LeCloudFacile.com

Fiche de révision Amazon VPC

Introduction

- **Virtual Private Cloud (VPC)** est un service AWS qui permet de créer un réseau virtuel isolé dans le cloud AWS où vous pouvez lancer vos ressources AWS.
  - Le VPC vous donne un contrôle total sur votre environnement réseau, y compris la sélection de votre propre plage d'adresses IP, la création de sous-réseaux, et la configuration de tables de routage et de passerelles réseau.
- **Concepts clés du VPC**
  - **Sous-réseaux (Subnets)** : Divisions logiques d'un réseau VPC dans des segments plus petits à l'intérieur d'une zone de disponibilité AWS.
  - **Groupes de sécurité (Security Groups)** : Pare-feu virtuels qui contrôlent le trafic entrant et sortant des instances EC2.
  - **Listes de contrôle d'accès réseau (Network ACLs)** : Contrôlent le trafic réseau entrant et sortant au niveau du sous-réseau.
  - **Passerelles Internet (Internet Gateways)** : Permettent aux instances dans un VPC de communiquer avec Internet.
  - **Passerelles NAT (Network Address Translation)** : Permettent aux instances dans un VPC privé d'accéder à Internet tout en empêchant Internet d'initier des connexions avec ces instances.
  - **Peering VPC (VPC Peering)** : Connexion entre deux VPC qui permet le routage du trafic entre eux à l'aide d'adresses IP privées.
  - **Points de terminaison VPC (VPC Endpoints)** : Permettent aux instances dans votre VPC d'accéder aux services AWS (comme S3) sans passer par Internet.
  - **VPN Site à Site et AWS Direct Connect** : Options pour connecter un réseau sur site à un VPC AWS de manière sécurisée.
  - **Passerelle de transit (Transit Gateway)** : Centralise la gestion des connexions VPN et Direct Connect pour plusieurs VPC et réseaux sur site.
- **Configuration par défaut du VPC**
  - AWS crée automatiquement un VPC par défaut pour chaque compte AWS dans chaque région.
  - Ce VPC par défaut comprend un seul sous-réseau public et une passerelle Internet attachée.

Composants du VPC

- **Structure du VPC**
  - **Plage CIDR**: Chaque VPC est associé à une plage d'adresses IP spécifique définie lors de sa création. Cette plage permet de déterminer les adresses IP privées disponibles pour les instances EC2 et autres ressources.
- **Sous-réseaux (Subnets)**
  - Les sous-réseaux sont des subdivisions d'un VPC qui sont associées à des zones de disponibilité (AZ) spécifiques d'une région AWS.
  - **Sous-réseau public**: Accessible depuis Internet, il permet aux instances EC2 d'avoir des adresses IP publiques et de communiquer directement avec Internet via une **passerelle Internet**.
  - **Sous-réseau privé**: N'est pas accessible directement depuis Internet. Idéal pour les bases de données ou autres instances ne nécessitant pas d'accès public direct.
- **Route Tables (Tables de routage)**
  - Les tables de routage définissent les règles pour diriger le trafic réseau dans et hors des sous-réseaux.
  - Un sous-réseau public a une route vers une **passerelle Internet** pour permettre l'accès à Internet.
  - Pour les sous-réseaux privés, on peut configurer une **passerelle NAT (Network Address Translation)** pour permettre l'accès à Internet tout en maintenant la sécurité en limitant l'accès direct.
- **Passerelles**
  - **Passerelle Internet**: Permet aux instances dans un sous-réseau public d'accéder à Internet.
  - **Passerelle NAT**: Utilisée dans les sous-réseaux privés pour permettre aux instances d'accéder à Internet de manière contrôlée et sécurisée.
- **Configuration par défaut du VPC**
  - AWS crée automatiquement un VPC par défaut pour chaque compte dans chaque région.
  - Ce VPC par défaut comprend généralement plusieurs sous-réseaux (publics et privés), une table de routage par défaut et une passerelle Internet attachée au sous-réseau public.
- **Utilisation pratique dans AWS**

- Lors du déploiement d'instances EC2, il est crucial de sélectionner le sous-réseau approprié pour déterminer l'accès Internet et les configurations de sécurité.
- Les concepts de VPC sont essentiels pour comprendre la conception sécurisée et efficace des architectures dans AWS.

Sécurité

- **Introduction à la sécurité réseau dans le VPC AWS**
  - **AWS Virtual Private Cloud (VPC)** permet de créer un réseau privé virtuel dans le cloud AWS pour déployer des ressources de manière isolée et sécurisée.
- **Network ACL (NACL) - Liste de contrôle d'accès réseau**
  - La NACL agit comme un pare-feu au niveau du sous-réseau dans le VPC.
  - **Contrôle du trafic** : Permet de définir des règles d'autorisation et de refus pour le trafic entrant et sortant, basées uniquement sur les adresses IP.
  - Les règles doivent être explicitement définies pour autoriser le trafic de retour, ce qui signifie qu'elle est **"sans état"**.
  - Associée à un ou plusieurs sous-réseaux dans le VPC pour filtrer le trafic avant qu'il n'atteigne les instances EC2.
- **Groupes de sécurité**
  - Les groupes de sécurité agissent également comme un pare-feu, mais au niveau de l'instance EC2.
  - **Contrôle du trafic** : Se compose uniquement de règles d'autorisation, permettant de spécifier quels types de trafic sont autorisés à destination et en provenance d'une instance.
  - Permet de référencer d'autres groupes de sécurité en tant que source de trafic, en plus des adresses IP.
  - Par défaut, les groupes de sécurité sont **"stateful"**, ce qui signifie que les réponses au trafic autorisé sont automatiquement permises.
- **Différences clés entre NACL et groupes de sécurité**
  - **NACL** :
    - Agit au niveau du sous-réseau.
    - Supporte les règles d'autorisation et de refus.
    - Doit explicitement autoriser le trafic de retour.
  - **Groupes de sécurité** :

        - Agissent au niveau de l'instance EC2.
        - Supportent uniquement les règles d'autorisation.
        - Sont "stateful", autorisant automatiquement le trafic de retour pour le trafic autorisé.
- **Utilisation pratique dans AWS**
    - Lors de la création ou de la configuration d'instances EC2 dans un VPC, il est essentiel de définir correctement les groupes de sécurité et les NACL pour assurer une sécurité efficace.
    - Les NACL offrent une couche de sécurité supplémentaire au niveau du sous-réseau, tandis que les groupes de sécurité permettent un contrôle granulaire sur le trafic au niveau de l'instance.
- **Configuration dans AWS Console**
    - Dans la console AWS, les NACL et les groupes de sécurité sont configurés sous l'onglet VPC.
    - Les NACL sont associées aux sous-réseaux spécifiques dans le VPC et permettent de configurer des règles d'autorisation et de refus.
    - Les groupes de sécurité sont associés aux instances EC2 individuelles et contrôlent le trafic entrant et sortant pour ces instances.

VPC Flow logs

- **Journaux de flux VPC (VPC Flow logs)**
    - **Définition** : Les journaux de flux VPC enregistrent tout le trafic IP passant par les interfaces de réseau dans un VPC.
    - **Utilisation** : Ils sont essentiels pour la surveillance et le dépannage des problèmes de connectivité réseau, comme les difficultés à se connecter à Internet ou entre différents sous-réseaux.
- **Caractéristiques des journaux de flux VPC (VPC Flow logs)**
    - **Types de journaux** :
        - **Flux VPC** : Capture tout le trafic d'un VPC.
        - **Flux de sous-réseau** : Spécifique à un sous-réseau.
        - **Flux d'interface réseau élastique** : Pour les interfaces ENI (Elastic Network Interface).
    - **Destination des journaux** : Les journaux peuvent être envoyés vers :
        - Amazon S3
        - CloudWatch Logs

        - Kinesis Data Firehose
    - **Configuration** : Lors de la création d'un flux log, vous pouvez spécifier :
        - Le nom du flux
        - Les filtres pour le trafic (tout, accepté, rejeté)
        - L'intervalle d'agrégation
        - La destination du journal
    - **Format des enregistrements** :
        - Les enregistrements des journaux incluent des informations telles que l'adresse source, l'adresse de destination, les ports, le protocole, le nombre de paquets, le début et la fin de la communication, l'action (accepté ou rejeté), et l'état du journal.
- **Connexions de peering VPC**
    - **Définition** : Le peering VPC permet de connecter deux VPC de manière privée, leur permettant de communiquer comme s'ils faisaient partie du même réseau.
    - **Conditions** : Les adresses IP des VPC ne doivent pas se chevaucher pour établir une connexion de peering.
- **Caractéristiques du peering VPC**
    - **Non transitif** : Une connexion de peering VPC entre VPC 1 et VPC 2 ne permet pas à VPC 2 de communiquer directement avec VPC 3, sauf si une connexion de peering distincte est établie entre VPC 2 et VPC 3.
    - **Régions et comptes** : Peut être établi entre VPC dans la même région ou entre régions différentes, ainsi que entre comptes AWS différents (à condition d'autoriser explicitement le peering).

Connectivité hybride : VPN site à site, Direct Connect

- **VPN de site à site**
    - **Définition** : Un VPN de site à site permet de connecter un centre de données sur site à un VPC AWS de manière sécurisée et cryptée via Internet public.
    - **Fonctionnement** : La connexion VPN établit un tunnel sécurisé entre le centre de données et AWS, assurant la confidentialité des données transitant entre les deux.
    - **Avantages** :
        - **Rapidité de déploiement** : Peut être mis en place en quelques minutes.
        - **Coût réduit** par rapport à la connexion directe.
    - **Inconvénients** :

        - **Bande passante limitée** et potentiellement sujette à des fluctuations de performance dues à l'Internet public.
        - **Sécurité** : Bien que cryptée, elle dépend de l'infrastructure publique d'Internet.
- **Direct Connect**
    - **Définition** : Une connexion directe (DX) établit une liaison physique entre le centre de données sur site et AWS via un réseau privé.
    - **Fonctionnement** : Utilise un circuit dédié (fibre optique) pour garantir une connexion privée, sécurisée et à faible latence entre les sites.
    - **Avantages** :
        - **Sécurité renforcée** : Pas de transmission via l'Internet public.
        - **Performances élevées et constantes** : Garantit une bande passante stable et prévisible.
    - **Inconvénients** :
        - **Coût élevé** : Nécessite des frais pour la mise en place du circuit physique et des frais de connexion.
        - **Temps de déploiement plus long** : Environ un mois pour établir la connexion avec un fournisseur de services Direct Connect.
- **Choix entre VPN de site à site et connexion directe**
    - **Critères de sélection** :
        - **Confidentialité** : Si la sécurité des données est cruciale, la connexion directe est préférable en raison de son réseau privé.
        - **Temps de déploiement** : Pour une mise en place rapide, le VPN de site à site est plus adapté.
        - **Coût** : Si le budget le permet, la connexion directe offre des performances supérieures et une meilleure fiabilité.
- **Configuration dans AWS**
    - **VPN de site à site** :
        - Nécessite une **CGW** (Customer Gateway) côté site et une **VGW** (Virtual Private Gateway) dans AWS.
        - Ces éléments sont configurés pour créer un tunnel VPN sécurisé via Internet public.
    - **Connexion directe (Direct Connect)** :
        - Implique l'établissement d'un circuit physique entre le centre de données et AWS via un fournisseur de connexion directe.

        - Offre des options de bande passante variées et des SLA pour la disponibilité et la performance.

AWS Client VPN

- Le AWS Client VPN est un service permettant aux utilisateurs individuels de se connecter de manière sécurisée et privée à un VPC AWS à partir de leurs périphériques locaux, tels que des ordinateurs portables ou des postes de travail.
- **Fonctionnement**
    - **Objectif** : Établir une connexion sécurisée entre un périphérique client et un VPC AWS, permettant un accès privé aux ressources dans le VPC.
    - **Protocole** : Utilise OpenVPN pour la configuration et l'établissement de la connexion VPN.
    - **Avantages** :
        - **Accès privé aux ressources** : Permet d'accéder aux instances EC2 et autres ressources dans un VPC à l'aide d'adresses IP privées.
        - **Simplicité d'utilisation** : Une fois configuré, l'accès aux ressources dans le VPC est transparent comme si l'utilisateur était localement connecté au réseau.
    - **Déploiement** :
        - **Installation du client VPN** : Le client VPN AWS doit être installé sur l'ordinateur ou le périphérique client.
        - **Configuration** : Configuration des paramètres de connexion VPN, y compris l'identification du VPC cible, les options de sécurité et les certificats nécessaires.
        - **Établissement de la connexion** : À travers Internet public, le client VPN établit une connexion sécurisée avec le VPC AWS, permettant à l'utilisateur d'accéder aux ressources privées dans le VPC.
    - **Intégration avec site à site** :
        - Si le VPC AWS a établi une connexion VPN site à site avec un centre de données sur site, l'utilisateur du AWS Client VPN peut également accéder de manière privée aux serveurs dans le centre de données via le même tunnel VPN.
    - **Avantages et cas d'utilisation**

- **Accessibilité** : Facilite l'accès aux ressources AWS depuis n'importe où, tout en garantissant la sécurité des communications.
- **Simplicité** : Offre une interface utilisateur conviviale pour configurer et gérer les connexions VPN.
- **Compatibilité** : Prise en charge des protocoles VPN standard tels que OpenVPN, assurant une intégration facile avec divers environnements clients.

- **Sécurité et gestion**
  - **Sécurité des données** : Toutes les communications sont cryptées, assurant la confidentialité des données transitant via le VPN.
  - **Gestion des accès** : Utilisation de groupes de sécurité pour contrôler précisément quelles ressources sont accessibles via le VPN Client AWS.

Suivez-nous

- **Site web** : https://lecloudfacile.com
- **Youtube** : https://www.youtube.com/@lecloudfacile
- **Linkedin** : https://www.linkedin.com/company/lecloudfacile/
- **Udemy** : https://www.udemy.com/course/nouveau-aws-cloud-practitioner-clf-c02/?referralCode=8CE99E6C2100F1998BDF
- **Communauté WhatsApp** : https://chat.whatsapp.com/HIeIlLVOJ9xCJKX8VhbLSr