

RDS doesn't assign a public IP address to the database. Only Amazon EC2 instances and other resources inside the VPC can connect to your database. Choose one or more VPC security groups that specify which resources can connect to the database.

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

bootcamp-db-sg X

Availability Zone [Info](#)

us-east-1a

Certificate authority - optional [Info](#)

Using a server certificate provides an extra layer of security by validating that the connection is being made to an Amazon database. It does so by checking the server certificate that is automatically installed on all databases that you provision.

rds-ca-rsa2048-g1 (default)

Expiry: May 26, 2061

If you don't select a certificate authority, RDS chooses one for you.

Estimated Monthly costs

DB instance	12.41 USD
Storage	2.30 USD
Total	14.71 USD

This billing estimate is based on on-demand usage as described in [Amazon RDS Pricing](#). Estimate does not include costs for backup storage, IOs (if applicable), or data transfer.

Estimate your monthly costs for the DB Instance using the [AWS Simple Monthly Calculator](#).


Estimated monthly costs

The Amazon RDS Free Tier is available to you for 12 months. Each calendar month, the free tier will allow you to use the Amazon RDS resources listed below for free:

- 750 hrs of Amazon RDS in a Single-AZ db.t2.micro, db.t3.micro or db.t4g.micro Instance.
- 20 GB of General Purpose Storage (SSD).
- 20 GB for automated backup storage and any user-initiated DB Snapshots.

[Learn more about AWS Free Tier.](#)

When your free usage expires or if your application use exceeds the free usage tiers, you simply pay standard, pay-as-you-go service rates as described in the [Amazon RDS Pricing page](#).

 You are responsible for ensuring that you have all of the necessary rights for any third-party products or services that you use with AWS services.

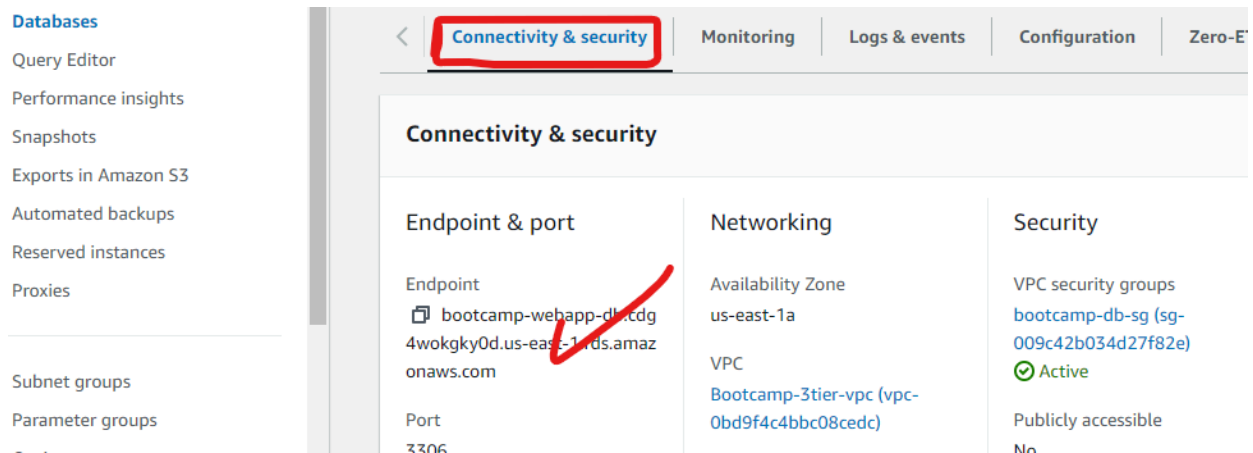
Cancel

Create database

- Se connecter à la base de données

Une fois la base de données créée, nous aurons besoin du point d'accès à la base de données pour établir une connexion à partir du serveur d'application.

Cliquons sur notre base de données et au niveau “connectivity & security”, copions le endpoint



Souvenez-vous dans notre AppServer, nous avons déjà installé MySQL, donc étant déjà connecté sur notre serveur d'application à travers le Bastion Host, nous allons coller la commande suivante sur le terminal.

```
mysql -h YOUR_DB_ENDPOINT -P 3306 -u YOUR_DB_USERNAME -p.
```