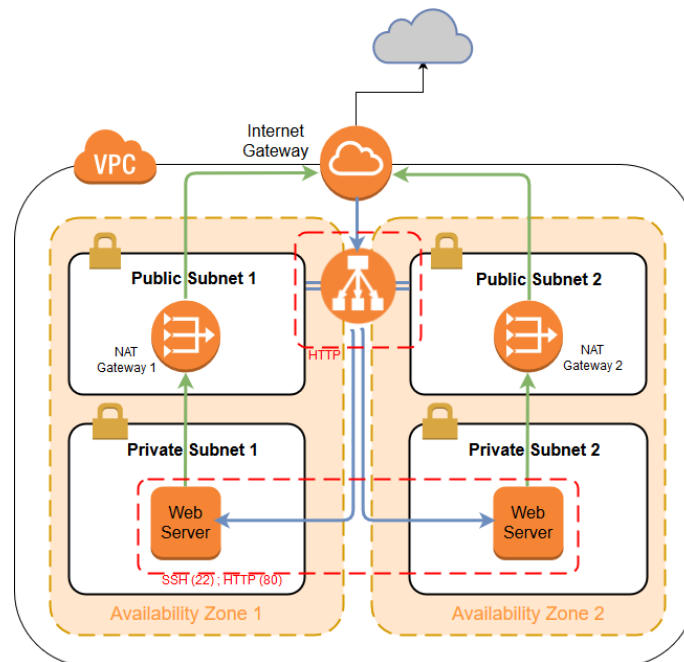


AWS PROJECT: Achieving high availability with multi-AZ architecture and Elastic Load Balancer

Objective: Install a web server and make it highly available by duplicating its image in a second availability zone inside the VPC. Use an elastic load balancer to divide the flow between the two availability zones.



1. Create a VPC with two public and two private subnets

Create two elastic IP addresses that will be used to generate two NAT gateway in your future VPC
Services -> VPC -> Elastic IPs -> Allocate new address

First, create a VPC with one public and one private subnet (using VPC wizard)

Étape 1 : Sélectionner une configuration VPC

VPC avec un seul sous-réseau public	Cette configuration intègre non seulement un sous-réseau public, mais elle ajoute également un sous-réseau privé dont les instances ne peuvent pas être adressées à partir d'Internet. Les instances du sous-réseau privé peuvent établir des connexions sortantes vers Internet via le sous-réseau public par le biais de NAT (Network Address Translation).	<p>Internet, S3, DynamoDB, SNS, SQS, etc.</p> <p>Amazon Virtual Private Cloud</p> <p>Public Subnet, Private Subnet, NAT</p>
VPC avec des sous-réseaux publics et privés	Crée : Un réseau en /16 dans deux sous-réseaux en /24. Des instances du sous-réseau public utilisent des adresses IP Elastic pour accéder à Internet. Les instances de sous-réseau privé accèdent à Internet via NAT (Network Address Translation). (Des tarifs horaires pour les périphériques NAT sont appliqués.)	
VPC avec des sous-réseaux publics et privés, et un accès VPN hardware		
VPC avec un sous-réseau privé seulement et un accès VPN hardware		

[Sélectionner](#)

Name your VPC and restrict the number of available IP addresses for each subnet

Choose the same availability zone for the public and the private subnet

Create a NAT gateway with one of the elastic IP address you created to allow internet outbound connection of the private subnet

Bloc d'adresse CIDR IPv6: ☒ Pas de bloc CIDR IPv6
☐ Bloc CIDR IPv6 fourni par Amazon

Nom du VPC:

Bloc CIDR IPv4 du sous-réseau public:* (251 adresses IP disponibles)

Zone de disponibilité:*

Nom du sous-réseau public:

Bloc CIDR IPv4 du sous-réseau privé:* (251 adresses IP disponibles)

Zone de disponibilité:*

Nom du sous-réseau privé:

Vous pouvez ajouter d'autres sous-réseaux une fois qu'AWS a créé le VPC.

Spécifiez les détails de votre passerelle NAT ([Des tarifs de passerelle NAT sont appliqués](#)).

ID d'allocation d'adresses IP Elastic:*

Points de terminaison de service

Activer les noms d'hôte DNS:* ☒ Oui ☐ Non

Location matérielle:*

Public Subnet

Private Subnet

NAT Gateway

Create two other subnets, public and private, in another availability zone

VPC -> Subnets -> Create subnet

Choose the VPC you created at the previous step

Choose a different availability zone from the one you chose at the creation of the VPC

Repeat the operation once to get two new subnets

Créer le sous-réseau

Utilisez le format CIDR pour spécifier le bloc d'adresse IP de votre sous-réseau (par exemple, 10.0.0.0/24). Notez que les tailles de bloc doivent être comprises entre un masque réseau en /16 et un masque réseau en /28. Notez aussi qu'un sous-réseau peut avoir la même taille que votre VPC. Un bloc d'adresse CIDR IPv6 doit correspondre à un bloc CIDR /64.

Balise Nom:
VPC:
CIDR de VPC:

CIDR	Statut	Motif du statut
10.0.0.0/16	associated	

Zone de disponibilité:
Bloc d'adresse CIDR IPv4:

New AZ!

In order to make the new subnets public or private, you have to specify their route tables:

- the public subnet has to be associated to the internet gateway
- the private subnet has to be associated with a second NAT gateway

Create a NAT gateway

Services -> VPC -> NAT Gateway

Choose the subnet id that corresponds to the public subnet of the second AZ (the NAT gateway stands in the public subnet)

Choose the second elastic IP address you have created

Créer une passerelle NAT

Créez une passerelle NAT et affectez-lui une adresse IP Elastic. [En savoir plus](#).

Sous-réseau*

ID d'allocation d'adresses IP Elastic*

Nouvelle adresse IP Elastic (34.247.247.156) créée avec succès.

* Obligatoire

Create a new route table that targets the NAT gateway you created
VPC -> Route table -> create route table
Give it a name and choose your VPC -> Create
On the route tab, add a new route that target the second NAT Gateway
In subnet association, associate the private subnet of the second AZ.

rtb-0f9b1baf346483b6a | rt-Private1b

Récapitulatif Routes Associations de sous-réseau Propagation de route Balises

Annuler Enregistrer

Afficher: Toutes les règles

Destination	Cible	Statut	Propagée	Supprimer
10.0.0.0/16	local	Actif	Non	
0.0.0.0/24	nat-080c09f623cd081fe		Non	✕

Ajouter une autre route

In Subnets, click on the public subnet of the second AZ and go to the route table tab.
If it points to the NAT, modify the route table and put the one that target the internet gateway (this route table has been automatically created at the creation of the VPC)

Public 1b subnet-0936fc9628... available vpc-091ad9f99e0d82420 | WebS...

subnet-00e12fe352 available vpc-07c52da8e5f929d75 | Rosett

subnet-0936fc9628714c2d7 | Public 1b

Récapitulatif Table de routage ACL réseau Journaux de flux Balises

Modifier

Table de routage: rtb-045fe3427f6866907

Destination	Cible
10.0.0.0/16	local
0.0.0.0/0	nat-05510c50a5fbb025e

Public 1b subnet-0936fc9628... available vpc-091ad9f99e0d82420 | WebS...

subnet-00e12fe352 available vpc-07c52da8e5f929d75 | Rosett

subnet-0936fc9628714c2d7 | Public 1b

Récapitulatif Table de routage ACL réseau Journaux de flux Balises

Annuler Enregistrer

Table de routage actuelle: rtb-045fe3427f6866907

Remplacer par: rtb-018cf429971650925

Destination	Cible
10.0.0.0/16	local
0.0.0.0/0	igw-09c9d3e52d568454a

You now have a VPC with two public and two private subnets in two distinct availability zones

2. Create an Elastic load Balancer to distribute the inbound flow between the two AZ

In services -> EC2 -> Load Balancing -> Load Balancer -> Create Load Balancer

Create a HTTP/HTTPS load balancer

Configure the load balancer:

Give it a name (e.g. ELB1) ; internet-facing ; listener HTTP (port 80)

Étape 1 : Configurer l'équilibreur de charge

Configuration de base

Pour configurer l'équilibreur de charge, entrez un nom, sélectionnez une méthode, spécifiez un ou plusieurs écouteurs et choisissez un réseau. La configuration un écouteur qui reçoit le trafic HTTP sur le port 80.

Nom ⁱ ELB-Private

Méthode ⁱ ☒ accessible sur Internet ☐ interne

Type d'adresse IP ⁱ ipv4

Écouteurs

Un écouteur est un processus qui vérifie les demandes de connexion à l'aide du protocole et du port configurés.

Protocole de l'équilibreur de charge	Port de l'équilibreur de charge
HTTP	80

Ajouter un écouteur

Availability zones:

Choose your VPC

Then select the first AZ and pick the public subnet

Select the second AZ and pick the public subnet

Zones de disponibilité

Spécifiez les zones de disponibilité à activer pour votre équilibreur de charge. L'équilibreur de charge achemine le trafic jusqu'aux cibles de ces zones de disponibilité uniquement. Vous devez spécifier les sous-réseaux d'au moins deux zones de disponibilité afin d'accroître la disponibilité de l'équilibreur de charge.

VPC (i) vpc-091ad9f99e0d82420 (10.0.0.0/16) WebServerELB ▼			
<input type="checkbox"/> Zone de disponibilité	ID de sous-réseau (subnet)	Sous-réseau CIDR IPv4	Nom
<input checked="" type="checkbox"/> eu-west-1a	subnet-0c8a5679379e77270	10.0.1.0/24	Public 1a
<input checked="" type="checkbox"/> eu-west-1b	subnet-0936fc9628714c2d7	10.0.2.0/24	Public 1b

► Balises

Configure security settings: ignore security warning (because we are using HTTP and not HTTPS protocol)

Configure security groups: create a new security group:

Protocol: HTTP (port80), source anywhere

Configure routing:

Étape 4 : Configurer le routage

Votre équilibreur de charge achemine les demandes vers les cibles de ce groupe cible à l'aide

Groupe cible

Groupe cible (i)	Nouveau groupe cible ▼
Nom (i)	<input type="text" value="TG1"/>
Protocole (i)	HTTP ▼
Port (i)	<input type="text" value="80"/>
Type de cible (i)	instance ▼

Vérifications de la santé

Protocole (i)	HTTP ▼
Chemin (i)	<input type="text" value="/"/>

▼ Paramètres avancés de vérification de l'état

Port (i)	<input checked="" type="radio"/> port du trafic	
	<input type="radio"/> substituer	
Seuil de bonne santé (i)	<input type="text" value="5"/>	
Seuil de défectuosité (i)	<input type="text" value="2"/>	
Expiration (i)	<input type="text" value="5"/>	secondes
Intervalle (i)	<input type="text" value="30"/>	secondes
Codes de réussite (i)	<input type="text" value="200"/>	

Register target: For the moment, you do not have any instance so no need to register the target, we will do it later.

3. Create instances in private subnets

EC2 -> Launch an instance

Choose a Linux AMI

Configuration: choose your VPC and the private subnet of the first AZ

Disable public IP address attribution

Nombre d'instances ⓘ 1 [Lancer dans un groupe Auto Scaling ⓘ](#)

Option d'achat ⓘ ☐ Demander des instances Spot

Réseau ⓘ vpc-091ad9f99e0d82420 | WebServerELB [Créer un nouveau VPC](#)

Sous-réseau ⓘ subnet-071cd94d02b59786d | Private 1a | eu-west-1a [Créer un nouveau sous-réseau](#)

251 adresses IP disponibles

Attribuer automatiquement l'adresse IP publique ⓘ Utiliser le paramètre de sous-réseau (désactiver) [Créer un nouveau sous-réseau](#)

Groupe de placement ⓘ ☐ Ajoutez une instance au groupe de placement.

We want to create a web server, so we are going to use user data to install it at launch and create an html page. To test the function of the load balancer we will create two different html pages in the two different AZ, one displaying “HELLO”, the other one “GOOD BYE”.

User data to install the web server:

```
#!/bin/bash
sudo yum update -y
sudo yum -y install httpd
sudo service httpd start
sudo bash -c 'echo HELLO > /var/www/html/index.html'
```

Next, configure security group. Create a new security group
SSH (if you want to connect to your instance)
HTTP

Source: Anywhere or your IP

Attribuer un groupe de sécurité: ☒ Créer un nouveau groupe de sécurité ☐ Sélectionner un groupe de sécurité existant

Nom du groupe de sécurité: Server1a-SG

Description: Server1a-SG created 2018-06-09T16:51:38.022+02:00

Type ⓘ	Protocole ⓘ	Plage de ports ⓘ	Source ⓘ	Description ⓘ
SSH	TCP	22	Personnalis 0.0.0.0/0	Par exemple, SSH pour le bureau de l
HTTP	TCP	80	Personnalis 0.0.0.0/0	Par exemple, SSH pour le bureau de l

[Ajouter une règle](#)

Review and create instance.

Create a second instance in the private subnet of the second AZ. Proceed exactly the same way as previously but change the location of the instance (private subnet 2) and modify the user data to display “GOOD BYE” instead of “HELLO” on the html page.

You now have two web servers with no public IP in two distinct AZ.

Filtrer par balises et attributs ou rechercher par mot clé						
Name	ID d'instance	Type d'instance	Zone de disponib	État de l'instance	Contrôles des statuts	
Server 1a	i-041bf7cf0856f6d02	t2.micro	eu-west-1a	running	2/2 contrôles réussis	
Server 1b	i-0a1ef7c5d93de9b39	t2.micro	eu-west-1b	running	2/2 contrôles réussis	

Instance: i-041bf7cf0856f6d02 (Server 1a) IP privée: 10.0.3.23

Description	Contrôles des statuts	Supervision	Balises
ID d'instance	i-041bf7cf0856f6d02		
État de l'instance	running		
Type d'instance	t2.micro		
Adresses IP Elastic			
Zone de disponibilité	eu-west-1a		
Groupe de sécurité	Server1a-SG afficher les règles		
Événements planifiés	Aucun événement planifié		
ID d'AMI	ami-zn-ami-hvm-2018.03.0.20180508-x86_64-gp2 (ami-ca0135b3)		
DNS public (IPv4)	-		
IP publique IPv4	-		
Adresses IP IPv6	-		
Private DNS	ip-10-0-3-23.eu-west-1.compute.internal		
IP privées	10.0.3.23		
IP privées secondaires			
ID de VPC	vpc-091ad9f99e0d82420		
ID de sous-réseau	subnet-071cd94d02b59786d		

2 different AZ

no public IP

4. Connect load balancer to instances

EC2 -> Load balancing -> target group

A target group has been created at the creation of the load balancer. For the moment, no instance is registered.

Register instances: choose the two private web servers, add to the group, save

Cibles enregistrées

Pour annuler l'enregistrement des instances, sélectionnez une ou plusieurs instances enregistrées, puis cliquez sur Supprimer.

Supprimer

Instance	Nom	Port	État	Groupes de sécurité	Zone
i-41b7c7c5656fd02	Server 1a	80	● running	Server1e-SG	eu-west-1a
i-4a1ef7cbe93d9b39	Server 1b	80	● running	Server1b-SG	eu-west-1b

Instances

Pour enregistrer des instances supplémentaires, sélectionnez une ou plusieurs instances en cours d'exécution, spécifiez un port, puis cliquez sur Ajouter. Le port par défaut est le port spécifié pour le groupe cible. Si l'instance a déjà été enregistrée sur le port spécifié, vous devez indiquer un port différent.

Ajouter au membre sur le port 80

Rechercher des instances

Instance	Nom	État	Groupes de	Zone	ID de sous-réseau (subnet)	CIDR du sous-réseau (subnet)
i-41b7c7c5656fd02	Server 1a	● running	Server1a-SG	eu-west-1a	subnet-07cc94802b09786d4	10.0.3.0/24
i-4a1ef7cbe93d9b39	Server 1b	● running	Server1b-SG	eu-west-1b	subnet-0b32d97f4bd2343d9	10.0.4.0/24

Wait few minutes and you should see your two registered instances with a “healthy” status

Cibles enregistrées

ID d'instance	Nom	Port	Zone de disponibilité	Statut
i-0f42478fe5e9a7fea	Server 1b	80	eu-west-1b	healthy ⓘ
i-090acd5e77b07a02d	Server 1a	80	eu-west-1a	healthy ⓘ

Come back on the elastic load balancer tab, copy the DNS name of the load balancer you have created for your two instances.

Nom	Nom du DNS	État	ID de VPC	Zones de disponibilité
ELB-Private	ELB-Private-1236706673.eu-west-1.elb.amazonaws....	provisioning	vpc-091ad9f99e0d82420	eu-west-1b, eu-west-1a

Configuration de base

Nom: ELB-Private	Heure de création: 9 juin 2018 16:46:34 UTC+2
ARN: arn:aws:elasticloadbalancing:eu-west-1:749933439688:loadbalancer/app/ELB-Private/6c3825167bf84b41	Zone hébergée: Z32O12XQLNTSW2
Nom du DNS: ELB-Private-1236706673.eu-west-1.elb.amazonaws.com (Enregistrement A)	État: provisioning
Méthode: internet-facing	VPC: vpc-091ad9f99e0d82420
Type: application	Type d'adresse IP: ipv4
Zones de disponibilité: subnet-0936fc9628714c2d7 - eu-west-1b, subnet-0c8a5679379e77270 - eu-west-1a	ACL Web AWS WAF: Une erreur s'est produite quand une demande a été envoyée à AWS WAF.

Modifier les zones de disponibilité

DNS name

Paste it in a new tab of your internet browser.

You should see a web page displaying “HELLO” or “GOOD BYE”. If you refresh the page several times, you should see an alternation in the page displayed, sometimes “HELLO”, sometimes “GOOD BYE”.