Créer un VPC (Virtual Private Cloud), des sous-réseaux (subnets), une gateway internet et une table de routage est essentiel pour la gestion et la sécurité des ressources dans AWS. Voici à quoi chacun de ces composants sert :

VPC (Virtual Private Cloud)

Un VPC est un réseau virtuel dédié à votre compte AWS. Il vous permet de lancer des ressources AWS, comme des instances EC2, dans un réseau virtuel que vous définissez. La création d'un VPC vous offre plusieurs avantages :

Isolation : Les ressources au sein d'un VPC sont isolées des autres réseaux AWS par défaut.

Contrôle : Vous avez un contrôle total sur la configuration 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 gateways.

Subnet

Un sous-réseau est une subdivision logique du VPC. Il vous permet de segmenter votre réseau en différentes zones de disponibilité pour une meilleure gestion des ressources et une haute disponibilité. Les sous-réseaux peuvent être de deux types :

Public Subnet : Un sous-réseau qui a une route directe vers Internet via une Internet Gateway (IGW).

Private Subnet : Un sous-réseau qui n'a pas de route directe vers Internet. Les instances dans ce sous-réseau peuvent accéder à Internet via un NAT Gateway ou NAT Instance.

Internet Gateway (IGW)

Une Internet Gateway est un composant qui permet aux instances dans un VPC de communiquer avec Internet. Lorsqu'une Internet Gateway est attachée à un VPC, elle fournit une route pour le trafic sortant et entrant vers et depuis Internet.

Accès Internet : Permet aux instances dans les sous-réseaux publics de se connecter à Internet.

Entrée et Sortie : Gère le trafic Internet entrant et sortant pour les instances.

Route Table

Une table de routage contient un ensemble de règles, appelées routes, qui sont utilisées pour déterminer où envoyer le trafic réseau. Chaque sous-réseau dans un VPC doit être associé à une table de routage. La table de routage détermine comment le trafic est dirigé :

Routes Locales : Par défaut, chaque table de routage contient une route locale pour permettre la communication au sein du VPC.

Routes Externes : Vous pouvez ajouter des routes vers des destinations externes, comme une Internet Gateway, pour permettre aux instances de communiquer avec des réseaux externes.

Pourquoi ces composants sont nécessaires ?

Isolation et Sécurité : En segmentant votre réseau avec des VPCs et des sous-réseaux, vous pouvez appliquer des politiques de sécurité granulaires, comme les ACLs (Access Control Lists) et les groupes de sécurité.

Haute Disponibilité : En répartissant vos ressources sur plusieurs sous-réseaux et zones de disponibilité, vous pouvez garantir une haute disponibilité et tolérance aux pannes.

Gestion du Trafic : Les tables de routage vous permettent de contrôler comment le trafic est dirigé, assurant que les ressources peuvent communiquer entre elles et avec Internet de manière contrôlée et sécurisée.

Accès Internet : Une Internet Gateway est nécessaire pour que vos instances puissent accéder à Internet, ce qui est essentiel pour de nombreuses applications et services.

Kube : liveness, readiness, rollback, nœud, ssl,