Les Services Cloud Computing

Axel TIFRANI

Janvier 2023


axeltifrani@logbrain.fr


+336 25 75 14 04


https://www.linkedin.com/in/axel-tifrani-b5790243/

Sommaire

Présentation

- A propos du formateur:
  - Diplômé de la MIAGE informatique Paris Dauphine
  - Architecte Big Data et Cloud en freelance
  - +13 ans d'expérience dans le Big Data et 6 ans dans le Cloud
  - Formateur Big Data, Cloud et DevOps (ESME, ECE, ESG, ESCP)
- A propos du Cours:

Durant les séances vous développerez des connaissances en matière de cloud AWS en étudiants les concepts du cloud AWS: Les services Sécurité, Réseau, calcul, stockage et base de données.

Les modules incluent une partie théorique et une partie pratique qui vous permettent de mieux comprendre les services AWS.

Les évaluations sont en deux parties: Une partie quiz pour examiner les concepts théoriques et une partie projet pour examnier les concepts pratiques.

- A propos de vous
  - Connaissance du cloud
  - Attentes du cours

- Introduction au Cloud Computing

- Qu’est-ce que le Cloud Computing ?
- Les différents types de services de cloud computing
- Responsabilité partagée et sécurité
- Les différents types de déploiement du cloud computing
- Les plateformes de cloud computing

Qu’est-ce que le Cloud Computing ?

- Presque toute l'informatique moderne s'articule autour d'un modèle client-serveur classique.

Qu’est-ce que le Cloud Computing ?

- Récapitulons ce qu'est un modèle client-serveur.

Un **client** peut être un navigateur web ou une application de bureau avec laquelle une personne interagit pour faire des requêtes aux serveurs informatiques. Un **serveur** peut être des services tels qu'Amazon Elastic Cloud Compute (Amazon EC2), un type de serveur virtuel.

Par exemple, supposons qu'un client fasse une requête pour un article, le score d'un jeu en ligne ou une vidéo amusante. Le serveur évalue les détails de cette requête et la remplit en renvoyant les informations au client.

Qu’est-ce que le Cloud Computing ?

- Le **Cloud** signifie « **nuage** » et **Computing** « **informatique** », le **Cloud Computing** est donc l’**informatique en nuage** pour une traduction littérale anglais français. Plusieurs définitions du Cloud Computing existent nous retiendrons cependant celle-ci, qui définit le Cloud Computing comme étant l'accès via un réseau **Internet**, à la **demande** et en **libre-service**, à des **ressources informatiques partagées configurables**. Par exemple réseaux, serveurs, stockage, applications et services qui peuvent être rapidement mises à disposition des utilisateurs sans **engagements** et **facturés à l'usage**.

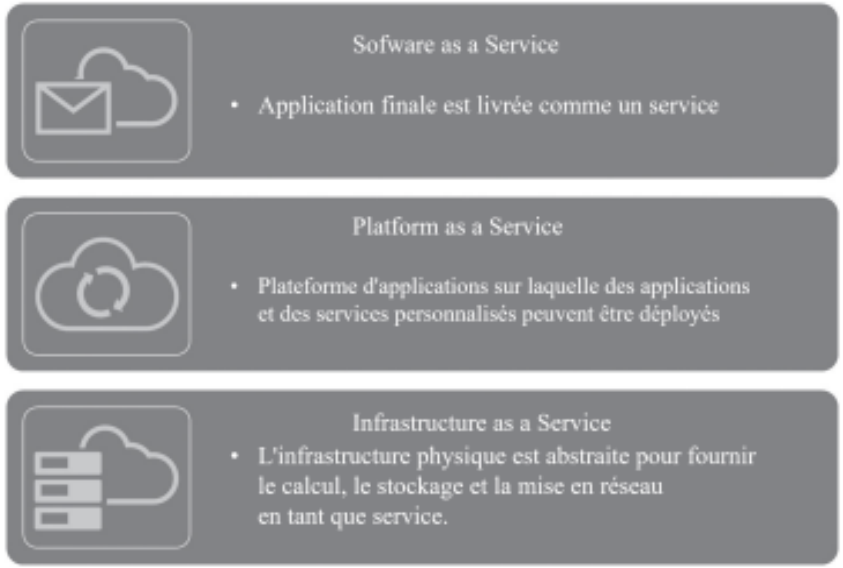
Les différents type de services de cloud computing

- Le cloud computing offre de multiple de possibilités d'utilisation. Trois grands modèles d’usage du Cloud se dégagent actuellement, tous présentent des caractéristiques différentes et n’ont pas le même niveau de maturité :

- SaaS :Software as a Services

- PaaS :Plateforme as a Services

- IaaS : Infrastructure as a Services



Les différents type de services de cloud computing

SaaS: Software as a Services (logiciel en tant que services):

Dans ce type de service, des **applications** sont mises à la disposition des consommateurs. Les applications peuvent être manipulées à l'aide d'un navigateur web, et le consommateur n'a pas à se soucier d'effectuer des **mises à jour**, d'ajouter des **patches de sécurité** et **d'assurer la disponibilité** du service. **Gmail** est un exemple de tel service. Il offre aux consommateurs un service de courrier électronique et le consommateur n'a pas à se soucier de la manière dont le service est fourni.

D'autres exemples de services mis à disposition en **SaaS** sont:

- **Storage as a services**: Correspond au service de stockage de données. Exemple: Amazon S3, DropBox, Google Drive, …

- **Desktop as a Service** : le Desktop as a Service (DaaS ; aussi appelé en français « bureau virtuel » ou « bureau virtuel hébergé ») est l'externalisation d'une Virtual Desktop Infrastructure VDI auprès d'un fournisseur de services.

Les différents type de services de cloud computing

PaaS: Plateforme as a Services (Plateforme en tant que services)

Dans ce type de service, situé juste au-dessous du précédent (Saas), le système d'exploitation et les outils d'infrastructure sont sous la responsabilité du fournisseur cloud. Le consommateur a le contrôle des applications et peut ajouter ses propres outils.

La situation est analogue à celle de l'hébergement web où le consommateur loue l'exploitation de serveurs sur lesquels les outils nécessaires sont préalablement placés et contrôlés par le fournisseur. La différence étant que les systèmes sont mutualisés et offrent une grande élasticité - capacité de s'adapter automatiquement à la demande, alors que dans une offre classique d'hébergement web l'adaptation fait suite à une demande formelle du consommateur

Le Paas offre une grande flexibilité:

- Développement rapide de prototype
- Service ou application utilisable via le Web
- Montée en charge garantie

Les différents type de services de cloud computing

IaaS: Infrastructure as a Services (L'infrastructure en tant que service)

c'est le service de plus bas niveau. Il consiste à offrir un accès à un parc informatique virtualisé. Des machines virtuelles sur lesquelles le consommateur peut installer un système d'exploitation et des applications. Le consommateur est ainsi dispensé de l'achat de matériel informatique. Ce service s'apparente aux services d'hébergement classiques des centres de traitement de données, et la tendance est en faveur de services de plus haut niveau, qui font d’avantage abstraction de détails techniques

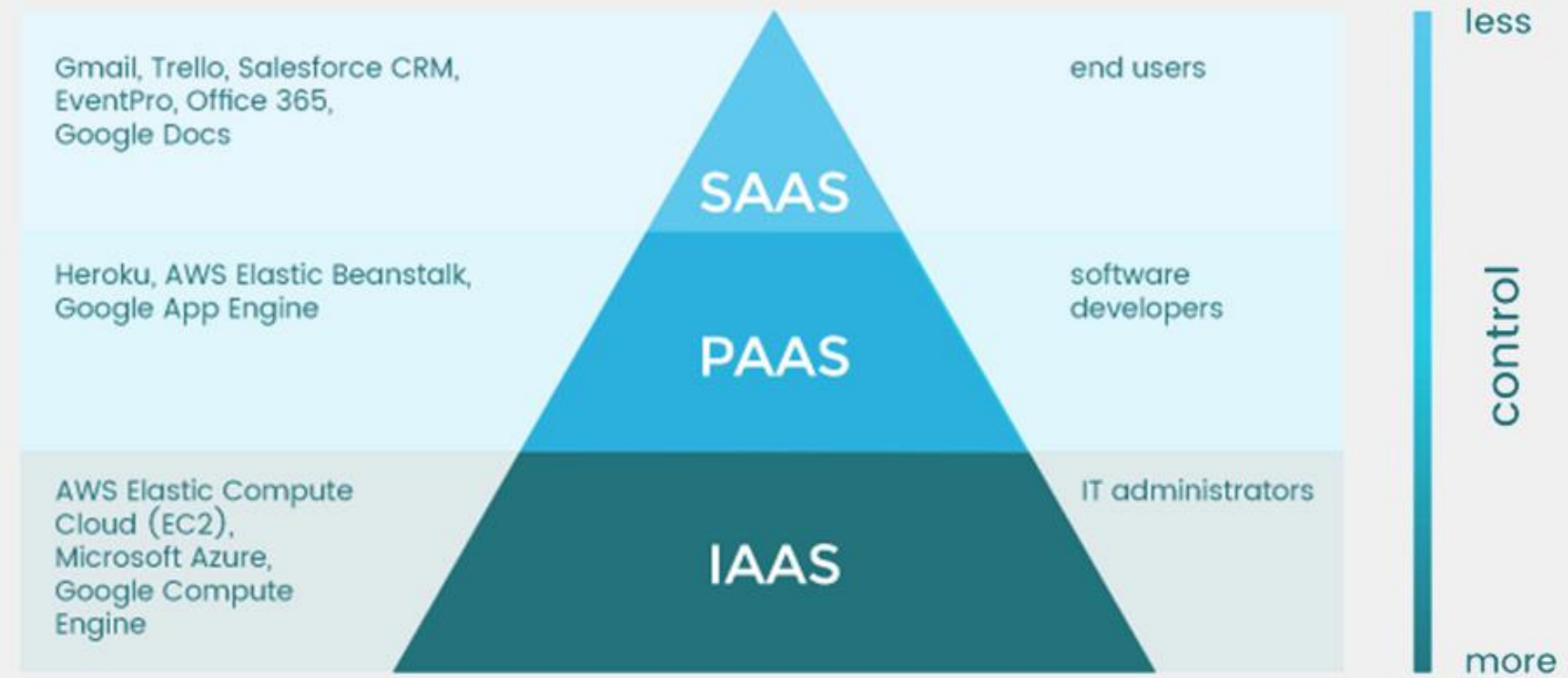
Les différents type de services de cloud computing

Deux nouveaux types de modéle de service s'ajoutent:

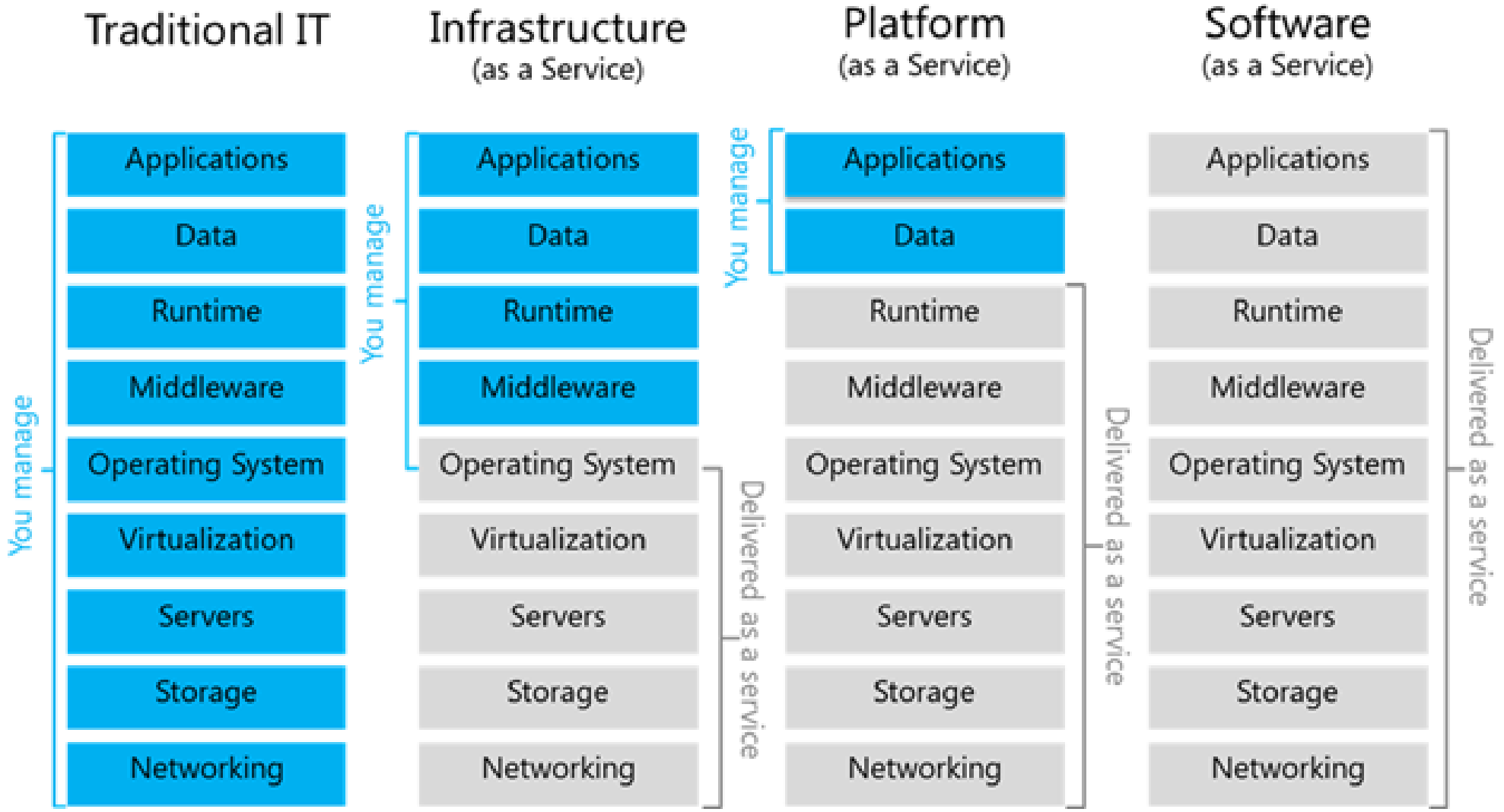
Le CaaS: Containers-as-a-Service (Le conteneur en tant que service), est un modèle qui permet aux utilisateurs de déployer et gérer des applications conteneurisées, dans le cloud ou dans des datacenters sur site. Parmi les services cloud, le **CaaS** est considéré comme une sous-catégorie de **l'IaaS** (Infrastructure-as-a-Service) et il se place entre **l'IaaS** et le **PaaS** (Platform-as-a-Service).

Le FaaS: Function-as-a-Service (La fonction en tant que service) est un type de service Cloud permettant de déployer une fonction en serverless (Abstraction complète des serveurs). **Le FaaS** est une manière de mettre en œuvre des applications sans se soucier de la partie infrastructure, où les développeurs écrivent une logique métier qui est ensuite exécutée dans des conteneurs entièrement gérés par une plateforme. Le **Faas** est modèle porche du **Paas**. La frontière qui sépare les deux modéles s'estompe avec le temps, puisque les solutions modernes de **PaaS** fournissent des capacités **sans serveur**.

Responsabilité partagée et sécurité



Responsabilité partagée et sécurité



Les différents types de déploiement du cloud computing

À mesure que le cloud computing a gagné en popularité, plusieurs modèles et stratégies de déploiement différents sont apparus pour répondre aux besoins spécifiques des différents utilisateurs.

Il existe de nombreux modèles de déploiement de Cloud computing parmi lesquels choisir. Votre infrastructure Cloud et le placement de chaque charge de travail dépendent de vos besoins d'utilisation. Il est essentiel de prendre en considération comment les coûts, la confidentialité et la disponibilité affecteront le placement de chaque application ou service utilisé par votre entreprise.

Modèles de déploiement de cloud computing:

- Le cloud Privé
- Le cloud Public
- Le cloud Hybride

Les différents types de déploiement du cloud computing

- **Le cloud Privé** (ou Interne):

Le Cloud Privé est un mode de consommation de informatique (**IaaS, PaaS, SaaS,…**) s'appuyant sur des ressources (**serveur, stockage, réseau, licences logicielles…**) mises à disposition **exclusive d'une entreprise**. Les ressources peuvent être géographiquement situées dans le **périmètre de l'entreprise** (on parlera d'un **Cloud privé interne**) ou chez un **intégrateur/service provider** (on parlera d'un **Cloud privé managé ou hosté**).

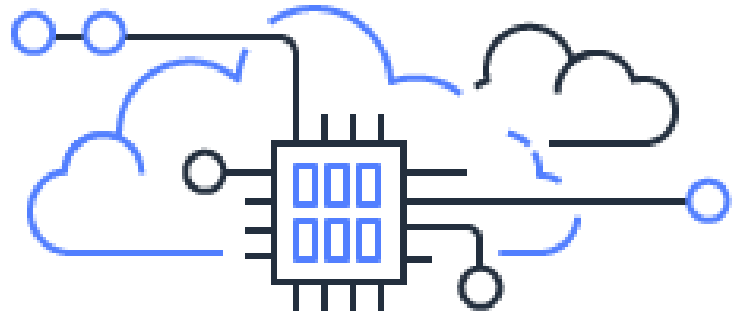
L'exploitation du Cloud privé peut être réalisée uniquement par les **équipes informatiques du client** (Cloud privé interne), ou par un **prestataire externe** (Cloud privé interne, Cloud privé hosté). Les services disponibles le sont via un catalogue de services exposés dans un portail, leur mise en service est automatisée, et peut faire l'objet d'une facturation liée à la consommation

Les différents types de déploiement du cloud computing

- **Le cloud Public**:

Le Cloud public est une **structure souple et ouverte**, géré par un fournisseur tiers.Plusieurs utilisateurs (individuels ou entreprises) peuvent y accéder **via Internet**. Avec le Cloud public, de multiples entités se partagent les mêmes ressources informatiques mises à disposition par le fournisseur.

Disponibles pour quiconque souhaite les utiliser ou les acheter. Ces services peuvent être gratuits ou vendus à la demande, de telle sorte que les clients ne doivent payer que pour les cycles de processeur, le stockage ou la bande passante qu'ils consomment.



Les différents types de déploiement du cloud computing

- **Le cloud Hybride:**

Un modèle de **cloud hybride** étend un **cloud privé** à un **cloud public** lorsque la demande de **ressources augmente**. Ce paradigme permet aux organisations de maintenir la **conformité** tout en profitant des **ressources** publiques. Les organisations qui utilisent un cloud hybride peuvent maximiser leurs ressources internes sans risquer une surcharge si leurs besoins augmentent de manière inattendue.

Une entreprise qui utilise un **Cloud hybride** peut par exemple avoir recours au **Cloud public ponctuellement**, lors de **pics d'activité** et le reste du temps se contenter des ressources à disposition en interne.

Les différents types de déploiement du cloud computing

- **Choisir un modèle de déploiement de Cloud:**

Voici quelques recommandations générales pour commencer.

Cloud privé – Un Cloud privé est idéal dans les cas d'utilisation où vous devez :

- Protéger des informations sensibles, y compris la propriété intellectuelle
- Respecter les exigences de souveraineté ou de conformité des données

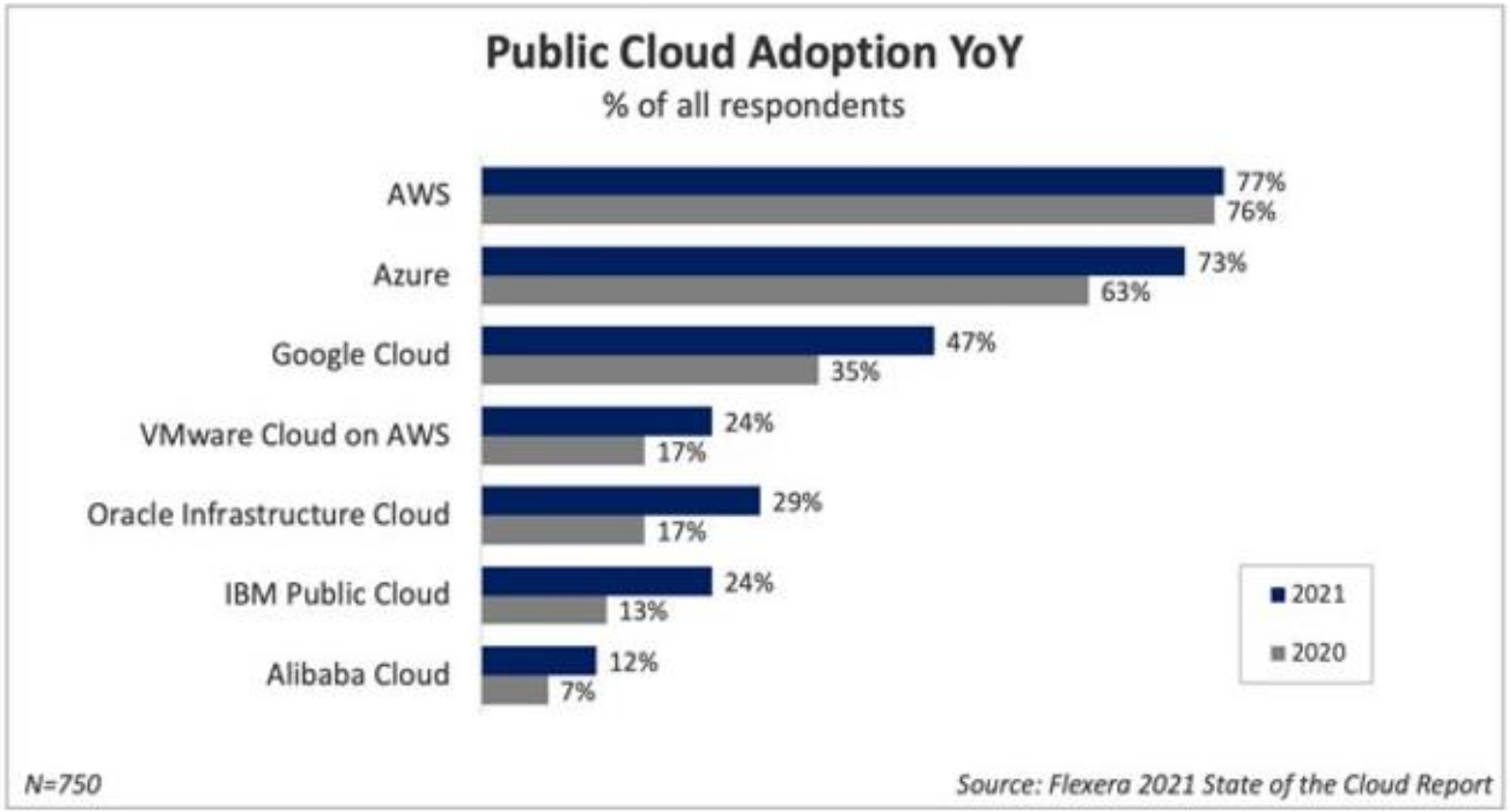
Cloud public – Le Cloud public est idéal dans les cas d'utilisation où vous devez :

- Faire rapidement évoluer le système et accélérer la mise sur le marché
- Traiter des charges de travail à court terme
- Gérer les coûts initiaux
- Soulager la pression sur les ressources informatiques

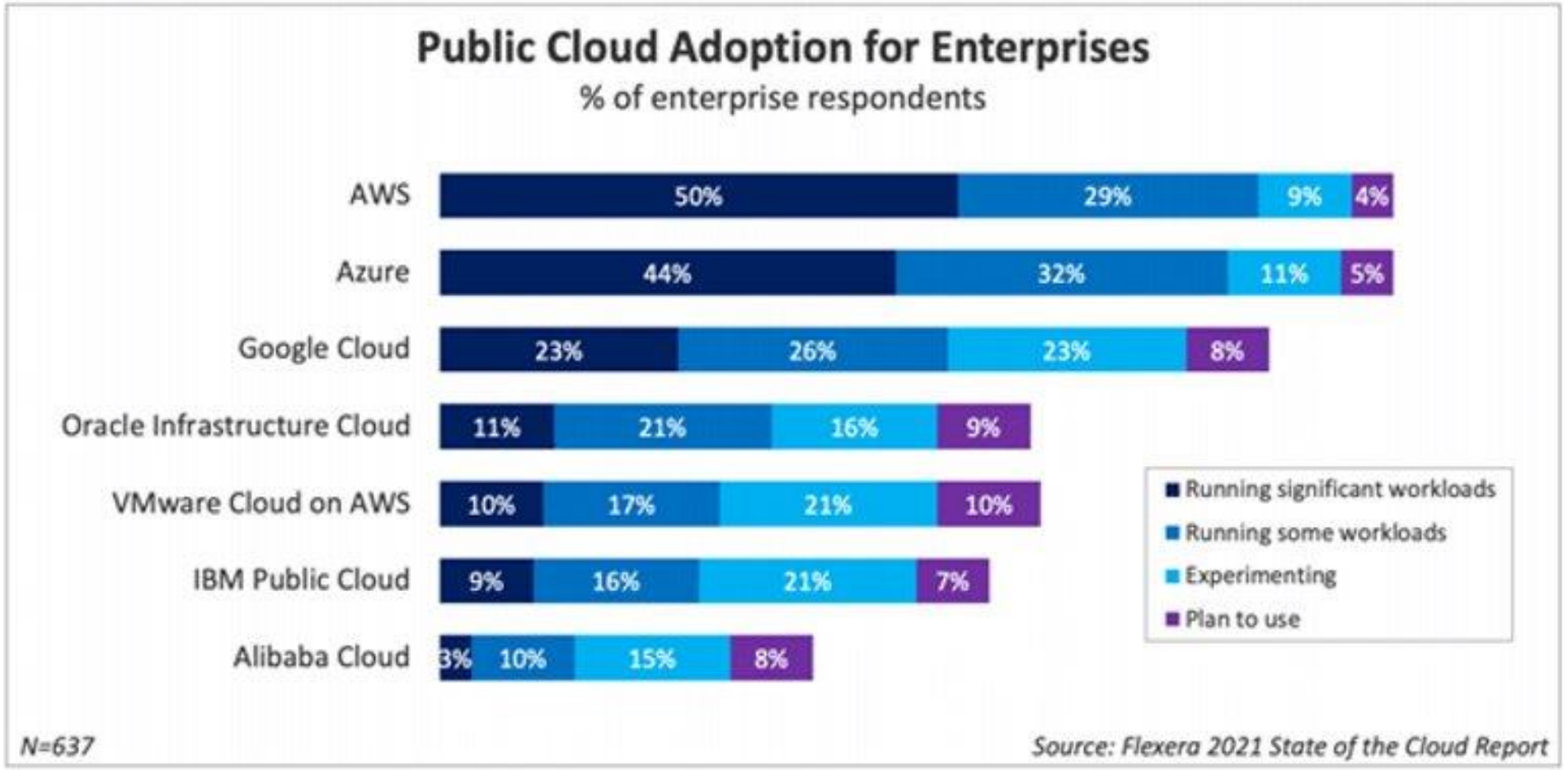
Souvenez-vous que pour répondre aux exigences de chaque application et optimiser les charges de travail, la plupart des organisations devront disposer à la fois de Clouds public et privé.

Les plateformes de cloud computing

- Il existe de nombreux fournisseurs d'hébergement cloud; cependant, très peu proposent une gamme de produits à héberger, allant d'un simple site Web statique à des applications d'apprentissage automatique complexes.



Les plateformes de cloud computing

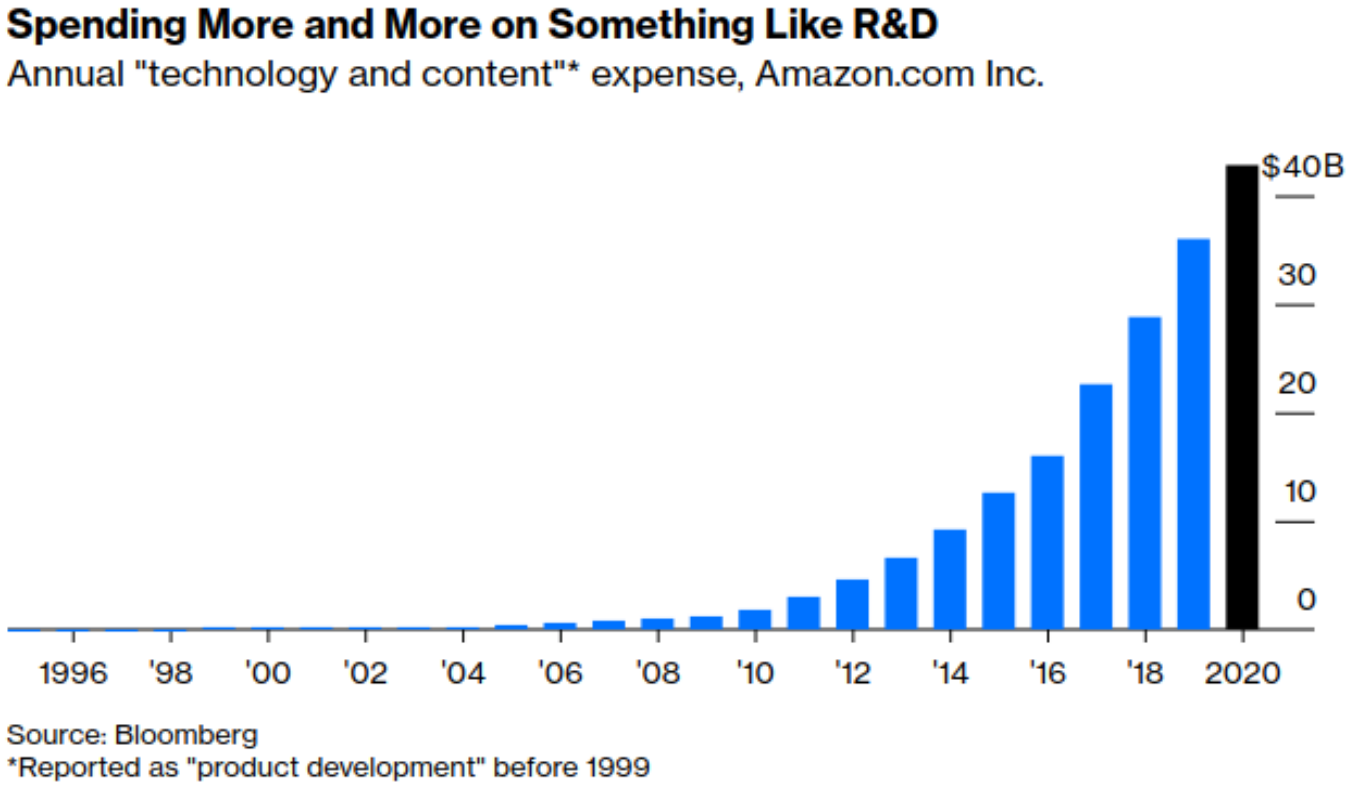


Les plateformes de cloud computing

- Si les qualificatifs de “**flexibilité**”, “**portabilité**”, “**modularité**” et “**élasticité**” lui sont communément associés, le cloud suscite également des craintes : 75% des entreprises interrogées pensent ainsi que le ***Cloud Act*** et le ***Patriot Act*** en vigueur aux ***États-Unis*** font courir un risque à la sécurité des données.
- Pour mémoire, le Cloud Act est une loi fédérale américaine promulguée en mars 2018, autorisant “les instances de justices judiciaires ou administratives (fédérales ou locales) à obtenir des opérateurs télécoms et des fournisseurs de services de Cloud Computing établis sur le territoire américain, des informations stockées sur leurs serveurs qu’ils soient basés aux États-Unis ou dans des pays étrangers”
- Malgré les craintes et les interrogations, peu d'entreprises européénes sont utilisatrices de solutions des fournisseurs de Cloud européens (***Orange, OVHcloud, Scaleway d’Illiad, Atos, Docaposte, Outscale***). À eux cinq, ***Amazon Web Services, Microsoft Azure, Alibaba Cloud, Google Cloud et IBM Cloud***, dominent nettement le marché : ils représentaient **80% du marché mondial.**

Les plateformes de cloud computing

Amazon est le champion du monde dans investissemnt en recherche et devellopement.
Le budget R&D de Amazoin en 2020 est égale au chiffre d'affaires d'une entreprise comme Oragne ou Renault.



Introduction projet Omega

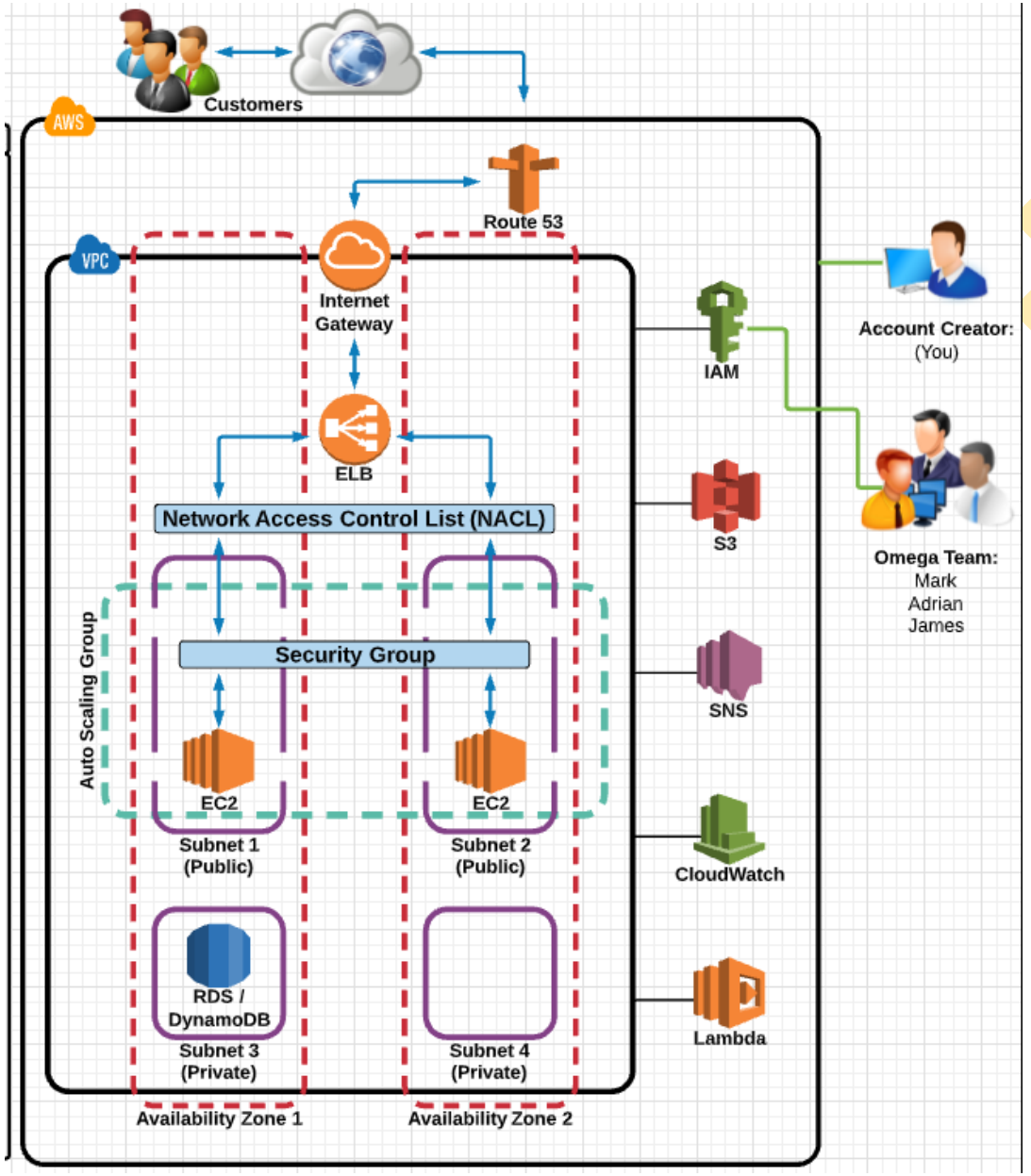
- Infrastructure AWS requise:
  1. Un Compte AWS
  2. Des comptes utilisateurs pour l'équipe de développement avec des accès aux services AWS
  3. Un routage approprié du trafic vers et depuis notre cloud virtuel privé VPC AWS
  4. Un emplacement pour le stockage en masse des fichiers
  5. Des servers pour héberger le projet
  6. Une base de données pour stocker et cataloguer les données
  7. Un service de notification (Mail ou sms) pour l'équipe du projet, basé sur les événements d'infrastructure
  8. Un service pour monitorer le projet et l'infrastructure du projet
  9. Automatiser le processus de distribution du trafic entrant entre les ressources AWS du projet Omega
  10. Automatiser le processus de scaling up ou scaling down des ressources AWS du projet Omega
  11. Mettre en place et configurer un domaine web qui pointe vers l'infrastructure de projet Omega
  12. Tester la possibilité d'utiliser des ressources de type serveless pour le projet Omega

Introduction projet Omega

Ce diagramme représente une vue de l'infrastructure et des services AWS nécessaire pour le projet Omega.

Nous allons dans les prochains chapitres découvrir chacun des services avec et procéder à sa mise en place pour construire l'infrastructure qui hébergera le projet Oméga.

Let's get Started



- Amazon services Gestion des Identité (IAM: Identiy and Acces Management)

- Introdution à IAM
- IAM Users et Policies
- IAM Groups et Policies
- IAM Roles

Amazon services Gestion des Identité

- Introdution à IAM:

AWS Identity and Access Management (IAM) est un **service web** qui vous permet de **contrôler l'accès aux ressources AWS**. Vous pouvez utiliser IAM pour **contrôler les personnes** qui **s'authentifient** (connectées) et sont **autorisées** (disposent d'autorisation) à utiliser les **ressources**.

Lorsque vous créez pour la première fois un Compte AWS , vous commencez avec une **identité de connexion unique** qui bénéficie d'un **accès complet** à tous les services et ressources AWS du compte. Cette identité est appelée la ***utilisateur racine (root)*** du Compte AWS et elle est accessible après connexion à l'aide de l'adresse e-mail et du mot de passe utilisés pour la création du compte. Il est **vivement recommandé de ne pas utiliser l'utilisateur racine** pour vos tâches quotidiennes, y compris pour les tâches administratives.

Au lieu de cela, respectez la bonne pratique qui consiste à avoir recours à l'utilisateur racine uniquement pour créer le premier utilisateurIAM. Ensuite, mettez en sécurité les informations d'identification de l'utilisateur racine et utilisez-les pour effectuer uniquement certaines tâches de gestion des comptes et des services.

Amazon services Gestion des Identité

IAM est conçu pour gérer:

- **User** (Utilisateur): correspond à un utilisateur physique (humain)
- **group** (groupe) : ensemble d'utilisateur appartenant à la même entité administrative (HR, technique, ...) et pouvant avoir les mêmes permissions
- **Roles** (rôles) : Ensemble d'action que une ressource peut réaliser (écrire dans S3,....)
- **Policy** (stratégies) : document définissant une ou plusieurs permissions

Introduction à Amazon Web Services

- Historique de Amazon Web Services
- Infrastructure Globale de Amazon Web Services
- Ouvrir un compte AWS gratuit

Historique de Amazon Web Services

Entreprise Américain de commerce en ligne qui a lancé sa filiale cloud AWS au début des années 2000.

- 2006: lancement du service de stockage S3 et du service de calcul EC2
- 2009: Lancement du service BigData avec EMR
- 2012: Lancement du service data warehouse Redshift

L'entreprise est depuis devenue une référence mondiale du marché des services cloud d'infrastructure. Et un moteur de croissance pour Amazon.

Aujourd'hui, Amazon Web Services est une plate-forme d'infrastructure à haute fiabilité, évolutive et à bas coût dans le cloud qui alimente des centaines de milliers d'entreprises dans **245 pays**. Avec des centres de données situés aux États-Unis, en Europe, au Brésil, à Singapour, au Japon et en Australie.

Infrastructure Globale de Amazon Web Services

Déjà 25 régions lancées

Chacune avec plusieurs zones de disponibilité (AZ)

81 zones de disponibilité

11 Zones locales

17 zones Wavelength

Pour des applications à très faible latence

8 régions annoncées

6 Local Zones annoncées

2 fois plus de régions

avec plusieurs zones de disponibilité que le deuxième plus grand fournisseur cloud

245 pays et territoires desservis

108 emplacements Direct Connect

Plus de 275 points de présence

Plus de 265 emplacements périphériques et 13 caches périphériques régionaux

Infrastructure Globale de Amazon Web Services

Infrastructure Globale de Amazon Web Services

- **Les régions:**

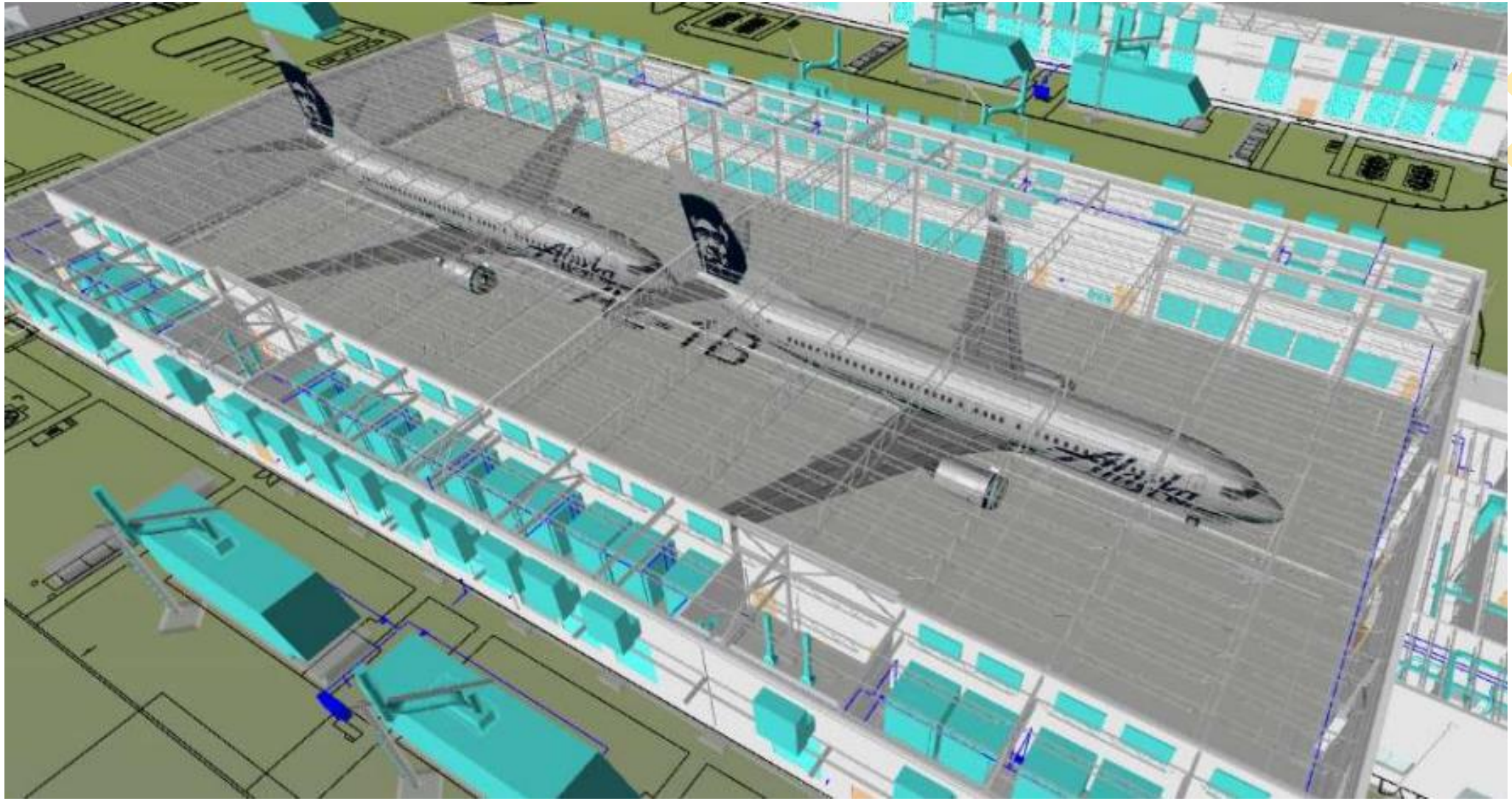
AWS fonctionne par région. Il s'agit d'un emplacement physique dans le monde où sont regroupés des centres de données. Nous appelons chaque groupe de centres de données logiques une « Zone de disponibilité ». Chaque région AWS se compose de zones de disponibilité multiples, isolées et physiquement séparées au sein d'une zone géographique.

- **Les zones de disponibilités:**

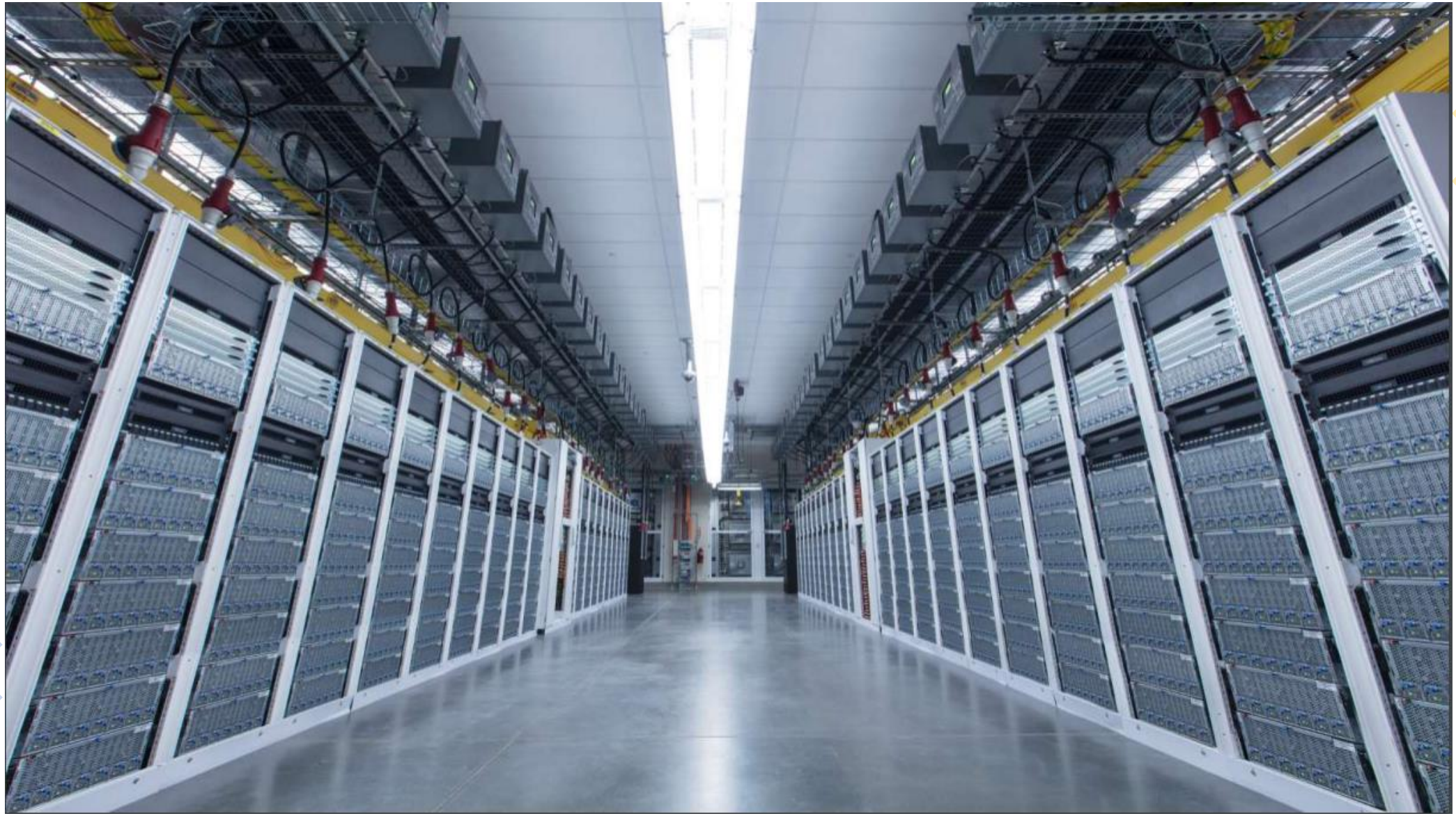
Une zone de disponibilité comprend un ou plusieurs centres de données discrets dotés d'une alimentation redondante, d'une mise en réseau et d'une connectivité au sein d'une région AWS. Les zones de disponibilité donnent aux clients la possibilité d'utiliser des applications de production et des bases de données plus disponibles, plus tolérantes aux pannes et plus évolutives que ce qui serait possible à partir d'un centre de données unique.

Infrastructure Globale de Amazon Web Services

Infrastructure Globale de Amazon Web Services



Infrastructure Globale de Amazon Web Services



Ouvrir un compte AWS gratuit

1. Accédez à la page d'accueil d'Amazon Web Services (AWS).
2. Sélectionnez Créer un compte gratuit.
   Remarque : si vous vous êtes récemment connecté à AWS, sélectionnez Sign in to the Console (Se connecter à la console). Si l'option Create a new AWS account (Créer un nouveau compte AWS) n'apparaît pas, sélectionnez d'abord l'option Sign in to a different account (Se connecter à un autre compte), puis Create a new AWS account (Créer un compte AWS).
3. Saisissez vos informations de compte, puis sélectionnez Continue (Continuer). Assurez-vous de saisir vos informations de compte correctement, en particulier votre adresse e-mail. Si l'adresse e-mail que vous saisissez est incorrecte, vous ne pourrez pas accéder à votre compte.
4. Sélectionnez Personnel ou Professionnel.
   Remarque : les comptes personnels et professionnels ont les mêmes fonctions et fonctionnalités.
5. Saisissez vos informations personnelles ou celles de votre entreprise.
6. Lisez le contrat client AWS et acceptez-en les conditions.
7. Choisissez Create Account and Continue (Créer un compte et continuer)

Ouvrir un compte AWS gratuit

Ajout d'un mode de paiement

Sur la page Informations de paiement, saisissez les informations relatives à votre mode de paiement, puis sélectionnez Vérifier et ajouter. Vous ne pouvez pas continuer l'inscription tant que vous n'avez pas ajouté un mode de paiement valide.

Vérification de votre numéro de téléphone

1. Sélectionnez le code de votre pays ou de votre région dans la liste.
2. Saisissez un numéro de téléphone où vous pouvez être joint dans les minutes qui suivent.
3. Saisissez le code CAPTCHA, puis soumettez les informations.
4. Un système automatisé vous contactera dans quelques instants ou vous receverez un sms avec un code.
5. Saisissez le code que vous avez reçu, puis sélectionnez Continuer.
6. Selectionnez support plan : Basic for no free/Free tier use
7. Connectez vous à la console AWS avec vos identifiants

Ouvrir un compte AWS gratuit

- Si vous possédez déjà un compte AWS, mais que vous ne savez pas si vous pouvez encore bénéficier de l'offre gratuite AWS, ouvrez la console de Gestion de la facturation et des coûts. Si votre compte est admissible à l'offre gratuite AWS, un message indiquant votre admissibilité s'affiche dans la section **Alerts & Notifications** (Alertes et notifications).
- Vous pouvez également choisir **Bills** (Factures) dans le panneau de navigation de la console pour consulter quand votre compte AWS a été créé. La zone de liste déroulante **Date** répertorie une facture pour chaque mois depuis l'ouverture de votre compte, même si vous n'avez eu aucun frais.
- Peu avant le terme de votre admissibilité à l'offre gratuite AWS, AWS envoie une notification à l'adresse e-mail que vous avez utilisée au moment de votre inscription à AWS. Si vous décidez de continuer à utiliser AWS après la fin de l'offre gratuite AWS, veillez à supprimer les ressources dont vous n'avez plus besoin afin d'éviter que leur utilisation vous soit facturée. Si vous décidez de ne pas continuer à utiliser AWS, vous pouvez close your account.

Ouvrir un compte AWS gratuit

- Liste de services AWS gratuits : https://aws.amazon.com/fr/free/

- Navigations dans la console AWS.
  - Les services, Alertes, mon compte, Régions
  - Barre de recherche et push pin, Favorites, cloudshell

- Création des Billing Alarms (Free Tier, Billing, CloudWatch)
  - Billing -> preferences, cochez la case recevoir des alertes de facturation (ajouter une adresse mail pour recevoir les alertes)
  - Cloudwatch -> alertes -> facturation (créez une alarme lorsque la facture dépasse 1USD)

- Documentation et support aws (change support plan if needed)

- Tarification https://aws.amazon.com/fr/ec2/pricing/

Introduction projet Omega

- **Présentation projet Omega**

Le projet Omega est un projet de développement classé qui doit être construit et exécuté à l'aide du service Web amazon. Pour le moment, nous ne connaissons que les besoins en infrastructure du projet Omega. Aucune information spécifique sur ce qu'il est ou ce qu'il fait n'a été divulguée.

- **Notre mission:**

En tant qu'architecte AWS, nous avons été chargés de créer l'infrastructure de base du projet Omega afin que l'équipe de développement puisse commencer à travailler sur le cœur du projet.

Malgré que nous ayons reçu très peu d'informations sur le projet oméga; cependant, nous avons pu lister les besoins nécessaires en collaboration avec l'équipe de développement.

Amazon services Gestion des Identité

Fonctionnalités d'IAM: IAM vous offre les fonctions suivantes

- Accès partagé à votre compte AWS
- Autorisations granulaires
- Accès sécurisé aux ressources AWS pour les applications s’exécutant
- sur Amazon EC2
- Authentification multi-facteurs (MFA)
- Fédération des identités
- Informations d’identité par sécurité
- Intégré à différents services AWS
- Cohérence à terme
- Gratuité

Amazon services Gestion des Identité

IAM Lab:

- Supprimer les acces pour le user **root:**
  - Activer le MFA pour le user root
  - Créer un nouveau IAM user
  - Utiliser les groups pour assigner les permissions
  - Appliquer un IAM password Policy

Amazon services Gestion des Identité

C'est quoi le MFA?

Pour plus de **sécurité**, nous vous recommandons de configurer l'**authentification multi-facteur**s (Multi-Factor Authentication, MFA) pour mieux protéger vos **ressources AWS.** Vous pouvez activer l'authentification MFA pour **les utilisateurs IAM** ou **l' Utilisateur racine** Compte AWS.

L'authentification MFA exige que les utilisateurs fournissent une **authentification** unique à partir d'un **mécanisme MFA** pris en charge par AWS.

Comment obtenir un code MFA?

- **Périphériques MFA virtuels** Une application logicielle qui s'exécute sur un téléphone ou un autre appareil et qui émule un périphérique physique.
- **Clé de sécurité U2F**. Un périphérique que vous branchez dans un port USB sur votre ordinateur.
- **Périphérique MFA matériel**. Périphérique matériel qui génère un code numérique à six chiffres basés sur un algorithme de mot de passe unique synchronisé
- **MFA basé sur les SMS**. Type de MFA dans lequel les paramètres de l'utilisateur IAM incluent le numéro de téléphone de l'appareil mobile compatible SMS de l'utilisateur.

Amazon services Gestion des Identité

Créer un utilisateur IAM:

- À titre de bonne pratique, il est recommandé de ne jamais utiliser l'utilisateur root pour les tâches quotidienne.
- Si vous avez besoin d'un access full admin à votre compte aws. Il vous suffit de créer un utilisateur IAM et lui rattacher la policy **AdminstratorAcess**
- Utilisez l'utilisateur IAM actions quotidienne.
- Pour certaines tâches de gestion des comptes et des services comme Clôturez votre compte AWS, vous devez vous connecter à l'aide des informations d'identification utilisateur racine. Pour afficher les tâches qui nécessitent que vous vous connectiez en tant qu'utilisateur racine, consultez Tâches AWS qui nécessitent un utilisateur racine.

Amazon services Gestion des Identité

Gestion des groupes d'utilisateurs IAM:

Un **groupe d'utilisateurs IAM** est un **ensemble d'utilisateurs IAM**. Les groupes d'utilisateurs vous permettent de **spécifier des autorisations pour plusieurs utilisateurs**, ce qui facilite la gestion des autorisations pour ces utilisateurs.

Par exemple, vous pouvez avoir un groupe d'utilisateurs appelé ***Administrateurs*****,** et accorder à ce groupe d'utilisateurs les types **d'autorisations dont les administrateurs** ont généralement besoin. Tous les utilisateurs de ce groupe d'utilisateurs reçoivent automatiquement les autorisations attribuées au groupe d'utilisateurs.

Voici quelques caractéristiques importantes des groupes d'utilisateurs :

- Un groupe d'utilisateurs peut contenir de nombreux utilisateurs, et un utilisateur peut appartenir à plusieurs groupes d'utilisateurs.
- Les groupes d'utilisateurs ne peuvent pas être imbriqués ; ils ne peuvent contenir que des utilisateurs, pas d'autres groupes d'utilisateurs.
- Il n'existe pas de groupe d'utilisateurs par défaut incluant automatiquement tous les utilisateurs du compte AWS.

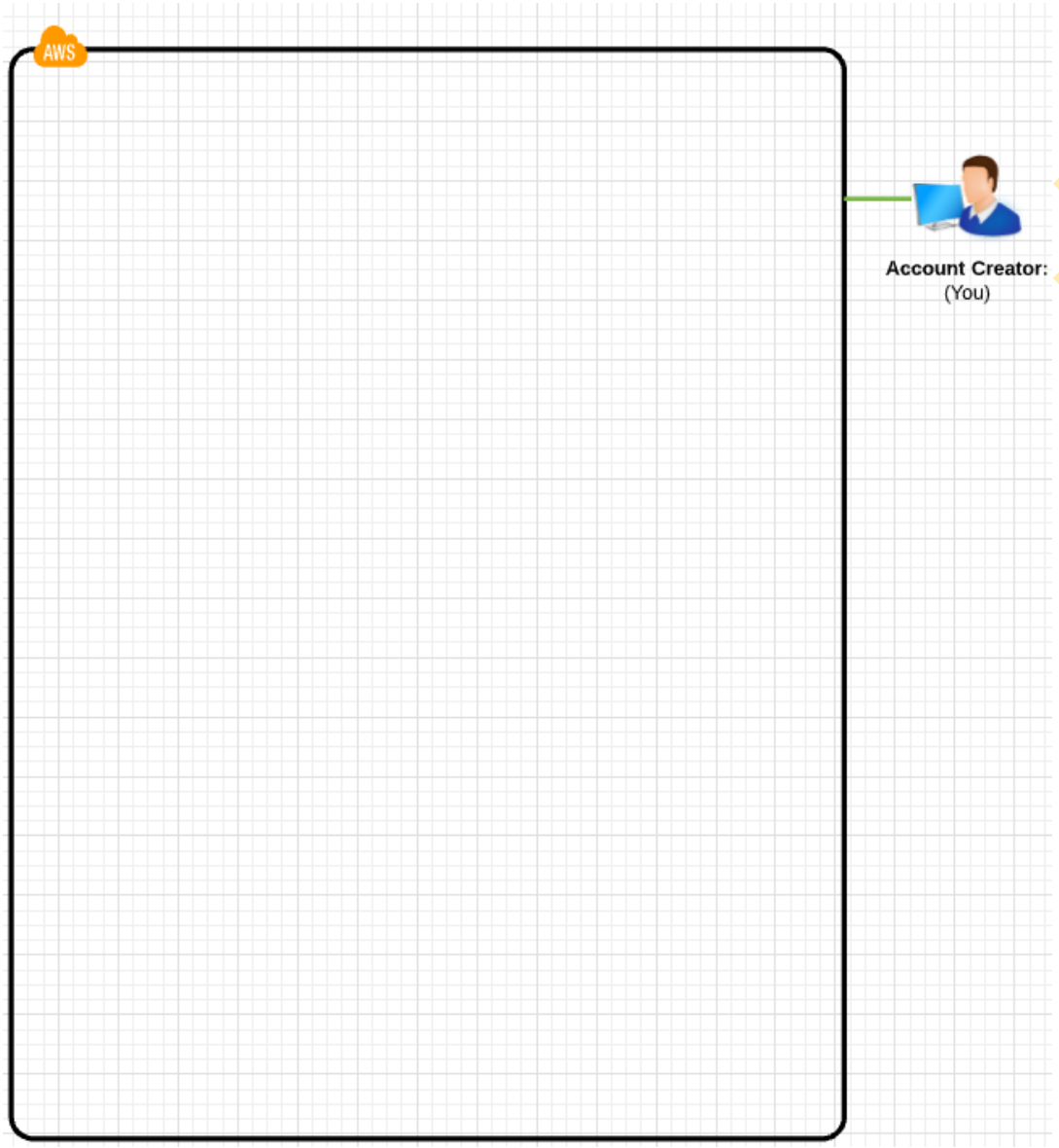
Amazon services Gestion des Identité

Configurer une stratégie de mot de passe fiable pour vos utilisateurs:

- Si vous autorisez les utilisateurs à modifier leurs propres mots de passe, créez une stratégie de mot de passe personnalisée qui les obligent à créer des mots de passe d'un niveau de sécurité élevé et à effectuer une rotation régulière de leurs mots de passe
- Vous pouvez créer une stratégie de mot de passe personnalisée pour votre compte. Vous mettez à niveau la stratégie de mot de passe par défaut AWS pour définir les exigences en matière de mot de passe. Comme:
  - La longueur minimale,
  - S'il nécessite des caractères non alphabétiques
  - A quelle fréquence il doit changer.
  - S'il est possible de réutiliser d'anciens mots de passe

Amazon services Gestion des Identité

- Création d'un compte AWS
- Création d'un compte avec des droits Admin
- Création d'un groupe Admin

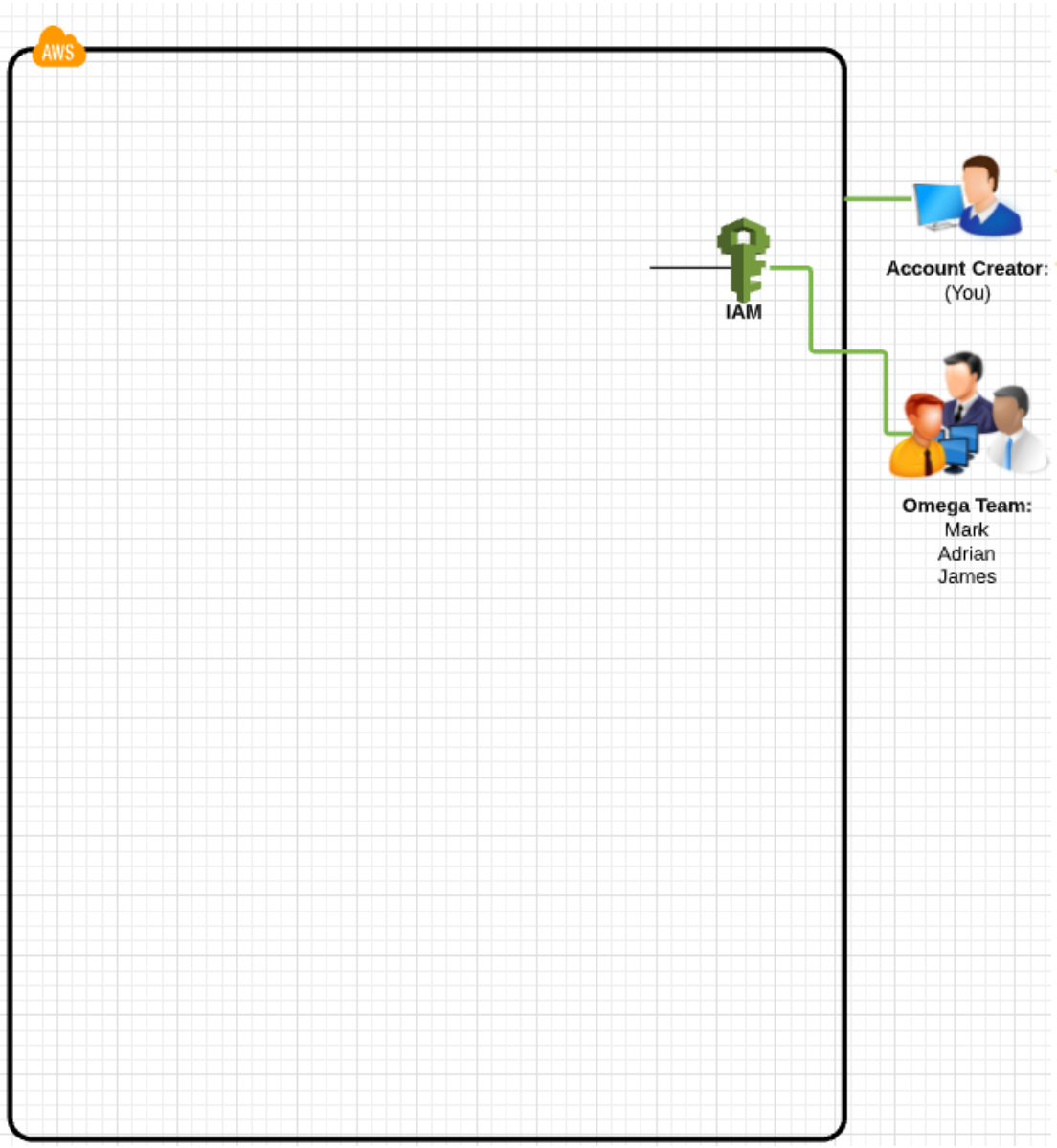


Amazon services Gestion des Identité

- Création de nouveaux users IAM:

Vous pouvez créer un ou plusieurs utilisateurs IAM dans votre compte AWS. Vous pouvez créer un utilisateur IAM lorsqu'une personne rejoint l'équipe ou lorsque vous créez une nouvelle application devant effectuer des appels d'API vers AWS.

Les 3 utilisateurs auront droit à une stratégie d'accès au service S3: **AmazonS3FullAccess**

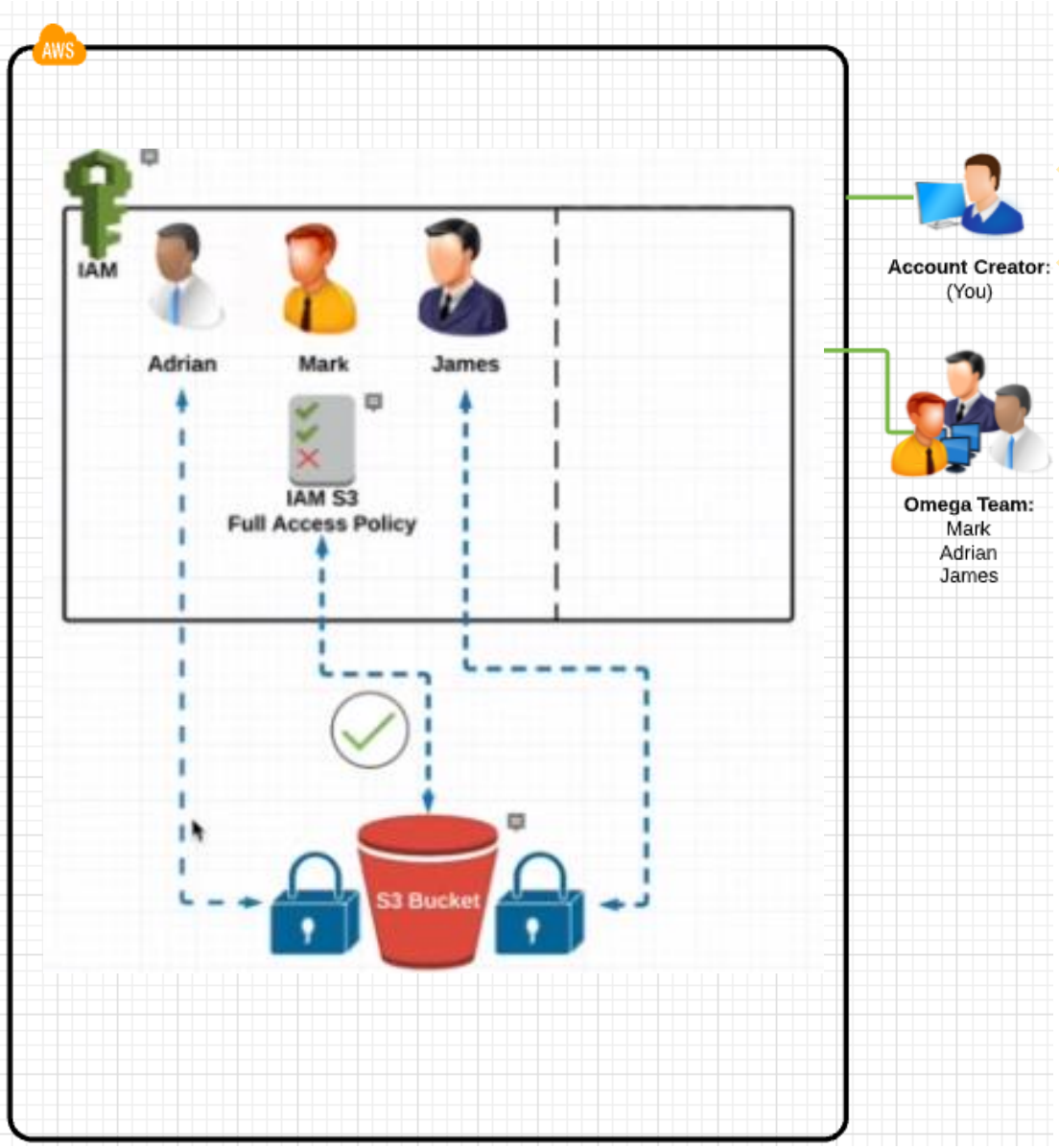


Amazon services Gestion des Identité

- Création de nouveaux users IAM:

Vous pouvez créer un ou plusieurs utilisateurs IAM dans votre compte AWS. Vous pouvez créer un utilisateur IAM lorsqu'une personne rejoint l'équipe ou lorsque vous créez une nouvelle application devant effectuer des appels d'API vers AWS.

Les 3 utilisateurs auront droit à une stratégie d'accès au service S3: **AmazonS3FullAccess**

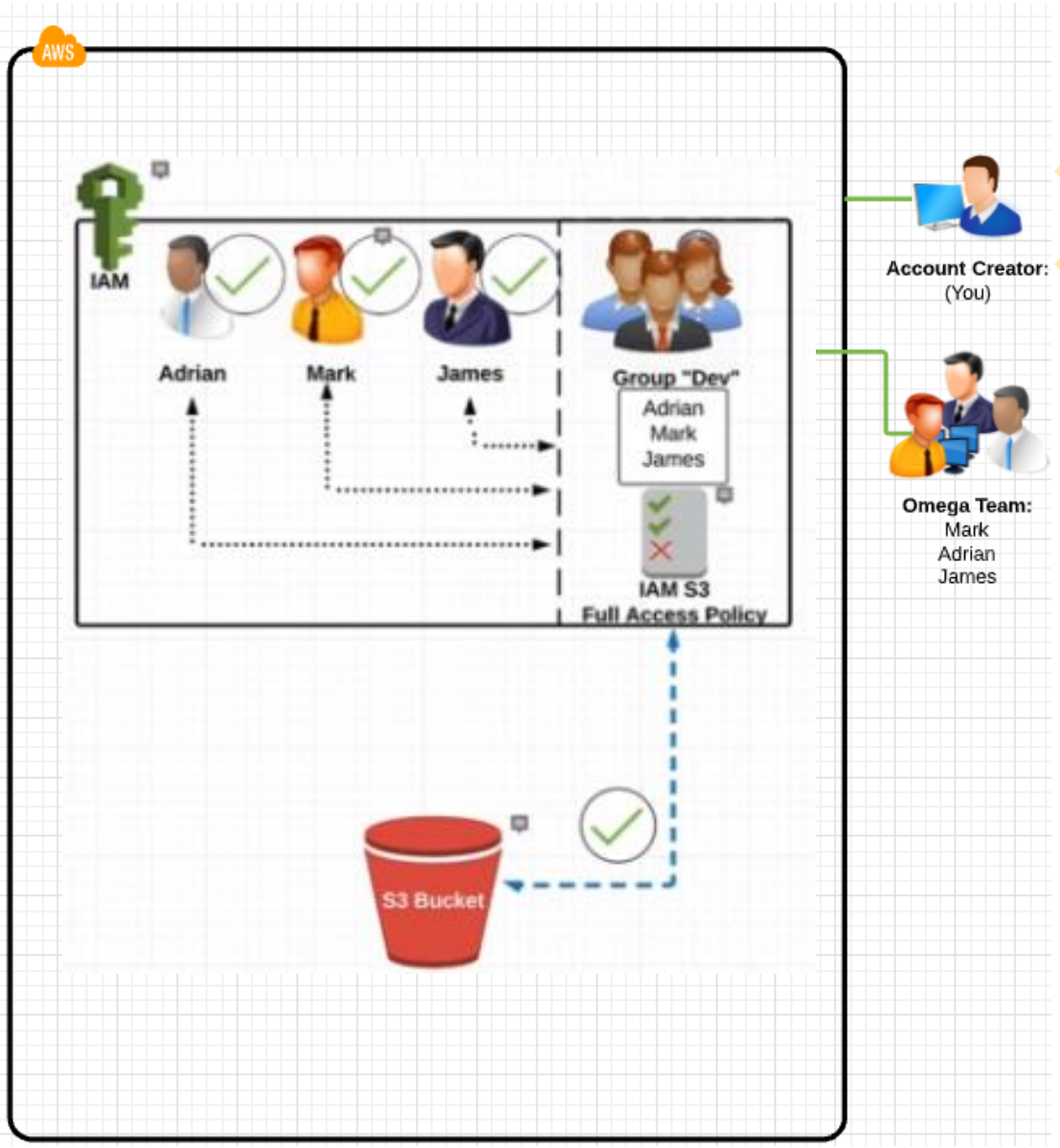


Amazon services Gestion des Identité

- Création de groupes d'utilisateurs IAM:

Pour configurer un groupe d'utilisateurs, vous devez le créer. Ensuite, attribuez au groupe des autorisations en fonction du type de tâche que les utilisateurs du groupe seront amenés à effectuer. Enfin, ajoutez les utilisateurs au groupe.

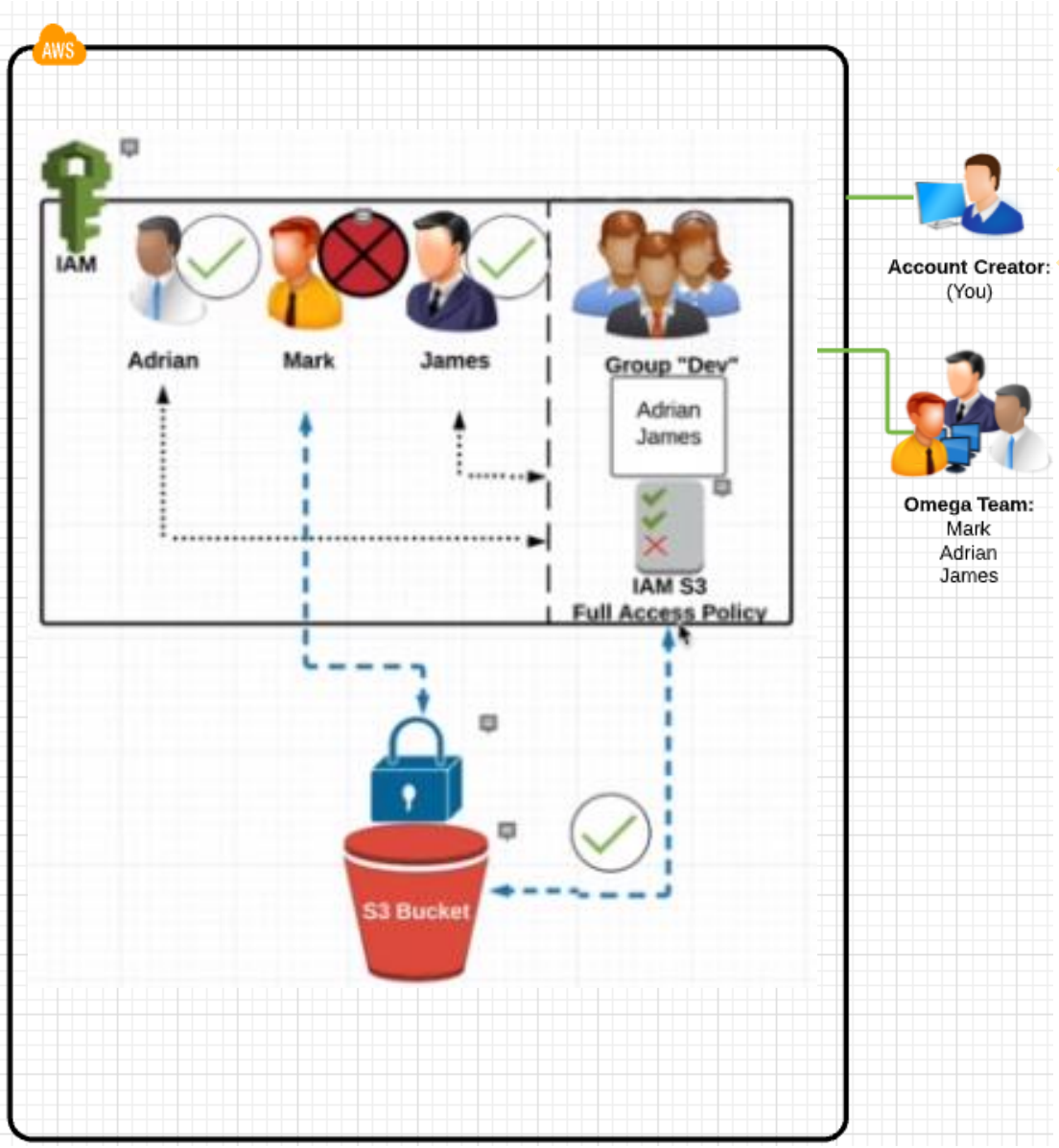
- Supprimez la strategie rattachée aux utilisateurs créés
- Créez un groupe **DEV** avec une stratégie d'accès au service S3: **AmazonS3FullAccess** dans l'onglet permissions
- Ajoutez les utilistaeurs au groupe **DEV** dans l'onglet users



Amazon services Gestion des Identité

- Création de groupes d'utilisateurs IAM:
- Supprimez l'utilisateur Mark du groupe DEV
- Remettez l'utilisateur Mark dans le groupe DEV

Il est recommandé d'utiliser les groupes pour gérer les access et autorisations des utilisateur IAM

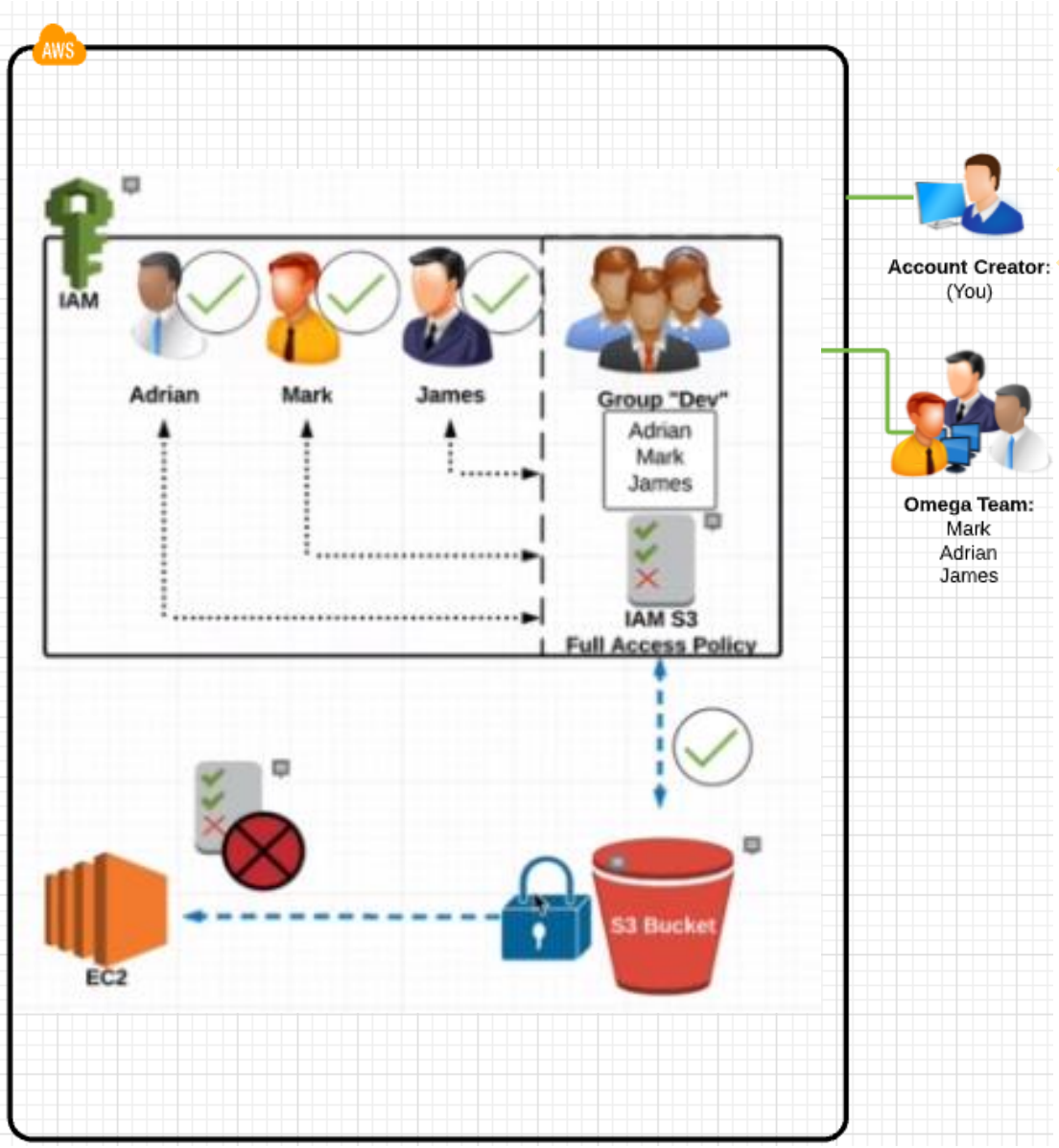


Amazon services Gestion des Identité

- Création d'un Rôle IAM:

Un *rôle* IAM est une **identité IAM** que vous pouvez créer dans votre compte et qui dispose d'autorisations spécifiques. **Un rôle IAM** est similaire à un **utilisateur IAM**, car il s'agit d'une identité AWS avec des stratégies d'autorisation qui déterminent ce que l'identité peut et ne peut pas faire dans AWS. En revanche, au lieu d'être associé de **manière unique à une personne**, un rôle est conçu pour être assumé **par tout utilisateur ou service qui en a besoin.**

J'ai besoin d'éxécuter un code sur une machine EC2 qui va lire des données depuis S3. Pour cela je dois autoriser le service EC2 accéder au services S

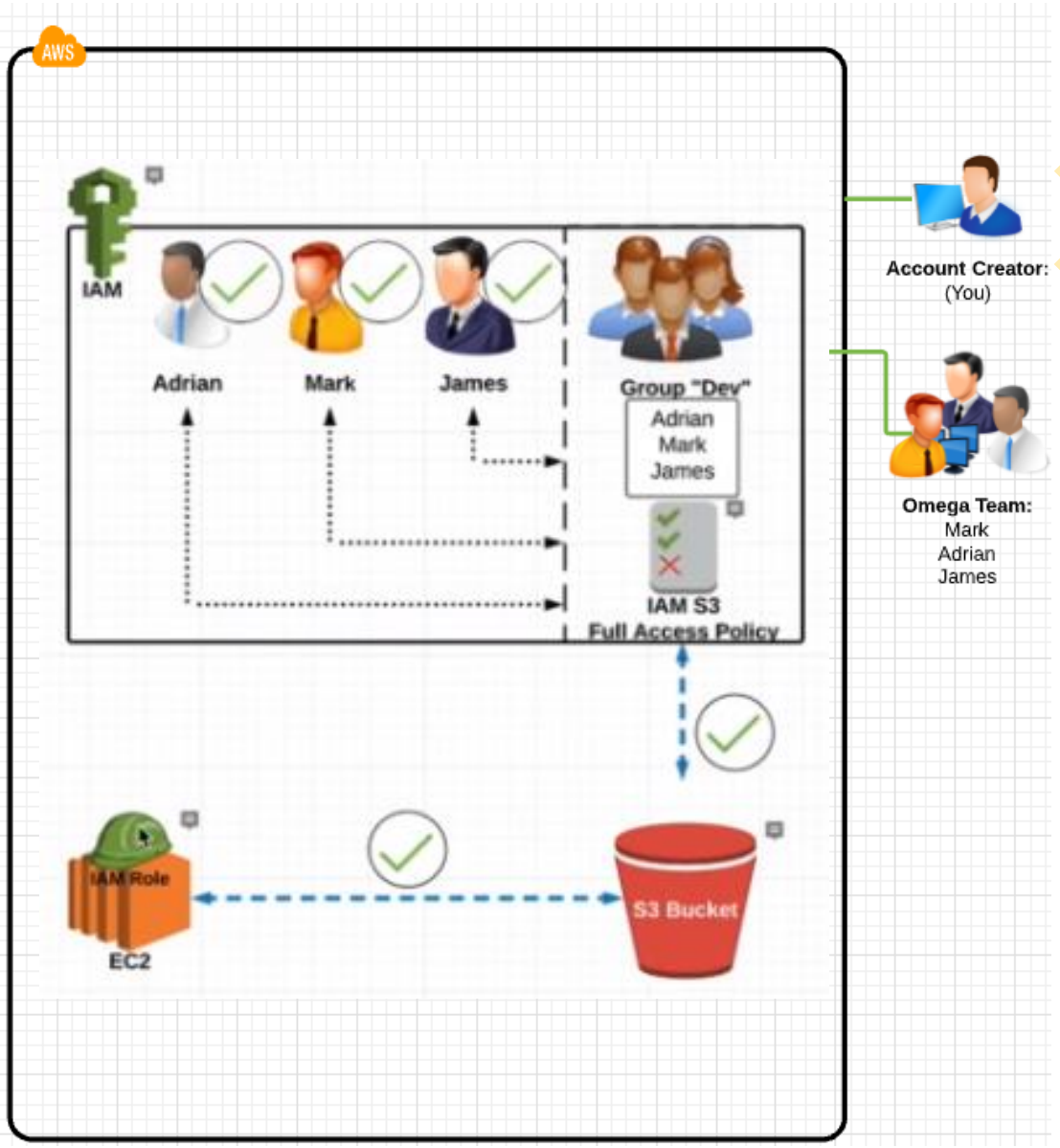


Amazon services Gestion des Identité

- Comme je ne peux pas rattacher ne strategie IAM a un service. Pour cela, je dois utiliser un Rôle IAM.

- Le Rôle IAM va permettre au service Ec2 à accéder au service S3.

- Dans Rôles
- Dans AWS services , selectionnez Ec2
- Attachez une strategie IAM **AmazonS3FullAccss** au rôle
- Créez le Rôle **ec2tos3**



Amazon services Gestion des Identité

En résumé, nous avons

1. Créer un Compte AWS et appliquer les recommandations et bonnes pratiques

2. Créer des comptes utilisateurs pour l'équipe de développement avec des accès aux services AWS

3. Céer un groupe DEV pour facilier la gestion des droits de l'équipe de développement

4. Créer un role pour permttre à deux services de communiquer

projet Omega

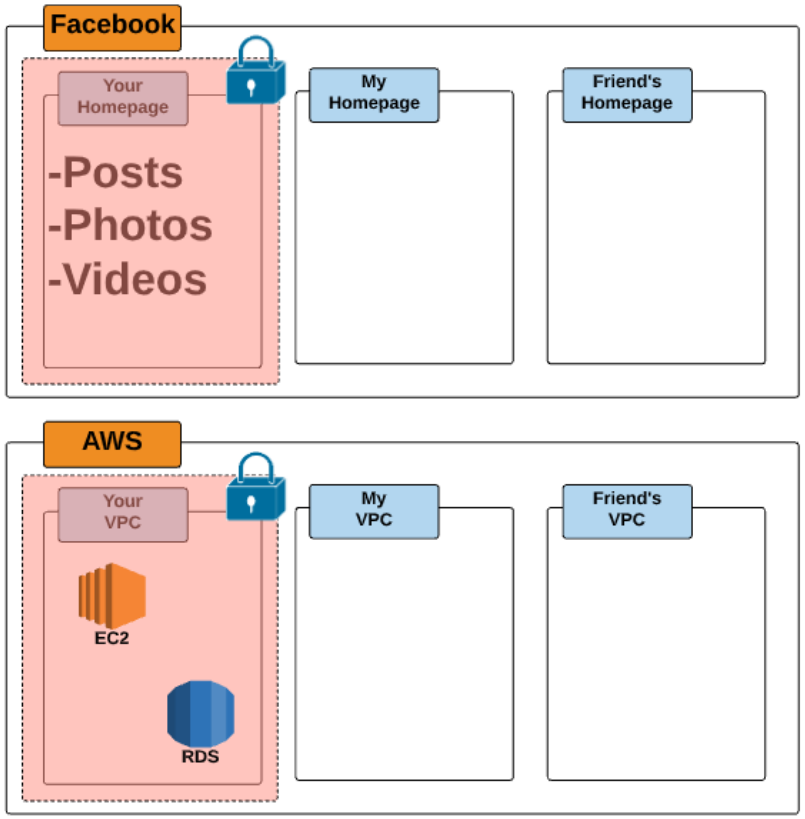
- Infrastructure AWS requise:
  1. Un Compte AWS
  2. Des comptes utilisateurs pour l'équipe de développement avec des accès aux services AWS
  3. Un routage approprié du trafic vers et depuis notre cloud virtuel privé VPC AWS
  4. Un emplacement pour le stockage en masse des fichiers
  5. Des servers pour héberger le projet
  6. Une base de données pour stocker et cataloguer les données
  7. Un service de notification (Mail ou sms) pour l'équipe du projet, basé sur les événements d'infrastructure
  8. Un service pour monitorer le projet et l'infrastructure du projet
  9. Automatiser le processus de distribution du trafic entrant entre les ressources AWS du projet Omega
  10. Automatiser le processus de scaling up ou scaling down des ressources AWS du projet Omega
  11. Mettre en place et configurer un domaine web qui pointe vers l'infrastructure de projet Omega
  12. Tester la possibilité d'utiliser des ressources de type serveless pour le projet Omega

- Amazon services Réseau

- Virtual Private Cloud - VPC
- Internet Gateways - IGW
- Route Tables (RTs)
- Network Acces Control List – NACLs
- Subnets
- Zones de disponibilité (Spécifique VPC)

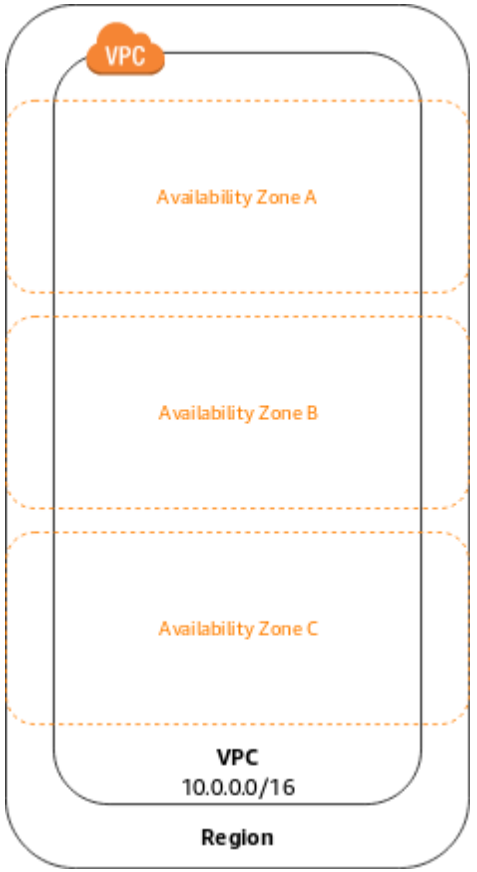
• Amazon services Réseau

Un cloud privé virtuel (**Virtuel private cloud VPC**) est un réseau virtuel dédié à votre compte AWS. Il est **logiquement isolé** des autres réseaux virtuels dans le cloud AWS. Vous pouvez lancer vos **ressources** AWS, telles que des instances Amazon EC2, dans votre **VPC**. Un default VPC est créé à la création de votre compte AWS.



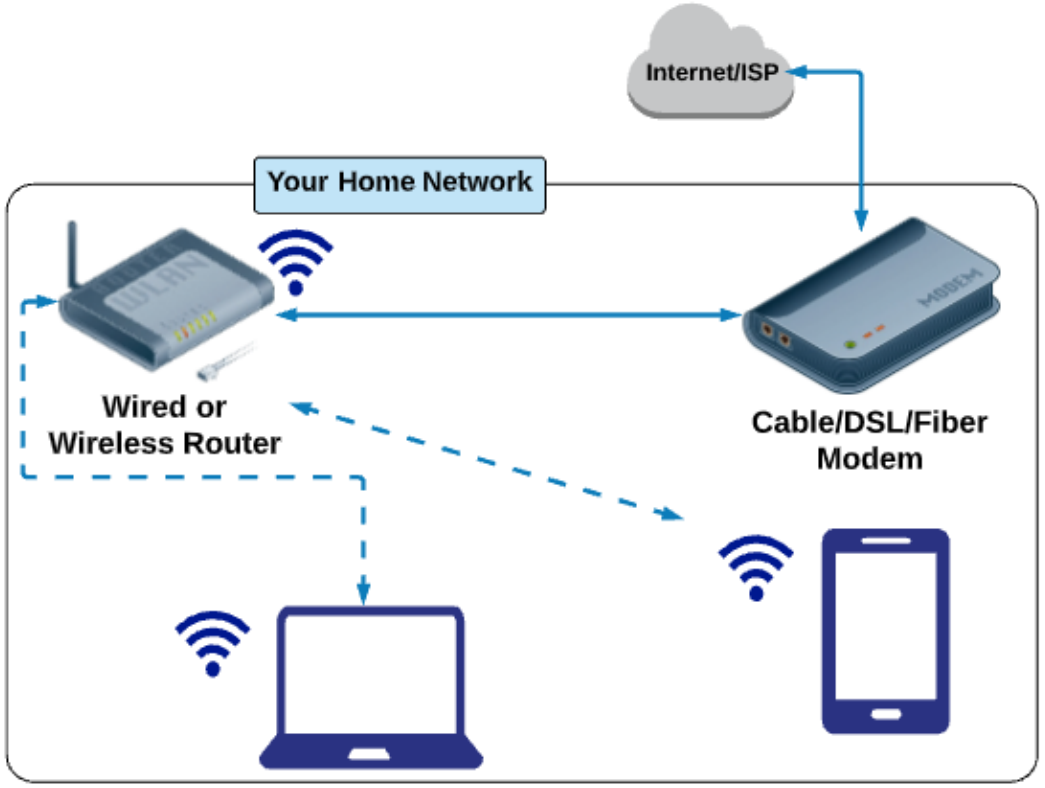
• Amazon services Réseau

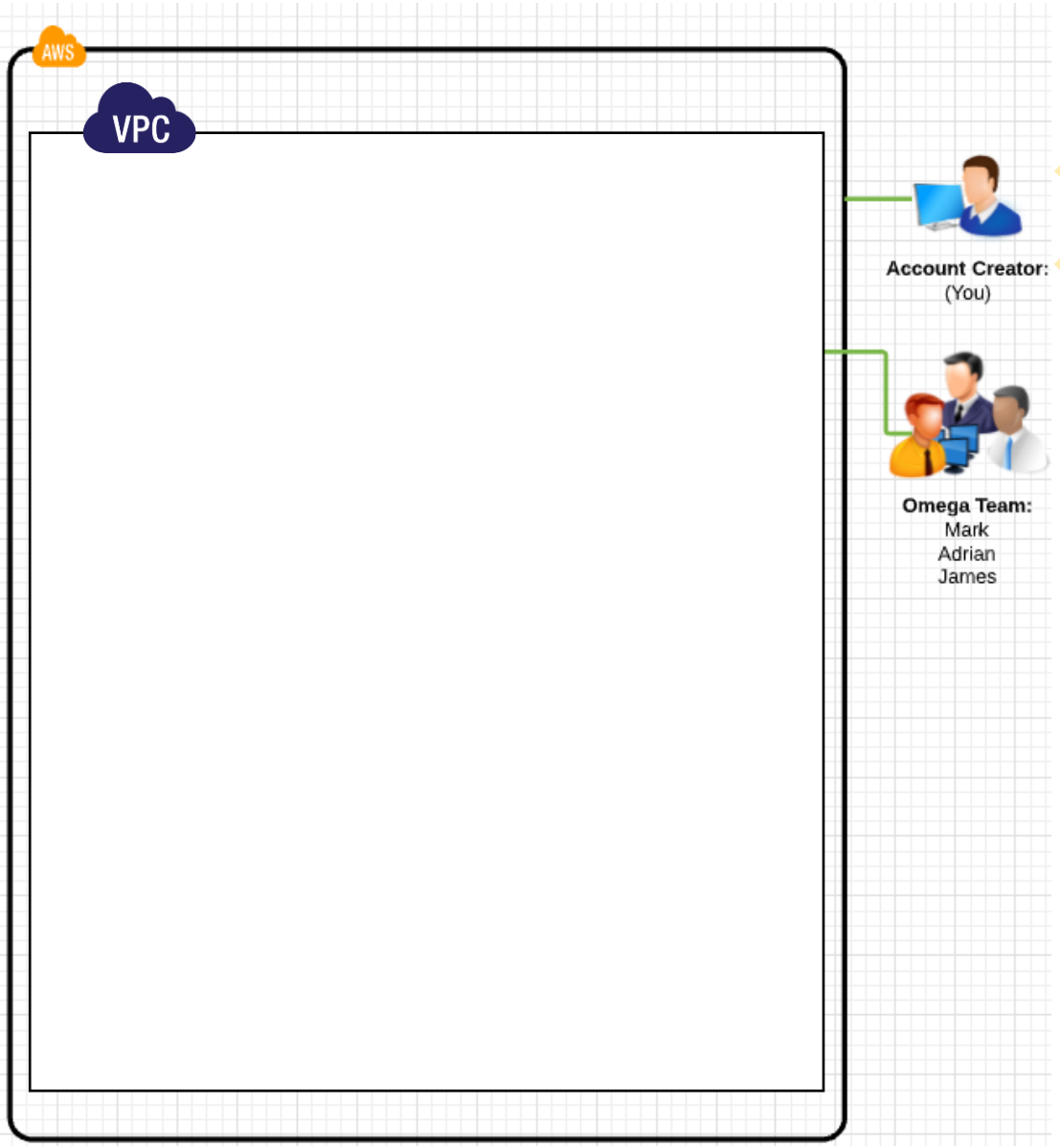
- Lorsque vous créez un nouveau VPC, vous devez spécifier une plage d'adresses **IPv4** pour le **VPC** sous la forme d'un bloc d'adresse **CIDR** (**Classless Inter-Domain Routing)**, par exemple, **10.0.0.0/16**. Il s'agit du bloc CIDR principal pour votre VPC.
- Un VPC couvre toutes les zones de disponibilité de la région.
- Le Default VPC inclus les composants réseau starndard:
  1. Internet Gateway
  2. Route table
  3. Network Access Control List
  4. Subnets (sous-réseau)
- Connectez vous à la console AWS et allez dans VPC.



- Amazon services Réseau

Default VPC:



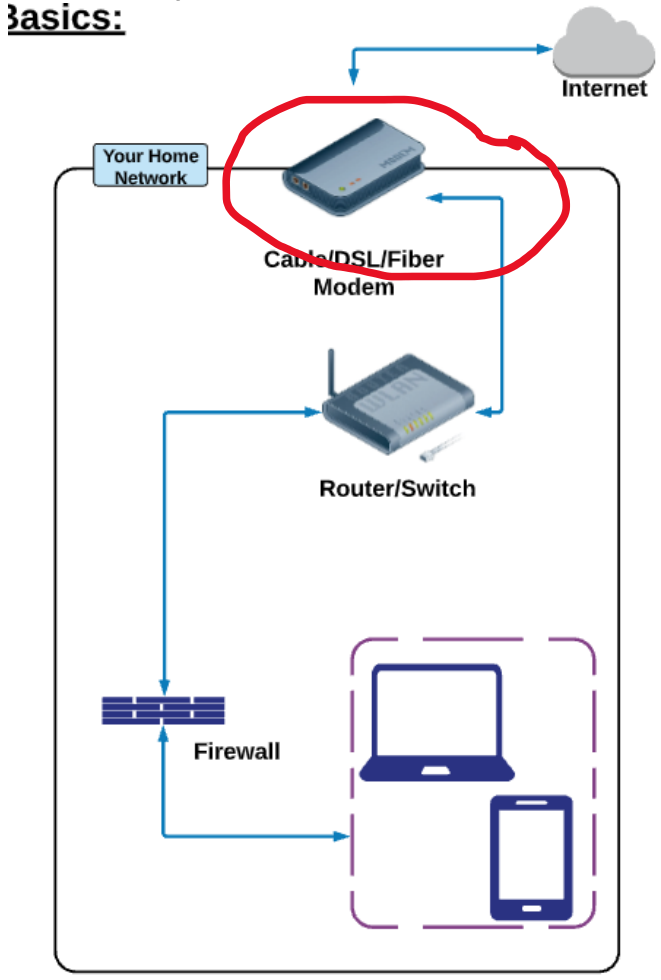


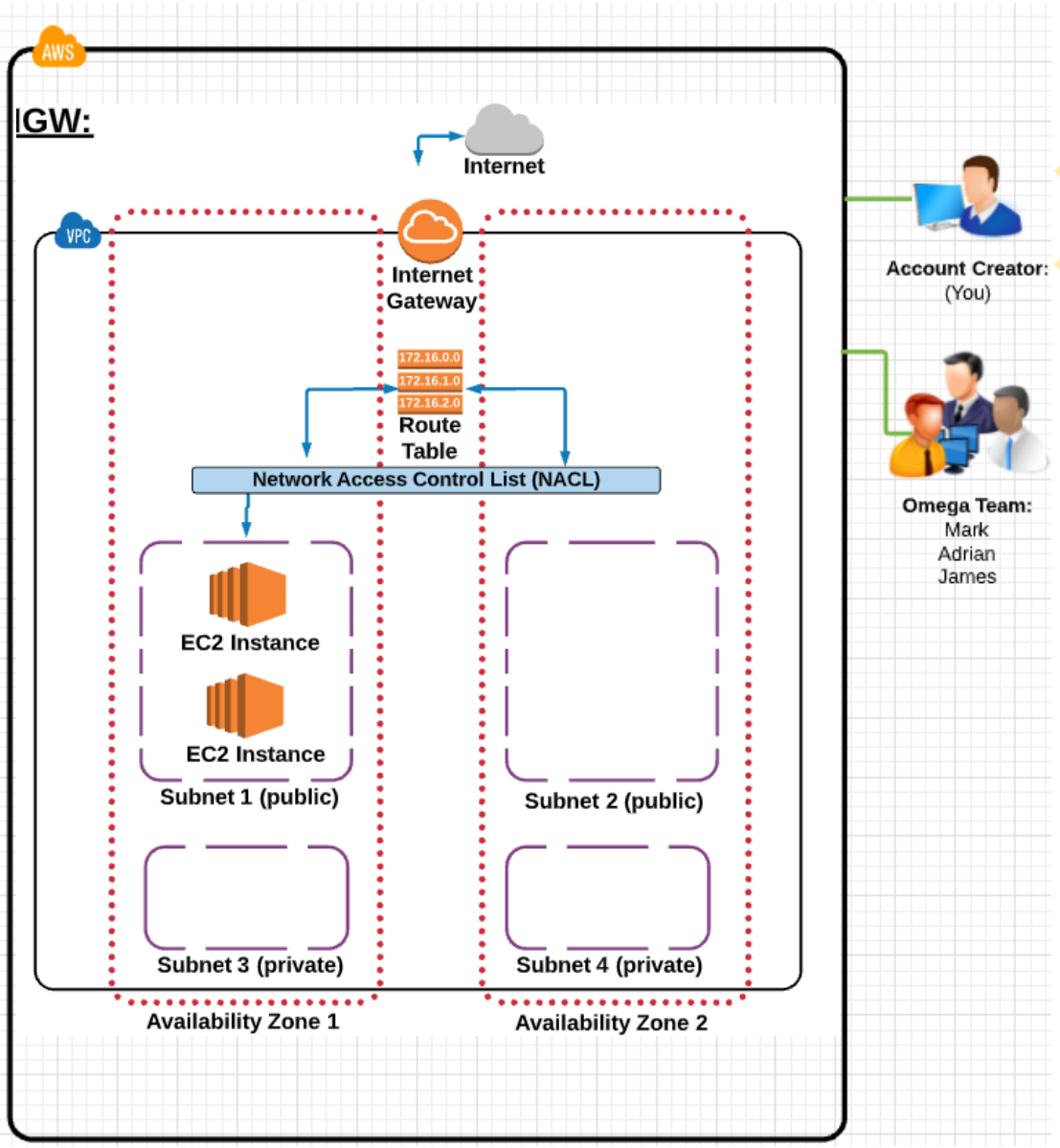
• Amazon services Réseau

- **Internet Gateway** (IGW) ou **Passerelle Internet** : est une passerelle que vous attachez à votre **VPC** pour permettre la communication entre les ressources de votre **VPC** et **Internet.**
- Une passerelle Internet a deux finalités : elle fournit
  - Une cible dans vos tables de routage VPC pour le trafic routable sur Internet
  - Elle effectue la conversion d'adresse réseau (NAT) pour les instances auxquelles ont été affectées des adresses IPv4 publiques.
- Une passerelle Internet prend en charge le trafic **IPv4 et IPv6.** Elle ne génère pas de risques de disponibilité ou de contraintes de bande passante sur votre trafic réseau. **Aucuns frais** supplémentaires ne s'applique si vous avez une passerelle Internet dans votre compte.

- Amazon services Réseau

Internet Gateway: Fonction Modem





• Amazon services Réseau

Internet Gateway:

Connectez-vous sur la console aws:

- Allez dans le service VPC
- Cliquez sur Internet gateway
- Vérifiez l'état de votre internet gatway
- Détattchez l'internet gateway au default VPC
- Attachez l'internet gateway au default VPC
- Créez une nouvelle internet Gateway
- Attachez la nouvelle internet gateway au default VPC

Note: Un vpc ne peut contenir qu'une seule internet gateway à la fois.

• Amazon services Réseau

Route tables RTs ou **tables de routage**s: Un ensemble de **règles,** appelées **routes**, qui permettent de déterminer où le **trafic réseau est dirigé.**

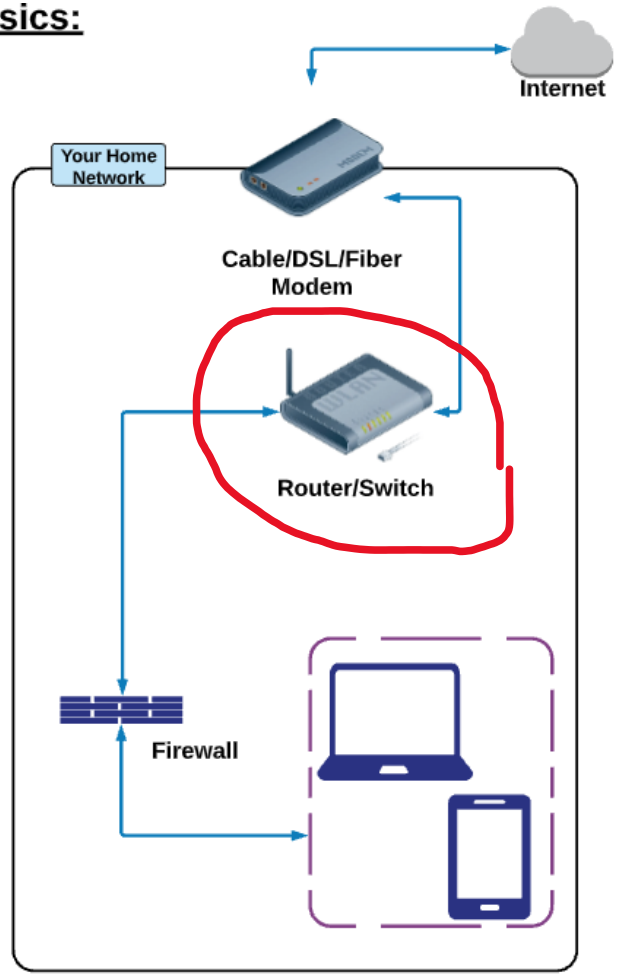
Votre **VPC** dispose d'un routeur implicite et vous utilisez les **tables de routage** pour contrôler où le trafic réseau est dirigé. Chaque s**ous-réseau** de votre **VPC** doit être associé à un**e table de routage**, qui contrôle le routage pour ce sous-réseau (table de routage de sous-réseau).

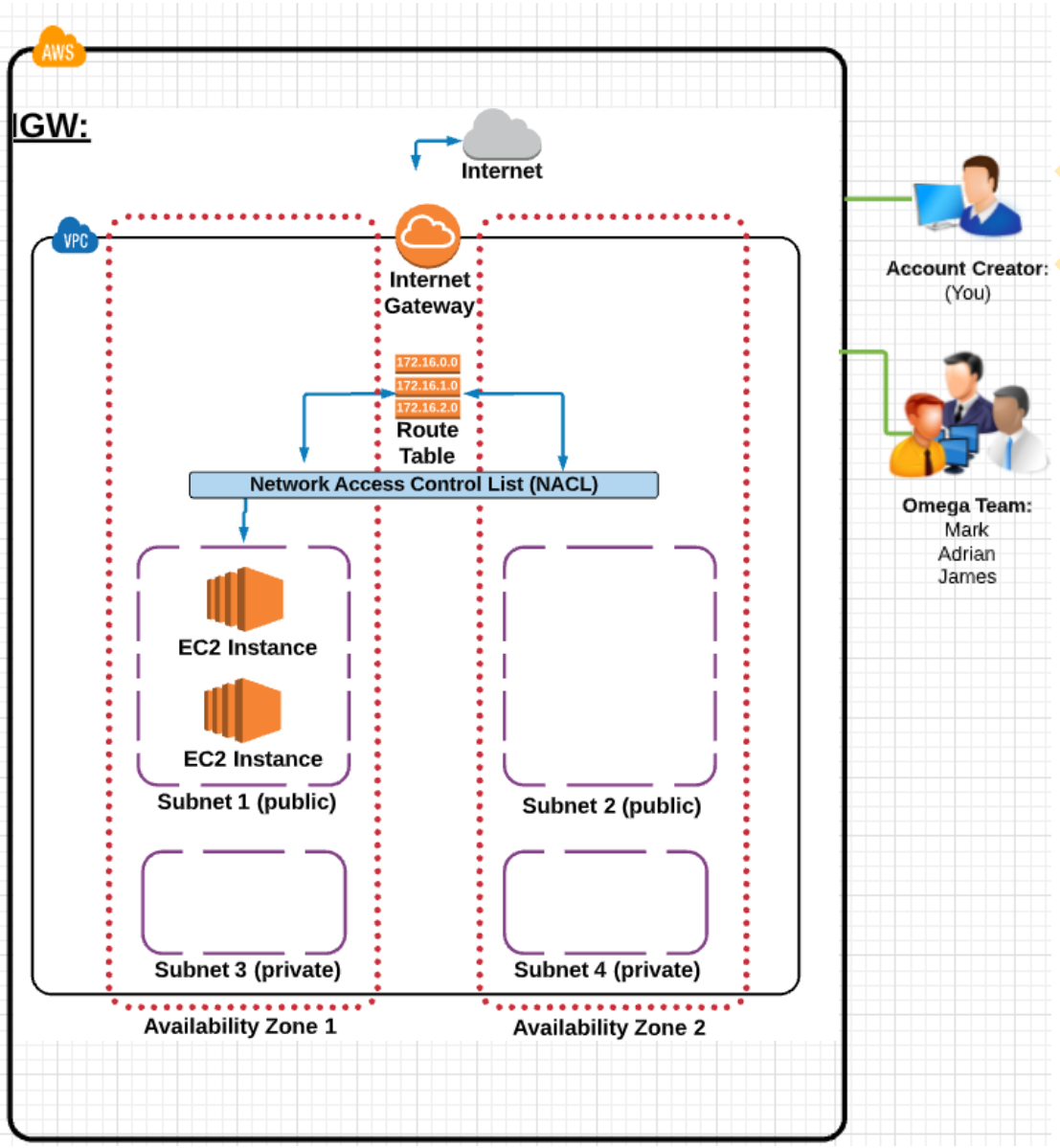
Vous pouvez éventuellement associer une **table de routage** à une **passerelle Internet**. Cela vous permet de spécifier des règles de routage pour le trafic entrant qui pénètre dans votre VPC via la passerelle.

Le **nombre de tables de routage** que vous pouvez créer par VPC est **limité**

- Amazon services Réseau

Route tables:





• Amazon services Réseau

Voici quelques concepts clés relatifs aux tables de routage :

- **Table de routage principale** : Il s'agit de la table de routage qui est associée automatiquement à votre VPC.
- **Table de routage personnalisée** : Il s'agit de la table de routage que vous créez pour votre VPC.
- **Table de routage de sous-réseau** : Il s'agit d'une table de routage associée à un sous-réseau.
- **Table de routage de passerelle** : Il s'agit d'une table de routage associée à une passerelle Internet ou
- **Destination** : Il s'agit de la plage d'adresses IP vers laquelle vous souhaitez acheminer le trafic (CIDR de destination). Par exemple, un réseau d'entreprise externe avec le CIDR 172.16.0.0/12.
- **Cible** : Il s'agit de la passerelle, l'interface réseau ou la connexion par laquelle le trafic de destination est à envoyer ; par exemple, une passerelle Internet.
- **Route locale** : Il s'agit de la route de communication par défaut au sein du VPC.

• Amazon services Réseau

Route tables:

Connectez-vous sur la console aws:

- Allez dans le service VPC
- Cliquez sur route tables
- Cliquez sur routes
- Cliquez sur interent gateway
- Déttachez l'internet gateway du default VPC
- Retournez dans route tables et cliquez sur routes
- Retournez dans internet gateway et attachez l'internet gateway au default VPC
- Supprimez la route 0.0.0.0/0 et recréez-la

• Amazon services Réseau

Network Access Control List NACL ou **Liste de contrôle d'accès réseau**: est une **couche de sécurité** au niveau **réseau**. Elle a le rôle d'un **pare-feu** pour contrôler le traffic entrants et sortants d'un ou plusieurs **sous-réseaux** de votre VPC.

Vous pouvez définir des listes ACL réseau à l'aide de **règles** similaires à vos **groupes de sécurité** afin d'ajouter une couche de sécurité supplémentaire à votre VPC.

Le default VPC posséde un NACL qui est associé au sous réseau par défault (defalut subnets)

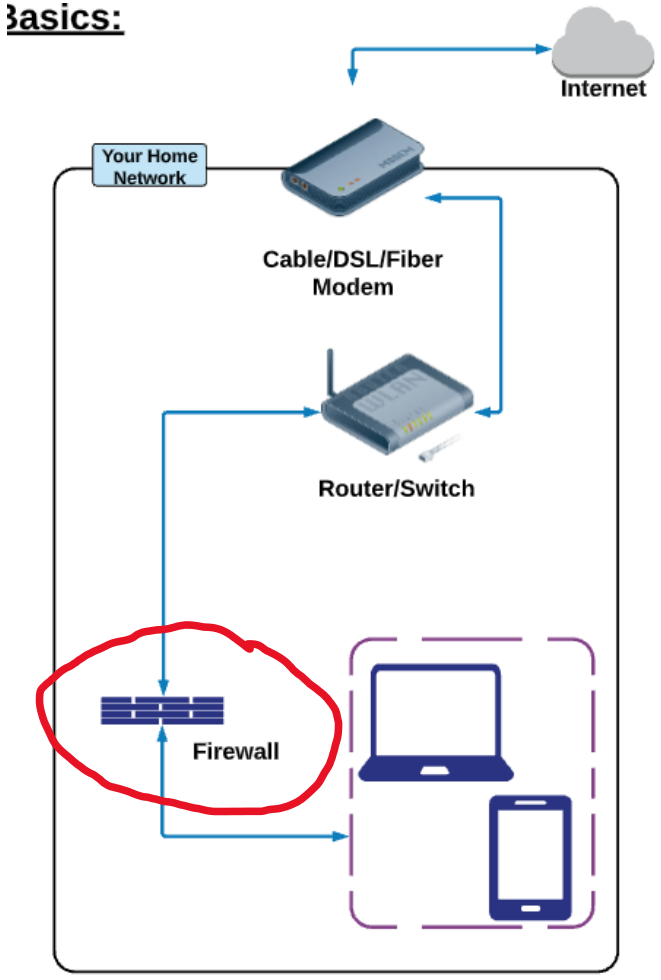
• Amazon services Réseau

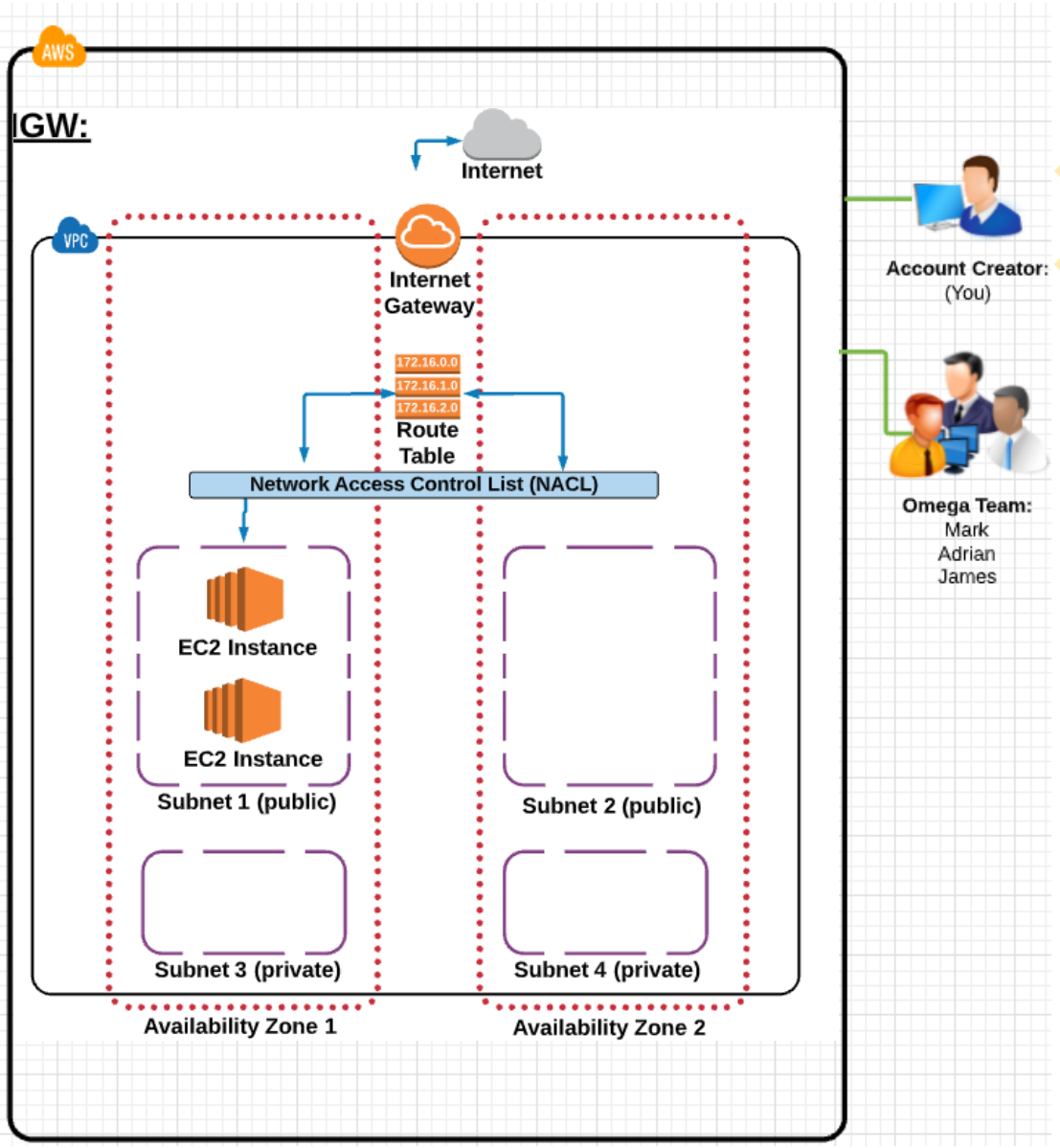
Une règle d'une liste ACL réseau est composée des éléments suivants :

- **Numéro de règle**. les règles sont évaluées en commençant par la règle comportant le numéro le plus bas. Lorsqu'une règle correspond au trafic, elle s'applique même si une règle avec un numéro plus élevé la contredit.
- **Type**. Type de trafic ; par exemple, SSH. Vous pouvez également spécifier tout le trafic ou une plage personnalisée.
- **Protocole**. Vous pouvez spécifier n'importe quel protocole associé à un numéro de protocole standard.
- **Plage de ports**. Port d'écoute ou plage de ports pour le trafic. Par exemple, 80 pour le trafic HTTP.
- **Source**. [Règles entrantes uniquement] Source du trafic (plage CIDR).
- **Destination**. [Règles sortantes uniquement] Destination du trafic (plage CIDR).
- **Autoriser/Refuser**. Indique s'il faut autoriser ou refuser le trafic spécifié.

- Amazon services Réseau

Network Access Control NACL:





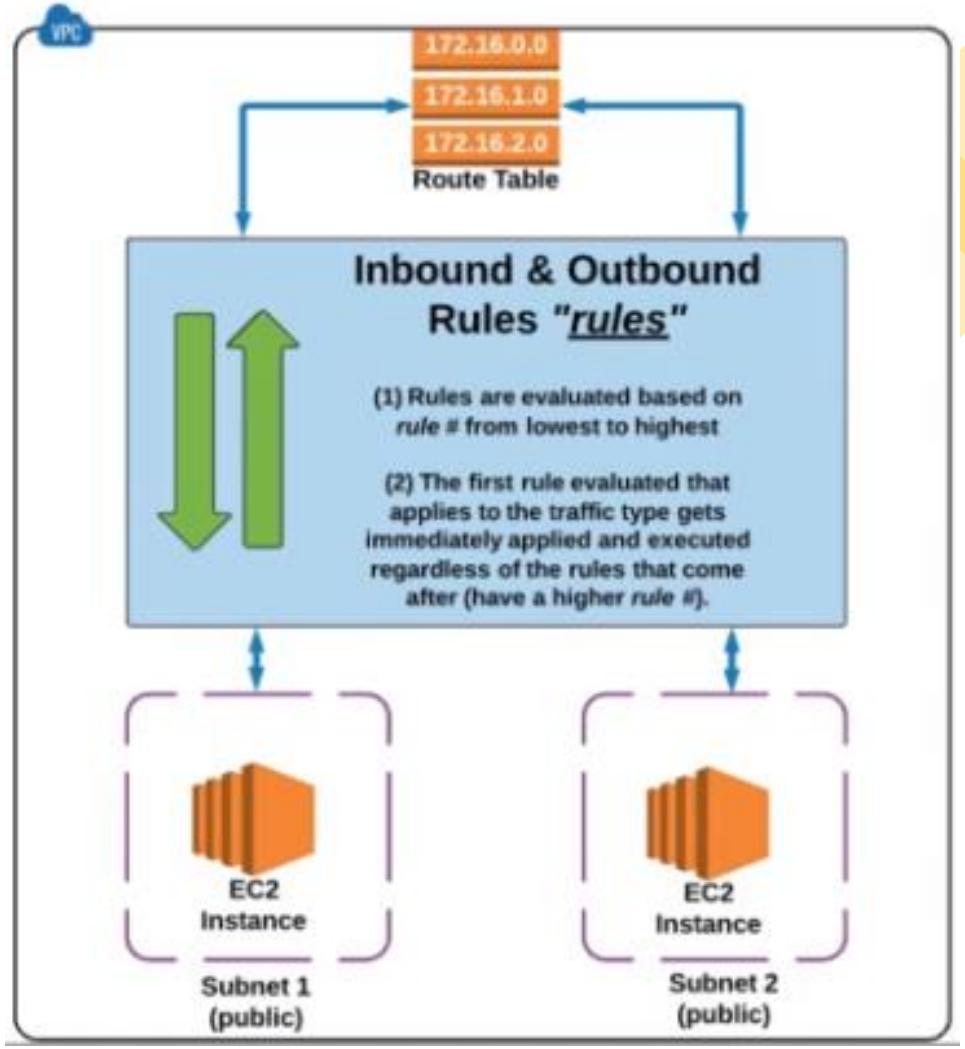
• Amazon services Réseau

Network Access Control List NACL:

Connectez-vous sur la console aws:

- Allez dans le service VPC
- Cliquez sur Network Access Control List
- Cliquez sur Inbound rules
- Modifiez la régle 100 pour autoriser le traffic SSH
- Créez une régle 90 pour intérdir le traffic SSH
- Cliquez sur Outbound rules
- Créez une régle pour autoriser le traffic TCP

100 – custome tcp – tcp – 1024-65535 – 0.0.0.0/0



• Amazon services Réseau

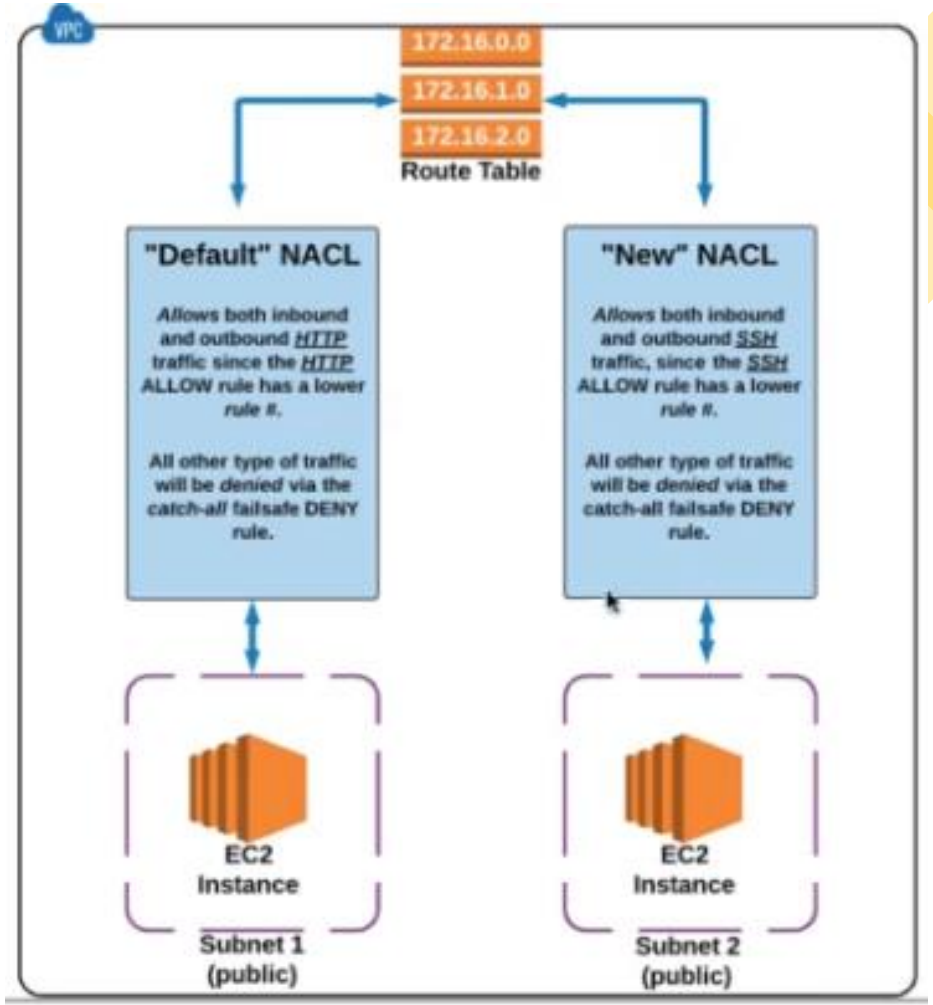
Network Access Control NACL:

- Créez un NCAL (NewNacl)
- Créer une régle pour autoriser le traffic

Entrant/sortant HTTP sur le port 80

100 – HTTP(80) - TCP – 80 – 0.0.0.0/0

- Cliquez sur subnets associations
- Editez la liste du subnet et associez un subnet.



• Amazon services Réseau

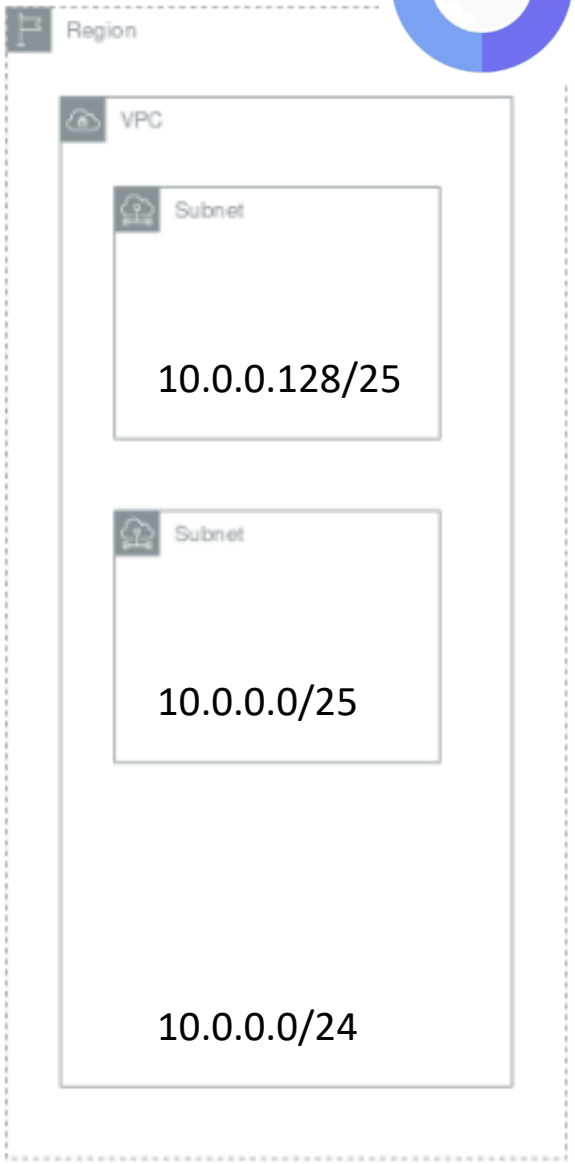
Subnets ou sous-réseau: Après avoir créé un **VPC**, vous pouvez ajouter **un** ou **plusieurs sous-réseaux** dans chaque **zone de disponibilité**. Un ***sous-réseau*** est une **plage d'adresses IP** dans votre **VPC**.

Vous pouvez lancer des ressources AWS, telles que des instances **EC2**, dans un **sous-réseau** spécifique. Lorsque vous créez un **sous-réseau**, vous spécifiez son bloc d'adresse **CIDR IPv4**, lequel est un **sous-ensemble** du bloc d'adresse **CIDR du VPC.** Chaque **sous-réseau** doit résider entièrement dans u**ne zone de disponibilité** et ne peut pas s'étendre sur plusieurs zones.

Si vous créez **plusieurs sous-réseaux** dans un **VPC**, les blocs d'adresse **CIDR** de ces s**ous-réseaux ne peuvent pas se chevaucher**

Exemple: si vous créez un **VPC** avec le bloc d'adresse **CIDR 10.0.0.0/24 (10.0.0.0 - 10.0.0.255)**, il prend en charge **256** adresses IP. Vous pouvez scinder ce bloc d'adresse CIDR en **deux sous-réseaux**, chacun prenant en charge **128** adresses IP.

Amazon services Réseau



Subnets ou sous-réseau:

- **Subnet 1 :** utilise le bloc d'adresse CIDR 10.0.0.0/25

(pour les adresses 10.0.0.0 - 10.0.0.127)

- **Subnet2** : utilise le bloc d'adresse CIDR 10.0.0.128/25

(pour les adresses 10.0.0.128 - 10.0.0.255)

Les quatre premières adresses IP et la dernière adresse IP du bloc d'adresse CIDR de chaque sous-réseau ne sont pas disponibles pour utilisation

- 10.0.0.0 : Adresse réseau.
- 10.0.0.1 : Réservée par AWS pour le routeur VPC.
- 10.0.0.2: réservé par AWS. Notez que l'adresse IP du serveur DNS
- 10.0.0.3 : Réservée par AWS pour un usage futur.
- 10.0.0.255 : Adresse de diffusion réseau.

Subnets calculator: cliquez-ici

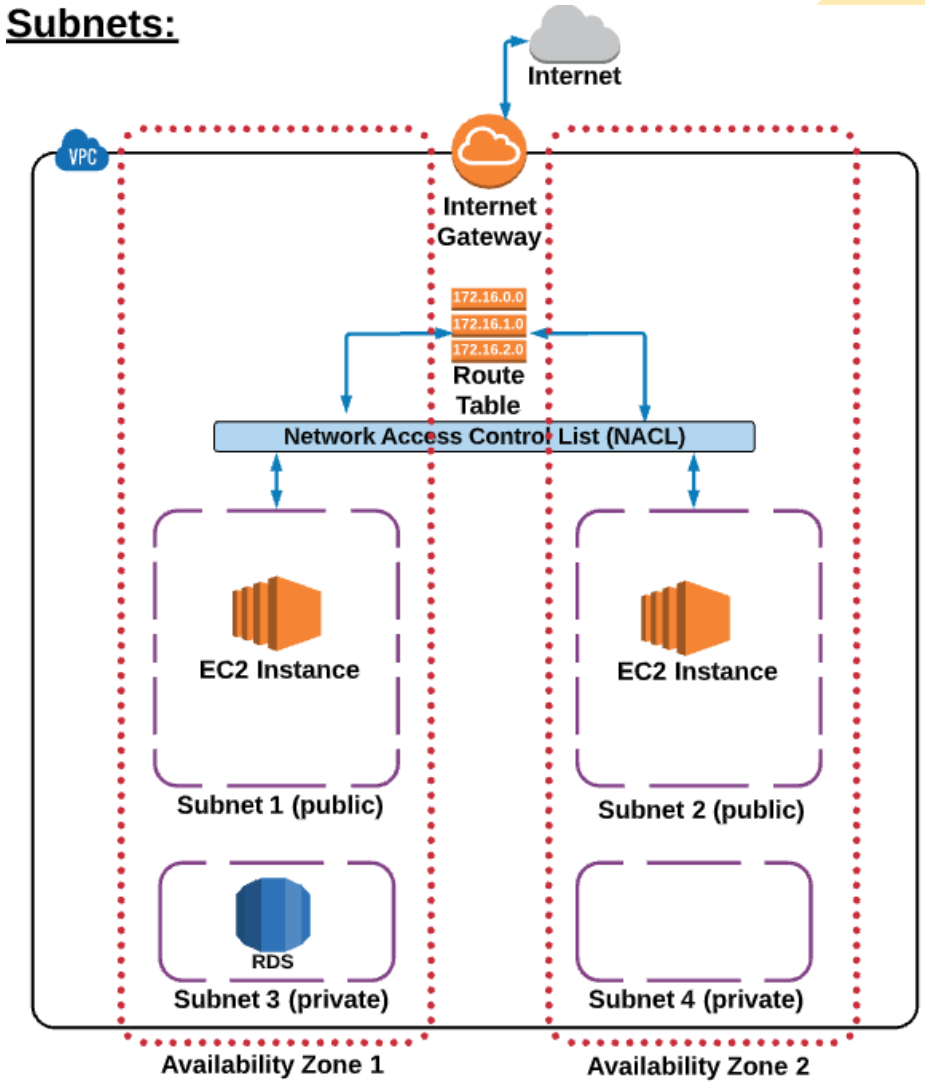
• Amazon services Réseau

Subnets ou sous-réseau:

Pour notre projet on a besoin de deux subnet (public et privé)

Subnet public: Si le trafic de votre s**ous-réseau** est acheminé vers une **passerelle Internet (Internet Gateway)**, le sous-réseau est reconnu comme un ***sous-réseau public***.

Subnet privé: Si un **sous-réseau** ne comporte pas de route vers la **passerelle Internet (Internet Gateway)**, le sous-réseau est reconnu comme un ***sous-réseau privé***.



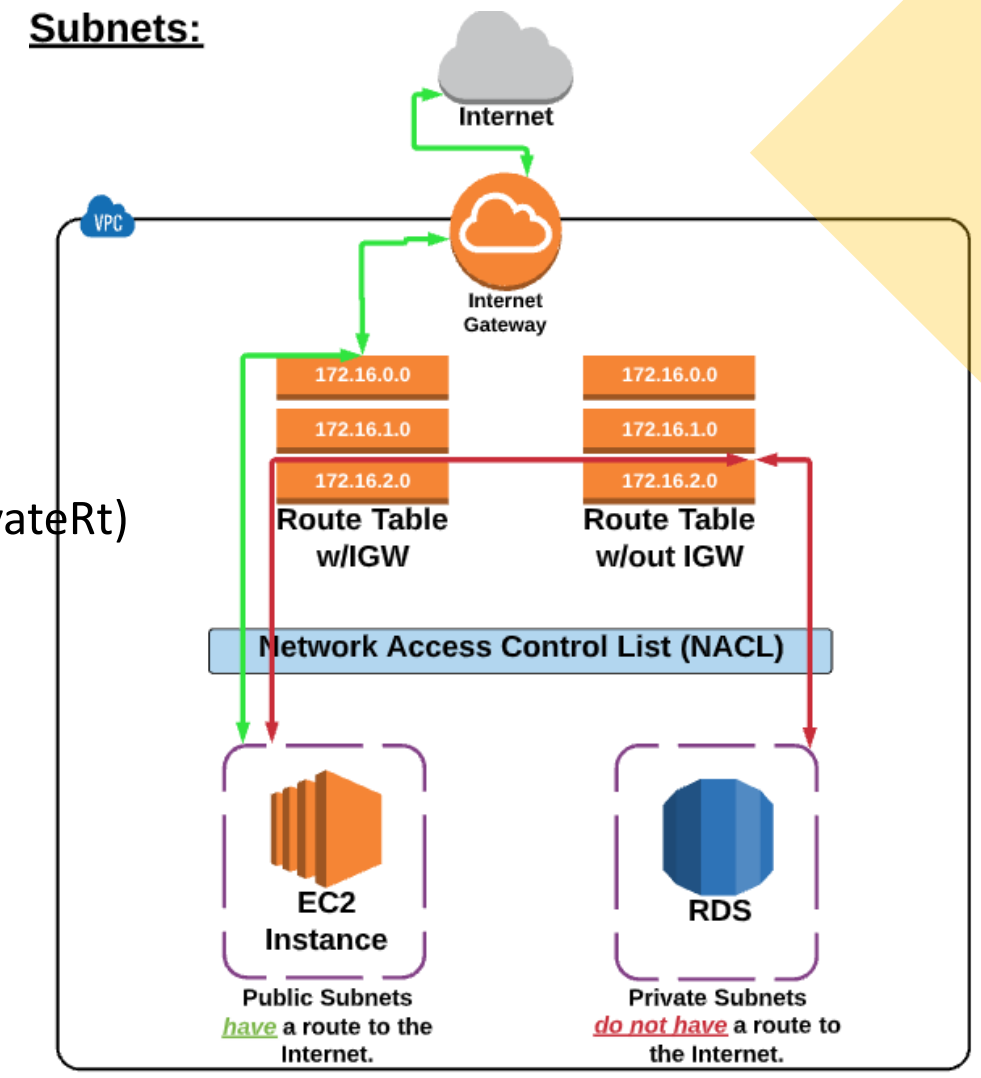
• Amazon services Réseau

Subnets ou sous-réseau:

1. Connectez-vous à la console AWS
2. Cliquez sur VPC (Verifiez que vous etes dans la région Ireland)
3. Cliquez sur subnets (3 subnets, 1 par zone)
4. Cliquez dans route tables, puis dans routes
5. Créez une route tables sans routage vers internet gateway (PrivateRt)
6. Cliquez dans subnet associations et selectionnez 2 subnets
7. Associez les subnets restant à la default route tables

(vérifier que la default route tables a un routage vers internet)

Allez dans subnets et renommez les subnets en fonction s'ils sont Public ou privé (rattacher ou non à internet gateway).



• Amazon services Réseau

Zones de disponibilité: Une zone de disponibilité comprend un ou plusieurs centres de données discrets dotés d'une alimentation redondante, d'une mise en réseau et d'une connectivité au sein d'une région AWS.

Les zones de disponibilité donnent aux clients la possibilité d'utiliser des applications de production et des bases de données **plus disponibles,** plus **tolérantes aux pannes** et plus évolutives que ce qui serait possible à partir d'un centre de données unique.

Haute disponibilité: High Availability ou HA permet d'assurer et de garantir le bon fonctionnement des services proposées et ce **7j/7 et 24h/24**. Cela consiste donc à mettre en place toutes les actions pour qu'une infrastructure informatique soit toujours disponible en appliquant certains principes tels que la **réplication des données**, la **sauvegarde**, la r**épartition de la charge**, la **redondance**, etc

Tolérance aux pannes: Fault Tolerence Permettant à un système de continuer à fonctionner, éventuellement de manière réduite (on dit aussi en « mode dégradé »), au lieu de tomber complètement en panne, lorsque l'un de ses composants ne fonctionne plus correctement ou tombe en panne.

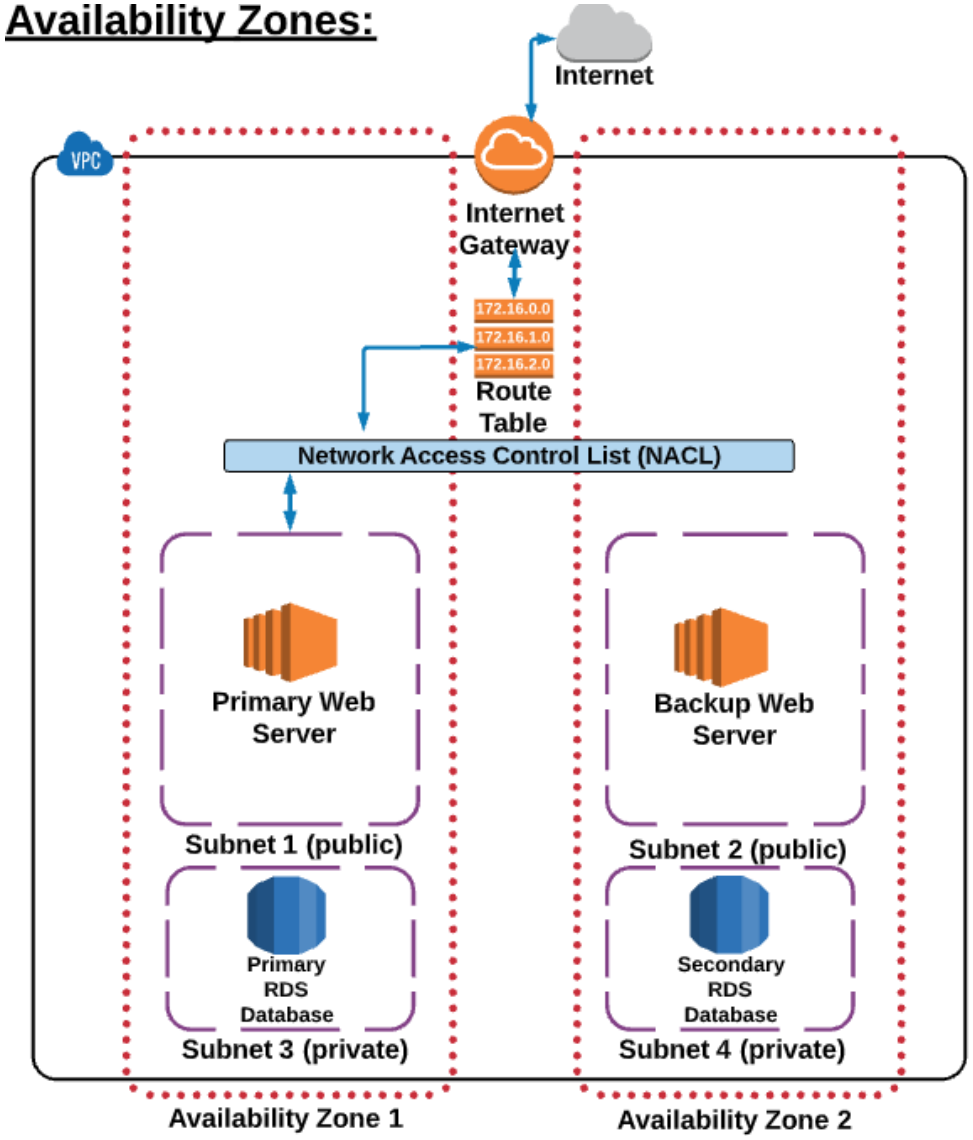
• Amazon services Réseau

Zones de disponibilité:
Le projet Omega founit un service web. L'architecture du Projet comporte une partie server web et une partie server de base de données.

Notre objectif est de mettre en place une infrastructure capable de garatir une architecture hautement disponible et tolérente aux pannes.

Pour cela chaque partie de notre architecture sera hébergée sur deux zone de disponibilité.

Que se passerait-il si un désatre (les coups de foudre, les tornades, les tremblements de terre, etc.) se produit dans la zone de disponibilité 1?



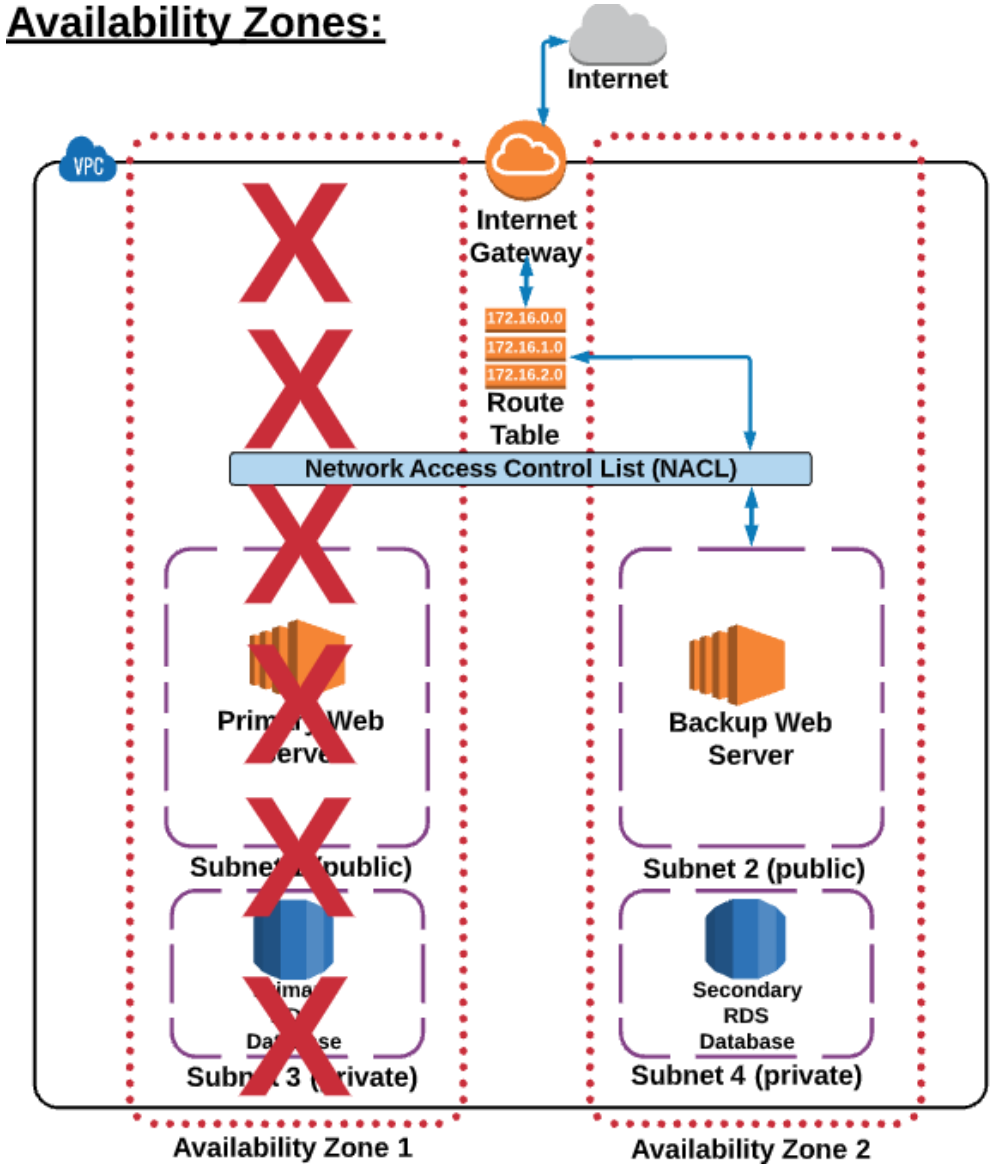
• Amazon services Réseau

Zones de disponibilité:
Le traffic sera automatique redérigé vers la zone de disponibilité 2.

Les zones de disponibilité d'une même région AWS sont interconnectées avec un réseau à bande passante élevée et à faible temps de latence.

le partitionnement des applications entre plusieurs zone de disponibilite (Mulit-az) permet de garantir une meilleure haute disponibilité et tolérance aux pannes.

Le SLA des services(ou Service Level Agreement, est le niveau de qualité et de performance contractuel d'un service ou d'une infrastructure technique), avec l'engagement de Amazon Web Services, est d'au moins 99.95%. À condition d'appliquer les bonnes pratiques d'architecture.



projet Omega

- Infrastructure AWS requise:
  1. Un Compte AWS
  2. Des comptes utilisateurs pour l'équipe de développement avec des accès aux services AWS
  3. Un routage approprié du trafic vers et depuis notre cloud virtuel privé VPC AWS
  4. Un emplacement pour le stockage en masse des fichiers
  5. Des servers pour héberger le projet
  6. Une base de données pour stocker et cataloguer les données
  7. Un service de notification (Mail ou sms) pour l'équipe du projet, basé sur les événements d'infrastructure
  8. Un service pour monitorer le projet et l'infrastructure du projet
  9. Automatiser le processus de distribution du trafic entrant entre les ressources AWS du projet Omega
  10. Automatiser le processus de scaling up ou scaling down des ressources AWS du projet Omega
  11. Mettre en place et configurer un domaine web qui pointe vers l'infrastructure de projet Omega
  12. Tester la possibilité d'utiliser des ressources de type serveless pour le projet Omega

- Amazon services de calcul (EC2)

- Elastic Compute Cloud (EC2)
- Amazon Machine Images (AMI)
- Type d'instance EC2
- Les volumes de stockage EBS
- Utilisation des security Group SG
- Adressage IP EC2
- Démarrer et se connecter à une EC2

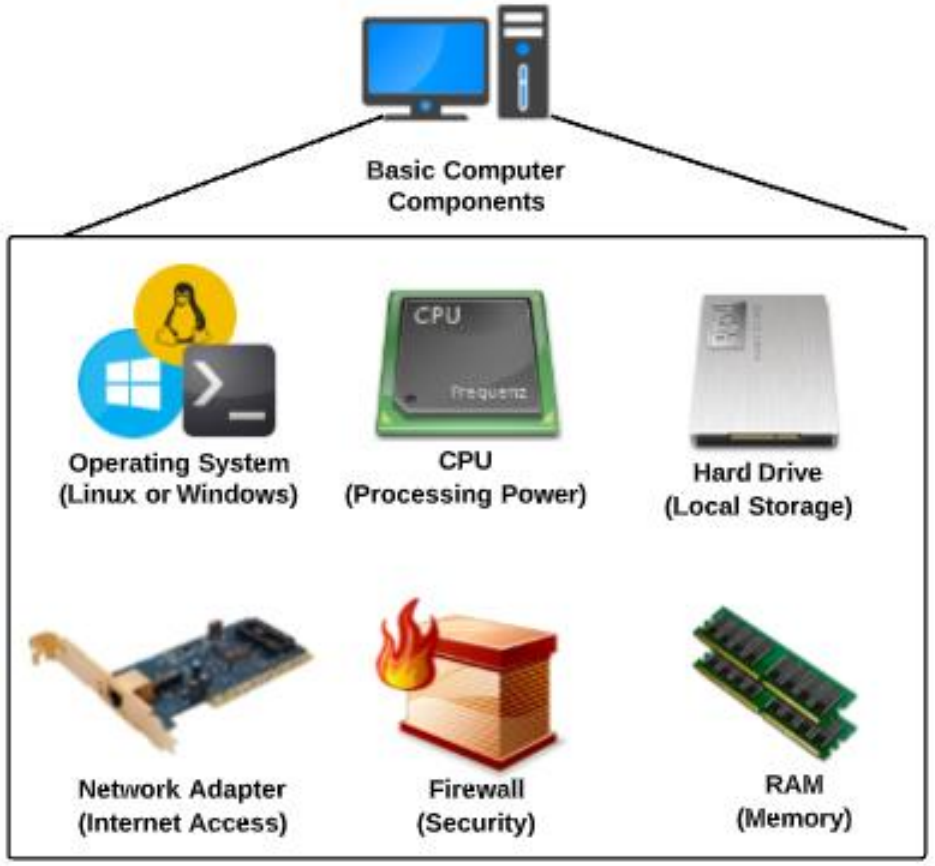
• Amazon services de calcul

Amazon Elastic Compute Cloud (Amazon EC2) est un service Web qui fournit une capacité de calcul sécurisée et redimensionnable dans le cloud sous forme de **machines virtuelles**. L'utilisation d'Amazon **EC2** vous dispense d'investir à l'avance dans du matériel et, par conséquent, vous pouvez développer et déployer les applications plus rapidement. Amazon **EC2** vous permet d'augmenter ou de diminuer l'échelle afin de gérer les modifications en termes d'exigences ou de pics de popularité, et réduire ainsi le besoin de prévoir le trafic.

- Environnements de calcul virtuels, appelés instances
- Modèles préconfigurés pour vos instances, appelés Amazon Machine Images (AMI)
- Diverses configurations de capacité d'UC de mémoire, de stockage et de mise en réseau
- Sécuriser les informations de connexion de vos instances à l'aide de paires de clés
- Volumes de stockage pour les données temporaires qui sont supprimées lorsque vous arrêtez
- Volumes de stockage permanents pour vos données à l'aide d'Amazon Elastic Block Store (EBS)

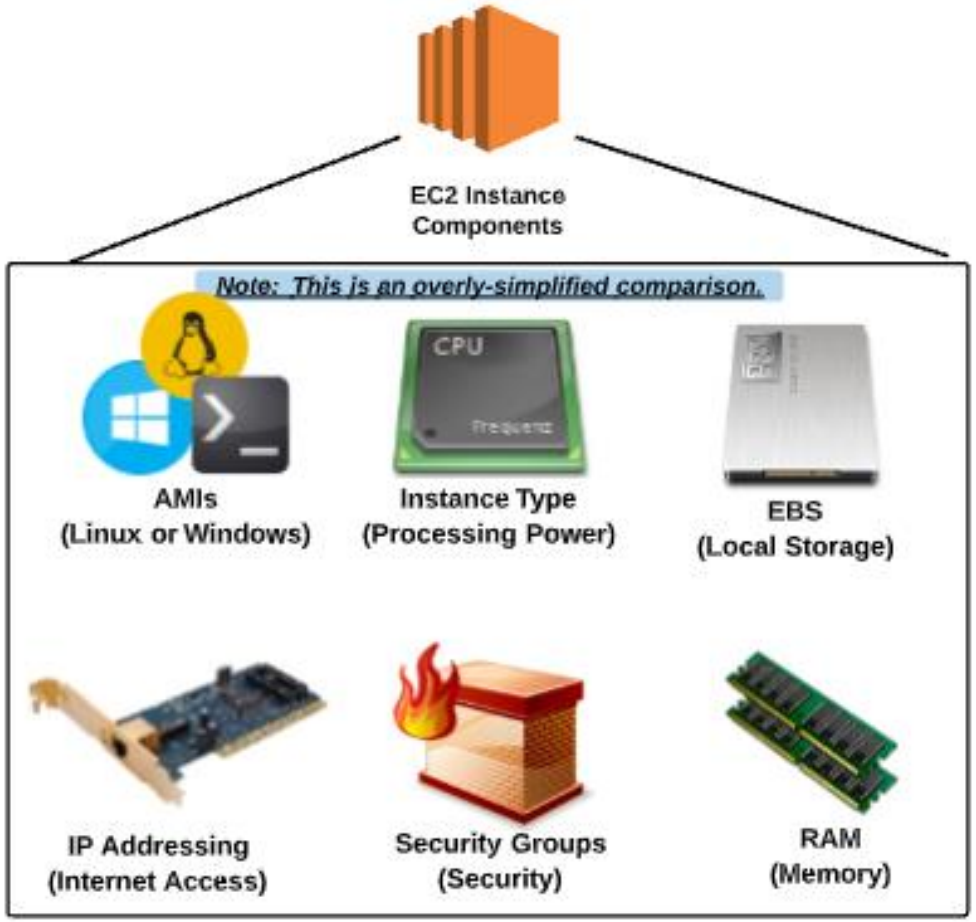
- Amazon services de calcul

Amazon Elastic Compute Cloud (Amazon EC2): Comprendre conceptuellement le service EC2

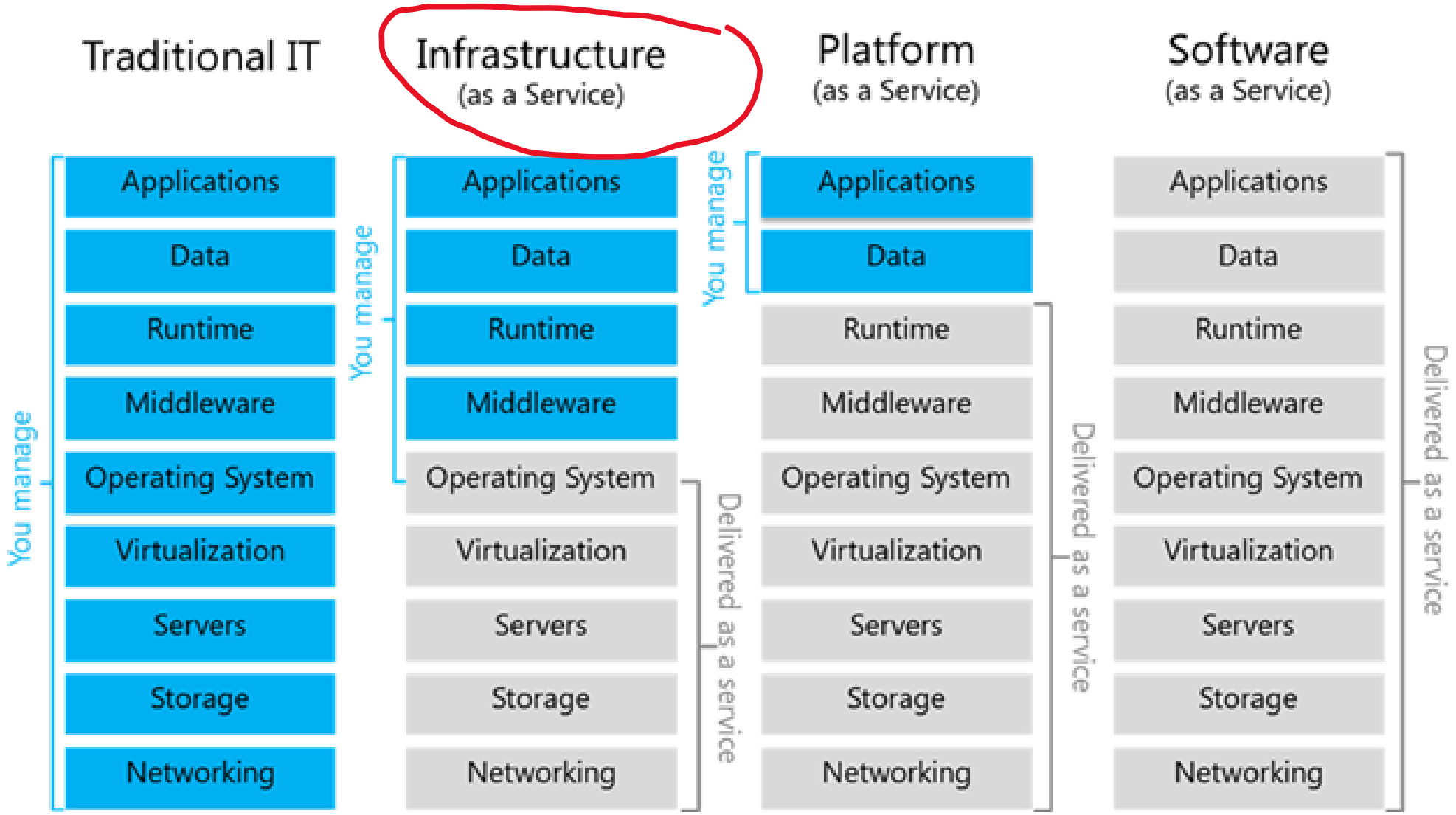


- Amazon services de calcul

Amazon Elastic Compute Cloud (Amazon EC2): Comprendre conceptuellement le service EC2



Amazon services de calcul



Amazon services de calcul

Tarification Amazon EC2:

- Il existe cinq méthodes de paiement pour les instances Amazon EC2 : les instances à la demande, les Savings Plans, les instances réservées et les instances Spot. Vous pouvez également payer des hôtes dédiés qui vous fournissent des capacités d'instance EC2 sur des serveurs physiques dédiés à votre utilisation.

Offre gratuite :

- L’offre gratuite AWS comprend **750 heures** d’instances Linux et Windows **t2.micro**, (**t3.micro** pour les régions dans lesquelles **t2.micro** n'est pas disponible) chaque **mois** pendant **un an**. Pour rester dans le cadre de l'offre gratuite, vous devez **uniquement** utiliser des **micro-instances EC2.**

Amazon services de calcul

A la demande (On demand)

Grâce aux instances **à la demande**, vous **payez une capacité de calcul à l'heure ou à la seconde** en fonction des instances que vous exécutez. **Aucun engagement à long terme ni frais initiaux ne sont requis**. Vous pouvez **augmenter** ou **diminuer** votre capacité de calcul en fonction des demandes de votre application et **ne payer que les tarifs horaires spécifiés** pour l'instance que vous avez **utilisée**.

Les instances à la demande sont recommandées pour :

- Les utilisateurs préférant profiter du coût avantageux et de la flexibilité d'Amazon EC2 sans engagements à long terme ou paiements initiaux
- Les applications ayant des charges de travail à court terme, irrégulières ou imprévisibles ne pouvant pas être interrompues
- Les applications développées ou testées sur Amazon EC2 pour la première fois.

Amazon services de calcul

Engagement consommation (Savings Plan)

- La tarification **Savings Plans** est un modèle de tarification flexible qui permet une utilisation **EC2 à bas prix** en **échange d'un engagement à une consommation régulière** (**mesurée en USD/heure**) sur une période **d'un ou trois ans**.
- Les tarifs sont **inférieurs** à la tarification à la **demande** en échange d'un **engagement** d'utilisation donné. Les EC2 Instance **Savings Plans** offrent **jusqu'à 72 % d'économies** par rapport à la tarification à la demande sur l'utilisation des instances Amazon EC2.
- L'engagement horaire peut être calculé sur la base de **l'historique d'utilisation à la demande.** Il est recommandé de se lancer dans une tarification Savings Plan avec **au minimum 1 an** d'utilisation AWS avec une tarification **on demand**.

Amazon services de calcul

Instances Spot

Les instances **Spot Amazon EC2** vous permettent **d'enchérir** sur les capacités de calcul Amazon EC2 **non utilisées** pour économiser jusqu'à **90 % du prix des instances à la demande**. En savoir plus.

Les prix spot sont définis par Amazon EC2 et **ajustés graduellement** en fonction des tendances à long terme en matière **d'offre et de demande** de capacité d'instance Spot. Consultez la page de l'historique des instances Spot.

Les instances Spot sont recommandées pour :

- les applications dont les heures de début et de fin d'exécution sont flexibles
- les applications réalisables uniquement à des prix de calcul extrêmement faibles
- les utilisateurs ayant des besoins de calcul urgents pour de grandes quantités de capacité supplémentaires
- Les applications non critiques pour le business

Amazon services de calcul

Hôtes dédiés

- Un hôte **dédié** est un **serveur EC2 physique dédié** à votre utilisation. Les hôtes dédiés peuvent vous aider à réduire les coûts en vous permettant d'utiliser vos **licences existantes de logiciels** liés aux serveurs, notamment Windows Server, SQL Server et SUSE Linux Enterprise Server (sous réserve des conditions de votre licence), et peuvent également vous aider à répondre aux **exigences de conformité**.
  - Possibilité d'achat à demande (à l'heure),
  - Possibilité d'achat sous forme de réservation,
- Une réservation d'hôte dédié vous permet de bénéficier d'une remise pouvant aller jusqu'à 70 % par rapport à la tarification à la demande.

Amazon services de calcul

Amazon Machine Image (AMI)

Un **package** (Image) préconfiguré nécessaire pour lancer **EC2** qui comprend un **système d'exploitation**, des packages **logiciels** et d'autres paramètres essentiels.

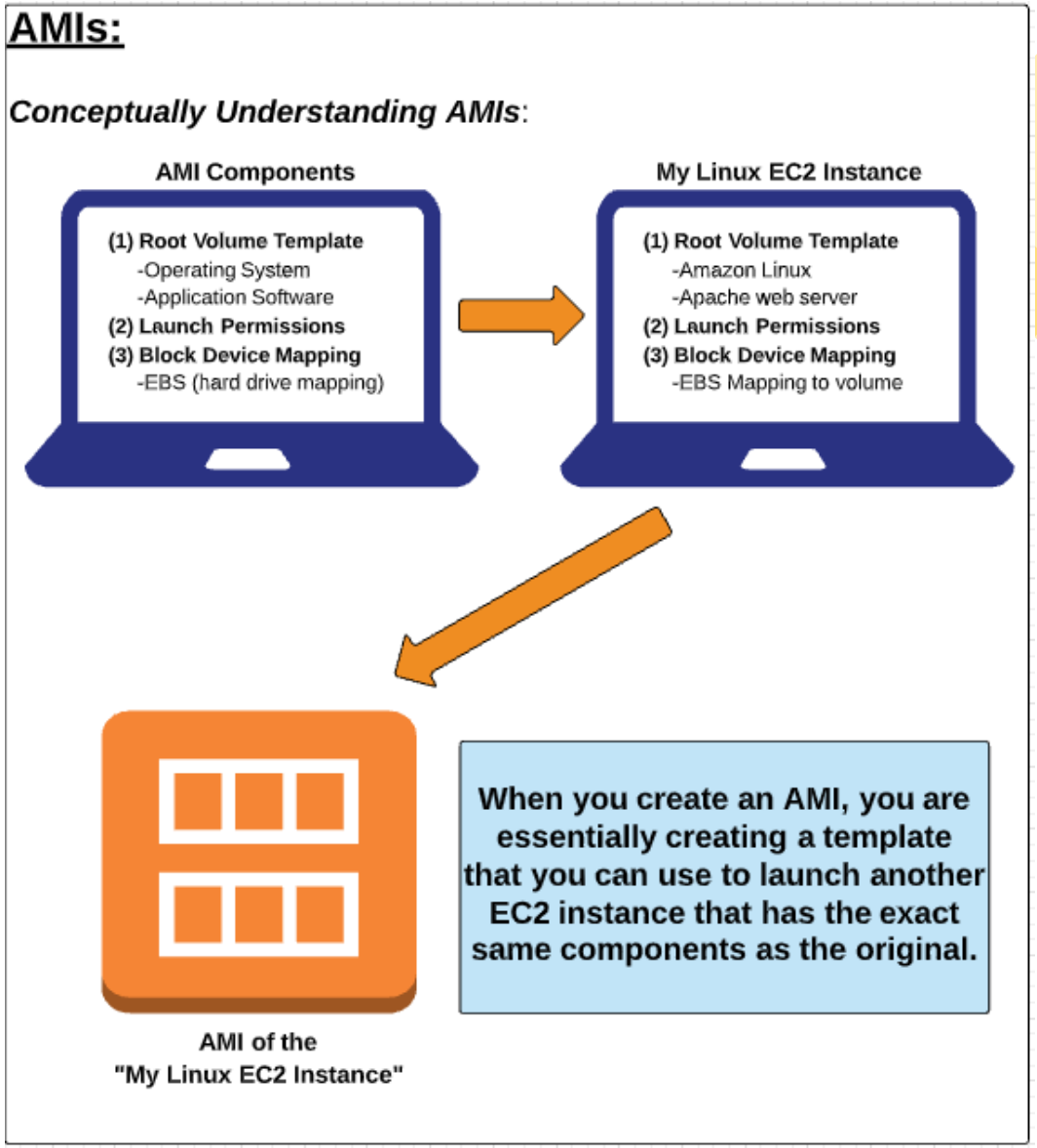
Une AMI comprend les éléments suivants :

- Un **système d'exploitation** Linux ou Windows
- Un ou plusieurs instantanés **Amazon Elastic Block Store** (Amazon EBS) ou **le stockage d'instance**
- **Les autorisations** de lancement qui contrôlent les comptes AWS qui peuvent utiliser l'AMI pour lancer les instances.
- **Un mappage de périphérique de stockage** en mode bloc qui spécifie les volumes à attacher à l'instance lorsqu'elle est lancée.

- Amazon services de calcul

Amazon Machine Image (AMI)

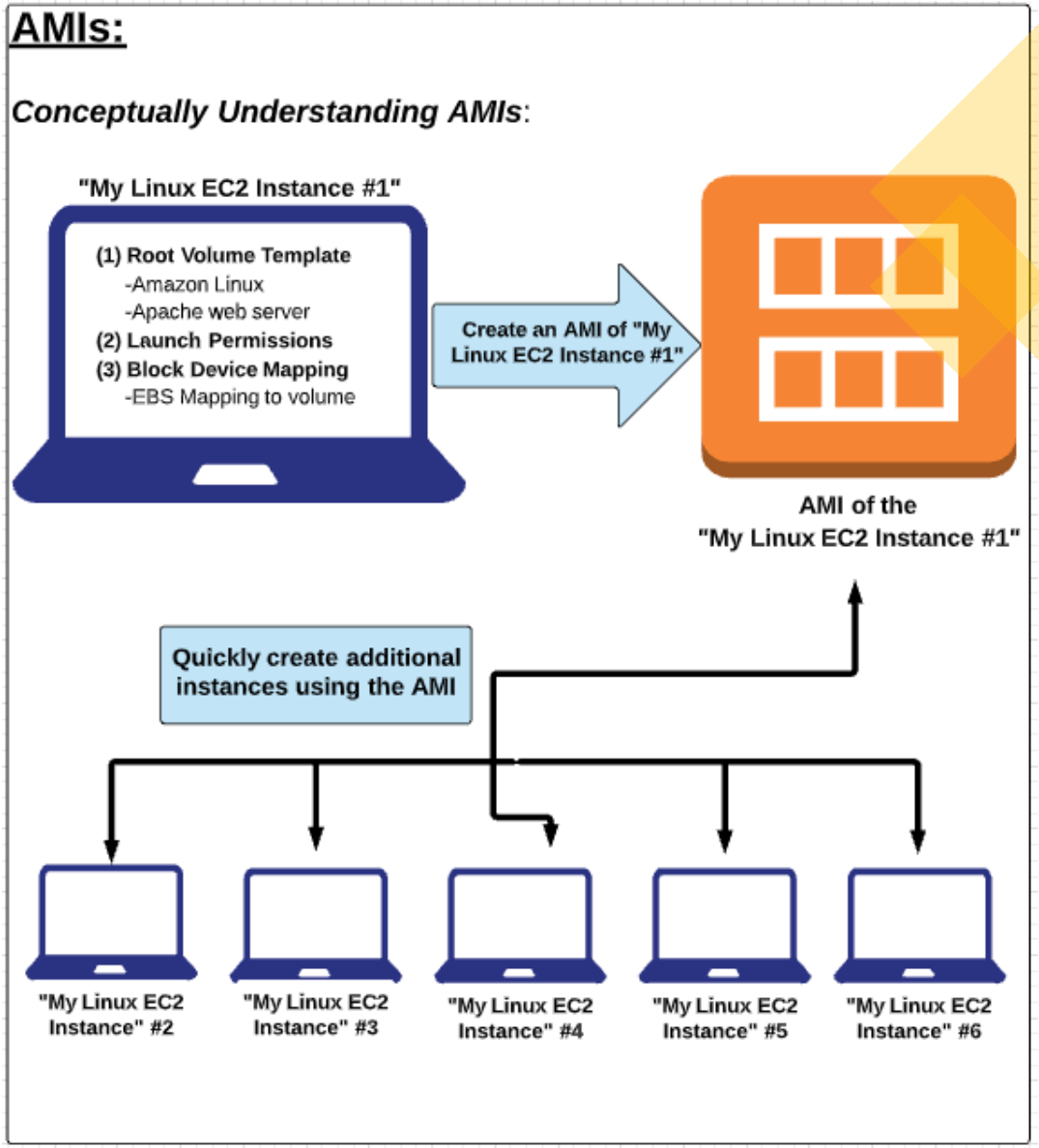
- Un template qui fournit les informations requises pour lancer une instance.
- Vous devez spécifier une AMI lorsque vous lancez une instance



Amazon services de calcul

Amazon Machine Image (AMI)

- Lorsque vous avez besoin de plusieurs instances configurées de manière identique, il est possible de lancer plusieurs instances à partir d'une même AMI.



Amazon services de calcul

Amazon Machine Image (AMI)

On retrouve 3 catégories d'AMI:

Community AMI

- Gratuite
- Généralement, elle embarque uniquement l'OS

AWS Marketplace AMI

- Payant à l'usage
- Embarque un logiciel sous licence

MY AMI

- **AMI** que vous créez

Allez sur la console AWS, Service EC2, lancez une instance. Pour découvrir les différentes AMIs.

Amazon services de calcul

Type d'instance EC2

Lorsque vous lancez une instance, **le type d'instance** que vous spécifiez détermine les capacités **matérielles** de l'ordinateur hôte utilisé pour votre instance. Chaque **type d'instance** propose différentes **capacités de calcul, de mémoire et de stockage**, et est **regroupé dans une famille** d'instance en fonction de ces capacités. Sélectionnez un type d'instance en fonction des exigences de l'application ou du logiciel que vous prévoyez d'exécuter sur votre instance.

les **Familles d'instances** correspondent à des **types d'usages**. Chaque **famille** propose un ensemble de **combinaisons** en termes de **CPU, RAM, Stockage et mise en réseau** qui vous permet de facilement choisir un ensemble de ressources parfaitement **adapté** à vos applications.

Pour découvrir le catalogue d'instances EC2, Cliques-ici.

Allez sur la console AWS, Service EC2, lancez une instance, choisissez une Community AMI, pour découvrir le catalogue des instances EC2

Amazon services de calcul

Elastic Block Store (EBS)

Amazon EBS fournit des volumes de **stockage de niveau bloc** que vous pouvez attacher à une instance en cours d'exécution. Vous pouvez utiliser **Amazon EBS** comme périphérique de **stockage principal** pour les **données nécessitant des mises à jour fréquentes et précises**.

Par exemple, Amazon EBS est l'option de stockage recommandée lorsque vous exécutez une base de données sur une instance.

- Le volume **EBS** persiste **indépendamment** de la durée d'exécution d'une instance. Une fois qu'un volume **EBS** est attaché à une instance, vous pouvez l'utiliser comme n'importe quel autre **disque dur physique.**
- Pour conserver une **copie de sauvegarde** de vos données, vous pouvez créer un ***instantané*** **(Snapshot)** d'un volume **EBS** qui est stocké dans **Amazon S3.** Vous pouvez créer un volume **EBS** à partir d'un **instantané**, puis l'attacher à une autre instance.
- Un **snapshot** d'un volume EBS est une **copie des données** dans le volume sur Amazon S3, où elles sont stockées de façon **redondante** dans plusieurs zones de disponibilité.

Amazon services de calcul

Elastic Block Store (EBS)

Amazon EBS fournit les types de volumes suivants :

- **Les volumes SSD à usage général** (gp2 et gp3), bon compromis en termes de prix et de performances pour un large éventail de charges de travail **transactionnelles**. Ils conviennent parfaitement aux cas d'utilisation tels que les volumes de démarrage, les bases de données de taille moyenne, ainsi que les environnements de développement et de test.
- **Les volumes provisionnés IOPS (io1 et io2)** sont conçus pour satisfaire les besoins des charges de travail très consommatrices **d'I/O** qui sont sensibles aux performances et à l'homogénéité du stockage. Ils fournissent **un taux d'IOPS** cohérent que vous spécifiez lorsque vous créez le volume.
- **Les volumes HDD optimisés pour le débit (st1)** offrent un stockage **magnétique** économique qui définit les performances en termes de **débit** plutôt que **d'IOPS**. Ce type de volume convient aux charges de travail séquentielles et volumineuses comme les Data warehouse le traitement des logs.
- **Les volumes HDD à froid (sc1)** offrent un stockage **magnétique** économique qui définit les performances en termes de **débit** plutôt que **d'IOPS**. Ces volumes conviennent à des charges de travail volumineuses et séquentielles de données légères et que vous n'avez pas besoin d'accéder souvent à vos données

Amazon services de calcul

Elastic Block Store (EBS)

Deux maniéres de créer un volume EBS:

1. Allez sur la console AWS, Service EC2, lancez une instance, choisissez une Community AMI,Selectionnez une instance t2.micro, cliquez sur add storage puis add new volume.

2. Allez sur la console AWS, Service EC2, cliquez sur Volumes puis cliquez sur create volume.

Amazon services de calcul

AWS Security group (SG)

Un *groupe de sécurité* agit en tant que **pare-feu virtuel** pour vos instances **EC2** afin de c**ontrôler le trafic entrant et sortant**. Les **règles entrantes** contrôlent le trafic entrant vers votre instance, et **les règles sortantes** contrôlent le trafic sortant de votre instance.

Lorsque vous lancez une instance, vous pouvez spécifier **un ou plusieurs groupes de sécurité**. Si vous ne spécifiez pas de groupe de sécurité, Amazon EC2 utilise le groupe de sécurité par **défaut**. Vous pouvez ajouter des règles à chaque groupe de sécurité pour autoriser le trafic vers ou depuis ses instances associées.

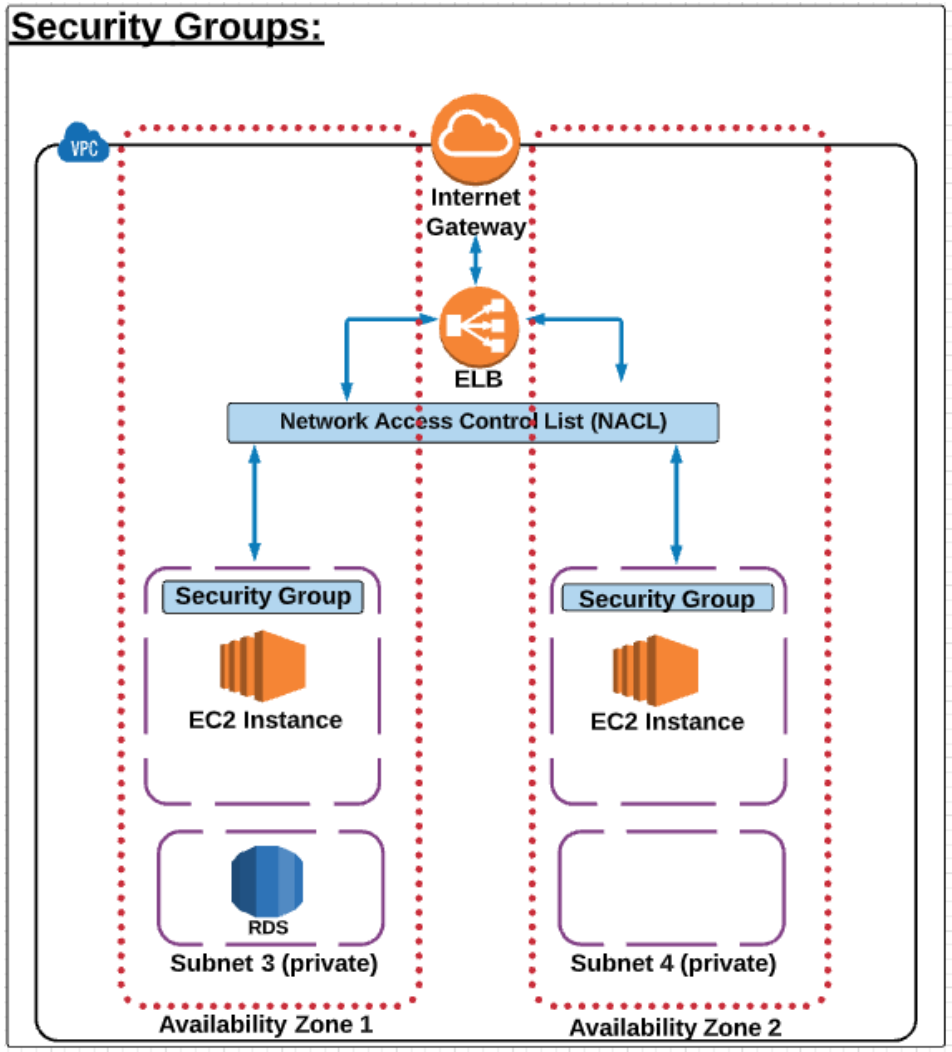
La différence entre le **NACL** et **SG**, le **NACL** agit au niveau d'un **zone de disponibilit**é alors que le **SG** agit au niveau du **service** comme **EC2**.

Amazon services de calcul

AWS Security group (SG)

AWS fournit des groupes de sécurité comme un des outils permettant de sécuriser vos instances ; vous devez les configurer pour répondre à vos besoins en matière de sécurité.

Dans notre cas on doit attacher un groupe de securité pour chaque instance EC2 pour contrôle le traffic entrant et sortant.



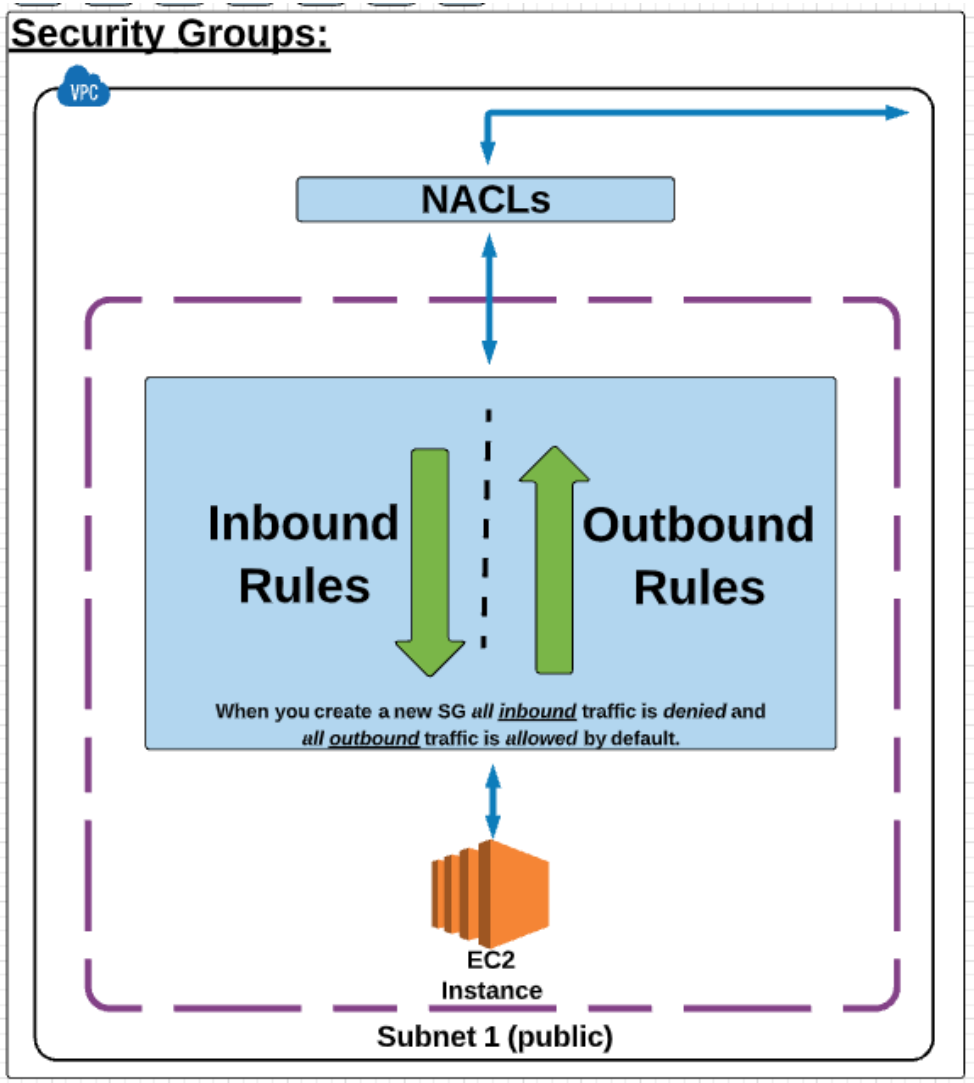
Amazon services de calcul

AWS Security group (SG)

Les règles d'un groupe de sécurité contrôlent le trafic entrant autorisé à atteindre les instances associées au groupe de sécurité. Les règles contrôlent également le trafic sortant autorisé à les quitter.

Lorsque vous créez un groupe de sécurité des régles de sécurité par defaut s'appliquent au SG.

- Tout trafic entrant est interdit
- Tout trafic sortant est autorisé



Amazon services de calcul

AWS Security group (SG)

Sur la console aws:

- Cliquez sur le service EC2, puis allez dans Network & Security et cliquez sur sécurity group
- Vous allez remarquer, qu'il existe un groupe de sécurité par defaut
- Pour créer un nouveau group de sécurité, cliquez sur Create security group
- Ajoutez les regles de trafic entrant

Http – tcp - 80 – custom – 0.0.0.0/0

- Ajoutez les regles de trafic sortant

All traffic – all – all- all – security group

Amazon services de calcul

Adressage IP pour EC2:

Par defaut à la création d'une instance EC2 une adresse **privée** est allouée, il est possible d'ajouter une adresse **publique** si votre **VPC/subnets** le permet.

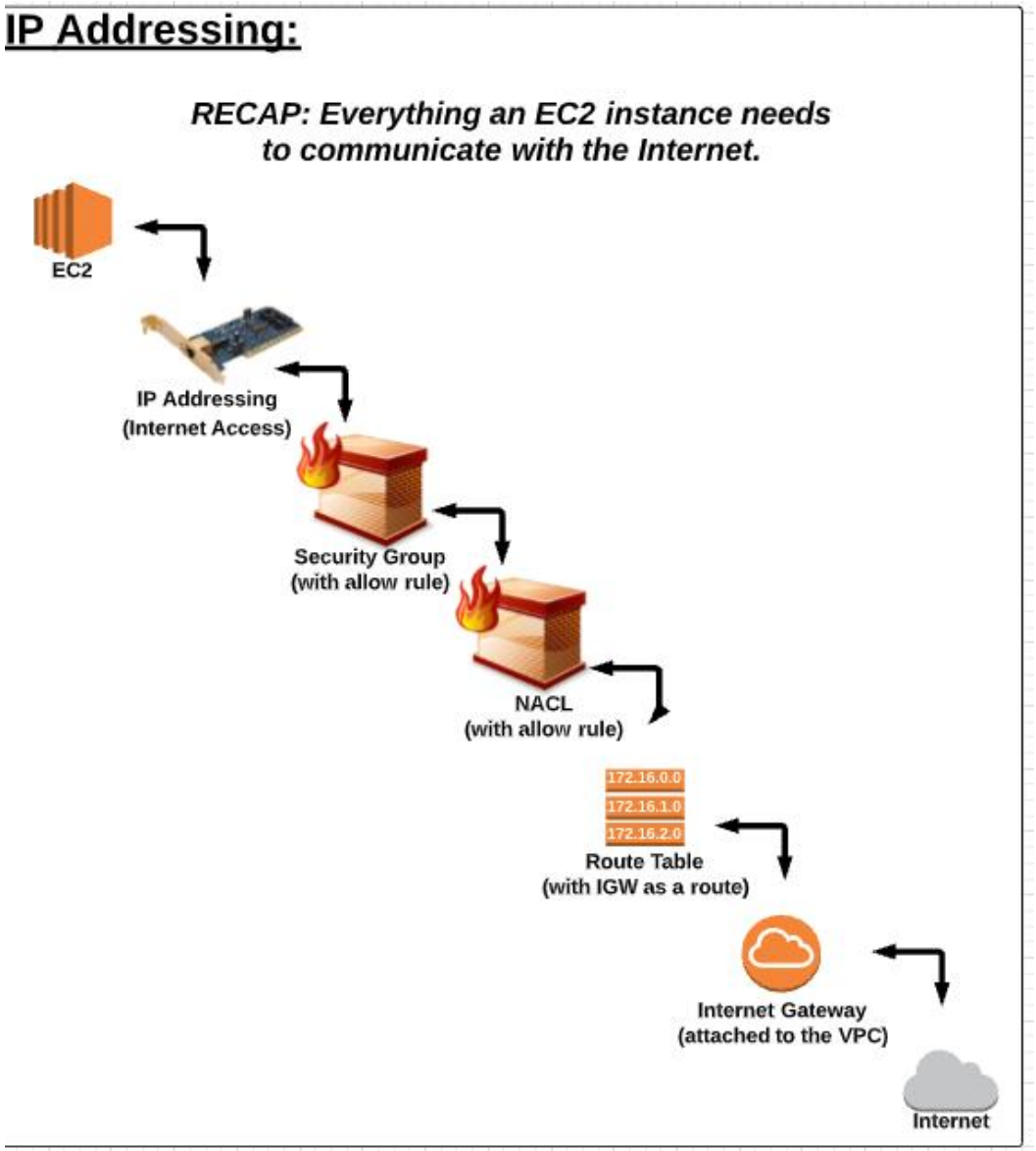
Adresses IPv4 privées et noms d'hôte DNS internes

- Une adresse IPv4 privée est une adresse IP qui ne peut pas être atteinte via Internet. Vous pouvez utiliser des adresses IPv4 privées et un nom d'hôte DNS interne pour toute communication entre des instances du même VPC.

Adresses IPv4 publiques et noms d'hôte DNS externes

- Une adresse IP publique est une adresse IPv4, qui est accessible depuis Internet. Vous pouvez utiliser des adresses publiques pour les communications entre vos instances et Internet.

Amazon services de calcul



Amazon services de calcul

Démarrer et se connecter à une EC2

Allez sur la console aws, cliquez sur le service VPC:

1. Vérifiez que une **IGW** est attachée à votre **VPC**
2. Vérifiez dans **routes tables**, que vous avez une route avec **IGW** et une route sans **IGW,** vérifiez l'association des **subnets** pour chaque Route table.
3. Vérifier que vous avez 2 NACL, 1 avec un **Traffic autorisé** et un autre avec un **Traffic interdit** (Vérifiez les subnets associés à chaque NACL)

Cliquez sur le service EC2:

1. Vérifiez que votre **security group** est correctement configuré. (autorise ssh depuis votre pc et HTTP pour tout le monde)

Amazon services de calcul

Démarrer et se connecter à une EC2

Cliquez sur Démarrer une EC2:

1. Selectionnez une AMI (community AMI – LAMP)
2. Selectionnez un type d'instance (t2.micro)
3. Configurez l'instance: On ajoute un script qui va s'exécuter au démarrage pour installer apache.
   ```
   #!/bin/bash
   yum update -y
   yum install –y httpd
   service http start
   ```
4. Ajoutez un stockage (pour l'instant on utilise le stockage par defaut)
5. Ajouter des tage (name: webserver)
6. Configurez un SG pour autoriser un trafic entrant SSH pour 22 et HTTP port 80 (0.0.0.0/0)
7. Vérifiez la configuration de la machine et lancer la création
8. Créez et téléchargez la **Key Pair**

Amazon services de calcul

En utilisant un client ssh comme Mobaxterm sur windows (utilisez le terminal directement pour les machines Mac et Linux), connectez-vous à la machine en ssh.

1. Cliquez sur connect sur la console AWS
2. Vérifiez les permissions de votre Key Pair (chmod 400)
3. Connectez-vous en utilisant la commande ssh (**Ssh –i "keypair.pem" public-dns-ec2)**
4. Vérifiez que le service HTTP est installé
5. Vérifiez que le server apache fonction (public-ip:80)
6. Vérifiez que les règles NACL autorise le trafic entrant/sortant sur le port 80.

projet Omega

AWS EC2 workshop:

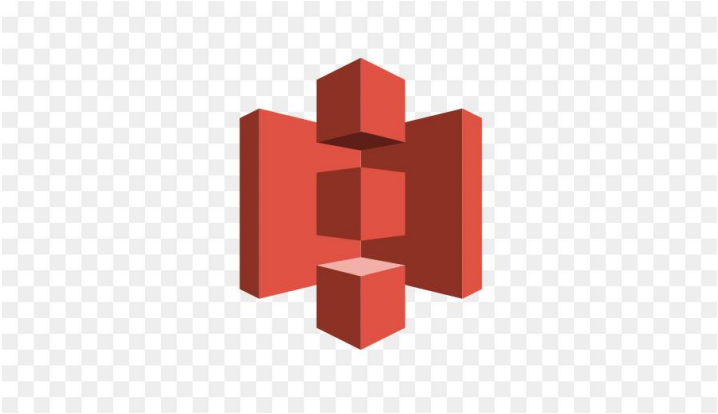
https://github.com/atifrani/ec2_webapp

https://github.com/atifrani/aws_ec2_webapp

projet Omega

- Infrastructure AWS requise:
  1. Un Compte AWS
  2. Des comptes utilisateurs pour l'équipe de développement avec des accès aux services AWS
  3. Un routage approprié du trafic vers et depuis notre cloud virtuel privé VPC AWS
  4. Un emplacement pour le stockage en masse des fichiers
  5. Des servers pour héberger le projet
  6. Une base de données pour stocker et cataloguer les données
  7. Un service de notification (Mail ou sms) pour l'équipe du projet, basé sur les événements d'infrastructure
  8. Un service pour monitorer le projet et l'infrastructure du projet
  9. Automatiser le processus de distribution du trafic entrant entre les ressources AWS du projet Omega
  10. Automatiser le processus de scaling up ou scaling down des ressources AWS du projet Omega
  11. Mettre en place et configurer un domaine web qui pointe vers l'infrastructure de projet Omega
  12. Tester la possibilité d'utiliser des ressources de type serveless pour le projet Omega

- Amazon Simple Storage Service S3



- Introduction à S3
- Tarification service S3
- Gestion des Buckets, Répertoires et Objets
- Chargement et téléchargement des objets
- Les classes de sotckages S3
- La gestion du Cycle de vie d'un Objet
- Gestion des permissions
- Versionning des Objets

Amazon Simple Storage Service S3

Introduction à S3

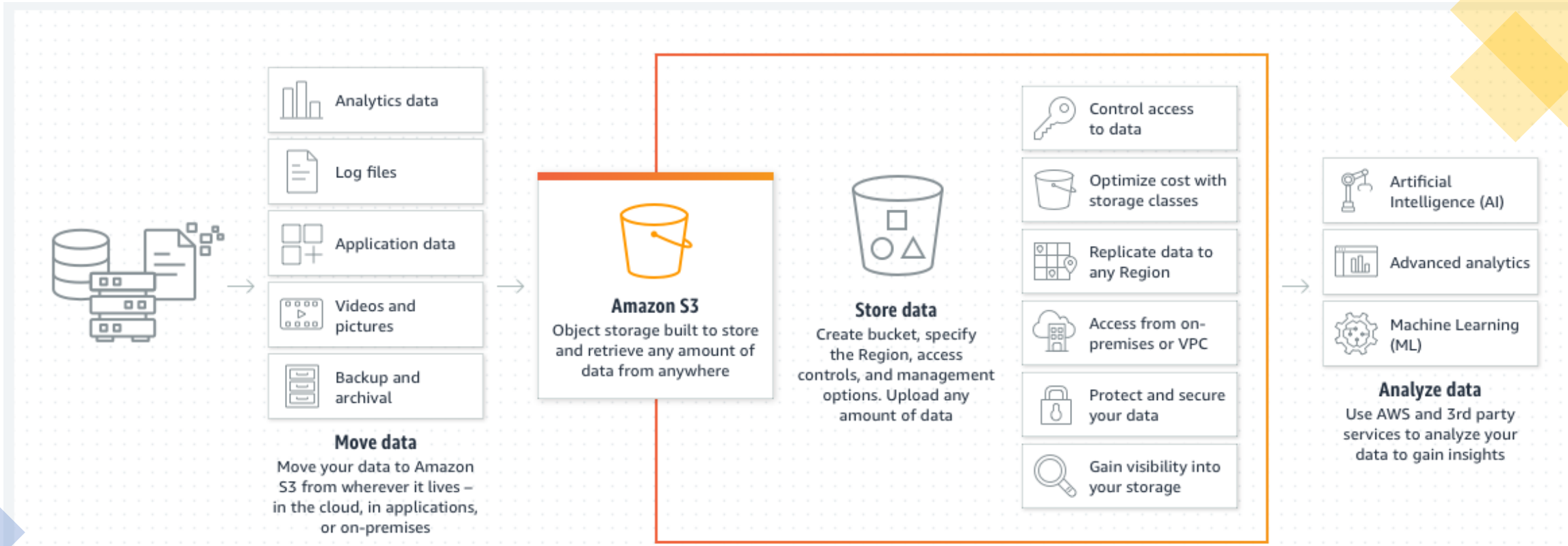
Amazon **S3** est un **services web** qui vous permet de **stocker et de récupérer** n'importe quelle quantité de données, à tout moment, **de n'importe où sur Internet**. Il permet aux développeurs d'accéder à la même infrastructure de stockage de données **hautement évolutive, fiable, rapide, peu coûteuse** qu'Amazon utilise pour faire fonctionner son propre réseau mondial de sites. Ce service vise à maximiser les avantages d'échelle et à en faire bénéficier les développeurs.

Bucket S3: Stockage niveau racine. Peut contenir des répertoires ou des objets

Répertoire S3: sous répertoire pour mieux organiser le stockage des objets

Objet S3: Tout fichiers stockés dans S3 sont des objets

Amazon Simple Storage Service S3



• Amazon Simple Storage Service S3

Introduction à S3

Connectez-vous à la console AWS et choisissez le service S3

1. Cliquez sur create bucket
2. Renseignez le nom du bucket (unique et lowercase: omega+initial)
3. Choisissez une région, next
4. Découvrez les options proposées, next
5. Dans permissions, faire attention pour l'accès public au bucket, next
6. Cliquez sur create bucket
7. Créez un répertoire 'dev'

Maintenant, vous pouvez stocker des données dans votre bucket S3

Amazon Simple Storage Service S3

Tarification service S3

Vous devez prendre en compte six éléments de coûts Amazon S3 lors du stockage et de la gestion de vos données :

1. la tarification du stockage,
2. la tarification des requêtes et de l'extraction des données,
3. la tarification du transfert des données et de l'accélération du transfert des données,
4. la tarification de la gestion et de l'analytique des données,
5. La tarification de la réplication des données,
6. le coût de traitement de vos données (exemple avec Lambda).

Pour découvrir les tarifications, cliques-ici

Amazon Simple Storage Service S3

Les classes de stockages S3

Dans Amazon S3, chaque objet possède une **classe de stockage** qui lui est associée, par défaut, la classe de stockage est **Standard**.

Amazon S3 offre une plage de classes de stockage pour les objets que vous stockez. Chaque classe de stockage est une classification de l'objet stocker selon différents paramètres (cas d'utilisateur, performance d'accès, fréquence d'accès, disponibilité, durabilité…)

- La classe de stockage d'un objet peut être spécifie à la création (standard par défaut)
- Vous pouvez modifier la classe de stockage d'un objet
- La tarification S3 varie en fonction de la classe de stockage

Le tableau suivant compare les classes de stockage.

Allez sur la console AWS, S3 et regardez la classe de stockage de votre objet.

Amazon Simple Storage Service S3

Gestion du cycle d'un objet S3

Pour **gérer vos objets** afin qu'ils soient stockés de **manière rentable** tout au long de leur **cycle de vie**, configurez leur *cycle de vie Amazon S3*. Une *configuration du **cycle de vie S3*** est un **ensemble de règles** définissant les actions appliquées par Amazon S3 à un groupe d'objets. Il existe deux types d'actions :

- **Actions de transition** - Définissez à quel moment les objets effectuent la **transition** vers une autre **classe de stockage**. Par exemple, vous pouvez choisir d'effectuer la transition des objets de la classe de stockage **S3 standard** vers classe de stockage **S3 Glacier** un an après leur création pour les archiver.

- **Actions d'expiration** - Définissez la date d'expiration des objets. Amazon S3 supprime les objets expirés à votre place. Les coûts d'expiration de cycle de vie dépendent du moment où vous choisissez de faire expirer des objets.

Amazon Simple Storage Service S3

Gestion du cycle d'un objet S3

Allez sur la console AWS, choisissez le service S3

1. Cliquez sur votre bucket et puis sur l'onglet **management**
2. Cliquez sur **ajouter un cycle de vie**
3. Entrez un nom pour la **règle**
4. Sélectionnez **current version**
5. Sélectionnez **Transition** to Standard-IA after 30 days (minimum 30 jours)
6. Ajoutez **Transition** to Amazon Glacier after 90 days, next
7. On ne va pas configurer d'expiration, next
8. Save

Amazon Simple Storage Service S3

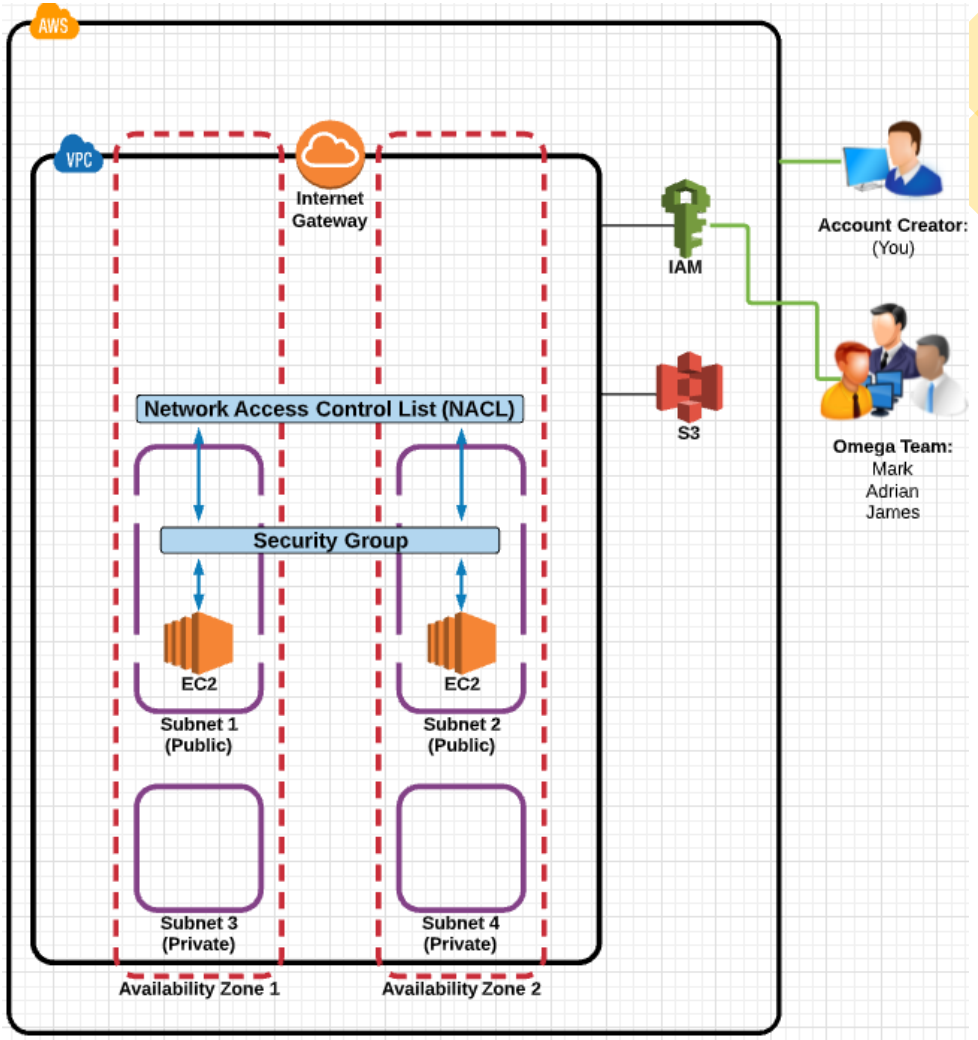
Gestion des permissions S3

Par défaut, toutes l**es ressources Amazon S3**, compartiments, objets et sous-ressources qui y sont liées sont **confidentielles**. Seul le **propriétaire** de la ressource, le compte AWS qui l'a créé, peut accéder à la ressource. Le **propriétaire** de la ressource **peut éventuellement accorder des autorisations** d'accès à d'autres personnes en rédigeant une stratégie d'accès.

Dans le cadre du projet **Omega**, on souhaite autoriser le groupe **Dev** à accéder à la ressource de stockage et au bucket.

Deux manières de faire:

- En mettant le bucket ou l'objet en **public**
- Autoriser le groupe **Dev (Ajout d'un role/stratégie)**



Amazon Simple Storage Service S3

Versionning des Objets S3

La gestion des versions est un moyen de conserver plusieurs variantes d'un objet dans le même compartiment. Vous pouvez utiliser le contrôle de version pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3.

Si vous activez la gestion des versions pour un compartiment, Amazon S3 génère automatiquement un ID de version unique pour l'objet stocké. Dans un compartiment, par exemple, vous pouvez avoir deux objets avec la même clé, mais différents ID de version, comme photo.gif (version 111111) et photo.gif (version 121212).

Le versionning s'applique au niveau du bucket.

Amazon Simple Storage Service S3

Allez sur la console aws et choisissez le service S3.

1. Cliquez sur votre bucket
2. Dans propriétés, activez la gestion de version
3. Chargez un fichier texte vide toto.txt dans votre bucket
4. Vérifiez la version du fichier toto.txt
5. Modifiez le contenu du fichier toto.txt localement
6. Rechargez le fichier toto.txt et vérifiez les versions du fichier

projet Omega

- Infrastructure AWS requise:
  1. Un Compte AWS
  2. Des comptes utilisateurs pour l'équipe de développement avec des accès aux services AWS
  3. Un routage approprié du trafic vers et depuis notre cloud virtuel privé VPC AWS
  4. Un emplacement pour le stockage en masse des fichiers
  5. Des servers pour héberger le projet
  6. Une base de données pour stocker et cataloguer les données
  7. Un service de notification (Mail ou sms) pour l'équipe du projet, basé sur les événements d'infrastructure
  8. Un service pour monitorer le projet et l'infrastructure du projet
  9. Automatiser le processus de distribution du trafic entrant entre les ressources AWS du projet Omega
  10. Automatiser le processus de scaling up ou scaling down des ressources AWS du projet Omega
  11. Mettre en place et configurer un domaine web qui pointe vers l'infrastructure de projet Omega
  12. Tester la possibilité d'utiliser des ressources de type serveless pour le projet Omega

AWS CLI

Installation de AWS CLI

https://docs.aws.amazon.com/fr_fr/cli/latest/userguide/install-windows.html

Configuration de AWS CLI

https://docs.aws.amazon.com/fr_fr/cli/latest/userguide/cli-configure-quickstart.html

AWS CLI

AWS S3 CLI : Les bases de la gestion des compartiments S3 et de ses objets à l'aide d'aws s3 cli :

1. Créer un bucket S3:

aws s3 mb s3://omegaat2 --region eu-west-1

2. Lister les bucket S3

aws s3 ls

aws s3 ls s3://omegaat

aws s3 ls s3://omegaat --recursive

aws s3 ls s3://omegaat --recursive --human-readable –summarize

3. Supprimer un bucket S3

aws s3 rb s3://omegaat2

aws s3 rb s3://omegaat2 --force

AWS CLI

4. Copier dans S3

aws s3 cp getdata.php s3://omegaat2

aws s3 cp webapp/app/index.php s3://omegaat2 --recursive

aws s3 cp s3://omegaat2/index.php webapp/app/

aws s3 cp webapp/ s3://omegaat2--recursive

aws s3 cp s3://omegaat2 /index.php s3://backup-bucketat

aws s3 cp s3://omegaat2 s3://backup-bucketat --recursive

4. Déplacer dans S3

aws s3 mv getdata.php s3://omegaat2
aws s3 mv webapp/app/index.php s3://omegaat2 --recursive
aws s3 mv s3://omegaat2/index.php webapp/app/
aws s3 mv webapp/ s3://omegaat2--recursive
aws s3 mv s3://omegaat2 /index.php s3://backup-bucketat
aws s3 mv s3://omegaat2 s3://backup-bucketat --recursive

AWS CLI

AWS ec2 CLI : Les bases de la gestion des machines ec2 et de ses objets à l'aide d'aws ec2 cli :

1. Lister les instances ec2

aws ec2 describe-instances

2. Démarrer une instance

aws ec2 start-instances --instance-ids i-dddddd70

3. Stopper une instance

aws ec2 stop-instances --instance-ids i-5c8282ed

4. Terminer une instance

aws ec2 terminate-instances --dry-run --instance-ids i-dddddd70

AWS CLI

5. Lancer une instance:

aws ec2 run-instances

--image-id ami-*xxxxxxxx*

--security-group-ids xxxxxxxxx

--instance-type *t2.micro*

--key-name example-key

Amazon Simple Storage Service S3

AWS S3 workshop:

https://github.com/atifrani/aws_s3_static_website

- Amazon Relational Database Service

- Introduction à RDS
- Type de base de données RDS (SQL, NOSQL)
- Tarification service RDS
- Lancer une base de données RDS

Amazon Relational Database Service

Introduction à RDS:

- Amazon Relational Database Service (Amazon RDS) vous permet d'installer, de gérer et de mettre à l'échelle facilement une base de données relationnelle dans le cloud. Ce service offre une capacité économique et ajustable ainsi qu'une automatisation des tâches administratives chronophages, telles que l'allocation de matériel, le paramétrage de bases de données, l'application de correctifs et les sauvegardes. Vous pouvez ainsi vous concentrer librement sur vos applications, afin de leur donner les performances rapides, la haute disponibilité, la sécurité et la compatibilité dont elles ont besoin.
- Amazon RDS est disponible sur plusieurs types d'instances de base de données, optimisées pour la mémoire, les performances ou les I/O. Amazon RDS vous donne le choix entre six moteurs de base de données communs, notamment Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle Database, et SQL Server.
- Vous pouvez utiliser AWS Database Migration Service pour migrer ou répliquer facilement vos bases de données existantes sur Amazon RDS.

Amazon Relational Database Service

Introduction à RDS:

Dans le monde des bases de données, on retrouve deux catégories

Base de données Relationnelle SQL: il s'agit de bases de données dans lesquelles l'information est organisée avec des tableaux à deux dimensions nommées « tables ». Les lignes correspondent aux enregistrements. Chaque enregistrement contient un groupe d'informations – les attributs – relatives à un sujet. La plupart des systèmes de gestion de bases de données relationnelles reconnaissent le SQL.

Base de données Non Relationnelle NoSQL 'Not Only SQL': La particularité des bases de données NoSQL est qu'elles n'utilisent pas le modèle relationnel. Il n'y a donc pas de tableau avec des caractéristiques et nombres d'attributs fixes. Les schémas sont donc absents ou flexibles. Cela permet de regrouper des données ayant des structures différentes.

Amazon Relational Database Service

Pourquoi Utiliser RDS:

- **Vous n'avez pas à installer le logiciel de base de données** (MySQL, PostgreSQL, MariaDB, Oracle...). **Vous n'avez pas à configurer le moteur de base de données**. La configuration de base est déjà optimisée
- **Vous n'avez pas à choisir le matériel de vos serveurs**. Des serveurs optimisés pour la gestion des bases de données.
- Vous n'avez **pas besoin de mettre à jour le logiciel de base de données**. C'est fait pour vous par Amazon.
- **La sauvegarde et la restauration des bases de données** peut se faire en quelques clics.
- Vous pouvez **augmenter la puissance du serveur si nécessaire**, en fonction de votre trafic (comme EC2).
- Vous pouvez lancer facilement **plusieurs serveurs de base de données en réplication** (la base de données est copiée en temps réel sur plusieurs serveurs). Cela vous sera très pratique si votre site devient gros !

Amazon Relational Database Service

Les moteurs de base de données disponibles

Quand vous utilisez RDS, vous avez le choix de votre moteur de base de données. Les plus connus sont disponibles, vous devriez trouver votre bonheur :

- MySQL
- MariaDB (qui est un fork de MySQL)
- PostgreSQL
- Oracle
- SQL Server
- Amazon Aurora

Allez sur la console aws et cliquez sur le service RDS

Amazon Relational Database Service

Qu'est-ce qu'Amazon Aurora ?

Il s'agit d'un moteur de base de données spécifique conçu par Amazon. Il est :

- **Compatible avec MySQL et PostgreSQL**. Si vous avez déjà une base de données MySQL ou PostgreSQL, vous devriez donc pouvoir utiliser Aurora quasiment sans problème. Vous pouvez par exemple tout à fait l'administrer avec un outil comme phpMyAdmin si vous le souhaitez.
- **Propriétaire**. Le code source d'Aurora n'est pas ouvert, ce qui pourra en refroidir certains. En revanche, étant compatible avec MySQL et PostgreSQL, vous pouvez normalement importer et exporter les données à tout moment si nécessaire.
- **Plus rapide**. Amazon indique qu'il est 5x plus rapide que MySQL et 3x plus rapide que PostgreSQL. Il est surtout optimisé pour le cloud d'Amazon.

Amazon Relational Database Service

Tarification service RDS:

Dans le cadre de l'offre gratuite AWS, Amazon RDS aide les nouveaux clients AWS à démarrer gratuitement avec un service de base de données gérée dans le cloud. Chaque mois civil, l'offre gratuite d'Amazon RDS vous autorise à utiliser :

- 750 heures d'utilisation de l'instance Amazon RDS Single-AZ **db.t2.micro** avec MySQL, MariaDB, PostgreSQL, Oracle BYOL ou SQL Server (qui exécute SQL Server Express Edition).
- 20 Go de stockage de base de données polyvalent (SSD).
- 20 Go de stockage pour vos sauvegardes automatisées de la base de données et pour tout instantané de bases de données initié par l'utilisateur.

La tarification est en fonction du type de moteur, consultez la page https://aws.amazon.com/fr/rds/pricing/

Amazon Relational Database Service

Lancer une instance RDS

Voici quelques-uns des menus à connaître :

- **Instances** : la liste de vos serveurs RDS.
- **Clusters** : si vous avez un gros trafic et que vous voulez copier votre base de données en temps réel sur plusieurs serveurs, vous aurez besoin de créer un cluster pour regrouper vos serveurs. C'est une fonctionnalité plus avancée que nous ne verrons pas dans ce cours d'introduction.
- **Instantanés** : les sauvegardes de vos bases de données.

Amazon Relational Database Service

Lancer une instance RDS

1. Allez sur aws console et selectionnez le service RDS

La première question qu'on nous pose est celle du choix du moteur de base de données.

Nous allons utiliser l'offre gratuite MySQL

2. On nous demande ensuite ce que nous comptons faire de la base de données.

Le mode production est optimisé : le serveur est répliqué et il est plus puissant. C'est effectivement conseillé pour un gros site qui tourne.

Le mode "Dev/Test" n'est pas répliqué et on peut commencer avec des serveurs plus petits . D'ailleurs, c'est la seule option qui soit gratuite.

3. On vous demande ensuite de faire quelques choix importants pour configurer votre serveur, laissez la valeur par défaut. Plus bas choisissez classe instance de type **db.t2.micro (offre gratuite).**

Il vous faut ensuite donner un nom à votre instance. Vous devrez aussi indiquer un nom d'utilisateur pour vous connecter à la base et un mot de passe

Amazon Relational Database Service

4.Configuration des paramètres avancés

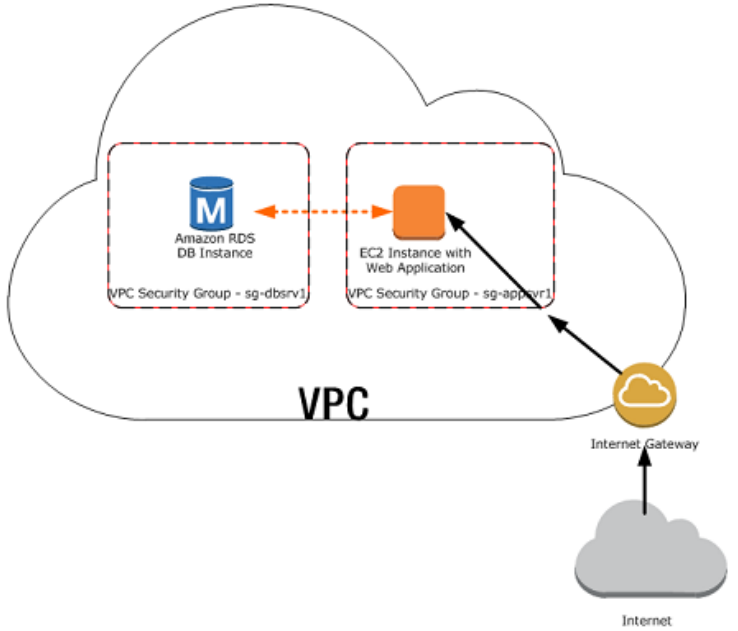
On commence par vous demander dans quel VPC vous souhaitez lancer votre serveur. Choisissez le VPC par defaut.

Désactivez "Accessibilité publique" dans les options, votre serveur RDS n'aura même pas d'IP publique. Cela voudra dire qu'il ne sera tout simplement pas accessible depuis Internet.

5. Cliquez sur créer l'instance.Nous pouvons maintenant voir

que notre instance est lancée et tourne, si nous allons dan

s la section "Instances" de RDS.



Amazon web service

AWS Lambda Workshop

1. https://github.com/atifrani/aws-data-exercices/blob/master/0.1-exercise.md

2. https://github.com/atifrani/EC2_rds_webapp

- Amazon Lambda (ServerLess)

- Lambda Overview
- Hello World using AWS Lambda
- Data intergration using AWS Lambda
- Deploying project on AWS Lambda

Amazon web service

Qu'est-ce que AWS Lambda ?

- AWS Lambda est un service informatique qui vous permet d'exécuter un code sans demander la mise en service ou la gestion des serveurs. Lambda exécute le code sur une infrastructure informatique à haute disponibilité et effectue toute l'administration des ressources informatiques, y compris la maintenance des serveurs et du système d'exploitation, l'allocation et la mise à l'échelle automatique des capacités, ainsi que la mise à l'échelle automatique et la journalisation. Avec Lambda, vous pouvez exécuter du code pour pratiquement n'importe quel type d'application ou de service backend. Il vous suffit de fournir votre code dans l'un des langages pris en charge par Lambda.
- Vous organisez votre code en fonctions Lambda. Lambda exécute le code uniquement si nécessaire et adapte son l'échelle automatiquement, qu'il s'agisse de traiter quelques requêtes quotidiennes ou des milliers de requêtes par seconde. Vous payez uniquement le temps de calcul que vous utilisez. Vous n'exposez aucuns frais quand votre code n'est pas exécuté. Pour plus d'informations, consultez AWS Lambda Pricing

Amazon web service

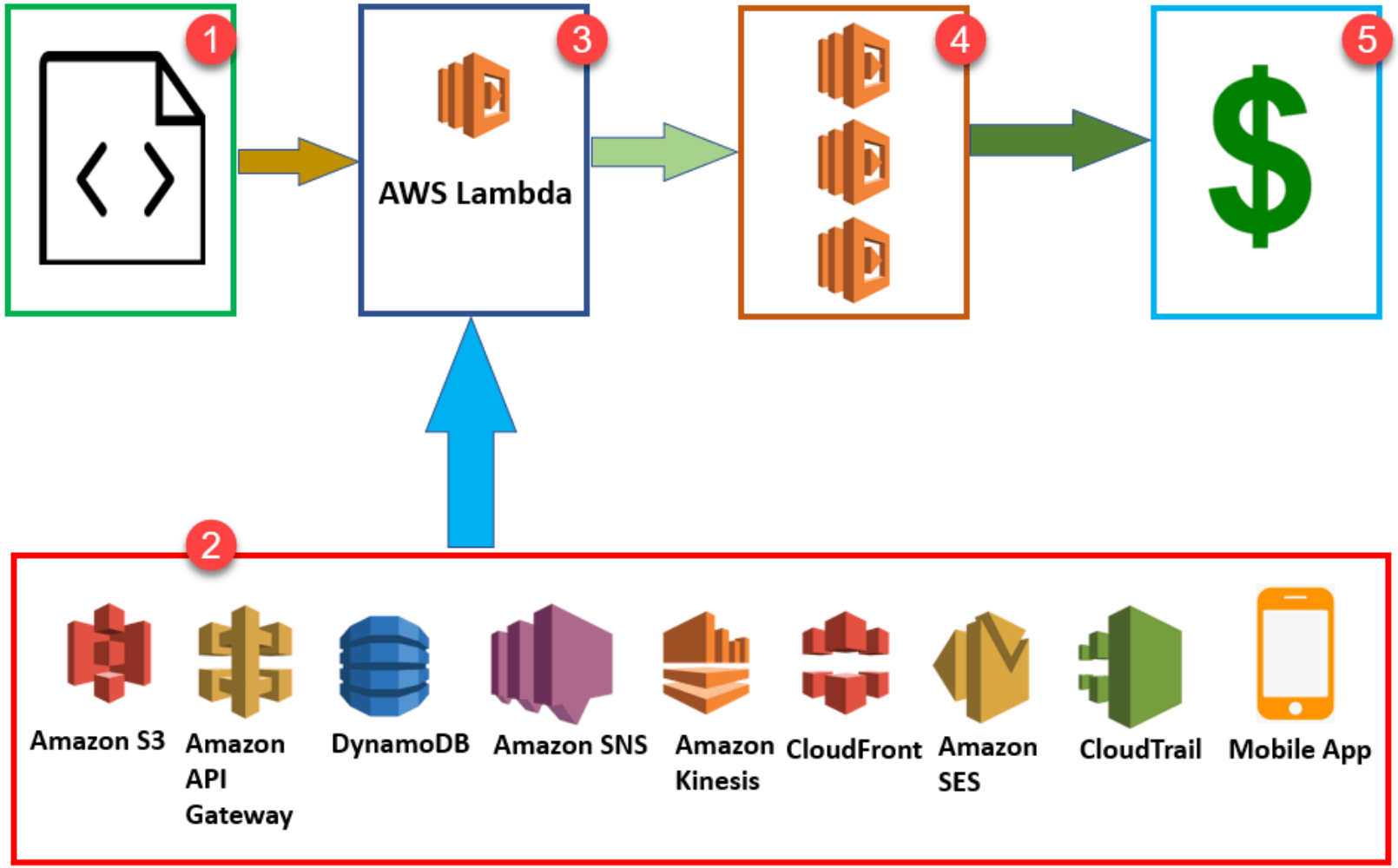
Cas d'utilisation de Lambda

Lambda est un service de calcul qui répond parfaitement aux besoins de nombreux scénarios d'application, à condition que vous soyez en mesure d'exécuter le code de votre application à l'aide de l'environnement d'exécution standard et au sein des ressources fournies par Lambda. Par exemple, vous pouvez utiliser Lambda pour :

- **Traitement de fichiers :** utilisez Amazon Simple Storage Service (Amazon S3) pour déclencher le traitement des données Lambda en temps réel après un chargement.
- **Traitement des flux :** utilisez Lambda et Amazon Kinesis pour traiter des données en flux en temps réel pour le suivi de l'activité des applications, le traitement des ordres de transaction, l'analyse du flux de clics, le nettoyage des données, le filtrage des journaux, l'indexation, l'analyse des médias sociaux, la télémétrie des données des appareils de l'Internet des objets (IoT) et les métriques.
- **Applications Web :** associez Lambda à d'autres services AWS pour créer de puissantes applications Web qui se mettent automatiquement à l'échelle et s'exécutent dans une configuration hautement disponible dans plusieurs centres de données.
- **Backends IoT :** créez des backends sans serveur à l'aide de Lambda pour gérer les demandes d'API Web, mobiles, IoT et tierces.
- **Backends mobiles :** créez des backends à l'aide de Lambda et d'Amazon API Gateway pour authentifier et traiter les demandes d'API. Utilisez AWS Amplify pour intégrer facilement votre backend à vos frontends iOS, Android, Web et React Native.

Amazon web service

Comment fonctionne AWS de Lambda



Amazon web service

Comment fonctionne AWS de Lambda

Étape 1: Téléchargez d'abord votre code AWS Lambda dans n'importe quelle langue prise en charge par AWS Lambda. Java, Python, Go et C# sont quelques-uns des langages pris en charge par la fonction AWS Lambda.

Étape 2: Voici quelques services AWS qui vous permettent de déclencher AWS Lambda.

Étape 3: AWS Lambda vous aide à télécharger du code et l'événement details sur lequel il doit être déclenché.

Étape 4: Exécute le code AWS Lambda lorsqu'il est déclenché par les services AWS :

Étape 5: AWS facture uniquement lorsque le code AWS lambda s'exécute, et pas d'autreswise.

Amazon web service

Comment fonctionne AWS de Lambda

Voici quelques exemples d'événements qui seront déclenchés lorsque vous utiliserez AWS Lambda.

- Insérer, mettre à jour et supprimer des données Table Dynamo DB
- DynamoDB peut déclencher AWS Lambda chaque fois que des données sont ajoutées, modifiées et supprimées dans la table.
- Chargement un objet S3
- Modifications apportées aux objets dans les compartiments S3
- API Gateway vous permet de déclencher AWS Lambda sur les méthodes GET/POST.

Amazon web service

AWS Lambda Concepts

Fonction:

Une fonction est un programme ou un script qui s'exécute dans AWS Lambda. Lambda transmet les événements d'appel à votre fonction, qui traite un événement et renvoie sa réponse.

Temps d'exécution:

Le runtime permet des fonctions dans différents langages qui s'exécutent sur le même environnement d'exécution de base. Cela vous aide à configurer votre fonction au moment de l'exécution. Il correspond également à votre sélection langage de programmation.

Source de l'événement :

Une source d'événement est un service AWS, tel que Amazon SNS, ou un service personnalisé. Cette fonction de déclenchement vous aide à exécuter sa logique.

Amazon web service

AWS Lambda Concepts

Couches Lambda :

Les couches Lambda constituent un mécanisme de distribution important pour les bibliothèques, les environnements d'exécution personnalisés et d'autres dépendances de fonctions importantes. Ce composant AWS vous aide également à gérer le code de votre fonction de développement séparément du code immuable et des ressources qu'il utilise.

Flux de journaux :

Le flux de journaux vous permet d'annoter votre code de fonction avec des instructions de journalisation personnalisées qui vous aident à analyser le flux d'exécution et les performances de vos fonctions AWS Lambda.

Amazon web service

AWS Lambda vs AWS EC2

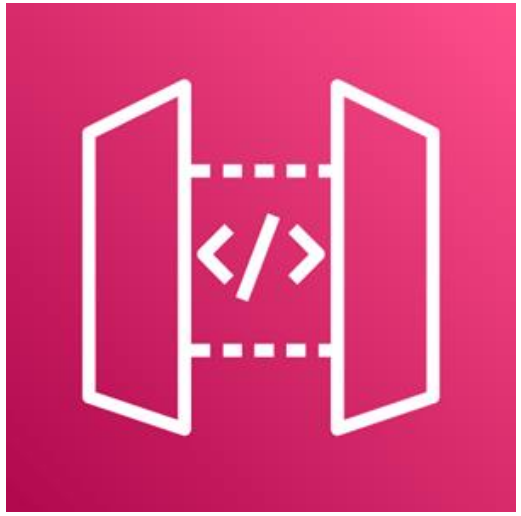
Paramètres	AWS Lambda	AWS EC2
Définition	AWS Lambda est une plateforme en tant que service (PaaS). Il vous aide à exécuter et à exécuter votre code backend.	AWS EC2 est une infrastructure en tant que service (laaS). Il fournit des ressources informatiques virtualisées.
Flexibilité	N'offre aucune flexibilité pour se connecter aux instances de calcul. Il vous permet de choisir un personnalisé operasystème de configuration ou d'exécution du langage.	Offre la flexibilité de sélectionner la variété d'instances, personnaliséesoperasystèmes de configuration, correctifs de sécurité et réseau, etc.
Processus d'installation	Vous devez sélectionner votre environnement dans lequel vous souhaitez exécuter le code et transférer le code dans AWS Lambda.	Pour la première fois dans EC2, vous devez choisir le système d'exploitation et installer tous les logiciels requis puis pousser votre code dans EC2.
Restrictions environnementales	Il est limité à quelques langues.	Aucune restriction d'environnement

Amazon web service

AWS Lambda Workshop

1. https://github.com/atifrani/lambda-hello-world/tree/master
2. https://github.com/atifrani/lambda-square
3. https://github.com/atifrani/lambda_formular
4. https://github.com/atifrani/aws-data-exercices/blob/master/0.2-exercise.md

- API Gateway (ServerLess)

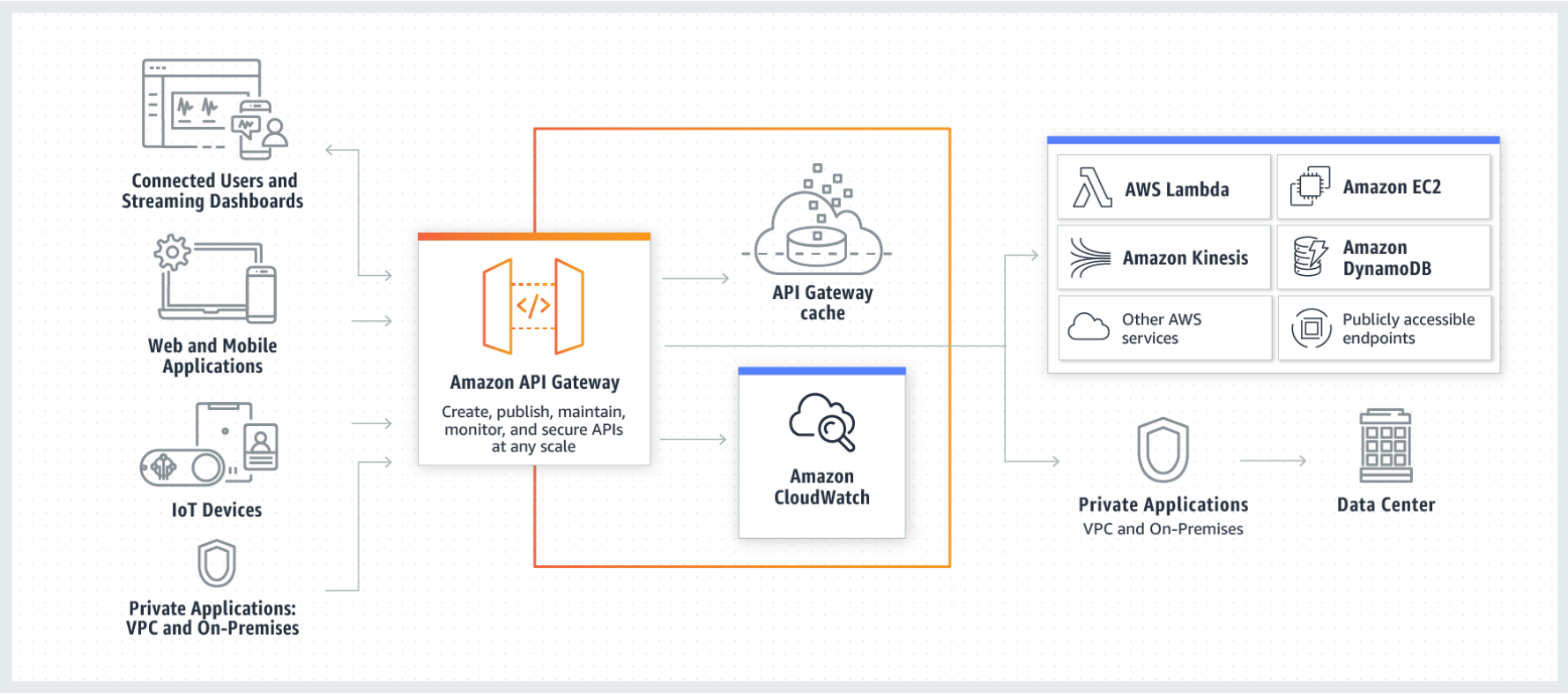


- API gateway Overview

Amazon web service

Introduction à API Gateway

Amazon API Gateway est un service entièrement opéré, qui permet aux développeurs de créer, **publier, gérer, surveiller et sécuriser facilement des API** à n'importe quelle échelle**. Les API servent de « porte d'entrée » pour que les applications puissent accéder aux données**



Amazon services Réseau

Introduction à API Gateway

- API Gateway crée des API RESTful qui :
- reposent sur le protocole HTTP ;
- permettent la communication client-serveur sans état ;
- mettent en œuvre les méthodes HTTP standard, telles que GET, POST, PUT, PATCH et DELETE.

AWS API Gateway Workshop:

https://github.com/atifrani/lambda_apigateway_webapp


Q&A