www.eazytraining.fr

Services réseau d’AWS

Par Lahda Biassou Alphonsine

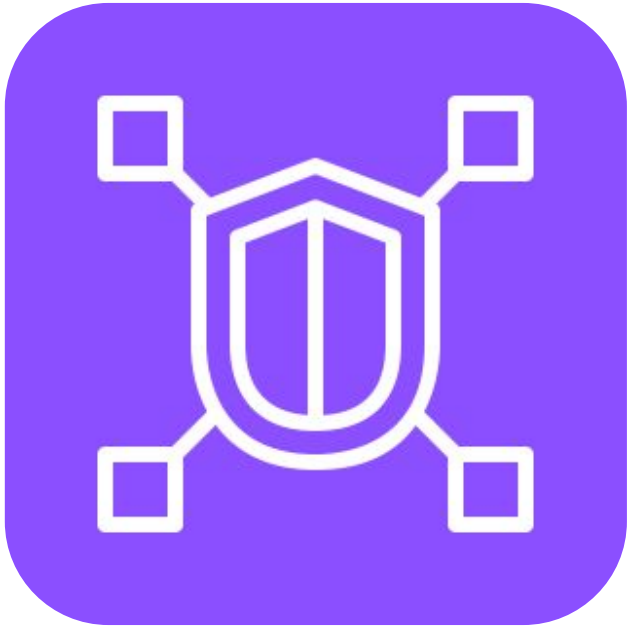
Lahda Biassou Alphonsine

Ingénieure cloud et formatrice

Plan

- **VPC Lattice**
- **Direct connect**
- **VPN**
- **Amazon route 53**
- **CloudMap**

Amazon VPC Lattice

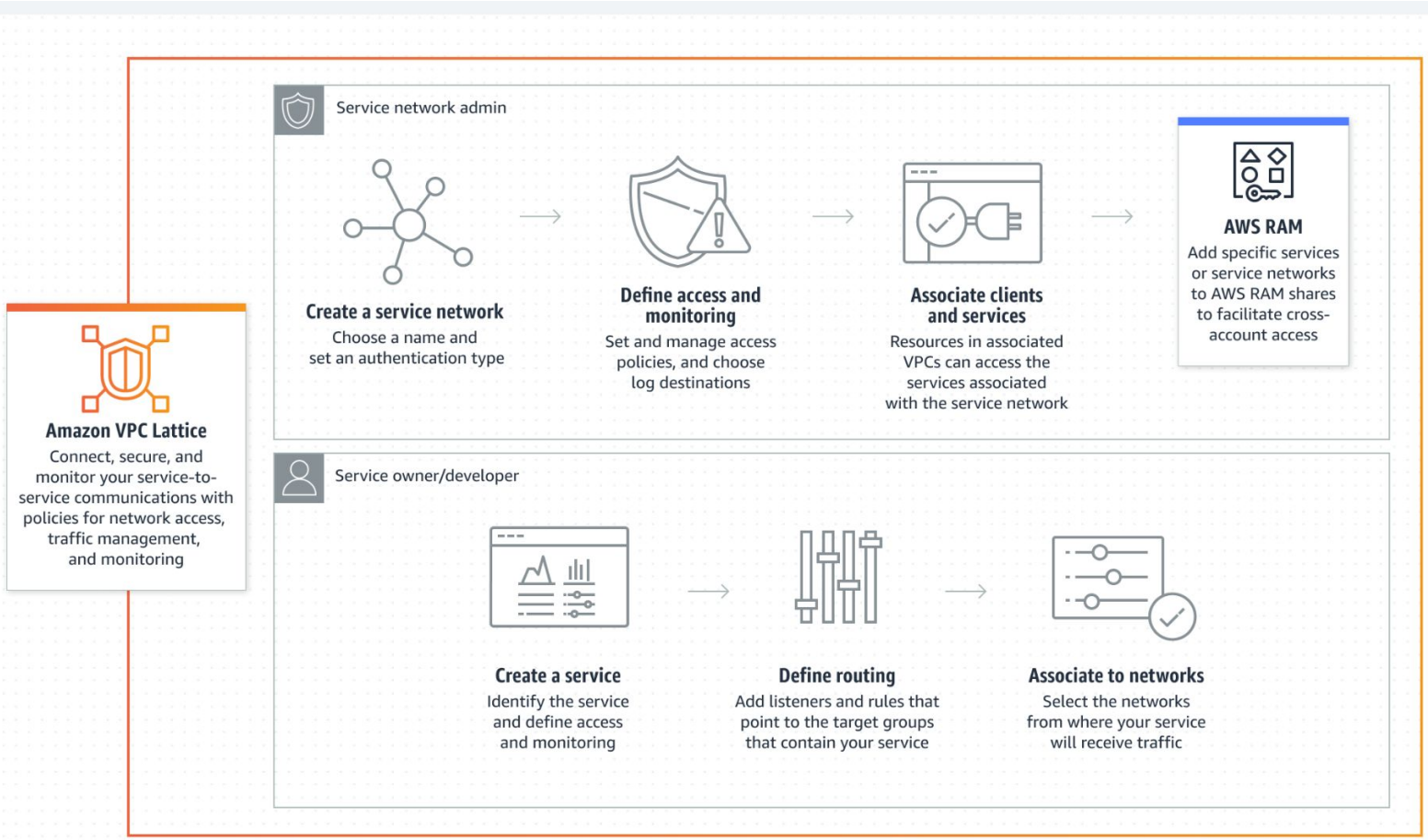


Amazon VPC Lattice gère automatiquement la connectivité réseau et le routage de la couche application entre les services à travers différents VPC et comptes AWS. Vous pouvez exploiter votre réseau sans avoir à gérer la connectivité réseau sous-jacente, les équilibreurs de charge frontaux ou les proxies latéraux à côté de chaque charge de travail. Amazon VPC Lattice s'intègre à AWS Identity et Access Management (IAM) pour vous fournir les mêmes capacités d'authentification et d'autorisation familières lorsque vous utilisez d'autres services AWS.

Amazon VPC Lattice -avantages

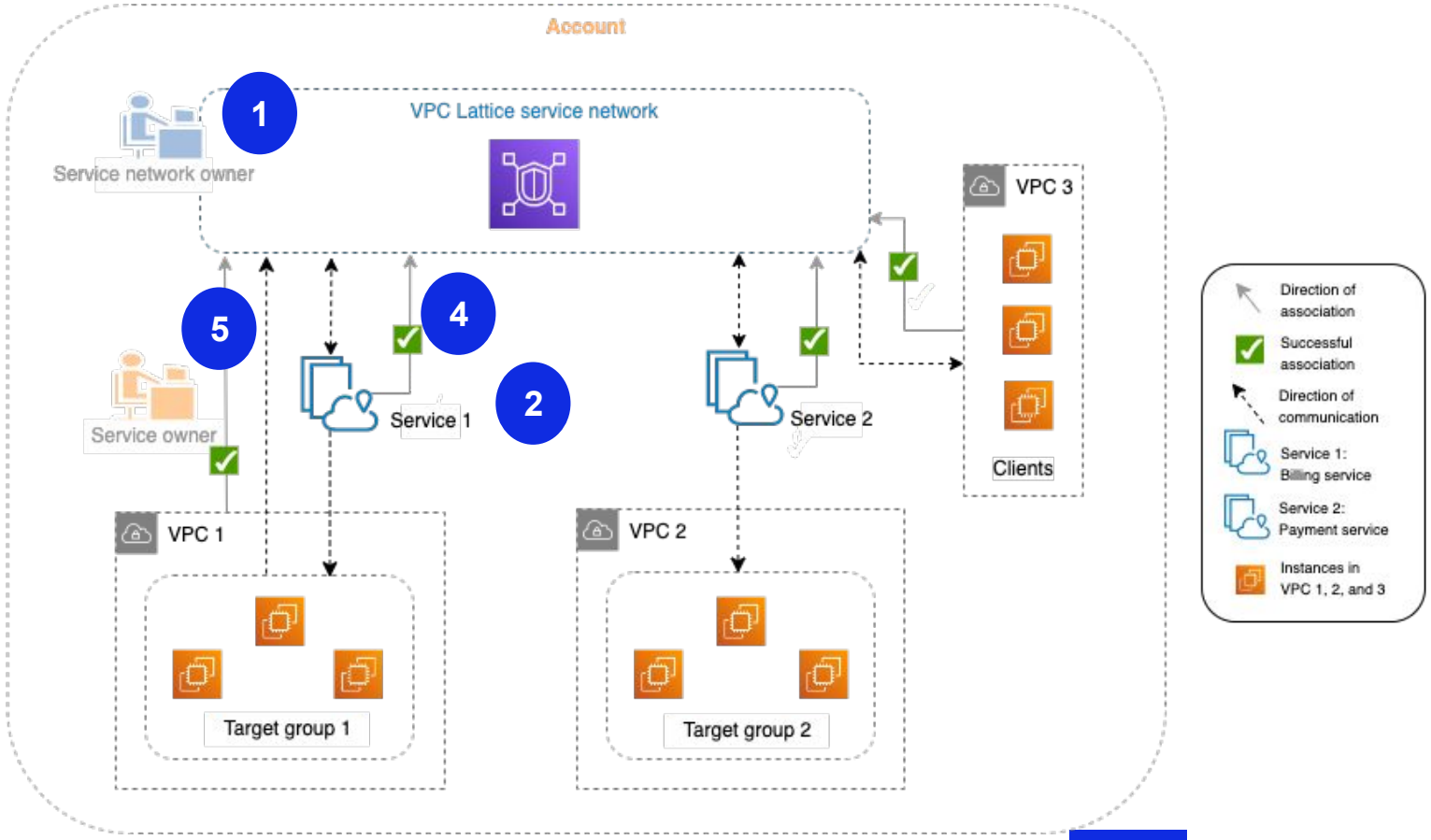
- **Connectivité simplifiée**
- **Securite renforcee**
- **Mise a l'échelle automatique**
- **Déploiement flexible**

VPC Lattice -fonctionnement



VPC Lattice -Exemple

Le schéma de flux suivant utilise un exemple de scénario pour expliquer le flux d'informations et le sens de la communication entre les composants au sein de **VPC Lattice**. Deux services sont associés à un réseau de services. Les deux services et les trois VPC ont été créés dans le même compte que le réseau de services. Les deux services sont configurés pour autoriser le trafic provenant du réseau de service.



VPC Lattice -cas d’usage

- Simplification de la connectivité service a service à l'échelle
- Renforcer la sécurité au niveau des applications
- Mettre en place une gestion avancée du trafic
- Gagner en visibilité sur les interactions entre les services

Plan

- VPC Lattice
- Direct connect
- VPN
- Amazon route 53
- CloudMap

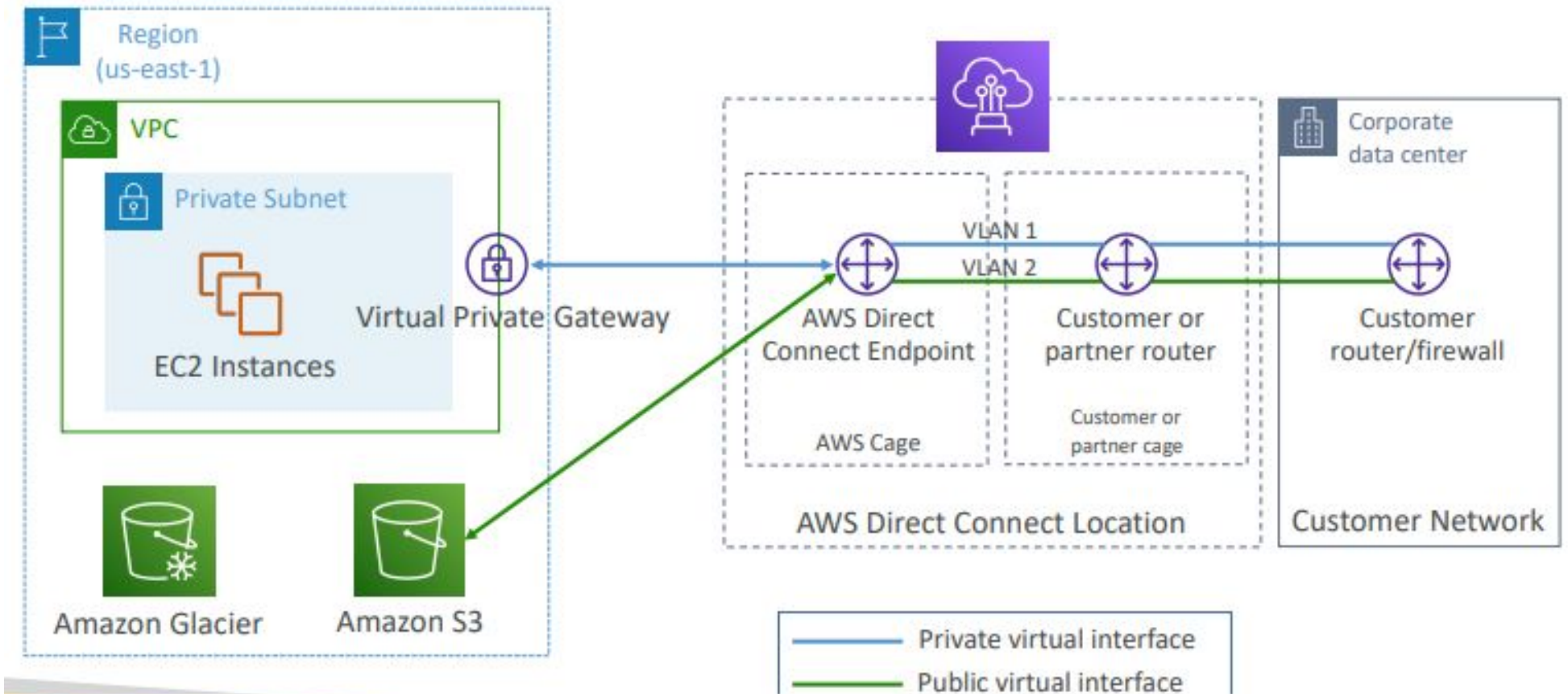
AWS Direct Connect

- Fournit une connexion privée dédiée depuis un réseau distant vers votre VPC
- Une connexion dédiée doit être configurée entre votre DC et AWS. Emplacements de Direct Connect
- Plus coûteux que l'utilisation d'une solution VPN
- Accès privé aux services AWS via VIF
- Permet de contourner le FAI, de réduire le coût du réseau, d'augmenter la bande passante et la stabilité.
- Pas de redondance par défaut (il faut configurer un DX ou un VPN de basculement).

Direct connect -virtual interface

- Public VIF - se connecter à des points d'extrémité publics AWS (buckets S3, service EC2, tout ce qui est AWS...)
- Private VIF - connexion aux ressources de votre VPC (instances EC2, ALB, ...)
- Transit Virtual Interface - se connecter aux ressources d'un VPC en utilisant un Transit Gateway
- Les points de terminaison VPC ne sont pas accessibles via Private VIF (vous n'en avez pas besoin).

Direct connect - diagramme



Direct connect - type de connexion

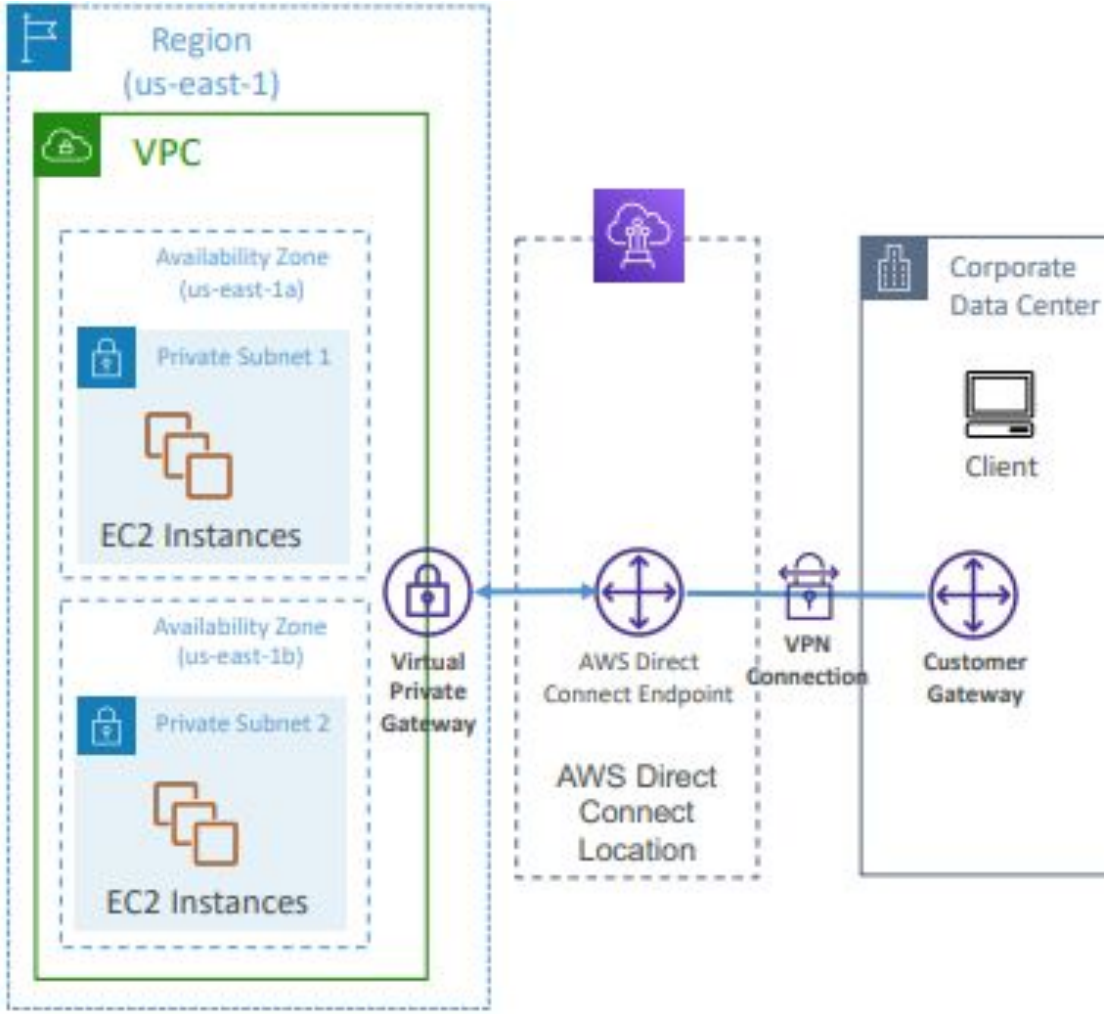
- **Connexions dédiées : Capacité de 1 Gbps, 10 Gbps, 100 Gbps**
  - Port Ethernet physique dédié à un client
  - La demande est d'abord adressée à AWS, puis complétée par les partenaires AWS Direct Connect.

- **Connexions hébergées : 50Mbps, 500 Mbps, à 10 Gbps**
  - Les demandes de connexion sont effectuées par les partenaires AWS Direct Connect.
  - La capacité peut être **ajoutée ou supprimée à la demande**
  - 1, 2, 5, 10 Gbps disponibles chez certains partenaires AWS Direct Connect.

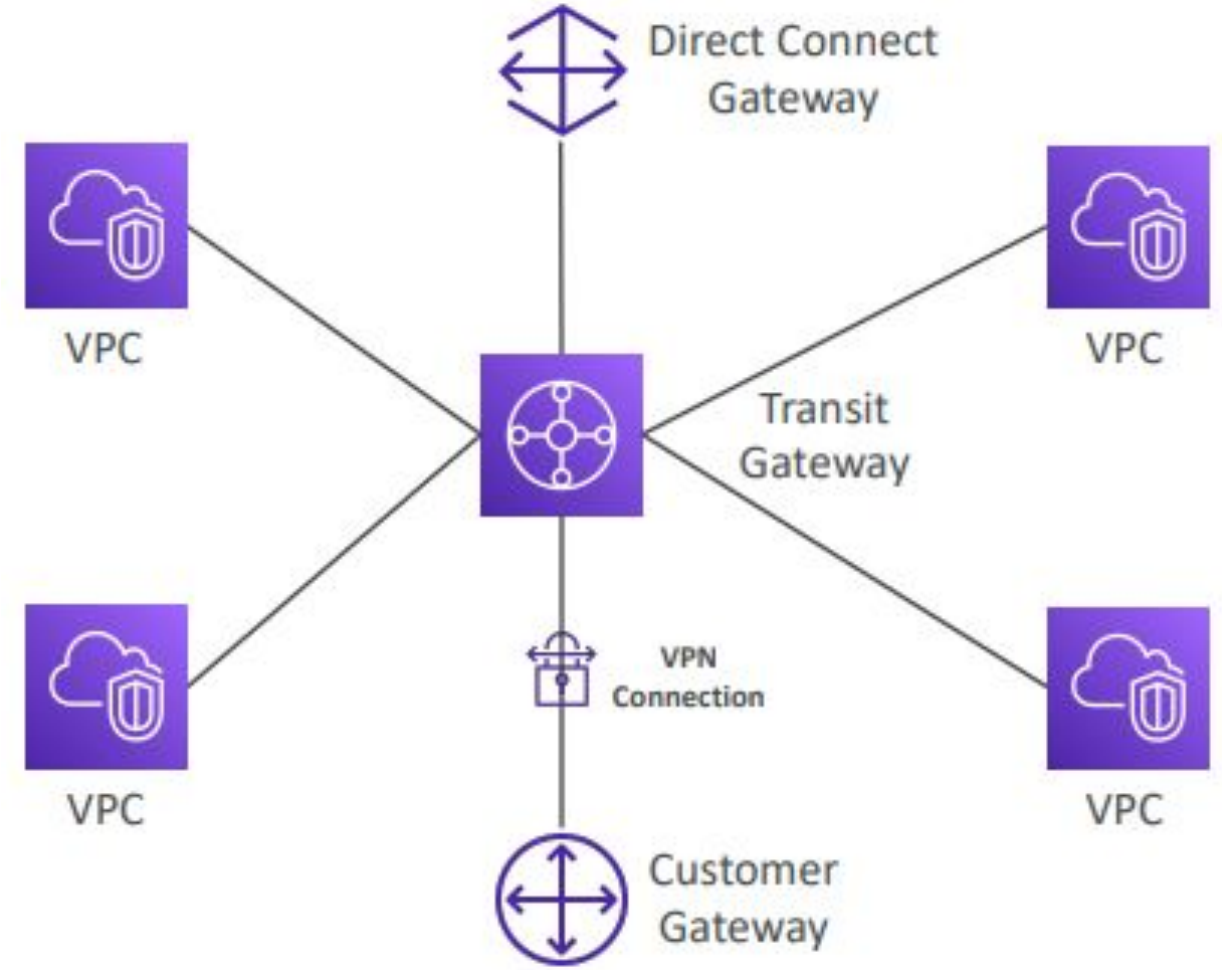
- Les délais d'établissement d'une nouvelle connexion sont souvent supérieurs à un mois.

Direct connect - cryptage

- Les données en transit ne sont pas cryptées mais sont privées
- AWS Direct Connect + VPN fournit une connexion privée cryptée par Ipsec
- VPN sur une connexion Direct Connect Utilise le VIF public
- Bon pour un niveau de sécurité supplémentaire, mais légèrement plus complexe à mettre en place

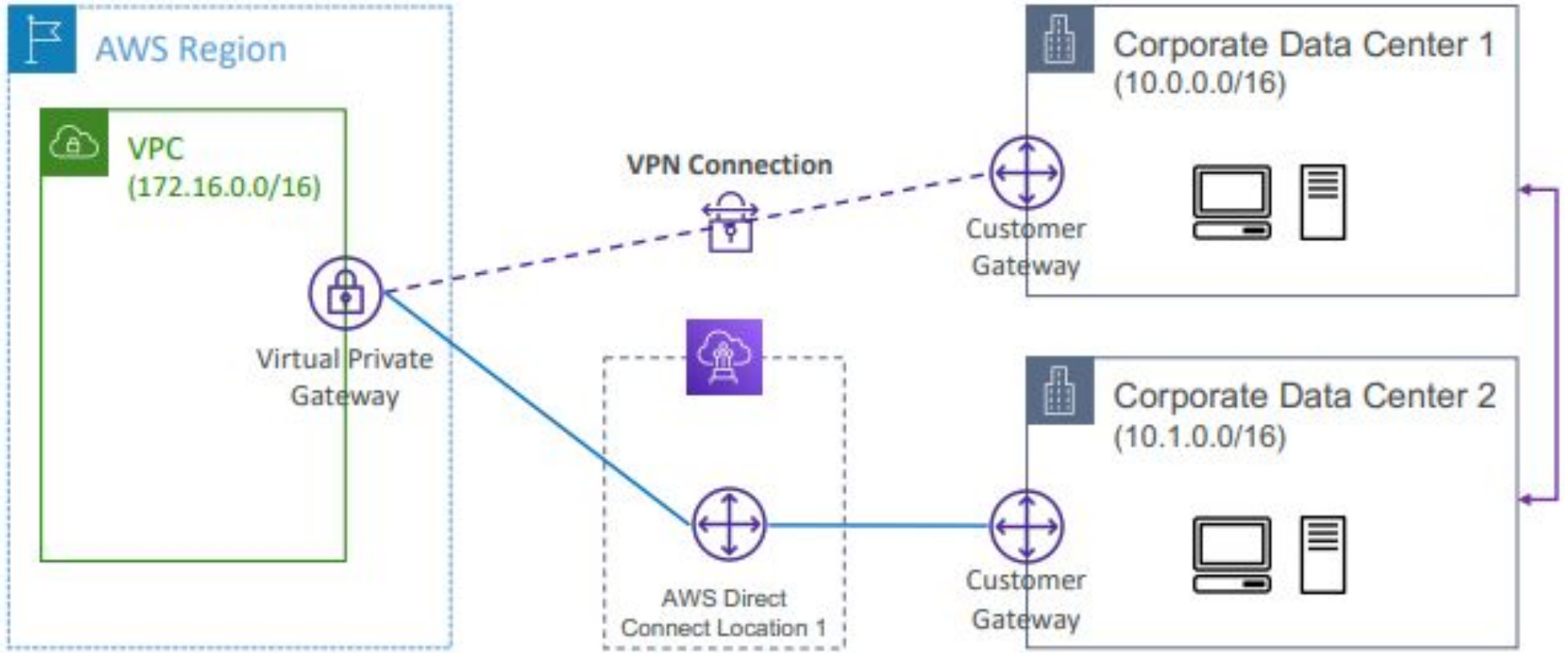


Direct connect + Transit Gateway



Direct connect - haute disponibilité

Backup VPN Connection

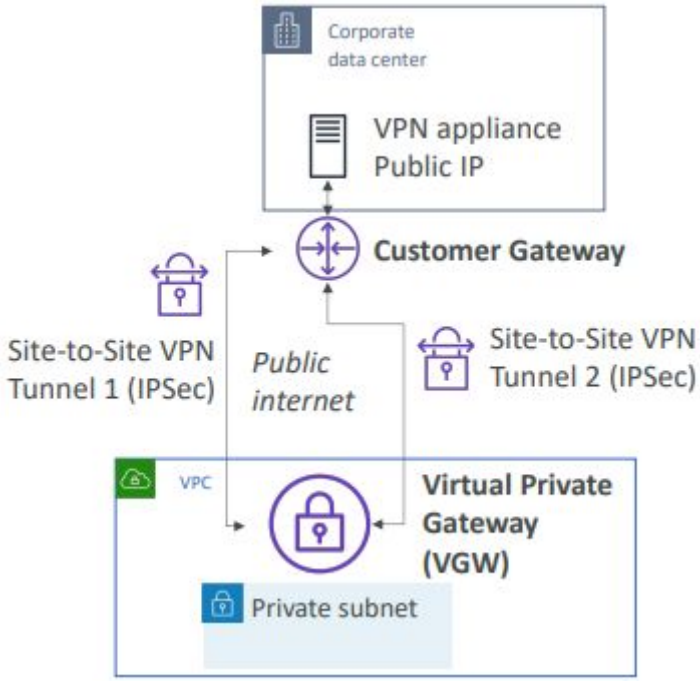


Plan

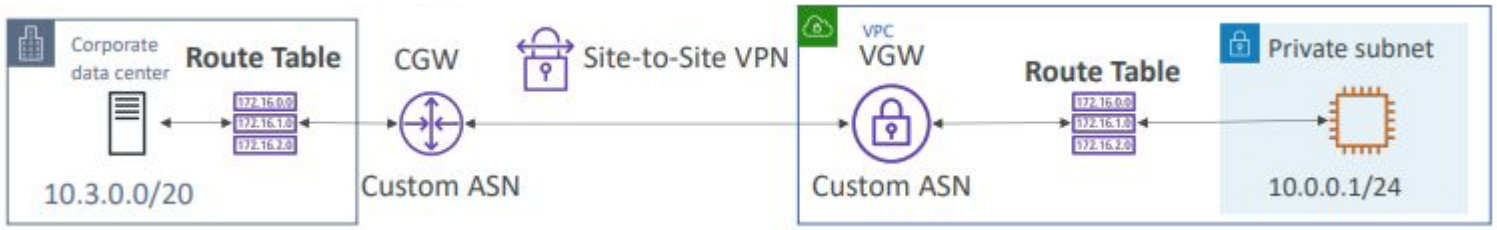
- VPC Lattice
- Direct connect
- VPN
- Amazon route 53
- CloudMap

Virtual Private Network (VPN) Site to Site

- **Sur site :**
  - Configurez un appareil VPN logiciel ou matériel à votre réseau sur site.
  - Le VPN sur site doit être accessible par une adresse IP publique.
- **Côté AWS :**
  - Configurez une passerelle privée virtuelle (VGW) et attachez-la à votre VPC.
  - Configurez une passerelle client pour pointer l'appareil VPN sur site.
- Deux connexions VPN (tunnels) sont créées pour la redondance, cryptées à l'aide de la technologie IPSec
- Deux connexions VPN (tunnels) sont créées pour la redondance, cryptées à l'aide de la technologie IPSec



VPN Site to Site - propagation des routes



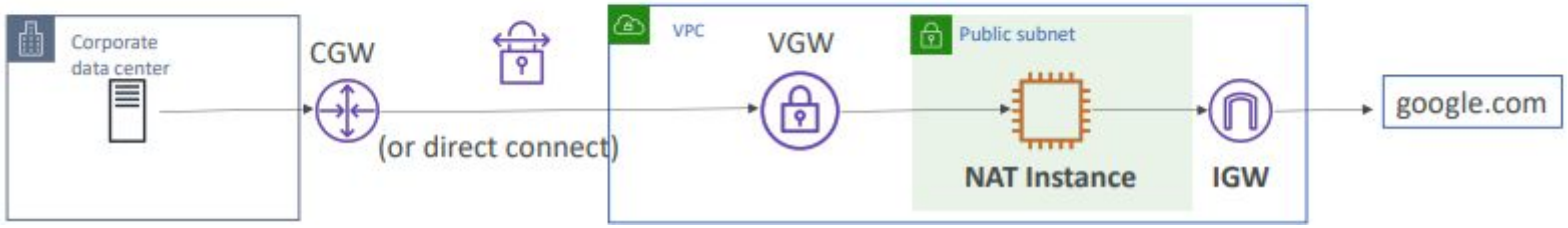
- **Routage statique :**
  - Créer une route statique dans le centre de données de l'entreprise pour 10.0.0.1/24 via le CGW.

  - Créer une route statique dans AWS pour 10.3.0.0/20 via le VGW.
- **Routage dynamique (BGP) :**
  - Utilise le protocole BGP (Border Gateway Protocol) pour partager les routes automatiquement (eBGP pour Internet).
  - Nous n'avons pas besoin de mettre à jour les tables de routage, cela sera fait pour nous dynamiquement.
  - Il suffit de spécifier l'ASN (Autonomous System Number) du CGW et du VGW.

VPN Site to Site et accès internet

- NOT OKAY (bloqué par la restriction NAT Gateway)

- OKAY (self managed NAT Instance – more control)

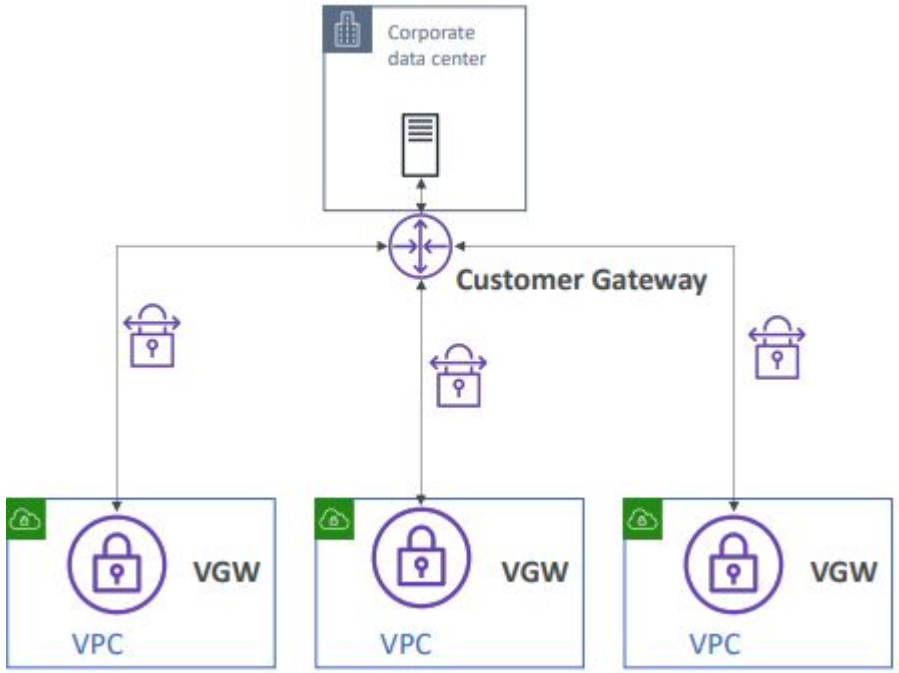


VPN Site to Site et accès internet

- OKAY (alternative à une instance NAT / Gateway)

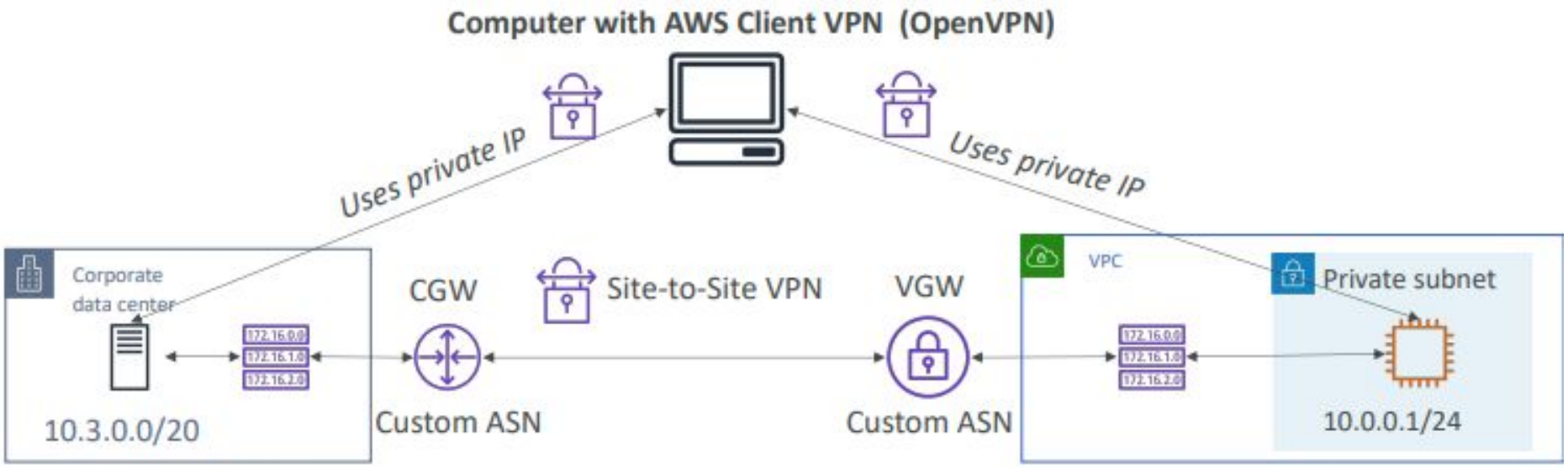
VPN a des multiples VPCs

- Pour les clients basés sur le VPN AWS recommande de créer un VPN distinct distincte pour chaque client VPC.
- Direct Connect est recommandé car il dispose d'une connexion directe Passerelle



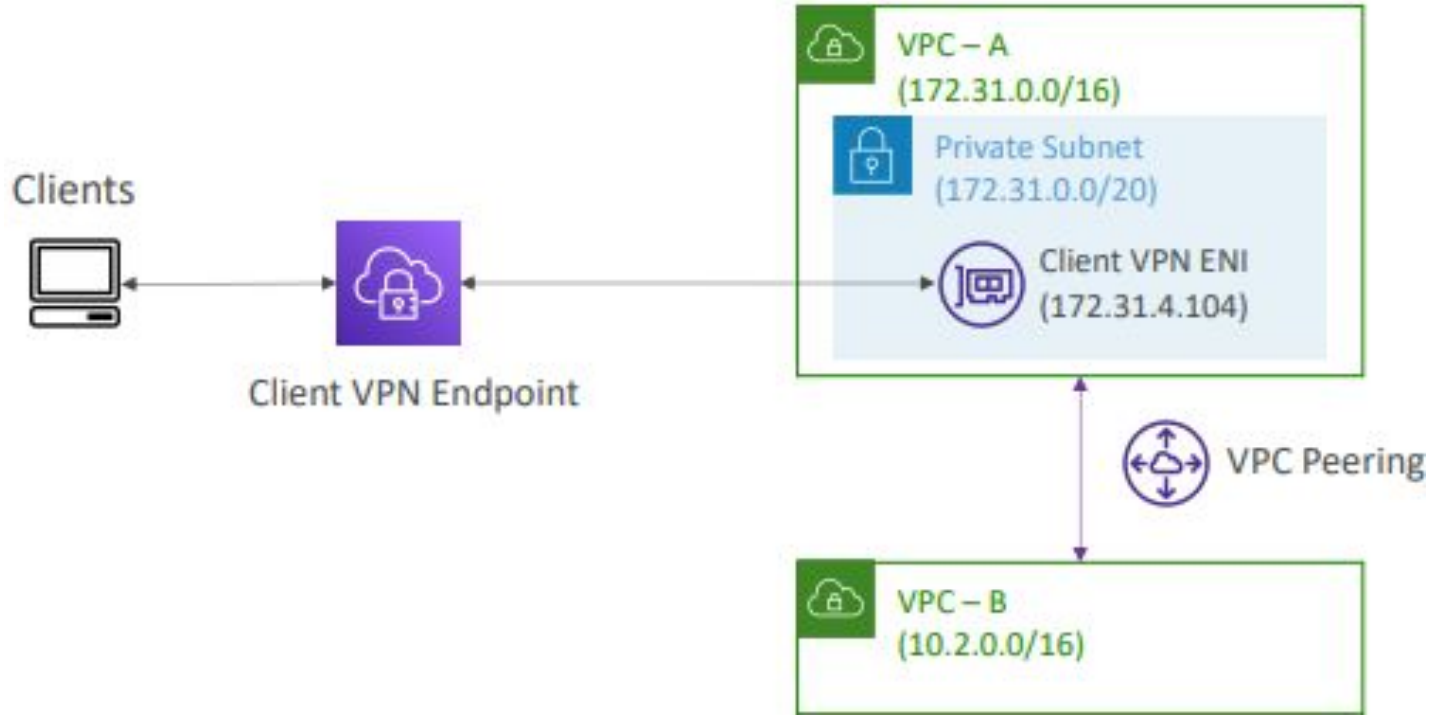
AWS Client VPN

- Connectez-vous à partir de votre ordinateur à l'aide d'OpenVPN à votre réseau privé dans AWS et sur site

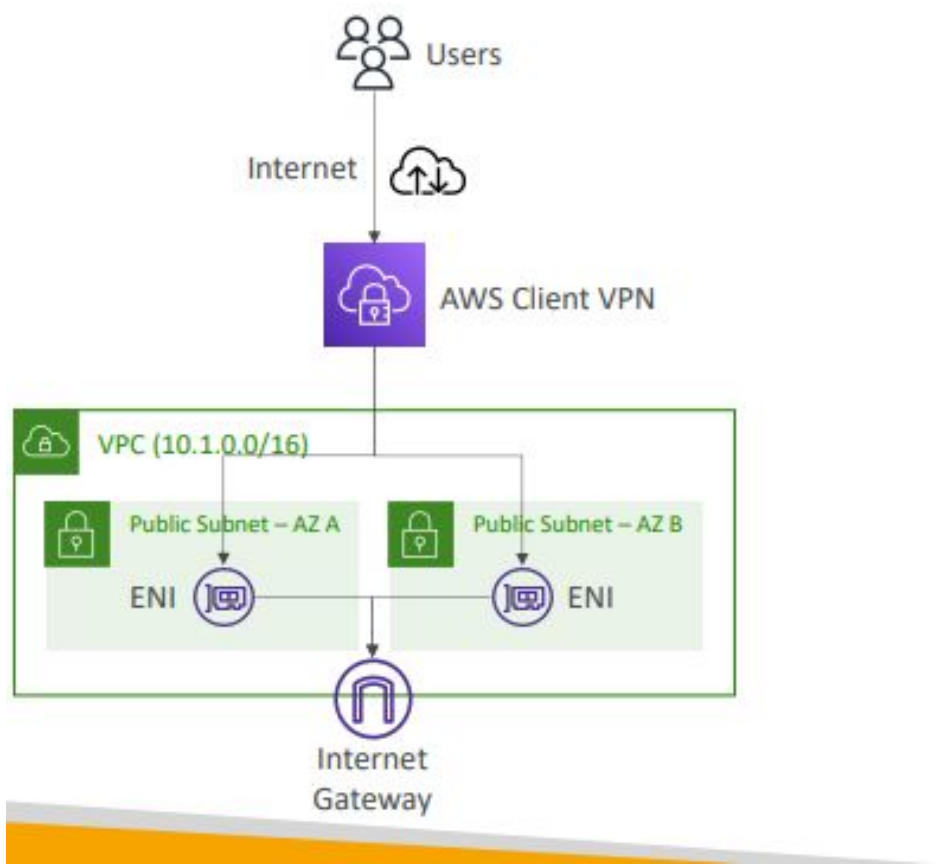


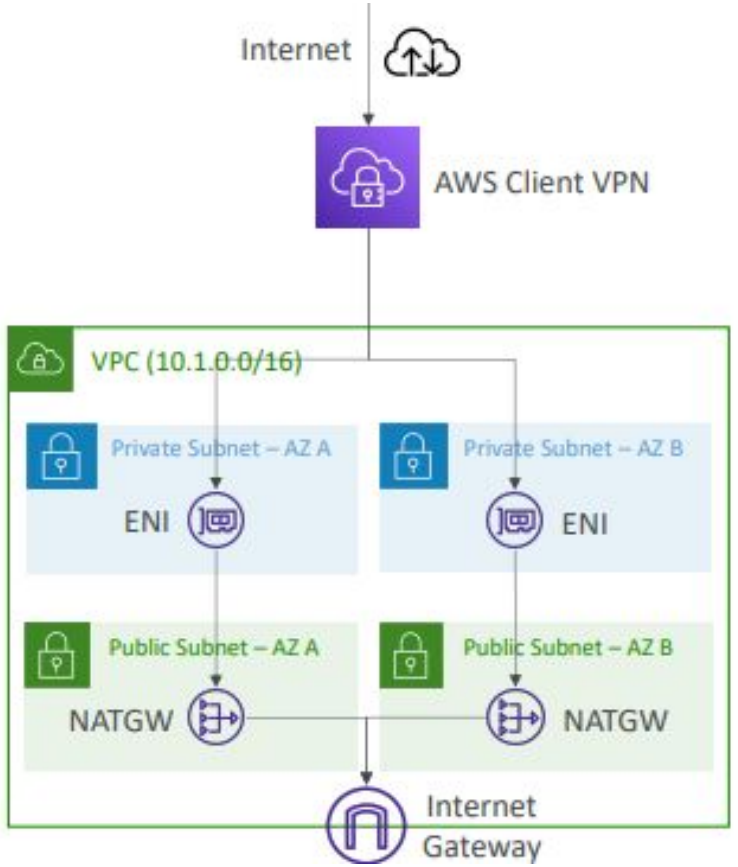
AWS Client VPN -Peered VPC

- Le VPN client est compatible avec le peering VPC



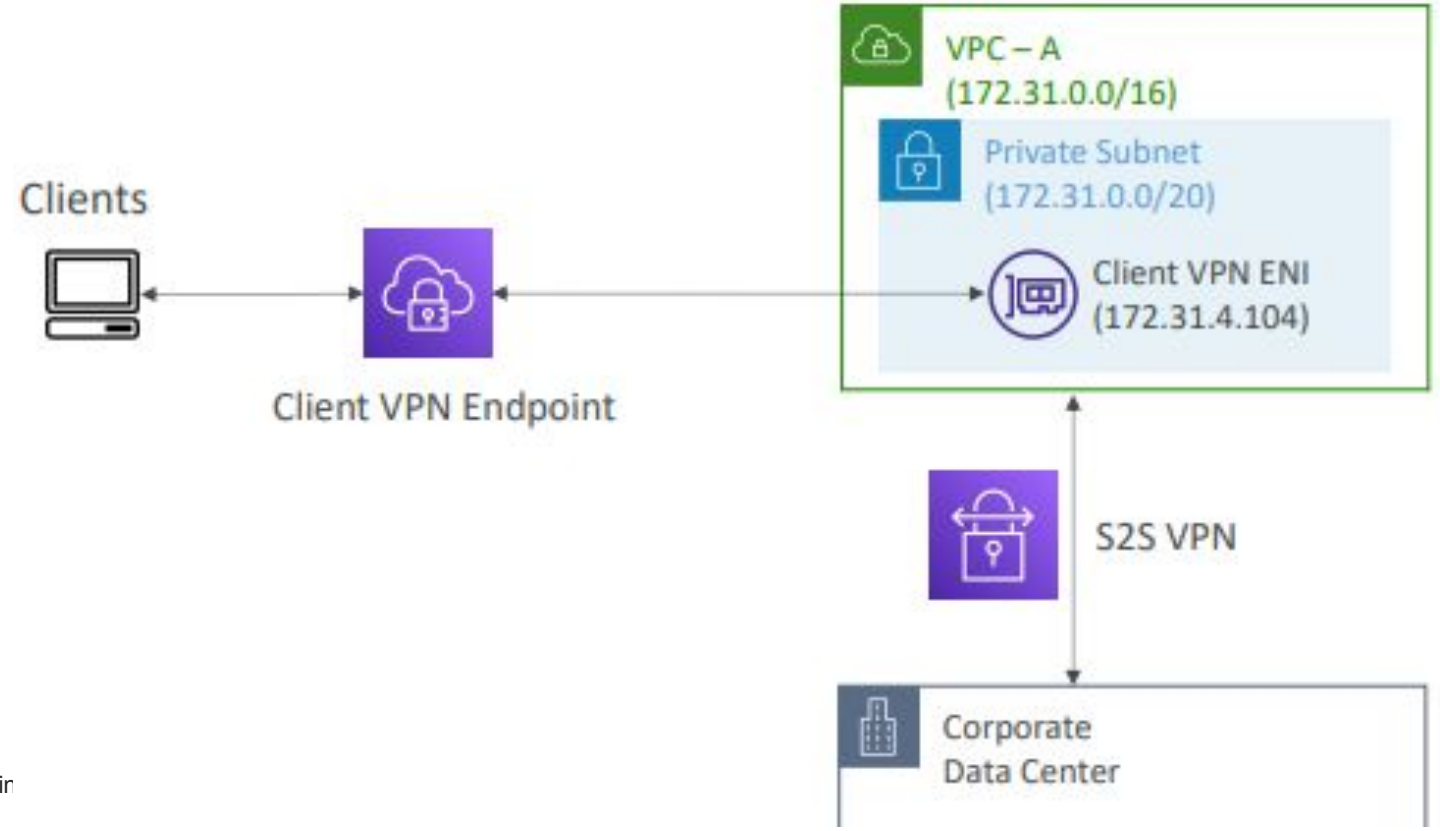
AWS Client VPN -accès internet



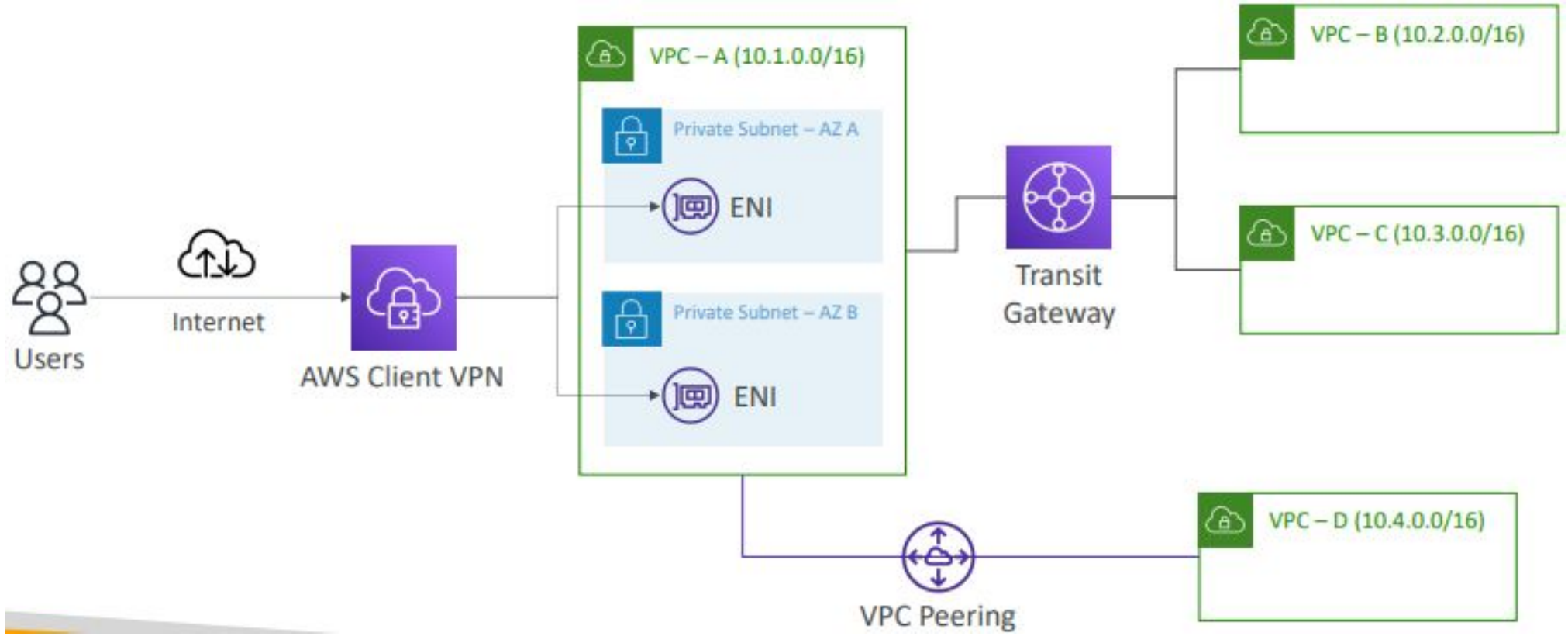


AWS Client VPN -accès On premise

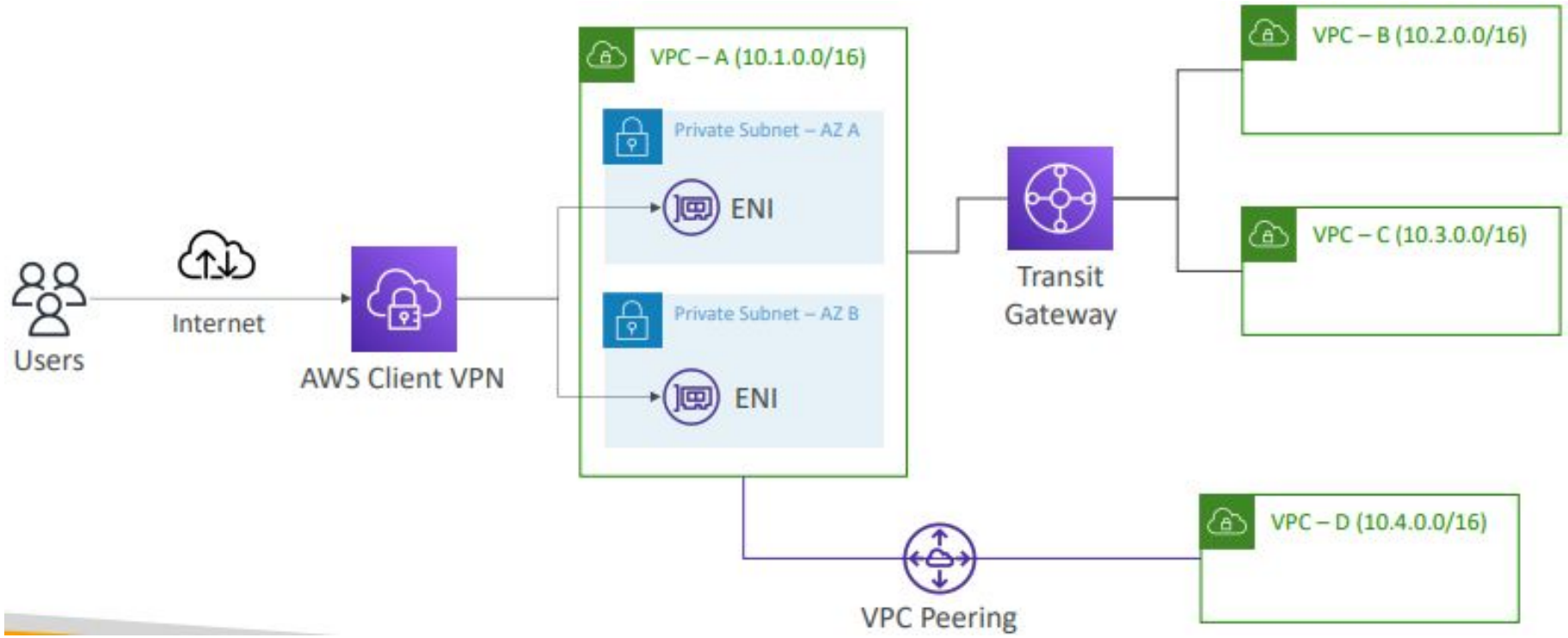
- Accéder aux ressources sur site via AWS avec Client VPN



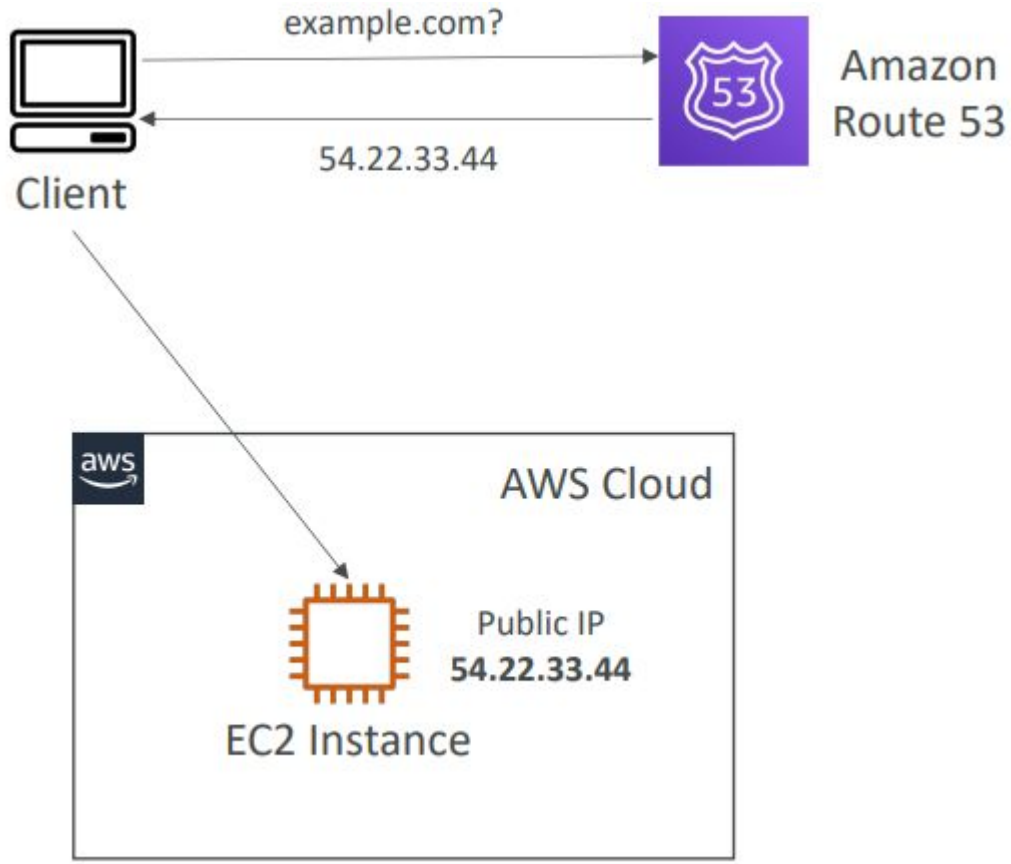
AWS Client VPN -Transit Gateway



AWS Client VPN -Transit Gateway



AWS Route 53 -diagramme d'un enregistrement



Plan

- VPC Lattice
- Direct connect
- VPN
- Amazon route 53
- CloudMap

AWS Route 53

Définition

La route 53 est un service DNS (Domain Name System) géré. où le DNS est un ensemble de règles et d'enregistrements destinés à aider les clients/utilisateurs à comprendre comment d'atteindre n'importe quel serveur par son nom de domaine.

- Les ressources AWS (Load Balancer, CloudFront...) exposent un nom d'hôte AWS : -lb1-1234.us-east-2.elb.amazonaws.com et vous voulez myapp.mydomain.com

- **CNAME :**
  -Pointe un nom d'hôte vers n'importe quel autre nom d'hôte. (app.mydomain.com => blabla.anything.com)
  -UNIQUEMENT POUR LES DOMAINES NON ROOT (aka. something.mydomain.com)
- **Alias :**
  -Pointe un nom d'hôte vers une ressource AWS (app.mydomain.com => blabla.amazonaws.com)
  -Fonctionne pour ROOT DOMAIN et NON ROOT DOMAIN (aka mydomain.com)
  - Gratuit
  - Bilan de santé natif

AWS Route 53 -Records vs Alias

- Les ressources AWS (Load Balancer, CloudFront...) exposent un nom d'hôte AWS :
  -lb1-1234.us-east-2.elb.amazonaws.com et vous voulez myapp.mydomain.com

- **CNAME :**
  -Pointe un nom d'hôte vers n'importe quel autre nom d'hôte. (app.mydomain.com => blabla.anything.com)
  -UNIQUEMENT POUR LES DOMAINES NON ROOT (aka. something.mydomain.com)

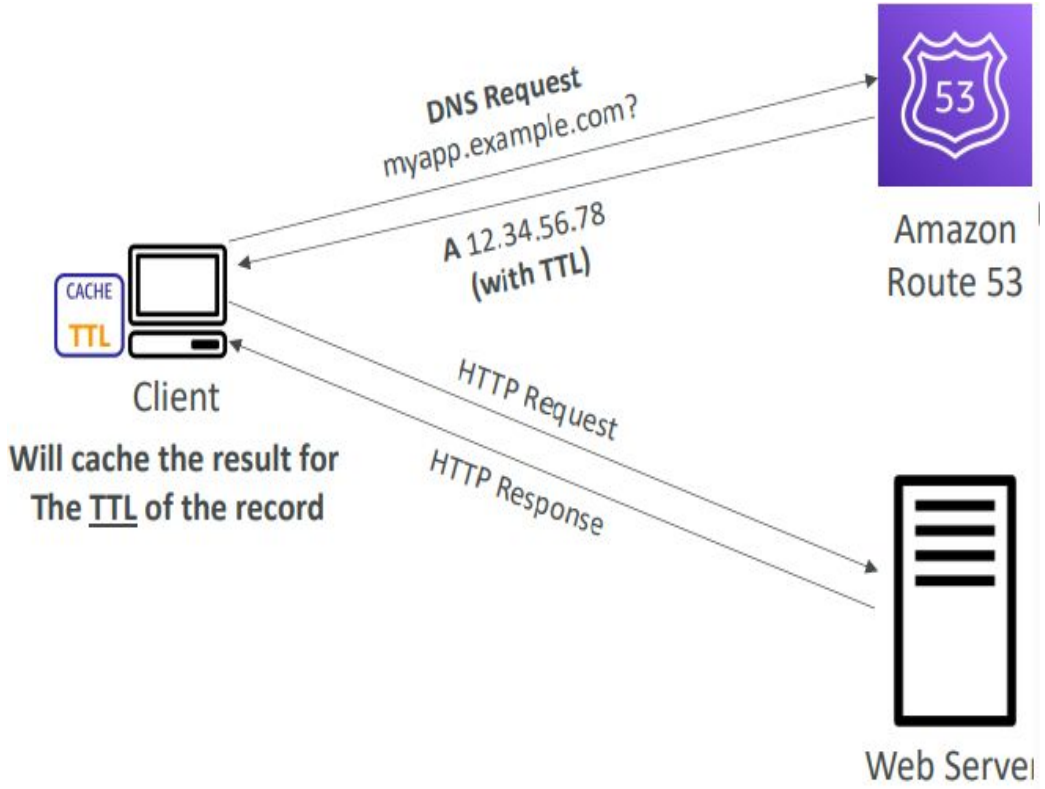
- **Alias :**
  -Pointe un nom d'hôte vers une ressource AWS (app.mydomain.com => blabla.amazonaws.com)
  -Fonctionne pour ROOT DOMAIN et NON ROOT DOMAIN (aka mydomain.com)
  - Gratuit
  - Bilan de santé natif

AWS Route 53 -cibles de l’alias records

- Équilibreurs de charge élastiques
- Distributions CloudFront
- Passerelle API
- Environnements Elastic Beanstalk
- Sites web S3
- Points d'extrémité de l'interface VPC
- Accélérateur Global Accelerator
- Enregistrement de route 53 dans la même zone hébergée
- Vous ne pouvez pas définir un enregistrement ALIAS pour un nom DNS EC2.

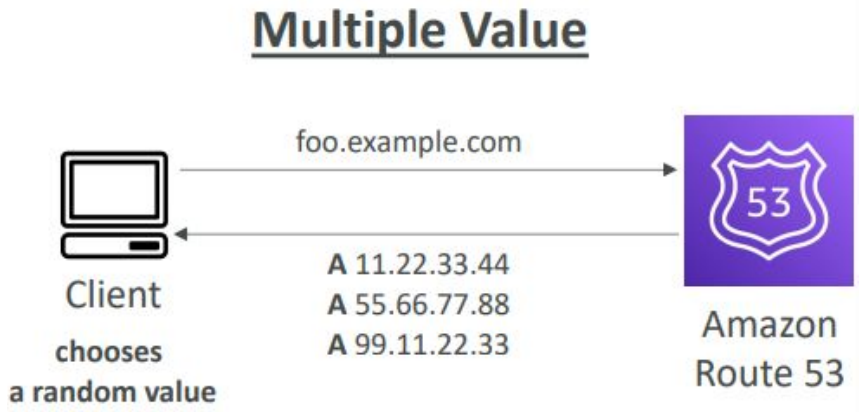
AWS Route 53 -records TTL (Time to Live)

- TTL élevé - par exemple, 24 heures
  - Moins de trafic sur la route 53
  - Enregistrements éventuellement périmés
- TTL faible - par exemple, 60 secondes
  - Plus de trafic sur la route 53 ($$)
  - Les enregistrements sont périmés moins longtemps
  - Facilité de modification des enregistrements
- À l'exception des enregistrements d'alias, le TTL est obligatoire pour chaque enregistrement DNS



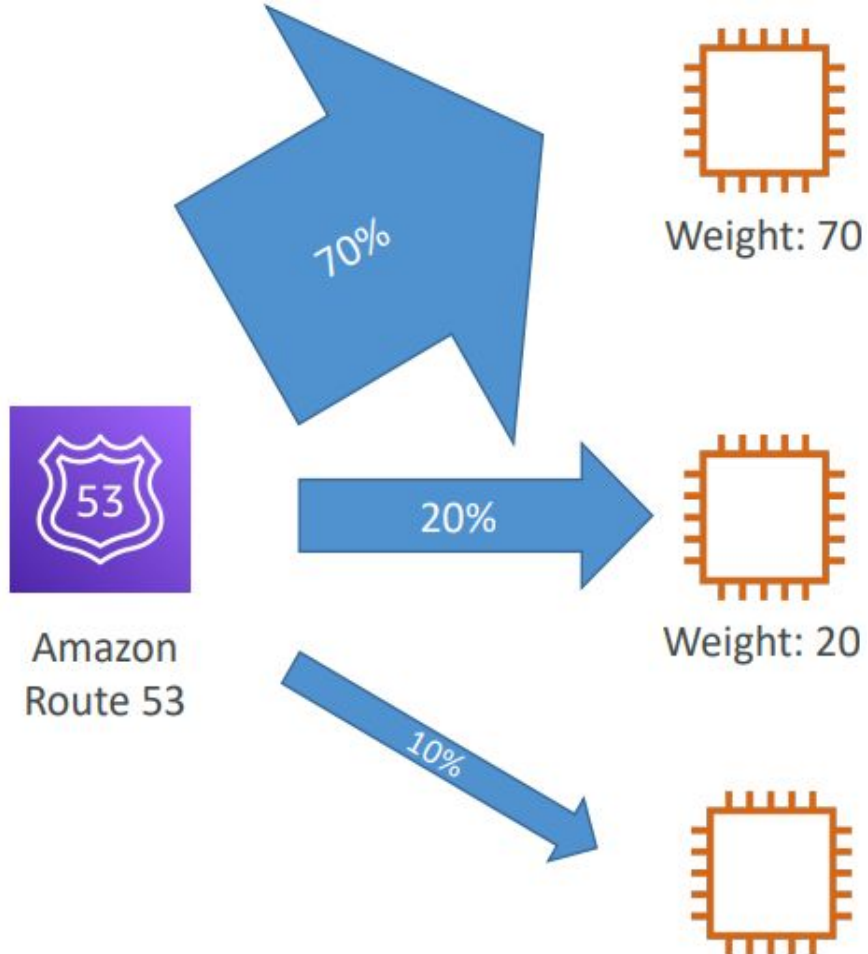
Politique de routage - Simple

- Généralement, l'acheminement du trafic vers une seule ressource
- Ne peut être associé à des contrôles de santé
- Peut spécifier plusieurs valeurs dans le même enregistrement
- Si plusieurs valeurs sont renvoyées, une valeur aléatoire est choisie par le client.



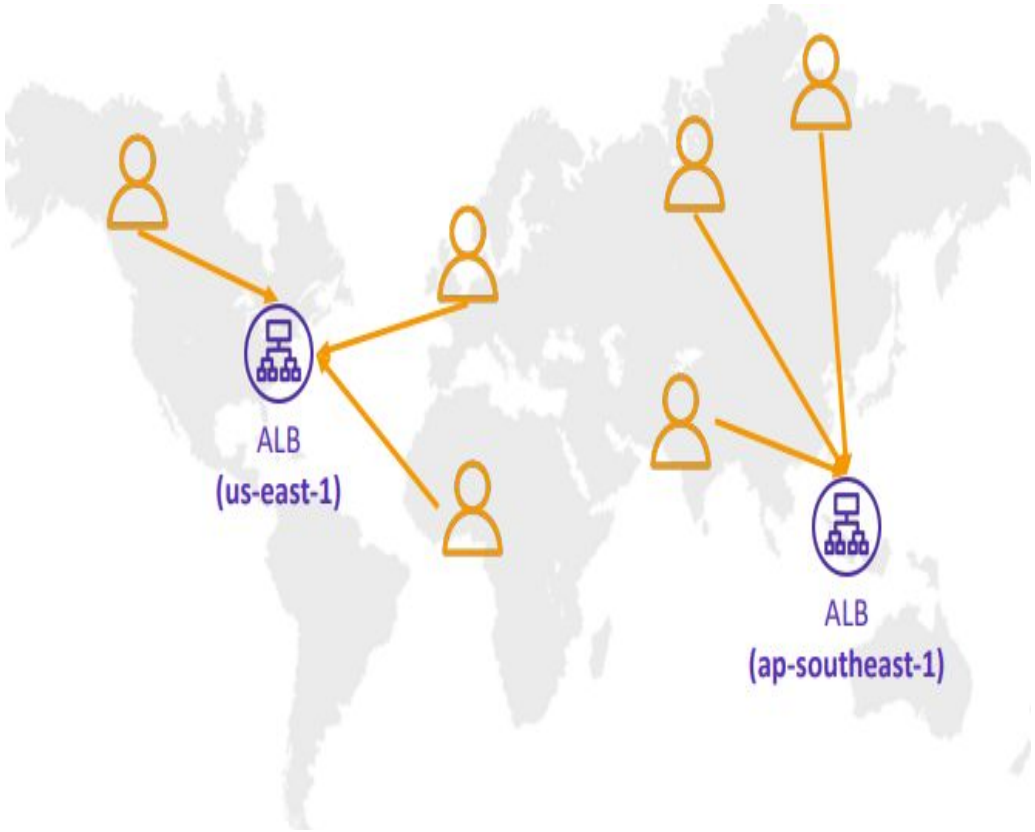
Politique de routage - Weighted

- Contrôler le pourcentage des demandes qui sont adressées à chaque ressource spécifique
- Peut être associé à des bilans de santé
- Cas d'utilisation : équilibrage de la charge entre les régions, test de nouvelles versions d'applications...



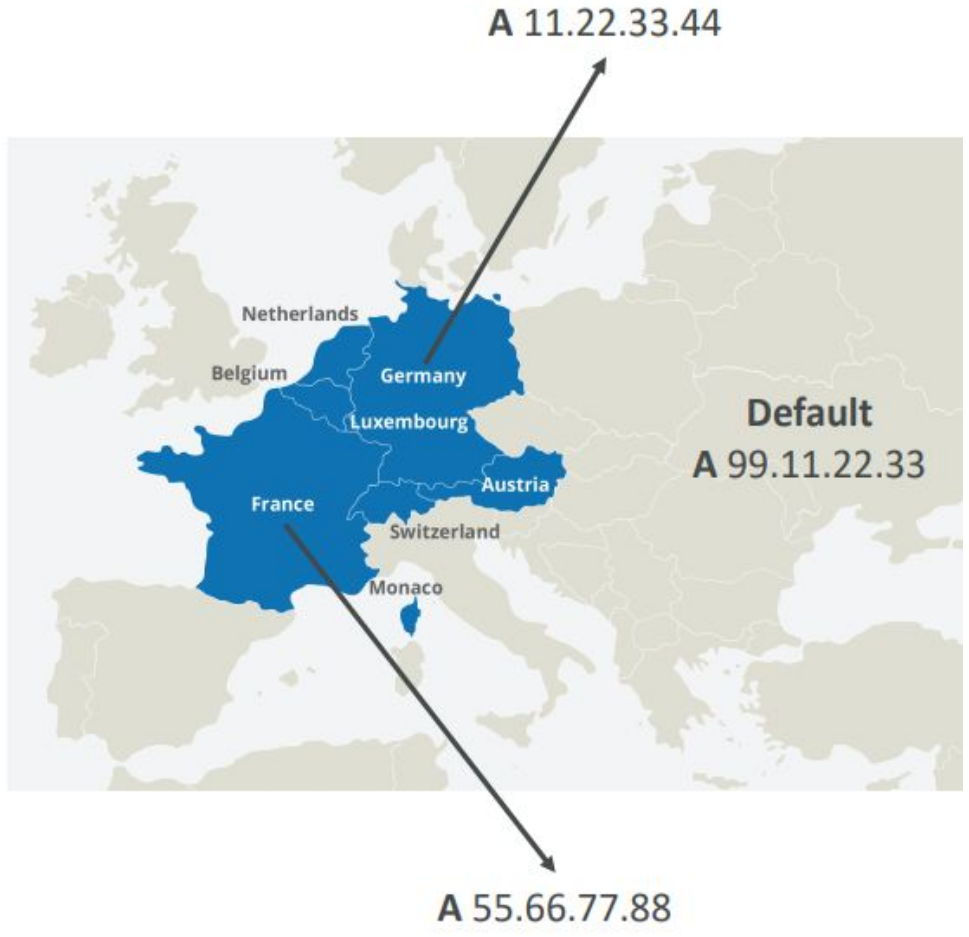
Politique de routage - Latency-based routing

- Redirection vers la ressource qui a le moins de temps de latence près de chez nous
- Très utile lorsque la latence pour les utilisateurs est une priorité
- La latence est basée sur le trafic entre les utilisateurs et AWS Régions
- Les utilisateurs allemands peuvent être dirigés vers les États-Unis (si c'est la latence la plus faible)
- Peut être associé à des bilans de santé(capacité de basculement)



Politique de routage - Failover (Active-passive)

- Différent de l'acheminement basé sur la latence !
- Ce routage est basé sur la localisation de l'utilisateur
- Spécifier la localisation par continent, pays ou par l'État américain (en cas de chevauchement), l'emplacement le plus précis est sélectionné)
- Il faut créer un enregistrement "par défaut" (au cas où il n'y aurait pas de correspondance sur la localisation).
- Cas d'utilisation : localisation de sites web, restriction distribution de contenu, équilibrage de charge,
- Peut être associé à des bilans de santé



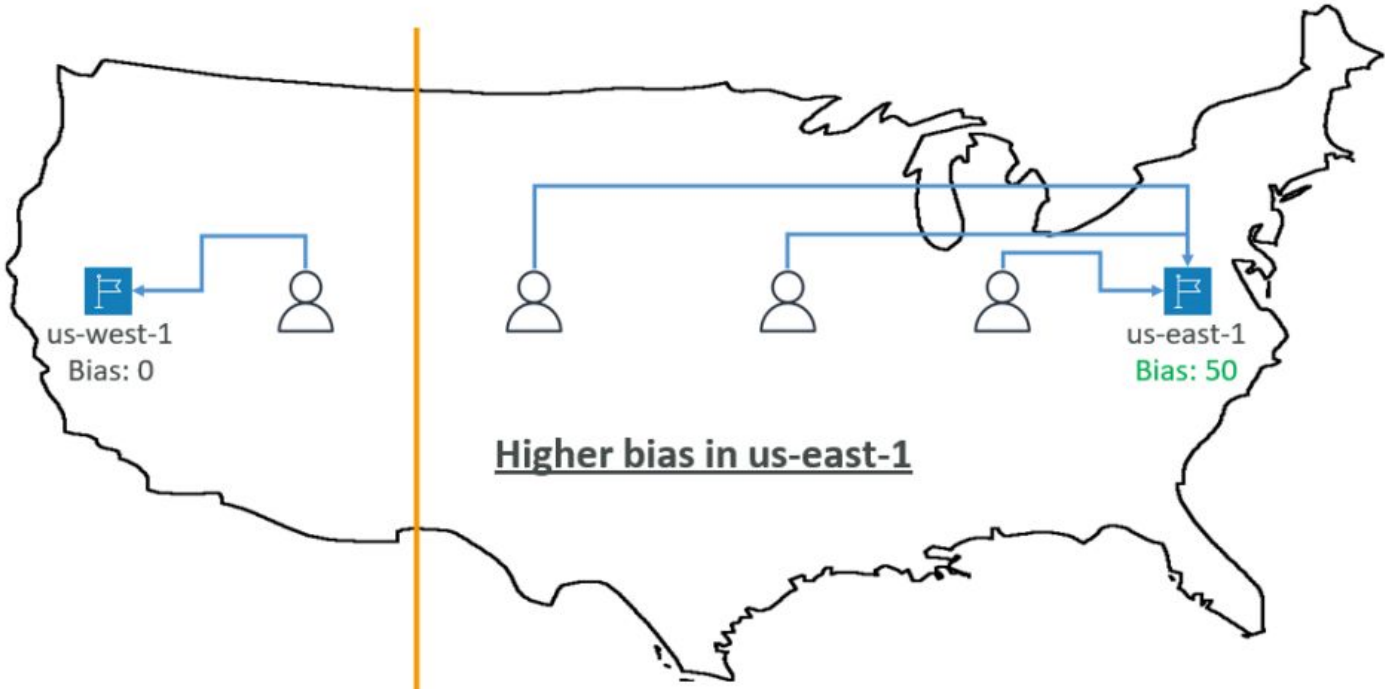
Politique de routage - Geopriximite

- Acheminer le trafic vers vos ressources en fonction de l'emplacement géographique des utilisateurs et des ressources

- Possibilité de déplacer davantage de trafic vers les ressources en fonction du biais défini

- Pour modifier la taille de la région géographique, spécifiez des valeurs de biais :
  - Pour augmenter (1 à 99) - plus de trafic vers la ressource
  - Pour réduire (-1 à -99) - moins de trafic vers la ressource

- Les ressources peuvent être
  - des ressources AWS (spécifier la région AWS)
  - Ressources non AWS (spécifier la latitude et la longitude)
- Vous devez utiliser Route 53 Traffic Flow pour utiliser cette fonctionnalité.



Politique de routage - Multi-Value

- À utiliser lors de l'acheminement du trafic vers plusieurs ressources
- La route 53 renvoie plusieurs valeurs/ressources
- Peut être associé à des bilans de santé (ne renvoie que des valeurs pour des ressources saines)
- Jusqu'à 8 enregistrements sains sont renvoyés pour chaque requête Multi-Value.
- Multi-Value ne remplace pas un ELB.

Name	Type	Value	TTL	Set ID	Health Check
www.example.com	A Record	192.0.2.2	60	Web1	A
www.example.com	A Record	198.51.100.2	60	Web2	B
www.example.com	A Record	203.0.113.2	60	Web3	C

Politique de routage - Hosted Zone

- Un conteneur pour les enregistrements qui définissent comment acheminer le trafic vers un domaine et ses sous-domaines.

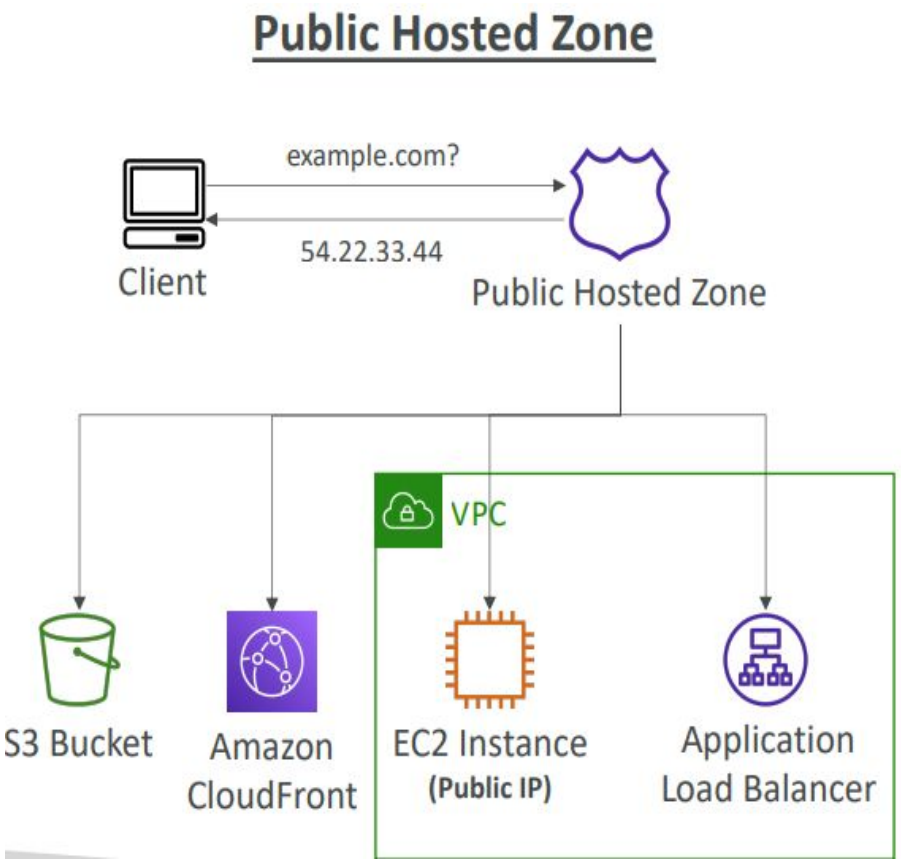
ses sous-domaines

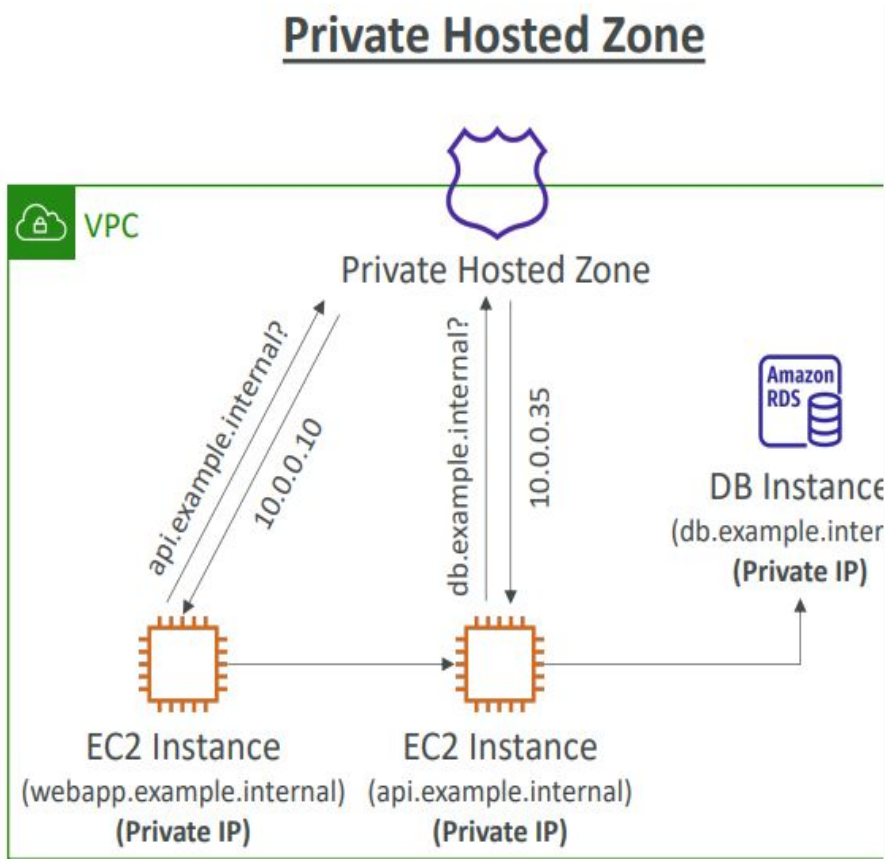
- Zones publiques hébergées - contient des enregistrements qui spécifient comment acheminer le trafic sur Internet (noms de domaines publics)

application1.mondomainepublic.com

- Zones d'hébergement privé - contient des enregistrements qui spécifient comment acheminer le trafic à l'intérieur d'un ou de plusieurs VPC. (noms de domaine privés) application1.company.internal

Politique de routage - Public Hosted Zone vs Private hosted zone





Politique de routage - bon a savoir

- Pour le DNS privé interne (Private Hosted Zone), vous devez activer les paramètres VPC enableDnsHostnames et enableDnsSupport

- **Extensions de sécurité DNS (DNSSEC)**
  -Protocole de sécurisation du trafic DNS, vérifiant l'intégrité et l'origine des données DNS.
  - Protège contre les attaques de l'homme du milieu (MITM).
  - La Route 53 supporte à la fois DNSSEC pour l'enregistrement des domaines et la signature DNSSEC.
  - Fonctionne uniquement avec les zones publiques hébergées

- **Route 53 avec un troisième bureau d'enregistrement**
  -Vous pouvez acheter le domaine sur AWS et utiliser Route 53 comme fournisseur DNS.
  -Mettre à jour les enregistrements NS sur le bureau d'enregistrement tiers

Politique de routage - Health Check

- Les contrôles de santé HTTP ne concernent que les publiques

- Bilan de santé => basculement automatique du DNS :

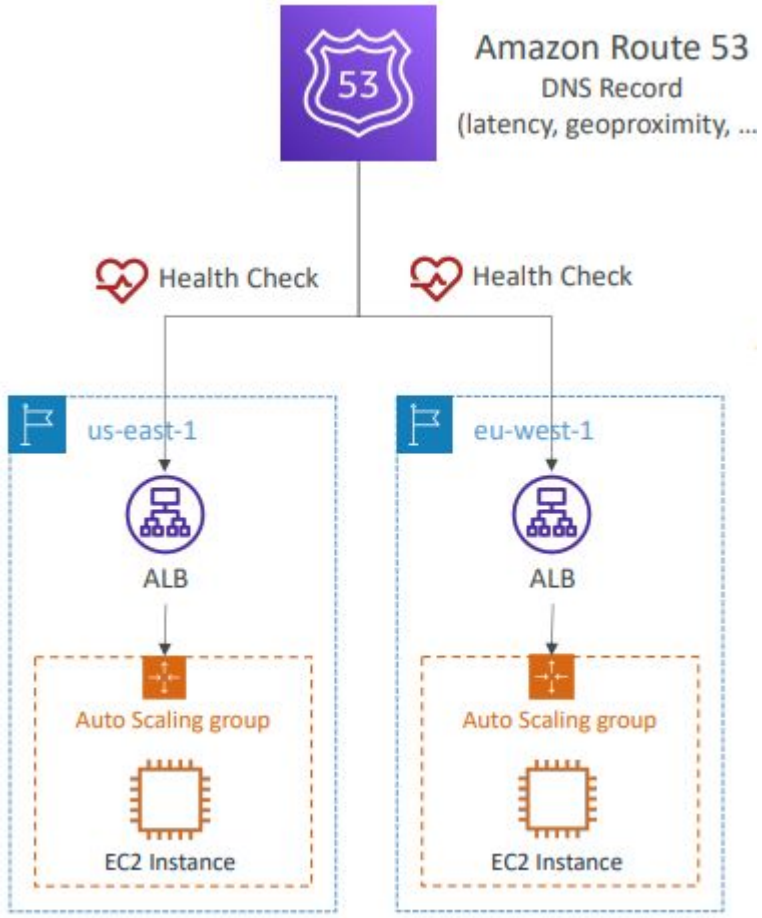
1. Les bilans de santé qui surveillent un point d'extrémité (application, serveur, autre ressource AWS)

2. Contrôles de santé qui surveillent d'autres contrôles de santé d'autres bilans de santé (bilans de santé calculés)

3. Contrôles de santé qui surveillent CloudWatch

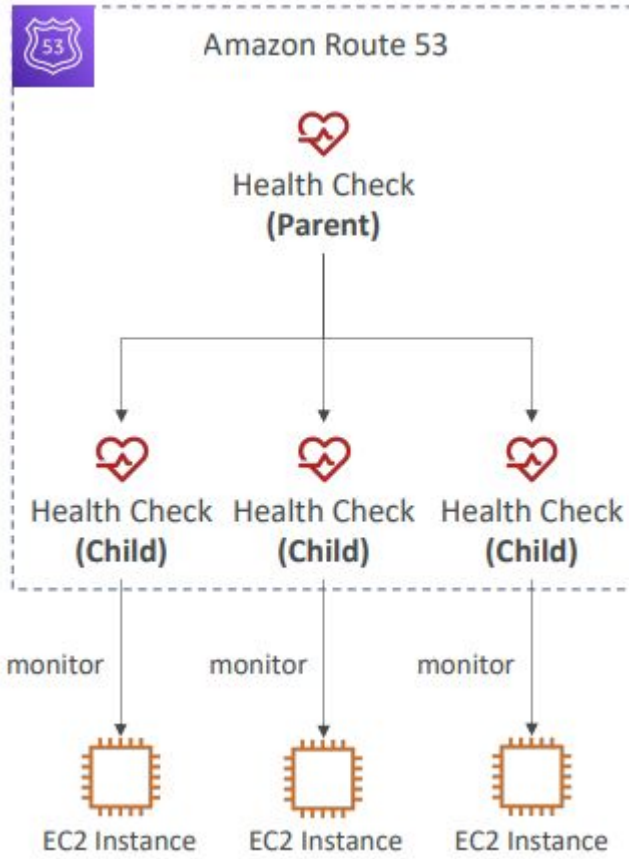
Alarmes (contrôle total ! !) - par exemple, étranglement de DynamoDB, alarmes sur RDS, métriques personnalisées, etc. DynamoDB, alarmes sur RDS, mesures personnalisées, ... (utile pour les ressources privées)

- Les contrôles de santé sont intégrés à CW métriques



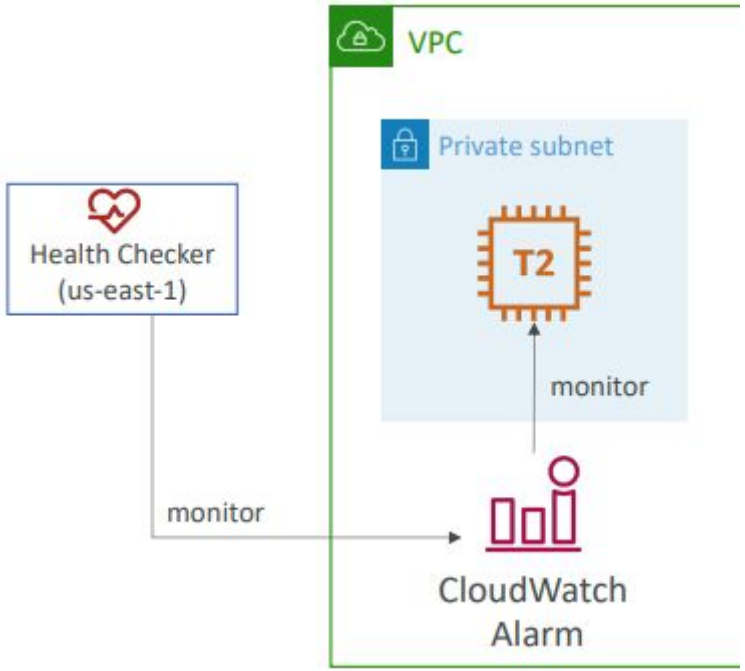
Politique de routage - Calculated Health Check

- Combiner les résultats de plusieurs bilans de santé en un seul bilan de santé
- Vous pouvez utiliser OR, AND ou NOT
- Peut contrôler jusqu'à 256 bilans de santé d'enfants
- Spécifiez le nombre de bilans de santé qui doivent pour que le parent soit accepté
- Utilisation : effectuer la maintenance de votre site web sans faire échouer tous les contrôles de santé



Health Check -Private Hosted Zone

- Les vérificateurs de santé de la route 53 se trouvent à l'extérieur de la VPC
- Ils ne peuvent pas accéder aux points d'extrémité privés (VPC privé ou ressource sur site)
- Vous pouvez créer une métrique CloudWatch et associer une alarme CloudWatch, puis créer un bilan de santé qui vérifie l'alarme elle-même.

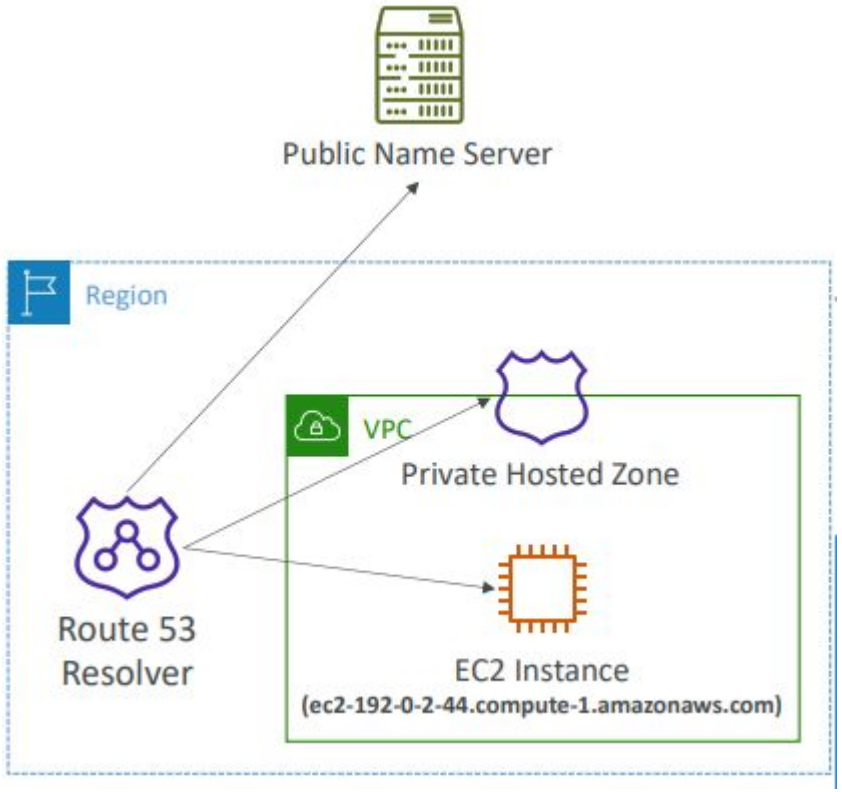


Health Check -Hybrid DNS

- Par défaut, Route 53 Resolver répond automatiquement aux requêtes DNS pour :
  - les noms de domaine locaux pour les instances EC2
  - Enregistrements dans les zones hébergées privées
  - Enregistrements dans les serveurs de noms publics

- DNS hybride - résolution des requêtes entre VPC (Résolveur Route 53) et vos réseaux (autres résolveurs DNS)

- Les réseaux peuvent être :
  - VPC lui-même / VPC en peering
  - Réseau sur site (connecté par Direct Connect ou AWS VPN)

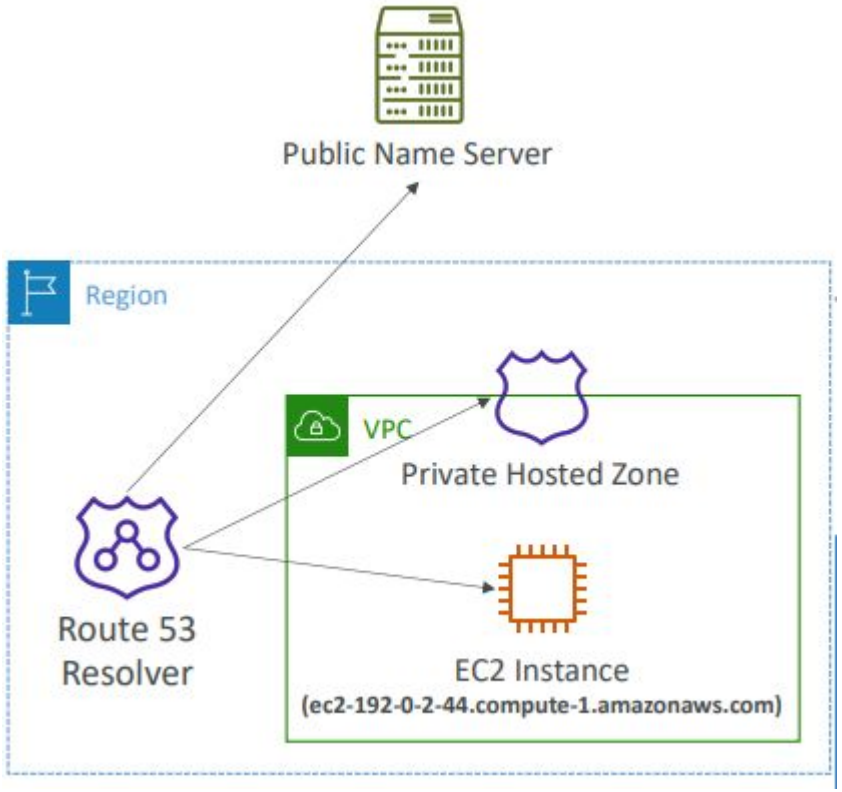


Health Check -Hybrid DNS

- Par défaut, Route 53 Resolver répond automatiquement aux requêtes DNS pour :
  - les noms de domaine locaux pour les instances EC2
  - Enregistrements dans les zones hébergées privées
  - Enregistrements dans les serveurs de noms publics

- DNS hybride - résolution des requêtes entre VPC (Résolveur Route 53) et vos réseaux (autres résolveurs DNS)

- Les réseaux peuvent être :
  - VPC lui-même / VPC en peering
  - Réseau sur site (connecté par Direct Connect ou AWS VPN)



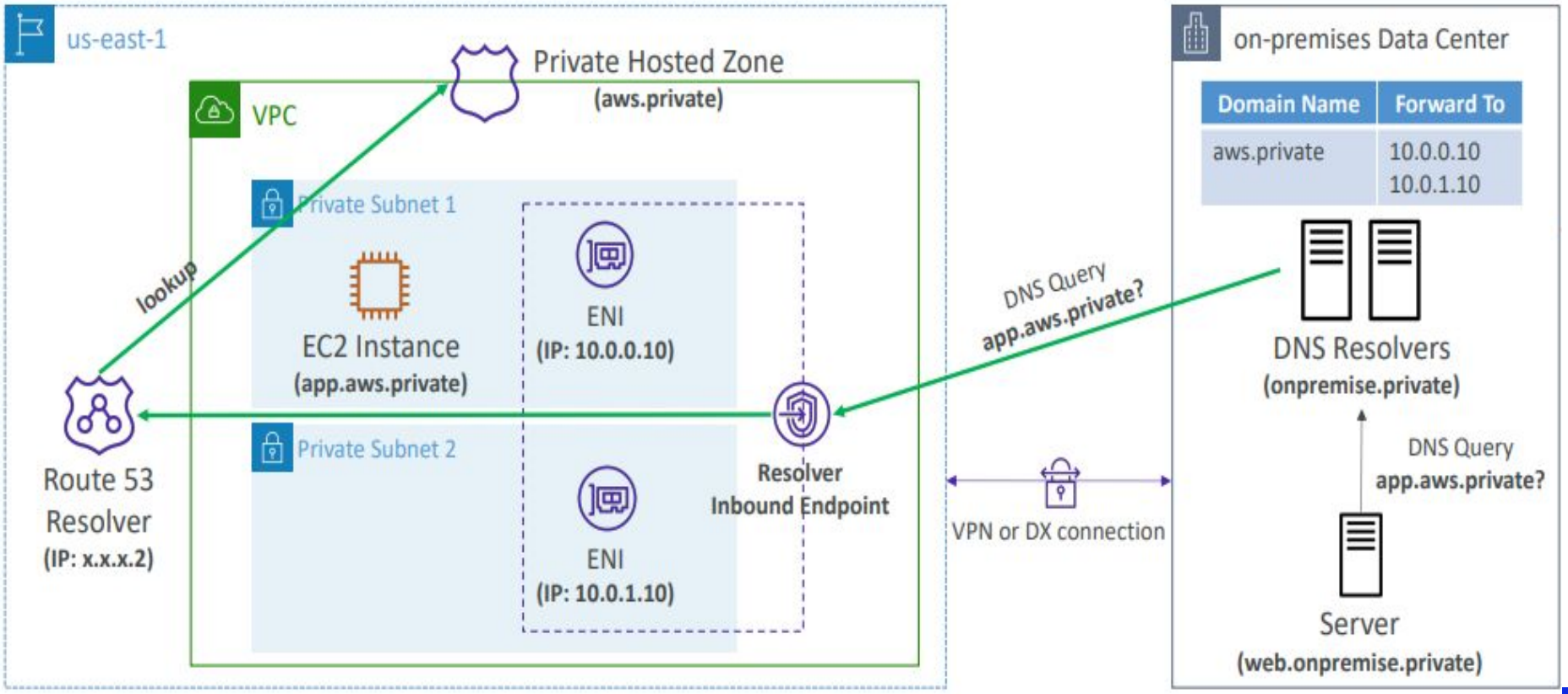
Health Check -Resolver Endpoints

- **Endpoint entrant**
  - Les résolveurs DNS de votre réseau peuvent transmettre les requêtes DNS au résolveur de la route 53.
  - Permet à vos résolveurs DNS de résoudre les noms de domaine pour les ressources AWS (par exemple, les instances EC2 et les enregistrements dans les Private Hosted Zones de la Route 53)

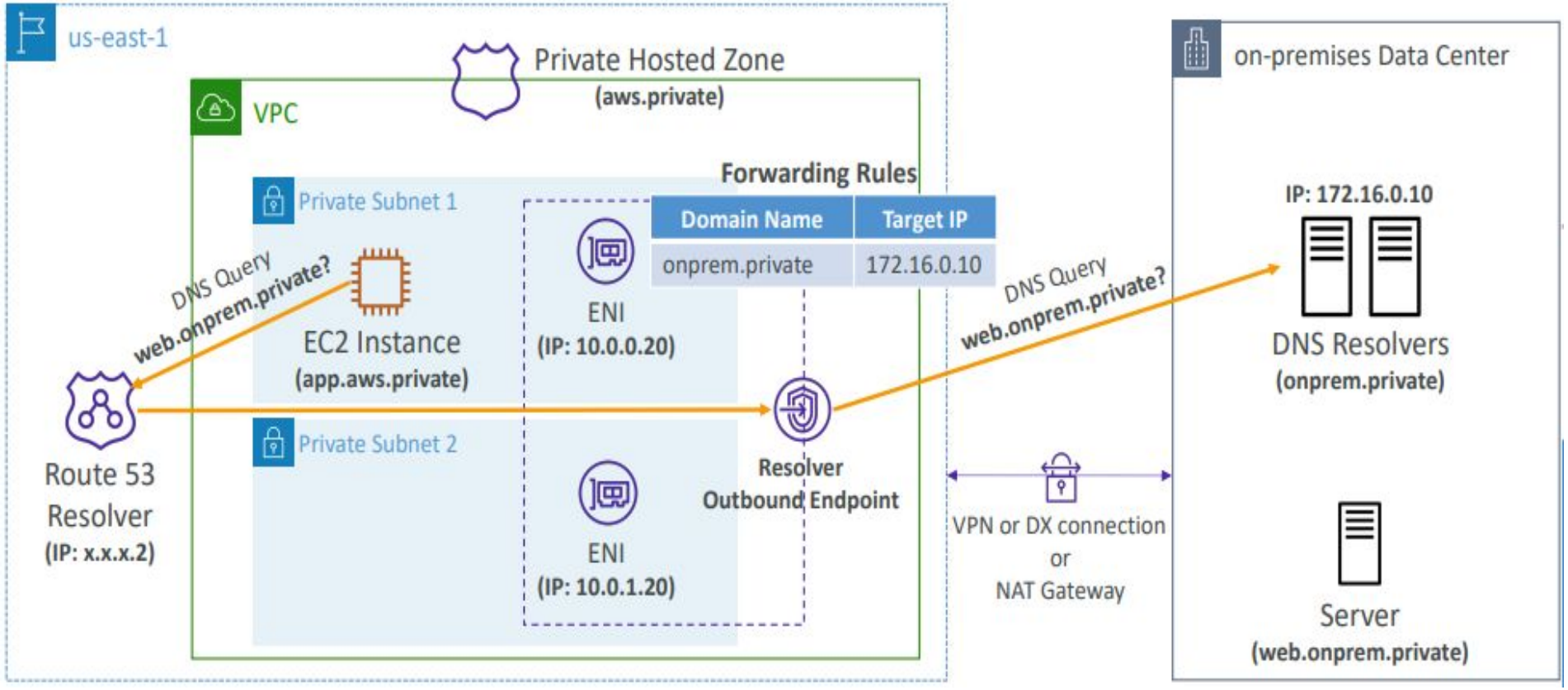
- **Endpoint sortant**
  - Route 53 Resolver transmet de manière conditionnelle les requêtes DNS à vos DNS Resolvers.
  - Utilisez les règles de résolution pour transmettre les requêtes DNS à vos résolveurs DNS.

- Associé à un ou plusieurs VPC dans la même région AWS
- Créé dans deux AZ pour la haute disponibilité
- Chaque point d'extrémité prend en charge 10 000 requêtes par seconde et par adresse IP.

Health Check -Resolver inbound Endpoints



Health Check -Resolver Outbound Endpoints



Plan

- VPC Lattice
- Direct connect
- VPN
- Amazon route 53
- CloudMap

AWS Cloud Map

Définition

AWS Cloud Map est un service qui assure le suivi des composants de l'application et de leur état de santé et permet une mise à l'échelle et une dynamique et la réactivité de l'application.

- Il utilise l'API de découverte pour renvoyer des URL et des adresses IP.
- Il permet de découvrir des services à l'aide du SDK AWS, d'appels API, ou de requêtes DNS.
- AWS Cloud Map ne renvoie des instances saines que si la vérification de l'état de santé est spécifiée lors de la création du service.
- Il s'intègre fortement à Amazon Elastic Container Service.

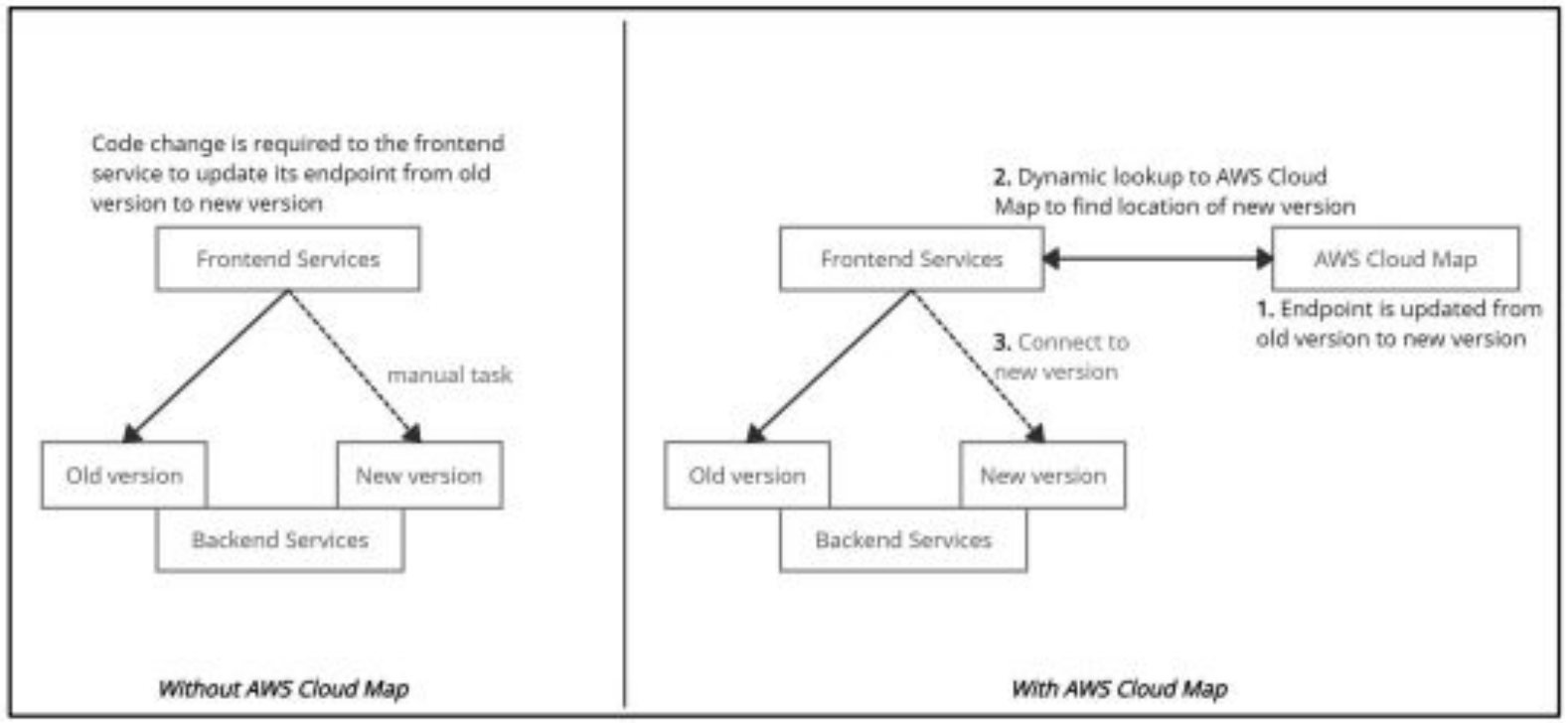
AWS Cloud Map

Lorsqu'une nouvelle ressource est ajoutée, une instance de service est créée en appelant l'action API **RegisterInstance**. L'instance de service aide à localiser la ressource à l'aide du DNS ou de l'action API AWS Cloud Map **DiscoverInstances.**

Il réduit la consommation de temps car il empêche l'utilisateur de gérer manuellement les noms des ressources et leur emplacement dans le code de l'application.

AWS Cloud Map fournit un registre pour les services d'application définis par les espaces de noms et empêche les développeurs de stocker, de suivre et de mettre à jour les noms de ressources et les informations de localisation dans le code de l'application.

AWS Cloud Map -exemple



AWS Cloud Map

MERCI POUR VOTRE AIMABLE ATTENTION!

EAZYTraining

Alphonsine Lahda

Lahda Biassou Alphonsine

Ingénieure cloud et Formatrice