

Formateur : Mohamed AIJOU

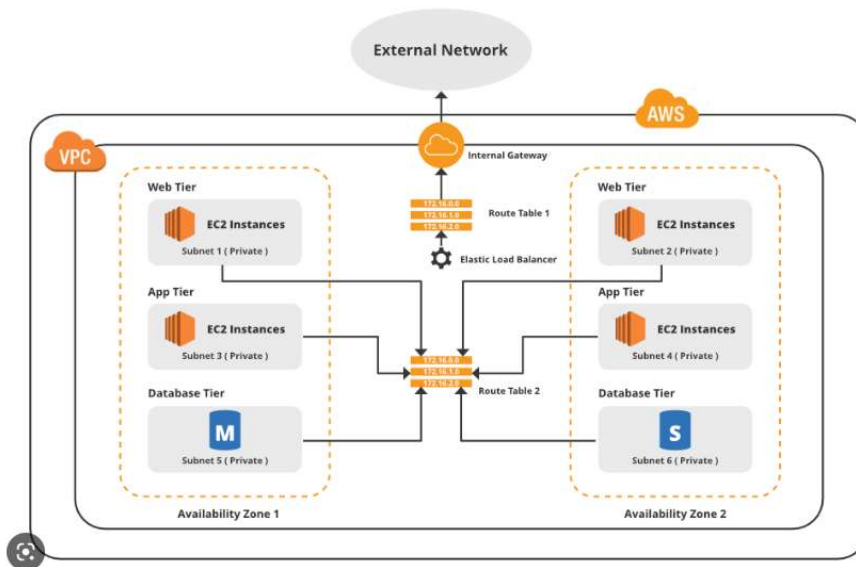
5 – SERVICE 2 : Virtual Private Cloud



https://docs.aws.amazon.com/fr_fr/vpc/latest/userguide/what-is-amazon-vpc.html

Amazon Virtual Private Cloud (Amazon VPC) vous permet de lancer des ressources AWS dans un réseau virtuel défini par vos soins. Ce réseau virtuel ressemble beaucoup à un réseau traditionnel que vous pourriez exécuter dans votre propre centre de données, et présente l'avantage d'utiliser l'infrastructure évolutive d'AWS.

- Un réseau virtuel privé dans le Cloud AWS.
- Accès complet à la configuration de votre réseau.
- Offre de nombreuses couches de contrôle de sécurité.
- D'autres services AWS sont déployés à l'intérieur du VPC.



5 – 2 – Les fonctionnalités





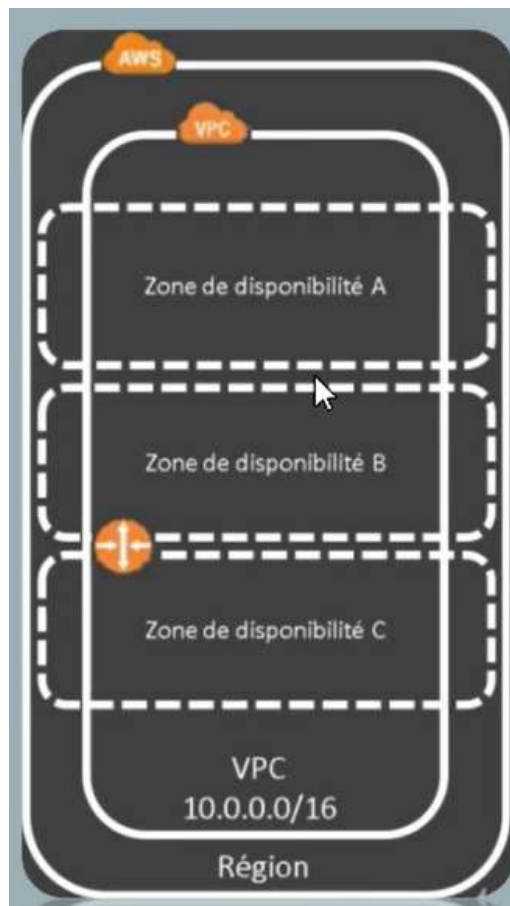
Amazon
S3



Amazon
DynamoDB

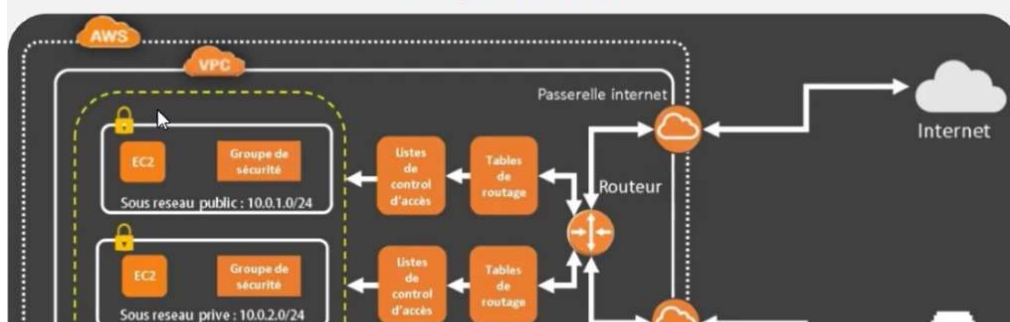


Amazon
ElastiCache



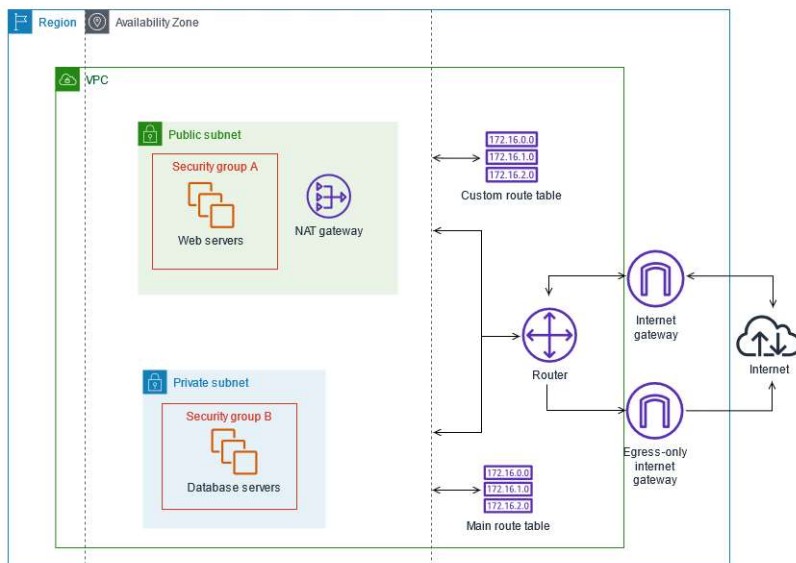
- **VPC s'appuie sur la haute disponibilité :**
 - *Régions.*
 - *Zones de disponibilité.*
- **Sous réseau (subnet).**
- **Passerelle internet (IGW) ou (NAT).**
- **Liste de contrôles d'accès réseau (NACL).**
- **Tables de routages (routes tables).**
- **Les points de terminaisons de services AWS.**

Exemple VPC AWS





Scénario de VPC avec sous-réseau public et sous réseau privé :
https://docs.aws.amazon.com/fr_fr/vpc/latest/userguide/VPC_Scenario2.html

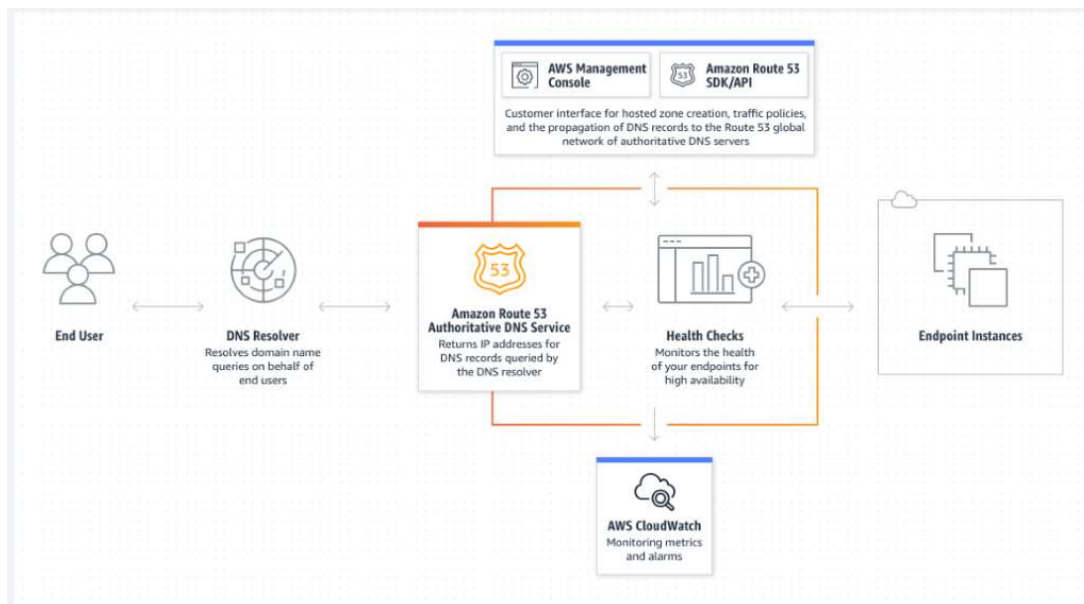


Le système des routes sur AWS : **route 53**

<https://aws.amazon.com/fr/route53/>

Fonctionnement

Amazon Route 53 est un service web de système de noms de domaine (DNS) hautement disponible et évolutif. Route 53 connecte les requêtes des utilisateurs aux applications Internet exécutées sur AWS ou sur site.



Créer un VPC :

Paramètres VPC

Ressources à créer **Infos**

Créez uniquement la ressource VPC ou le VPC et d'autres ressources réseaux.

☒ VPC uniquement

☐ VPC et plus encore

Identification de nom - *facultatif*

Crée une identification avec une clé du « Nom » et une valeur que vous spécifiez.

Bloc d'adresses CIDR IPv4 [Infos](#)

- ☒ Entrée manuelle CIDR IPv4
- ☐ Bloc d'adresse CIDR IPv4 alloué à IPAM

CIDR IPv4

Bloc CIDR IPv6 [Infos](#)

- ☒ Aucun bloc d'adresses CIDR IPv6
- ☐ Bloc d'adresse CIDR IPv6 alloué à IPAM
- ☐ Bloc d'adresses CIDR IPv6 fourni par Amazon
- ☐ CIDR IPv6 dont je suis propriétaire

Location [Infos](#)

Balises

Une balise est une étiquette que vous attribuez à une ressource AWS. Chaque balise est constituée d'une clé et d'une valeur facultative. Vous pouvez utiliser des balises pour rechercher et filtrer vos ressources ou réaliser le suivi vos coûts AWS.

Clé

Valeur - *facultatif*

Vous pouvez ajouter 49 d'autres balises.

vpc-0d4e0d8e7dd75ebcf / vpc_test_benoit_irlande

Détails [Infos](#)

ID de VPC

 vpc-0d4e0d8e7dd75ebcf

Location

Default

VPC par défaut

Non

Métriques d'utilisation d'adresses réseau

Désactivé

État

 Available

Jeu d'options DHCP

dopt-0e15b2b410a29b9a9

CIDR IPv4

10.0.0.0/16

Groupes de règles du pare-feu DNS de Route 53

Resolver

 **Echec du chargement des groupes de règles**

Noms d'hôte DNS

Désactivé

Table de routage principale

rtb-0e95266e6e1cca4e1

Groupe IPv6

-

ID du propriétaire

 639962416620

Créer sous-réseau :

Pour cet exemple, nous partons sur la création d'un subnet public

▼ Cloud privé virtuel

Vos VPC

[Sous-réseaux](#)

Créer un sous-réseau [Infos](#)

VPC

ID de VPC

Créez des sous-réseaux dans ce VPC.

CIDR de VPC associés

CIDR IPv4

Paramètres du sous-réseau

Précisez les blocs d'adresse CIDR et la zone de disponibilité pour le sous-réseau.

Sous-réseau 1 sur 1

Nom du sous-réseau (subnet)

Créez une balise avec une clé « Name » et une valeur à spécifier.

Le nom peut comporter jusqu'à 256 caractères.

Zone de disponibilité [Infos](#)

Choisissez la zone dans laquelle votre sous-réseau résidera ou laissez Amazon en choisir une pour vous.

Bloc d'adresses CIDR IPv4 [Infos](#)

▼ Balises - *facultatif*

Clé

Valeur - *facultatif*

Vous pouvez ajouter 49 d'autres balises.

✓ Vous avez créé 1 sous-réseau avec succès : subnet-09dc485b6cf92d39f

Sous-réseaux (1) [Infos](#)

<input type="checkbox"/>	Name	ID de sous-réseau	État	VPC	CIDR IPv4
<input type="checkbox"/>	subnet_benoit_public	subnet-09dc485b6cf92d39f	✓ Available	vpc-0d4e0d8e7dd75ebcf vpc...	10.0.1.0/24

Création du subnet privé :

Paramètres du sous-réseau

Précisez les blocs d'adresse CIDR et la zone de disponibilité pour le sous-réseau.

Sous-réseau 1 sur 1

Nom du sous-réseau (subnet)

Créez une balise avec une clé « Name » et une valeur à spécifier.

Le nom peut comporter jusqu'à 256 caractères.

Zone de disponibilité [Infos](#)

Choisissez la zone dans laquelle votre sous-réseau résidera ou laissez Amazon en choisir une pour vous.

Bloc d'adresses CIDR IPv4 [Infos](#)

▼ Balises - *facultatif*

Clé

Valeur - *facultatif*

Vous pouvez ajouter 49 d'autres balises.

Ajouter un nouveau sous-réseau

Rajout de l'adresse IP publique sur le sous-réseau public :

Name	ID de sous-réseau	État	VPC	CIDR IPv4
-	subnet-0e4b35e9989b5f8e	🟢 Disponible	vpc-05ca2332a6290131	172.31.0.0/20
-	subnet-012a8888a8a8a8a8	🟢 Disponible	vpc-05ca2332a6290131	172.31.16.0/20
-	subnet-01945112b054819	🟢 Disponible	vpc-05ca2332a6290131	172.31.32.0/20
subnet_benoit_priv...	subnet-0a4e0d8e7dd75ebcf	🟢 Disponible	vpc-0a4e0d8e7dd75ebcf vpc...	10.0.2.0/24
subnet_benoit_public	subnet-09dc485b6cf92d39f	🟢 Disponible	vpc-0a4e0d8e7dd75ebcf vpc...	10.0.1.0/24
subnet_fais_privat...	subnet-0505d6a109a81114	🟢 Disponible	vpc-0a4e0d8e7dd75ebcf vpc...	10.0.2.0/24
subnet_fais_priv...	subnet-0505d6a109a81114	🟢 Disponible	vpc-0a4e0d8e7dd75ebcf vpc...	10.0.1.0/24

VPC > Sous-réseaux > subnet-09dc485b6cf92d39f > Modifier les paramètres de sous-réseau

Modifier les paramètres de sous-réseau [Infos](#)

Sous-réseau

ID de sous-réseau

🔗 subnet-09dc485b6cf92d39f

Nom

🔗 subnet_benoit_public

Paramètres d'attribution automatique d'une adresse IP [Infos](#)

Activez les paramètres d'attribution automatique de l'adresse IP pour demander automatiquement une adresse IPv4 ou IPv6 publique pour une nouvelle interface réseau dans ce sous-réseau.

☒ Activer l'attribution automatique d'une adresse IPv4 publique [Infos](#)

☐ Activer l'attribution automatique d'une adresse IPv4 détenue par le client [Infos](#)
Option désactivée car aucun groupe appartenant au client n'a été trouvé.

Vérification du VPC :

vpc-0d4e0d8e7dd75ebcf / vpc_test_benoit_irlande

Détails **Resource map** CIDR Journaux de flux Balises

Resource map [Infos](#)

VPC [Afficher les détails](#)
Votre réseau virtuel AWS

vpc_test_benoit_irlande

Sous-réseaux (2)
Sous-réseaux au sein de ce VPC

eu-west-1a

- subnet_benoit_public
- subnet_benoit_private

Tables de routage (1)
Acheminer le trafic réseau vers les ressources

rtb-0e95266e6e1cca4e1

Connexions réseau (0)
Connexions à d'autres réseaux

Introducing the VPC resource map
The new resource map helps you visualize the resources in your VPC. It shows your VPC, subnets, route tables, internet

Il nous manque une table de routage + gateway

Création gateway :

VPC > Passerelles Internet > Créer une passerelle Internet

Créer une passerelle Internet [Infos](#)

Une passerelle Internet est un routeur virtuel qui connecte un VPC à Internet. Pour créer une nouvelle passerelle Internet, spécifiez le nom de la passerelle ci-dessous.

Paramètres de passerelle Internet

Identification de nom

Crée une identification avec une clé du « Nom » et une valeur que vous spécifiez.

internet_gateway_benoit_irlande

Balises - facultatif

Une balise est une étiquette que vous attribuez à une ressource AWS. Chaque balise est constituée d'une clé et d'une valeur facultative. Vous pouvez utiliser des balises pour rechercher vos ressources ou réaliser le suivi vos coûts AWS.

Clé

🔍 Name

Valeur - facultatif

🔍 internet_gateway_benoit_irland

Supprimer

Ajouter une nouvelle balise

Vous pouvez ajouter 49 d'autres balises.

[Annuler](#)[Créer une passerelle Internet](#)

Suite à la création de la gateway : on peut l'attacher à notre VPC

[Attacher à un VPC](#)

VPC > Passerelles Internet > Attacher au VPC (igw-0a161ff415b842695)

Attacher au VPC (igw-0a161ff415b842695) [Infos](#)

VPC

Attachez une passerelle Internet à un VPC pour permettre au VPC de communiquer avec Internet. Spécifiez le VPC à attacher ci-dessous.

VPC disponibles

Attachez la passerelle Internet à ce VPC.

vpc-0d4e0d8e7dd75ebcf - vpc_test_benoit_irlande

► [Commande AWS Command Line Interface](#)

[Annuler](#)[Attacher une passerelle Internet](#)

(on peut également faire cette manipulation via une ligne de commande), par exemple :

```
aws ec2 attach-internet-gateway --vpc-id "vpc-0d4e0d8e7dd75ebcf" --internet-gateway-id "igw-0a161ff415b842695" --region eu-west-1
```

▼ Commande AWS Command Line Interface

Vous pouvez exécuter les mêmes actions sur cette page à l'aide des outils AWS Command Line Interface (CLI). [En savoir plus](#) [↗](#).

Plateforme

Choisissez la plateforme à partir de laquelle vous voulez exécuter cette commande. Les paramètres de commande doivent être spécifiés différemment selon la plateforme. En savoir plus sur la [spécification des valeurs de paramètres](#) [↗](#).

Linux/Unix/OS X

Commande CLI

Si vous utilisez les outils AWS CLI, vous pouvez copier et coller cette commande (qui inclut les paramètres que vous avez spécifiés dans cette page) dans l'invite ou le terminal de la ligne de commande. En savoir plus sur les [commandes AWS CLI](#) [↗](#) disponibles.

```
aws ec2 attach-internet-gateway --vpc-id "vpc-0d4e0d8e7dd75ebcf" --internet-gateway-id "igw-0a161ff415b842695" --region eu-west-1
```

[Copier](#)

VPC > Passerelles Internet > igw-0a161ff415b842695

igw-0a161ff415b842695 / internet_gateway_benoit_irlande

[Actions](#)

Détails [Infos](#)

ID de passerelle Internet
igw-0a161ff415b842695

État
Attached

ID de VPC
vpc-0d4e0d8e7dd75ebcf | vpc_test_benoit_irlande

Propriétaire
639962416620

Resource map [Infos](#)

VPC [Afficher les détails](#)

Votre réseau virtuel AWS

vpc_test_benoit_irlande

Sous-réseaux (2)

Sous-réseaux au sein de ce VPC

eu-west-1a

subnet_benoit_public

subnet_benoit_private

Tables de routage (1)

Acheminer le trafic réseau vers les ressources

rtb-0e95266e6e1cca4e1

Connexions réseau (1)

Connexions à d'autres réseaux

internet_gateway_benoit_irlande

Introducing the VPC resource

Créer table de routage pour le réseau privée :

Créer une table de routage [Infos](#)

Une table de routage spécifie comment les paquets sont transférés entre les sous-réseaux au sein de votre VPC, sur Internet et votre connexion VPN.

Paramètres de la table de routage

Nom - *facultatif*

Créez une balise avec une clé « Name » et une valeur à spécifier.

VPC

VPC à utiliser pour cette table de routage.

Balises

Une balise est une étiquette que vous attribuez à une ressource AWS. Chaque balise est constituée d'une clé et d'une valeur facultative. Vous pouvez utiliser des balises pour rechercher et filtrer vos ressources ou réaliser le suivi vos coûts AWS.

Clé

Valeur - *facultatif*

Supprimer

Ajouter une nouvelle balise

Vous pouvez ajouter 49 d'autres balises.

Suite à la création : il faut associer notre table de routage à notre subnet privée et modifier la route de notre table de routage publique

Modifiez les sous-réseaux associés à cette table de routage.

Sous-réseaux disponibles (1/2)

	Nom	ID de sous-réseau	CIDR IPv4
<input type="checkbox"/>	subnet_benoit_public	subnet-09dc485b6cf92d39f	10.0.1.0/24
<input checked="" type="checkbox"/>	subnet_benoit_private	subnet-0ac0d8e7ab0145300	10.0.2.0/24

Sous-réseaux sélectionnés

Modifier des routes

Destination

Cible

Ajouter une route

Routes mises à jour pour rtb-0e95266e6e1cca4e1 avec succès

Détails

VPC > Tables de routage > rtb-0e95266e6e1cca4e1

rtb-0e95266e6e1cca4e1

Actions

Vous pouvez désormais vérifier la connectivité réseau avec Reachability Analyzer.

Exécuter Reachability Analyzer

Détails

Infos

ID de la table de routage

rtb-0e95266e6e1cca4e1

VPC

vpc-0d4e0d8e7dd75ebcf | vpc_test_benoit_irlande

Principal

Oui

ID du propriétaire

639962416620

Associations de sous-réseau explicites

subnet-09dc485b6cf92d39f / subnet_benoit_public

Associations de périphérie

-

Routes

Associations de sous-réseau

Associations de périphérie

Propagation de routage

Balises

Routes (2)

Modifier des routes

Filtrer les routes				Les deux	
Destination	Cible	Statut	Propagée		
0.0.0.0/0	lgw-0a161ff415b842695	Actif	Non		
10.0.0.0/16	local	Actif	Non		

Vérification du VPC :



Après la création des instances : test de ping :

```
[ec2-user@ip-10-0-1-40 ~]$ ping 10.0.2.163
PING 10.0.2.163 (10.0.2.163) 56(84) bytes of data.
^C
--- 10.0.2.163 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1006ms

[ec2-user@ip-10-0-1-40 ~]$ |
```

Pour autoriser les pings entre les sous-réseaux :

Règles entrantes (2)									Gérer les balises
Filtrer les règles des groupes de sécurité									
<input type="checkbox"/>	Name	ID de règle de grou...	Version IP	Type	Protocole	Plage de ports	Source		
<input type="checkbox"/>	-	sgr-00d295130d24ffcd	IPv4	Tous les ICMP - IPv4	ICMP	Tous	0.0.0.0/0		

Test de ping suis à l'ouverture de l'ICMP :

```
[ec2-user@ip-10-0-1-40 ~]$ ping 10.0.2.163
PING 10.0.2.163 (10.0.2.163) 56(84) bytes of data.
64 bytes from 10.0.2.163: icmp_seq=1 ttl=255 time=0.455 ms
64 bytes from 10.0.2.163: icmp_seq=2 ttl=255 time=0.462 ms
64 bytes from 10.0.2.163: icmp_seq=3 ttl=255 time=0.462 ms
64 bytes from 10.0.2.163: icmp_seq=4 ttl=255 time=0.572 ms
```

