

Ce document est réservé aux personnes inscrites à la formation
« AWS Certified Solutions Architect Associate 2020 [SAA-C02] »



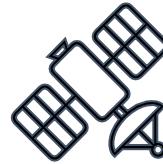
- **Veuillez ne pas partager ce document**
- Il est fourni pour votre seul usage personnel
- Vous devez utiliser ce document en accompagnement des vidéos de la formation
- Servez-vous de la formation pour compléter le document
- Il vous aidera à mémoriser les informations importantes à retenir pour la certification
- **Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>**

L'examen **AWS Certified Solutions Architect Associate** est prévu pour des personnes travaillant en tant qu'architecte de solutions et possédant une ou plusieurs années d'expérience pratiques dans la conception de systèmes disponibles, rentables, tolérants aux pannes, distribués et évolutifs sur AWS. Vous pourrez passer l'examen dans un centre de test ou depuis votre domicile ou votre entreprise grâce à la surveillance en ligne.



Compétences validées par la certification :

- Capacité à démontrer de façon efficace que vous avez les connaissances pour réaliser l'architecture d'applications sécurisées et robustes, ainsi que pour les déployer sur les technologies AWS
- Définir une solution en utilisant des principes de conception architecturale basés sur les exigences client
- Fournir des conseils d'implémentation basés sur les bonnes pratiques à l'organisation, tout au long du cycle de vie du projet



Vous
êtes
ici



Certification Foundational

Certifications Associate

Certifications Professional

Certifications Specialty

Certifications AWS disponibles.

Professional

Deux ans d'expérience complète dans la conception, l'exploitation et la résolution des problèmes des solutions en utilisant le Cloud AWS.



Associate

Un an d'expérience dans la résolution de problèmes et la mise en œuvre de solutions à l'aide du Cloud AWS



Architect



Operations



Developer

Bases

Six mois d'apprentissage des concepts de base du Cloud AWS et du secteur



Spécialité

Expérience technique sur le Cloud AWS dans le domaine Specialty, comme indiqué dans le **guide de l'examen**



Testez gratuitement la plateforme, les produits et les services AWS.

Types d'offres

Découvrez plus de 60 produits et commencez à créer sur AWS grâce à notre offre gratuite. Trois types d'offres gratuites sont disponibles en fonction du produit que vous utilisez. Consultez les éléments ci-dessous pour plus d'informations sur chaque produit.



Toujours gratuit

Ces offres gratuites n'expirent pas et sont disponibles pour tous les clients AWS



12 mois gratuits

Profitez de ces offres pendant 12 mois après votre date d'inscription de départ sur AWS



Essais

Les offres d'essai gratuit à court terme débutent à la date d'activation d'un service en particulier.

**Important : durant les ateliers veillez bien à supprimer vos ressources avant de quitter la console aws.
Suivez bien mes instructions soyez attentifs.
En effet des frais pourraient vous être imputés si vous laissez des services actifs.**

Domaine 1 : Conception d'architectures résilientes

- 1.1 Concevoir une solution d'architecture multi-tiers
- 1.2 Concevoir des architectures hautement disponibles et/ou tolérantes aux pannes
- 1.3 Concevoir des mécanismes de découplage en utilisant les services AWS
- 1.4 Choisir un stockage résilient approprié

30%

Domaine 2 : Conception d'architectures performantes

- 2.1 Identifier des solutions de calcul élastiques et évolutives pour une charge de travail
- 2.2 Choisir des solutions de stockage performantes et évolutives pour une charge de travail
- 2.3 Choisir des solutions de mise en réseau performantes pour une charge de travail
- 2.4 Choisir des solutions de bases de données performantes pour une charge de travail

28%

Domaine 3 : Conception d'applications et d'architectures sécurisées

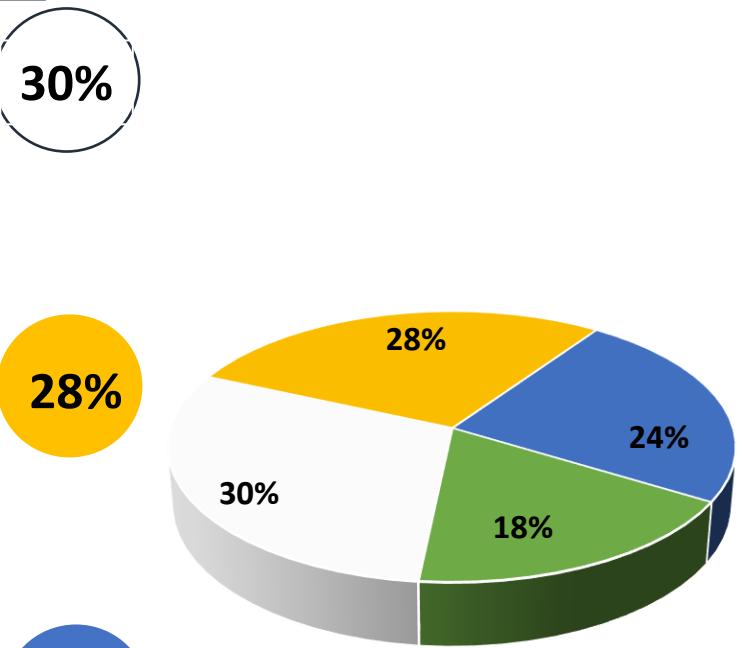
- 3.1 Concevoir un accès sécurisé aux ressources de l'AWS
- 3.2 Concevoir des niveaux d'application sécurisés
- 3.3 Choisir les options de sécurité des données appropriées

24%

Domaine 4 : Conception d'architectures à coûts optimisés

- 4.1 Identifier des solutions de stockage rentables
- 4.2 Identifier les services de calcul et de bases de données rentables
- 4.3 Concevoir des architectures de réseau à coûts optimisés

18%



Informations de l'examen**Format**

Choix multiples, réponses multiples

**Type**

Associate

**Méthode d'administration**

Centre d'examen ou surveillance en ligne

**Durée**

L'examen dure 130 minutes.

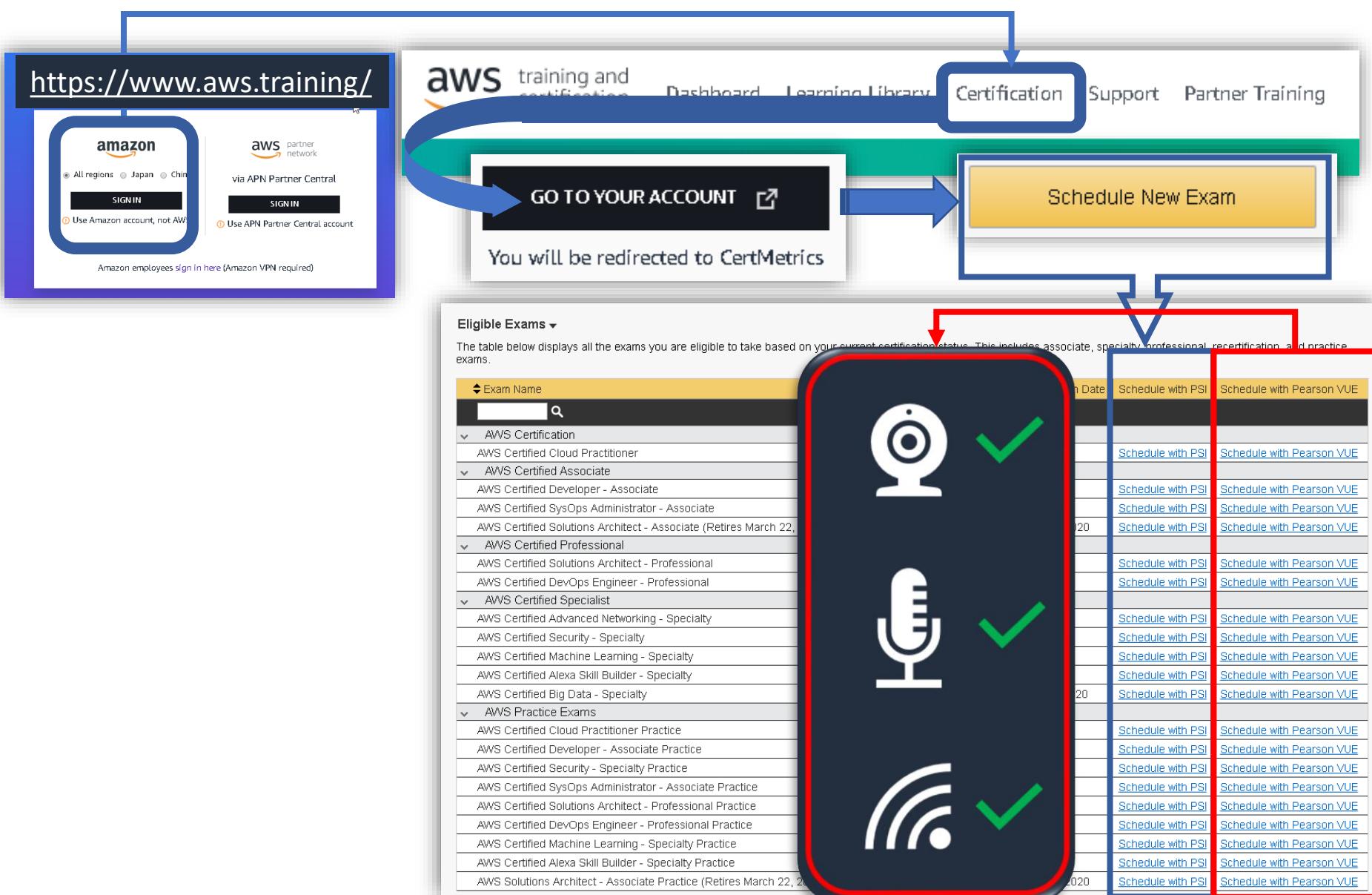
**Coût**

150 USD (Examen blanc : 20 USD)

**Langue**

Disponible en anglais, en japonais, en coréen et en chinois simplifié

coréen et en chinois simplifié
disponible en anglais, en japonais, en coréen et en chinois simplifié



Informations de l'examen



Format

Choix multiples, réponses multiples



Type

Bases



Méthode d'apprentissage

Centre d'examen ou surveillance en ligne



Durée

L'examen dure 90 minutes.



Coût

100 USD (Examen blanc : 20 USD)



Langue

Disponible en anglais, en japonais, en coréen et en chinois simplifié

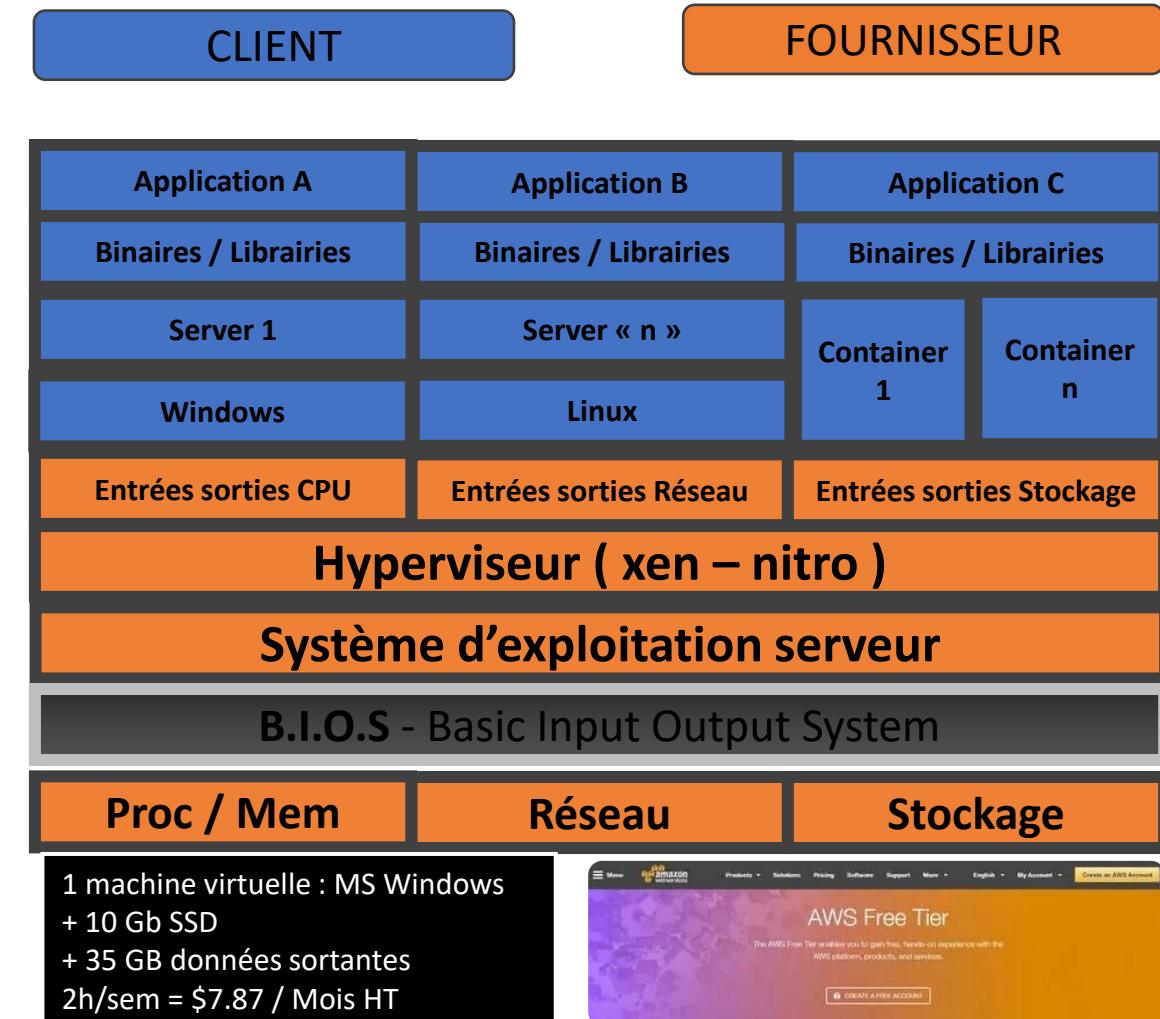
Attention si vous réclamez une « accommodation », vous devrez réserver votre examen par téléphone avec une personne anglophone.

The screenshot shows two main windows. The top window is titled 'Exam Accommodations' and contains a table with one row: 'There is no data to display.' Below this table is a yellow button labeled 'Request Accommodation'. A blue arrow points from this button to the 'Request Exam Accommodations' button in the sidebar of the bottom window. The bottom window is titled 'Accommodation Type *' and shows a dropdown menu with 'ESL +30 MINUTES' selected. Another blue arrow points from the 'Request Accommodation' button to the 'Create' button at the bottom right of this window. The sidebar on the left of the bottom window includes buttons for 'Manage PSI Exams' and 'Manage Pearson VUE Exams'.

Cloud Practitioner available via online proctoring at Pearson VUE

To register, from the Eligible Exam table below - select "Schedule with Pearson VUE" next to the AWS Certified Cloud Practitioner exam. Then, on the Select Exam Delivery Option Page - choose "At a home or office". Note: Online proctoring is not available in China, Japan, South Korea or Slovenia.

Virtualisation (software defined)



Virtualization & containers

Amazon Elastic Container Registry

Stocker gérer et déployer facilement des images de conteneurs

Amazon Elastic Container Service (ECS)

Un moyen très sûr, fiable et évolutif d'exécuter des conteneurs

Vous devez dédier des instances EC2 pour ECS

Amazon Elastic Kubernetes Service (EKS)

La méthode la plus sûre pour exécuter Kubernetes

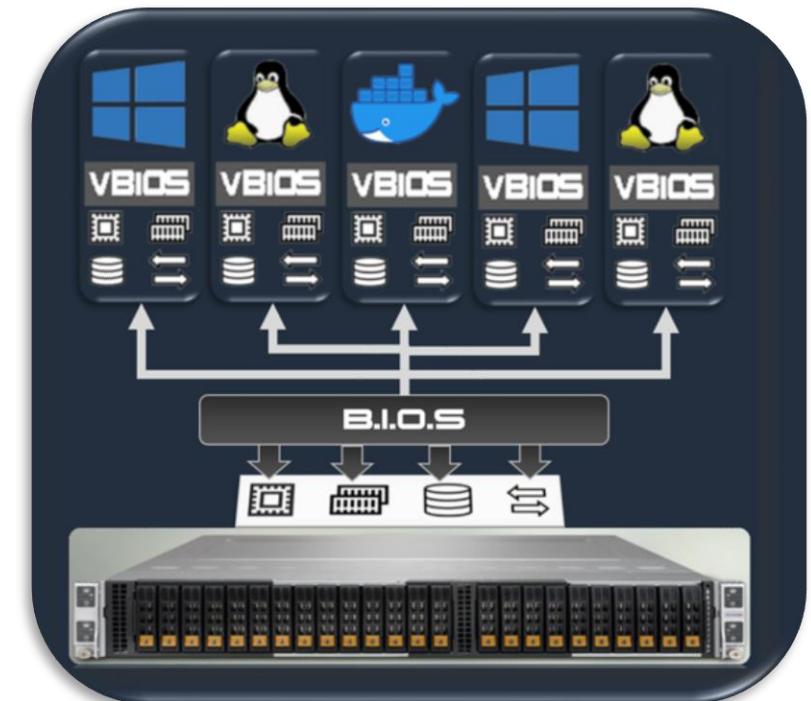
AWS Fargate

Calcul sans serveur pour conteneurs (serverless container)

Vous n'avez pas à gérer d'instances EC2 pour Fargate

Virtualisation permet de réduire

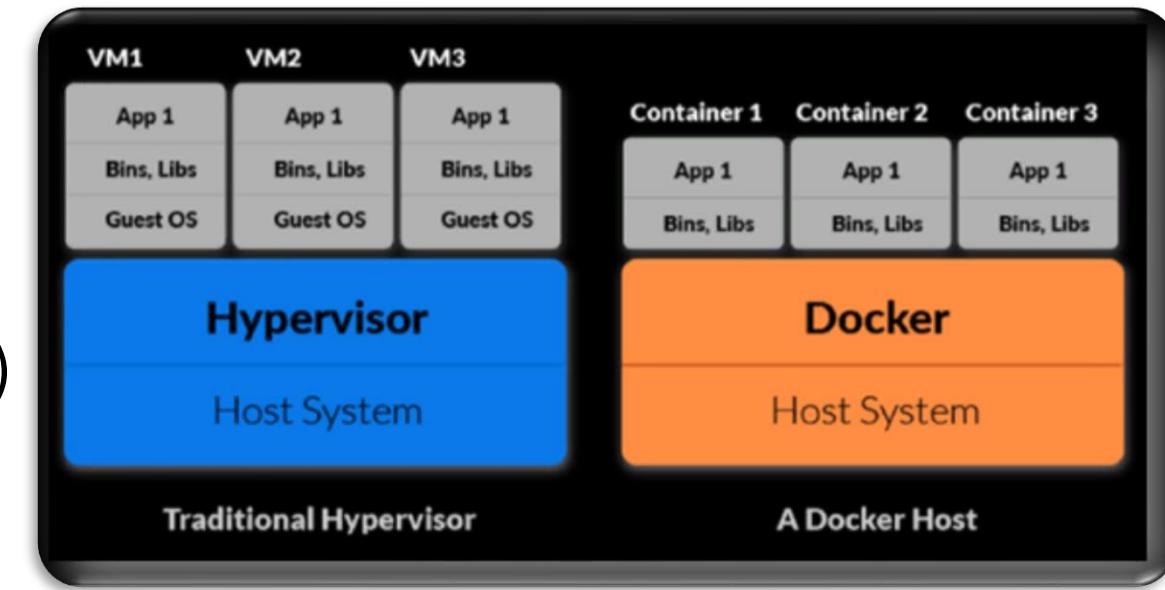
- Les dépenses CAPEX
- Les coûts opérationnels
- La place nécessaire
- Le gaspillage de ressources



Virtualization vs containers



- Docker (voir aussi LXC / LXD)
- Container = micro noyaux contenant uniquement ce qui est nécessaire pour faire fonctionner une application
- Déployer des applications dans des containers
- On obtient une « docker image »
- Une image est stockée dans un dépôt
- « Docker Hub » ou ECR (Elastic container registry)
- Un container fonctionne sur tous les systèmes
- Plusieurs containers sur une machine virtuelle
- Mise à l'échelle facilitée sur une seule VM car un container est petit



Définition « Cloud » « infonuagique »



National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-145

The NIST Definition of Cloud Computing

Recommendations of the National Institute of Standards and Technology

Peter Mell
Timothy Grance

Caractéristiques :

- Libre-service à la demande (On-demand self-service)
- Large accès au réseau (Broad network access)
- Mise en commun des ressources (Resource pooling)
- Élasticité rapide (Rapid elasticity)
- Service mesuré (Measured service)

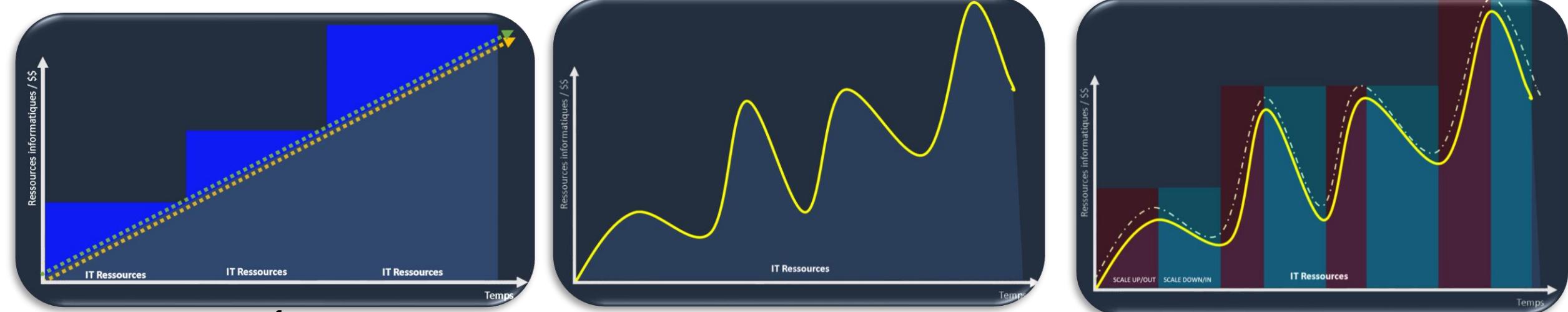
Modèles de service :

- Software as a service (SAAS)
- Plateforme as a service (PAAS)
- Infrastructure as a service (IAAS)

Modèles de déploiement :

- Nuage privé (Private Cloud)
- Nuage communautaire (Community Cloud)
- Nuage public (Public Cloud)
- Nuage hybride (Hybrid Cloud)

- Élasticité rapide (Rapid elasticity)
 - Agilité, flexibilité, haute disponibilité



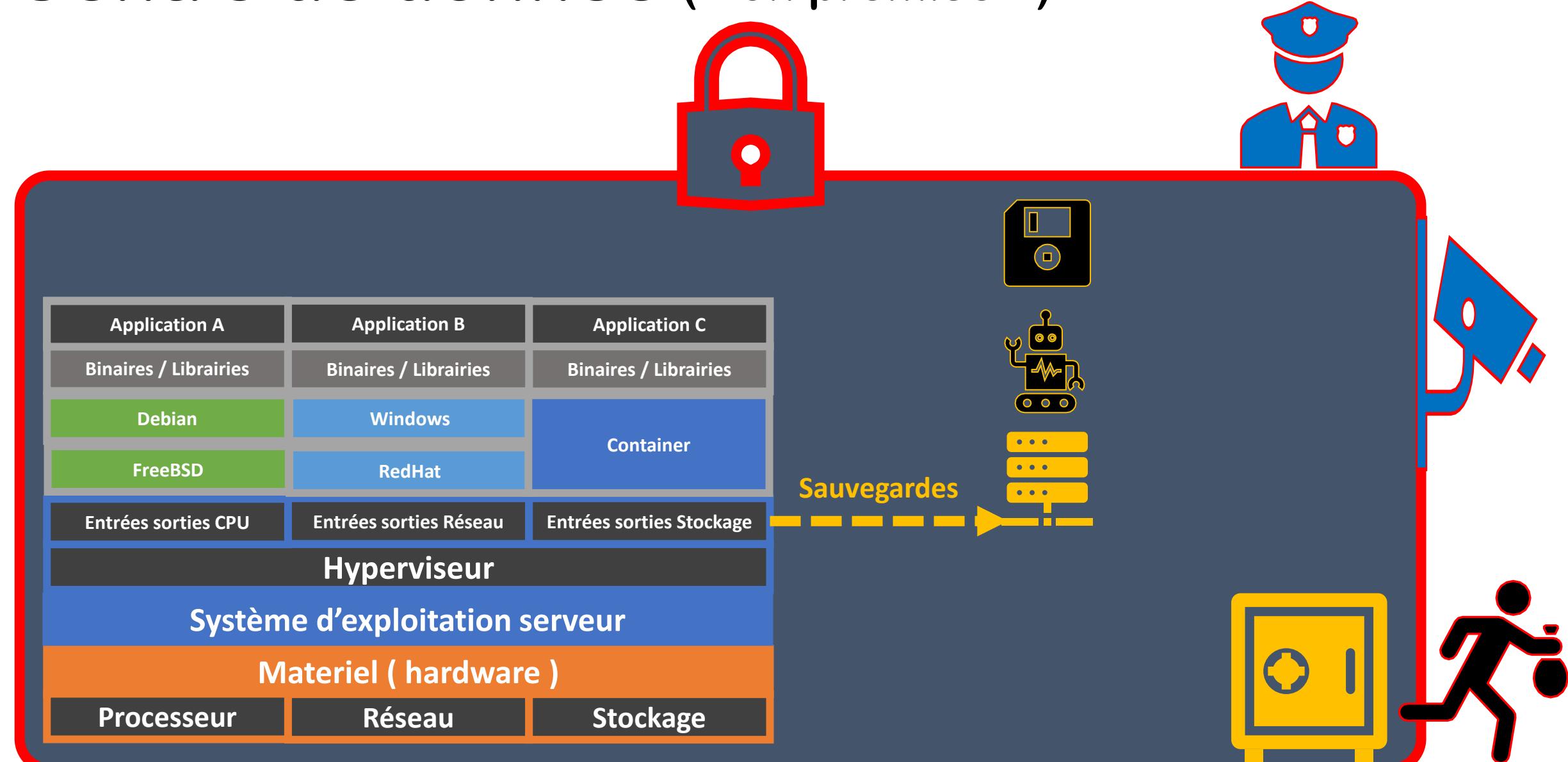
SCALABILITÉ - capacité d'un système à augmenter la charge de travail sur ses ressources matérielles actuelles (un serveur) (*scale-up*) ;

ÉLASTICITÉ - capacité d'un système à augmenter la charge de travail sur ses ressources matérielles actuelles et supplémentaires (ajoutées dynamiquement à la demande, autres serveurs); l'élasticité est fortement liée au déploiement sur le cloud (*scale-out*);

Cas d'usages (Cloud)

- Environnements de développement
- Démonstration de faisabilité (POC)
- Hébergement des sites web
- Plan continuité de service
- Plan de reprise d'activité
- Sauvegardes archivage
- Big Data Datawarehouse
- Augmentation du trafic
- IA Machine Learning
- Migrations (...)

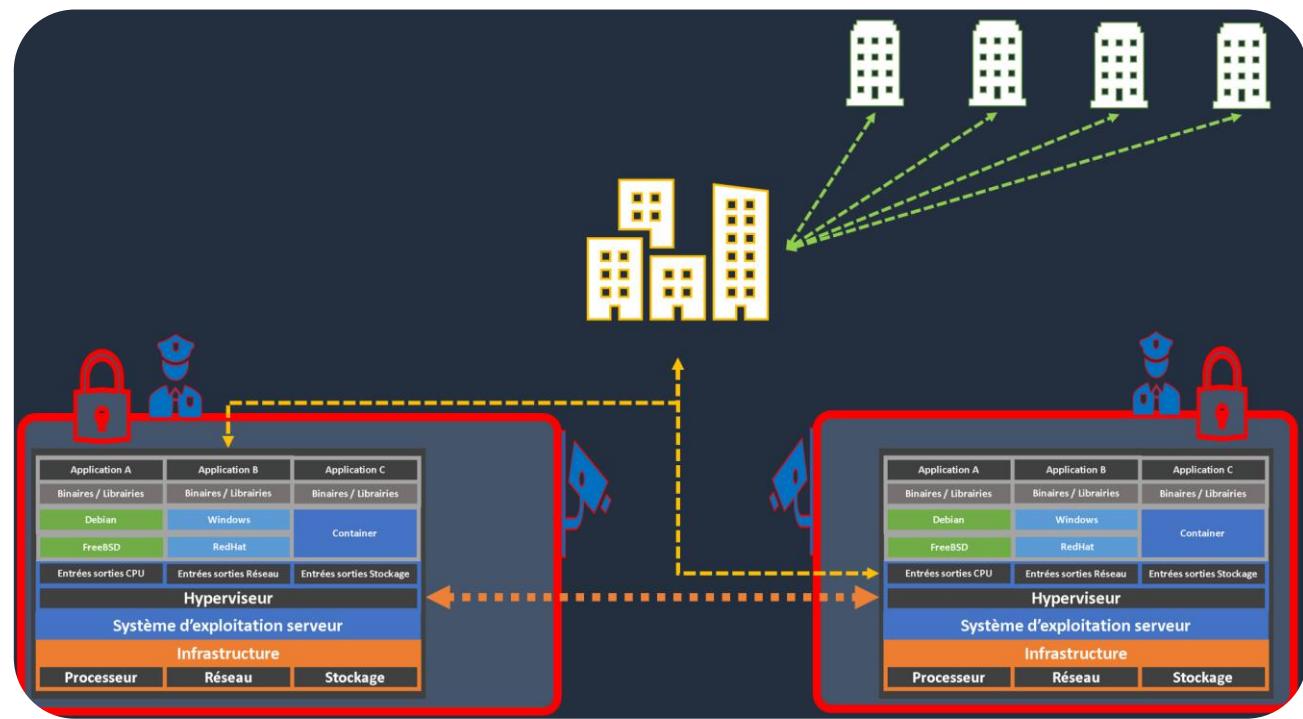
Centre de donnée (« on premise »)



Centre de données (dual site on premise)

est composé des caractéristiques et composants suivants :

- Localisation géographique du centre
- Sécurité physique et contrôle d'accès
- Alimentation et environnement
- Composants réseau
- Composants serveur
- Composants stockage

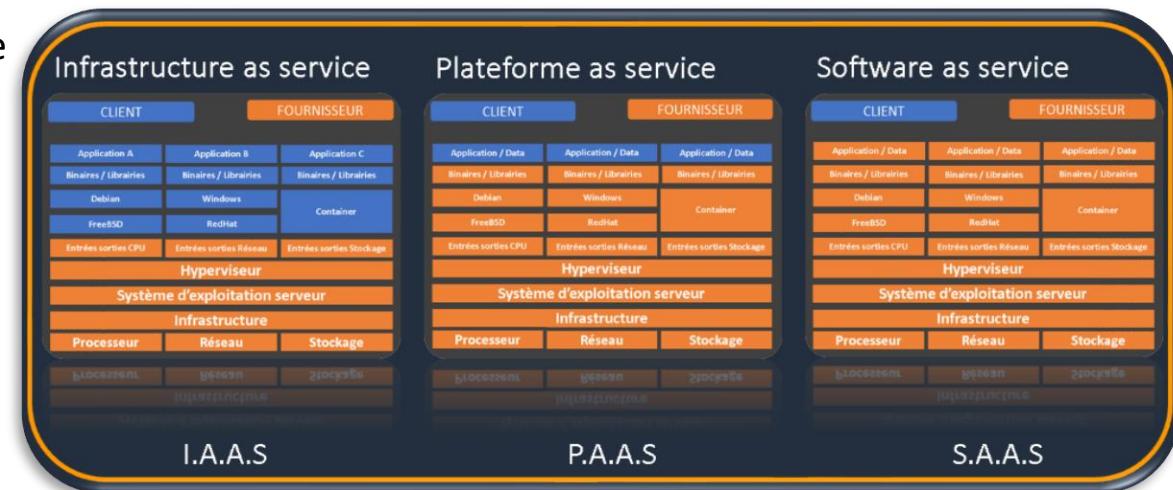


En résumé

Caractéristiques essentielles

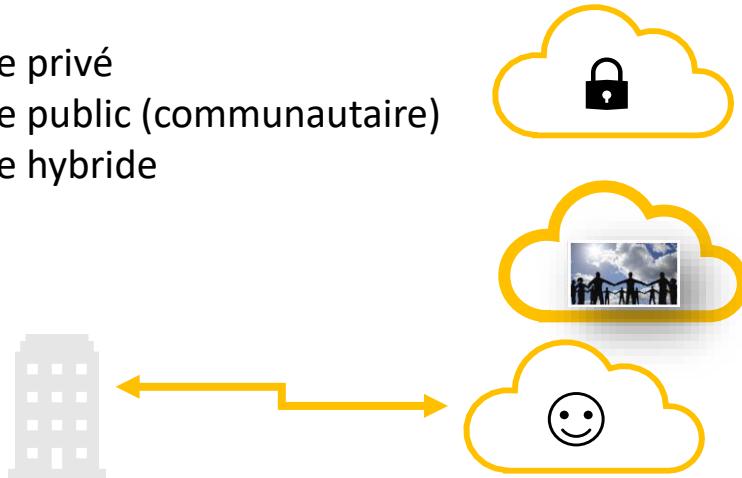
- Libre-service à la demande (On-demand self-service)
- Large accès au réseau (Broad network access)
- Mise en commun des ressources (Resource pooling)
- Élasticité rapide (Rapid elasticity)
- Service mesuré (Measured service)

Modèles de service

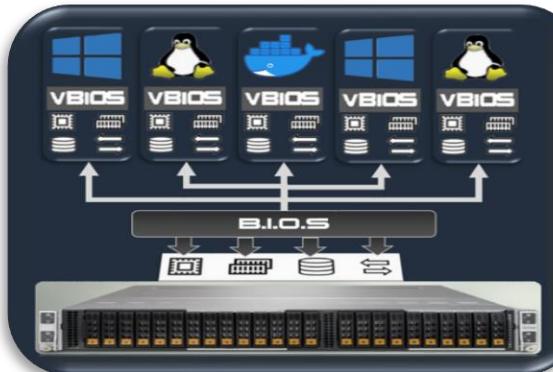


Différents types de déploiements

- Nuage privé
- Nuage public (communautaire)
- Nuage hybride



Virtualisation des ressources



Cas d'usage

- Migrations (...)
- Environnements de développement
- Démonstration de faisabilité (POC)
- Hébergement des sites web
- Plan continuité de service
- Plan de reprise d'activité
- Sauvegardes archivage
- Big Data Datawarehouse
- Augmentation du trafic
- IA Machine Learning

(Cloud Computing) est un regroupement virtuel distant de ressources partagées, à la demande, offrant des services de calcul, de stockage et de réseau qui peuvent être rapidement déployées à l'échelle et accessibles directement depuis internet.

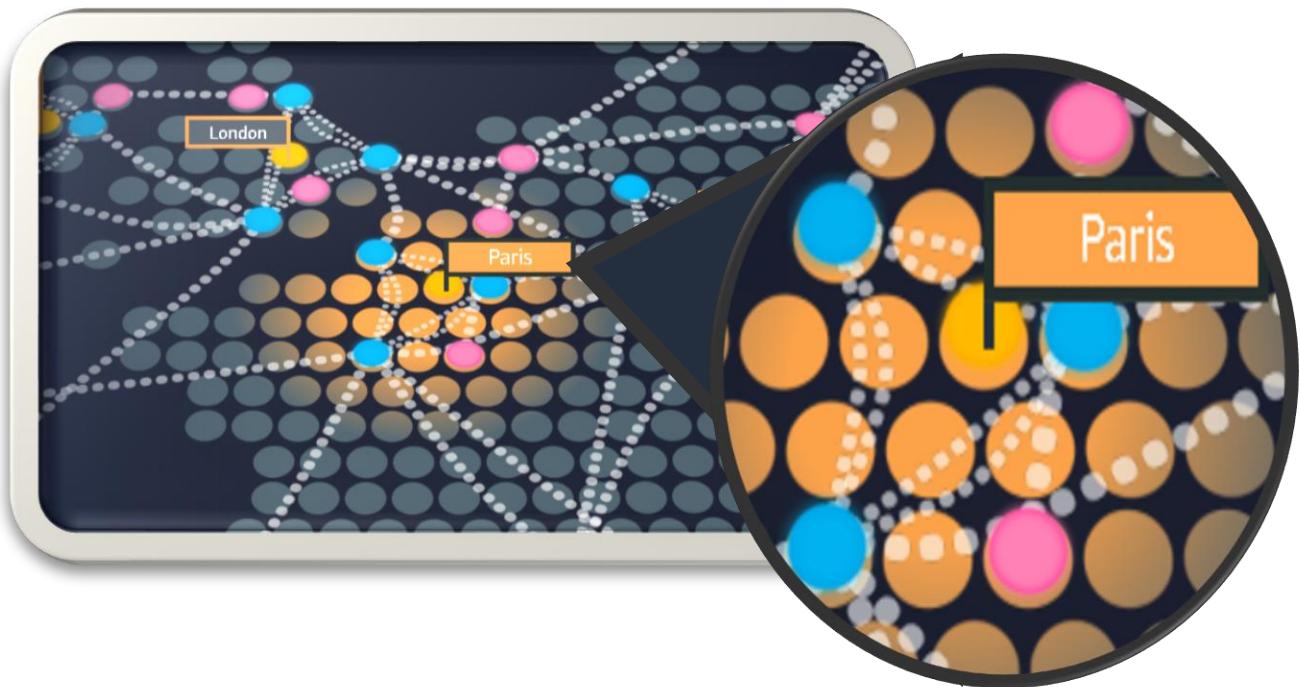
Où se trouve le CLOUD?

Régions et zones de disponibilité

- **US East N.**
 - Virginia (6), Ohio (3)
- **US West**
 - N. California (3), Oregon (4)
- **Asia Pacific**
 - Mumbai (3), Seoul (3), Singapore (3), Sydney (3), Tokyo (4),
 - Osaka-Local (1), Hong Kong SAR (3)
- **Canada**
 - Central (2)
- **Mainland China**
 - Beijing (2), Ningxia (3)
- **Europe**
 - Frankfurt (3), Ireland (3), London (3), Paris (3), Stockholm (3)
- **South America**
 - São Paulo (3)
- **GovCloud (US)**
 - US-East (3), US-West (3)
- **Middle East**
 - Bahrain (3)

Nouvelles regions (bientot)

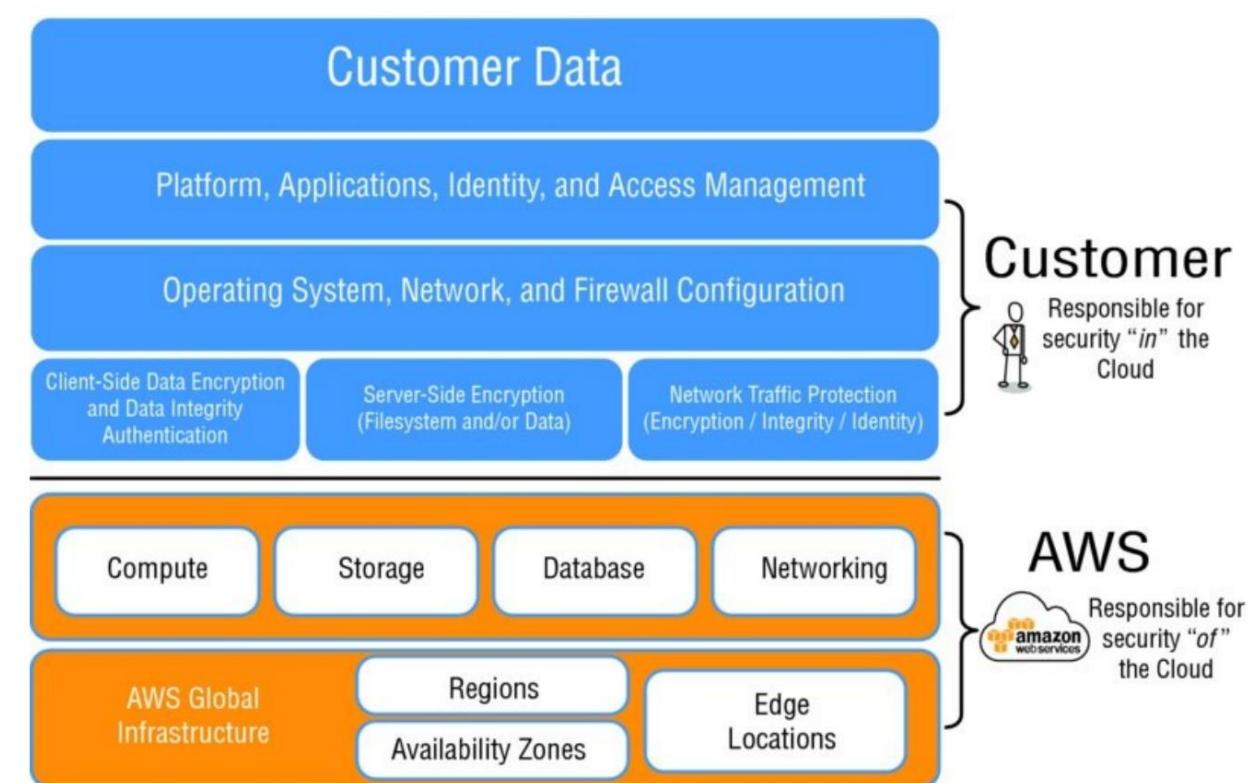
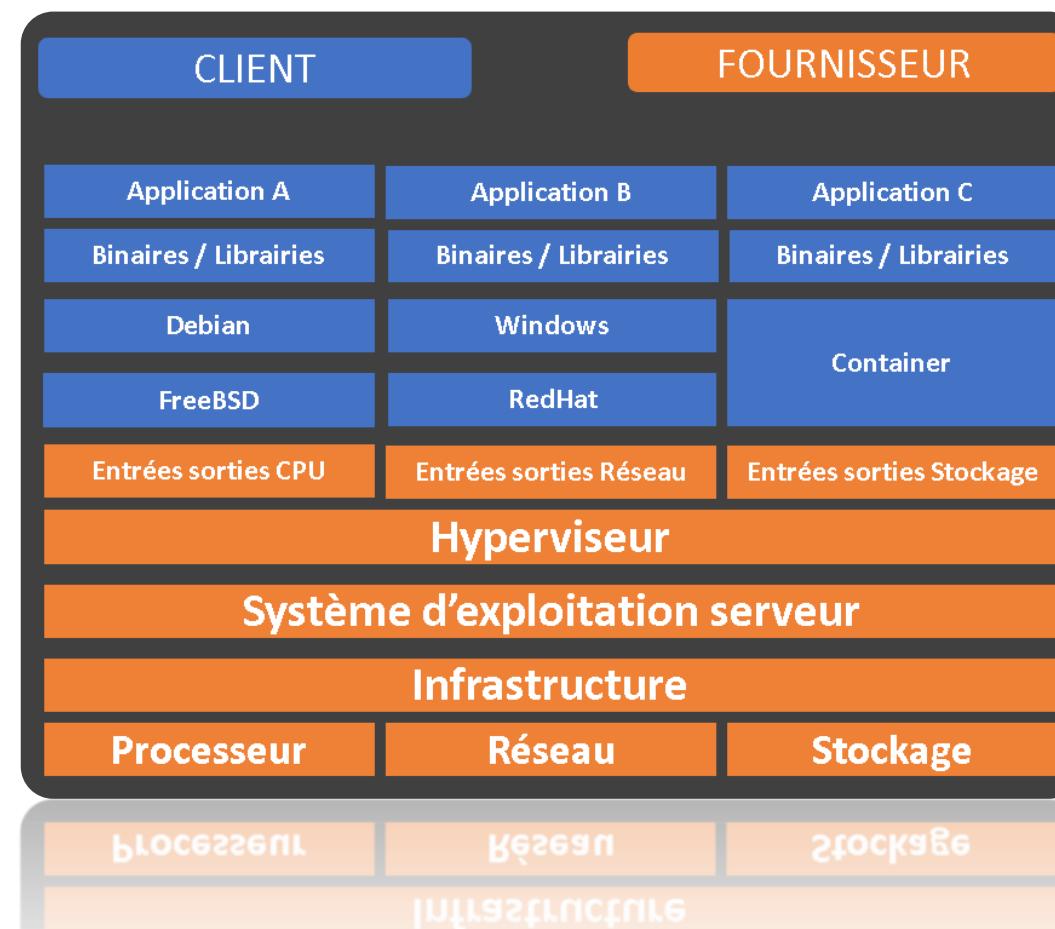
- Indonesia / Italy / Osaka / South Africa / Spain



- Régions
- Zones de disponibilités (Availability Zones)
- Emplacements périphériques (Edge locations)

Modèle de responsabilités partagées

(AWS shared responsibility model)





Solution Architect Associate (SAA-C02)

CONSOLE

AWS Management Console

Services AWS

Trouvez des services
Vous pouvez entrer des noms, mots-clés ou acronymes.
Exemple : Service de base de données relationnelle, base de données, RDS

Services AWS

- Calcul
 - EC2
 - ElastiCache
 - ECR
 - ECS
 - EKS
 - Lambda
 - Batch
 - Amazon ElastiCache
 - Serverless Application Repository
 - AWS Outposts
 - EC2 Image Builder
- Stockage
 - S3
 - Amazon S3
 - Amazon EFS
 - Amazon FSx
 - Amazon S3 Glacier
 - Storage Gateway
 - AWS Backup
- Base de données
 - RDS

Accéder aux ressources lors de vos déplacements

Explorez AWS

Gestion et gouvernance

Exécutez des conteneurs sans serveur avec AWS Fargate

Sauvegarde et restauration évolutives, durables et sécurisées avec Amazon S3

Interface facile à utiliser qui permet l'usage des services AWS pour accéder à la console vous devez disposer d'un _____ et d'un _____.

Bonne pratiques
(protected by password + MFA)

N'oubliez pas : ne partagez JAMAIS vos clés d'accès ou mot de passe

Command Line (CLI)

```
(work) 15:31:21 user:~/Desktop/work $ aws-shell
aws> configure
AWS Access Key ID [None]: Your AWS Access Key ID
AWS Secret Access Key [None]: Your AWS Secret Access Key
Default region name [us-east-1]:
Default output format [None]:
aws>
```

Accès aux services via des commandes Propres à chaque service AWS pour accéder en ligne de commande aux ressources aws il vous faut disposer d'une _____ et d'une _____.

Bonne pratiques
(protected by password + MFA)

Software Dev Kit (SDK)

Sélectionnez votre plateforme



Android »



Navigateur »



iOS »



Java »



.NET »



Node.js »



PHP »



Python »



Ruby »

Insérer vos commandes directement dans le code de vos applications d'accéder les unes aux autres on attribue un _____ IAM. Vous pouvez également utiliser vos clé d'accès avec votre code mais attention à ne pas l'intégrer en clair dans vos codes sources dans des dépôts public

Bonnes pratiques en matière de gestion des clés d'accès AWS

Lorsque vous accédez à AWS par programmation, vous utilisez une clé d'accès pour vérifier votre identité et l'identité de vos applications. Une clé d'accès se compose d'un ID de clé d'accès (similaire à AAIAIOSFODNN7EXAMPLE) et une clé d'accès secrète (similaire à wJalrAUtnFEMI/K8MDENG/bPxRfiCYEXAMPLEKEY).

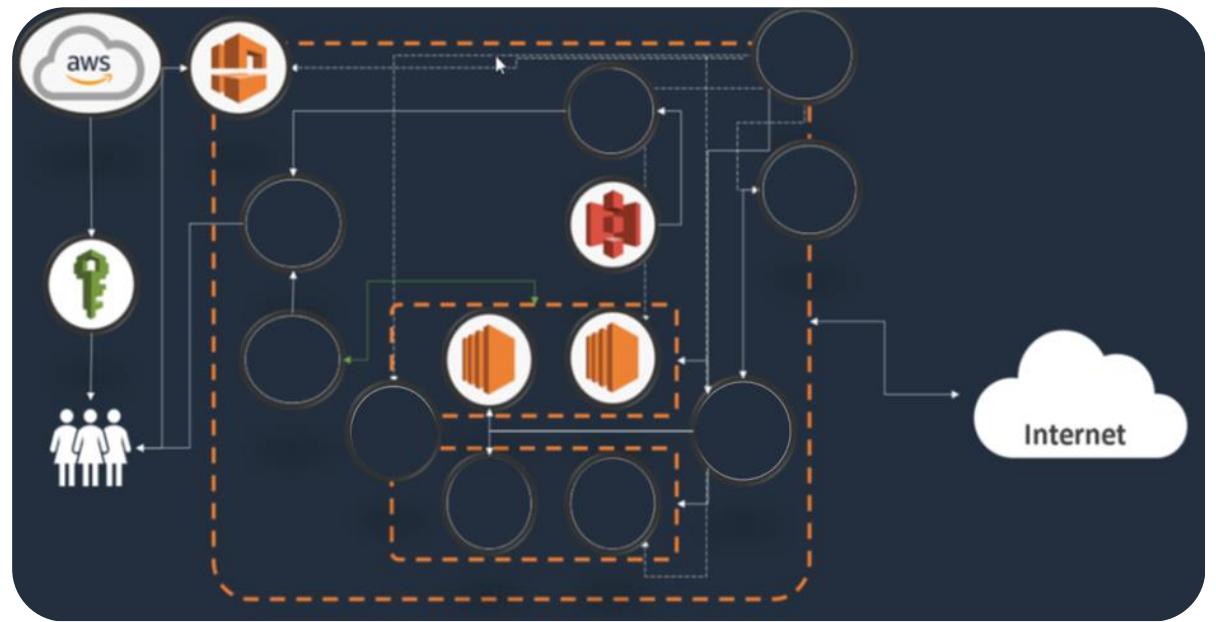
- Supprimer (ou ne pas générer) une clé d'accès de compte
- Utilisation des informations d'identification de sécurité temporaires (rôles IAM) au lieu des clés d'accès à long terme
- Utilisez des clés d'accès différentes pour chaque application
- **N'intégrez pas de clés d'accès directement dans le code**
- Procédez à une rotation régulière des clés d'accès
- Supprimez les clés d'accès inutilisées
- Configurez l'authentification multi-facteurs pour vos opérations les plus sensibles

Les kits SDK AWS et l'AWS CLI utilisent automatiquement les informations d'identification que vous stockez dans le fichier d'informations d'identification AWS ou peuvent bénéficier des rôles IAM.

Services de base AWS



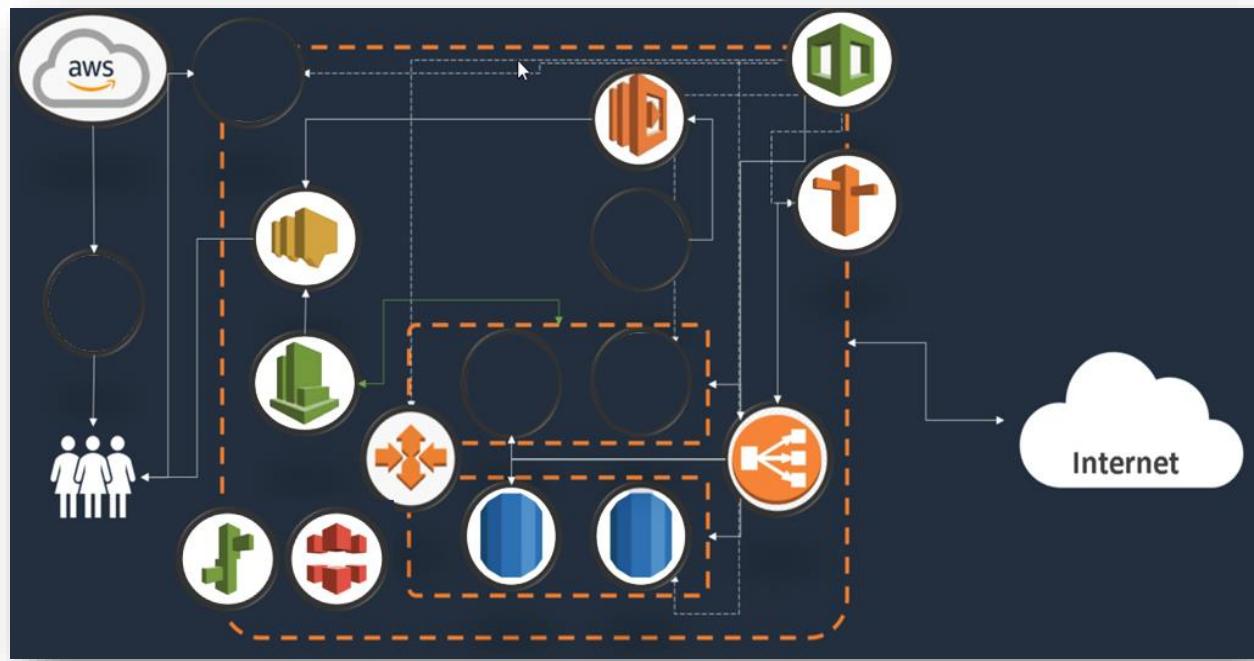
- AWS Identity and Access Management (IAM)
 - Amazon Virtual Private Cloud (VPC)
 - Amazon Elastic Compute Cloud (EC2)
 - Amazon Elastic Block Store (EBS)
 - Amazon Simple Storage Service (S3)



Services intégrés aws



- Elastic load balancer (ELB)
 - Auto Scaling
 - Amazon Route53
 - Amazon Relational Database Services (RDS)
 - AWS Lambda
 - * AWS Elastic Beanstalk
 - Amazon Simple Notification Service (SNS)
 - Amazon Cloudwatch
 - Amazon Cloudfront
 - AWS Cloudformation



* AWS Elastic Beanstalk est présent dans cette liste, AWS porte beaucoup d'intérêt à ce service qui est un service PaaS qui s'appuie sur EC2, Elastic load balancer (ELB) et Auto Scaling et dont il vous affranchit de la complexité.



Création d'un compte AWS

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

The screenshot shows the AWS homepage with a dark blue background featuring a geometric cube pattern. At the top, there's a navigation bar with links for 'Produits', 'Solutions', 'Tarification', 'Documentation', 'Apprendre', 'Réseau de partenaires', 'AWS Marketplace', 'Déploiements clients', 'Découvrir davantage', and a search icon. On the right side of the top bar are links for 'Contacter l'équipe commerciale', 'Support', 'Français', 'Mon compte', and a prominent orange 'Créer un compte AWS' button. Below the navigation bar, a purple banner contains the text 'Voir les initiatives prises par AWS et sa réponse dans le contexte du COVID-19 >'. The main content area features a large white text block: 'Commencez dès aujourd'hui à créer avec AWS'. Below this, a paragraph explains: 'Que vous recherchez des options de puissance de calcul, de stockage de bases de données, de diffusion de contenu ou d'autres fonctionnalités, AWS dispose des services nécessaires pour vous aider à créer des applications sophistiquées en améliorant la flexibilité, l'évolutivité et la fiabilité'. A thick yellow arrow points from the bottom left towards the 'Créer un compte gratuit' button, which is highlighted with a yellow box.

Formulaire d'inscription
À remplir avec un email valide
vous allez devoir confirmer votre compte.

Créer un compte AWS

Les comptes AWS comprennent 12 mois d'accès à l'offre gratuite

Comprend l'utilisation d'Amazon EC2, Amazon S3 et Amazon DynamoDB

Pour connaître les conditions complètes de l'offre, visitez le site aws.amazon.com/free

Adresse e-mail

Mot de passe

Confirmer le mot de passe

Nom de compte AWS ⓘ

Continuer

Connectez-vous à un compte AWS existant

© 2019 Amazon Web Services, Inc. ou ses filiales. Tous droits réservés.
[Politique de confidentialité](#) [Conditions d'utilisation](#)

Veuillez sélectionner le type de compte et indiquer vos coordonnées dans les champs ci-dessous.

Type de compte ⓘ

Professionnel Personnel

Nom complet

→ Nom complet

Numéro de téléphone

→ Numéro de téléphone
0606060606

Pays/Région

→ Pays/Région
France

Adresse

→ Adresse
1 ma rue principale

Appartement, suite, ensemble, bâtiment, étage, etc.

Ville

→ Ville
MaVille

État/Province ou région

Code postal

Veuillez cocher cette case pour indiquer que vous avez lu et accepté les conditions générales du [Contrat client AWS](#)

→ Crée un compte et continuer

Informations paiement :

Veuillez saisir vos informations de paiement, afin que nous puissions vérifier votre identité. Votre compte ne sera pas débité, sauf si votre utilisation dépasse les [limites de l'offre gratuite AWS](#). Pour plus d'informations, consultez [les questions fréquentes](#).

Numéro de carte de crédit ou de paiement



Date d'expiration



Nom du titulaire de la carte



Adresse de facturation

Utiliser mon adresse de contact

Utiliser une nouvelle adresse



Vérification téléphonique

Phone Verification

AWS will call you immediately using an automated system. When prompted, enter the 4-digit number from the AWS website on your phone keypad.

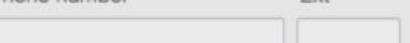
Provide a telephone number

Please enter your information below and click the "Call Me Now" button.

Country/Region code



Phone number



Ext

Security Check





Accès Support AWS



Select a Support Plan

AWS offers a selection of support plans to meet your needs. Choose the support plan that best aligns with your AWS usage. [Learn more](#)

Basic Plan	Developer Plan	Business Plan
Free	From \$29/month	From \$100/month
<ul style="list-style-type: none">Included with all accounts24/7 self-service access to forums and resourcesBest practice checks to help improve security and performanceAccess to health status and notifications	<ul style="list-style-type: none">For early adoption, testing and developmentEmail access to AWS Support during business hours1 primary contact can open an unlimited number of support cases2-hour response time for nonproduction systems	<ul style="list-style-type: none">For production workloads & business-critical dependencies24/7 chat, phone, and email access to AWS SupportUnlimited contacts can open an unlimited number of support cases1-hour response time for production systems

Need Enterprise level support?

Contact your account manager for additional information on running business and mission critical-workloads on AWS (starting at \$15,000/month). [Learn more](#)

Connectez vous à la Console AWS

AWS Management Console

AWS services

Find Services
You can enter names, keywords or acronyms.

▶ Recently visited services

▶ All services

Build a solution
Get started with simple wizards and automated workflows.

Launch a virtual machine With EC2 2-3 minutes 	Build a web app With Elastic Beanstalk 6 minutes 	Build using virtual servers With Lightsail 1-2 minutes 	Connect an IoT device With AWS IoT 5 minutes 
Start a development project With CodeStar 5 minutes 	Register a domain With Route 53 3 minutes 	Deploy a serverless microservice With Lambda, API Gateway 2 minutes 	Create a backend for your mobile app With Mobile Hub 5 minutes 

Access resources on the go

 Access the Management Console using the Mobile App. [Learn more](#)

Explore AWS

Amazon RDS
Set up, operate, and scale your relational database cloud. [Learn more](#)

AWS Marketplace
Find, buy, and deploy popular software products to AWS. [Learn more](#)

Amazon SageMaker
Machine learning for every developer and data scientist. [Learn more](#)

Open Distro for Elasticsearch
A 100% open-source, community driven distribution of Elasticsearch with enterprise-grade security and all features. [Learn more](#)

Have feedback?

 Submit feedback to tell us about your experience with the AWS Management Console.

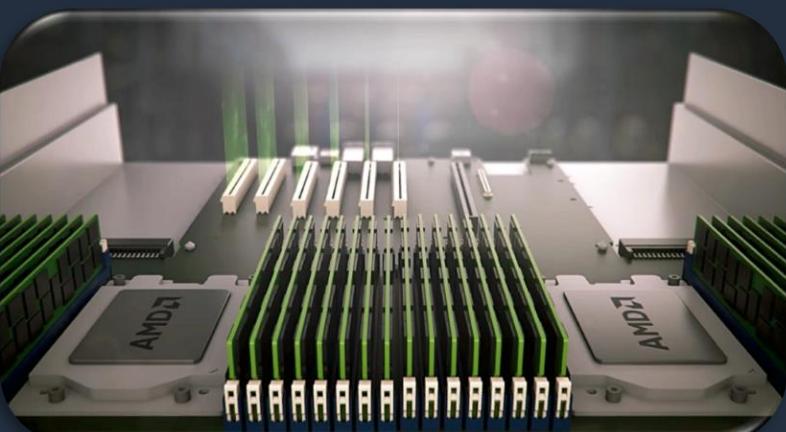
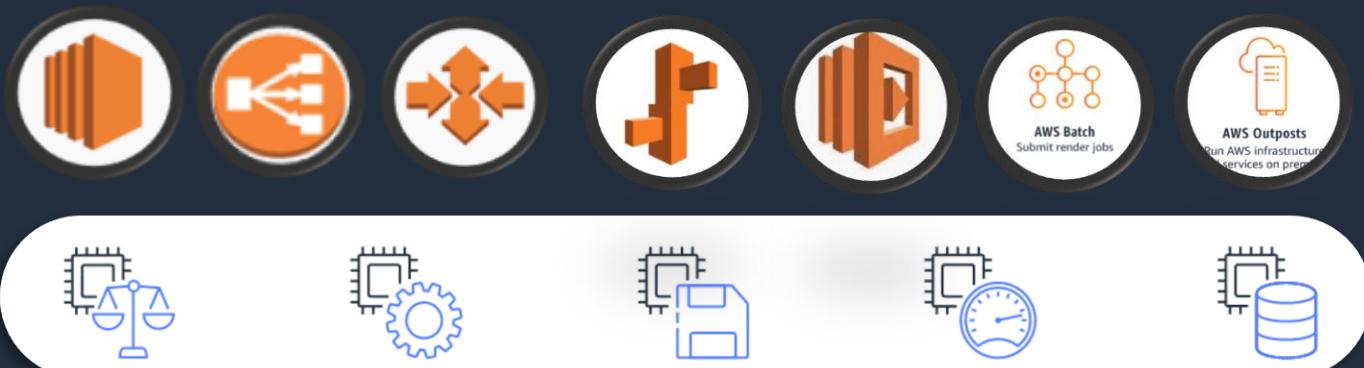
 [Leave feedback](#)

Les services de CALCUL



Qu'est ce que le CALCUL ?

Il s'agit des ressources nécessaires à l'accomplissement des **tâches élémentaires** sur lesquelles reposent les applications logicielles et les systèmes exécutant des processus et des algorithmes



Amazon EC2

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (région)

Fonctionnalités :

Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>



Elastic Compute Cloud

VM ou instance (IAAS)

- Amazon Machine Image (AMI)
- Données utilisateurs (userdata)
- Stockage
- Réseau
- Groupes de Sécurité
- Monitoring

Tarification

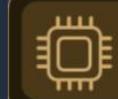
- On demand
- Reserved
- Spot
- Dedicated instance
- Dedicated Host

Ec2

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.prahsield.com/home>



Types d'instance



CPU

- Small models
- Small datasets
- Useful for design space exploration

General



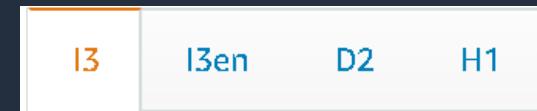
Compute



Memory



Storage



GPU

- Medium-to-large models, datasets
- Image, video processing
- Application on CUDA or OpenCL



TPU

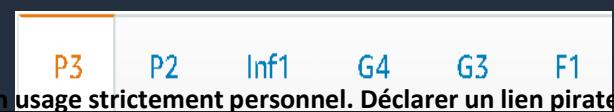
- Matrix computations
- Dense vector processing
- No custom TensorFlow operations



FPGA

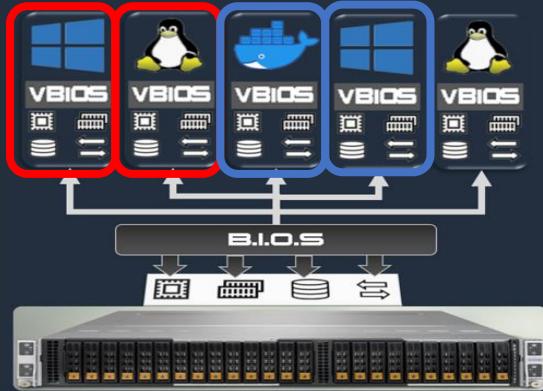
- Large datasets, models
- Compute intensive applications
- High performance, high perf / cost ratio

Accelerated Computing



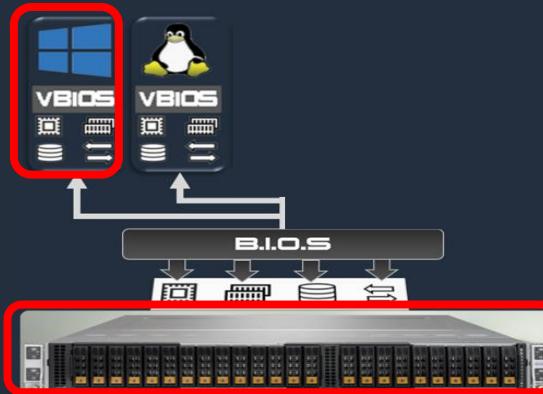


Understanding AWS Tenancy



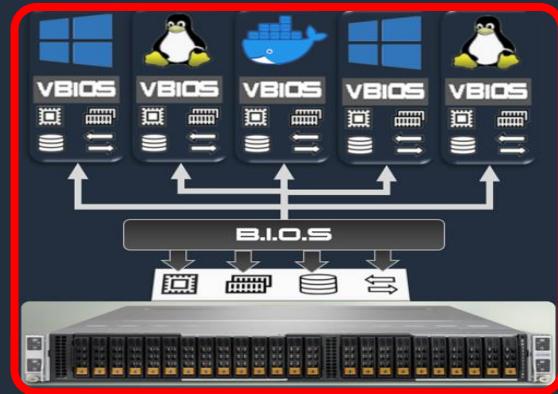
Shared (Partagée)

- Instance démarrée sur des ressources partagées avec plusieurs clients
- Sécurité par isolation logique des instances
- Changement d'hôte possible



Dedicated instance

- Instance démarrée sur du matériel avec accès restreint
- Répond aux contraintes de sécurité spécifiques
- Frais supplémentaires
- Changement d'hôte possible



Dedicated Host

- Matériel dédiée pour plusieurs instances
- Contrôles matériel avancés
- Répond aux contraintes de sécurité spécifiques
- Pas de changement d'hôte

BYOL



AWS License Manager

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

<https://aws.amazon.com/fr/license-manager/>



vmware



Windows Server



ORACLE



Elastic Compute Cloud



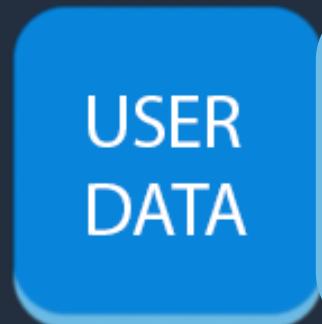
AMI



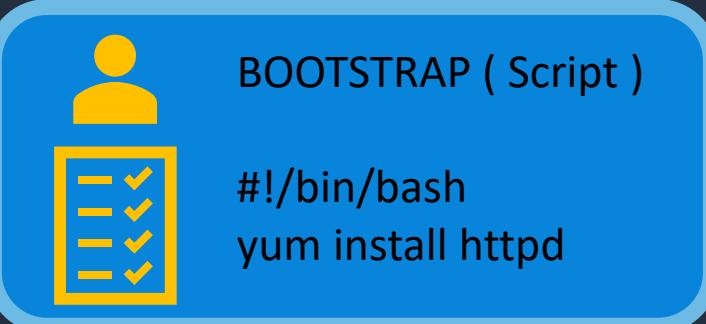
EC2 Instances



Type



USER DATA



Stockage



Ephemeral
Interne au serveur
Données perdues en
cas d'arrêt de
l'instance mais
supporte les
redémarrages



Persistent
EBS Accessibles via le
réseau aws
Indépendant de
l'instance
Chiffrement et
données à 100%
accessibles via
backup



Cloudwatch

Security Groups



Status checks et groupes de sécurité

System Status Checks

- Problèmes de logiciels sur l'hôte physique
- Perte de connectivité au réseau
- Perte de pouvoir du système
- Problèmes de matériel sur l'hôte physique (accessibilité)

Instance Status Checks

- Configuration incorrecte de la mise en réseau ou du démarrage
- Échec des vérifications de l'état du système
- Système de fichiers corrompus
- Noyau incompatible
- Mémoire saturée

Screenshot of the AWS Management Console showing the 'Status Checks' tab for an instance. The tab is highlighted in orange.

Description **Status Checks** **Monitoring** **Tags**

Status checks detect problems that may impair this instance from running your applications. [Learn more](#) about status checks.

Create Status Check Alarm

System Status Checks ⓘ

These checks monitor the AWS systems required to use this instance and ensure they are functioning properly.

System reachability check passed

Instance Status Checks ⓘ

These checks monitor your software and network configuration for this instance.

Instance reachability check failed at October 7, 2013 11:52:11 AM UTC+2 (16 minutes ago)

[Learn more about this issue](#)

Additional Resources

[Submit feedback](#) if our checks do not reflect your experience with this instance or if they do not detect the issues you are having.

Please note that we will not respond to customer support issues reported via this form. Please post your issue on the [Developer Forums](#) or contact [AWS Support](#) if you need technical assistance with this instance.



groupes de sécurité

Source & destination

Règles entrées sorties

Ports et protocoles autorisés

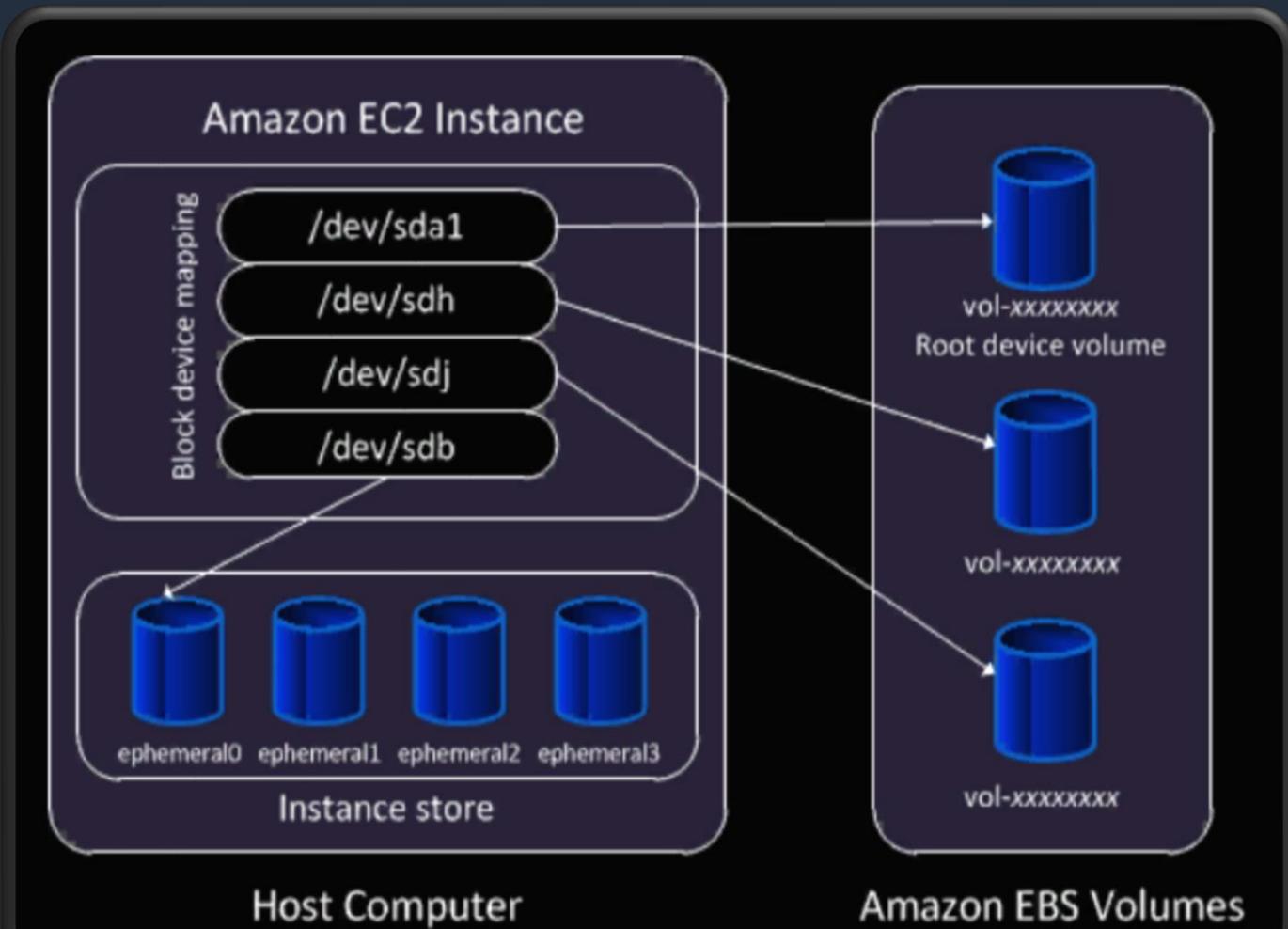


Le stockage par bloc

DAS (Direct-Attached Storage) ou SAN (Storage Area Network).

Amazon Elastic Block Store (EBS), connecté aux serveurs virtuels offre une latence extrêmement faible, requise pour les charges de travail à hautes performances.

- Données découpées en bloc de taille fixe (ex : 4ko)
- Une table d'allocation est nécessaires pour localiser les données
- Lectures et écritures se font au niveau des blocs
- Protocoles : Hdd sas, iSCSI, FC, FCoE
- Ultra rapide, débit important, latence ultra faible
- Magnétiques, SSD, Nvme, (snapshots, AMI) (RAID0,1,10)





Tarifications & Cas d'usages

**ON
DEMAND**

- Disponible 24h/24h - 7j/7j
- Sans engagement
- Pas de frais initiaux
- Paiement à l'usage
- Facturé l'heure ou à la seconde

Recommandé pour :

- Les utilisateurs préférant profiter du coût avantageux et de la flexibilité du cloud
- Les charges de travail irrégulières ou imprévisibles ne pouvant être interrompues
- Les applications développées ou testées sur Amazon EC2 pour la première fois



Tarifications & Cas d'usages

SPOT

- Accessibles via des enchères pour les ressources non utilisées AWS
- Sans garantie de durée et peut être interrompu à tout moment
- Sans engagement
- Pas de frais initiaux
- Paiement à l'usage
- Facturé l'heure ou à la seconde

Recommandé 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 besoins de calculs urgents pour de grandes quantités de calcul ponctuelles



Tarifications & Cas d'usages

RESERVED

- Avec engagement
- Pour une durée définie qui conditionne la baisse du prix
- Frais initiaux complets pour une durée 1 an ou 3 an
- Frais initiaux partiels réduction de la réduction de prix obtenue
- Sans frais initiaux réduction la plus basse

Recommandé pour :

Les applications à usage d'état stable

Les applications pouvant nécessiter des capacités réservées

Les clients qui peuvent s'engager pendant 1 ou 3 ans pour réduire leurs coûts



Tarifications & Cas d'usages

DEDICATED

- Accès aux contrôles avancés matériel
- Sans engagement (réservation possible)
- Pas de frais initiaux (sauf en cas de réservation)
- Paiement à l'usage
- Facturé l'heure

Recommandé pour :

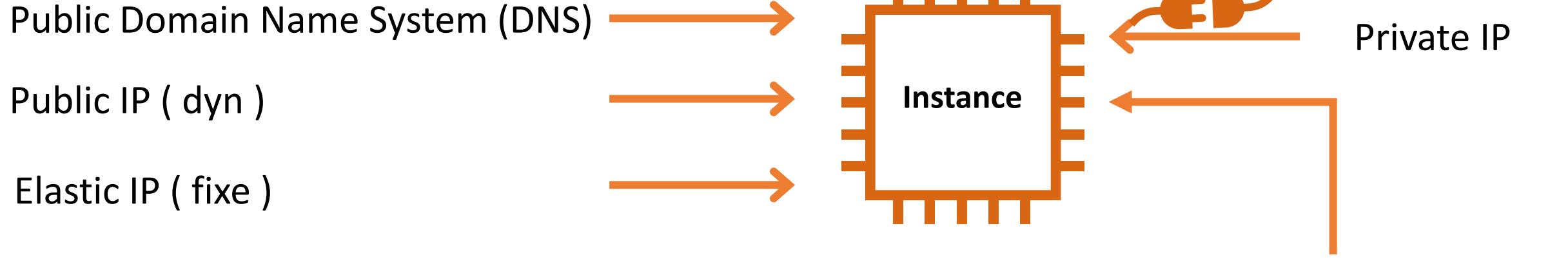
- Réduction des coûts en utilisant vos propres licences (-70%)
- Contraintes licences logiciels
- Contraintes sécurité des données ou de conformité



Une instance peut être accessible de plusieurs façons dès sa création

Carte Ethernet Ethernet :

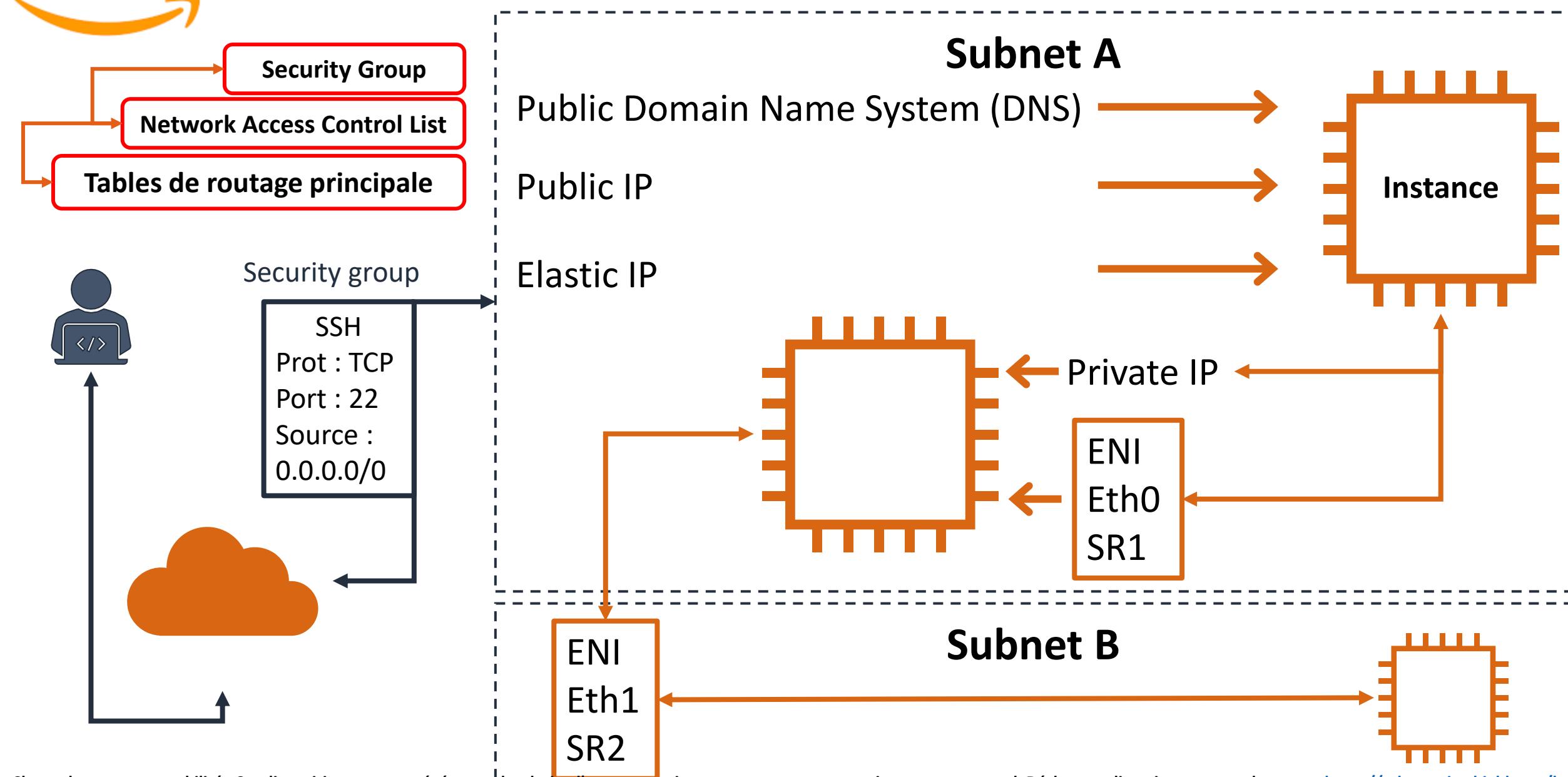
```
Suffixe DNS propre à la connexion. . . . . :  
Adresse IPv4. . . . . : 192.168.1.30  
Masque de sous-réseau. . . . . : 255.255.255.0  
Passerelle par défaut. . . . . : 192.168.1.254
```



Les adresses IP privées et les interfaces de réseau élastiques (ENI) sont des méthodes supplémentaires d'adressage des instances disponibles mais uniquement dans le cadre interne d'un VPC Amazon



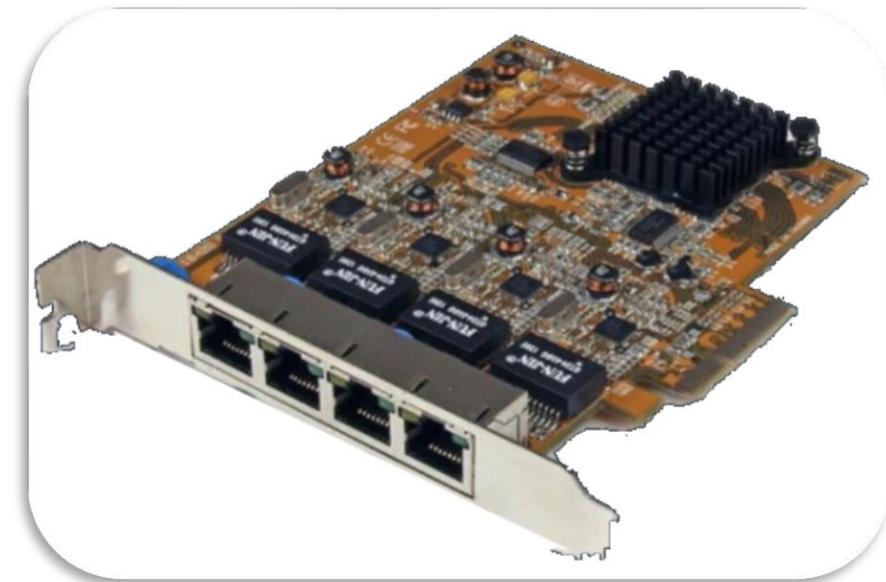
Accès externes - Accès internes (Subnet)





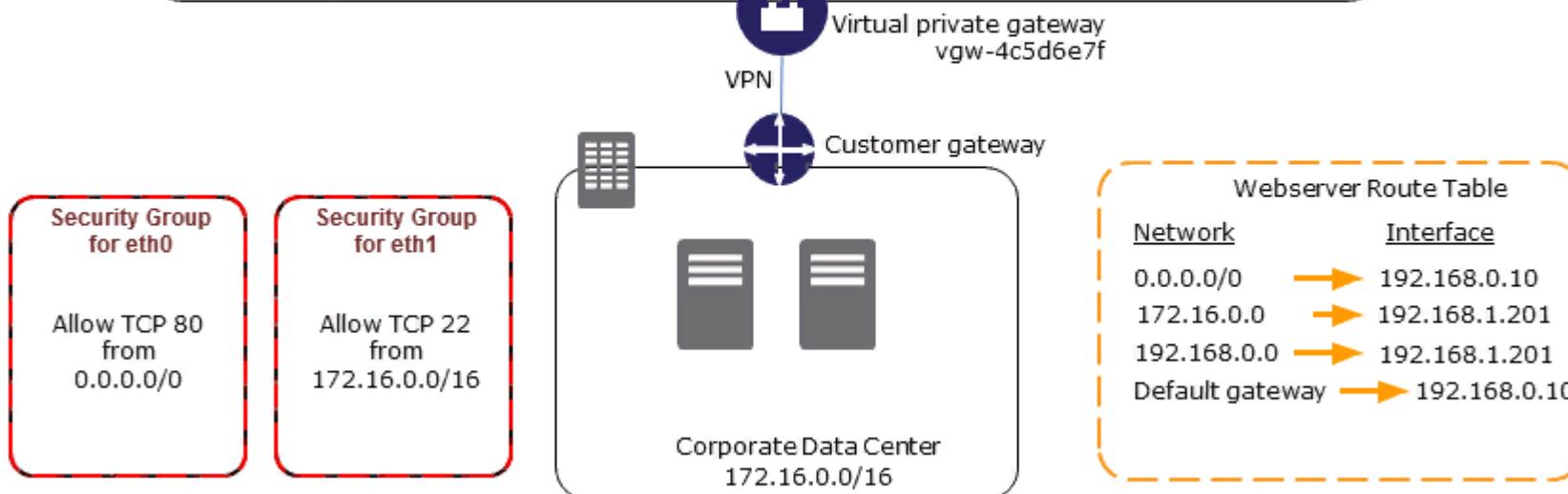
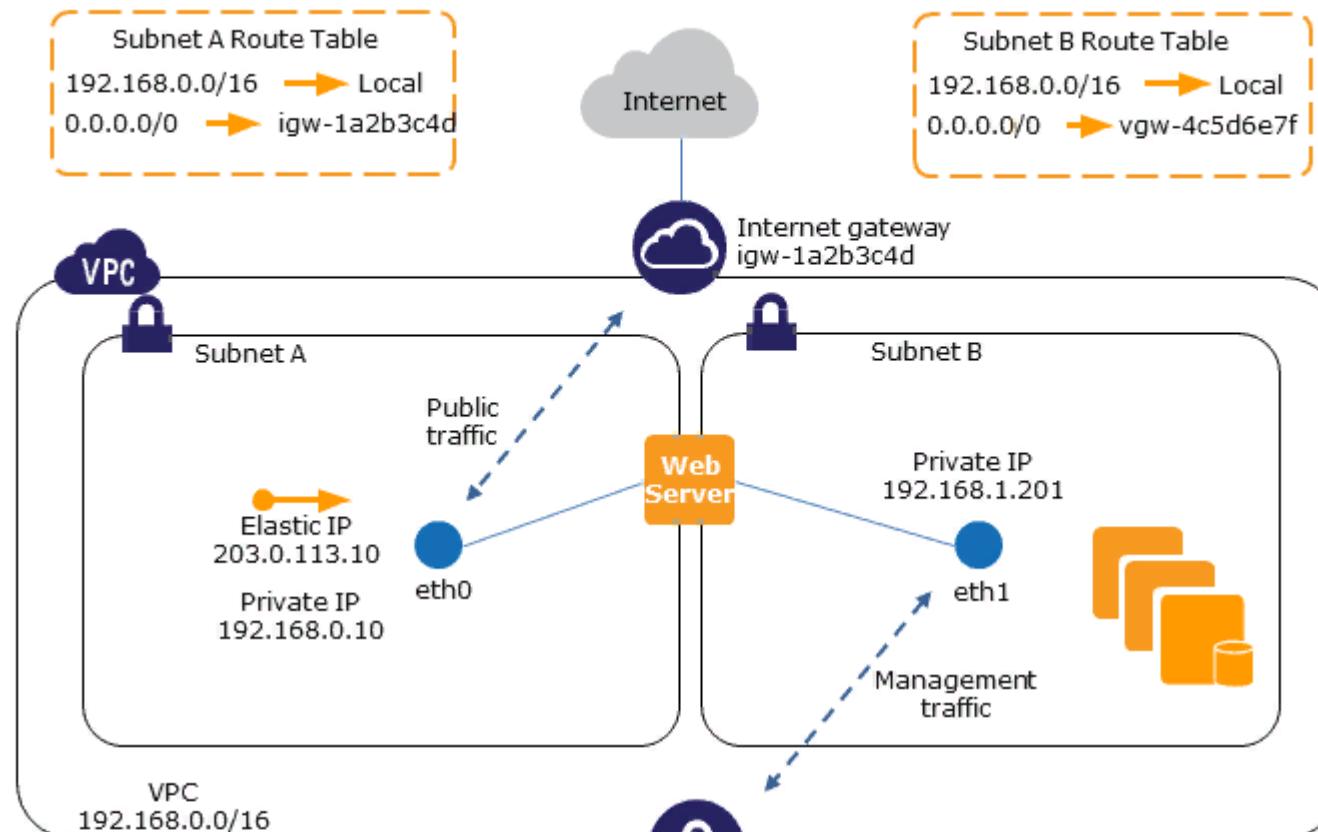
Une *interface réseau élastique* (ENI) est un composant réseau logique dans un VPC qui représente une carte réseau virtuelle.

- Une adresse IPv4 privée « primaire »
- Une ou plusieurs adresses IPv4 privées « secondaires »
- Une adresse IP Elastic (IPv4) (par adresse IPv4 privée)
- Une adresse IPv4 publique
- Une ou plusieurs adresses IPv6
- Un ou plusieurs groupes de sécurité
- Une adresse MAC
- Un indicateur de vérification de source/destination
- Une description



Cas d'usages :

- créer un réseau de gestion
- utiliser des composants de réseau et de sécurité dans votre VPC
- créer des instances à 2 interfaces réseau avec des charges de travail sur des sous-réseaux distincts;
- créer une solution haute disponibilité à faible coût.





La mise en réseau améliorée utilise la virtualisation d'I/O d'une racine unique (**SR-IOV**) pour fournir des fonctionnalités de mise en réseau hautes performances sur les types d'instance pris en charge.

Types de mise en réseau améliorée

- Mise en réseau améliorée : **Intel 82599 VF**
 - L'interface Intel 82599 **Virtual Function** prend en charge les vitesses réseau allant jusqu'à **10 Gbit/s**
 - Les instances C3, C4, D2, I2, M4 (à l'exclusion de m4.16xlarge) et R3
- Mise en réseau améliorée : **ENA Elastic Network Adapter**
 - Elastic Network Adapter (ENA) prend en charge des vitesses réseau allant jusqu'à **100 Gbit/s**
 - Les instances A1, C5, C5d, C5n, F1, G3, G4, H1, I3, I3en, m4.16xlarge, M5, M5a, M5ad, M5d, M5dn, M5n, P2, P3, R4, R5, R5a, R5ad, R5d, R5dn, R5n, T3, T3a, u-6tb1.metal, u-9tb1.metal, u-12tb1.metal, u-18tb1.metal, u-24tb1.metal, X1, X1e, and z1d

Avantages :

- bande passante supérieure allant jusqu'à 100 Gbps (limité à 10 pour l'intel 82599)
- Performances de paquet par seconde (PPS) nettement plus élevées
- Latences réduites entre les instances.

Cas d'usages :

- Débit important > 10Gbps ou 100Gbps
- Latence très faible
- Mise en réseau améliorée sur Linux

>> L'utilisation de la mise en réseau améliorée n'implique aucun coût supplémentaire.

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

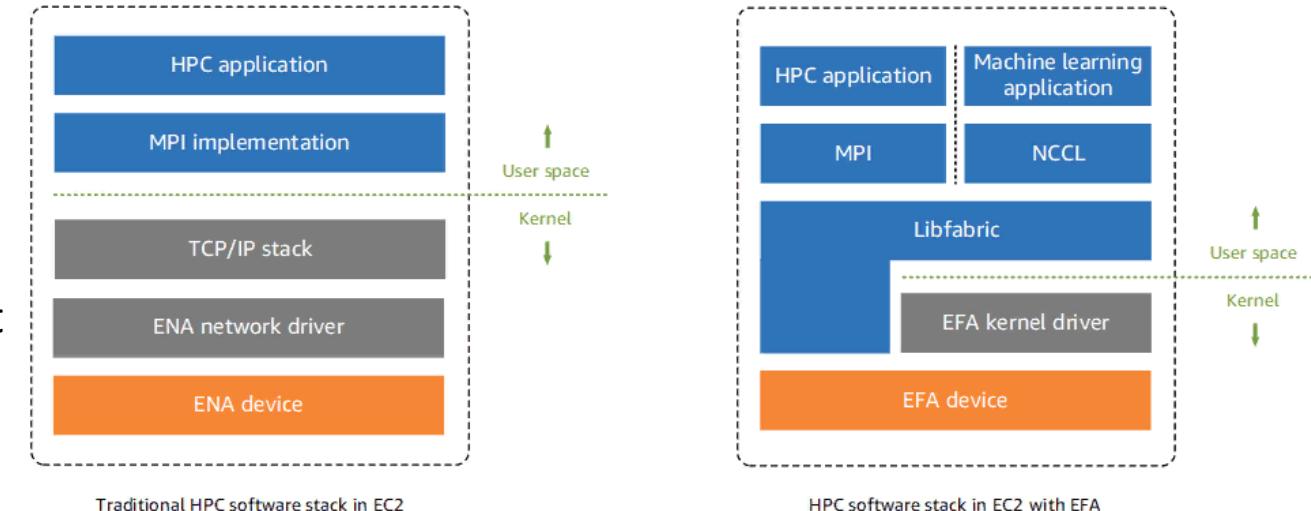


Elastic Fabric Adapter (EFA) est un périphérique réseau que vous pouvez attacher à votre instance Amazon EC2 pour accélérer les applications HPC (Calcul Haute Performance).

Principes de base EFA

Un EFA est un adaptateur Elastic Network Adapter (ENA) avec des capacités ajoutées. Il offre toutes les fonctionnalités d'un ENA, avec des capacités de contournement du système d'exploitation supplémentaires (OS Bypass)

Le contournement du système d'exploitation (**OS-Bypass**) est un modèle d'accès qui permet aux applications **HPC** et de **Machine Learning** de communiquer directement avec le matériel de l'interface réseau pour offrir des fonctionnalités de transport fiable à faible latence.



Limitations :

- Vous ne pouvez attacher qu'un seul EFA par instance.
- Si **OS-Bypass** EFA est limité à un seul sous-réseau
- Si **OS-Bypass** le trafic EFA n'est pas routable

Cas d'usages :

- Applications HPC
- Machine Learning
- OS-Bypass





Groupes de placement (placement groups)

Cluster : regroupe des instances rapprochées à l'intérieur d'une Zone de disponibilité. Cette stratégie permet aux charges de travail d'atteindre les performances réseau à faible latence nécessaires à une communication de nœud à nœud étroitement couplée, typique des applications HPC.

Partition : répartit les instances entre les partitions logiques de façon à ce que des groupes d'instances d'une partition ne partagent pas le matériel sous-jacent avec des groupes d'instances d'autres partitions. Cette stratégie est généralement utilisée par les grandes charges de travail distribuées et répliquées telles que **Hadoop, Cassandra, et Kafka**.

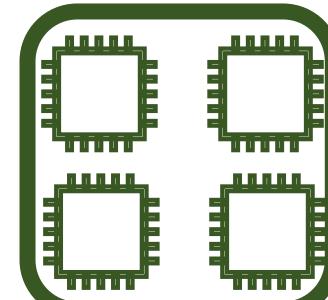
Spread : place strictement un petit groupe d'instances sur un matériel sous-jacent distinct pour réduire les défaillances corrélées. Un groupe de placement par répartition peut également s'étendre sur plusieurs Zones de disponibilité dans la même région. Vous pouvez disposer de jusqu'à **sept instances en cours d'exécution par Zone de disponibilité et par groupe**.

Il n'y a aucun frais pour la création d'un groupe de placement.

Cluster Partition Spread

Region EU-WEST-1

AZ-A

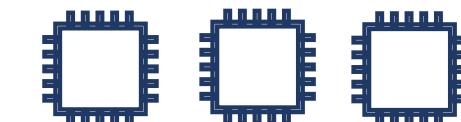
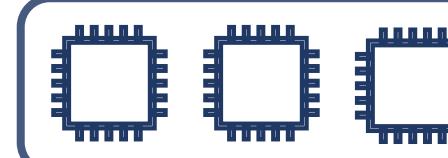
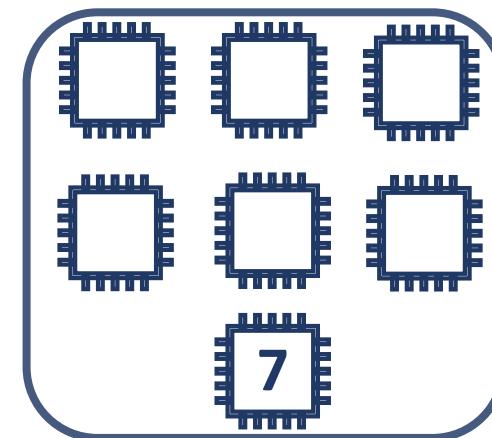
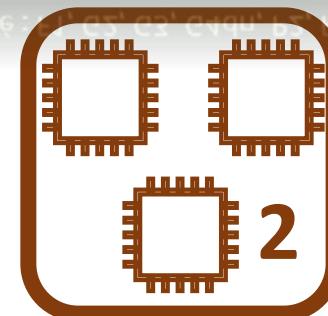
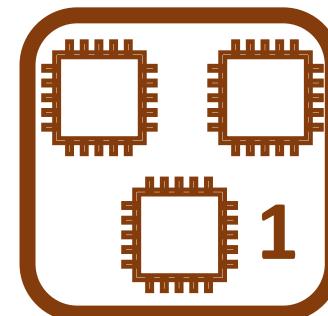
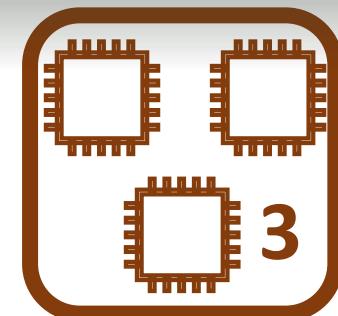


AZ-B

- Usage général : A1, M4, M5, M5a, M5ad, M5d, M5dn, M5n
- Calcul optimisé : C3, C4, C5, C5d, C5n, cc2.8xlarge
- Mémoire optimisée : cr1.8xlarge, R3, R4, R5, R5a, R5ad, R5d, R5dn, R5n, X1, X1e, z1d
- Stockage optimisé : D2, H1 hs1.8xlarge, I2, I3, i3en
- Calcul accéléré : F1, G2, G3, G4dn, P2, P3, P3dn

up to 10 Gbps for TCP/IP

AZ-C





Règles et restrictions des groupes de placement

- Le nom que vous spécifiez pour un groupe de placement doit être unique au sein de votre compte AWS pour la région.
- Vous ne pouvez pas fusionner (to merge) des groupes de placement.
- Une instance peut être lancée dans un seul groupe de placement à la fois et ne peut pas s'étendre sur plusieurs groupes de placement.
- Réservation de capacité à la demande et les Instances réservées zonales fournissent une réservation de capacité pour les instances EC2 dans une zone de disponibilité spécifique.
- La réservation de capacité peut être utilisée par les instances d'un groupe de placement. Toutefois, il n'est pas possible de réserver explicitement de la capacité pour un groupe de placement.
- Les instances avec une location d'hôte serveur ne peuvent pas être lancées dans des groupes de placement.

Il n'y a aucun frais pour la création d'un groupe de placement.

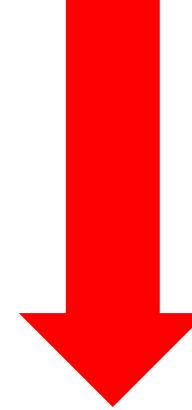


Règles et restrictions des groupes de placement

Règles et restrictions des groupes de placement du cluster

Règles et restrictions des groupes de placement par partition

Règles et restrictions des groupes de placement par répartition



https://docs.aws.amazon.com/fr_fr/AWSEC2/latest/UserGuide/placement-groups.html#placement-groups-cluster



Amazon machine image (AMI)

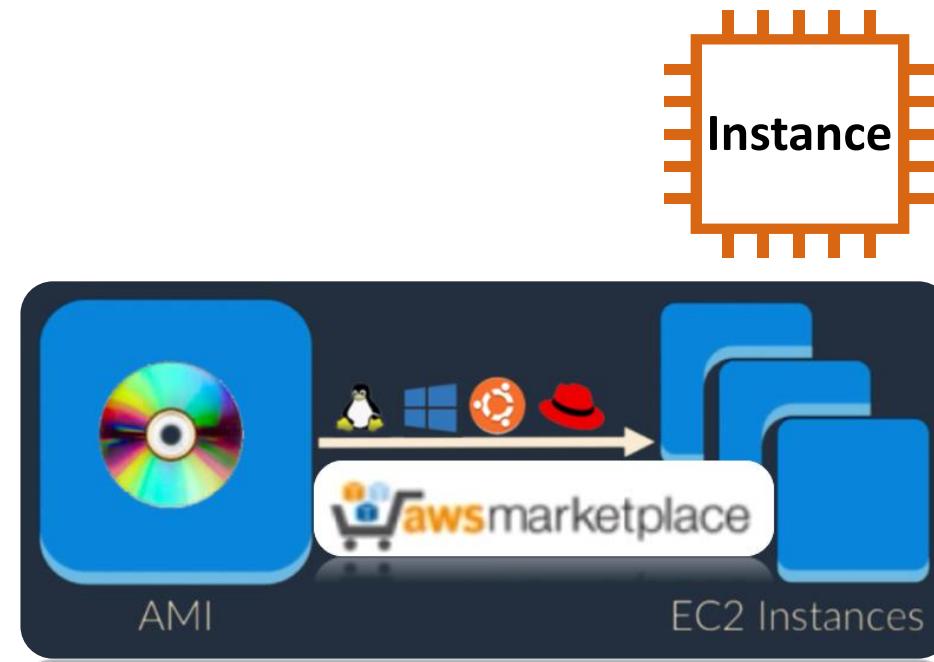
Deux concepts sont essentiels pour lancer des instances sur AWS : Les ressources matérielles dédiées à l'instance et le logiciel chargé sur l'instance. (en résumé Le type d'instance et l'AMI)

Une AMI définit chaque aspect de l'état du logiciel au lancement de l'instance :

- Le système d'exploitation (OS) et sa configuration
- L'état initial de tout patch
- Logiciel d'application ou de système

Il existe quatre sources d'AMI :

- Publiées par AWS
- L'AWS Marketplace
- Générées à partir d'instances existantes
- Serveurs virtuels téléchargés



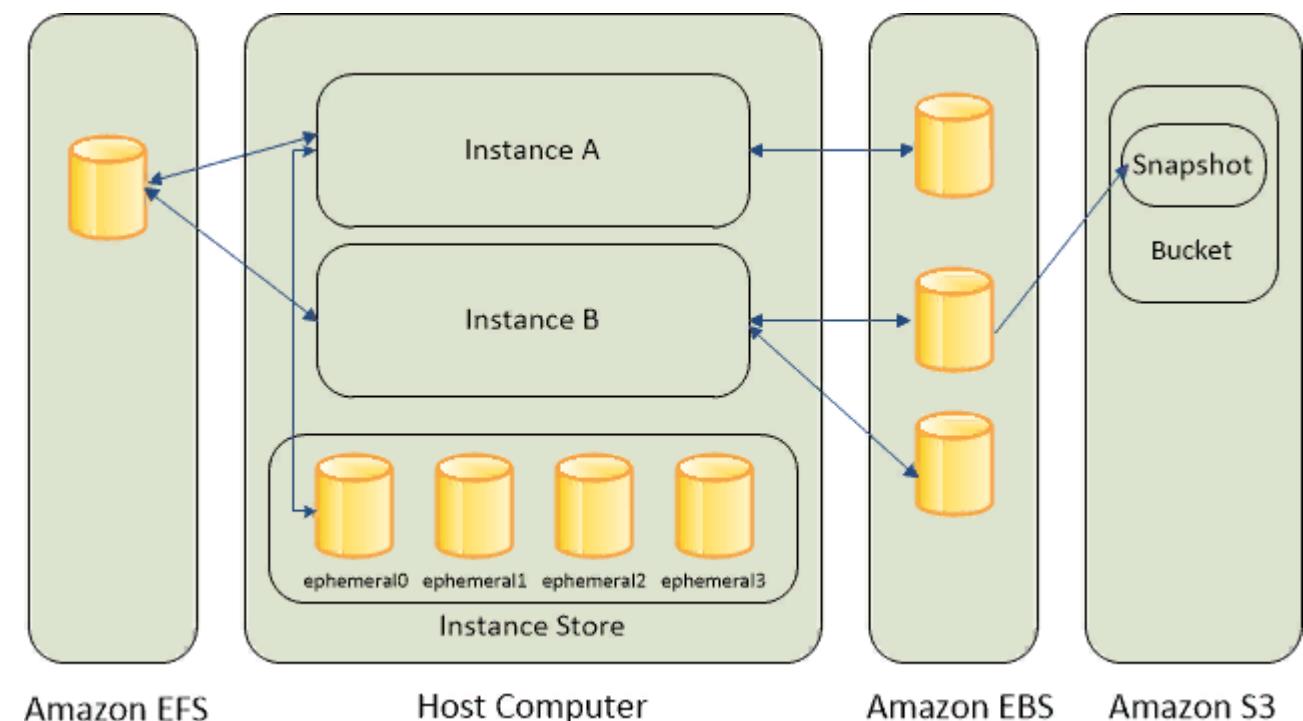


Amazon machine image (AMI)

Lors de la sélection d'une AMI :

- Région (déploiement dans une région et une zone de disponibilité)
- Le système d'exploitation et son architecture – 32 ou 64 bits
- Permissions de lancement
- Stockage pour le volume système (EBS ou Instance Store aka ephemeral storage volume)

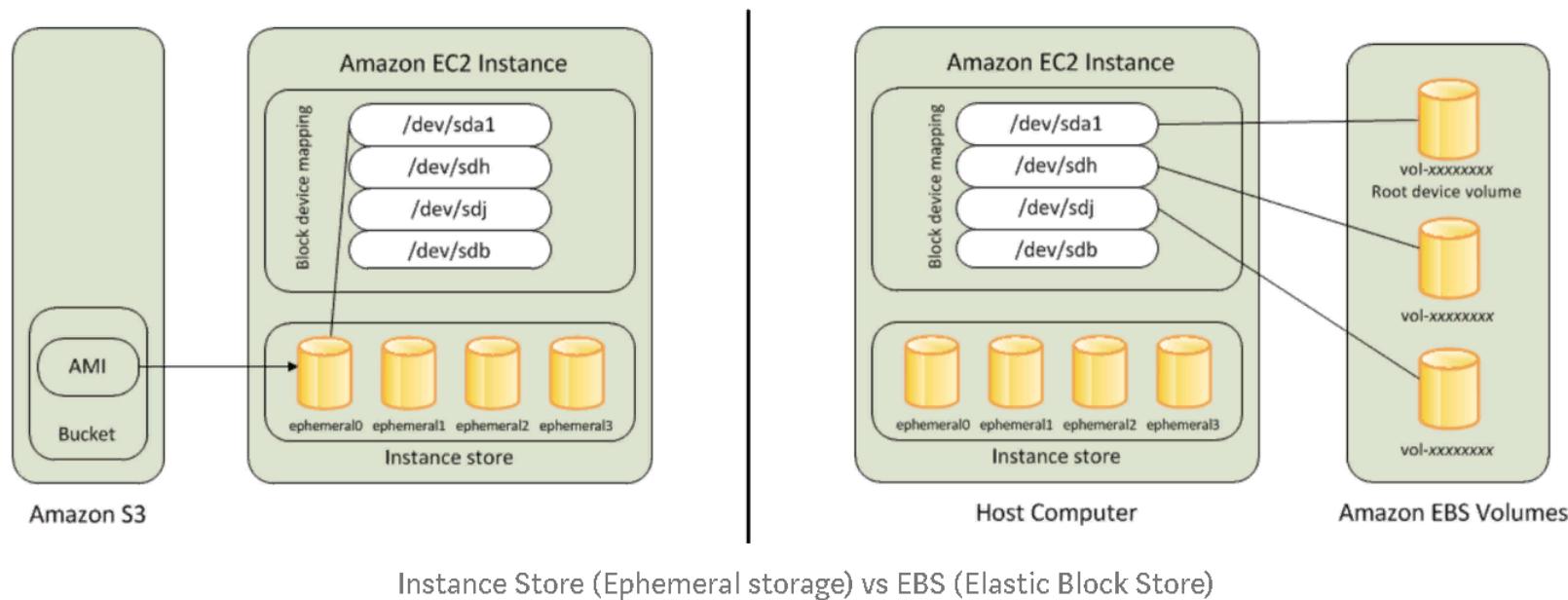
Un *stockage d'instance* fournit un stockage temporaire de niveau bloc pour votre instance. Le stockage réside sur les disques physiquement attachés à l'ordinateur hôte. Le stockage d'instance est particulièrement adapté pour le stockage temporaire d'informations qui changent fréquemment, telles que les tampons, les caches, les données temporaires et autres contenus provisoires, ou pour les données répliquées sur une flotte d'instances, telle qu'un pool à charge équilibrée de serveurs web.





Amazon machine image (AMI)

- “Instance store backed instance” est une instance EC2 utilisant un magasin d'instance comme volume de périphérique racine créé à partir d'un modèle stocké dans S3.



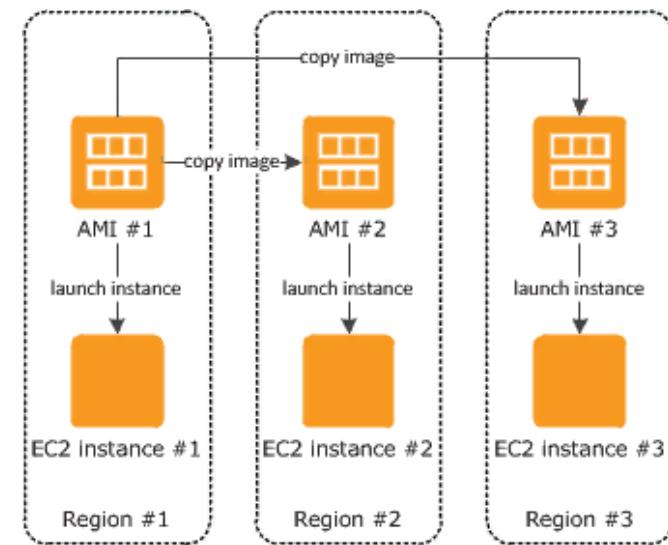
- An “EBS-backed” instance signifie que le point de montage racine d'une instance lancée depuis l'AMI est un volume EBS créé à partir d'un snapshot EBS.



Amazon machine image (AMI)

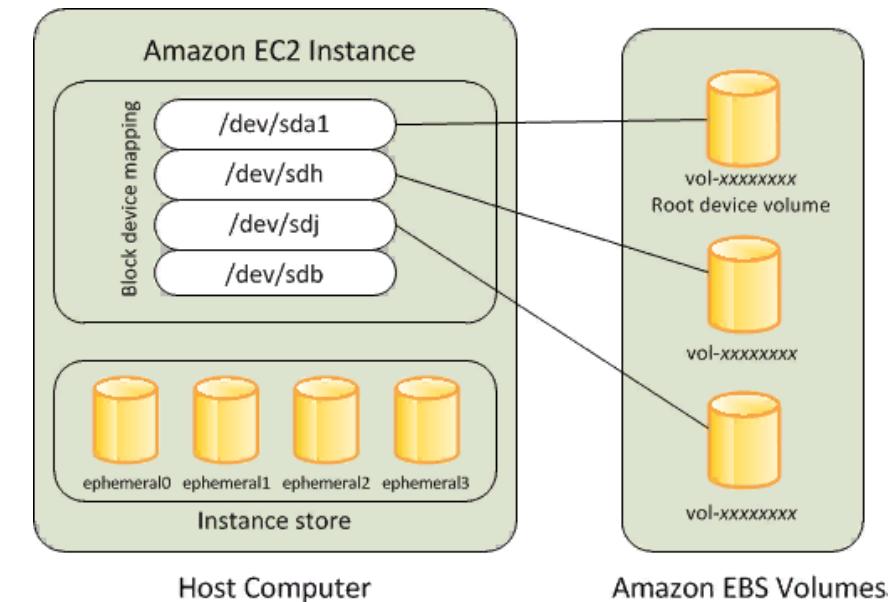
Copie et partage d'une AMI :

- Vous pouvez partager une AMI avec un autre compte AWS. Le partage d'une AMI n'affecte pas la propriété de celle-ci. Le compte propriétaire est facturé pour le stockage dans la région.
- Vous pouvez copier une Amazon Machine Image (AMI) au sein d'une région AWS ou de plusieurs régions à l'aide d'AWS Management Console, CLI, SDK, ou encore de l'API Amazon EC2, qui prennent tous en charge l'action CopyImage.
- Si vous copiez une AMI qui a été partagée avec votre compte, vous êtes le propriétaire de l'AMI cible de votre compte. Le propriétaire de l'AMI source se voir facturer des frais de transfert Amazon EBS ou Amazon S3, et vous devez régler le stockage de l'AMI cible dans la région de destination.
- Vous pouvez copier les AMI avec des instantanés chiffrés et également modifier le statut de chiffrement pendant le processus de copie. Sauf en cas de partage d'une AMI chiffrée.
- Vous ne pouvez pas copier une AMI obtenue à partir d'AWS Marketplace, que vous l'ayez obtenue directement ou qu'elle ait été partagée avec vous. *À la place, lancez une instance EC2 en utilisant l'AMI d'AWS Marketplace, puis créez une AMI à partir de cette instance.* (Idem pour les produits soumis à licences, comme les instances Windows ou les instances avec un code d'activation logiciel.)



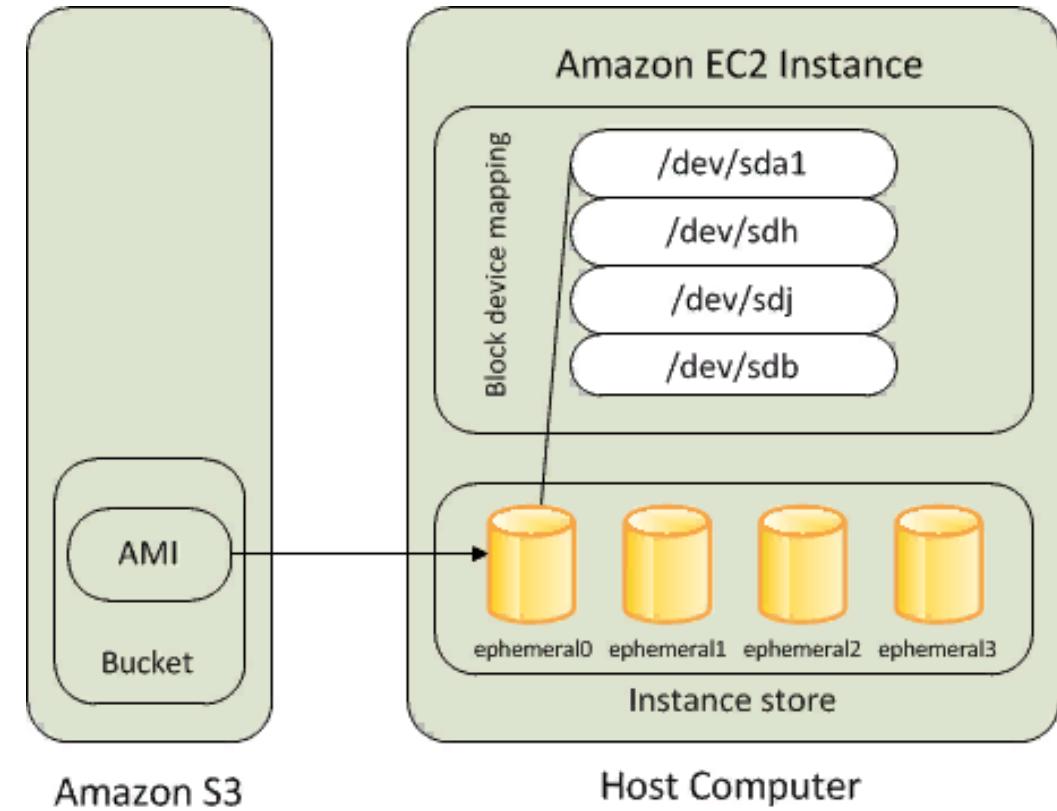
aws Amazon machine image (AMI) instance store

- Une instance "EBS-backed" signifie que le point de montage racine d'une instance lancée depuis l'AMI est un volume EBS créé à partir d'un snapshot EBS
- Un volume EBS se comporte comme un périphérique de bloc externe brut, non formaté, qui peut être attaché à une seule instance et n'est pas physiquement attaché à l'ordinateur hôte de l'instance (voir comme un NAS).
- Le volume persiste indépendamment de la durée de vie 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.
- Un volume EBS peut être détaché d'une instance et attaché à une autre instance.
- Les volumes EBS peuvent être créés en tant que volumes cryptés à l'aide de la fonction de cryptage EBS.
- L'EBS est une mémoire de bloc qui est attachée séparément à l'EC2. Il est également conçu de telle sorte qu'il sera répliqué dans sa zone de disponibilité, ce qui lui confère une grande disponibilité et une grande durabilité.
- Et l'avantage supplémentaire est que vous pouvez avoir des sauvegardes pour EBS en créant des instantanés, ce qui n'est pas possible avec le stockage d'instance. Ainsi, lorsque vous souhaitez récupérer les données, il vous suffit de créer le volume EBS à partir de l'instantané.



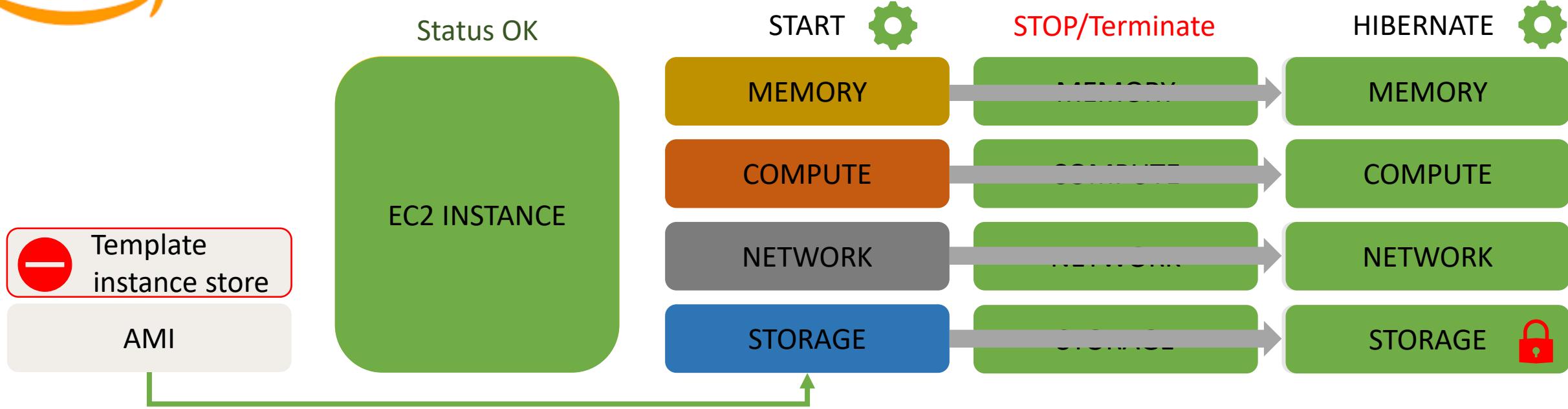
aws Amazon machine image (AMI) instance store

- **Instance store backed instance** est une instance EC2 utilisant un magasin d'instance comme volume de périphérique racine créé à partir d'un modèle stocké dans S3.
- **Instance store** est un stockage éphémère qui fournit un stockage temporaire au niveau du bloc pour votre instance. **Instance store** est idéal pour le stockage temporaire comme les tampons, les caches et autres contenus temporaires.
- Les volumes de stockage d'instance accèdent au stockage à partir de disques qui sont physiquement attachés à l'ordinateur hôte.
- **Instance stored instance** est lancée, l'image qui est utilisée pour démarrer l'instance est copiée sur le volume racine (généralement sda1).
- **Instance store** fournit un stockage temporaire au niveau du bloc pour les instances.
- Les données sur un volume de stockage d'instance ne persistent que pendant la durée de vie de l'instance associée ; si une instance est arrêtée ou terminée, toutes les données sur les volumes de stockage d'instance sont perdues.





EC2 Hibernation (suspend-to-disk)



Limitations :

- Instances C3, C4, C5, M3, M4, M5, R3, R4, R5.
- Mémoire : inférieure à 150 Go
- Bare metal non supporté
- Volume EBS doit être chiffré
- Instance (on demand or reserved) for 60 days max.

Cas d'usage

- Instances a démarrage long
- Processus intolérant au redémarrage
- Conserver les données mémoire



Spot instance – Spot Fleet – Request

- Permet d'accéder aux ressources de calcul non utilisées par Amazon, avec 90% de remise au maximum
- Le prix varie en fonction de la région et de la zone de dispo
- Par défaut, un compte ne peut pas avoir plus de 20 Instances Spot par région. (++ > AWS Support)
- Requêtes spot : prix max, nombre d'instances souhaitées
- Type de lancement : 1x (one time) ou persistant (persistent)
- Instances T3 ou T2 (standard ou unlimited)
- Spot Block permet de conserver une instance (1h et 6h)
- « Spot fleet » est un ensemble, ou parc, d'Instances Spot et, le cas échéant, d'Instances à la demande.
- états : Open, Active, Failed, Closed, disabled, cancelled.

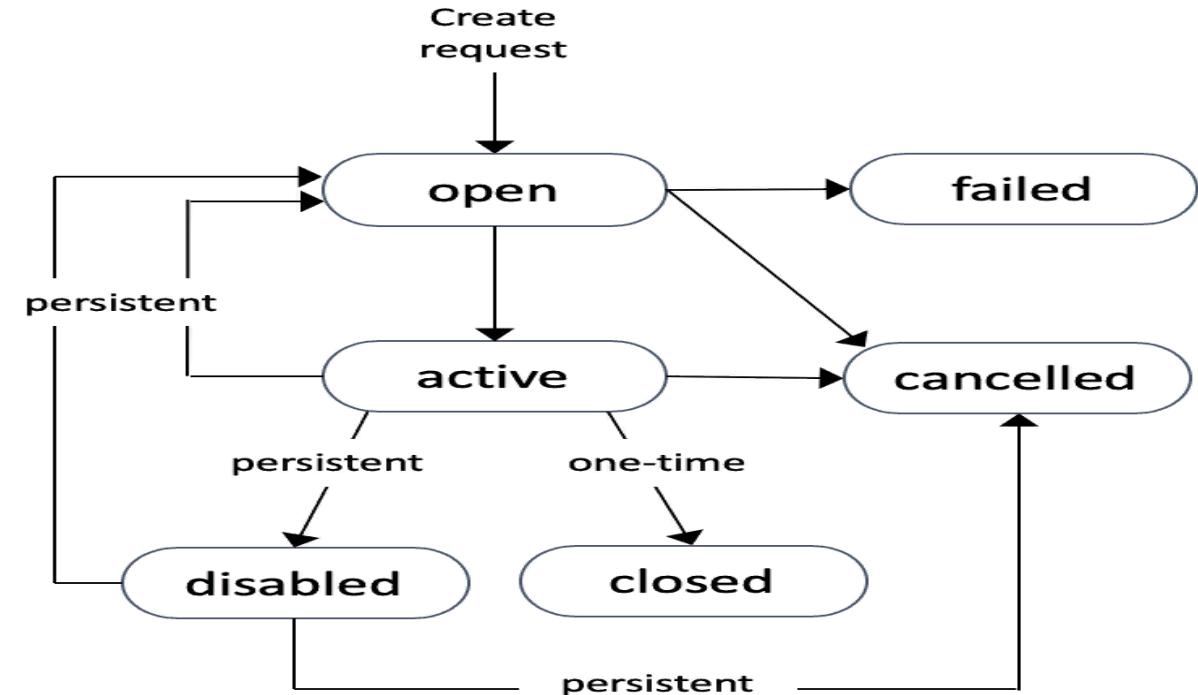
Important : Par défaut, les Instances Spot interrompues sont résiliées mais vous pouvez :

- Arrêter une instance Spot
- Mettre en veille prolongée une instance Spot
- Résilier une instance Spot (défaut)

Vous disposez d'une alerte 2 minutes avant résiliation.

✓ Analytics, Big Data, Web services, HPC, CI/CD, Container, traitement par lots de médias ou documents ...

✗ Bases de données, tâches continues, données persistantes



Les instances spot fonctionnent sauf si :

- Le client les résilie.
- Le prix actuel est supérieur au prix offert par le client
- Il n'y a pas assez de capacité inutilisée pour répondre à la demande d'instances spot.



Stratégie d'allocation et particularités

La stratégie d'allocation des Instances Spot dans votre « spot fleet » (parc d'instances spot) détermine la façon dont votre demande est satisfaite à partir des groupes (pools) d'instance Spot indiqués dans les spécifications de lancement.

- **LowestPrice** : Les Instances Spot proviennent du groupe offrant le prix le plus bas. Il s'agit de la stratégie par défaut.
- **Diversified** : Les Instances Spot sont réparties entre tous les groupes.
- **CapacityOptimized** : Les Instances Spot proviennent du pool d'instances Spot avec une capacité optimale pour le nombre d'instances qui sont lancées.
- **InstancePoolsToUseCount** : Les Instances Spot sont réparties entre le nombre de groupes d'instances Spot que vous spécifiez. Ce paramètre n'est valide que s'il est utilisé conjointement avec lowestPrice.

- ✓ *Les instances SPOT peuvent offrir des réductions de prix allant jusqu'à 90%*
- ✓ *Vous pouvez figer une instance spot pour empêcher son arrêt (Spot Block 1h à 6h max)*
- ✓ *Utilisable pour les traitements sans données persistantes*
- ✓ *Un parc (spot fleet) est une collection d'instance spot et potentiellement On demand.*
- ✓ *Différents état de demande : Open, Active, Failed, Closed, disabled, cancelled*



Instance Meta-data vs User-Data

Les *métadonnées d'instance* sont des données portant sur votre instance que vous pouvez utiliser pour configurer ou gérer l'instance en cours d'exécution. Vous pouvez créer des AMI génériques et utiliser des données utilisateur (*user-data*) pour modifier les fichiers de configuration fournis au moment du lancement.

- Les métadonnées d'instance sont des données relatives à votre instance que vous pouvez utiliser pour configurer ou gérer l'instance en cours.
- Ce mécanisme est unique en ce sens qu'il permet d'obtenir les propriétés AWS de l'instance depuis le système d'exploitation sans faire un appel à l'API AWS.
- Un appel HTTP à `http://169.254.169.254/latest/meta-data/` renvoie le nœud supérieur de l'arbre de métadonnées des instances.

Les métadonnées d'instance comprennent une grande variété d'attributs, notamment :

- Les groupes de sécurité associés
- L'identification de l'instance
- Le type d'instance
- L'AMI utilisé pour lancer l'instance
- Voir la documentation dans les ressources

Bien que les métadonnées d'instance et les données utilisateur ne soient accessibles qu'au sein de l'instance elle-même, elles ne sont pas protégées par des méthodes d'authentification ou de chiffrement. Toute personne ayant un accès direct à l'instance, et potentiellement tout logiciel s'exécutant sur l'instance, peut afficher ses métadonnées. Vous ne devez donc pas stocker de données sensibles, telles que des mots de passe ou des clés de chiffrement à longue durée, ou des données utilisateur.

Elastic Load Balancing

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

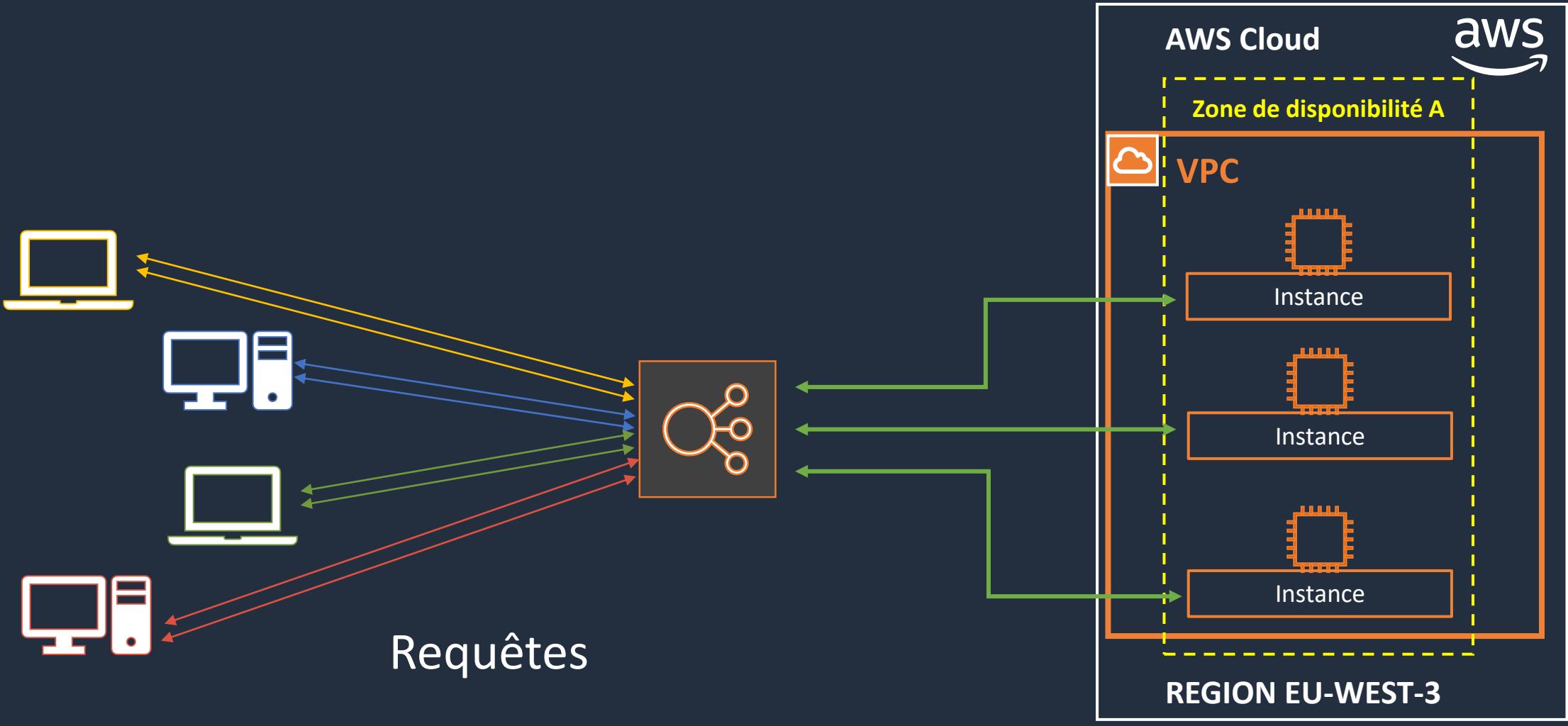
Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>



ELB : Elastic Load Balancing





Elastic Load Balancing

ALB

Équilibreur de charge d'application



ALB : Niveau 7 du model OSI

Supporte le routage « intelligent »

NLB

Équilibreur de charge réseau



NLB : Niveau 4 du model OSI

« ultra performant, faibles latences »

CLB

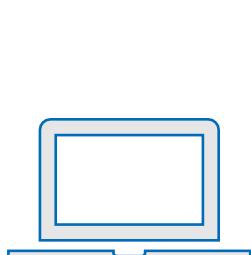
Équilibreur de charge classique

GÉNÉRATION PRÉCÉDENTE
pour HTTP, HTTPS et TCP

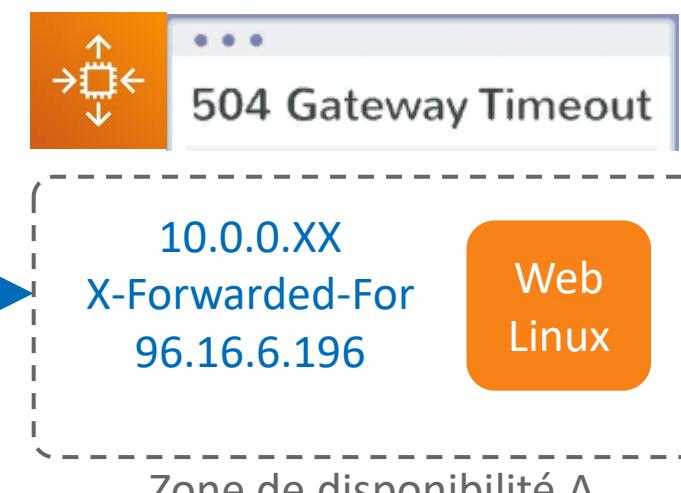
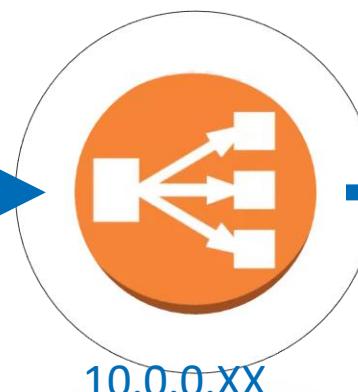
Niveau 7 et 4 (ou 4 forcé)

Supporte X-Forwarded-for (XFF)

Sticky session (activé ou désactivé)



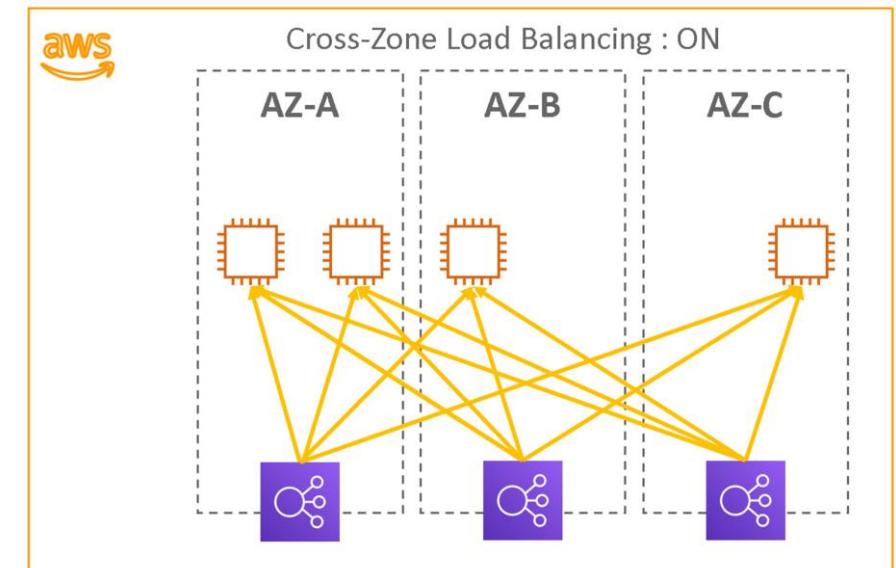
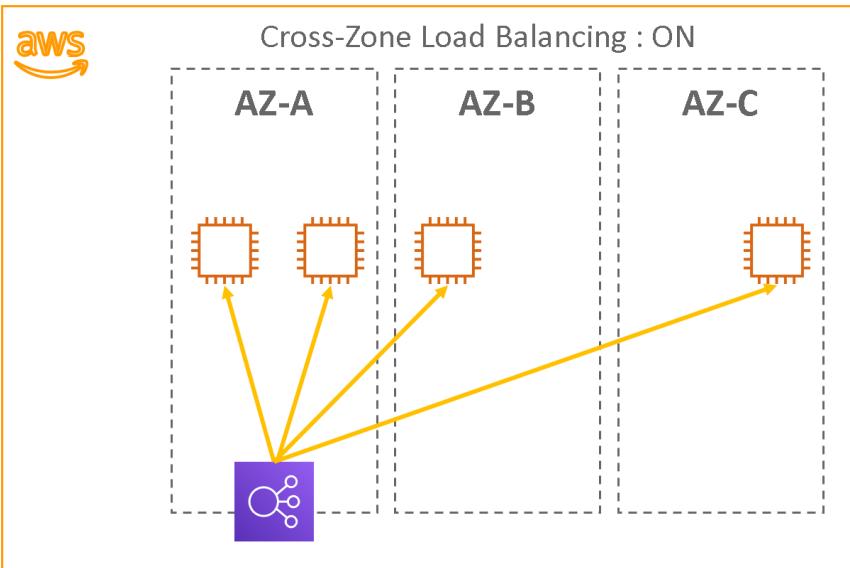
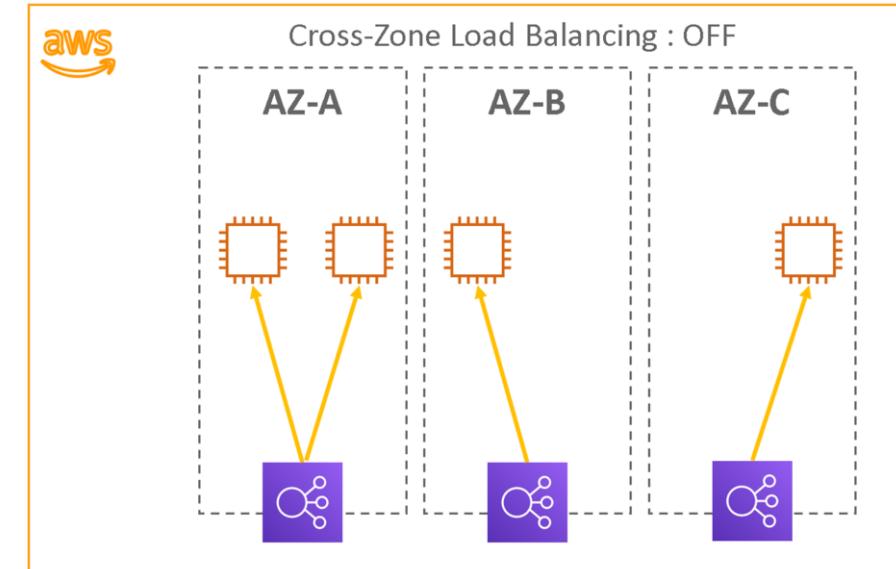
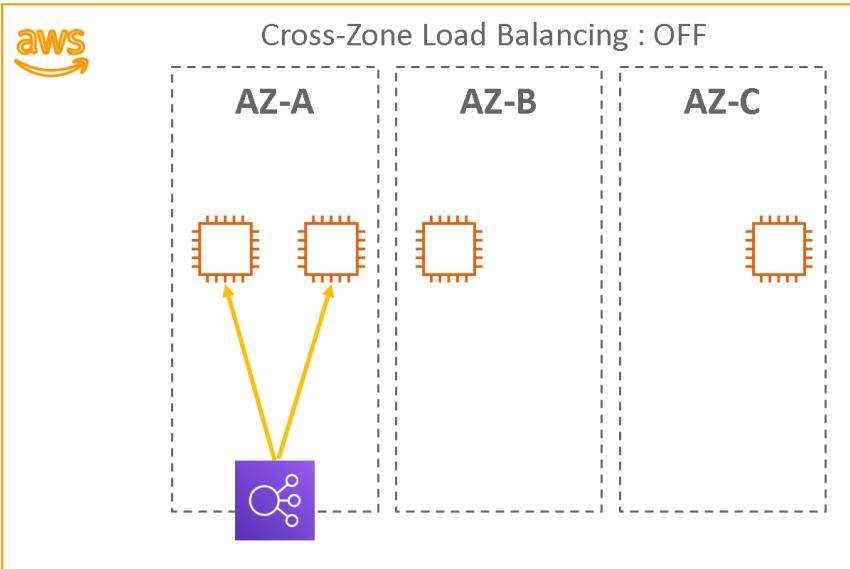
96.16.6.196



Zone de disponibilité A

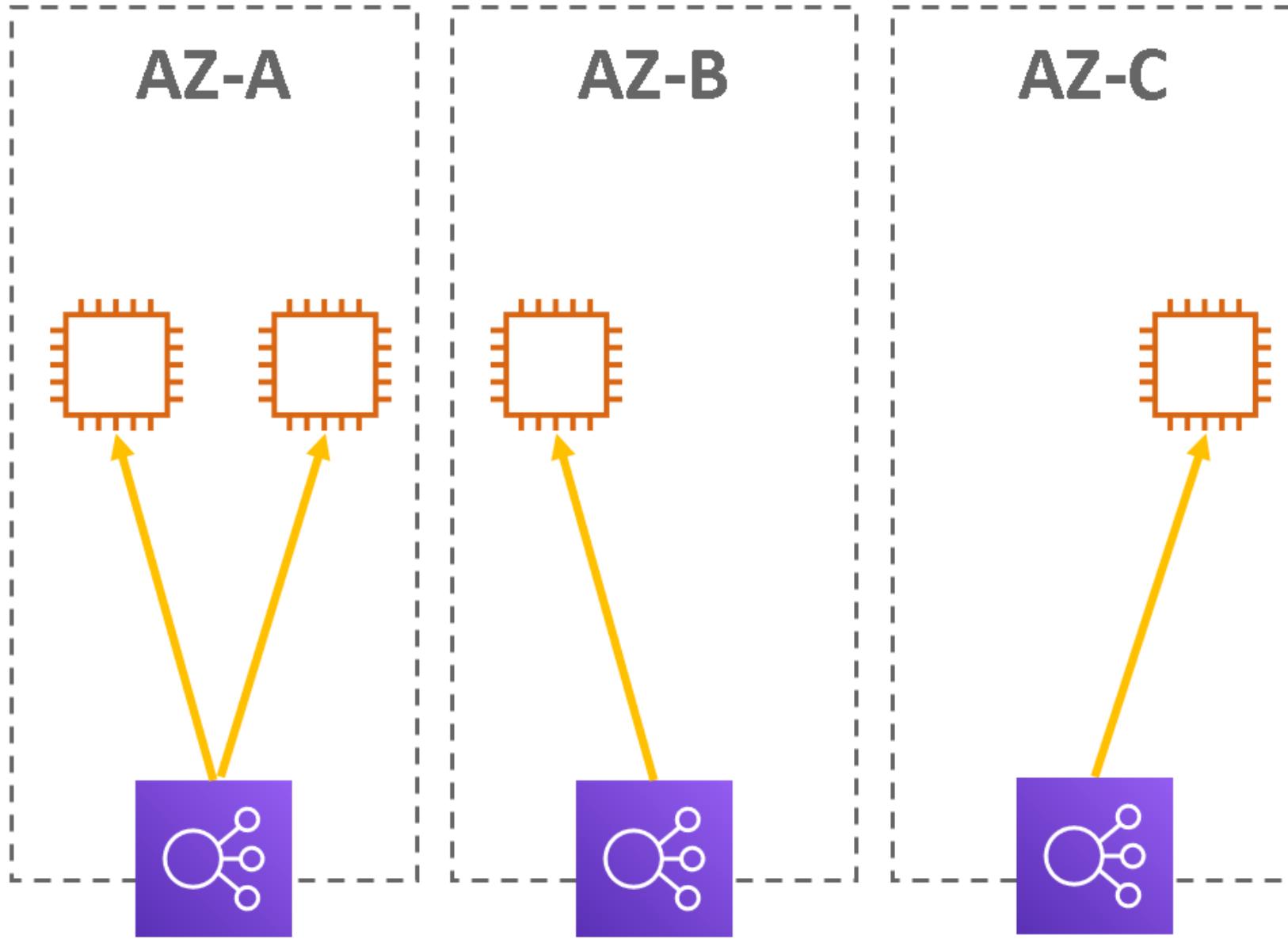


CROSS ZONE Load Balancing

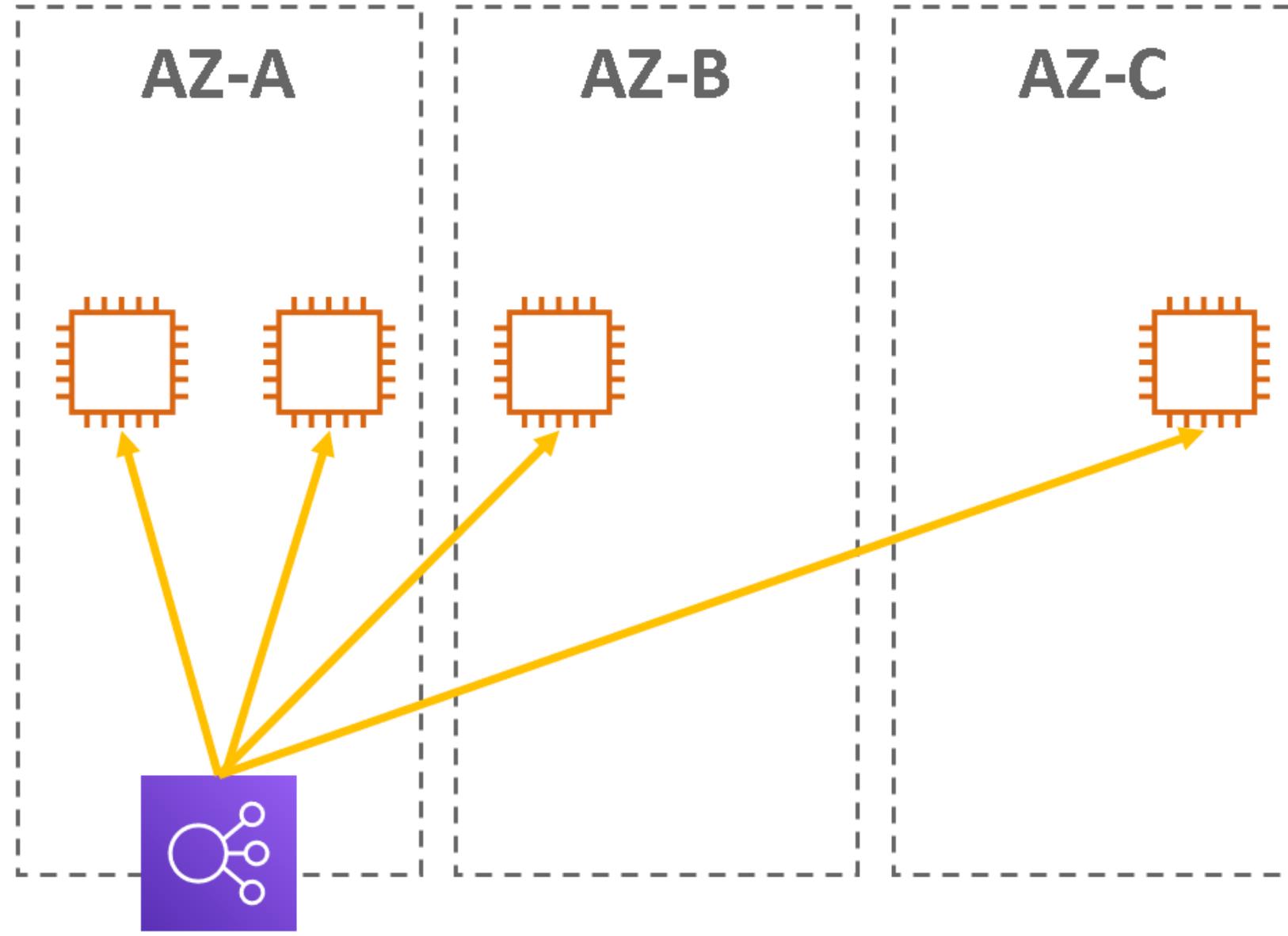




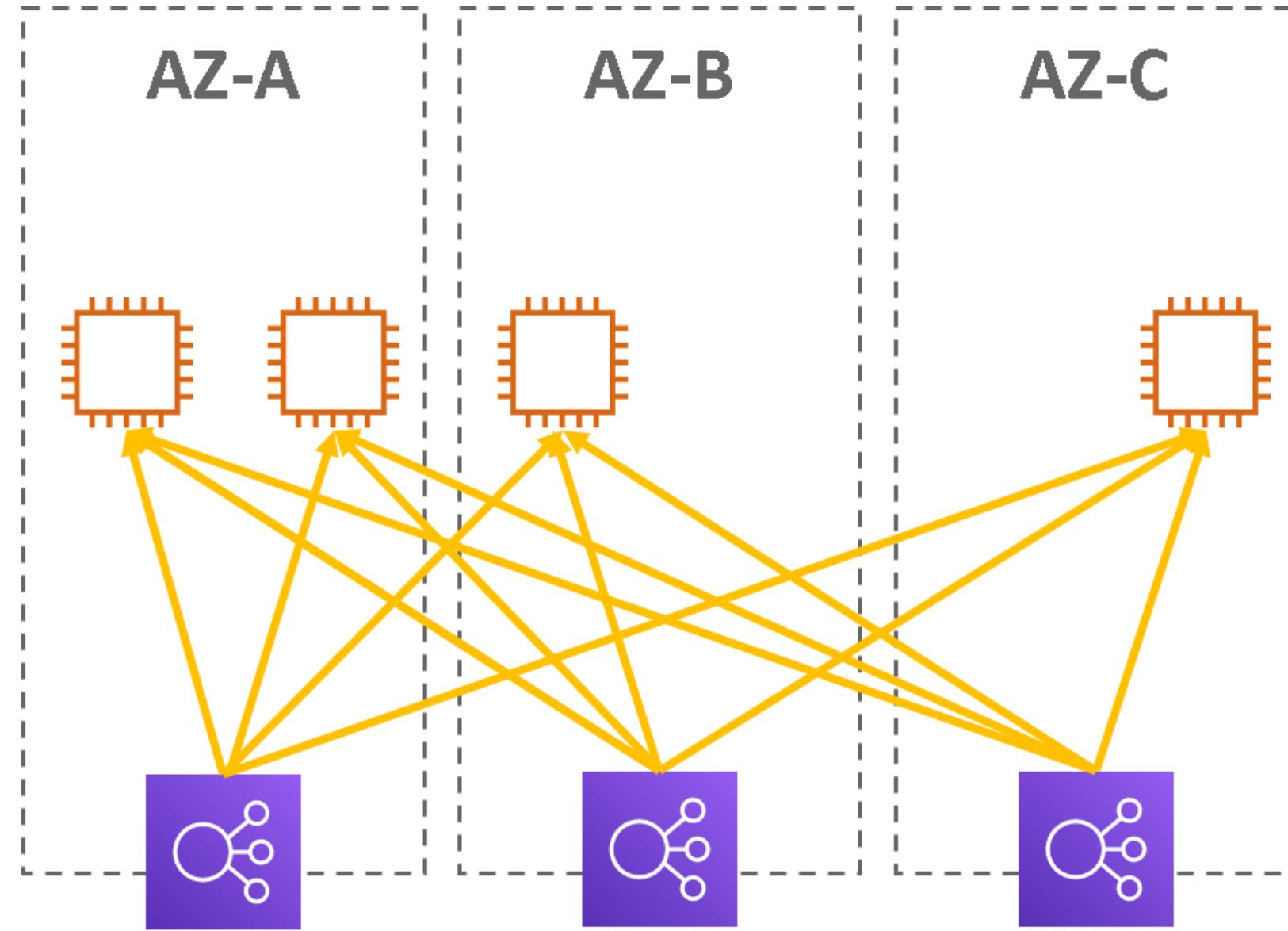
Cross-Zone Load Balancing : OFF



Cross-Zone Load Balancing : ON

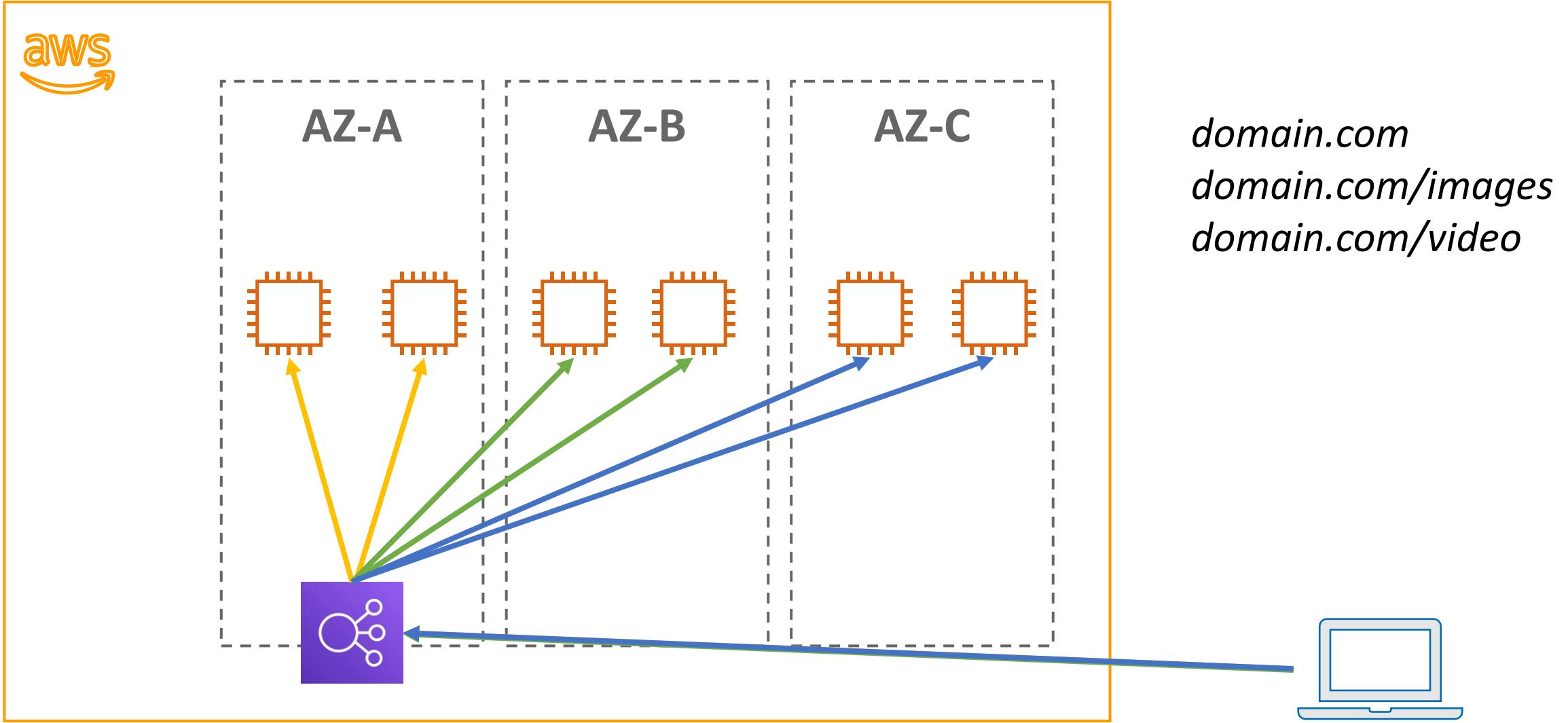


Cross-Zone Load Balancing : ON

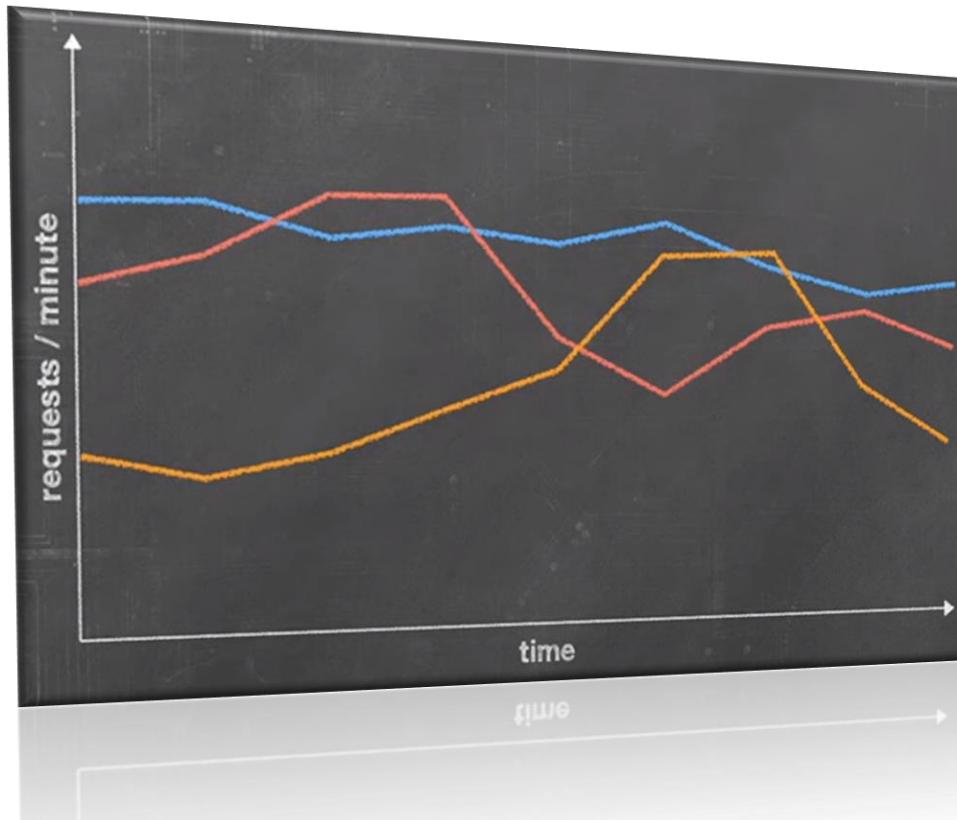




Path patterns Load Balancing

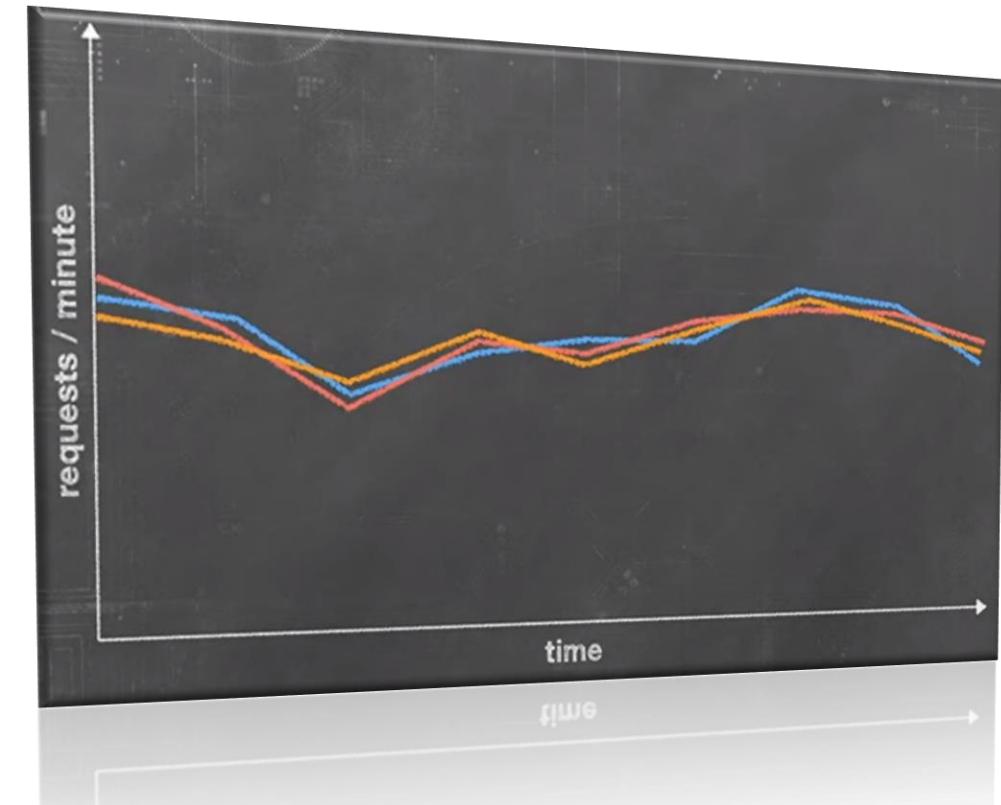


Cross-Zone Load Balancing : OFF



AZ-A
AZ-B
AZ-C

Cross-Zone Load Balancing : ON





Elastic Load Balancing (health check)

- Votre Equilibreur de charge classique envoie périodiquement des demandes à ses cibles enregistrées pour tester leur état. Ces tests sont appelés *vérifications de l'état*. L'état des instances qui sont saines au moment de la vérification de l'état est **InService**. L'état des instances qui sont défectueuses au moment de la vérification de l'état est **OutOfService**. L'équilibreur de charge effectue des vérifications de l'état sur toutes les instances enregistrées, que l'instance soit saine ou non.
- L'équilibreur de charge n'achemine les demandes que vers les instances **saines**. Lorsque l'équilibreur de charge détermine qu'une instance est défectueuse, il arrête d'acheminer les demandes vers celle-ci. L'équilibreur de charge recommence à acheminer les demandes vers l'instance lorsque cette dernière a été restaurée à un état sain.
- L'équilibreur de charge vérifie l'état de santé des instances enregistrées à l'aide de la configuration de vérification de l'état par défaut fournie par Elastic Load Balancing ou d'une vérification de l'état que vous configurez.
- Si vous avez associé votre groupe Auto Scaling à un Equilibreur de charge classique, vous pouvez utiliser la vérification de l'état de l'équilibreur de charge pour déterminer l'état de santé des instances de votre groupe Auto Scaling. Par défaut, un groupe Auto Scaling détermine périodiquement l'état de santé de chaque instance.
- **Consultez les ressources et liens de cette session**

Amazon EC2 Auto Scaling

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

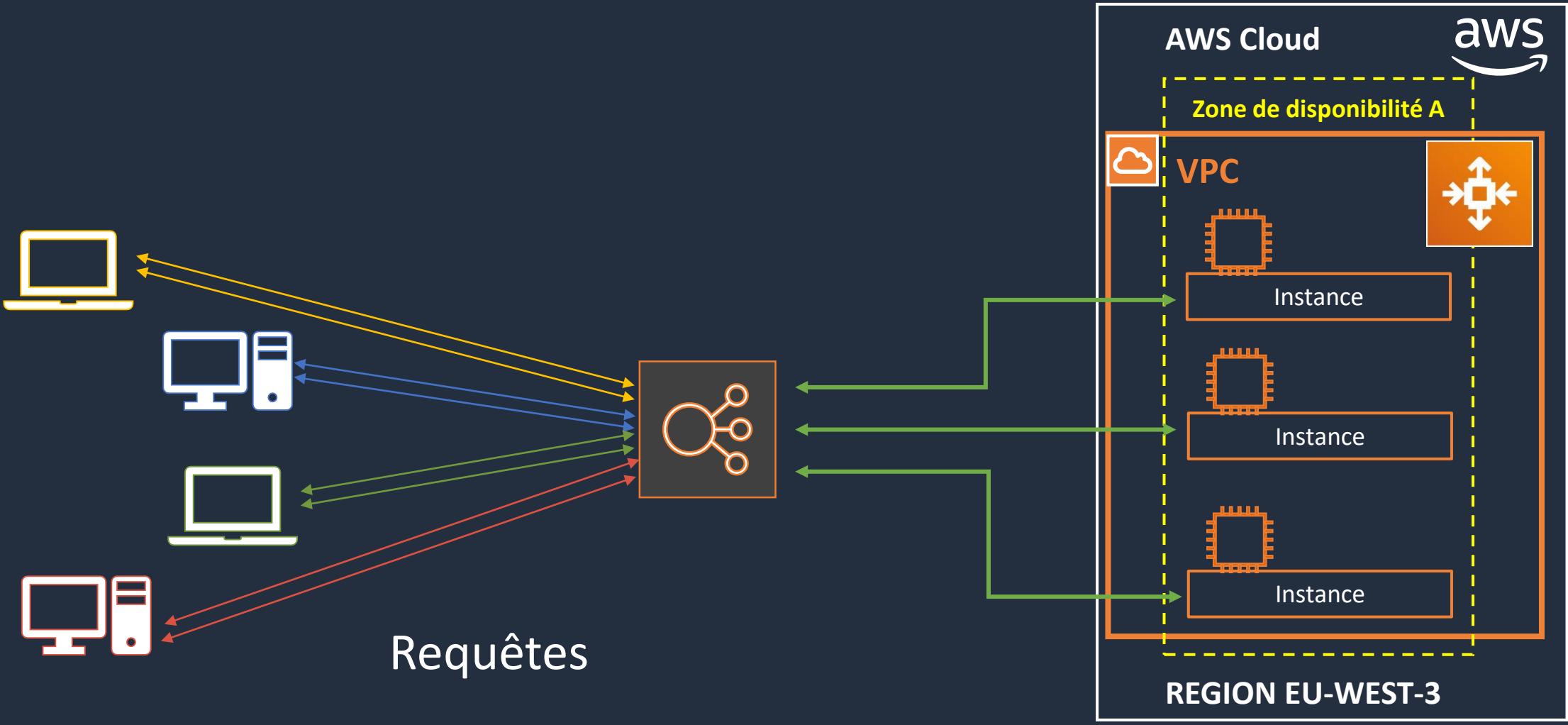
Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>



Auto Scaling : Mise à l'échelle





Auto Scaling (scale out Scale in)

Tolérance aux pannes

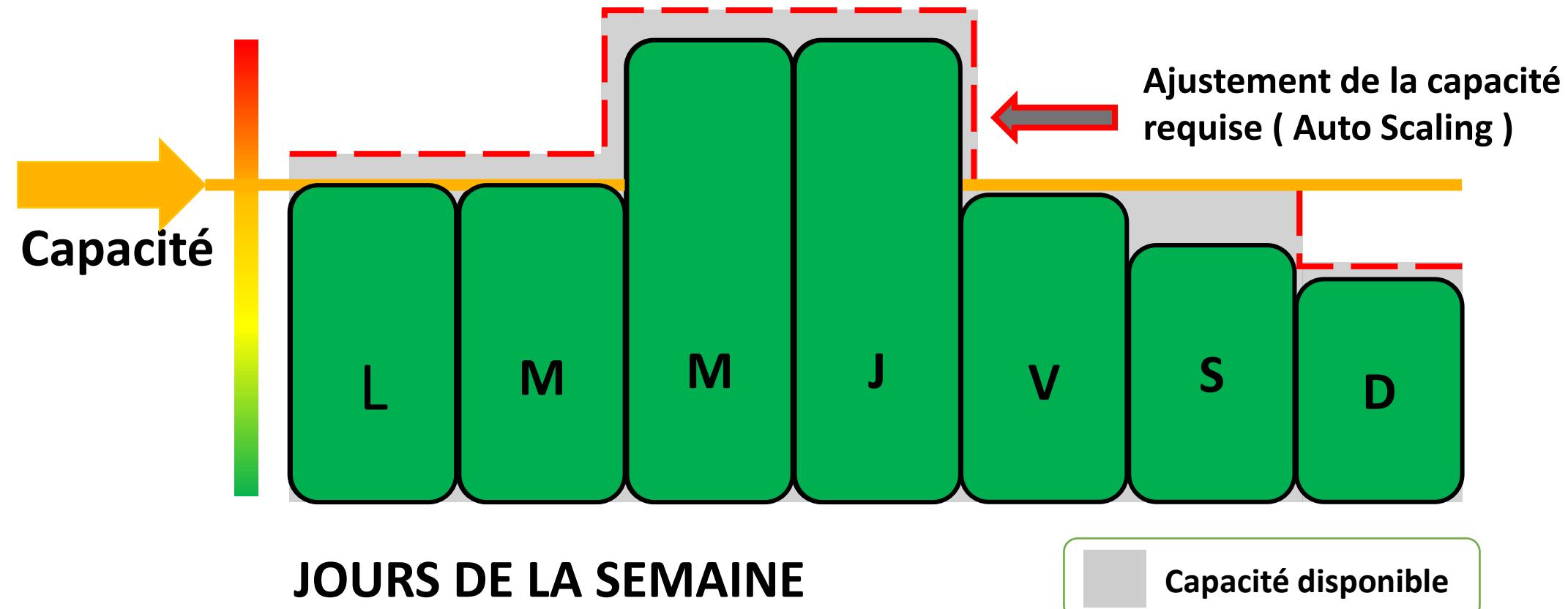
Déetecter les défaillances d'une instance, de la résilier et de lancer une instance afin de la remplacer.

Gestion des coûts

Économiser de l'argent en lançant dynamiquement des instances lorsqu'elles sont nécessaires et en les résiliant lorsqu'elles ne le sont plus.

Disponibilité

Assurez-vous que votre application dispose toujours de la bonne quantité de capacité afin de gérer la demande de trafic en temps réel.





Pré requis et configuration Auto Scaling

- ▼ Auto Scaling
 - Configurations de lancement
 - Groupes Auto Scaling

Configuration de lancement (Launch configuration)

- AMI Linux-Win
- Type d'instance (compute, storage, network)
- User Data / Rôle IAM
- Groupes de sécurité + Clé d'accès
- ELB Source
- Réseau

GRATUIT

Groupe d'auto scaling (AS Group)

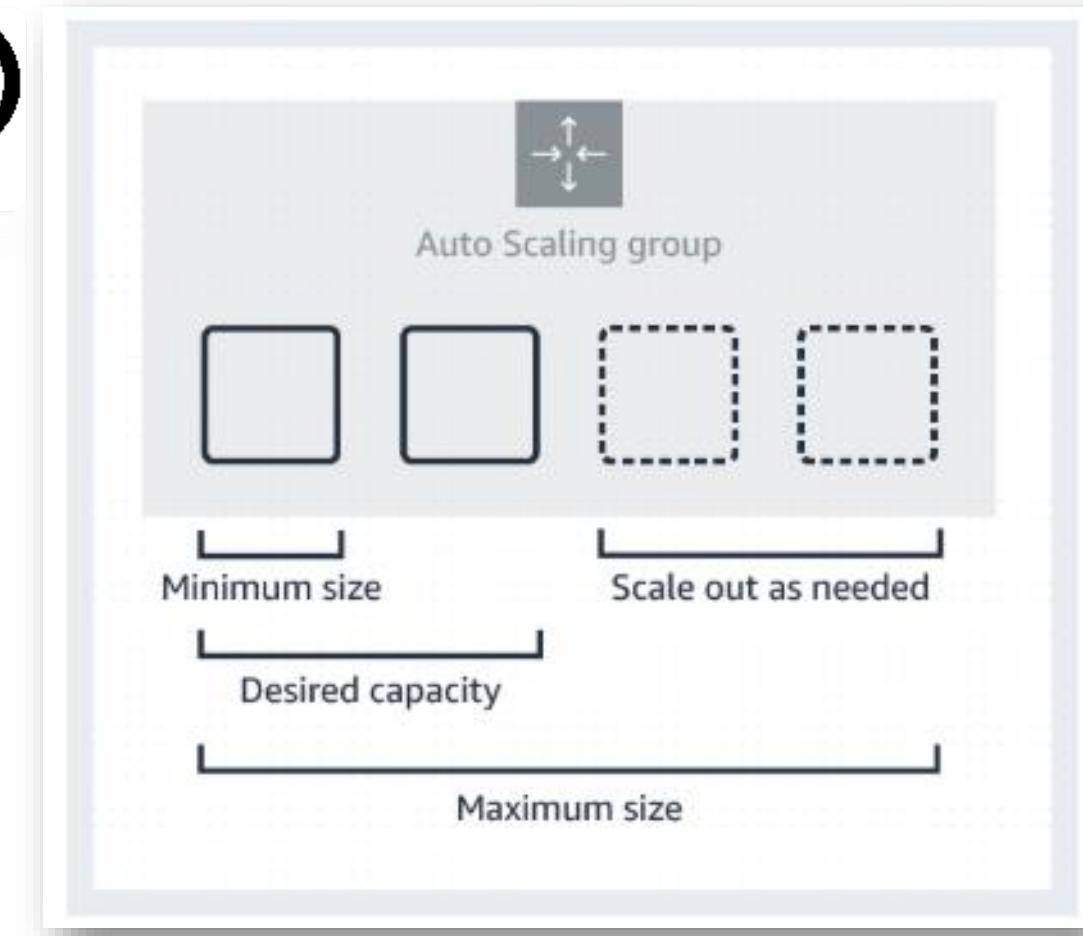
- Contient un ensemble d'instances Amazon EC2 qui sont traitées comme un regroupement logique à des fins de dimensionnement automatique et de gestion.

Options de dimensionnement (Scaling options)

- Maintenir les niveaux d'instance actuels à tout moment
- Mise à l'échelle manuelle
- Dimensionnement selon un calendrier
- Dimensionnement en fonction de la demande
- Utiliser le dimensionnement prédictif (*ec2 Auto Scaling + AWS Auto Scaling (new)*)

Services connexes

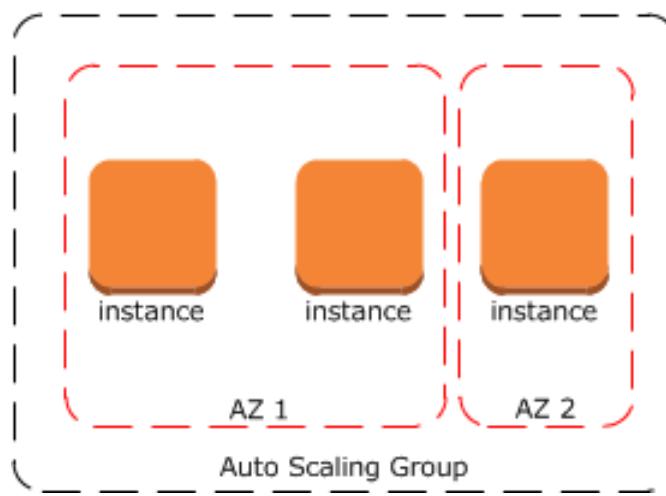
- Amazon EC2
- Elastic Load Balancing
- Amazon CloudWatch





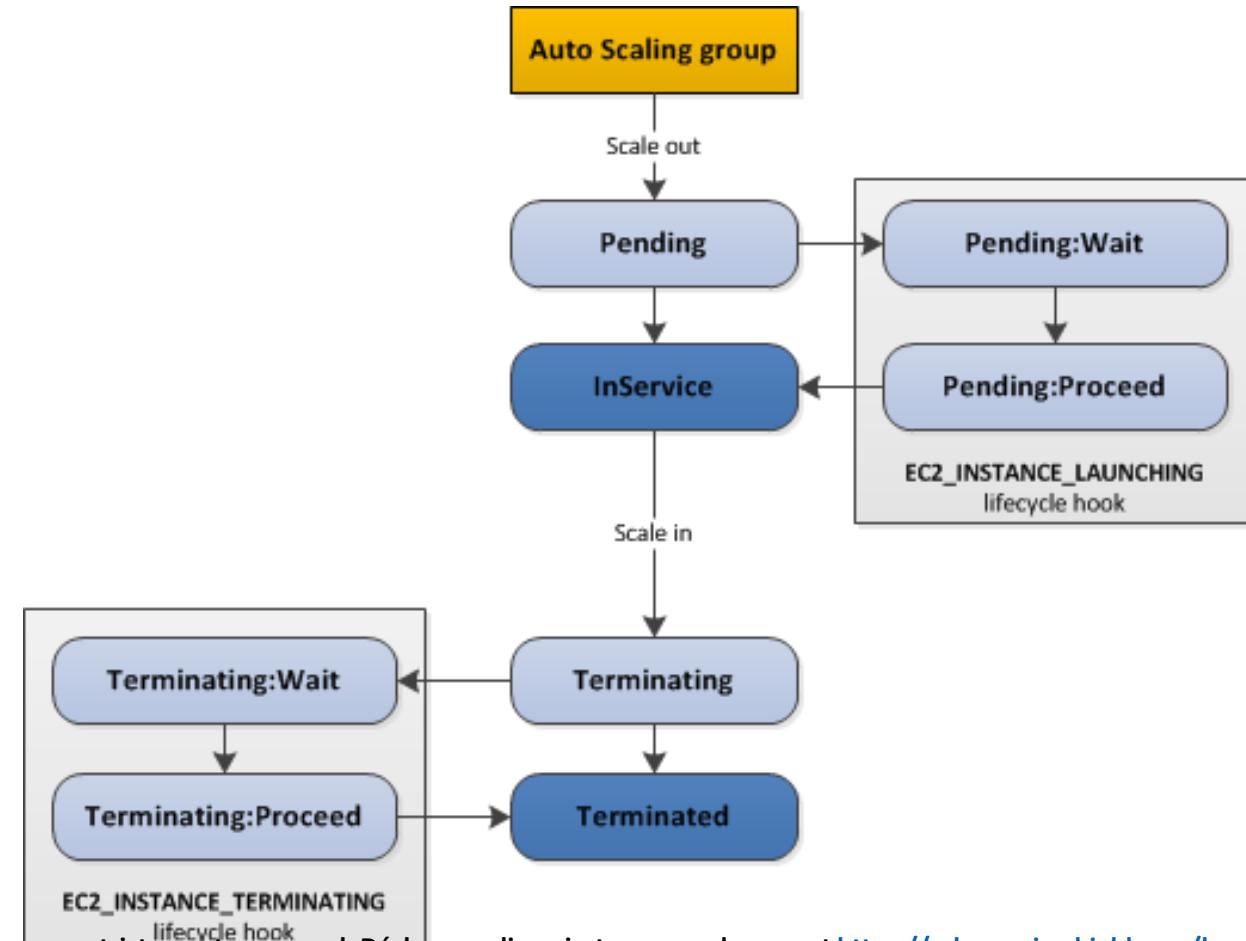
Stratégies de résiliation & LifeCycle Hooks

Si vous n'avez pas attribué de stratégie de mise hors service spécifique au groupe, il utilisera la stratégie de mise hors service par défaut.



Il sélectionne la zone de disponibilité avec deux instances, puis met fin à l'instance lancée depuis la plus ancienne configuration de lancement. Si les instances ont été lancées depuis la même configuration de lancement, Amazon EC2 Auto Scaling sélectionne l'instance la plus proche de la prochaine heure de facturation et y met fin.

Les Hooks de cycle de vie vous permettent de réaliser des actions personnalisées en *suspendant* des instances à mesure qu'un groupe Auto Scaling lance ou résilie ces instances.

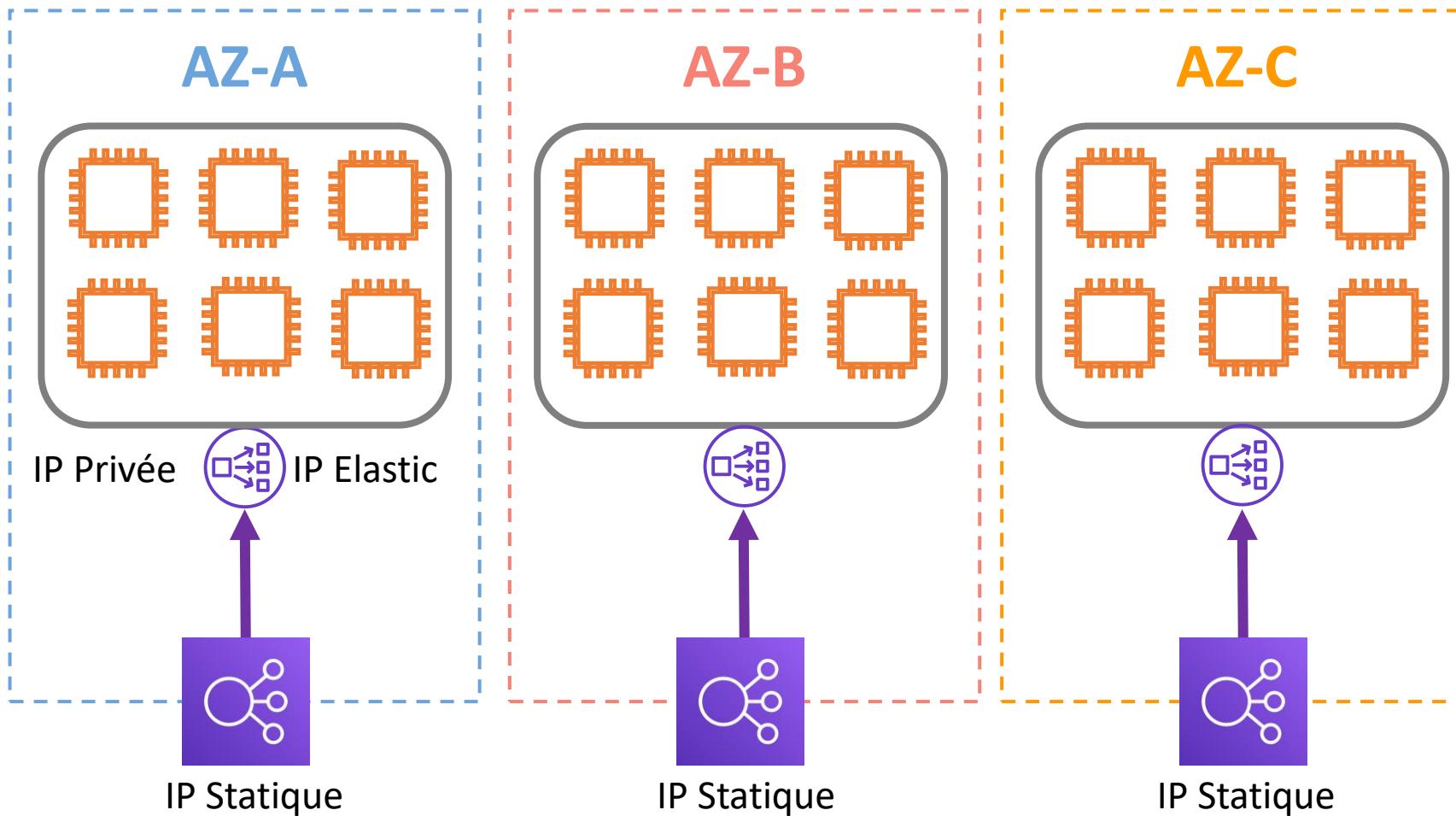




Équilibreurs de charge réseau

Network Load Balancer (NLB)

- Un équilibrage de charge TCP et UDP
- OSI (couche 4)
- Hautes performances (par millions)
- Latences ultra faibles < 100ms
- Préserve l'adresse IP source du client
- NLB par région : 50
- Groupes cible par région : 3000 *
- Écouteurs par NLB : 50
- Sous-réseaux par AZ et par NLB : 1
- Équilibreurs de charge par groupe cible : 1
- Certificats par NLB : 25



Lorsque vous activez une zone de disponibilité, vous spécifiez un sous-réseau depuis cette zone :

- Elastic Load Balancing crée un nœud d'équilibreur de charge dans la zone de disponibilité et une interface réseau pour le sous-réseau
- Chaque nœud d'équilibreur de charge de la zone de disponibilité utilise cette interface réseau pour obtenir une adresse IPv4.
- Si accessible depuis internet, vous pouvez associer une adresse IP Elastic à chaque sous-réseau.
- Si ELB interne, vous pouvez spécifier une adresse IP privée pour chaque sous-réseau.



Tarification Elastic Load Balancing

[Announcing Network Load Balancer for Elastic Load Balancing](#)

<https://aws.amazon.com/about-aws/whats-new/2017/09/announcing-network-load-balancer-for-elastic-load-balancing/>

Posted On: Sep 7, 2017

[Announcing Application Load Balancer for Elastic Load Balancing](#)

<https://aws.amazon.com/about-aws/whats-new/2016/08/announcing-application-load-balancer-for-elastic-load-balancing/>

Posted On: Aug 11, 2016

- **ÉquilibrEUR de charge d'application :** Vous êtes facturé pour chaque heure ou heure partielle pendant laquelle un équilibrEUR de charge d'application fonctionne et selon le nombre d'unités de capacité d'équilibrage de charge (LCU) utilisées par heure.
- **ÉquilibrEUR de charge du réseau :** Vous êtes facturé pour chaque heure ou heure partielle pendant laquelle un Network Load Balancer fonctionne et selon le nombre d'unités de capacité d'équilibrage de charge (LCU) utilisées par heure par celui-ci.
- **ÉquilibrEUR de charge classique :** Vous êtes facturé pour chaque heure ou heure partielle pendant laquelle un Classic Load Balancer fonctionne et pour chaque Go de données transférÉ par votre équilibrEUR de charge.

AWS Elastic Beanstalk

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>



AWS Elastic Beanstalk

AWS Elastic Beanstalk est un service qui vous aide à déployer vos applications web dans le cloud



Service géré
par AWS



Déployer des
applications et services web
à l'échelle



Déployer n'importe où
(Région)



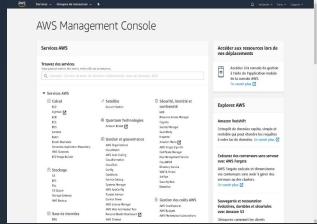
(PAAS)



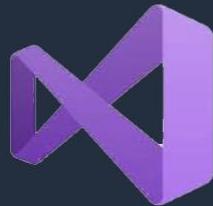


AWS Elastic Beanstalk

Fonctionnement



```
(work) 15:31:21 user:~/Desktop/work $ aws-shell
AWS> configure
AWS Access Key ID [None]: Your AWS Access Key ID
AWS Secret Access Key [None]: Your AWS Secret Access Key
Default region name [us-east-1]:
Default output format [None]:
AWS>
```



Téléchargez votre code

.NET

Docker

GlassFish

Go

Java

Node.js

PHP

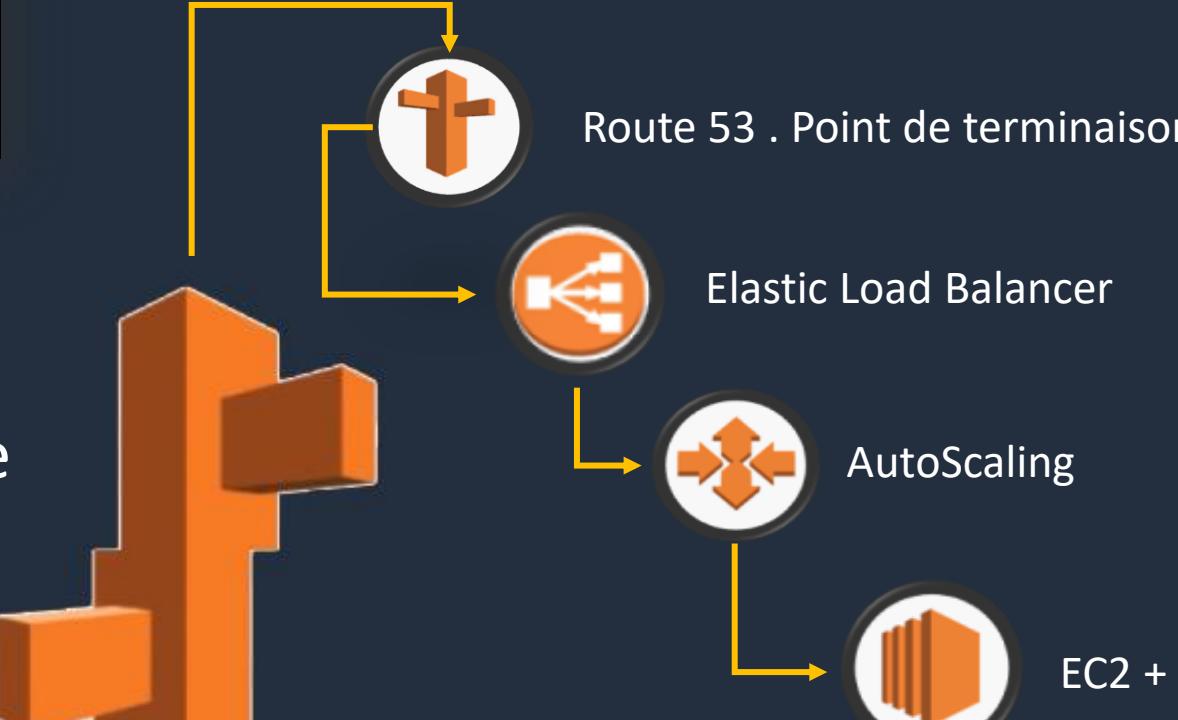
Python

Ruby

Tomcat



Configuration



Route 53 . Point de terminaison

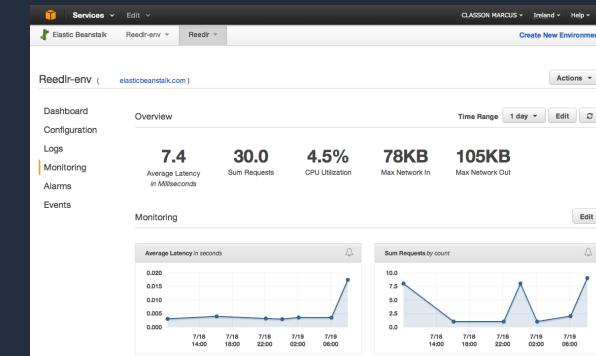
Elastic Load Balancer

AutoScaling

EC2 + Security Groups



CloudWatch / X-RAY



AWS Lambda

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>



Lambda

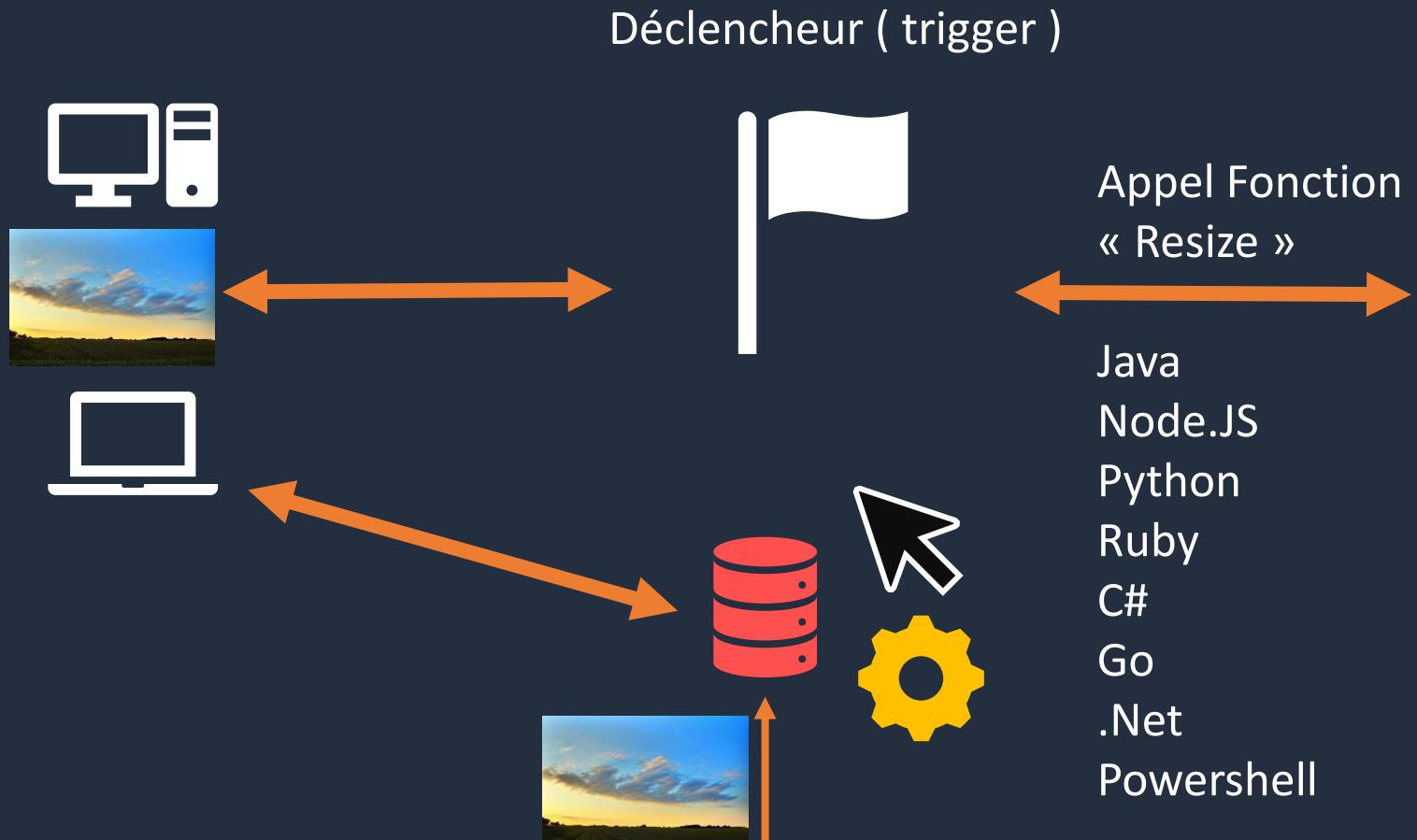
AWS Lambda *ServerLess

permet d'exécuter du code
sans vous soucier des
serveurs.



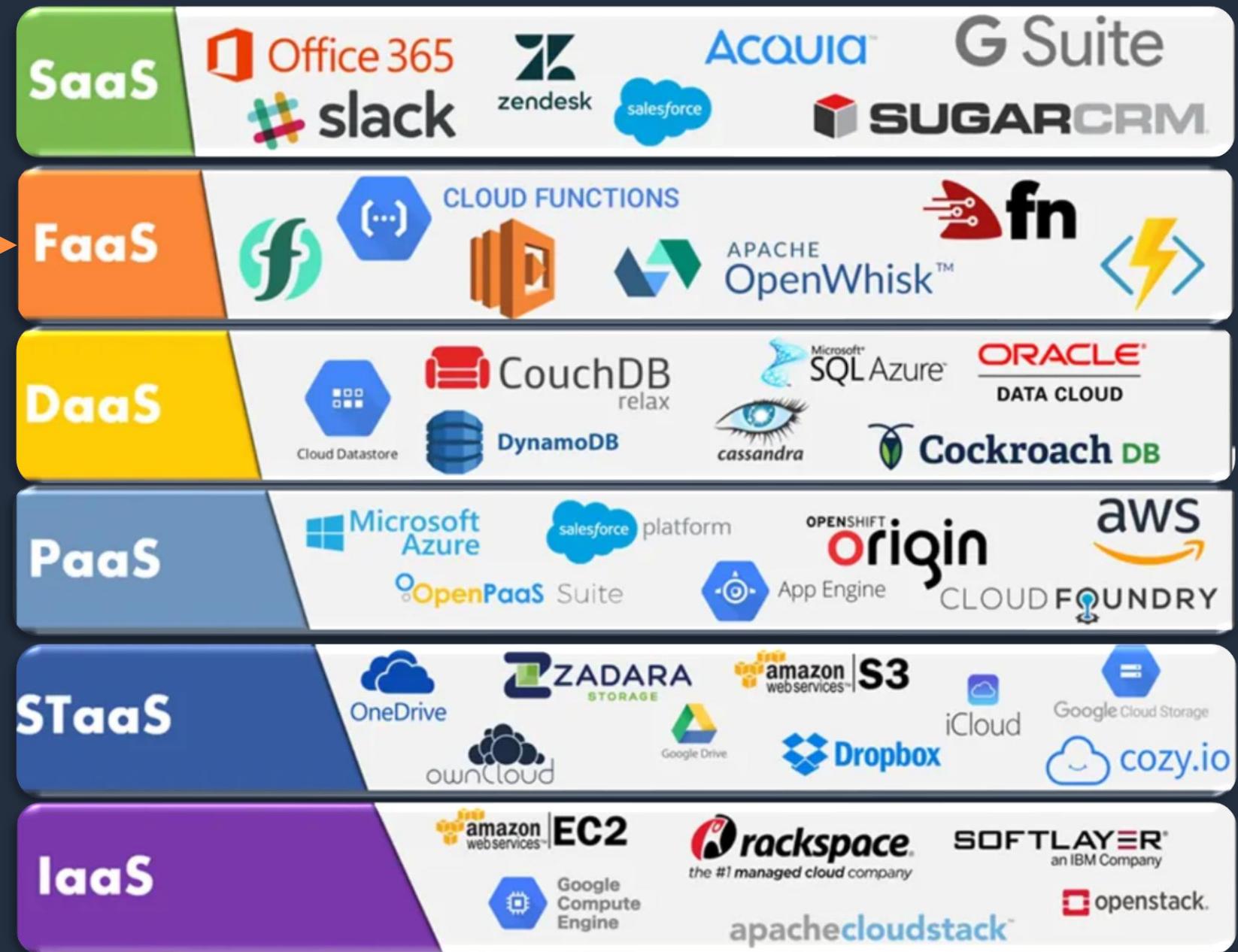


Lambda vs Beanstalk vs EC2





Lambda





AWS Lambda

Plateforme de calcul sans administration (serverless *) pour les développeurs web back-end, ce service exécute votre code rapidement dans le cloud AWS et vous fournit une tarification réduite.

- Offre gratuite Lambda comprend 1 million de requêtes offertes, ainsi que 400 000 Go-secondes de temps de calcul / mois
- Lambda se met à l'échelle automatiquement
- Chaque fonction est indépendante et ne s'exécute pas sur le même matériel que les autres fonctions
- Une fonction peut appeler « N » fonction lambda
- Connaitre les services en capacité d'interagir avec Lambda

AWS Lambda limite la quantité de ressources de calcul et de stockage que vous pouvez utiliser pour exécuter et stocker des fonctions. Les limites suivantes s'appliquent par région et peuvent être augmentées **

- Exécutions simultanées 1,000 **
- Stockage de couche et fonction : 75 GB **
- Elastic network interfaces par VPC : 250 **
- Les fonctions AWS Lambda peuvent être configurées pour que chaque exécution dure jusqu'à 15 minutes. 10/10/18 (SAA-C02)
- Vous pouvez définir le délai de réponse sur une valeur comprise entre 1 seconde et 15 minutes.
- Allocation de mémoire des fonctions : De 128 Mo à 3,008 Mo, par incrément de 64 Mo
- Stockage dans le répertoire /tmp : 512 MB
- Variables d'environnement des fonctions : 4 KB
- Stratégie de fonction basée sur les ressources 20 KB
- Couches de fonctions : 5 couches
- La facturation d'AWS Lambda s'effectue en fonction de l'utilisation du service.

Amazon Elastic Container Service

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

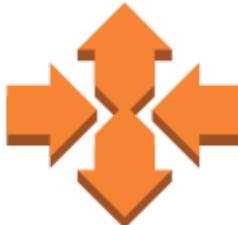


Elastic Container Service (ECS)



Amazon ECS

- Amazon ECS est un service d'orchestration de conteneurs hautement évolutif et performant qui prend en charge les conteneurs « Docker » et vous permet d'exécuter et de mettre à l'échelle facilement des applications conteneurisées sur AWS.
- Vous n'aurez plus besoin d'installer et d'exploiter votre propre logiciel d'orchestration de conteneurs, de gérer et de faire évoluer un groupe de machines virtuelles ou de programmer des conteneurs sur ces machines virtuelles.
- ECS est également profondément intégré dans le reste de l'écosystème AWS.



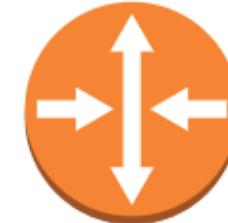
Autoscaling



Load balancing



IAM



Networking



Logging

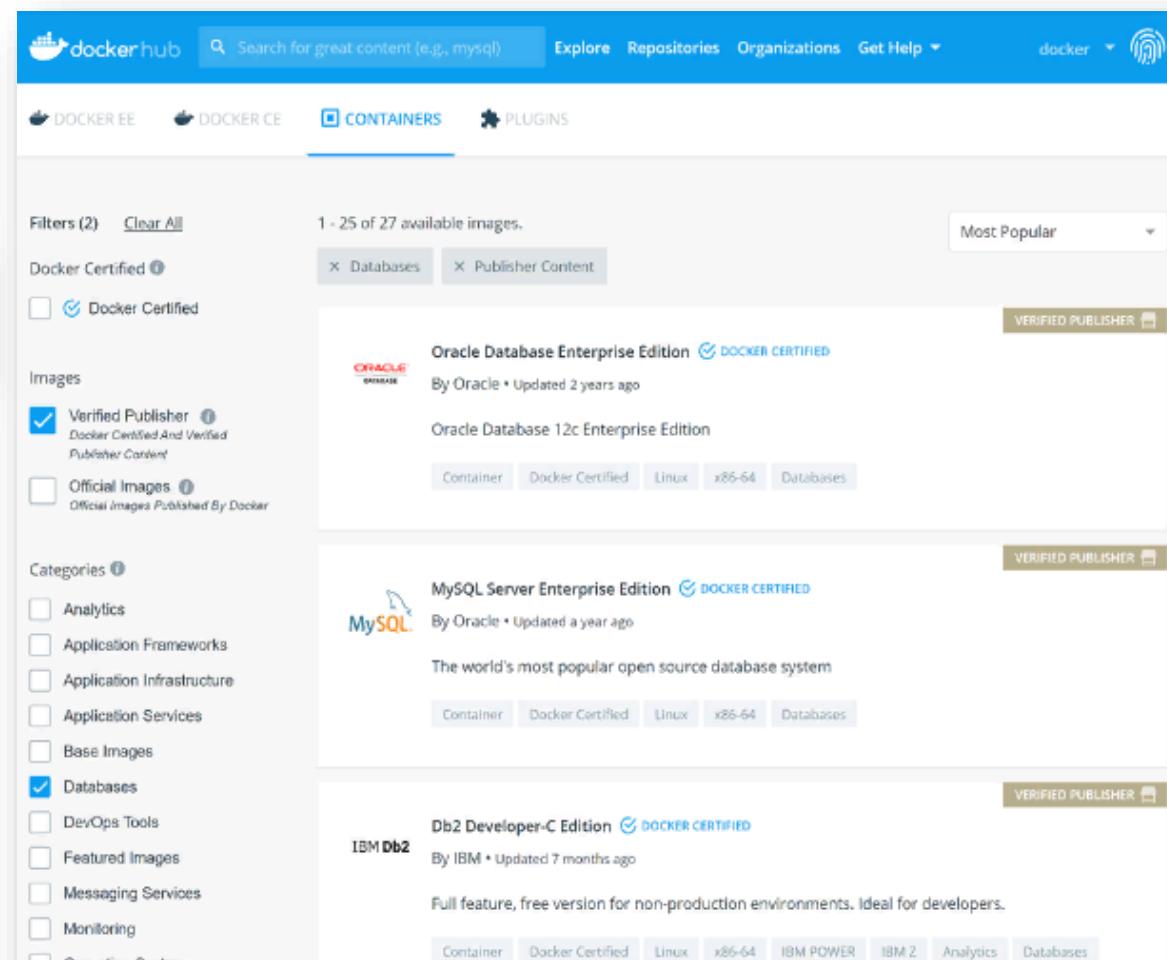


Monitoring

ECS & Docker – ECR & Docker Hub



Un conteneur est une unité standard de logiciel qui regroupe le code et toutes ses dépendances afin que l'application s'exécute rapidement et de manière fiable d'un environnement informatique à un autre. Une image de conteneur Docker est un ensemble de logiciels léger, autonome et exécutable qui comprend tout ce qui est nécessaire pour faire fonctionner une application : code, temps d'exécution, outils système, bibliothèques système et paramètres.

The screenshot shows the Docker Hub interface with the following details:

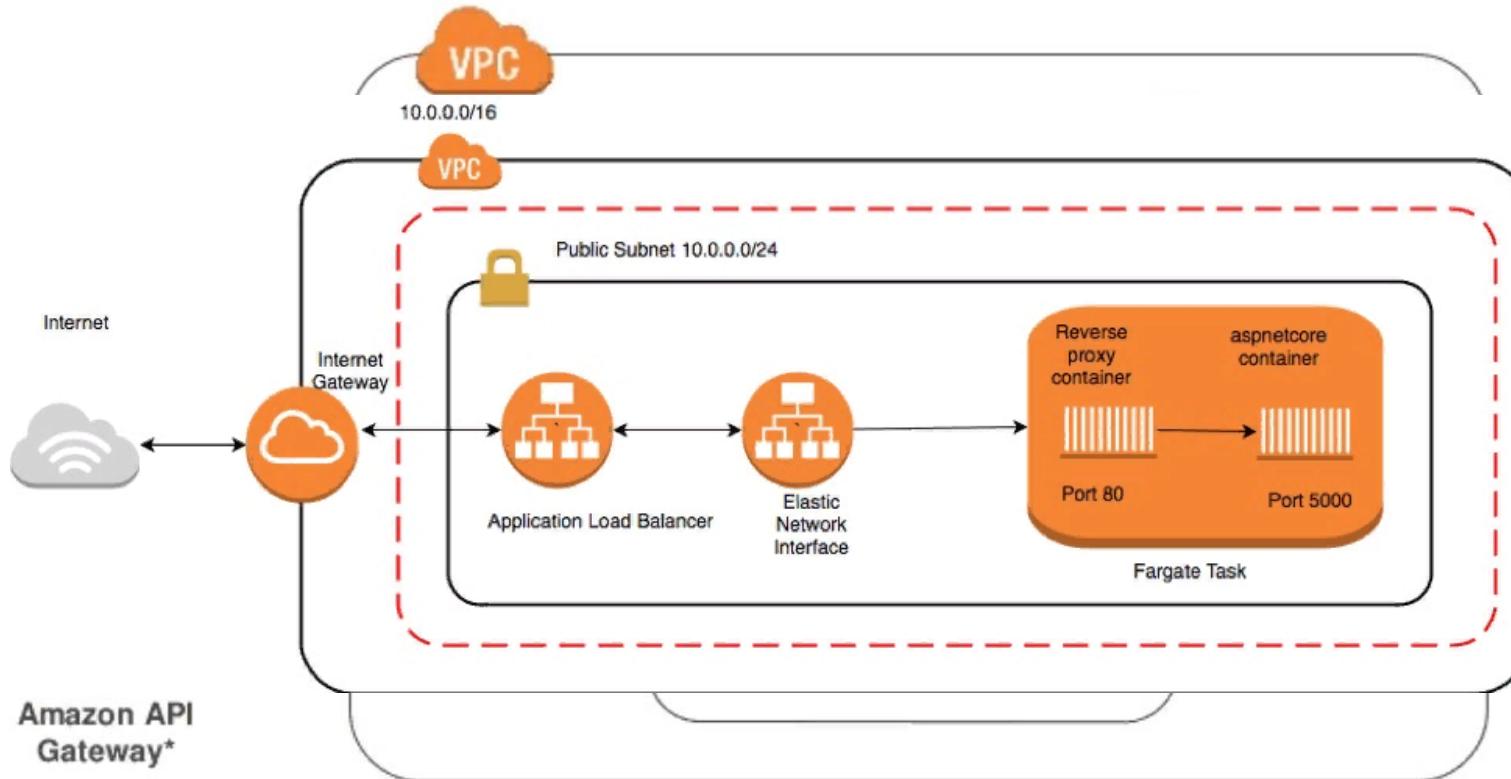
- Header:** dockerhub, Search for great content (e.g., mysql), Explore, Repositories, Organizations, Get Help, docker, Fingerprint.
- Navigation:** DOCKER EE, DOCKER CE, CONTAINERS (selected), PLUGINS.
- Filters:** Filters (2) Clear All, Docker Certified (unchecked), Docker Certified (checked), Verified Publisher (checked), Official Images (unchecked).
- Results:** 1 - 25 of 27 available images.
 - Oracle Database Enterprise Edition:** By Oracle • Updated 2 years ago. Docker Certified. Categories: Container, Docker Certified, Linux, x86-64, Databases.
 - MySQL Server Enterprise Edition:** By Oracle • Updated a year ago. The world's most popular open source database system. Docker Certified. Categories: Container, Docker Certified, Linux, x86-64, Databases.
 - IBM Db2 Developer-C Edition:** By IBM • Updated 7 months ago. Full feature, free version for non-production environments. Ideal for developers. Docker Certified. Categories: Container, Docker Certified, Linux, x86-64, IBM POWER, IBM Z, Analytics, Databases.



Elastic Container Service (ECS)

Service de gestion de conteneurs hautement scalable et rapide, qui permet d'exécuter, d'arrêter et de gérer facilement des conteneurs Docker sur un **cluster**.

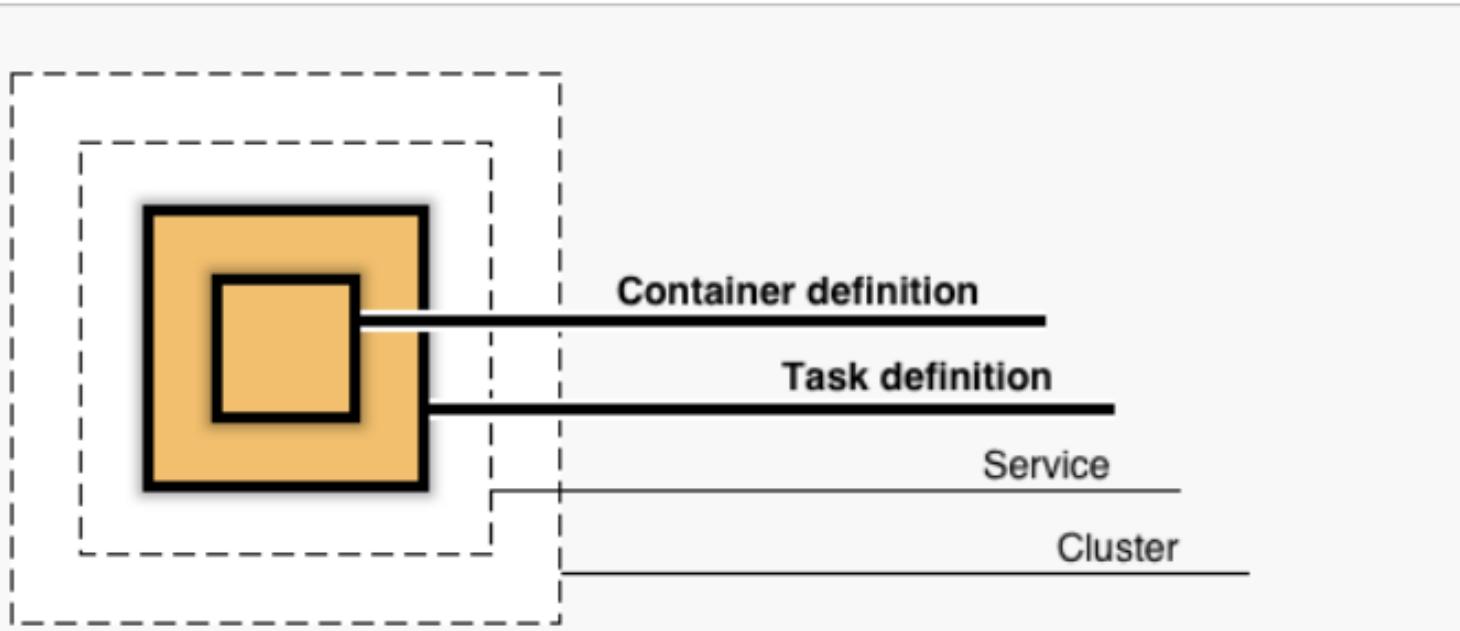
- Un **cluster** est une grappe de serveurs sur un réseau, appelé ferme ou grille de calcul
- Service d'orchestration de conteneurs entièrement géré
- Vous pouvez héberger votre cluster sur une infrastructure sans serveur gérée par Amazon ECS en lançant vos services ou les tâches via le type de lancement **Fargate**
- Vous pouvez héberger vos tâches sur un cluster d'instances Amazon Elastic Compute Cloud (**Amazon EC2**)
- Planifier la provision de conteneurs de manière optimale
- Dimensionner les ressources requises en terme processeur et mémoire
- Superviser l'activité et conditionner des actions
- Gérer les déploiements, les mises à jour, et les plan de retour en cas d'échec



GRATUIT



Diagramme d'objets ECS et de leurs relations



Amazon
Elastic Container Registry



Registry



docker



Image

WEB SERVERS

APP SERVERS

CACHES

QUEUES

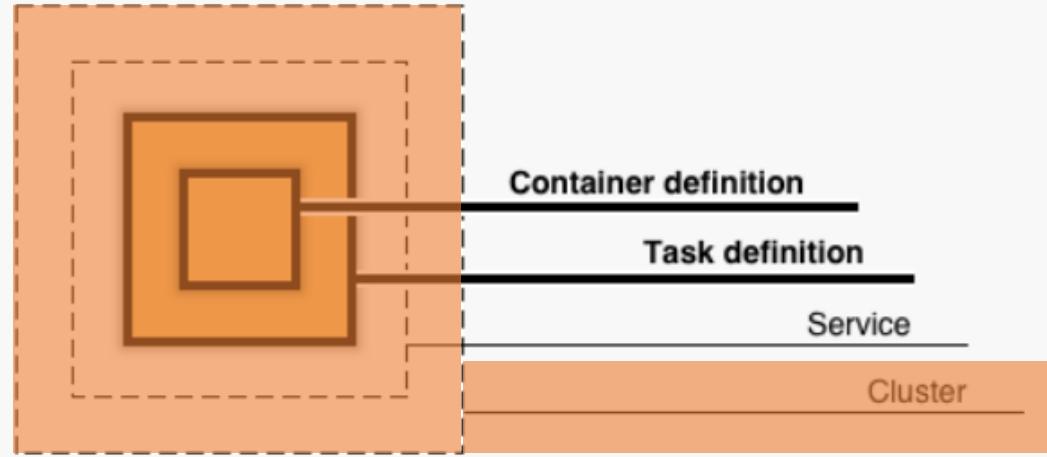
API BACKENDS

WORKERS

Un cluster Amazon ECS est un regroupement logique de tâches ou de services

- L'infrastructure sous-jacente peut être une combinaison des types de lancement Fargate et EC2
- Après la création d'un cluster on peut y ajouter des groupes logiques d'instances
- Les instances EC2 disposent d'une AMI avec docker et l'agent ECS
- Les instances rejoignent un cluster ECS grâce à l'agent ECS installé
- Les instances EC2 peuvent accueillir plusieurs tâches ou services

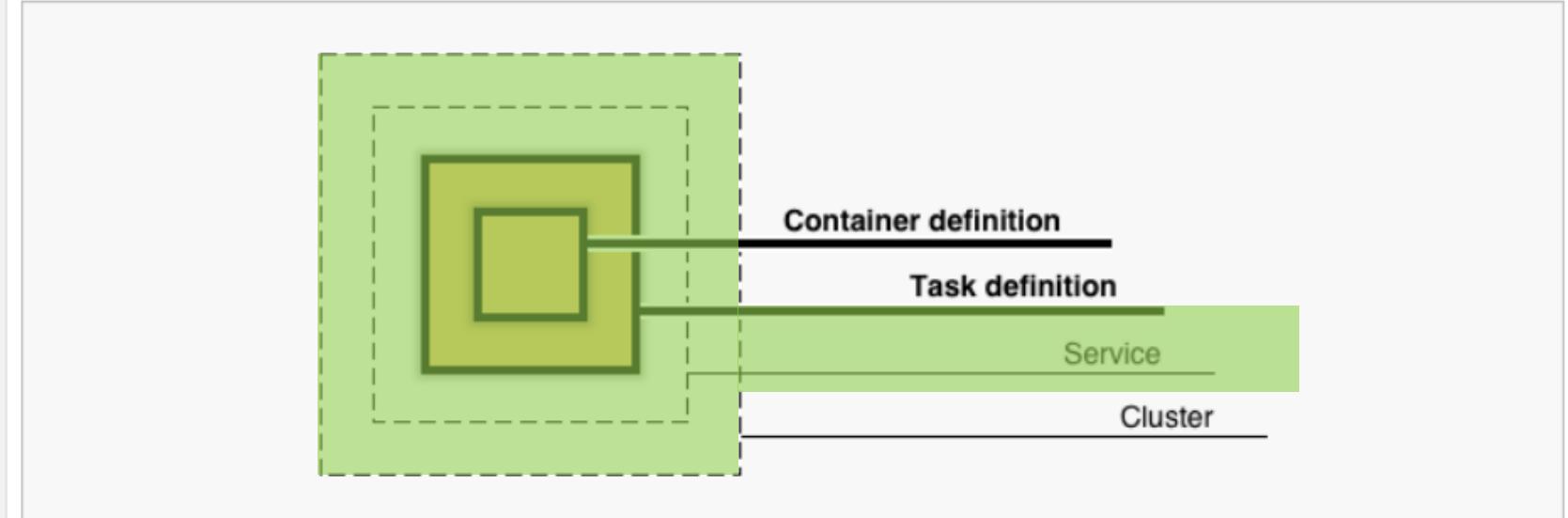
Diagramme d'objets ECS et de leurs relations



Un service Amazon ECS permet d'exécuter et de gérer simultanément, un nombre paramétré d'instances d'une définition de tâche, dans un cluster Amazon ECS.

- Permet aux définitions de tâches d'être mise à l'échelle par l'ajout de tâches et définir les valeurs min et max
- Si l'une de vos tâches échoue ou s'arrête, le planificateur de service ECS lance une autre instance
- Vous pouvez éventuellement faire fonctionner votre service derrière un équilibrEUR de charge. ALB/NLB/CLB

Diagramme d'objets ECS et de leurs relations

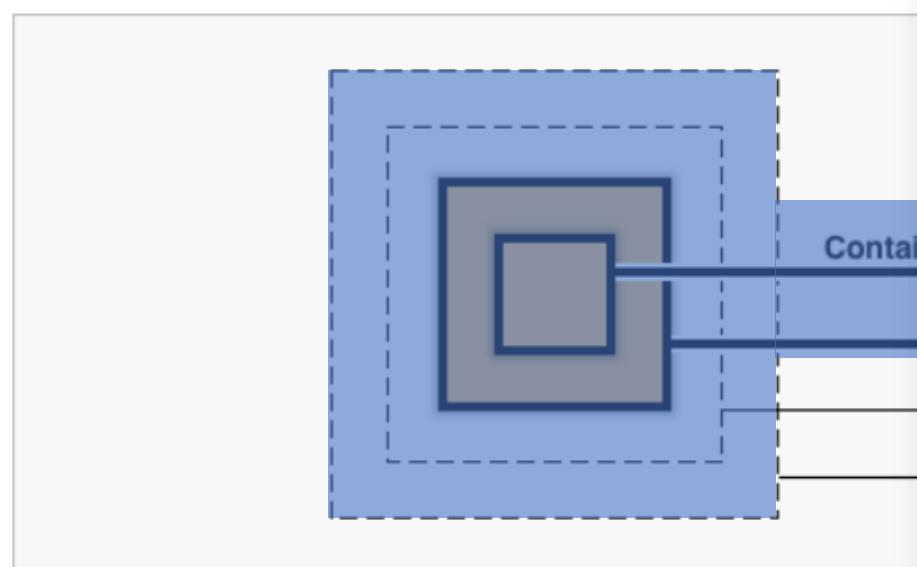


Une définition de tâche est requise pour exécuter des conteneurs Docker dans Amazon ECS

C'est un document JSON qui définitie les paramètres de lancement d'un conteneur Docker

- L'image Docker à utiliser avec chaque conteneur dans la tâche
- Les ressources d'UC et de mémoire à utiliser avec chaque conteneur au sein d'une tâche
- Le type de lancement à utiliser, qui détermine l'infrastructure sur laquelle vos tâches sont hébergées
- Le mode réseau Docker à utiliser pour les conteneurs dans votre tâche
- La configuration de journalisation à utiliser pour les tâches
- Si la tâche doit continuer à s'exécuter
- Les commandes que le conteneur doit exécuter
- Les volumes de données à utiliser avec les conteneurs
- Le rôle IAM que les tâches doivent utiliser

Diagramme d'objets ECS et de leurs relations



```
{  
  "family": "webserver",  
  "containerDefinitions": [  
    {  
      "name": "web",  
      "image": "nginx",  
      "memory": "100",  
      "cpu": "99"  
    },  
  ],  
  "requiresCompatibilities": [  
    "FARGATE"  
  ],  
  "networkMode": "aws_vpc",  
  "memory": "512",  
  "cpu": "256",  
}
```



Une tâche : est l'instanciation d'une définition de tâche au sein d'un cluster.

- Le cluster regroupe les ressources
- Le service exécute et maintient un nombre déterminé de tâches simultanément.
- **Le planificateur de tâches** est responsable du placement des tâches au sein de votre cluster.
- Chaque tâche qui utilise le type de lancement Fargate a sa propre limite d'isolement et ne partage pas le noyau sous-jacent, les ressources CPU, les ressources mémoire ou l'interface réseau élastique (ENI) avec une autre tâche.



Composants ECS

Pour préparer votre application, vous devez créer une définition de tâche.

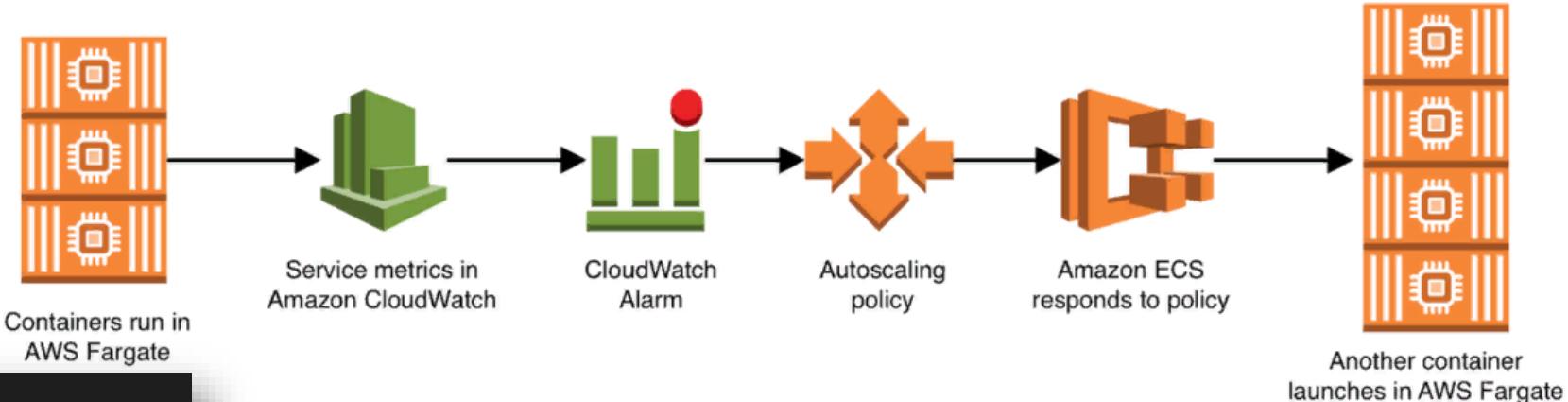
- La définition de tâche est un fichier texte, au format JSON, qui décrit un ou plusieurs conteneurs, jusqu'à un maximum de dix, qui forment votre application.
- Elle peut être considérée comme un plan de votre application. Les définitions de tâches précisent divers paramètres pour votre candidature. Les exemples de paramètres de définition de tâches sont les suivants : quels conteneurs utiliser, quel type de lancement utiliser, quels ports ouvrir pour votre application et quels volumes de données utiliser avec les conteneurs de la tâche.
- Les paramètres spécifiques disponibles pour la définition de la tâche dépendent du type de lancement que vous utilisez. Pour plus d'informations sur la création de définitions de tâches, voir Amazon ECS Task Definitions.
- Voici un exemple de définition de tâche contenant un seul conteneur qui fait tourner un serveur web NGINX en utilisant le type de lancement Fargate. Pour un exemple plus détaillé démontrant l'utilisation de plusieurs conteneurs dans une définition de tâche.

TASK DEFINITIONS

```
{  
  "family": "webserver",  
  "containerDefinitions": [  
    {  
      "name": "web",  
      "image": "nginx",  
      "memory": "100",  
      "cpu": "99"  
    },  
  ],  
  "requiresCompatibilities": [  
    "FARGATE"  
  ],  
  "networkMode": "awsVpc",  
  "memory": "512",  
  "cpu": "256",  
}
```



AutoScaling



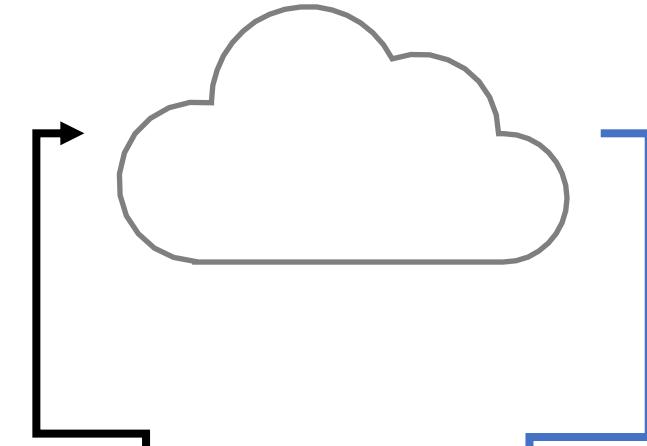
```
ScaleUpPolicy:  
Type: AWS::ApplicationAutoScaling::ScalingPolicy  
DependsOn: ScalableTarget  
Properties:  
  PolicyName: !Sub scale-${EnvironmentName}-${ServiceName}-up  
  PolicyType: StepScaling  
  ResourceId:  
    Fn::Join:  
      - '/'  
      - - service  
      - Fn::ImportValue: !Sub ${EnvironmentName}:ClusterName  
      - !Ref 'ServiceName'  
  ScalableDimension: 'ecs:service:DesiredCount'  
  ServiceNamespace: 'ecs'  
  StepScalingPolicyConfiguration:  
    AdjustmentType: 'ChangeInCapacity'  
    StepAdjustments:  
      - MetricIntervalLowerBound: 0  
        MetricIntervalUpperBound: 15  
        ScalingAdjustment: 1  
      - MetricIntervalLowerBound: 15  
        MetricIntervalUpperBound: 25  
        ScalingAdjustment: 2  
      - MetricIntervalLowerBound: 25  
        MetricIntervalUpperBound: 35  
        ScalingAdjustment: 3  
    MetricAggregationType: 'Average'  
    Cooldown: 60
```

```
ScaleDownPolicy:  
Type: AWS::ApplicationAutoScaling::ScalingPolicy  
DependsOn: ScalableTarget  
Properties:  
  PolicyName: !Sub scale-${EnvironmentName}-${ServiceName}-down  
  PolicyType: StepScaling  
  ResourceId:  
    Fn::Join:  
      - '/'  
      - - service  
      - Fn::ImportValue: !Sub ${EnvironmentName}:ClusterName  
      - !Ref 'ServiceName'  
  ScalableDimension: 'ecs:service:DesiredCount'  
  ServiceNamespace: 'ecs'  
  StepScalingPolicyConfiguration:  
    AdjustmentType: 'ChangeInCapacity'  
    StepAdjustments:  
      - MetricIntervalUpperBound: 0  
        ScalingAdjustment: -1  
    MetricAggregationType: 'Average'  
    Cooldown: 60
```

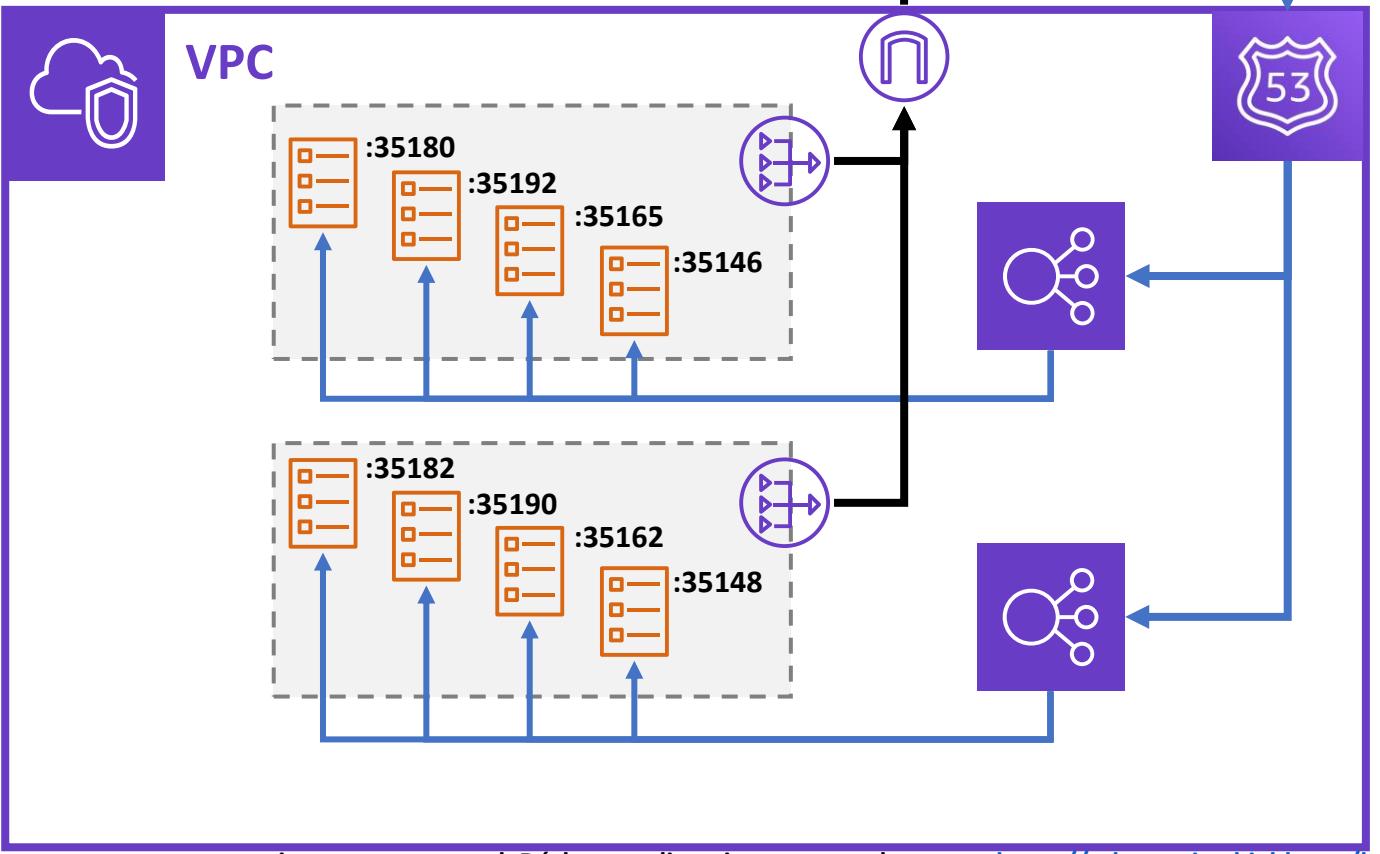


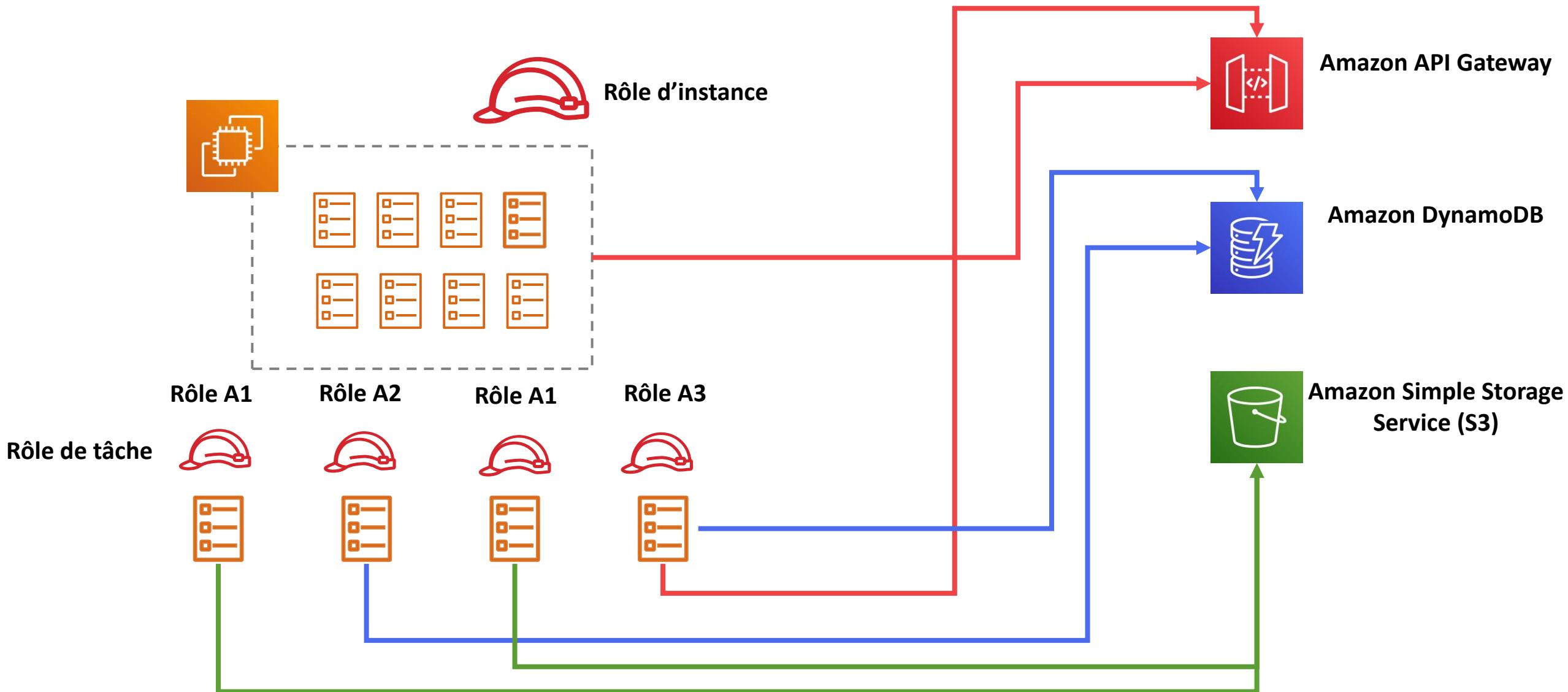
ECS avec Elastic Load Balancing

Vous pouvez configurer votre service Amazon ECS de manière à utiliser Elastic Load Balancing pour répartir uniformément le trafic entre les tâches de votre service.



- Support des **ALB**, NLB et CLB
- Pour EC2 et Fargate
- ALB offre à chaque service la capacité de desservir le trafic provenant de plusieurs équilibreurs de charge et exposer plusieurs ports en spécifiant plusieurs groupes cibles.
 - Dynamic port mapping
 - Path based routing
 - Priority rules



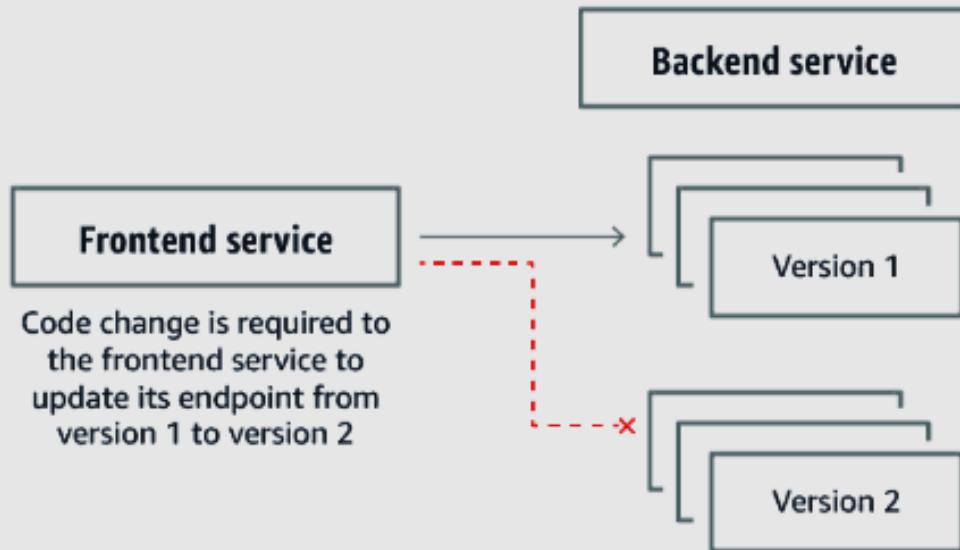




- Les conteneurs étant immuables par nature, ils peuvent être régulièrement renouvelés et remplacés par des versions plus récentes du service. Cela signifie qu'il est nécessaire d'enregistrer les nouveaux services et de résilier les services anciens ou instables.
- Faire cela par soi-même est un défi, d'où la nécessité d'un service de découverte et AWS Cloud Map est un service de découverte des ressources disponibles.
- Avec Cloud Map, vous pouvez définir des noms personnalisés pour vos ressources applicatives, et il maintient l'emplacement actualisé de ces ressources qui changent dynamiquement. Cela augmente la disponibilité de vos applications, car votre service web découvre toujours les emplacements les plus récents de ses ressources.

Without Cloud Map

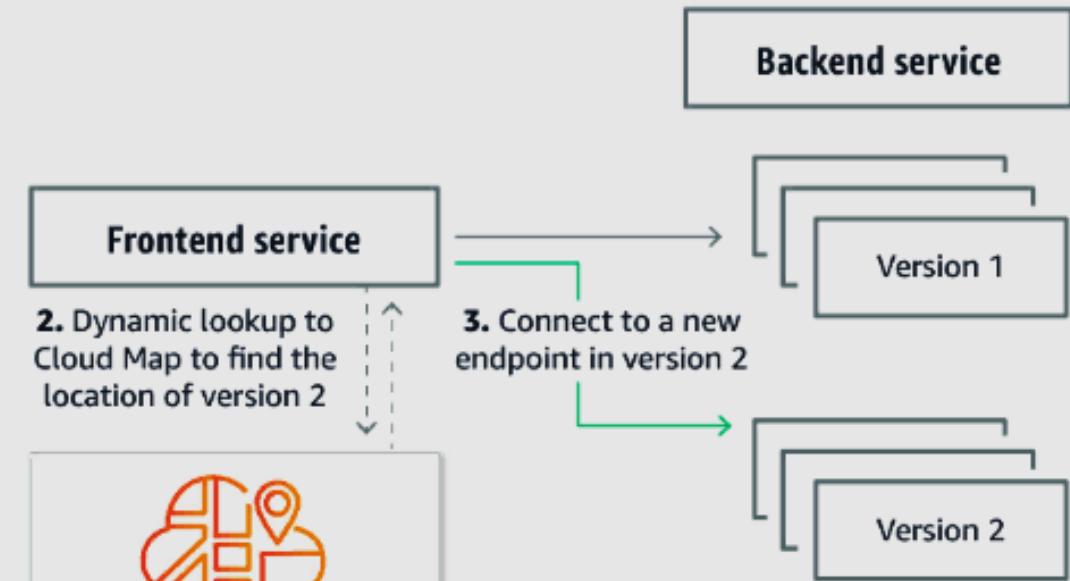
Endpoints are statically coded into your application



Code change is required to the frontend service to update its endpoint from version 1 to version 2

With Cloud Map

Endpoints are dynamically located



2. Dynamic lookup to Cloud Map to find the location of version 2

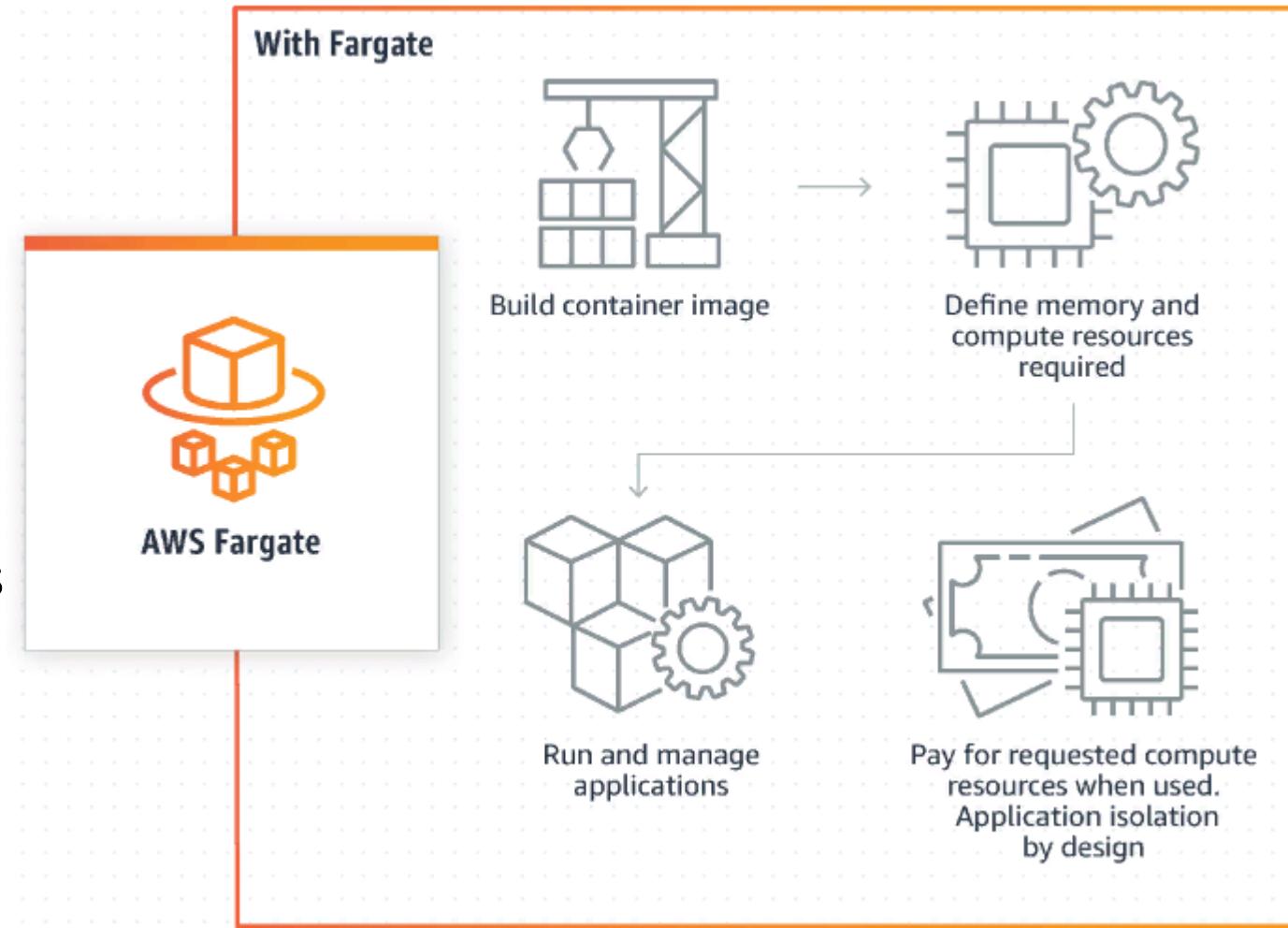
3. Connect to a new endpoint in version 2

1. Endpoint is updated from version 1 to version 2



FARGATE (serverless containers service)

- AWS Fargate est un moteur de calcul sans serveur pour les conteneurs.
- Fonctionne avec Amazon Elastic Container Service (ECS) et Elastic Kubernetes Service (EKS).
- Service entièrement géré
- Supprime le besoin de gestion globale des serveurs
- Payez pour les ressources consommées
- Chaque tâche fonctionne sur son propre noyau système
- Ressources sont isolées et sécurisées





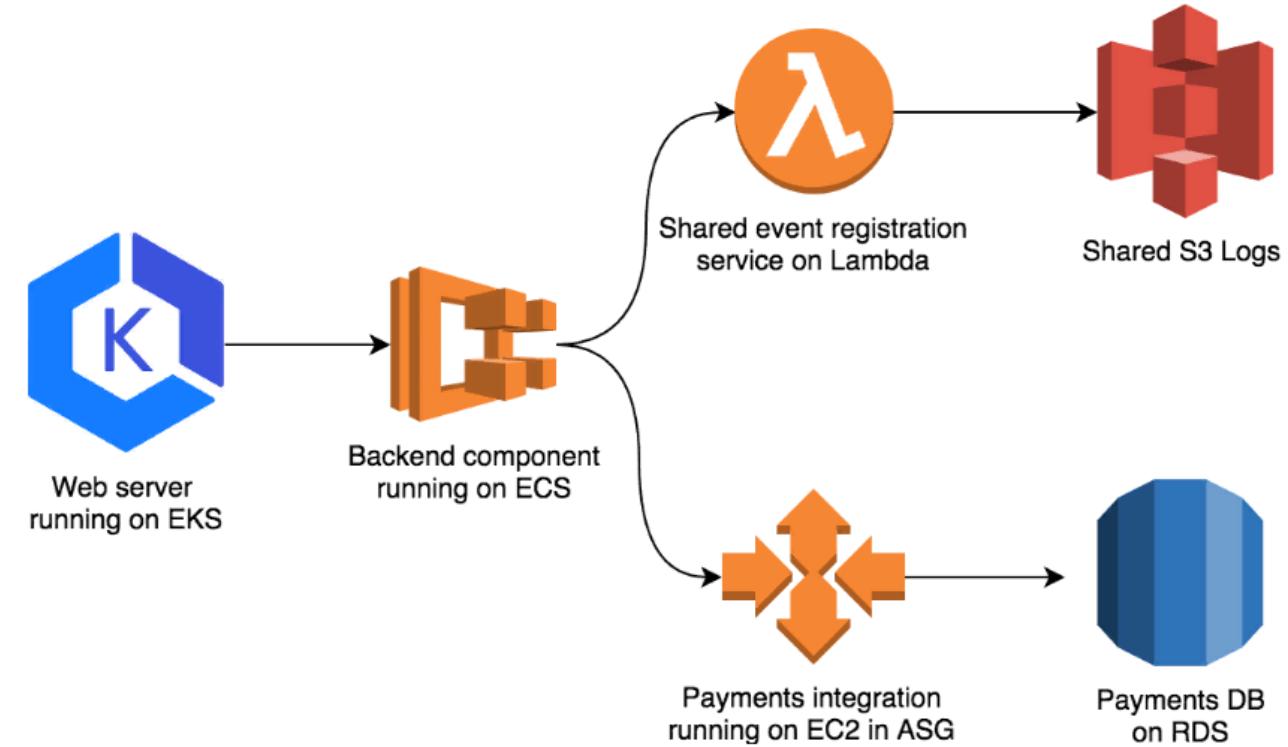
Elastic Kubernetes Service (EKS).

K - Kubernetes (K8s)



kubernetes

- K8s est un système open-source pour automatiser le déploiement, la mise à l'échelle et la gestion des applications conteneurisées
- Sécurisé, fiable, évolutif
- Amazon EKS supporte Fargate ou EC2
- Taches équivalent à des « Pods »
- Utilisation on premise ou cloud
- Vous payez 0,10\$/H pour chaque cluster
- Équipes connaissent déjà K8s
- Migration vers AWS





ECS Cas d'usage

ECS on EC2 :

- Contraintes de conformité
- personnalisation particulière
- Calcul par GPU

Une charge de travail importante, optimisée pour le prix

Si votre charge de travail nécessite de nombreux cœurs de processeur et de nombreux gigaoctets de mémoire, et que vous souhaitez optimiser le prix, vous devriez envisager de faire fonctionner un cluster d'instances EC2 réservées, ou des instances spot. Vous serez responsable de la maintenance et de l'optimisation de ce cluster, mais vous pourrez profiter des stratégies d'économie plus importantes grâce à ce type d'instances.

Une charge de travail importante, optimisée pour faible coût de fonctionnement

La gestion d'un grand nombre d'instances EC2 peut être quelque peu difficile. Vous devez vous assurer qu'elles sont toutes patchées, sécurisées et mises à jour avec la dernière version de Docker et de l'agent ECS. Si vous ne voulez pas vous occuper de ces instances, AWS **Fargate** peut être un bon choix.

Une charge de travail réduite, avec des pics de charges occasionnelles

Si votre charge de travail est faible et que vous avez des événements occasionnels, comme un site web qui a du trafic pendant la journée mais peu de trafic la nuit, alors AWS **Fargate** est un choix adapté. Vous pouvez réduire la taille de votre site à un minuscule conteneur la nuit, ce qui ne coûte pas grand-chose, mais l'augmenter le jour, tout en ne payant que pour les cœurs de processeur et les gigaoctets de mémoire nécessaires à votre tâche.

Une charge de travail minime

Pour un petit environnement d'essai, AWS **Fargate** est la solution idéale. Il est généralement inutile d'exécuter un petit environnement de test sur une instance EC2, car l'instance EC2 est trop puissante et vous aurez du mal à obtenir un bon pourcentage d'utilisation.

Charges de travail par lots

Si votre charge de travail consiste en des tâches périodiques, qui n'est effectué qu'une fois par heure, ou des travaux occasionnels qui proviennent d'une file d'attente, alors AWS **Fargate** est la solution idéale. Au lieu de payer pour une instance EC2, et de devoir la démarrer et l'arrêter entre deux utilisations, vous pouvez simplement demander à AWS Fargate de faire fonctionner votre conteneur quand vous en avez besoin, et de cesser de payer quand votre conteneur s'arrête.

Amazon Lightsail

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

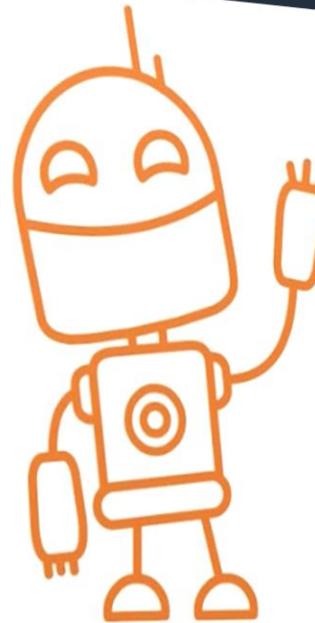
Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>



Lightsail

Est un service de VPS (virtual private server) hébergé par AWS

Imaginez le comme une version allégée et simplifiée du service EC2



Amazon **Lightsail**

- Configuration rapide et ultra simple
- Idéal pour les ingénieurs et développeurs non experts aws
- Service dédié aux petits sites web, blogs ou petites applications
- Les instances lightsail peuvent communiquer avec d'autres ressources aws et « migrer » vers EC2
- Prix de départ à 3.5\$





Lightsail



Est un service VPS (virtual private server) hébergé par AWS

* version allégée et simplifiée du service EC2

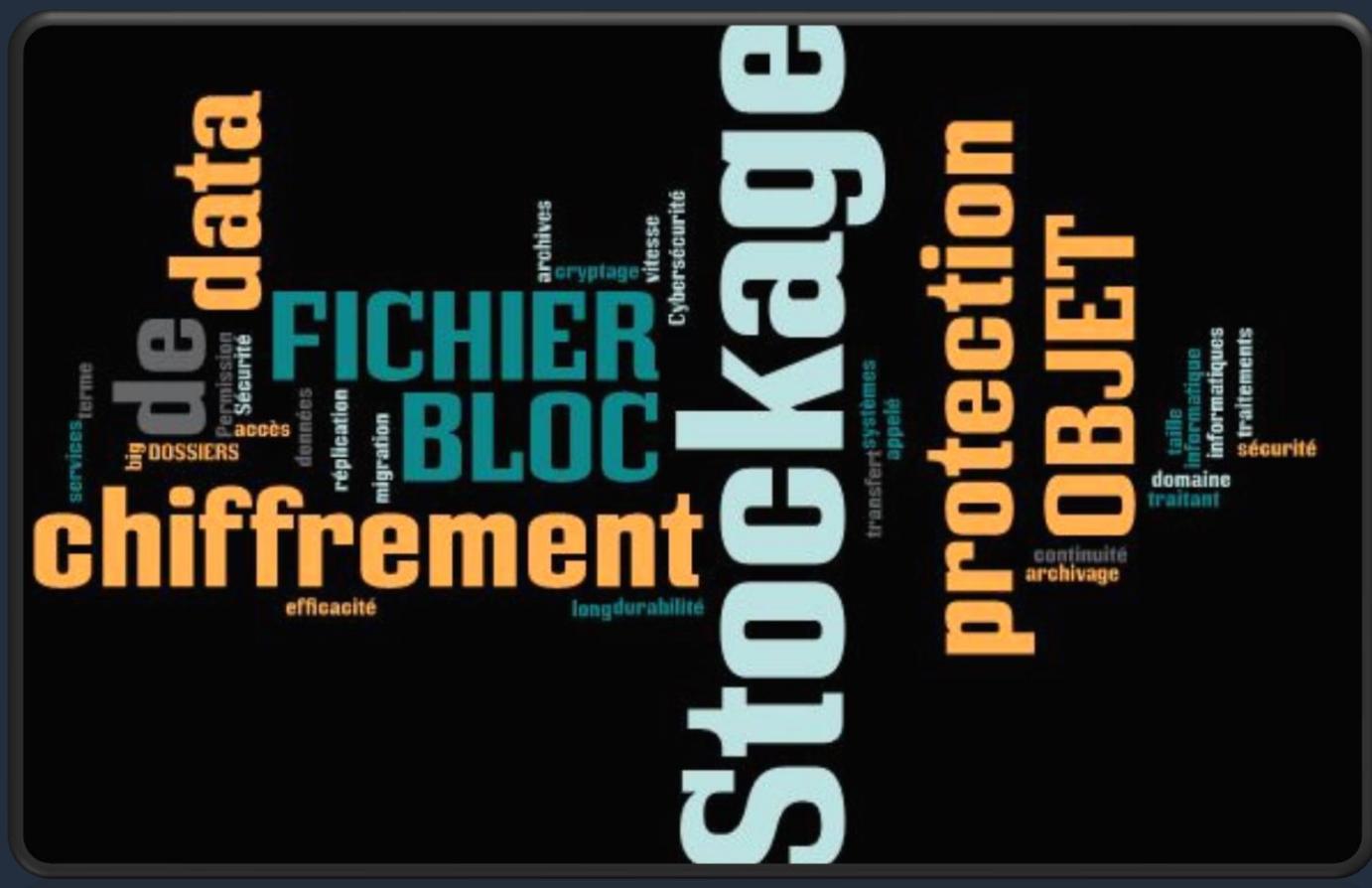


Fonctionnalités

- Serveur virtuel Lightsail dans votre région
- Accès SSH RDP en 1 click
- Stockage SSD à l'échelle et prise en charge des snapshots
- Modèles de systèmes d'exploitation et d'applications
- Gestion des DNS et adresse IP statique
- Équilibrage de charge simplifié
- Bases de données gérées
- Accès aux services AWS (VPC peering)
- Mise à niveau vers EC2
- Accès via API



Les services de stockage aws



Qu'est ce que le stockage ?

Le stockage dans le nuage est un modèle de stockage de données informatiques dans lequel les données numériques sont stockées dans des regroupements logiques.



Amazon Elastic Block Store



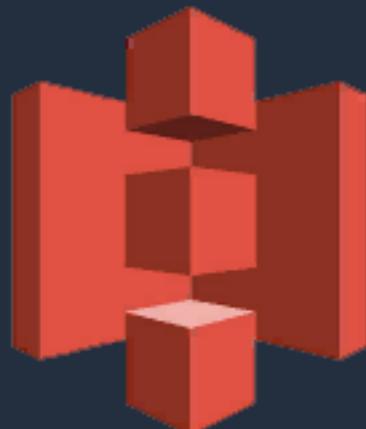
Stockage par blocs

Amazon EFS



Stockage de ticiers

Amazon S3



Stockage d'objets

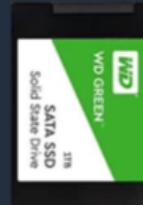
Stockage (Storage)

Le stockage dans le nuage est un modèle de stockage de données informatiques dans lequel les données numériques sont stockées dans des regroupements logiques. (blocs, fichiers, objets)

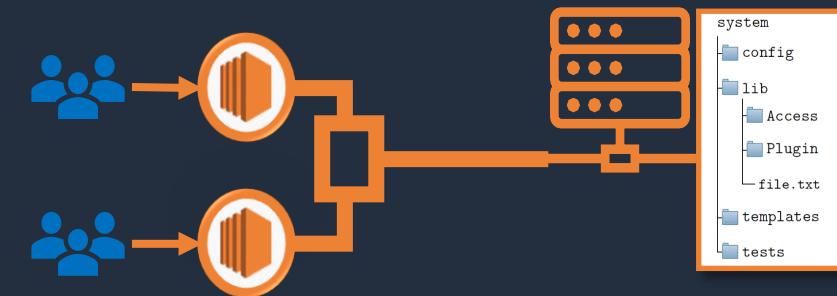


Amazon

Elastic Block Store



Amazon EFS



Amazon S3



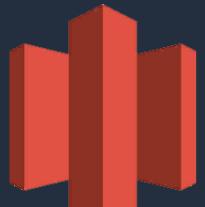
Amazon CloudFront



Amazon RDS



Amazon Glacier



Amazon Elastic Block Store

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

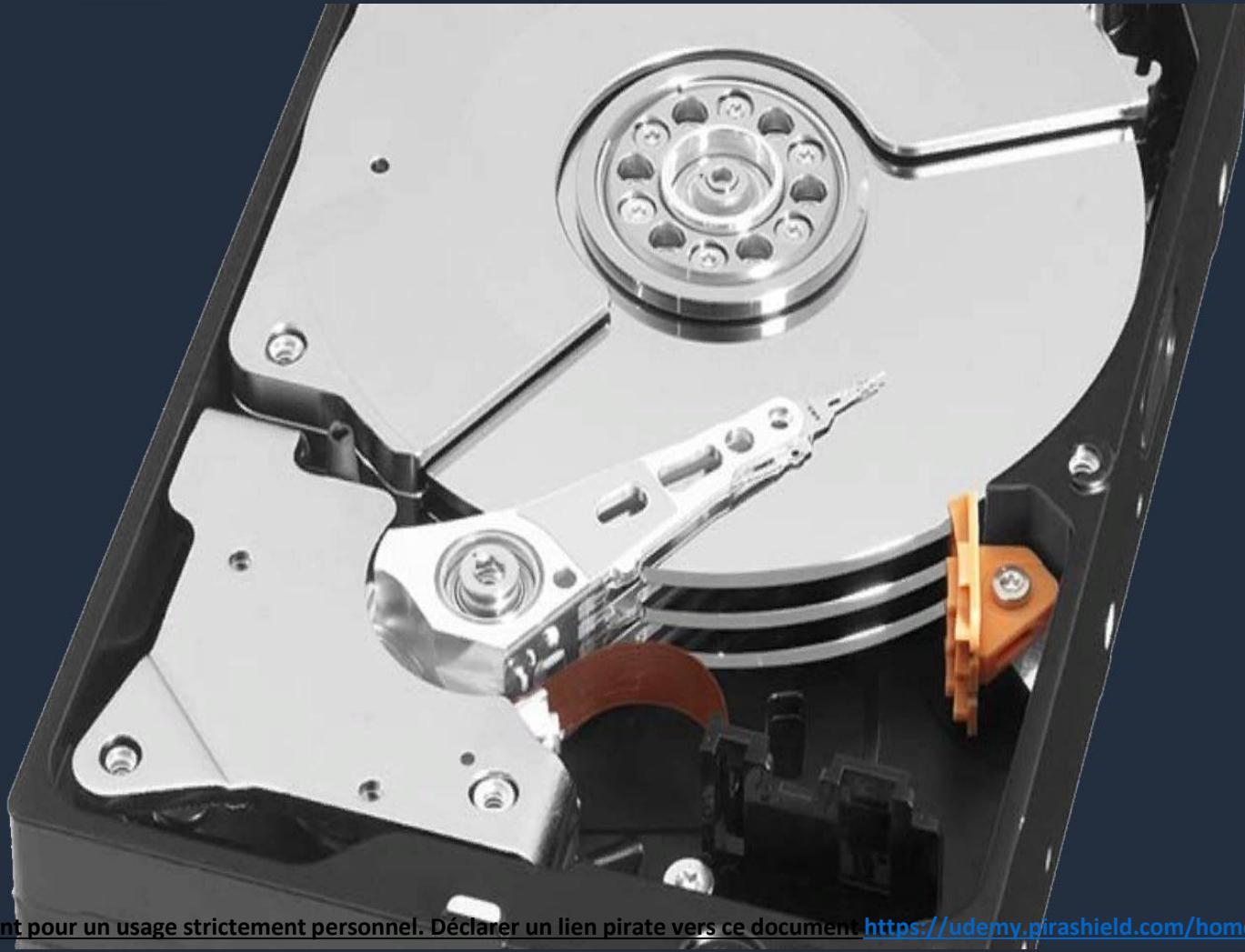
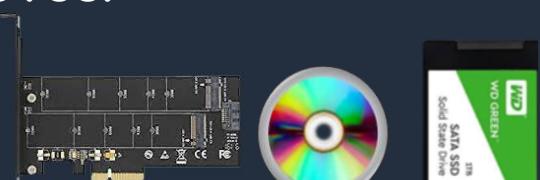
Le stockage en mode bloc (EBS)

DAS (Direct-Attached Storage) ou SAN (Storage Area Network).

Amazon Elastic Block Store (EBS), connecté aux serveurs virtuels offre une latence extrêmement faible, requise pour les charges de travail à hautes performances.



- Données sont découpées en bloc de taille fixe (ex : 4ko)
- Une table d'allocation est nécessaires pour localiser les données
- Lectures et écritures se font au niveau des blocs
- Protocoles : Hdd sas, iSCSI, FC, FCoE
- Données persistantes, consistantes, accessibles à faible latence : volumes EBS.
- Magnétiques, SSD, Nvme, (AMI) (RAID0,1)
- Données répliquées dans une seule AZ
- Sauvegarde sous forme de « snapshot » ou « instantanés » point in time.
- Chiffrement en temps réel
- Taille évolutive
 - dynamiquement



Le stockage par bloc

Stocké de manière redondante dans une seul AZ



Avantages :

- Performances pour n'importe quelle charge de travail
- Hautement disponible et durable
- Évolutivité presque illimitée
- Facilité d'utilisation Web CLI
- Paiement à l'usage
- Élasticité
- Sécurisé
- 1GB/s (not 1Gb/s)



Max supported by EBS

2 TiB

16 TiB

A La taille d'un volume IOPS provisionnées SSD (io1) ne peut pas dépasser 16384 Gio.

A La taille d'un volume Magnétique (standard) ne peut pas dépasser 1024 Gio.



Cas d'utilisation

Continuité de l'activité ↗

Applications d'entreprise ↗

Bases de données NoSQL ↗

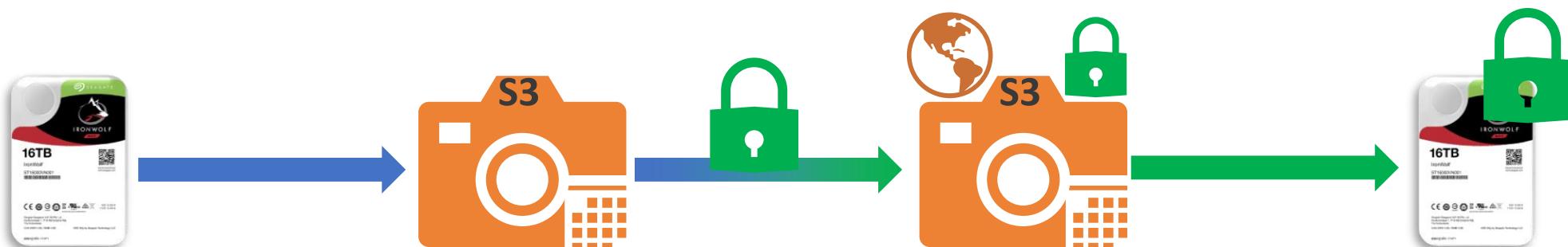
Moteurs d'analyse Big Data ↗

Bases de données relationnelles ↗

Systèmes de fichiers et flux de travail multimédias ↗



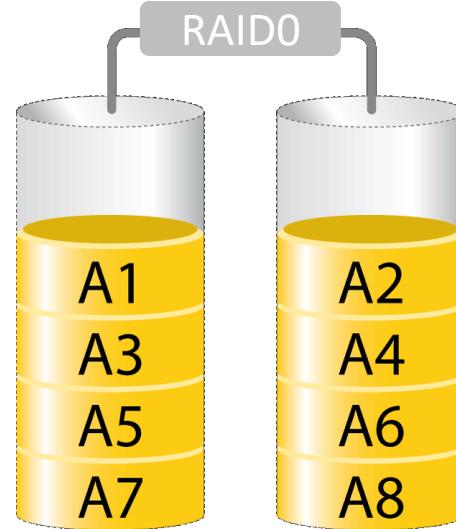
- Vous ne pouvez pas chiffrer un volume à chaud
- Vous pouvez chiffrer un volume à sa création
- Vous pouvez chiffrer un instantané en réalisant une copie
- Vous pouvez migrer un instantané vers une autre région en réalisant une copie
- Toutes les données comprises dans ce volume seront chiffrées
- Les données qui transitent par le réseau vers l'instance sont chiffrées
- Tous les instantanés de ce volume seront également chiffrés
- La clé de chiffrement utilisée par EBS est fournie par KMS (AES-256)



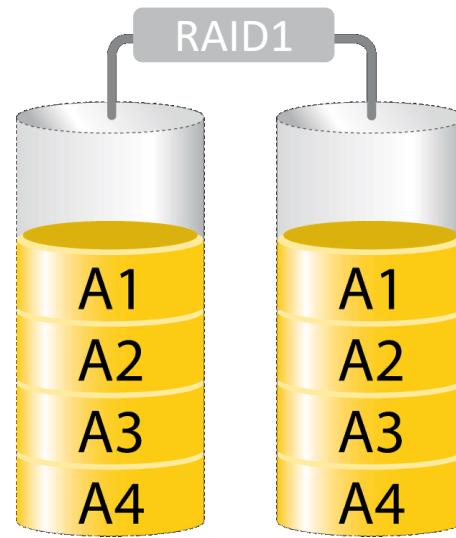


Striping - Mirroring EBS Volumes

- Lorsque les performances d'E/S ont plus d'importance que la tolérance aux pannes, par exemple, dans une base de données très utilisée (où la réPLICATION de données est déjà configurée séPARÉMENT).
- Les E/S sont réPARTIES entre les volumes dans un agrégat PAR bandes. Si vous ajoutez un volume, du débit et des IOPS sont ajoutés directement.
- Les performances de l'agrégat PAR bandes sont limitées au volume du jeu dont les performances sont les plus mauvaises. La perte d'un seul volume se traduit par une perte complète de données pour la grappe.



- Lorsque la tolérance aux pannes a plus d'importance que les performances d'E/S, par exemple, dans une application critique.
- Plus sûr en matière de durabilité des données.
- N'offre pas d'amélioration des performances en écriture ; nécessite une plus grande bande passante entre Amazon EC2 et Amazon EBS que les configurations non-RAID, car les données sont écrites simultanément sur plusieurs volumes.



RAID 5 et RAID 6 ne sont pas recommandés pour Amazon EBS, car les opérations d'écritures de parité de ces modes RAID consomment certaines des E/S par seconde (IOPS) disponibles pour vos volumes. En fonction de la configuration de votre grappe RAID, ces modes RAID fournissent de 20 à 30 % d'E/S par seconde utilisables en moins qu'une configuration RAID 0. Le coût accru est également un facteur à prendre en compte avec ces modes RAID ; avec l'utilisation de tailles et de vitesses de volume identiques, une grappe RAID 0 à 2 volumes peut offrir de meilleures performances qu'une grappe RAID 6 à 4 volumes dont le coût est deux fois plus élevé.

Amazon Elastic File System

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

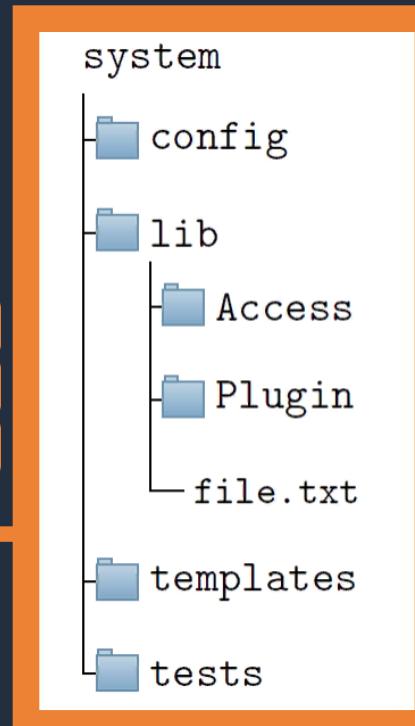
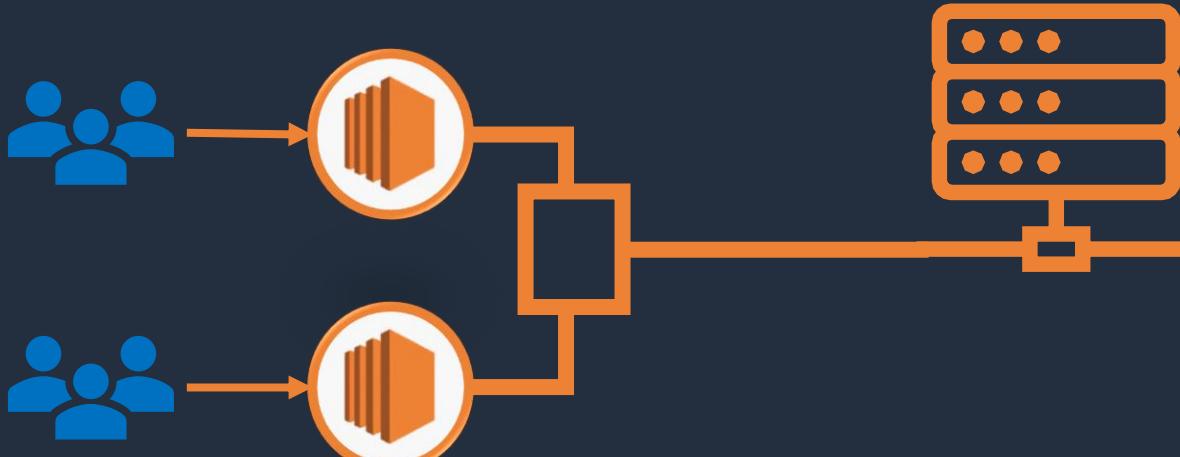
Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

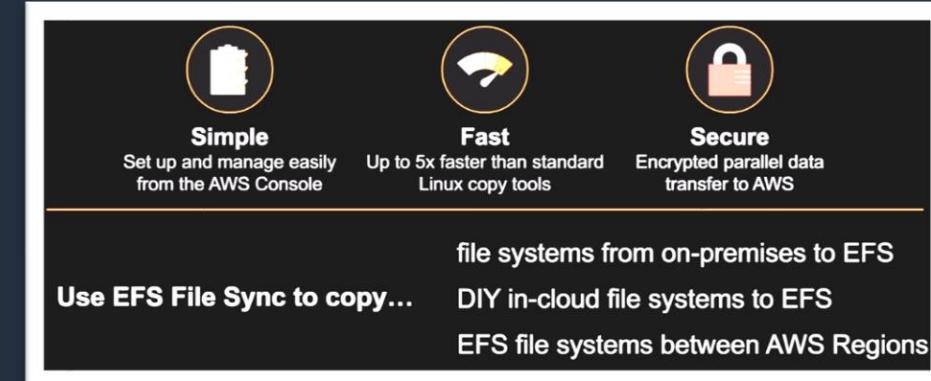
Le stockage en mode fichier (EFS)

Le stockage de fichiers dans le cloud est une méthode de stockage des données qui permet aux serveurs et aux applications d'accéder aux données via des systèmes de fichiers partagés.

- Données sont sous forme de fichier dans un système de stockage hiérarchique
- Il fournit un accès partagé aux données
- Les utilisateurs peuvent créer, supprimer, modifier, lire et écrire des fichiers
- Protocole : NFSv4



EFS File Sync



Amazon S3

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

Le stockage en mode objet (S3)

Le stockage d'objet est idéal pour créer des applications modernes de bout en bout qui exigent mise à l'échelle et flexibilité. S3 permet d'importer des magasins de données existants à des fins d'analyse, de sauvegarde ou d'archivage.



- Structure plate non hiérarchique
- Compartiments sécurisés avec gestion des accès
- Idéal pour les applications « cloud native »
- Classes de stockage avancées
- Migrations Snowball SnowMobile
- Accessible depuis n'importe où
- Protocoles : Web (API / SDK)



<https://images-504.s3.eu-west-3.amazonaws.com/orange.jpg>

`aws s3 rm s3://mybucket/test2.txt`

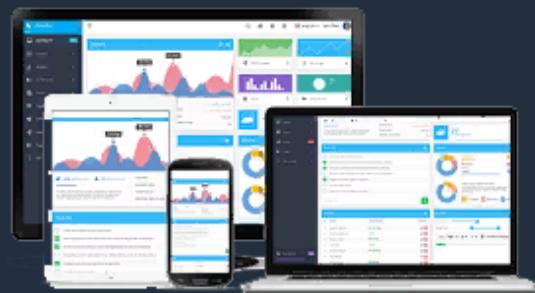
Stockage en mode objet (S3)

Objets stockés de manière redondante dans plusieurs AZ



Avantages :

- Performance, scalabilité, disponibilité
- Durabilité 99,99999999%
- Tiering intelligent & Access points
- Capacités de sécurité, de conformité et d'audit sans précédent
- Gérer facilement vos données et vos contrôles d'accès
- Services de requêtes sur place pour l'analyse
- Service de stockage dans le cloud n°1



Cas d'utilisation

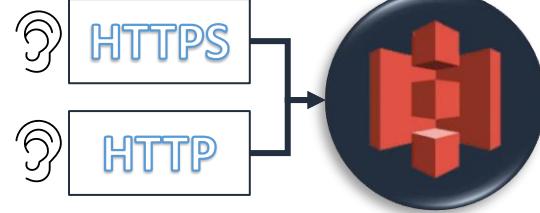


- Lacs de données et analyse de Big Data ↗
- Données d'application natives cloud ↗
- Stockage hybride dans le cloud ↗
- Sauvegarde et restauration ↗
- Reprise après sinistre ↗
- Archivage ↗



Chiffrement des objets S3

SSE-C



SSE-S3

- Chiffrement géré par le service S3
- Chiffrement uniquement coté serveur
- Chiffrement AES-256
- Header x-amz-server-side-encryption: est ajouté à la requête avec le paramètre « AES-256 »

SSE-KMS

- Chiffrement géré par le service S3 et KMS qui fournit
- L'accès à KMS est natif pour les services AWS et offre la sécurité et la traçabilité
- Toutes les demandes GET et PUT exigent SSL et Signature V4
- Header x-amz-server-side-encryption: est ajouté à la requête avec le paramètre « aws:kms »

SSE-C

HTTPS

- Chiffrement géré par S3 avec la clé du client
- Chiffrement uniquement coté serveur – S3 ne stocke pas vos clés de chiffrement
- Amazon S3 **rejette** toute demande faite via HTTP lors de l'utilisation de SSE-C.
- La clé de chiffrement est ajoutée à la requête pour réaliser le chiffrement coté serveur

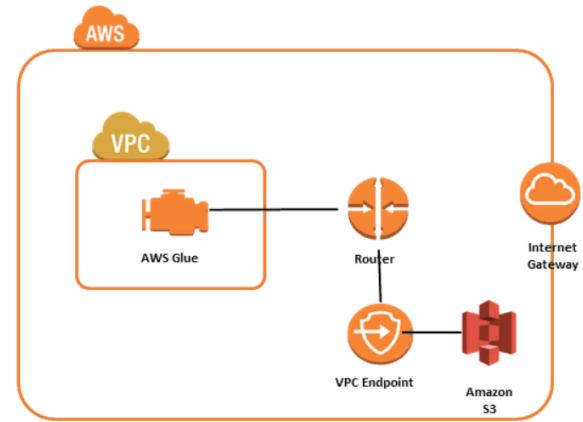
CSE

- Chiffrement géré coté client
- Le client chiffre ses objets avant l'envoi vers S3
- Le client déchiffre ses objets à la réception du service S3
- Amazon n'a jamais connaissance des clés utilisées et ne gère aucun chiffrement



Sécurité des objets S3

- Par défaut un compartiment S3 est privé
- Les objets déposés peuvent être chiffrés
- Autoriser un accès utilisateur avec IAM
- Autoriser l'accès à un compartiment avec S3 Bucket policies (depuis plusieurs comptes aws)
 - JSON (ressources, actions, effets, principal) Accès publique, chiffrement, accès croisée (cross account)
- Autoriser l'accès à un compartiment avec S3 Bucket ACL
- Autoriser l'accès à un objet avec des S3 ACL
- Autoriser un accès réseau interne au VPC (endpoint)
- Grader une trace des accès en stockant les logs d'accès dans un autre compartiment
- Conserver une trace des appels API dans AWS cloudtrail
- Sécuriser vos objets en imposant la double authentification pour l'effacement d'un objet
- Sécuriser vos objets grâce à des URL signées (signed URLs) pour une durée définie .

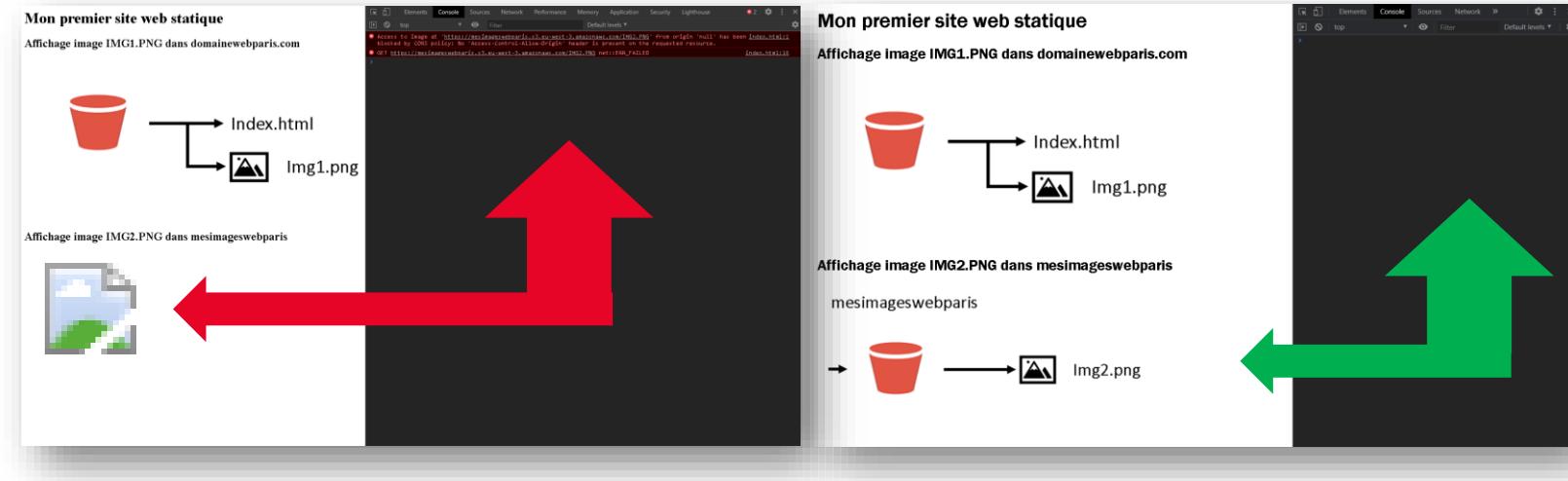
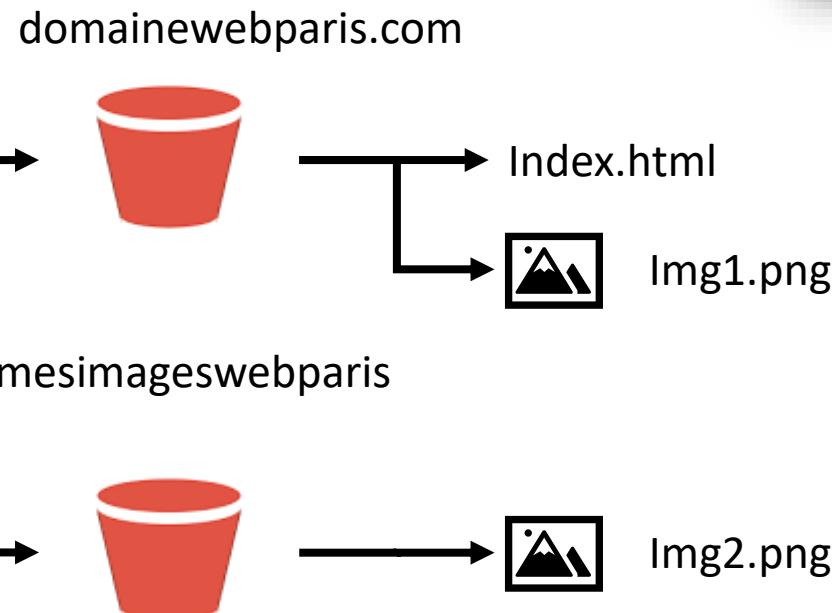




Site web statiques avec AMAZON S3

- Compartiment + index.html
- Activer l'accès public
- Site web statique
- Partage des ressources d'origine croisée (CORS)

S3



- Création d'un compartiment **domainewebparis.com**
- Autoriser l'accès en lecture (stratégie)
- Copier les objets index et image
- Création d'un compartiment **mesimageswebparis**
- Autoriser l'accès en lecture (stratégie)
- Tester
- Corriger les erreurs



Opérations courantes

- Crée un compartiment
- Écrire un objet
- Lire un objet
- Supprimer un objet
- Répertorier des clés

Le résultat est valable un certain temps



- Consistency (cohérente)
- Eventual consistency (cohérente à terme)

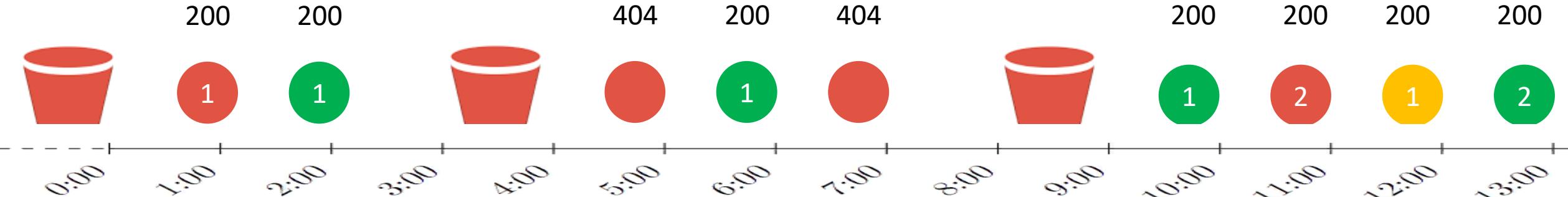
Un code de statut HTTP 2xx

- *HTTP Status Code: 200 OK*

Un code de statut HTTP 3xx, 4xx ou 5xx.

- *HTTP Status Code: 301 Moved Permanently*
- *HTTP Status Code: 400 Bad Request*
- *HTTP Status Code: 404 Not Found*

Name	Status	Type	Initiator	Size	Time
amazon.com	307		Other	0 B	13 ms
amazon.com	301	text/html	amazon.com/	192 B	280 ms
ATVPDKIKX0DER:136-5472361-2217854...	204	text/plain	(in...		Queued at 13.34 ms
136-5472361-2217854	200	xhr	61-		
favicon.ico	200	x-icon	Oth...		Started at 15.60 ms





Facturation du service S3

S3 Standard

Hiérarchisation intelligente S3

S3 Standard - IA

S3 One Zone – IA

S3 Glacier

S3 Glacier Deep Archive

S3 Standard - stockage à usage général pour n'importe quel type de données. Cette classe de stockage est généralement utilisée pour les données à accès peu fréquent.

50 premiers To/mois	0,023 USD par Go
450 To suivants/mois	0,022 USD par Go
Plus de 500 To/mois	0,021 USD par Go

S3 Intelligent-Tiering * - cette classe de stockage génère automatiquement des économies de coûts pour les données ayant des modèles d'accès inconnus ou irréguliers.

Niveau d'accès fréquent, premiers 50 To/mois	0,023 USD par Go
Niveau d'accès fréquent, prochains 450 To/mois	0,022 USD par Go
Niveau d'accès fréquent, plus de 500 To/mois	0,021 USD par Go
Niveau d'accès peu fréquent, tous le stockage/mois	0,0125 USD par Go
Surveillance et automatisation, tout le stockage/mois	0,0025 USD par tranche de 1 000 objets

S3 Standard	S3 Intelligent-Tiering	Hiérarchisation intelligente S3
S3 Standard - IA		
S3 One Zone – IA		
S3 Glacier		
S3 Glacier Deep Archive		

S3 Standard - accès peu fréquent * - pour les données à longue durée de vie, mais à accès peu fréquent nécessitant un temps d'accès de l'ordre de la milliseconde.

Tout le stockage/mois	0,0125 USD par Go
-----------------------	-------------------

S3 unizone - accès peu fréquent * - pour les données pouvant être recréées, mais à accès peu fréquent nécessitant un temps d'accès de l'ordre de la milliseconde.

Tout le stockage/mois	0,01 USD par Go
-----------------------	-----------------

S3 Glacier ** - pour les sauvegardes et les archives durables disposant de temps d'extraction allant de 1 minute à 12 heures;

Tout le stockage/mois	0,004 USD par Go
-----------------------	------------------

S3 Glacier Deep Archive ** - pour l'archivage durable des données nécessitant un ou deux accès par an et un temps de restauration inférieur à 12 heures.

Tout le stockage/mois	0,00099 USD par Go
-----------------------	--------------------



Cycle de vie des objets S3

Une configuration du Cycle de vie S3 est un ensemble de règles qui définit des actions que Amazon S3 applique à un groupe d'objets.

Actions de transition :

- Vous définissez à quel moment les objets migrent vers une autre classe de stockage.
- Des coûts sont associés aux demandes de transition de cycle de vie

Actions d'expiration :

- Vous définissez la date d'expiration des objets. Amazon S3 supprime en votre nom les objets ayant expiré.
- Les coûts d'expiration de cycle de vie dépendent du moment où vous choisissez de faire expirer des objets.



Stratégie de verrouillage (Lock policy) AMAZON S3 - Glacier

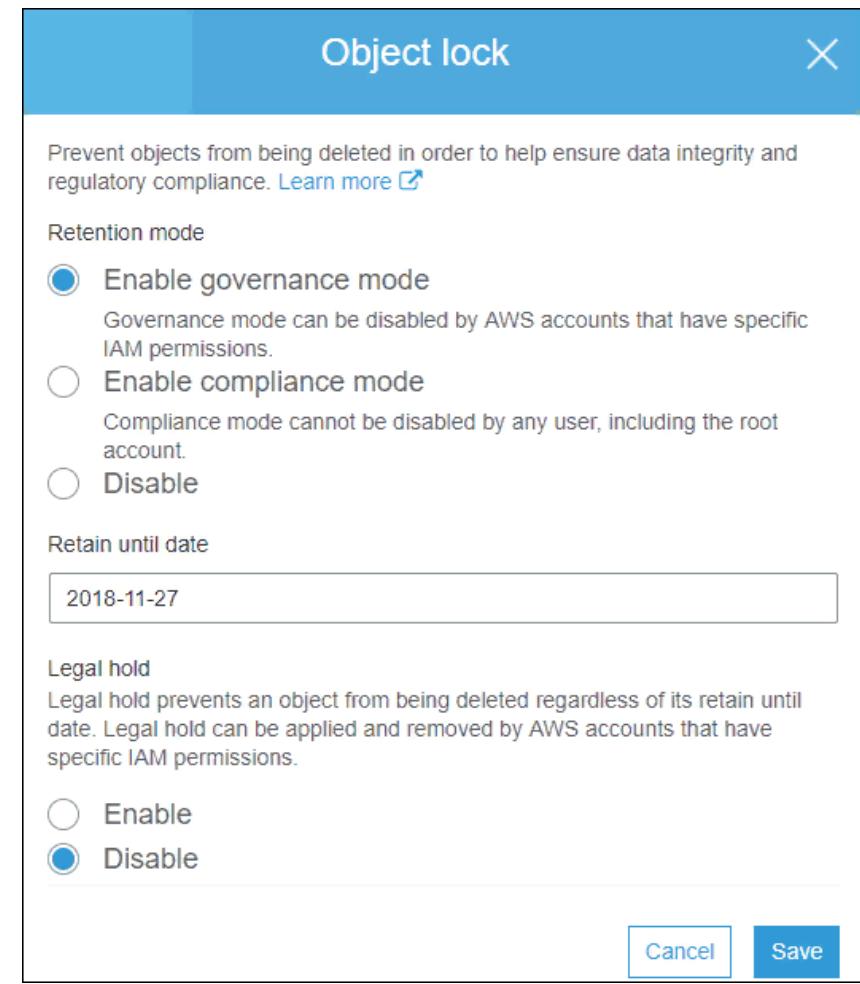
Un coffre (vault) ou un objet S3 peut être attaché à une stratégie d'accès au coffre ou à l'objet basée sur une ressource et à une stratégie de verrouillage de coffre ou de l'objet.

Verrouillage d'un objet S3 (object lock policy) Nov 26, 2018

- Adoption du modèle **WORM** (Write Once Read Many)
- Bloque la possibilité de suppression d'un objet pendant un temps T
- Mode Gouvernance** : les utilisateurs ne peuvent écraser, ou supprimer un objet. Toutefois certains utilisateurs peuvent obtenir les droits de modifier la rétention ou de supprimer l'objet si nécessaire.
- Mode Conformité** : Personne ne pourra écraser, ou supprimer un objet. Même le compte Racine. Vous avez la garantie que vos fichiers ne seront ni écrasés, ni effacés, durant la durée définie.
- Legal holds** : verrouille l'objet via s3:PutObjectLegalHold permission
- Applicable sur un objet ou au contenu d'un compartiment**

Verrouillage d'un coffre Glacier (vault lock policy) Jul 8, 2015

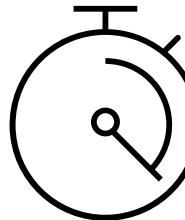
- Adoption du modèle WORM (Write Once Read Many)
- Bloque la possibilité de suppression d'un coffre glacier avec une stratégie, qui une fois appliquée ne pourra être changée.



Via AWS SDK, AWS CLI, API REST ou la console web



Instructions sur les performances pour Amazon S3



- Performances des mesures
- Mettre à l'échelle horizontalement les connexions de stockage
- Utiliser les extractions de plages d'octets (Multipart Up – Bytes range fetches Download)
- Combiner Amazon S3 (stockage) et Amazon EC2 (calcul) dans la même région AWS
- Utiliser Amazon S3 Transfer Accélération pour réduire la latence provoquée par la distance
- Choisissez la version la plus récente des kits AWS SDK



- péta-octets de données
- jusqu'à 100 Gbits/s sur une seule instance
- 100 à 200 millisecondes (10 ms cloudfront / elasticache)

Moncompartiment

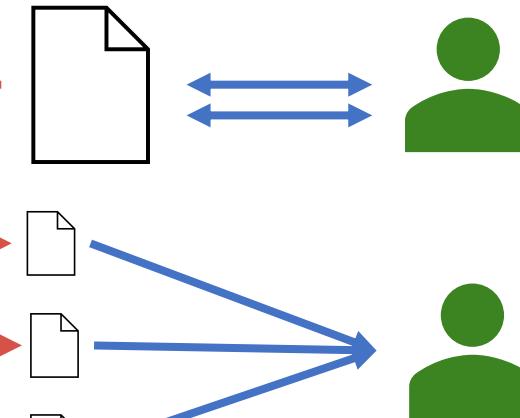
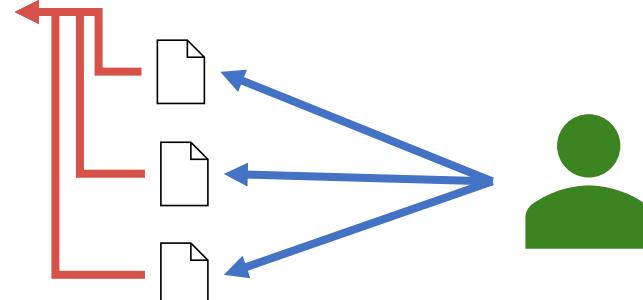
SSE-KMS limite les performances (UPL-DNL)

5500/10.000/30.000ops



$\frac{1}{1}$ 3500 ops PCPD
 $\frac{1}{1}$ 5500 ops GH

$\frac{1}{1} \times 3$ 10500 ops Put-Copy-Post-Delete
 $\frac{1}{1}$ 16500 ops Get-Head



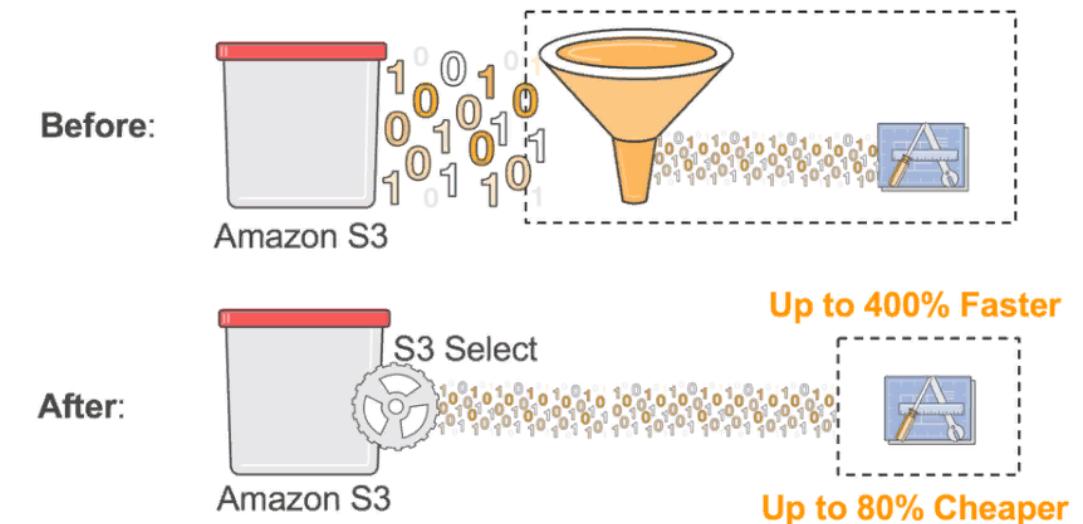


AMAZON S3 Select & Glacier Select (29 NOV 2017) « Exécution de requêtes sur place »

S3 Select, permet aux applications de ne récupérer qu'un sous-ensemble de données d'un objet en utilisant de simples expressions SQL.

- Récupérer uniquement les informations souhaitées via une simple requête SQL exécutée côté serveur.
- Amazon S3 Select prend en charge quelques fonctions agrégées (Glacier ne les prend pas en charge).
- Amazon S3 Select, Glacier Select supportent les fonctions SQL (Conditional, Conversion, Date, String)
- Les requêtes Amazon S3 Select et S3 Glacier Select ne prennent pas en charge les sous-requêtes ou les jointures. (act.)

- Amazon S3 Select fonctionne avec les objets stockés au format CSV, JSON ou Apache Parquet.
- fonctionne avec les objets compressés avec GZIP ou BZIP2 (pour les objets CSV et JSON)
- Supporte les objets chiffrés côté serveur (SSE)
- Filtre les résultats par ligne et colonnes.
- Réduit la consommation réseau et processeur côté client

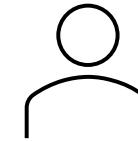
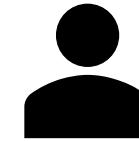




Accorder un accès entre comptes à des objets dans des compartiments S3

Pour accorder l'accès entre comptes aux objets stockés dans des compartiments S3 vous pouvez utiliser :

- Stratégies basées sur les ressources (s3) et stratégies AWS Identity and Access Management (IAM) pour un accès par programmation uniquement aux objets du compartiment S3 (**Bucket Policies & IAM programmatic only**)
- Liste de contrôle d'accès (ACL) (s3) et stratégies IAM basées sur les ressources pour un accès par programmation uniquement aux objets du compartiment S3 (**Bucket ACL's & IAM programmatic only**)
- Rôles IAM entre comptes pour l'accès par programmation et par console aux objets du compartiment S3 (**Cross account IAM Roles programmatic + web console**)

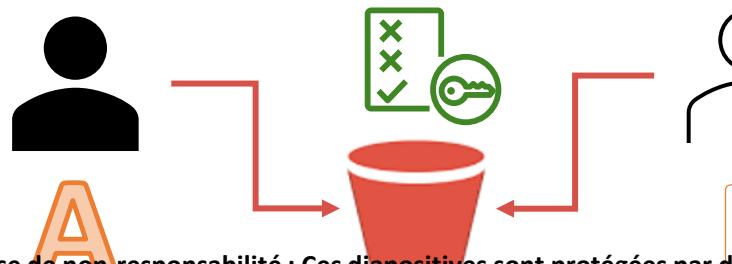




Stratégies basées sur les ressources et stratégies IAM

accès par programmation uniquement

1. Créez un compartiment S3 dans le compte A.
2. Créez un rôle IAM ou un utilisateur dans le compte B.
3. Accordez au rôle IAM ou à l'utilisateur du compte B l'autorisation souhaitée
4. Configurez la stratégie de compartiment pour le compte A afin d'accorder des autorisations au rôle IAM ou à l'utilisateur que vous avez créé dans le compte B.



Rôle S3



Lister
Lecture
Ecriture

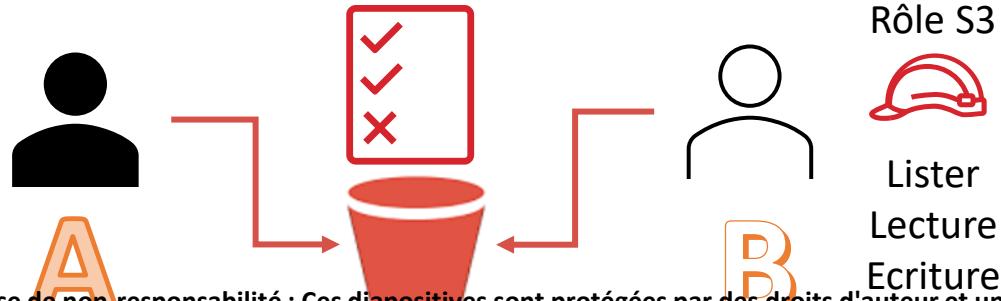




Liste de contrôle d'accès (ACL) basée sur les ressources et stratégies IAM

accès par programmation uniquement

1. Créez un rôle IAM ou un utilisateur dans le compte B. accordez à ce rôle ou à cet utilisateur des autorisations
2. Configurez la liste ACL du compartiment pour inclure au moins l'autorisation WRITE pour le compte B. Cela garantit que les rôles IAM ou utilisateurs du compte B peuvent charger des objets (appel de l'API PutObject) dans un compartiment appartenant au compte A
3. Configurez les listes ACL d'objets pour inclure au moins l'autorisation READ pour le compte B.



```
...
<AccessControlPolicy>
  <Owner>
    <ID> AccountACanonicalUserID </ID>
    <DisplayName> AccountADisplayName </DisplayName>
  </Owner>
  <AccessControlList>
    ...
      <Grant>
        <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="CanonicalUser">
          <ID> AccountBCanonicalUserID </ID>
          <DisplayName> AccountBDisplayName </DisplayName>
        </Grantee>
        <Permission> WRITE </Permission>
      </Grant>
    ...
  </AccessControlList>
</AccessControlPolicy>
...
<AccessControlPolicy>
  <Owner>
    <ID> AccountACanonicalUserID </ID>
    <DisplayName> AccountADisplayName </DisplayName>
  </Owner>
  <AccessControlList>
    ...
      <Grant>
        <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="CanonicalUser">
          <ID> AccountBCanonicalUserID </ID>
          <DisplayName> AccountBDisplayName </DisplayName>
        </Grantee>
        <Permission> READ </Permission>
      </Grant>
    ...
  </AccessControlList>
</AccessControlPolicy>
```



Rôles IAM entre comptes

accès par programmation et par console

- Créez un rôle IAM dans le compte A. Ensuite, accordez au rôle les autorisations nécessaires pour effectuer les opérations S3 requises.

Dans la stratégie d'approbation du rôle, accordez à un rôle ou à un utilisateur du compte B les autorisations nécessaires pour assumer le rôle dans le compte A

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "arn:aws:iam::AccountB:user/AccountBUserName" }, "Action": "sts:AssumeRole" } ] }
```

```
{ "Version": "2012-10-17", "Statement": [ { "Action": [ "s3>ListAllMyBuckets" ], "Effect": "Allow", "Resource": [ "arn:aws:s3:::*" ] }, { "Action": [ "s3>ListBucket", "s3>GetBucketLocation" ], "Effect": "Allow", "Resource": "arn:aws:s3:::AccountABucketName" }, { "Effect": "Allow", "Action": [ "s3GetObject", "s3PutObject" ], "Resource": "arn:aws:s3:::AccountABucketName/*" } ] }
```

- Accordez à un rôle ou à un utilisateur IAM du compte B les autorisations nécessaires pour assumer le rôle IAM que vous avez créé dans le compte A.

- Depuis un rôle ou un utilisateur du compte B, assumez le rôle dans le compte A par programmation afin que les entités IAM du compte B puissent effectuer les opérations S3 requises.

```
{ "Version": "2012-10-17", "Statement": { "Effect": "Allow", "Action": "sts:AssumeRole", "Resource": "arn:aws:iam::AccountA:role/AccountARole" } }
```



AMAZON S3 RéPLICATION

(CRR – Cross Region Replication)

Pour activer la réPLICATION d'objet, il vous suffit d'ajouter une configuration de réPLICATION à votre COMPARTIMENT source.

La configuration minimale doit fournir :

- Le COMPARTIMENT de destination dans lequel vous souhaitez qu'Amazon S3 réPLIQUE les objets
- Un rôle AWS Identity and Access Management (IAM) pouvant être endossé par Amazon S3 pour réPLIQUER les objets en votre nom

Exigences et points d'attention :

- La gestion des versions doit être activée pour les compartiments source et de destination.
- Amazon S3 doit disposer des autorisations adéquates pour réPLIQUER en votre nom les objets issus du COMPARTIMENT source vers le COMPARTIMENT de destination.
- Les fichiers existants ne sont pas réPLIQUÉS par défaut vous devez réaliser la copie manuellement si besoin.
- Les marqueurs de fichiers effacés ne sont pas réPLIQUÉS.

Quand utiliser la réPLICATION entre régions ?

- Respecter les exigences de conformité
- Réduire la latence
- Augmenter l'efficacité opérationnelle

Pourquoi utiliser la réPLICATION

- RéPLIQUER des objets tout en conservant les métadonnées
- RéPLIQUER des objets dans différentes classes de stockage
- Conserver des copies d'objets sous différents propriétaires
- RéPLIQUER des objets dans les 15 minutes



AWS DataSync

Service de transfert de données en ligne

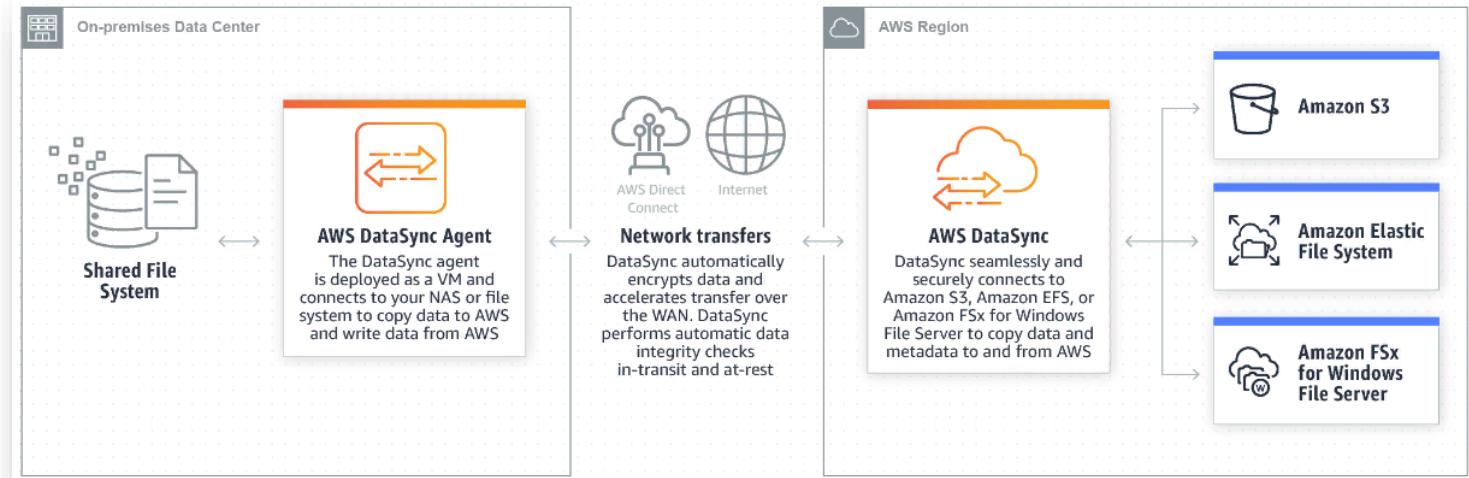


Simplifie, automatise et accélère la copie de grands volumes de données vers et depuis les services de stockage AWS via Internet ou AWS Direct Connect.

- Installation d'un agent sur un serveur local ayant une connexion au système de stockage
- Peut copier vers AWS ou écrire en local depuis AWS (synchro)
- Dispose d'un protocole propriétaire AWS qui permet d'accélérer la copie et de chiffrement automatiquement à la volée
- Dispose d'un mécanisme de vérification d'intégrité des données en transit ou au repos (at rest)
- Connecte S3, EFS, FSx pour windows file server, pour copier les données et les métadonnées vers ou depuis AWS

Quand utiliser AWS DataSync ?

- Déplacer un volume important de donnée
- Utile pour les volumes NFS ou SMB
- RéPLICATION planifiées /heure/jour/semaine
- Possibilité de déployer des agents
- Réaliser des sync EFS vers EFS
- Service gratuit
- Paiement des données transférées





AMAZON FSx pour Windows & FSx pour Lustre



Exécuter des systèmes de fichiers riches en fonctionnalités et très performants

Amazon FSx permet de lancer et d'exploiter facilement et à moindre coût des systèmes de fichiers populaires qui sont entièrement gérés par AWS.

Amazon FSx pour Windows File Server :

- Accéder à un stockage de fichiers très fiable, évolutif et entièrement géré, via le protocole SMB standard
- Idéale pour les organisations qui s'appuient sur un annuaire Active Directory (AD), et des applications « Windows based », MS Sharepoint, MS SQL Server, Workspaces, IIS Server Web et autres fortement liées à l'environnement Microsoft.
- Fonctionne sous **Windows server** (utilisateurs, acl, groupes, gpo ...) supporte le nommage et la réPLICATION DFS (Distributed File System)

Amazon FSx pour Lustre :

- Lustre est une plateforme logicielle de système de fichiers parallèles distribués à code source ouvert, conçue pour l'évolutivité, la haute performance et la haute disponibilité. (existe en mode intégré à S3)
- Idéale pour le **HPC**, **ML**, **MPW**, **EDA**, et le besoin de très hautes performances **100GB/S**, Millions **IOPS**, latences inférieures à la **milliseconde**.

EFS : Elastic File system

- Système NAS géré pour les instances EC2 accessible via le protocole NFSv4
- Idéale pour le partage de fichier (sans limites de volumétrie) pour les environnements **Unix et Linux**

Amazon CloudFront

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

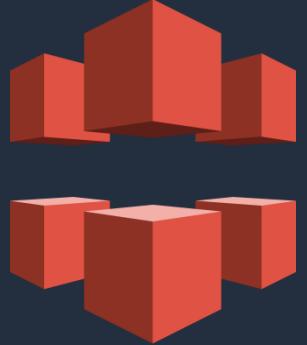
Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

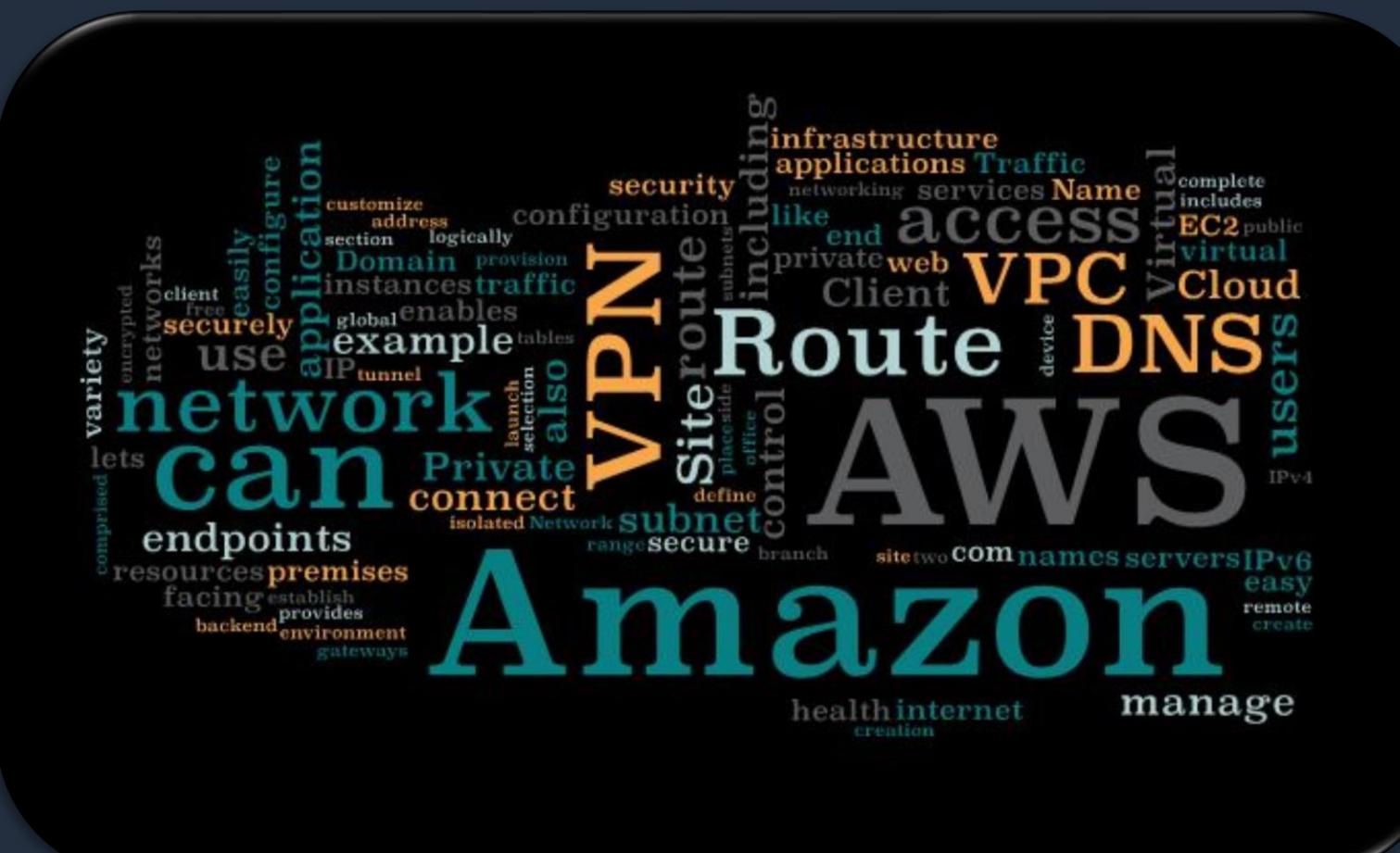
Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

Cloudfront (Content Delivery Network)

Réplique les données S3 au plus proche des clients



Les services réseaux

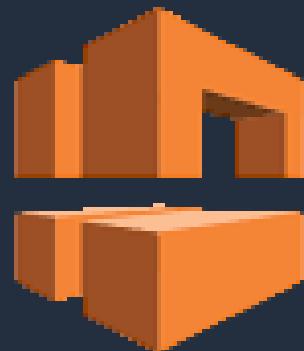


A cloud-shaped collage of network-related terms and concepts, including:

- VPN
- Route
- DNS
- AWS
- Amazon
- management
- internet creation
- health
- IPv6
- IPv4
- users
- Cloud
- Virtual
- EC2
- public
- virtual
- Client
- VPC
- Device
- Name
- Traffic
- networking services
- services
- traffic
- subnets
- place
- office
- branch
- site
- two
- com
- names
- servers
- private
- web
- access
- like
- end
- control
- secure
- range
- Network
- subnet
- define
- selection
- also
- launch
- isolation
- connect
- Private
- can
- network
- example
- tunnel
- IP
- global
- enables
- tables
- instance
- traffic
- Domain
- provision
- section
- logically
- customize
- address
- section
- client
- free
- securely
- use
- application
- network
- can
- variety
- encrypted
- networks
- lets
- comprise
- endpoints
- resources
- premises
- facing
- establish
- backend
- provides
- environment
- gateways

Qu'est ce que le réseau ?

Un Nuage Privé Virtuel, ou Cloud Virtuel Privé, ou Virtual Private Cloud (VPC) est un groupe de ressources informatiques configurables à la demande dans un environnement de cloud public.



Virtual Private cloud



Route 53



Virtual Private Network



Introduction

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



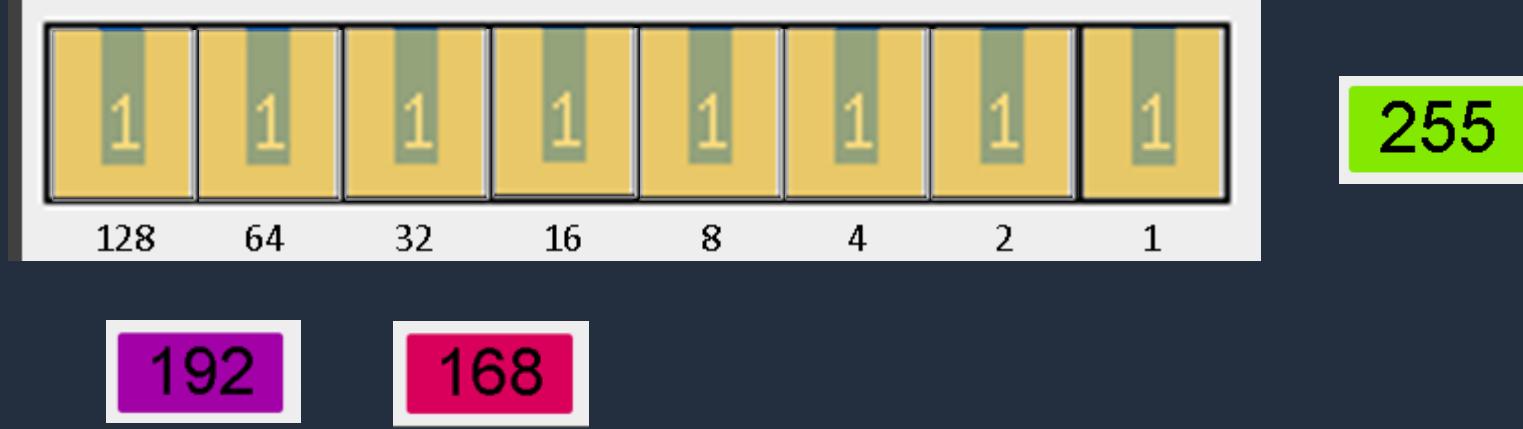


Adresses IP

Un adresse IP est composée de 4 octets (décimal)

192 . 168 . 1 . 30

Un octet est composé de 8 bits (binaires 0 ou 1)





Les sous réseaux

Adresse IPv4 : 192.168.1.30
Masque de sous-réseau : 255.255.255.0

11000000.10101000.00000001.00011110
11111111.11111111.11111111.00000000 (/24)

Opération ET LOGIQUE (1+1 =1 sinon = 0)

11000000.10101000.00000001.00000000

192 . 168 . 1 . 0 / 24

De 192.168.1.0 à 192.168.1.255 = 256 adresses moins 2 adresses réservées (0 et 255)

La plage d'adresses disponibles est donc : 192.168.1.1 à 192.168.1.254

10 . 0 . 0 . 0 / 16 65 534 (0 -> 65535 = 65536 -2)

0 . 0 . 0 . 0 / 0 4 294 967 296 pour IPv4 32 bits

0000:0000:0000:0000:0000:000F 340282366920938463463374607431768211456 IPv6 128Bits

Amazon Virtual Private Cloud

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

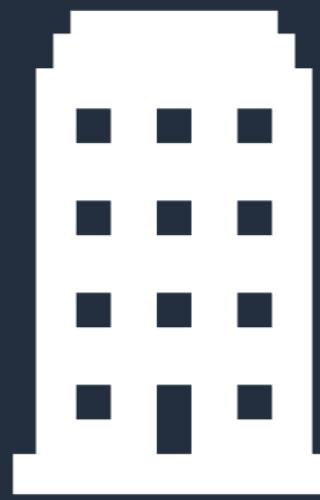


Virtual Private Cloud

- Votre réseau virtuel privé
 - isolé logiquement dans le cloud AWS
 - conçu pour la haute disponibilité et la continuité de service
- Accès complet à la configuration de votre réseau
 - Sous réseaux (CIDR blocks « Classless Inter-Domain Routing »)
 - Table de routage
 - Sécurité (SG – ACL)
 - Internet Gateway
- Les services AWS dans un VPC sont accessibles via des « Endpoints »

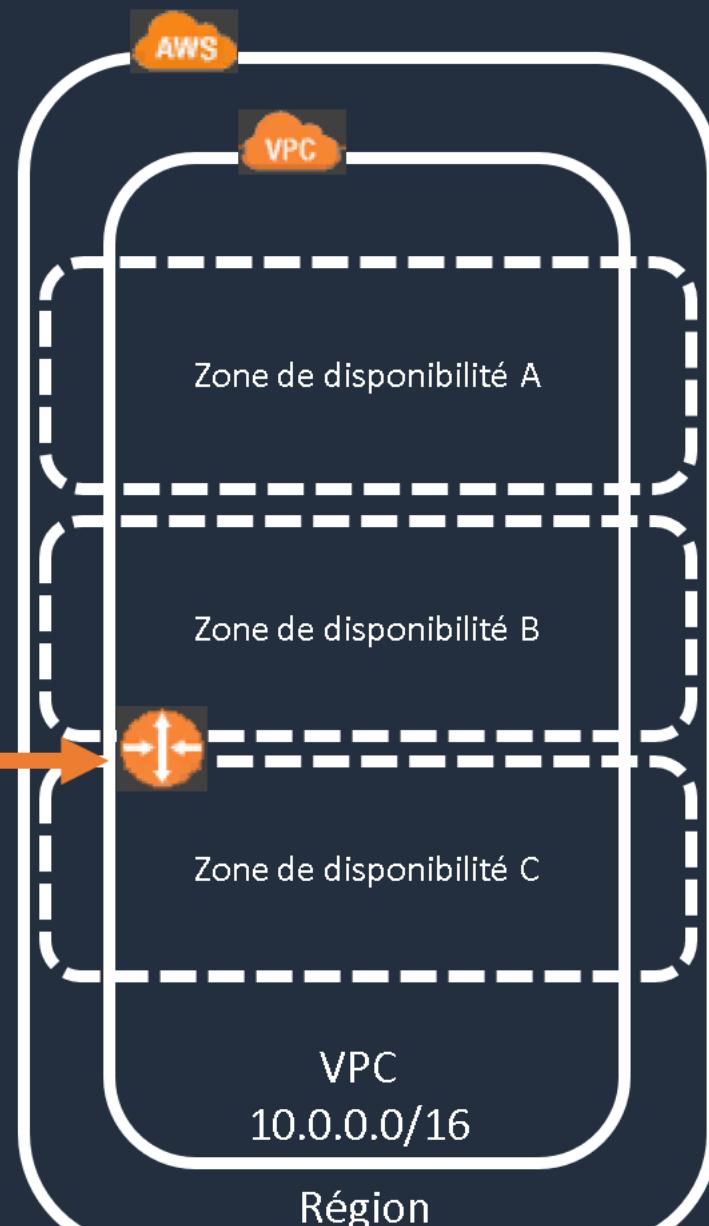


VPC : Virtual Private Cloud



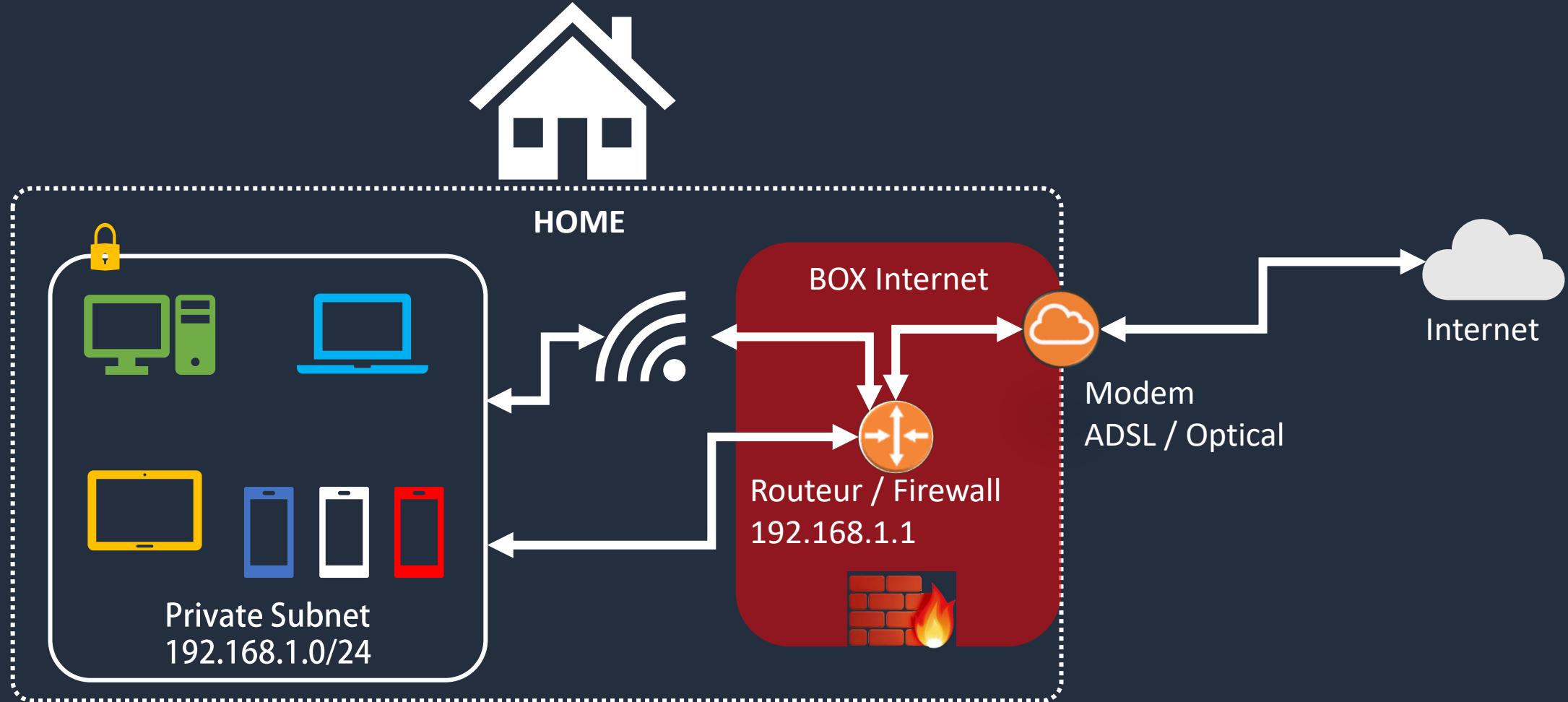
VPN – Direct Connect

VPC est un service qui offre la capacité de créer une zone réseau qui vous appartient dans le cloud AWS. Dans cette zone vous avez la possibilité déplacer des ressources comme des instances EC2 ou des bases de données vous avez un contrôle total sur « qui » accèdent aux ressources que vous avez placé dans cette zone. Aussi vous pouvez étendre ce réseau dans votre centre de données historique, cela permet de simplifier l'accès aux différentes ressources.



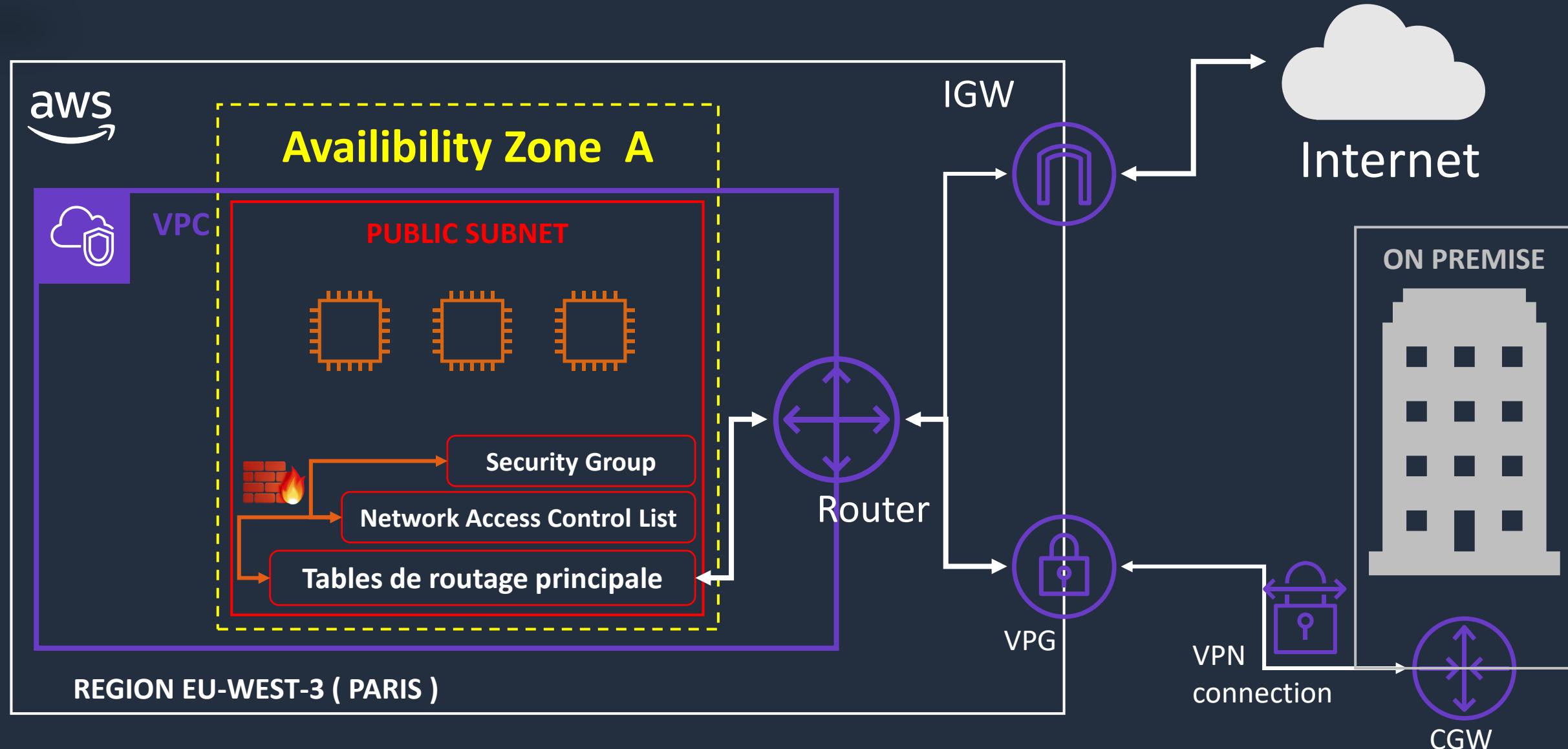


Home Private network





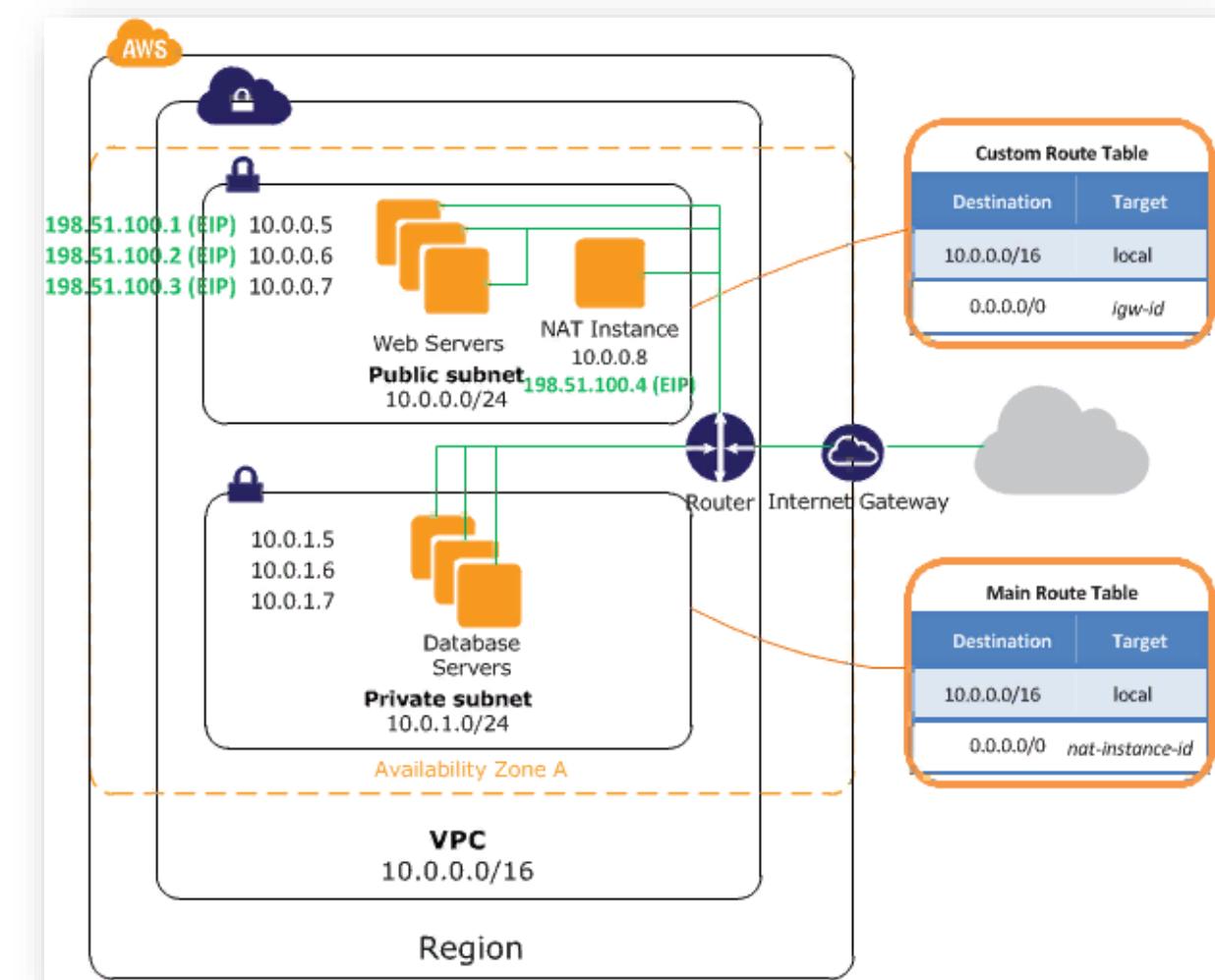
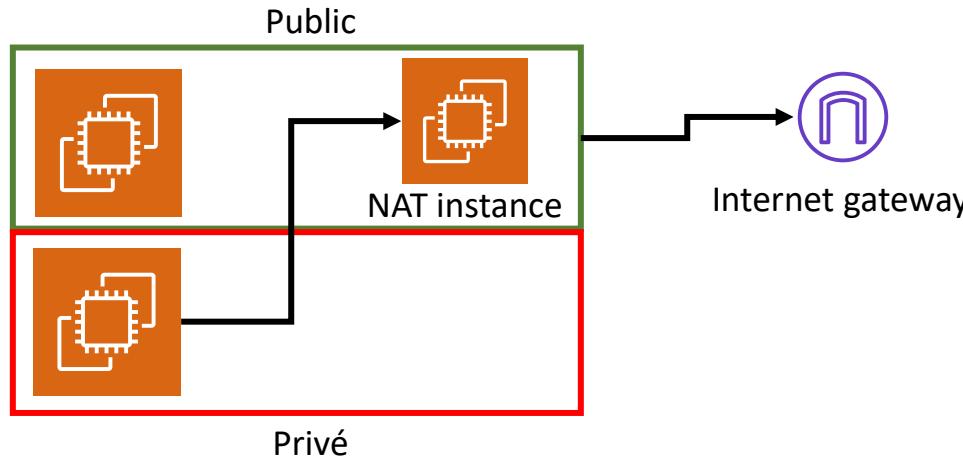
VPC et Cloud hybride





NAT instances (Network Adress Translation)

- Obtention de l'ID d'une AMI NAT
- Mise à jour de votre instance NAT existante
- Configuration de l'instance NAT
- Création du groupe de sécurité NATSG
- Désactivation des contrôles de source/destination
- Mise à jour de la table de routage principale
- Test de la configuration de votre instance NAT

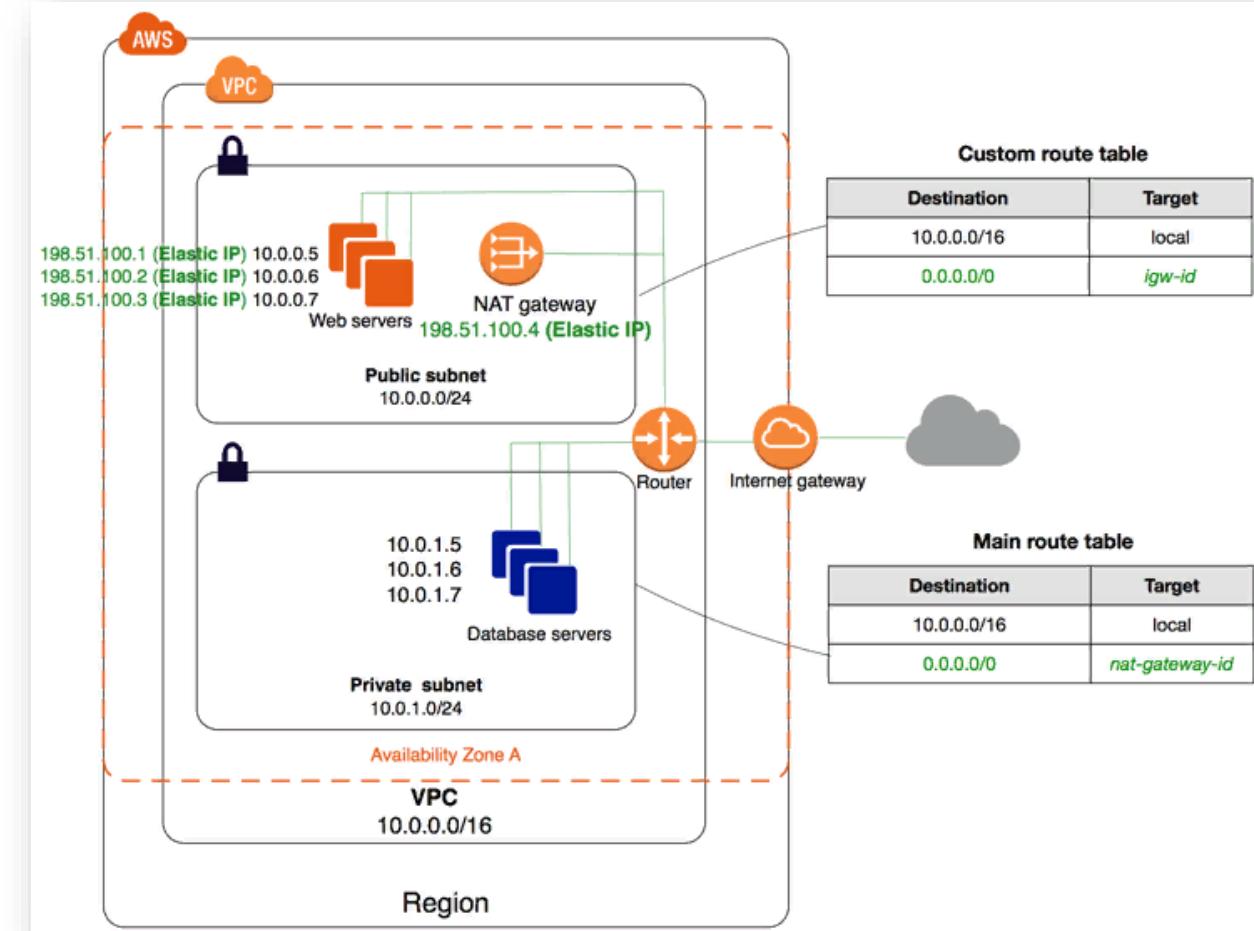
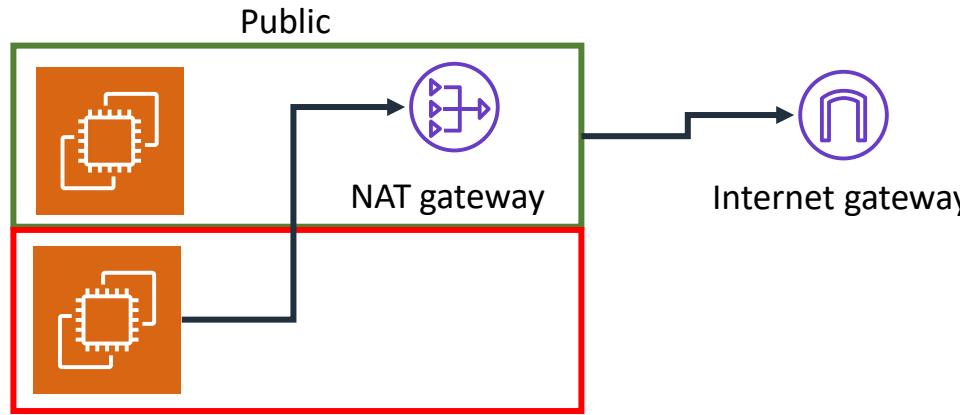


- AMI « amzn-ami-vpc-nat »
- Le transfert IPv4 est activé et les redirections ICMP sont désactivées dans /etc/sysctl.d/10-nat-settings.conf
- Un script situé à /usr/sbin/configure-pat.sh s'exécute au startup et configure les masques d'adresses IP iptables.
- **Mise à jour des instances NAT existantes « yum update –security »**



NAT Gateway

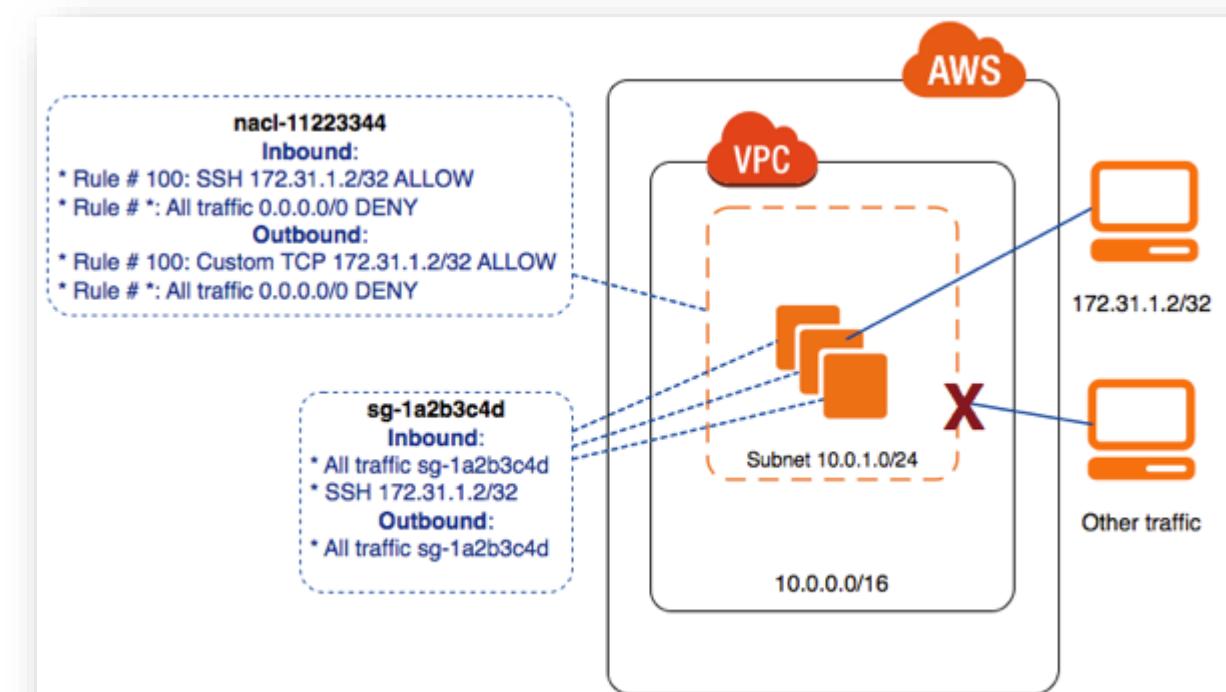
- Crédation d'une passerelle NAT
- Mise à jour de votre table de routage
- Test d'une passerelle NAT
- Test de la connexion Internet



- Une passerelle NAT prend en charge jusqu'à 5 Gb/s de bande passante et est mise à l'échelle jusqu'à 45 Gb/s. protocoles : TCP, UDP et ICMP.
- Vous pouvez utiliser une liste ACL réseau pour contrôler le trafic entrant et sortant du sous-réseau dans lequel la passerelle NAT est située.
- La liste ACL réseau s'applique au trafic de la passerelle NAT et utilise les ports dynamique de 1024–65535.
- Tolérant aux pannes géré par AWS (entreprise standard)
- Fonctionne dans une zone de disponibilité, favorisez la création d'une NAT Gateway par AZ
- Pas d'association au groupes de sécurité (Un groupe de sécurité est appliqué à une ENI)
- Affectation automatique d'une adresse ip publique
- Pas de désactivation de la fonction source destination checks (car c'est un service géré par aws)

Network Access Control List (NACL) - liste de contrôle d'accès réseau

- Votre VPC est automatiquement associé à une liste ACL réseau par défaut, que vous pouvez modifier. Par défaut, il autorise tout le trafic IPv4 entrant et sortant, ainsi que le trafic IPv6, le cas échéant.
- Vous pouvez créer une liste ACL réseau personnalisée et l'associer à un sous-réseau. Par défaut, chaque liste ACL réseau personnalisée refuse tout trafic entrant et sortant jusqu'à ce que vous ajoutiez des règles.
- Chaque sous-réseau de votre VPC doit être associé à une liste ACL réseau. Si vous n'associez pas explicitement un sous-réseau à une liste ACL réseau, le sous-réseau est automatiquement associé à la liste ACL réseau par défaut.
- Vous pouvez associer une liste ACL réseau à plusieurs sous-réseaux. Cependant, un sous-réseau ne peut être associé qu'à une seule liste ACL réseau à la fois. Lorsque vous associez une liste ACL réseau à un sous-réseau, l'association antérieure est supprimée.
- Une liste de contrôle d'accès réseau contient une liste numérotée de règles. Une liste ACL réseau est une liste numérotée de règles que nous évaluons dans l'ordre, en commençant par le numéro le plus bas.
- Le numéro le plus élevé que vous pouvez utiliser pour une règle est le 32 766. Lorsque vous créez des règles, nous vous recommandons de commencer par des incrémentations (par exemple, des incrémentations de 10 ou 100)



Liste ACL réseau par défaut

Entrant					
Règle n°	Type	Protocole	Plage de ports	Source	Autoriser/Refuser
100	Tout le trafic IPv4	Tous	Tous	0.0.0.0/0	AUTORISER
*	Tout le trafic IPv4	Tous	Tous	0.0.0.0/0	REFUSER
Sortant					
Règle n°	Type	Protocole	Plage de ports	Destination	Autoriser/Refuser
100	Tout le trafic IPv4	Tous	Tous	0.0.0.0/0	AUTORISER
*	Tout le trafic IPv4	Tous	Tous	0.0.0.0/0	REFUSER



Ports éphémères

Network ACLs are stateless

Un port éphémère est un port de protocole de transport de courte durée pour les communications par protocole Internet (IP). (TCP-UDP-SCTP cf. IANA The Internet Assigned Numbers Authority)

Le client qui initie la demande choisit la plage de ports éphémères, qui varie en fonction de son système d'exploitation.

- De nombreux noyaux Linux (y compris le noyau Amazon Linux) utilisent les ports 32768-61000.
- Les demandes provenant d'Elastic Load Balancing utilisent les ports 1024-65535.
- Les systèmes d'exploitation Windows exécutant Windows Server 2003 utilisent les ports 1025-5000.
- Windows Server 2008 et les versions ultérieures utilisent les ports 49152-65535.
- Une passerelle NAT utilise les ports 1024-65535.
- Les fonctions AWS Lambda utilisent les ports 1024-65535.

Sortant					
Règle n°	Type	Protocole	Plage de ports	Destination	Autoriser/Refuser
100	HTTP	TCP	80	0.0.0.0/0	AUTORISER
110	HTTPS	TCP	443	0.0.0.0/0	AUTORISER
120	TCP personnalisé	TCP	32768/65535	0.0.0.0/0	AUTORISER
*	Tout le trafic	Tous	Tous	0.0.0.0/0	REFUSER

Entrant					
Règle n°	Type	Protocole	Plage de ports	Source	Autoriser/Refuser
100	HTTP	TCP	80	0.0.0.0/0	AUTORISER
110	HTTPS	TCP	443	0.0.0.0/0	AUTORISER
120	SSH	TCP	22	192.0.2.0/24	AUTORISER
130	RDP	TCP	3389	192.0.2.0/24	AUTORISER
140	TCP personnalisé	TCP	32768/65535	0.0.0.0/0	AUTORISER
*	Tout le trafic	Tous	Tous	0.0.0.0/0	REFUSER

Les listes ACL réseau sont sans état, les réponses au trafic entrant autorisé sont soumises aux règles du trafic sortant (et vice versa).



VPC Flow logs (Jun 10, 2015)

La fonctionnalité de journaux de flux VPC vous permet de capturer des informations sur le trafic IP circulant vers et depuis les interfaces réseau dans votre VPC. (VPC, sous réseau, interfaces réseaux)

Les journaux de flux peuvent vous aider pour de nombreuses tâches :

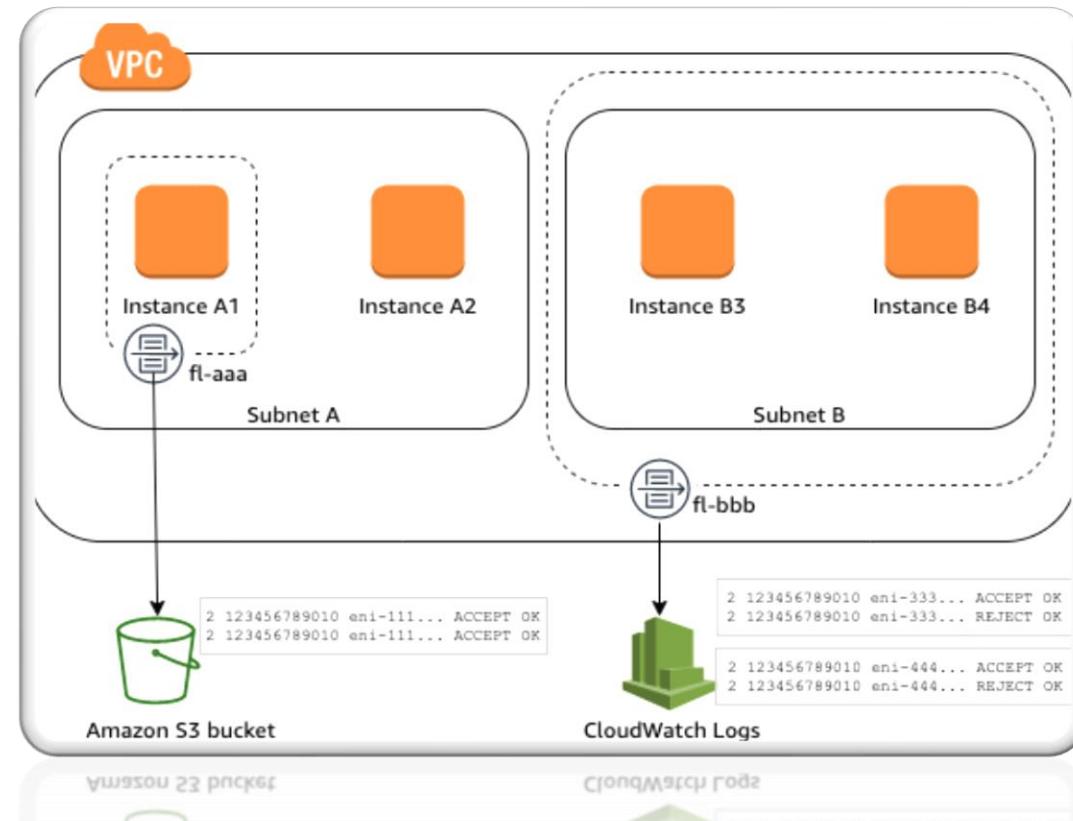
- Diagnostiquer les règles de groupe de sécurité trop restrictives
- Surveiller le trafic qui accède à votre instance
- Déterminer la direction du trafic vers et depuis les interfaces réseau

Les types de trafic suivants ne sont pas consignés :

- Le trafic généré par des instances lorsqu'elles contactent le serveur DNS Amazon. Si vous utilisez votre propre serveur DNS, tout le trafic vers ce dernier est consigné.
- Le trafic généré par une instance Windows pour l'activation de la licence Windows d'Amazon.
- Le trafic depuis et vers 169.254.169.254 pour les métadonnées de l'instance.
- Le trafic depuis et vers 169.254.169.123 pour Amazon Time Sync Service.
- Le trafic DHCP.
- Le trafic vers l'adresse IP réservée pour le routeur VPC par défaut.
- Le trafic entre un point de terminaison d'interface et une interface réseau ÉquilibrEUR de charge du réseau.

VPC flow logs Tarification :

- Des frais d'ingestion de données s'appliquent lorsque vous utilisez des journaux de flux. Des frais pour les journaux de flux sont facturés lorsque vous publiez des journaux de flux vers CloudWatch Logs.
- Des frais de remise des journaux à Amazon S3 s'appliquent lorsque vous publiez des journaux de flux vers Amazon S3.
- Utilisez des balises pour simplifier le filtrage des logs





Instance Bastion (bastion host)

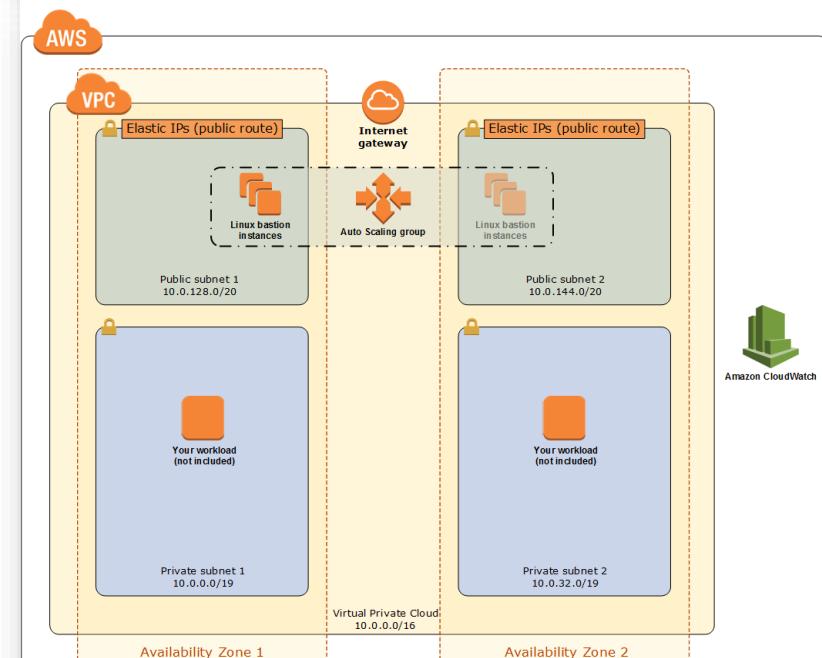
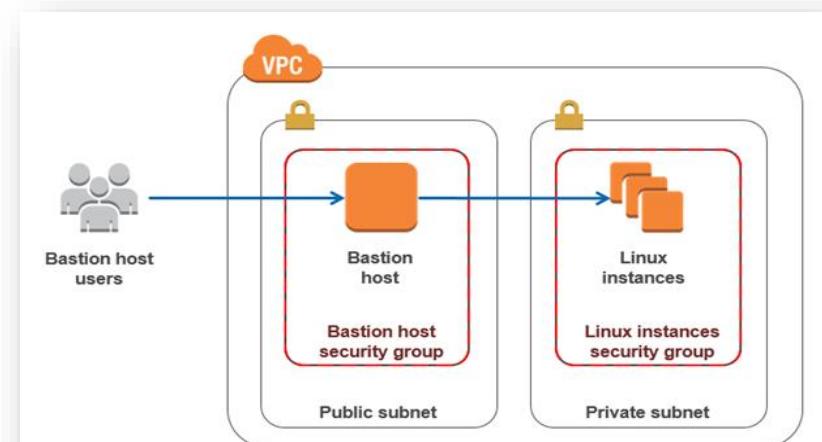
Un serveur bastion a pour but est de fournir un accès à un réseau privé à partir d'un réseau externe, ou depuis internet.

Un serveur bastion, vous aide pour :

- Réduire la surface d'attaque de votre réseau
- Permet les connexions via SSH ou RDP
- Enregistrer les connexions (effectuer des audits)
- Connecter vos instances via VPC peering

Un serveur bastion, les bonnes pratiques :

- Les hôtes du bastion Linux sont déployés dans deux zones de disponibilité pour permettre un accès immédiat à l'ensemble du VPC.
- Un groupe de mise à l'échelle automatique.
- Les hôtes bastion sont déployés dans les sous-réseaux publics (DMZ) du VPC.
- Des adresses IP élastiques sont associées aux instances du bastion.
- L'accès aux hôtes du bastion est verrouillé aux CIDR connus (votre réseau)
- Les ports sont limités pour ne permettre que l'accès nécessaire aux hôtes du bastion. port TCP 22 ou 3389.
- L'accès : table de routage > Acl réseau > groupes de sécurité > Bastion > instances
- Bastion = Jump box = serveur de rebond



AWS VPN

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

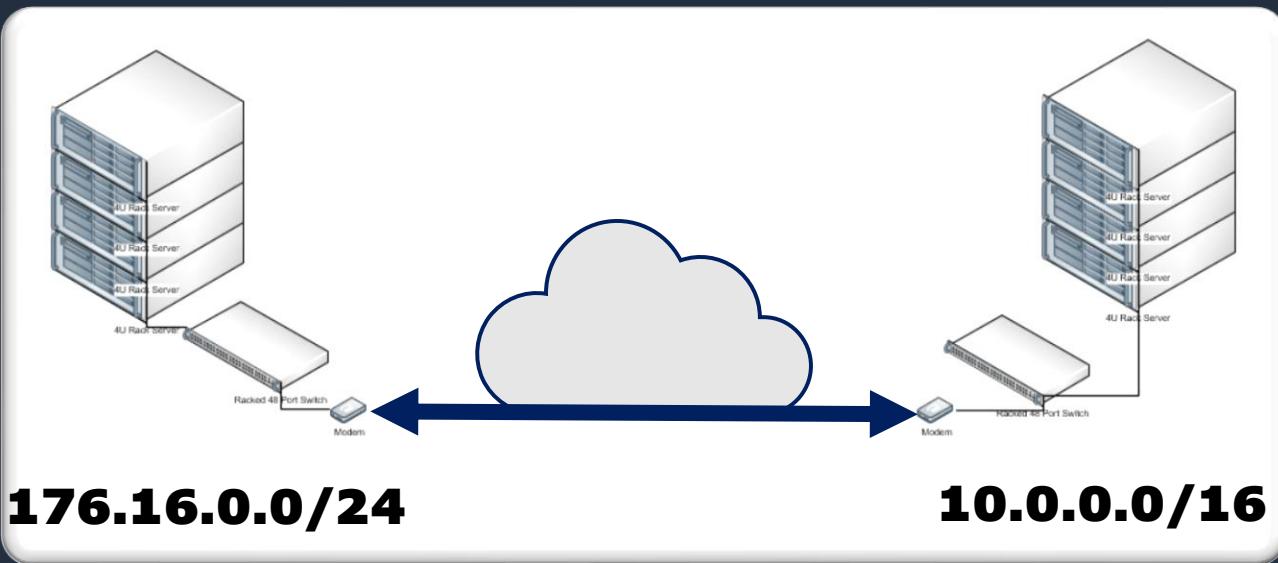
Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>



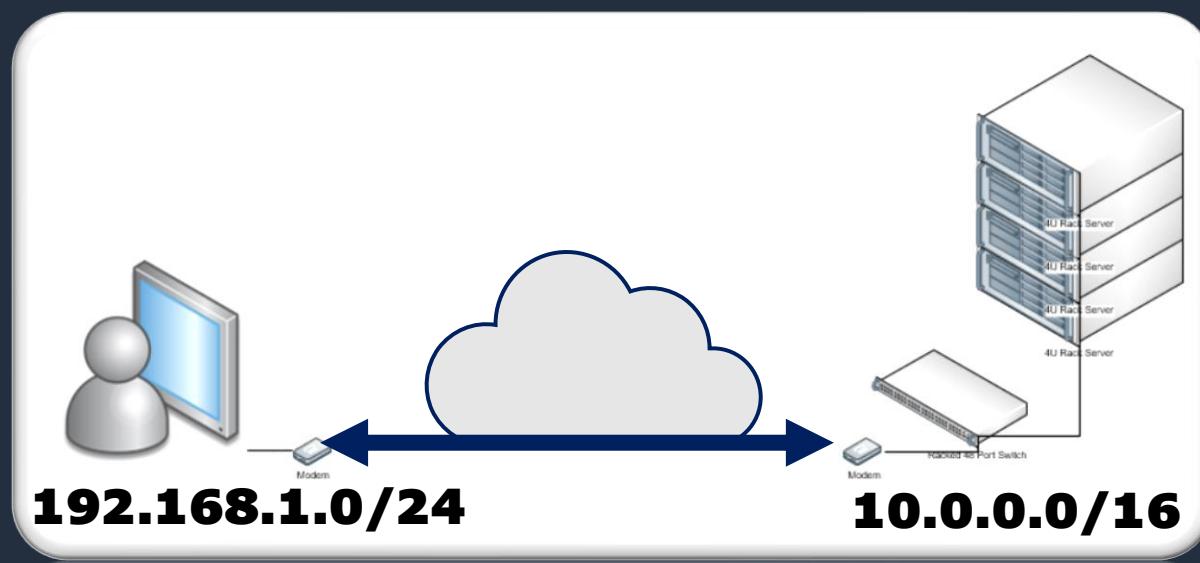
AWS Virtual Private Network

Permet d'établir une liaison sécurisée via un tunnel privé depuis un réseau d'entreprise avec le réseau global AWS

AWS Site-to-Site VPN

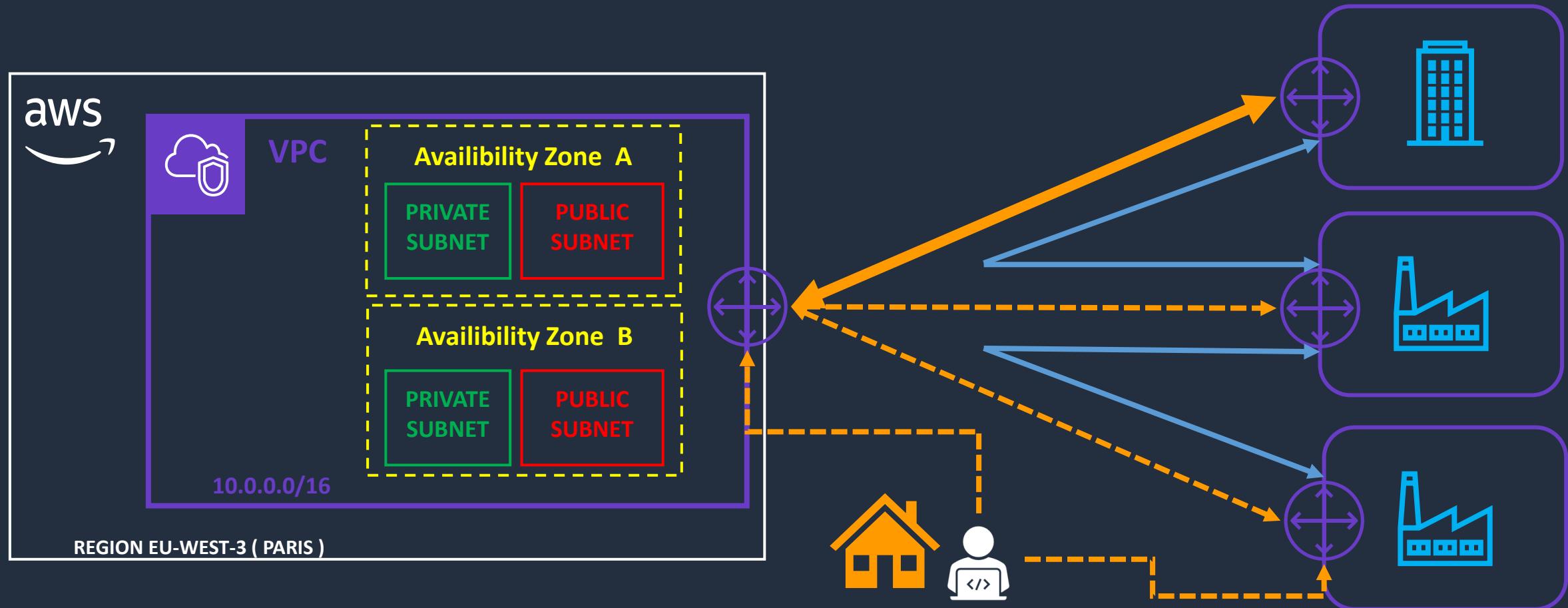


AWS Client VPN





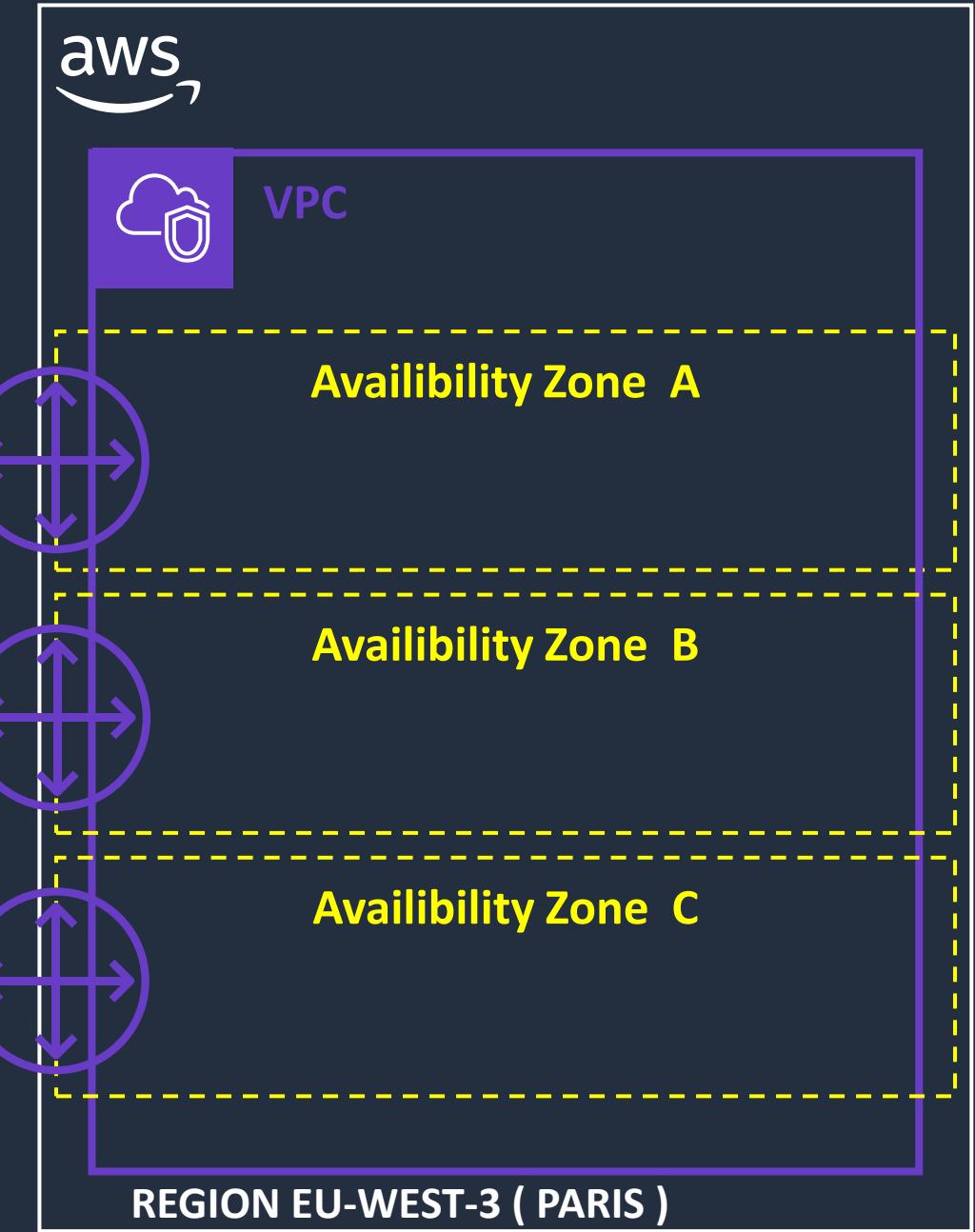
AWS Site-to-Site Vs AWS Client VPN





Fonctionnalités

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

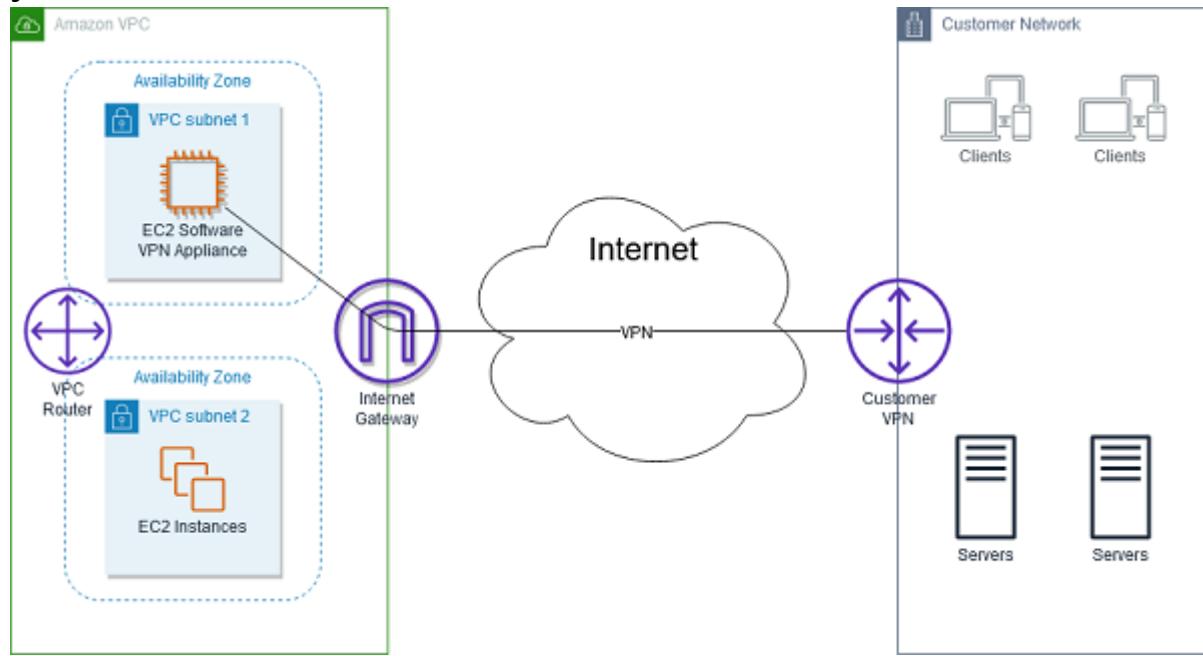




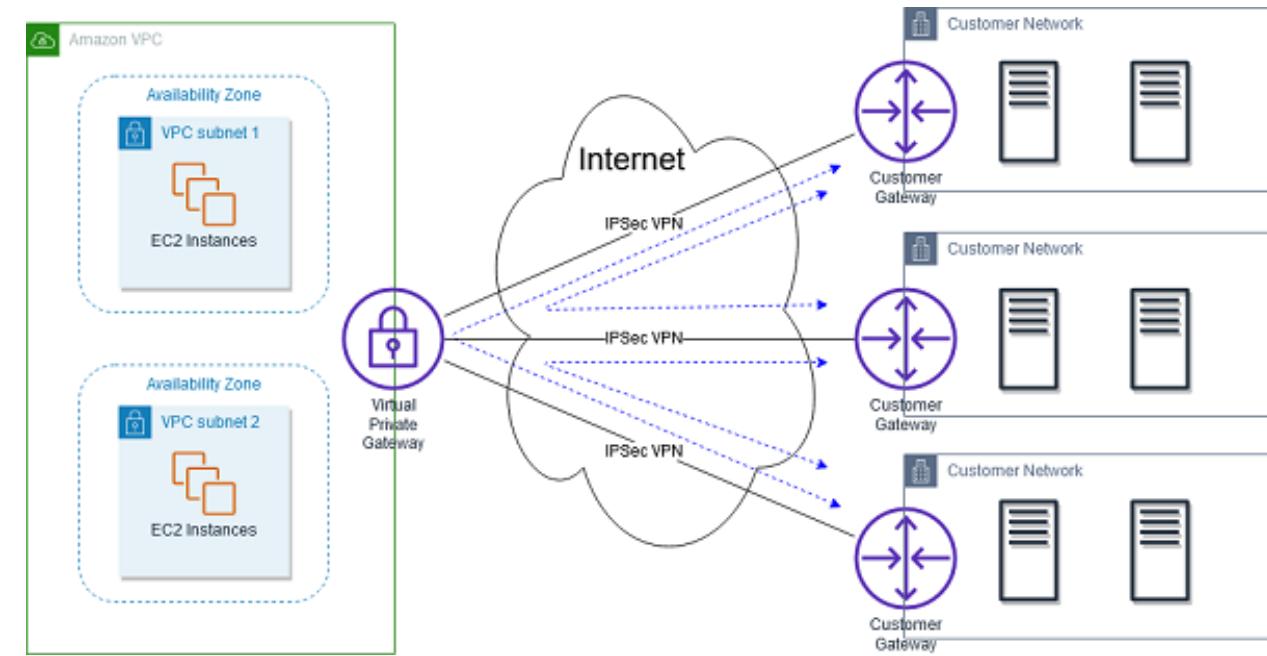
VPN Cloud HUB

Si vous avez plusieurs connexions AWS Site-to-Site VPN, vous pouvez assurer une communication sécurisée entre les sites à l'aide de l'AWS VPN CloudHub.

VPN de site à site : Vous pouvez choisir parmi un écosystème de partenaires multiples et de communautés open source qui ont produit des logiciels VPN qui fonctionnent sur Amazon EC2. Ce choix s'accompagne de la responsabilité de gérer l'Appliance logicielle, y compris la configuration, les correctifs et les mises à jour.



AWS VPN CloudHub utilise une passerelle privée virtuelle Amazon VPC avec plusieurs passerelles clients, chacune utilisant des numéros de système autonome (ASN) BGP uniques.



AWS Direct Connect

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>



Direct Connect

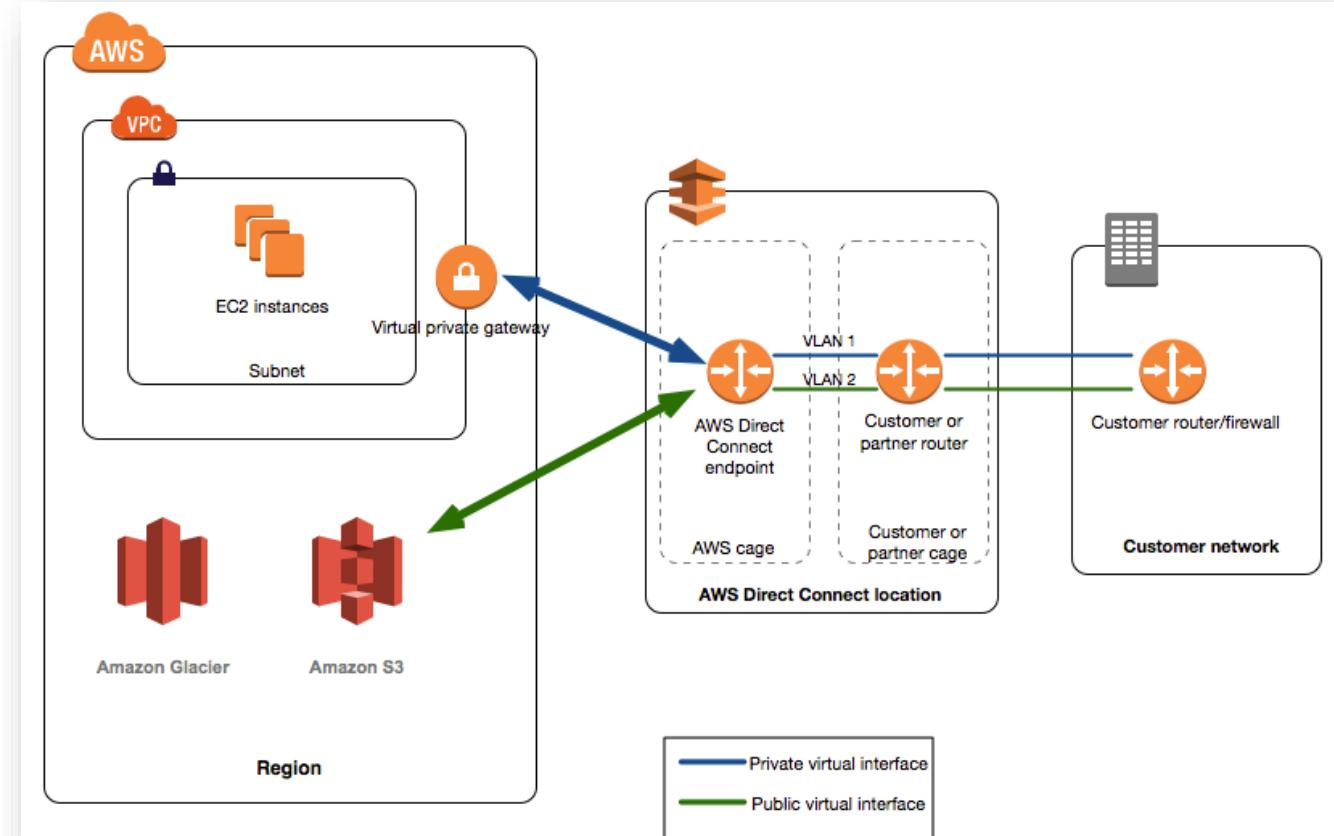
AWS Direct Connect relie votre réseau interne à un emplacement AWS Direct Connect via une fibre optique.

- Une extrémité du câble est raccordée à votre routeur et l'autre à un routeur AWS Direct Connect.
- fibre optique monomode, avec émetteur-récepteur 1000BASE-LX
- La négociation automatique pour le port doit être désactivée
- L'encapsulation VLAN 802.1Q doit être prise en charge
- Votre appareil doit prendre en charge BGP (Border Gateway Protocol) et l'authentification MD5 BGP
- Vous pouvez aussi configurer la détection de transmission bidirectionnelle (BFD) sur votre réseau
- Pour les connexions hébergées, les valeurs possibles sont de 50 Mb/s, 100 Mb/s, 200 Mb/s, 300 Mb/s, 400 Mb/s et 500 Mb/s, 1 Gb/s, 2 Gb/s, 5 Gb/s et 10 Gb/s.

AWS Direct Connect connections (plusieurs semaines)

Connexion dédiée : Une connexion Ethernet physique associée à un seul client. Les clients peuvent demander une connexion dédiée AWS Direct Connect, le CLI ou l'API. (1 à 10 Gbps) contacter AWS en premier lieu puis un partenaire de votre choix (Equinix Intercloud Interxion Colt). Non modifiable.

Connexion hébergée : Une connexion Ethernet physique qu'un Partenaire AWS Direct Connect fournit au nom d'un client. Les clients demandent une connexion hébergée en contactant un partenaire des Programmes partenaires AWS Direct Connect, qui fournit la connexion. 50 Mb/s, 100 Mb/s, 200 Mb/s, 300 Mb/s, 400 Mb/s et 500 Mb/s, 1 Gb/s, 2 Gb/s, 5 Gb/s et 10 Gb/s. Modification de l'offre sur demande.





Direct connect Gateway

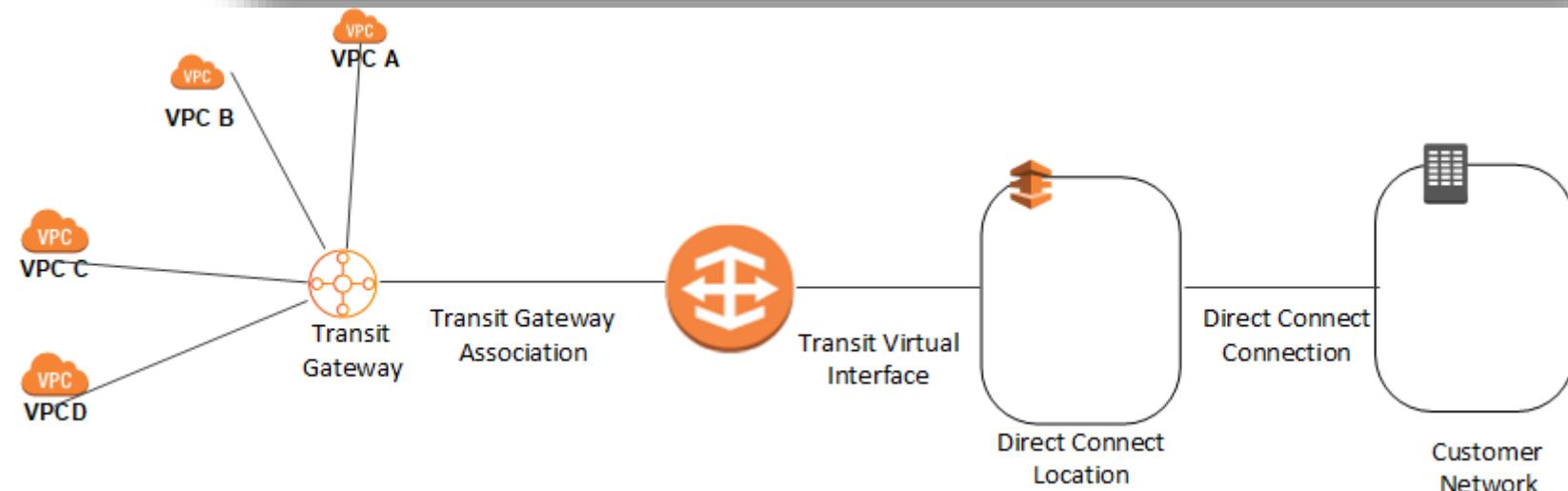
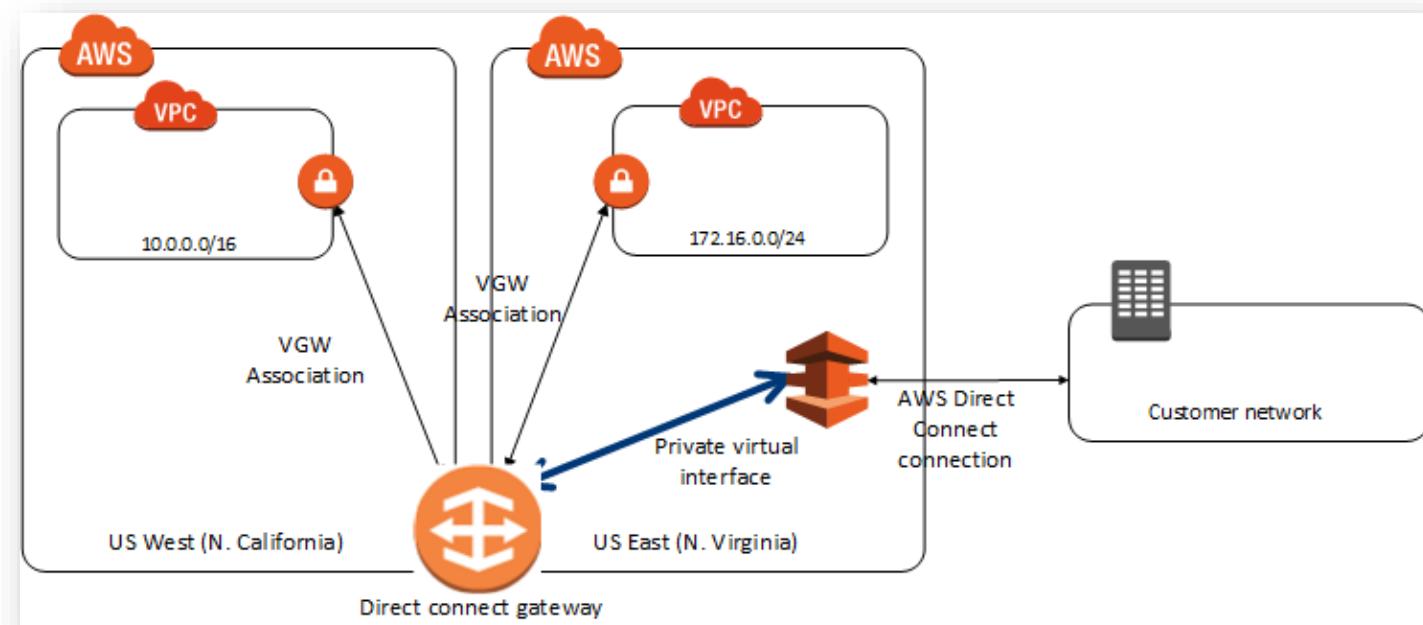
Utilisé AWS Direct Connect gateway pour connecter vos vpcs.

Vous associez une passerelle AWS Direct Connect à l'une des passerelles suivantes :

- Une passerelle privée virtuelle (VPG)
- Une passerelle de transit (transit gateway) si vous avez plusieurs VPC dans la même région

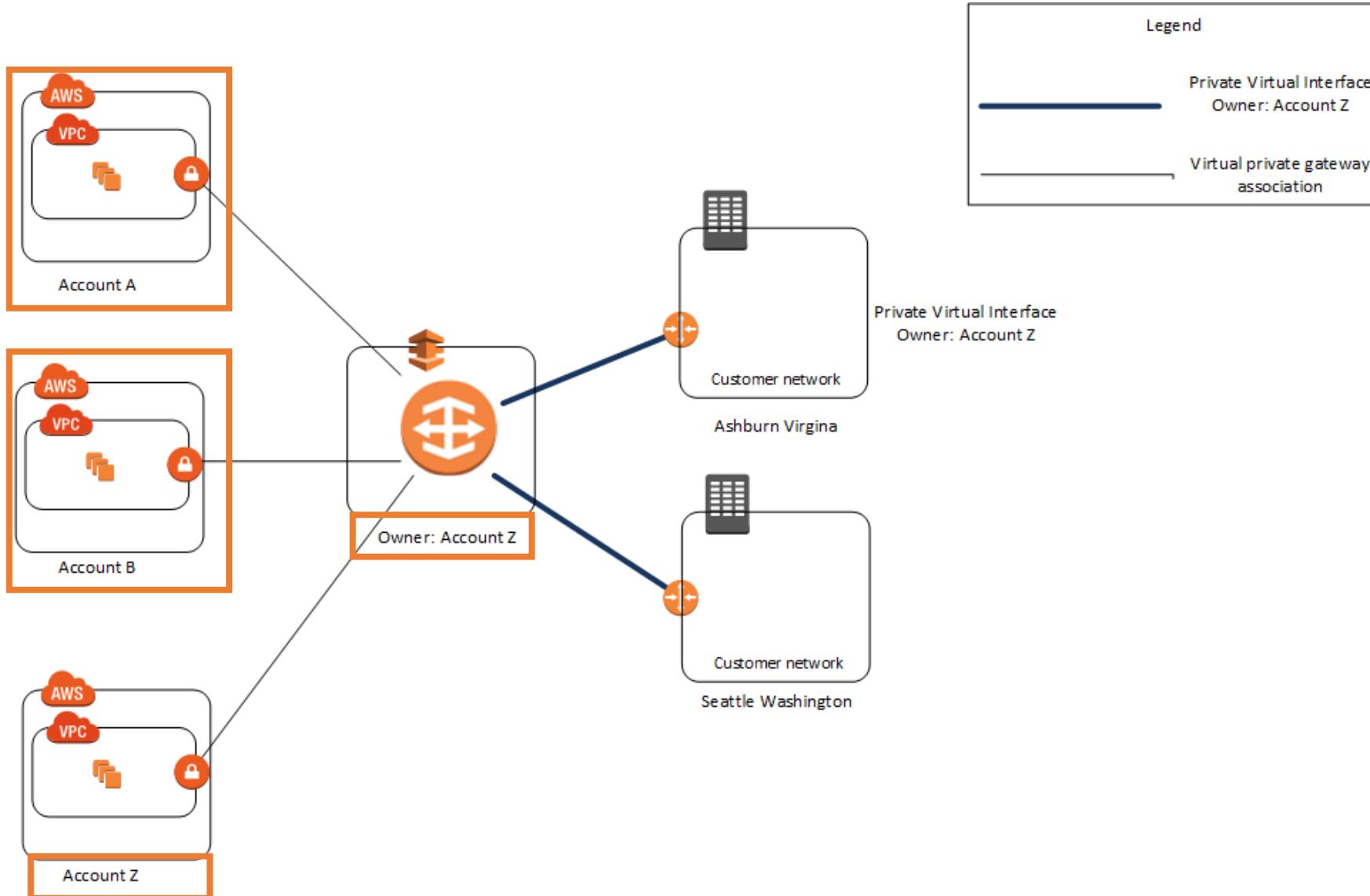
Transit gateway

- Des politiques de routage centralisées dans les VPC et sur place
- « Scale » pour soutenir des milliers de VPC sur plusieurs comptes clients
- Des règles de segmentation et routage plus souples
- Scale out (horizontale)
- Augmenter le débit de la connectivité grâce à des connexions VPN multiples
- Une gestion simplifiée





Virtual private gateway associations across accounts



AWS Global Accelerator

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

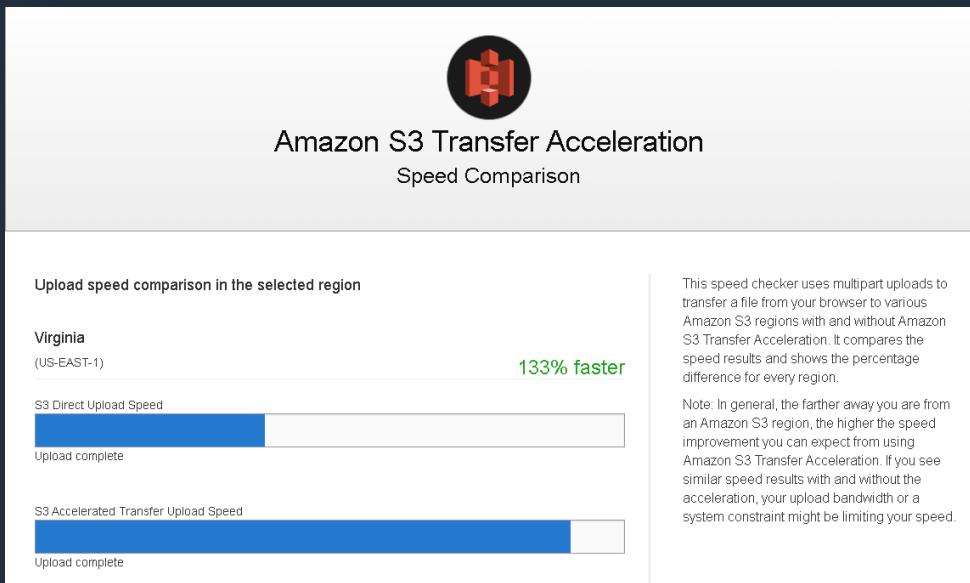
Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

AWS Global Accelerator

Un service qui améliore la disponibilité et les performances de vos applications auprès des utilisateurs locaux ou internationaux.

- 2 Adresses IP anycast statiques (deux réseaux distincts)
- Tolérance aux pannes à l'aide des zones de réseau
- Routage global selon les performances (up to 60%)
- Ne met pas en cache les données (!= cloudfront)
- Protège contre les attaques 1vsN DDoS
- Bring Your Own IP (BYOIP)
- Amazon S3 Transfer Acceleration



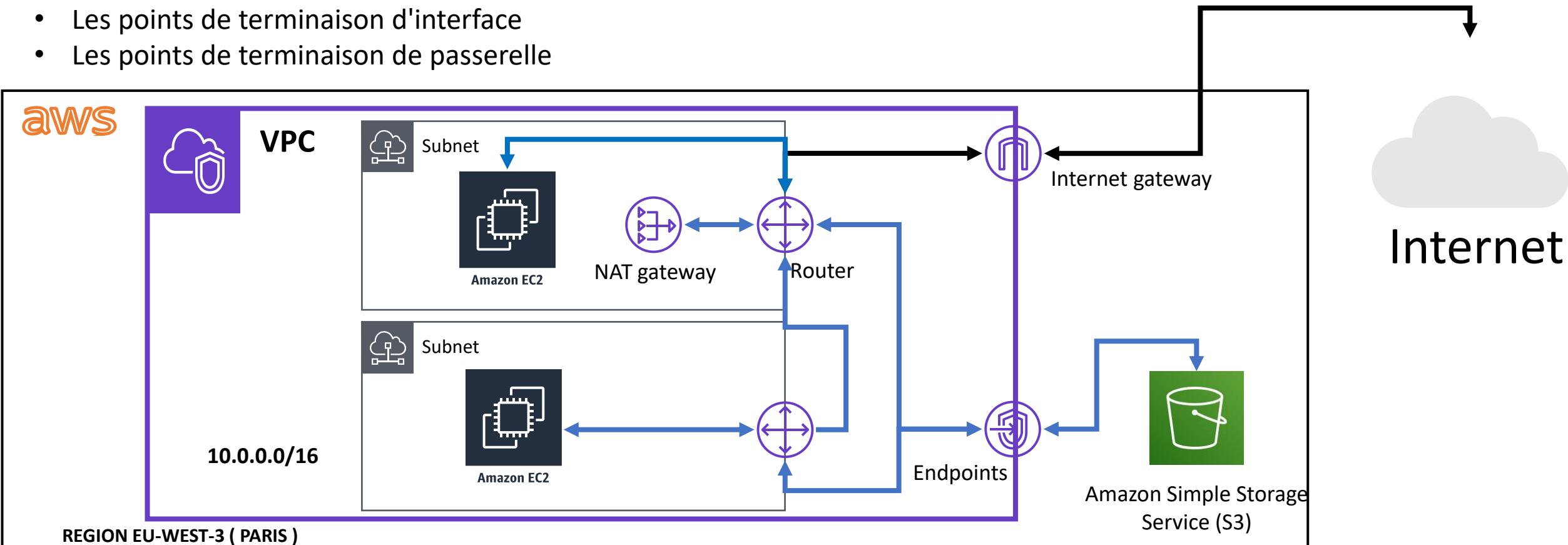
- <http://s3-accelerate-speedtest.s3-accelerate.amazonaws.com/en/accelerate-speed-comparsion.html>



Points de terminaison d'un VPC (VPC Endpoint)

Un Point de terminaison d'un VPC permet une connexion privée entre votre VPC et les services AWS pris en charge ou les services de point de terminaison de VPC alimentés par AWS PrivateLink sans nécessiter une passerelle Internet, un périphérique NAT ou une connexion VPN ou une connexion AWS Direct Connect.

- Interface réseau interne avec ip privée (ENI)
- composants VPC mis à l'échelle horizontalement, redondants et hautement disponibles.
- Les points de terminaison d'interface et les points de terminaison de passerelle.
- Les points de terminaison d'interface
- Les points de terminaison de passerelle





VPC Peering (appairage VPC)

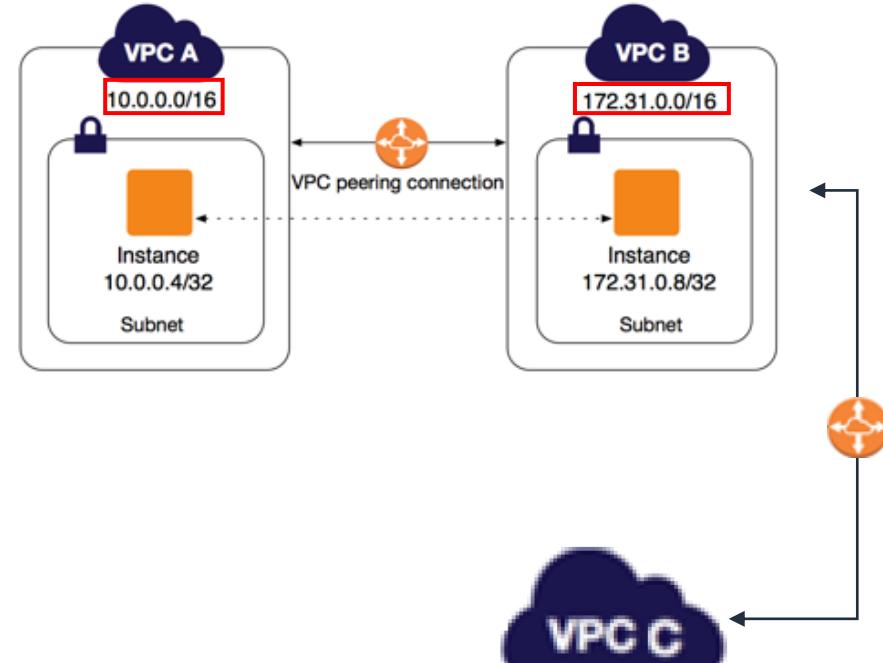
Overlapping CIDR



Une connexion d'appairage de VPC est une connexion de mise en réseau entre deux VPC qui permet d'acheminer le trafic entre ces derniers à l'aide d'adresses IPv4 privées ou d'adresses IPv6.

- Les instances des deux VPC peuvent communiquer entre elles comme si elles se trouvaient dans le même réseau.
- Faire un appairage de VPC entre vos propres VPC, ou avec un VPC situé dans un autre compte AWS.
- Les VPC peuvent se trouver dans différentes régions (aussi appelé connexion d'appairage de VPC inter-région).
- Vous pouvez sécuriser vos accès via les groupes de sécurité d'un VPC appairé (explicitement, directement)
- Les appairages ne sont pas transitifs. (chaque VPC doit avoir sa connexion d'appairage vers chaque autre VPC)
- **Si VPC-A est appairé à VPC-B et VPC-B appairé à VPC-C alors VPC-A ne voit pas VPC-C !**
- Un appairage nécessite la mise à jour des tables de routages des sous réseaux que vous souhaitez faire communiquer.

1. Le propriétaire du VPC **demandeur** envoie une demande au propriétaire du VPC **accepteur** pour créer une connexion d'appairage de VPC.
2. Le propriétaire du VPC accepteur accepte la demande de connexion d'appairage de VPC pour activer cette connexion.
3. Pour activer le flux du trafic entre les VPC à l'aide d'adresses IP privées, le propriétaire de chaque VPC de la connexion d'appairage de VPC doit manuellement ajouter un itinéraire vers une ou plusieurs des tables de routage de son VPC
4. Par défaut, si des instances sur l'un des côtés d'une connexion d'appairage de VPC s'adressent à l'autre côté à l'aide d'un nom d'hôte DNS public, le nom d'hôte est résolu en l'adresse IP publique de l'instance.





AWS PrivateLink

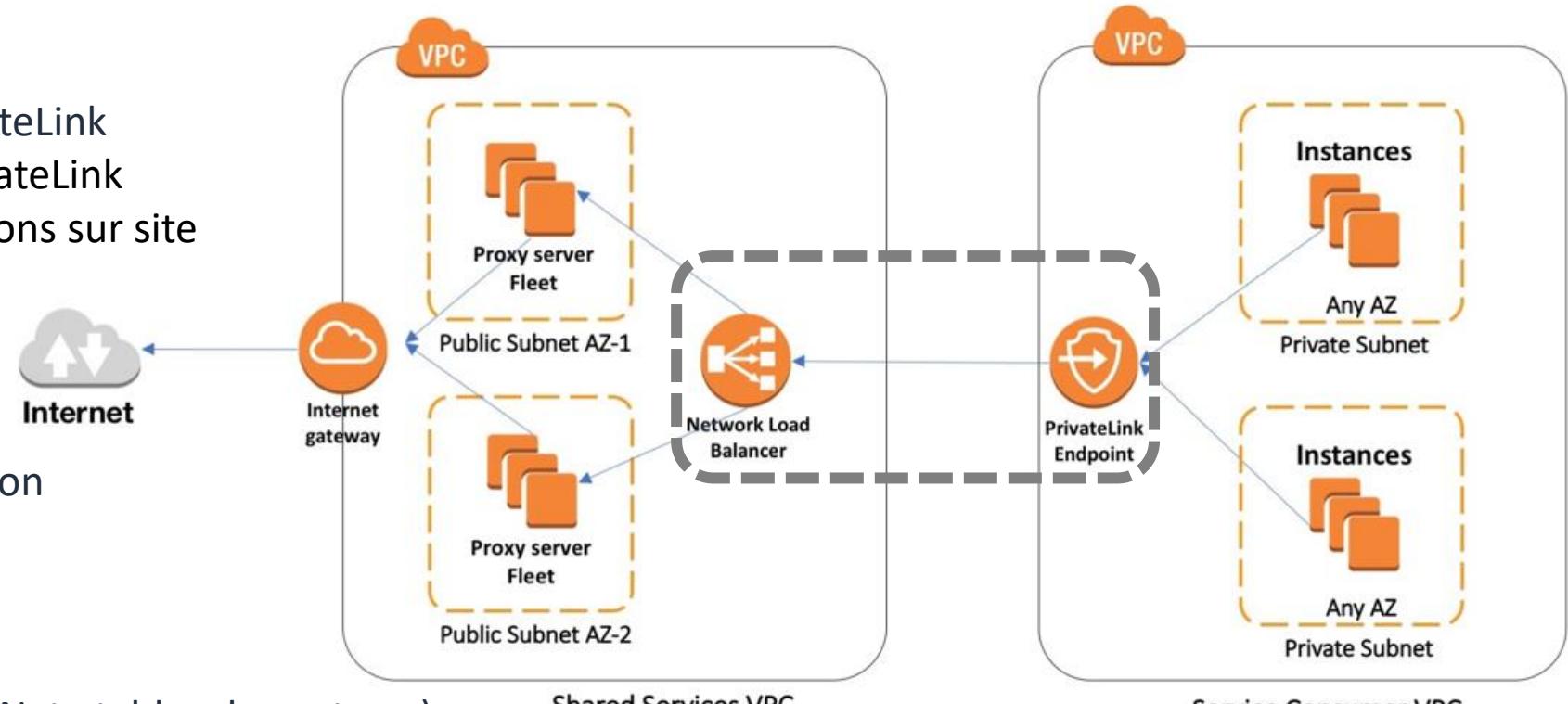
Simplifie la sécurité des données partagées avec les applications cloud en éliminant l'exposition des données à l'Internet public.

Fonctionnalités :

- Accès aux services via AWS PrivateLink
- Partage de services via AWS PrivateLink
- Connexion privée à vos applications sur site
- Intégration à AWS Marketplace

Configuration :

- Création d'un NLB
- Création d'un point de terminaison
- Liaison PrivateLink



Avantages :

- Aucun Peering requis (Gateway, Nat , tables de routage)
- Moins de gestion d'infrastructures (administration)
- Plus de publication sur internet (augmente la sécurité)
- Accès sécurisé et hautement disponible aux applications
- Connexion de centaines ou milliers de VPC (plusieurs comptes)

Tarification par point de terminaison de VPC par zone de disponibilité (USD/heure) = 0,01\$

Tarification par Go de données traitées (USD) = 0,01\$

Amazon Route 53

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>



Route53



mondomainepro.com



amazon.com

=

205.251.242.103



Amazon Route 53 est un service Web de système de noms de domaine (DNS) dans le cloud hautement disponible et évolutif. Il sert principalement à traduire des nom de domaine comme amazon.com par des adresse IP de type 205,251,242,103 que les ordinateurs utilisent pour se connecter les uns aux autres. Il dispose aussi de la capacité de surveiller l'état de santé des destinations et d'alerter en cas de défaillance.

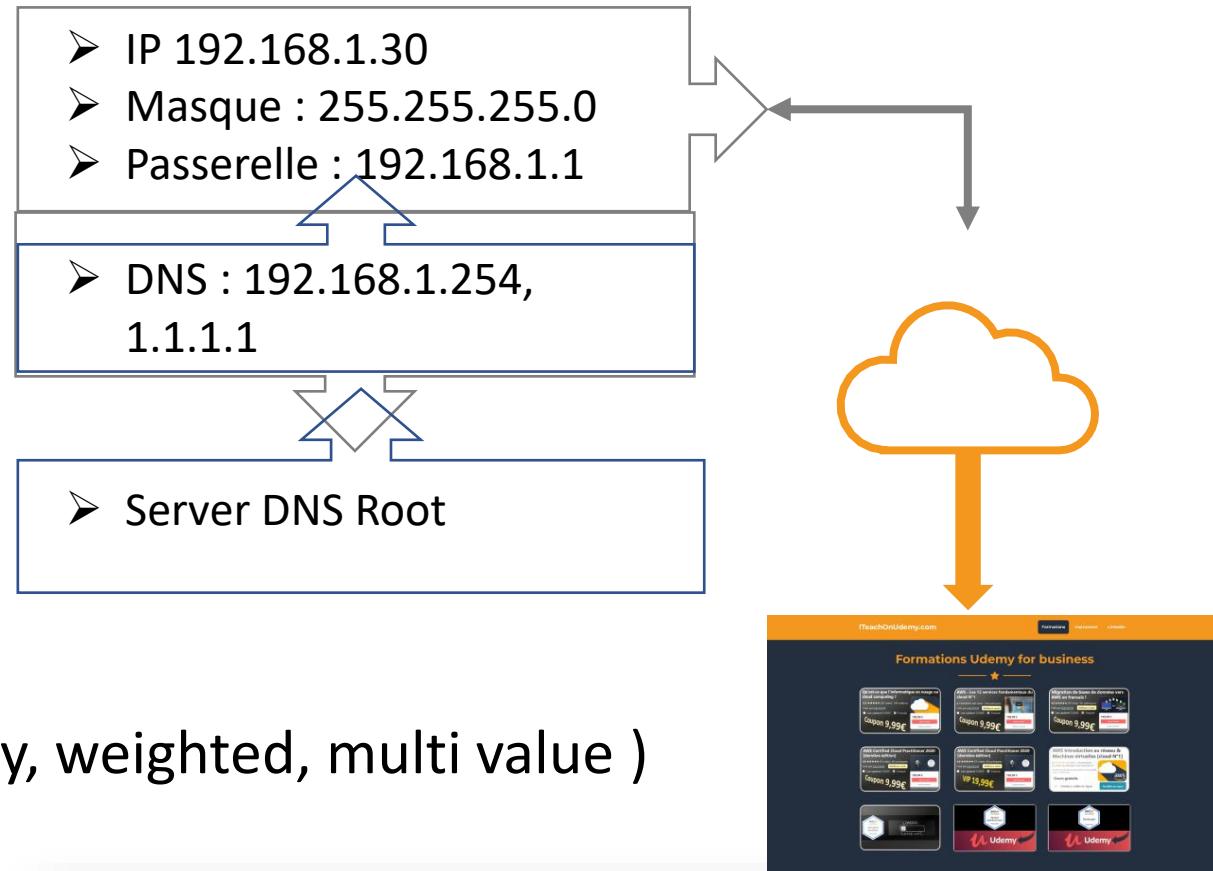


Route53 - Enregistrements

Acheminer les utilisateurs finaux vers des applications en traduisant des noms comme www.example.com par des adresses IP de type 192.0.2.1

Enregistrements :

- A : URL vers adresse IPV4
- AAAA : URL vers adresse IPV6
- CNAME : URL vers URL
- Alias : URL vers une ressources AWS
- Tester la santé d'une URL
- Basculer (load balancing)
- Routage (simple, failover, geolocation, latency, weighted, multi value)
- Hébergement de domaine



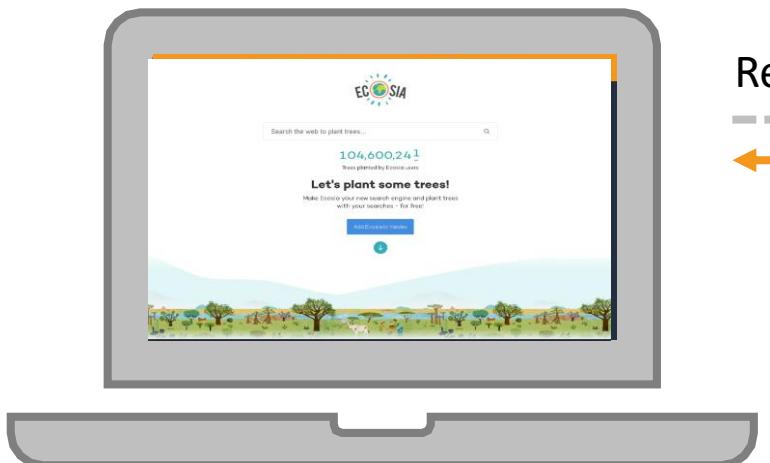
```
Adresse IPv4. . . . . : 192.168.1.30(préféré)
Masque de sous-réseau. . . . . : 255.255.255.0
Bail obtenu. . . . . : jeudi 20 août 2020 08:18:20
Bail expirant. . . . . : jeudi 20 août 2020 22:43:26
Passerelle par défaut. . . . . : 192.168.1.254
Serveur DHCP . . . . . : 192.168.1.254
Serveurs DNS. . . . . : 192.168.1.254
1.1.1.1
```

```
Adresse IPv4. . . . . : 172.16.217.4(préféré)
Masque de sous-réseau. . . . . : 255.255.255.224
Bail obtenu. . . . . : jeudi 20 août 2020 10:46:22
Bail expirant. . . . . : vendredi 20 août 2021 10:46:22
Passerelle par défaut. . . . . : 172.16.217.1
Serveur DHCP . . . . . : 172.16.217.30
Serveurs DNS. . . . . : 185.156.173.165
185.156.173.166
```



TTL DNS (Time to live)

Le DNS utilise la mise en cache, ce qui réduit la charge sur les serveurs de noms faisant autorité. Cependant, les enregistrements peuvent être obsolètes. La durée de mise en cache d'un enregistrement dépend de sa valeur de temps de vie (TTL). Le TTL est un nombre qui est spécifié en secondes.



Requête DNS : iteachonudemy.com

Cache expiration = TTL

- 143.204.222.63
- 143.204.222.100
- 143.204.222.43
- 143.204.222.18

```
C:\Users\root>ping iteachonudemy.com
Envoi d'une requête 'ping' sur iteachonudemy.com [143.204.222.18] avec 32 octets de données
Réponse de 143.204.222.18 : octets=32 temps=5 ms TTL=245
Réponse de 143.204.222.18 : octets=32 temps=5 ms TTL=245
Réponse de 143.204.222.18 : octets=32 temps=5 ms TTL=245
Réponse de 143.204.222.18 : octets=32 temps=6 ms TTL=245
```

Réponse DNS :

- 143.204.222.63
- 143.204.222.100
- 143.204.222.43
- 143.204.222.18



```
C:\Users\root>nslookup -type=soa iteachonudemy.com
Serveur : UnKnown
Address: 192.168.1.254
```

Réponse ne faisant pas autorité :
iteachonudemy.com

```
primary name server = ns-513.awsdns-00.net
responsible mail addr = awsdns-hostmaster.amazon.com
serial = 1
refresh = 7200 (2 hours)
retry = 900 (15 mins)
expire = 1209600 (14 days)
default TTL = 86400 (1 day)
```

```
C:\Users\root>nslookup iteachonudemy.com
Serveur : UnKnown
Address: 192.168.1.254
```

Réponse ne faisant pas autorité :

```
Nom : iteachonudemy.com
Adresses: 143.204.222.63
          143.204.222.100
          143.204.222.43
          143.204.222.18
```



Utiliser Route 53 comme service DNS d'un domaine existant

Vous pouvez utiliser Amazon Route 53 en tant que service DNS pour votre domaine, par exemple, example.com.

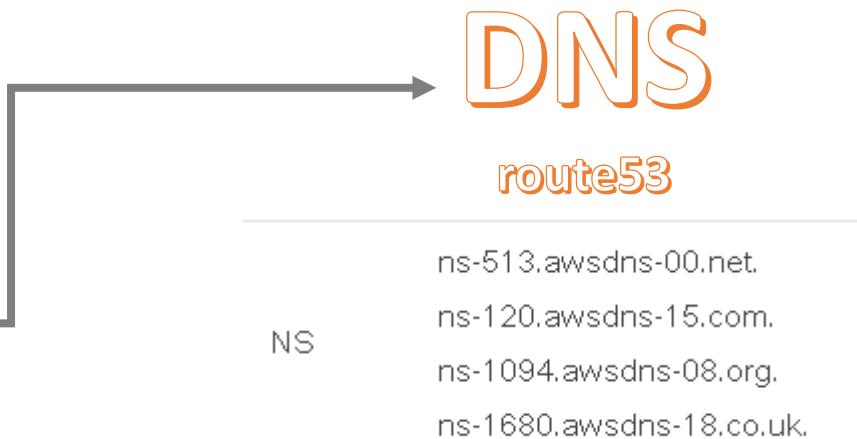
Lorsque Route 53 est votre service DNS, il achemine le trafic Internet vers votre site web en traduisant les noms de domaine descriptifs comme www.example.com en adresses IP de type 192.0.2.1, qui sont utilisées par les ordinateurs pour se connecter les uns aux autres.

Lorsque quelqu'un entre votre nom de domaine dans un navigateur ou vous envoie un e-mail, une requête DNS est envoyée à Route 53, qui répond avec la valeur appropriée. Par exemple, Route 53 peut répondre avec l'adresse IP du serveur web pour example.com.

- [Domain.com.](#)
- [GoDaddy.com.](#)
- [Namecheap.com.](#)
- [Domains. Google.](#)
- [Name.com.](#)
- [Bluehost.com.](#)
- [HostGator.com.](#)

Registrar

iteachonudemy.com.





Route53 et VPC

Votre VPC a des attributs qui déterminent si des instances lancées dans le VPC reçoivent des noms d'hôte DNS publics qui correspondent à leurs adresses IP publiques, et si la résolution DNS via le serveur DNS Amazon est prise en charge pour le VPC.

- **enableDnsHostnames** : Indique si des instances avec des adresses IP publiques ont des noms d'hôte DNS publics correspondants. Si cet attribut est true, les instances dans le VPC obtiennent des noms d'hôte DNS publics, mais seulement si l'attribut enableDnsSupport est défini sur true.
- **enableDnsSupport** : Indique si la résolution DNS est prise en charge. Si cet attribut est défini sur false, le serveur Amazon Route 53 Resolver qui résout les noms d'hôte DNS publics en adresses IP n'est pas activé. Si cet attribut est défini sur true, les requêtes envoyées au serveur DNS fourni par Amazon à l'adresse IP 169.254.169.253** aboutiront.

Par défaut, **les deux attributs sont définis sur true** dans un VPC par défaut ou un VPC créé par l'assistant VPC. Par défaut, **seul l'attribut enableDnsSupport est défini sur true** dans un VPC créé d'une autre manière.

- **Si les deux attributs sont définis sur true, les actions suivantes ont lieu :**
 - Les instances avec une adresse IP publique reçoivent les noms d'hôte DNS publics correspondants.
 - Le serveur Amazon Route 53 Resolver peut résoudre les noms d'hôtes DNS publics fournis par Amazon.

- **Si l'un de ces deux attributs ou les deux sont définis sur false, les actions suivantes ont lieu :**

Les instances avec une adresse IP publique ne reçoivent pas les noms d'hôte DNS publics correspondants.
Le Amazon Route 53 Resolver ne peut pas résoudre les noms d'hôtes DNS publics fournis par Amazon.

Analytics & bases de données





Bases de données relationnelles

Les bases de données relationnelles stockent des données avec des schémas prédéfinis qui communiquent entre eux. Elles sont conçues pour prendre en charge les transactions ACID, maintenir l'intégrité du référentiel et entretenir une forte cohérence des données.

Amazon Aurora

PostGreSQL - MySQL



Amazon RDS

PostgreSQL, MySQL, MariaDB,
Oracle ,MS SQL Server (OLTP)



scale a (relational database) in the cloud

Amazon Redshift

Data warehouse
(OLAP)

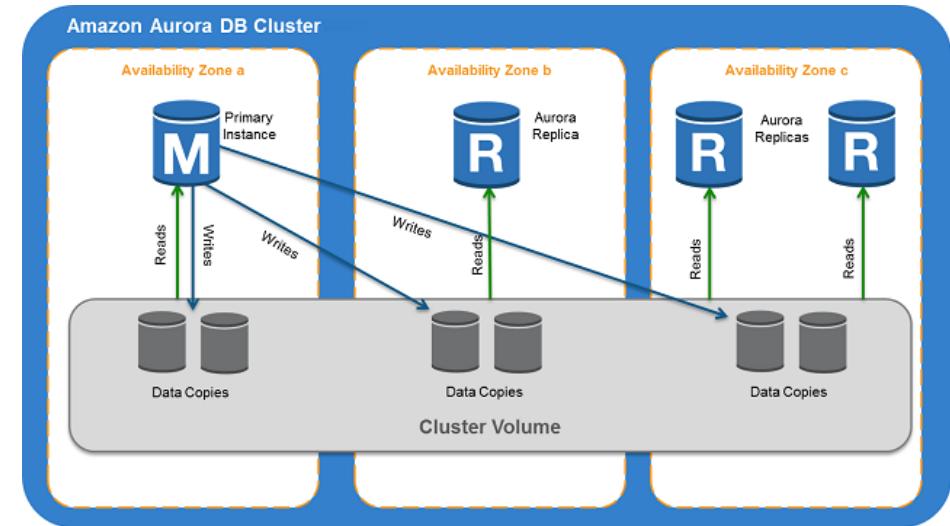




AMAZON Aurora & Aurora Serverless

Base de données relationnelle compatible avec MySQL et PostgreSQL créée pour le cloud, qui associe les performances et la disponibilité des bases de données d'entreprises traditionnelles à la simplicité et à la rentabilité des bases de données open source.

- Service géré via RDS mise en service, la configuration de bases de données, l'application de correctifs et les sauvegardes.
- jusqu'à 5 fois plus rapide que les bases de données MySQL et 3 fois plus rapide que les bases de données PostgreSQL
- Comprend un système de stockage distribué, flexible et auto-récupérant qui se redimensionne jusqu'à 64 To par instance
- Possibilité de déployer 15 répliques de lecture contre 5 seulement pour MySQL (réPLICATION est plus rapide)
- La bascule en cas d'échec est gérée automatiquement, Aurora est une solution hautement disponible.
- Données répliquées sur 3 « AZ » et dispose de 6 copies de vos données
- 1 Maître (primary) + jusqu'à 15 replicas en lecture (via autoscaling)
- haute disponibilité dans plusieurs régions AWS, vous pouvez configurer des bases de données Aurora globales. (région principale + jusqu'à 5 secondaires et jusqu'à 15+1 read replicas par region secondaires)
- Écritures sont réalisées sur le **Writer EndPoint**
- Lectures sont réalisées sur le **Reader Endpoint**
- Même services gérés que RDS : fail over automatique, sauvegarde et restauration, chiffrement KMS, haute disponibilité 'entreprise grade', autoscaling, gestion des OS, patchs management sans interruption, supervision avancée, Backtrack (10 MAY 2018)
- Aurora Serverless : Instanciation automatique de base de données



Rewinds the DB cluster to a previous point in time without creating a new DB cluster.

Earliest restorable time is May 7, 2018 at 1:03:22 PM UTC-7 (Local) ⓘ

Date	Time
May 7, 2018	16 : 25 : 18 UTC-7
25	25

Amazon Relational Database Service (RDS)

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>



RDS : Relational Database Service & DynamoDB



SQL = Base de données relationnelles

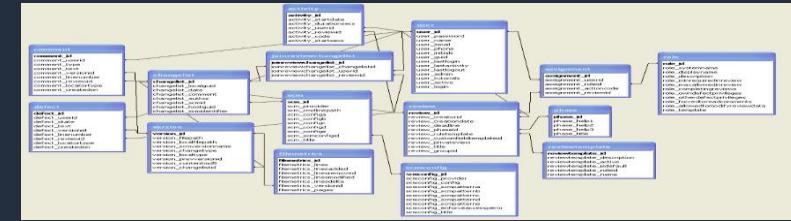


NoSQL DATABASE



SQL vs NoSQL

« Le schéma SQL » vs « La logique noSQL »



Différences :

- SQL
- NoSQL

KeyP	ISBN	title	author	format	price
1	0				
2					

Exemple :

```
{  
  ISBN: 1119138558,  
  title: "AWS Certified Solutions Architect Official Study Guide",  
  author: "Joe Baron",  
  format: "book",  
  price: 28.00  
}
```



Introduction RDS

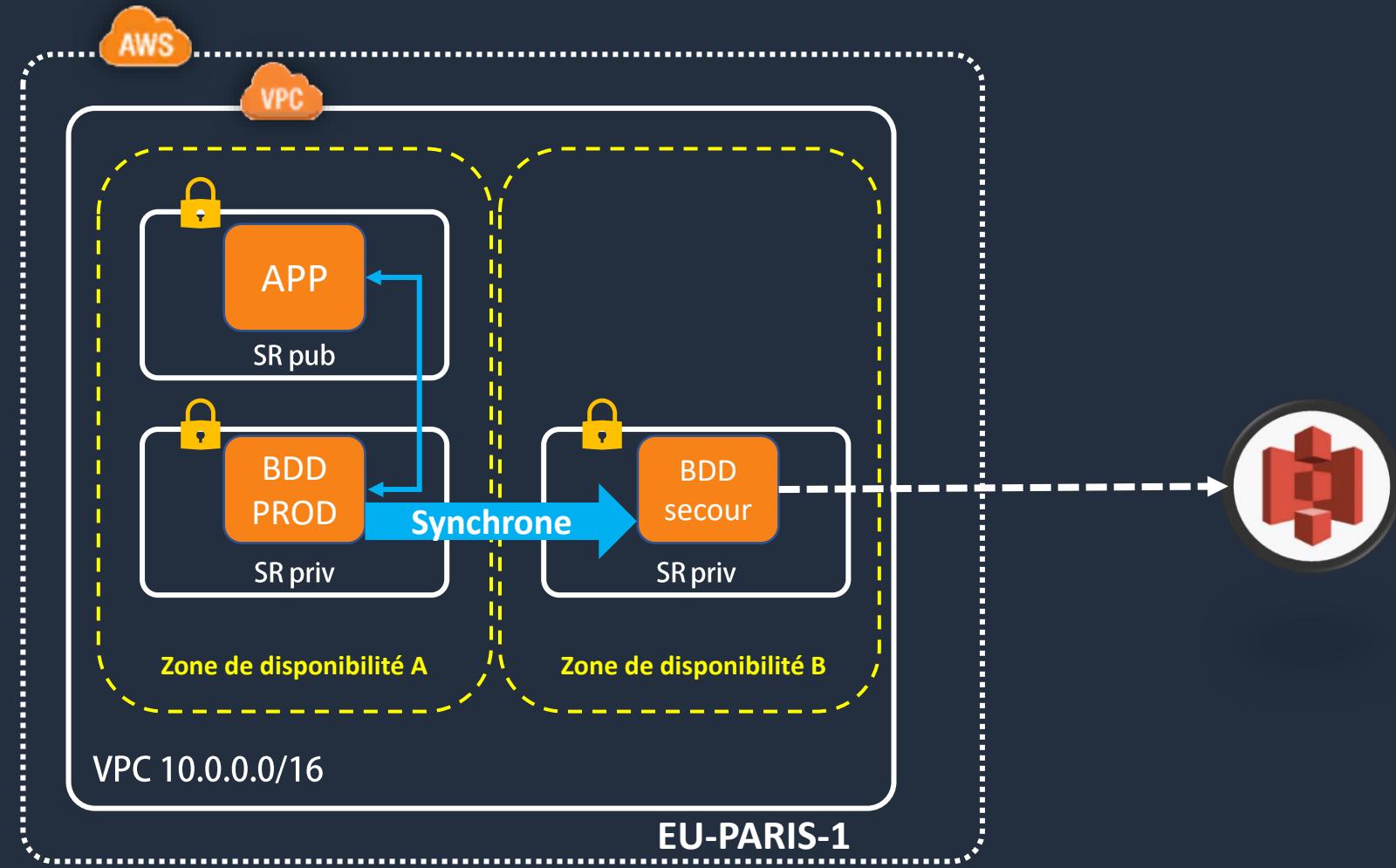


- Tarification à l'usage
- Modèle de gestion partagé
- Supporte les principaux acteurs de l'industrie
- Permet de conserver l'usage des outils habituels
- Accélère les performances et la continuité de service
- Permet aux clients de se concentrer sur leurs métiers
- Relève les défis imposés par une base de donnée relationnelle



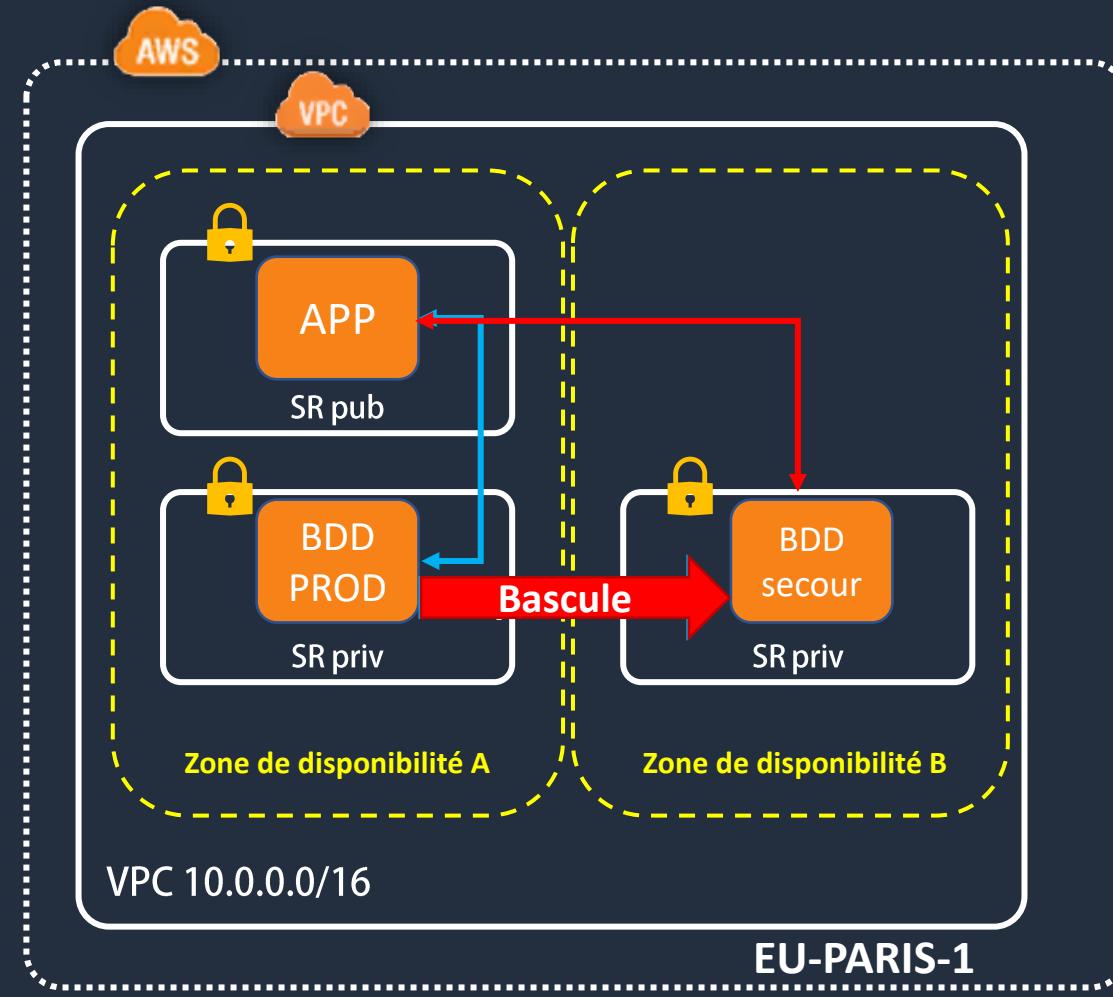


RéPLICATION et sauvegarde



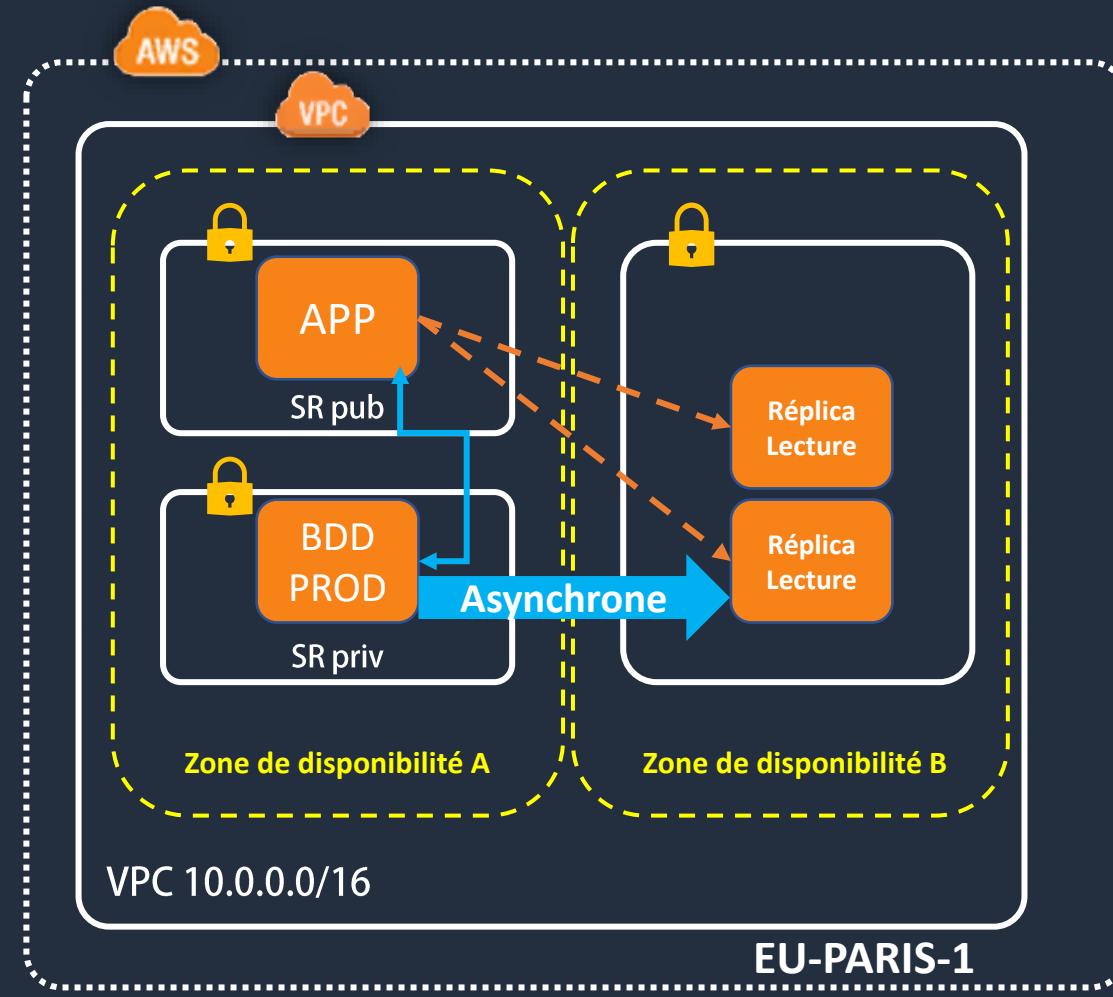


Haute disponibilité



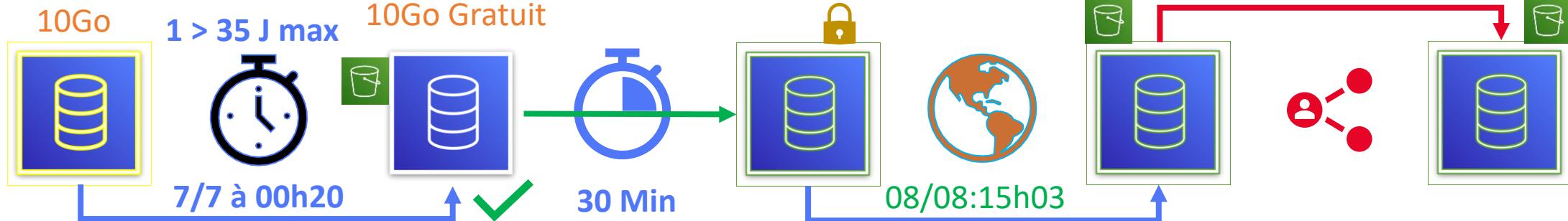


Réplicas en lecture





- **Sauvegardes automatiques** : Activées par défaut, stockée dans S3, sauvegarde la base et les journaux de transactions (volume de l'instance). Rétention entre 1 et 35 jours. Vous pouvez restaurer à la seconde de votre choix sur une nouvelle instance. Vous disposez d'un **volume de 1/1 gratuit** pour la sauvegarde, elle a lieu pendant une période donnée et peut occasionner quelques lenteurs. La sauvegarde a lieu chaque jour durant 30 min à l'heure souhaitée par le client.
- **Point in time restores** : Vous pouvez restaurer votre instance de base de données à tout moment pendant la période de conservation de la sauvegarde, en créant une nouvelle instance de base de données.
- **Databases snapshots** : Les instantanés de la base de données sont des sauvegardes de votre instance effectuées par l'utilisateur et stockées dans Amazon S3, qui sont conservées jusqu'à ce que vous les supprimiez explicitement.
- **Snapshot copies** : vous pouvez copier des instantanés de la base de données et des instantanés d'un cluster RDS. Vous pouvez copier un instantané au sein d'une même région ou entre régions AWS, et entre comptes clients AWS.
- **Snapshot sharing** : vous pouvez partager un instantané manuel de la base de données ou un instantané d'un cluster RDS chiffré ou non avec d'autres comptes clients AWS, qui par conséquent pourront en réaliser une copie.





Multi-AZ et Réplicas de lecture (accélérer la lecture)

La base de données principale est une instance « master » qui gère les accès en lecture et en écriture mais est limitée dans sa mise à l'échelle et l'on peut utiliser si besoin des réplicas de lecture.

Réplicas de lecture RDS :

- Jusqu'à 5 read replicas
- Dans une même zone de disponibilité, région ou autre région
- La réPLICATION des données est asynchrone
- Un réplica peut être promu « master »

Cas d'usage :

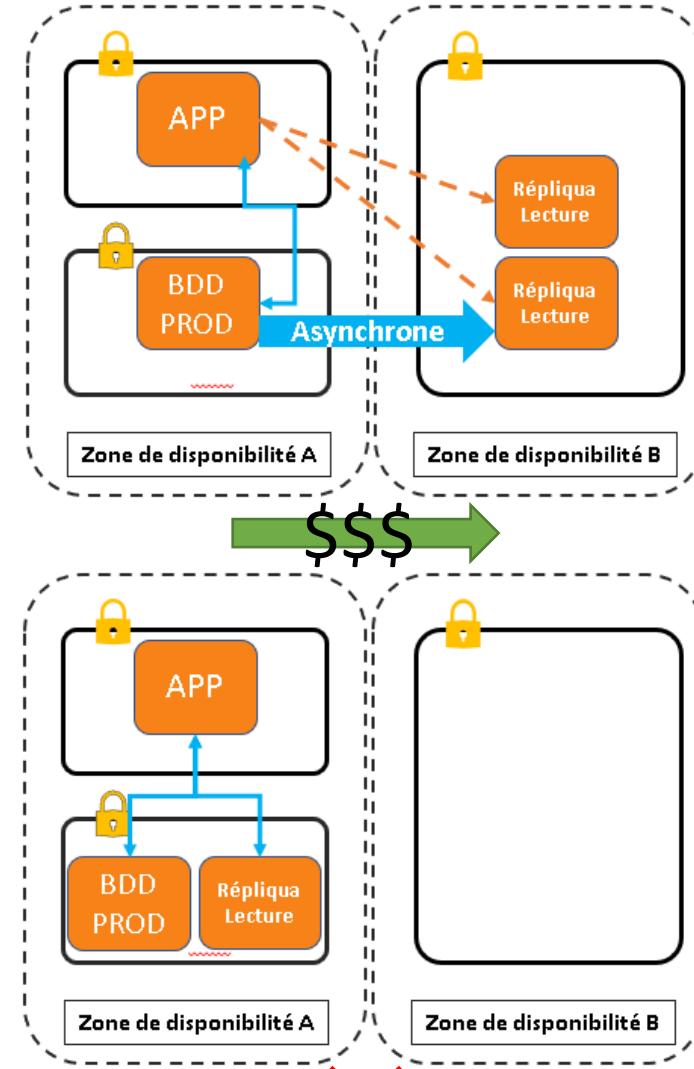
- Big data, Analytics, reporting, stats sur les données de prod
- Dédier un réplica de lecture
- Soulager la base de donnée principale

Optimisation :

- Conserver les Read réplicas sur une même AZ
- Supprimer les frais de transfert de donnée entre deux AZ

Sécurité :

- Une instance RDS peut être chiffrée au repos avec KMS AES-256
- Un réplica de lecture peut être chiffrée si la base principale est chiffrée
- TDE (transparent data encryptions) supporté pour Oracle et MS SQL Server
- La configuration se fait au lancement de l'instance (provisionnement)
- SSL en transit est possible avec un certificat de chiffrement
- Forcer le chiffrement est possible PostgreSQL (via console) et MySQL (via commande SQL)

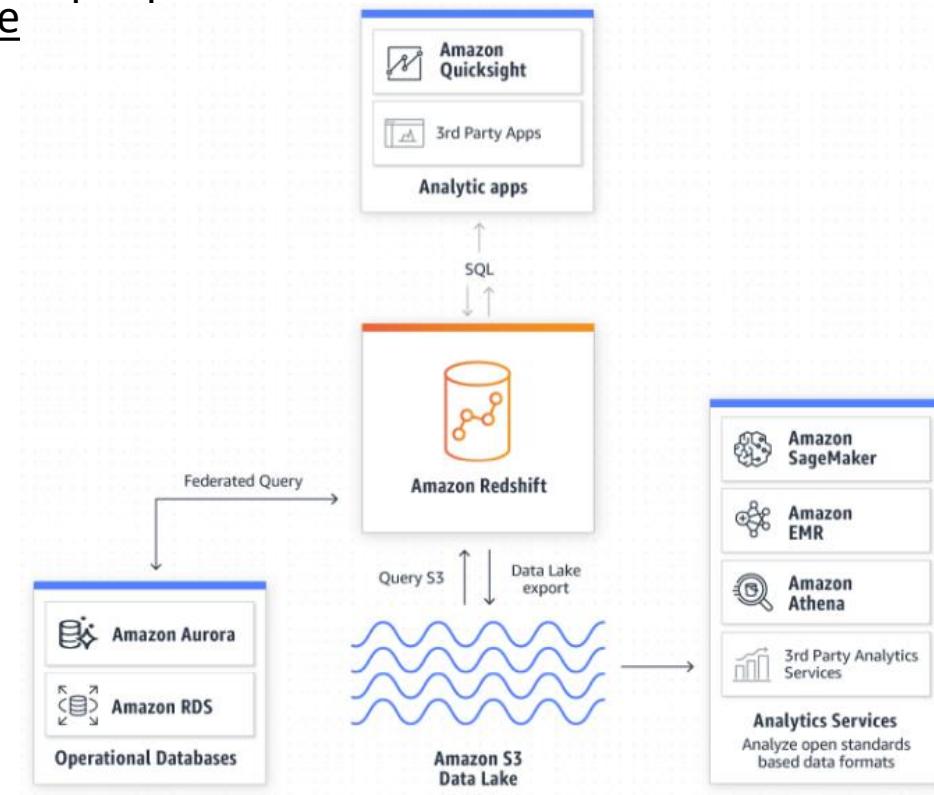




AMAZON Redshift – BI – Datawarehouse

Redshift permet d'exécuter de manière simple et rentable des requêtes hautes performances sur des pétaoctets de données structurées, de sorte que vous puissiez créer des rapports et des tableaux de bord performants à l'aide de vos outils d'informatique décisionnelle existants.

- Offre des performances jusqu'à trois fois plus élevées que n'importe quel autre entrepôt de données
- OLAP Online analytical processing (datawarehouse à l'échelle du Petabyte)
- Columnar data storage Data compression, Query optimizer (MPP), Mise en cache des résultats
- Coûte jusqu'à 75 % moins cher que n'importe quel autre entrepôt de donnée
- Interrogation et exportation de données vers et depuis votre data lake
- Requête fédérée (version préliminaire, RDS, Aurora)
- Utilisable avec Quicksight ou Tableau et l'écosystème d'analyse AWS
- Pay as you Go (à partir de 0,25\$/h) sans frais ni upfront
- Single node ou multi nodes (leader ou compute) jusqu'à 128 et 160GB
- Leader : planifie les requêtes, agrège les résultats. Compute
- Sauvegarde activée par défaut avec **1 jour de rétention (max 35j)**
- Données répliquées à minima 3 fois (leader + compute + backupS3)
- Possibilité de réplication des sauvegardes dans une autre région (PRA)
- Instances RA3 ou DC2 (DS2 recommandé de migré vers RA3)
- Chiffrement activé par défaut (HSM possible ou via KMS)
- Redshift est mono AZ (restauration d'un snapshot dans une autre AZ)
- Utilisation Business Intelligence & datawarehouse
- Redshift Spectrum accès aux données directement dans S3





Bases de données clé-valeur

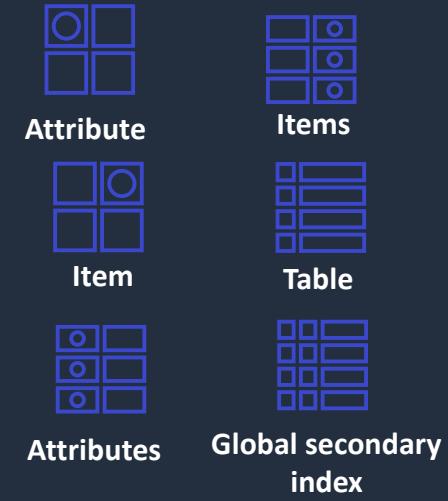
Les bases de données clé-valeur sont optimisées pour des modèles d'accès communs, généralement pour stocker et récupérer de grands volumes de données. Ces bases de données garantissent des temps de réponse rapides, même quand il s'agit de traiter des volumes extrêmement importants de demandes simultanées.

Amazon DynamoDB

(Serverless)



(NoSQL)





AMAZON DynamoDB – On demand vs Provisionned

DynamoDB facture des frais pour la lecture, l'écriture et le stockage de données dans vos tables, ainsi que pour les fonctions facultatives que vous choisissez d'activer.

Amazon DynamoDB offre deux modes de capacité en lecture/écriture pour traiter les lectures et écritures dans vos tables.

Capacité à la demande : On-demand capacity

Avec le mode de capacité à la demande, vous payez à la demande pour les données lues et écrites par votre application sur vos tables. Vous n'avez pas besoin de spécifier le débit de lecture et d'écriture attendu de votre application, car DynamoDB s'adapte instantanément à vos charges de travail, qu'elles augmentent ou diminuent. (WCU & RCU illimités cf quotas service + tarification + importante /requete)

Cas d'usage

- Vous créez de nouvelles tables avec des charges de travail incertaines.
- Vous avez un trafic d'applications imprévisible.
- Vous préférez la facilité de ne payer que ce que vous utilisez.

Capacité Allouée : Provisioned Capacity (default, free-tier)

En mode de capacité provisionnée, vous spécifiez le nombre de lectures et d'écritures de données par seconde nécessaires pour votre application. Vous pouvez utiliser la scalabilité automatique pour ajuster automatiquement la capacité de votre table en fonction du taux d'utilisation spécifié afin de garantir les bonnes performances de l'application tout en réduisant les coûts. (WCU & RCU définis + auto scaling)

Cas d'usage :

- Vous avez un trafic d'applications prévisible.
- Vous exécutez des applications dont le trafic est constant ou augmente progressivement.
- Vous pouvez prévoir les besoins en capacité pour contrôler les coûts.

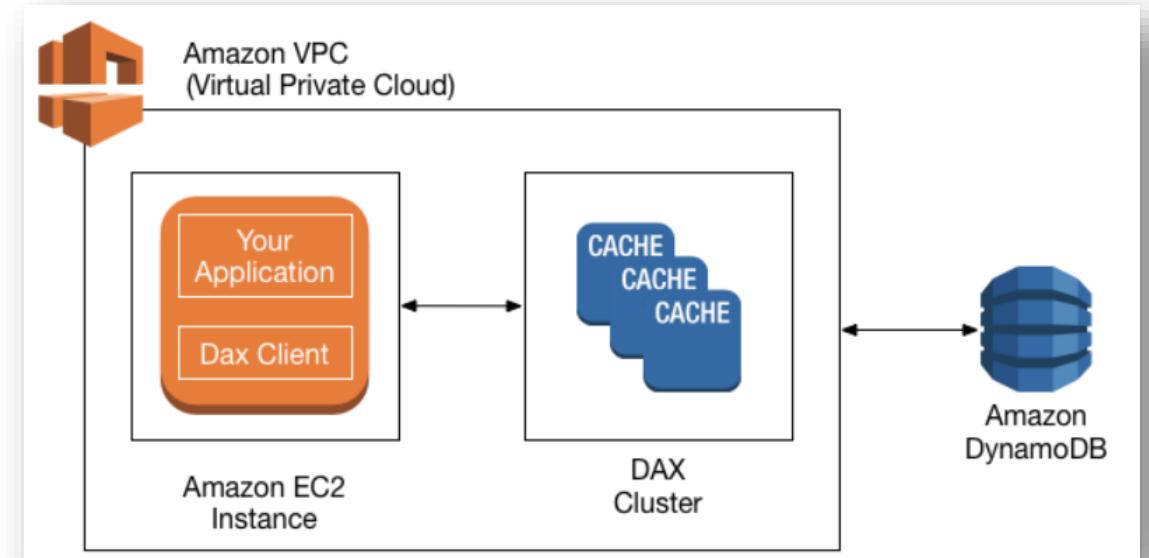


AMAZON DynamoDB – DAX – Transaction mode

Amazon DynamoDB Accelerator (DAX) est un cache en mémoire entièrement géré et hautement disponible pour Amazon DynamoDB.

DAX :

- Service géré, hautement scalable, cache en mémoire
- Pas de gestion de cache par les développeurs
- Augmente les performances par x10
- Réduit la latence de milliseconde à microsecondes
- 5 Minutes par défaut en TTL pour le cache DAX
- Jusqu'à 10 noeuds dans un cluster DAX (3 AZ)
- Support le chiffrement avec KMS + rôles IAM, SSL/TLS
- Compatible avec les appels API DynamoDB



Transaction : Gestion des flux de travail complexes

- Apporter des modifications « tout ou rien » coordonnées à plusieurs éléments à l'intérieur des tables et entre les tables.
- Les transactions offrent atomicité, cohérence, isolation et durabilité (ACID) dans DynamoDB.
- Avec l'API d'écriture de transaction, vous pouvez regrouper plusieurs actions Put, Update, Delete et ConditionCheck.
- Il n'y a pas de frais supplémentaires pour activer les transactions pour vos tables DynamoDB
- Vous payez uniquement les lectures ou écritures qui font partie de votre transaction.
- DynamoDB effectue deux lectures ou écritures sous-jacentes de chaque élément faisant partie de la transaction : une pour préparer la transaction et une pour la valider. (prepare and commit) révisez vos ressources allouées en mode transaction.
- Une transaction ne peut pas contenir plus de 25 éléments uniques. (Jun 24, 2019 , avant limite était 10)
- Une transaction ne peut pas contenir plus de 4 Mo de données.



AMAZON DynamoDB – Streams

Flux DynamoDB est une fonction facultative qui capture les événements de modification de données dans les tables DynamoDB. Les données sur ces événements apparaissent dans le flux de données presque en temps réel et dans l'ordre où les événements se sont produits.

Si vous activez un flux sur une table, il est écrit un enregistrement lorsque un des événements suivants se produit

- **Un nouveau champ (put item) est ajouté à la table :**

Le flux capture une image de l'élément entier, y compris tous ses attributs.

- **Un élément est mis à jour (update item) :**

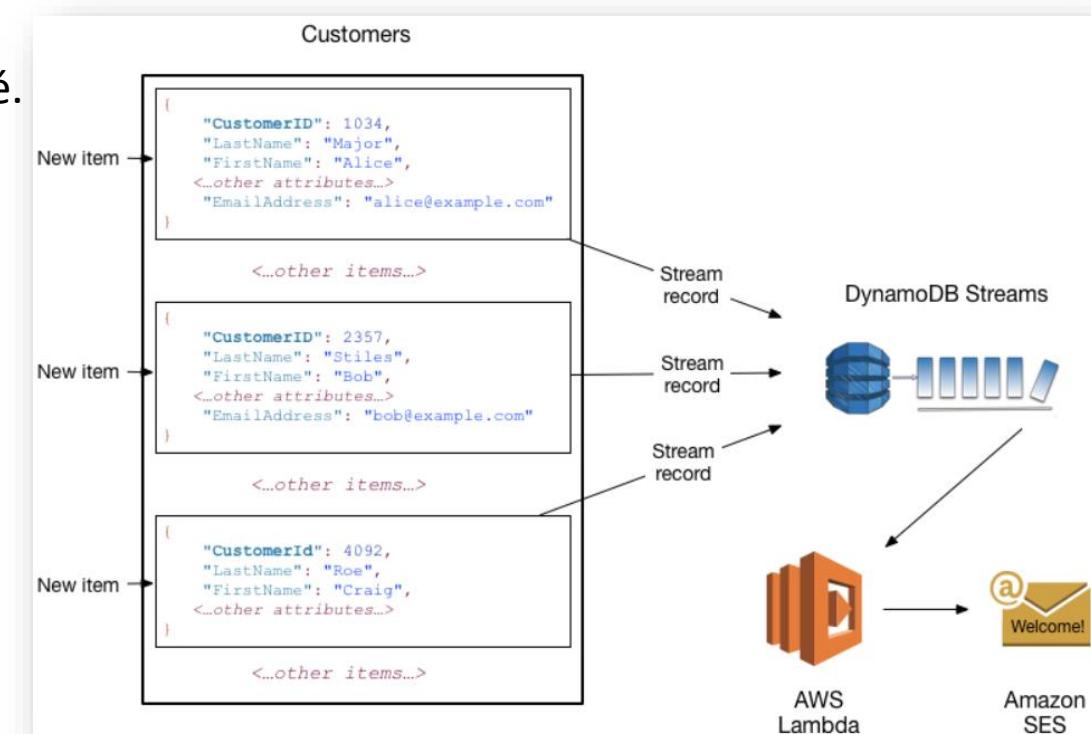
Le flux capture l'image "avant" et "après" de tous les attributs qui ont été modifiés dans l'élément.

- **Un élément est supprimé du tableau (delete item) :**

Le flux capture une image de l'élément entier avant qu'il ne soit supprimé.

Chaque enregistrement de flux contient aussi le nom de la table, l'horodatage de l'événement et autres métadonnées. Les enregistrements de flux ont une durée de vie de 24 heures ; passé ce délai, ils sont automatiquement supprimés du flux.

Vous pouvez utiliser Flux DynamoDB avec AWS Lambda pour créer un 'trigger—code' qui s'exécute automatiquement chaque fois qu'un événement d'intérêt apparaît dans un flux.





AMAZON DynamoDB – Tables globales

Les tables globales Amazon DynamoDB fournissent une solution entièrement gérée pour déployer une base de données à multiples maîtres sur plusieurs régions, sans avoir à créer et gérer votre propre solution de réPLICATION.

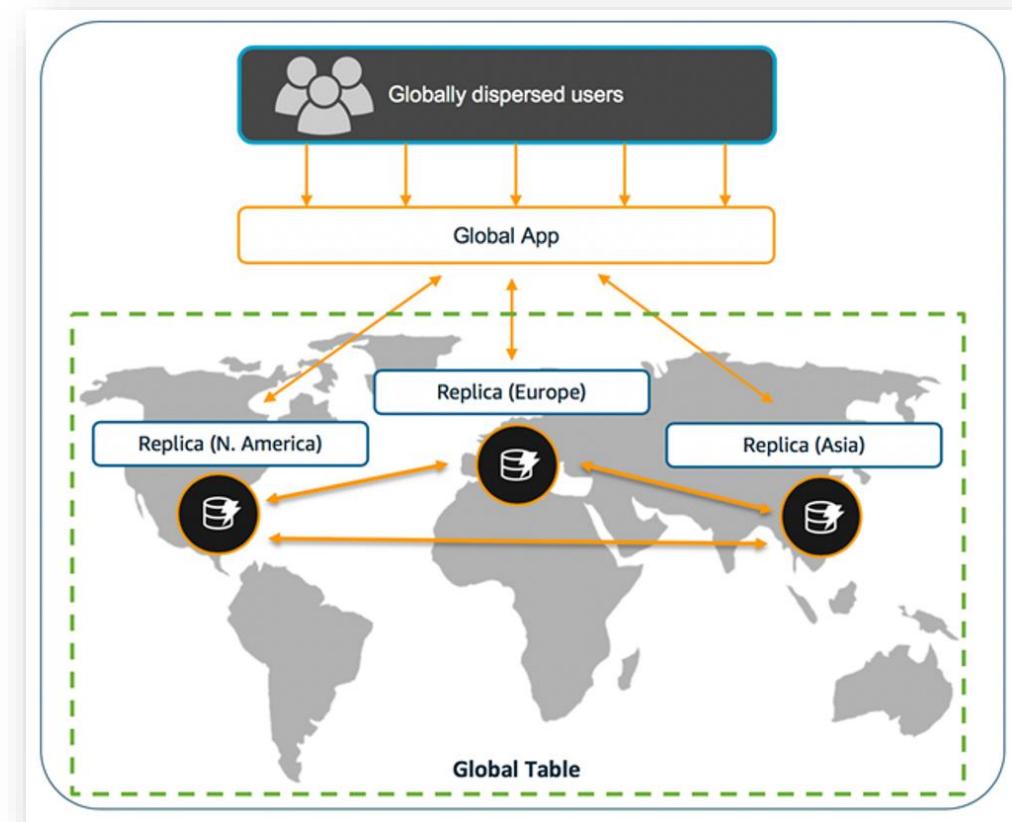
Lorsque vous créez une table globale DynamoDB, elle se compose de plusieurs tables de réPLICA (une par région AWS) que DynamoDB traite comme une seule unité. Chaque réPLICA porte le même nom de table et a le même schéma de clé primaire. Lorsqu'une application écrit des données dans une table de réPLICA dans une région, DynamoDB propage automatiquement l'écriture dans les autres tables de réPLICA des autres régions AWS.

Solution :

- Distribue les applications mondialement
- S'appuie sur les flux (streams DynamoDB)
- Redondance multi régions pour PRA ou haute disponibilité
- Ne nécessite pas de re écriture l'application
- Latence de réPLICATION inférieur à une seconde.

Avantages :

- Lecture et écriture locales et accès mondial aux données
- Performances élevées
- Configuration et utilisation simples
- Disponibilité, durabilité et tolérance aux pannes multi-régions
- Cohérence et résolution des conflits





AMAZON DynamoDB – On demand Backup and Restore

Vous pouvez créer des sauvegardes à la demande pour vos tables Amazon DynamoDB ou activer des sauvegardes continues avec restauration à un instant dans le passé.

Les sauvegardes DynamoDB à la demande sont disponibles sans frais supplémentaires par rapport au prix normal en vigueur pour la taille du stockage de sauvegarde.

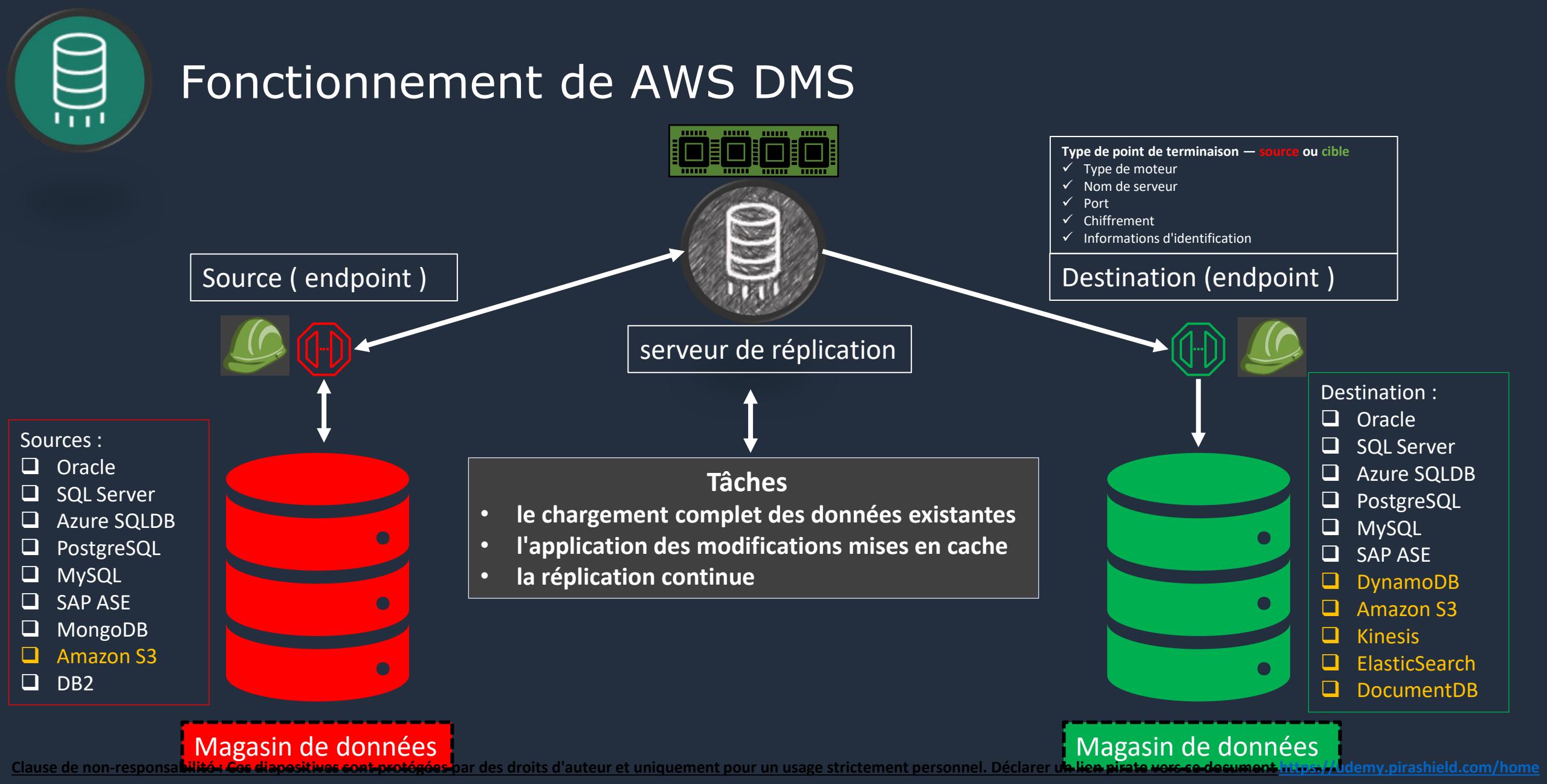
- Vous pouvez utiliser la fonction de sauvegarde DynamoDB à la demande pour créer des sauvegardes complètes de vos tables pour l'archivage et la conservation à long terme, à des fins de conformité réglementaire.
- Le processus de sauvegarde et de restauration à la demande évolue sans dégrader les performances ni la disponibilité de vos applications.
- Sauvegarde utilise une technologie distribuée nouvelle et unique, qui vous permet d'effectuer des sauvegardes complètes en quelques secondes quelle que soit la taille de la table.
- Les sauvegardes sont réalisées dans la même région que la table sauvegardée, vous ne pouvez pas sauvegarder ailleurs.

Point in time recovery : Restauration à un instant dans le passé

- permet de protéger vos tables DynamoDB contre les opérations d'écriture ou de suppression accidentelles.
- Restaurer à la seconde sur les 35 derniers jours
- Sauvegarde incrémentales (delta change)
- Non activé par défaut
- Sauvegarde par tranche de 5 minutes
- Restauration possible à partir de 5 minutes dans le passé

Migration possible vers dynamoDB avec Database migration service DMS (version locale disponible pour les développeurs)

Fonctionnement de AWS DMS





Bases de données en mémoire

Les bases de données en mémoire sont utilisées pour les applications qui nécessitent un accès en temps réel aux données. En stockant les données directement en mémoire, ces bases de données fournissent une latence en microsecondes aux applications pour lesquelles la latence en millisecondes n'est pas suffisante.

ElastiCache
for
Redis



ElastiCache



ElastiCache
for
Memcached



(in memory)

Microsecondes - under milliseconds

Stratégie de mise en cache AWS (il faut tout cacher ...)

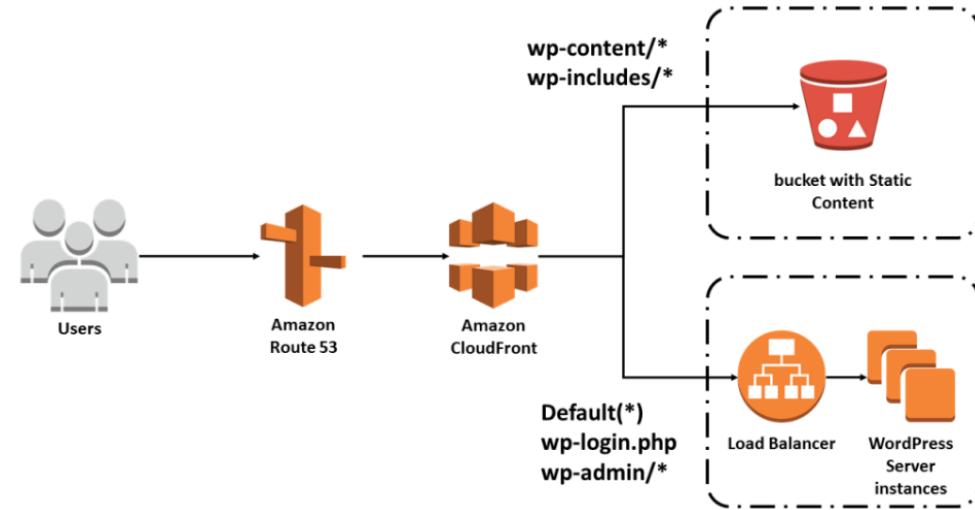
Comment offrir au mieux une données à jour, précise, et le plus rapidement possible.

Services avec cache :

- Cloudfront (edge caching / Lambda@edge)
- API Gateway (Web tiers caching)
- ElastiCache (App caching)
- DAX (DynamoDB Caching)

Cache stratégies :

- Time to live TTL (expiration)
- Permanent sync (synchrone)



Amazon EMR est une plateforme leader de Big Data dans le cloud dédiée au traitement de grandes quantités de données à l'aide d'outils open source tels que Apache Spark, Apache Hive, Apache HBase, Apache Flink, Apache Hudi et Presto.

Amazon Kinesis facilite la collecte, le traitement et l'analyse de données en streaming en temps réel, afin d'obtenir rapidement des informations stratégiques et de réagir rapidement.

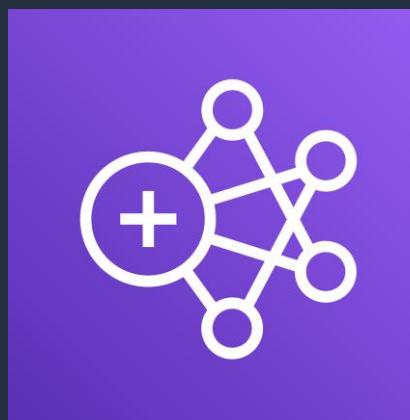
Amazon Athena est un service de requête interactif qui facilite l'analyse des données dans Amazon S3 à l'aide de la syntaxe SQL standard. Athena fonctionne sans serveur. Il n'existe aucune infrastructure à gérer et vous ne payez que pour les requêtes que vous exécutez.

Amazon Athena



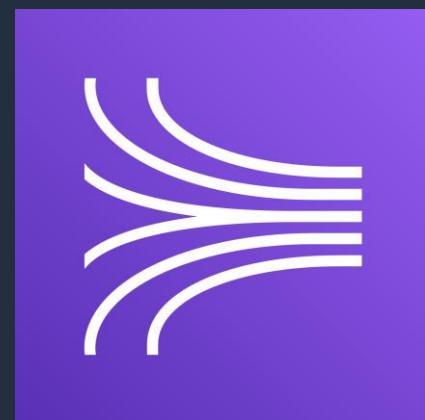
(serverless service
SQL queries S3 data)

Amazon EMR



(Hadoop)

Amazon Kinesis



(Real time
streaming data)



AMAZON Athena

Amazon Athena est un service de requête interactif qui facilite l'analyse des données dans Amazon S3 à l'aide de la syntaxe SQL standard.

Athena est un service serveless, pas de configuration de ressources, paiement par requête et par volumétrie traitée

- Inutile d'exécuter des tâches ETL complexes pour préparer vos données en vue de leur analyse.
- Créer votre schéma en écrivant des instructions DDL dans la console ou en utilisant un assistant de création de table
- Sélectionnez l'emplacement de vos données dans un **compartiment S3** et utilisez SQL pour vos requêtes
- Amazon Athena utilise Presto un moteur de **requêtes SQL** distribué open source
- Athena prend en charge un large éventail de **formats de données tels que CSV, JSON, ORC, Avro ou Parquet**
- contrôler l'accès à vos données à l'aide de stratégies AWS Identity and Access Management (IAM), de listes de contrôle d'accès (ACL) et de stratégies de compartiment Amazon S3
- Optimiser les coûts grâce aux formats de données en colonnes, au partitionnement et à la compression de données (90%)
- **Ne pas confondre avec MACIE** (qui lui utilise l'IA coté sécurité et essaye d'identifier les données PII / PCI-DSS)
- 5,00 USD par To de données analysées

Cas d'usage :

- Business intelligence
- Analytics (utilisé en tandem avec GLUE)
- Permet d'établir des analyses de logs
- VPC Flows logs, ELB logs, Cloudtrails Logs
- Créer des rapports avec Quicksight





Elastic Map Reduce - EMR

Amazon EMR est une plateforme leader de **Big Data** dans le cloud dédiée au traitement de grandes quantités de données à l'aide d'outils à code source libre

Noeuds : (maîtres, principaux, de tâches)

- **Master Node** : gère le cluster et exécute les composants maîtres des applications distribuées. Par ex, le service YARN ResourceManager pour gérer les ressources des applications, ainsi que le service HDFS NameNode. Il suit également le statut des tâches soumises au cluster et surveille l'intégrité des groupes d'instances.
- **Core Node** : Les nœuds principaux sont gérés par le nœud maître. Exécutent le démon de nœud de données pour coordonner le stockage des données dans le cadre du système de fichiers distribué Hadoop (HDFS). Ils exécutent également le démon du dispositif de suivi des tâches et exécutent d'autres tâches de calcul parallèles sur les données dont ont besoin les applications installées.
- **Task Node** : Les nœuds de tâches sont facultatifs. Vous pouvez les utiliser afin d'ajouter de la puissance pour l'exécution de tâches de calcul parallèles, comme les tâches Hadoop MapReduce et les exécuteurs Spark. Les nœuds de tâches n'exécutent pas le démon de nœud de données et ne stockent pas les données dans HDFS.

Amazon EMR et Hadoop génèrent des fichiers journaux qui indiquent le statut du cluster.

Par défaut, ces journaux sont écrits sur le nœud maître dans le répertoire **/mnt/var/log/**

En fonction de la façon dont vous avez configuré votre cluster lorsque vous l'avez lancé,

ces journaux peuvent également être archivés sur Amazon S3 et être affichés grâce à

l'outil de débogage graphique. (20 noeuds max tous clusters confondus)

Toutes les 5 min





AMAZON Kinesis

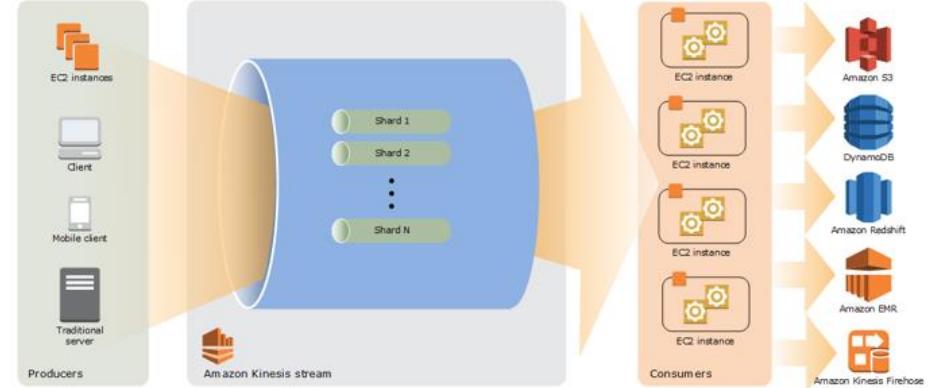
LIVE STREAMING
DATA / Données

Amazon Kinesis facilite la collecte, le traitement et l'analyse de flux vidéo et de données en temps réel.

- Amazon Kinesis Data Streams
- Amazon Kinesis Data Firehose
- Amazon Kinesis Data Analytics

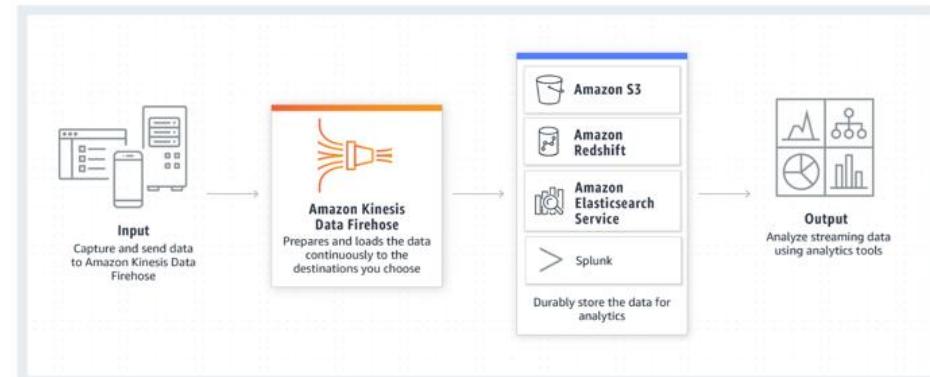
Amazon Kinesis Data Streams :

- Producers (source de données stream EC2, mobile, pc, iot)
- Shards (5 tps en lecture – 2MB / 1000 tps écriture – 1 MB,PK incluse)
- Stockage persistent (par defaut 24h et jusqu'a 7 jours)
- Consumers : instances EC2 de traitement des données et peuvent les copiers S3, dynamodb, emr, redshift.



Amazon Kinesis Data Firehose

- Producers (source de données stream EC2, mobile, pc, iot)
- Peut traiter les données via Lambda (optionnel)
- Pas de persistence de données, doit être stocké (S3, elasticsearch)



Amazon Kinesis Data Analytics

- Analyser les données de streaming en temps réel
- Apache Flink
- Pas de persistence de données, doit être stocké (S3, redshift , elasticsearch cluster)





Sécurité, Identité, Conformité !



Sécurité, Identité Et Conformité

- IAM
- Resource Access Manager
- Cognito
- Secrets Manager
- GuardDuty
- Inspector
- Amazon Macie
- AWS Single Sign-On
- Certificate Manager
- Key Management Service
- CloudHSM
- Directory Service
- WAF & Shield
- Artifact
- Security Hub
- Detective



- Une infrastructure résiliente
- Sécurité top niveau
- Des garanties solides



- Innovation rapide
- 1^{er} avec 22M\$ R&D 2018
- Évolution permanente de la sécurité



- Firewalling intégré
- Chiffrement à la volée
- Connexions dédiées
- Atténuation des attaques
- DDOS



- Outils de déploiements
- Outils d'inventaires et de configuration
- Définition de modèles et outils de gestion
- Annuaire
- Accès protégé MFA
- Fédération d'identité
- Amazon Cognito
- AWS Single Sign On (SSO)

Sécurité dans le cloud AWS

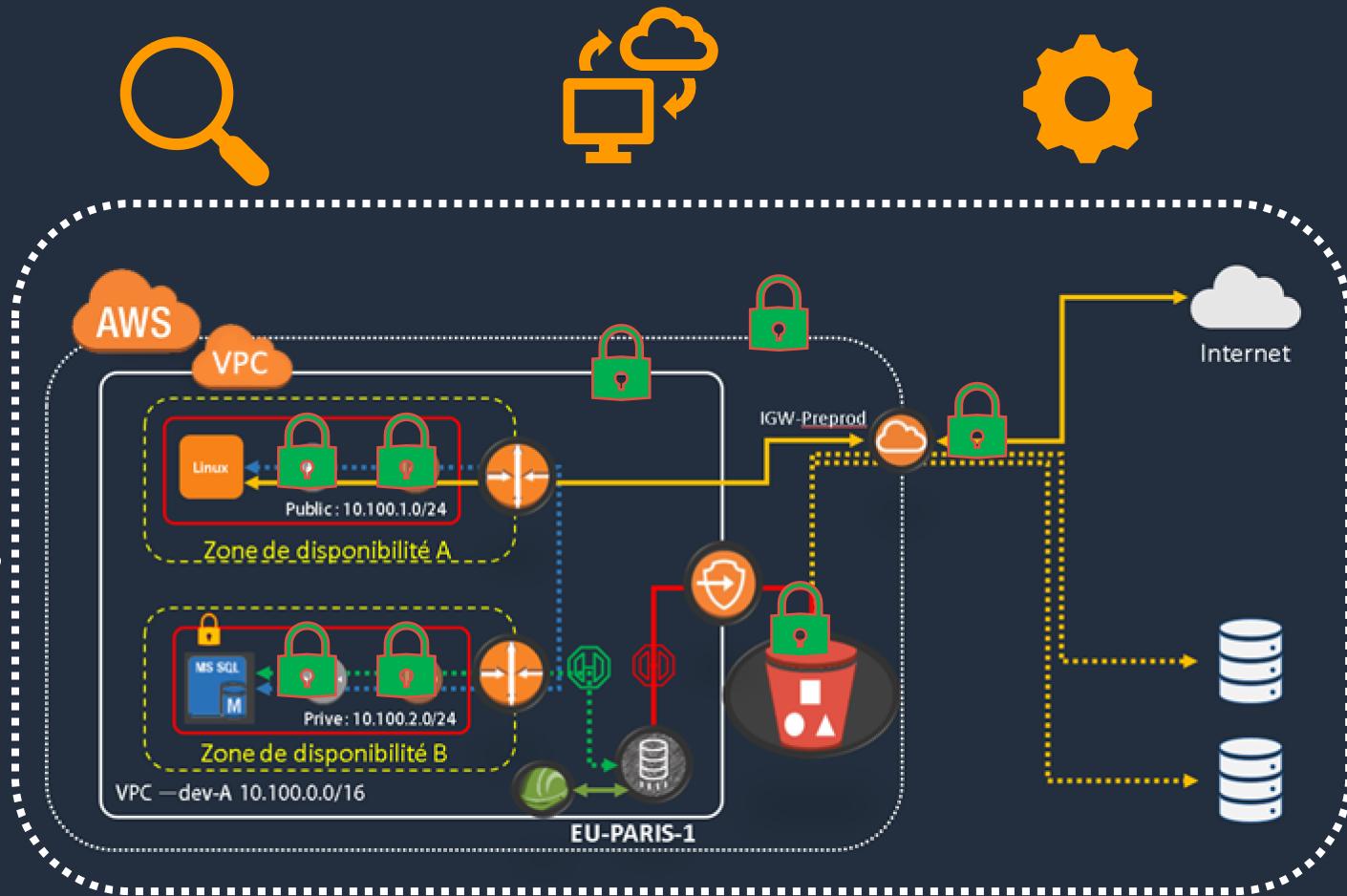


Les principes :

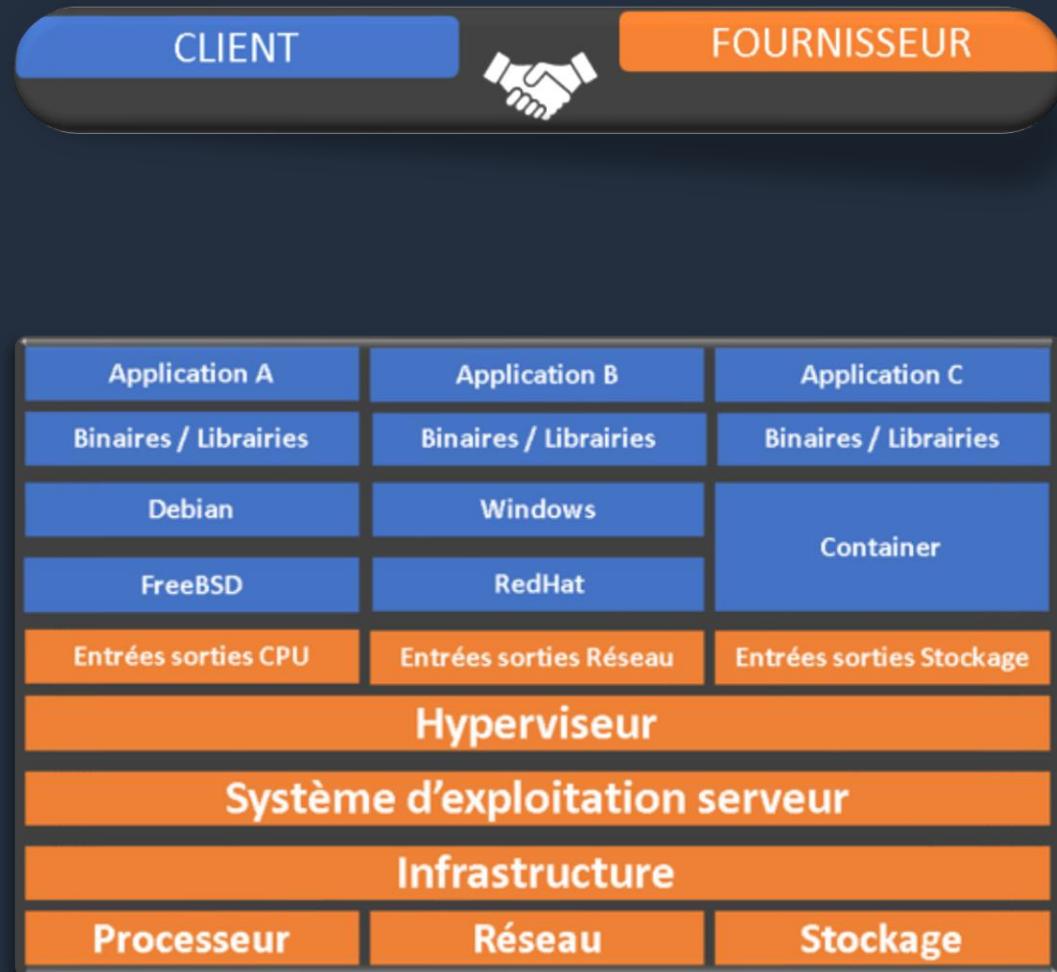
- Qui (identification)
- Quand (traçabilité)
- Niveau (où)
- Automatiser
- Données en transit et au repos
- Limiter le facteur humain
- Être prêt (préparation)

Comment ?

- Garantir l'accès aux données
- Se maintenir à jour
- Appliquer des nouveaux outils services
- S'assurer de la conformité
- Responsabilité partagées
- Outils configuration
- Sécuriser son réseau
- Chiffrer les données
- Contrôles des accès



Modèle de responsabilité partagée



Ex : Infrastructure as service (IAAS)

AWS Identity and Access Management (IAM)

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

AWS Identity and Access Management (IAM)

Gérez en toute sécurité l'accès aux charges de travail et aux applications.



Bonnes pratiques IAM

- Protéger les clés d'accès du compte racine AWS
- Créer des utilisateurs IAM individuels
- Utiliser des groupes pour attribuer des autorisations à des utilisateurs IAM
- Accorder le privilège le plus faible
- Mise en route avec les autorisations à l'aide des stratégies gérées AWS
- Utiliser les stratégies gérées par le client au lieu des stratégies en ligne
- Utiliser des niveaux d'accès pour examiner les autorisations IAM
- Configurer une stratégie de mot de passe fiable pour vos utilisateurs
- Activer MFA
- Utiliser des rôles pour les applications qui s'exécutent sur des instances Amazon EC2
- Utiliser des rôles pour déléguer des autorisations
- **Ne pas partager des clés d'accès**
- Effectuer une rotation régulière des informations d'identification
- Supprimer les informations d'identification inutiles
- Utiliser les conditions des stratégies pour une plus grande sécurité
- Surveillance de l'activité de votre compte AWS

AWS Organizations

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

AWS Organizations



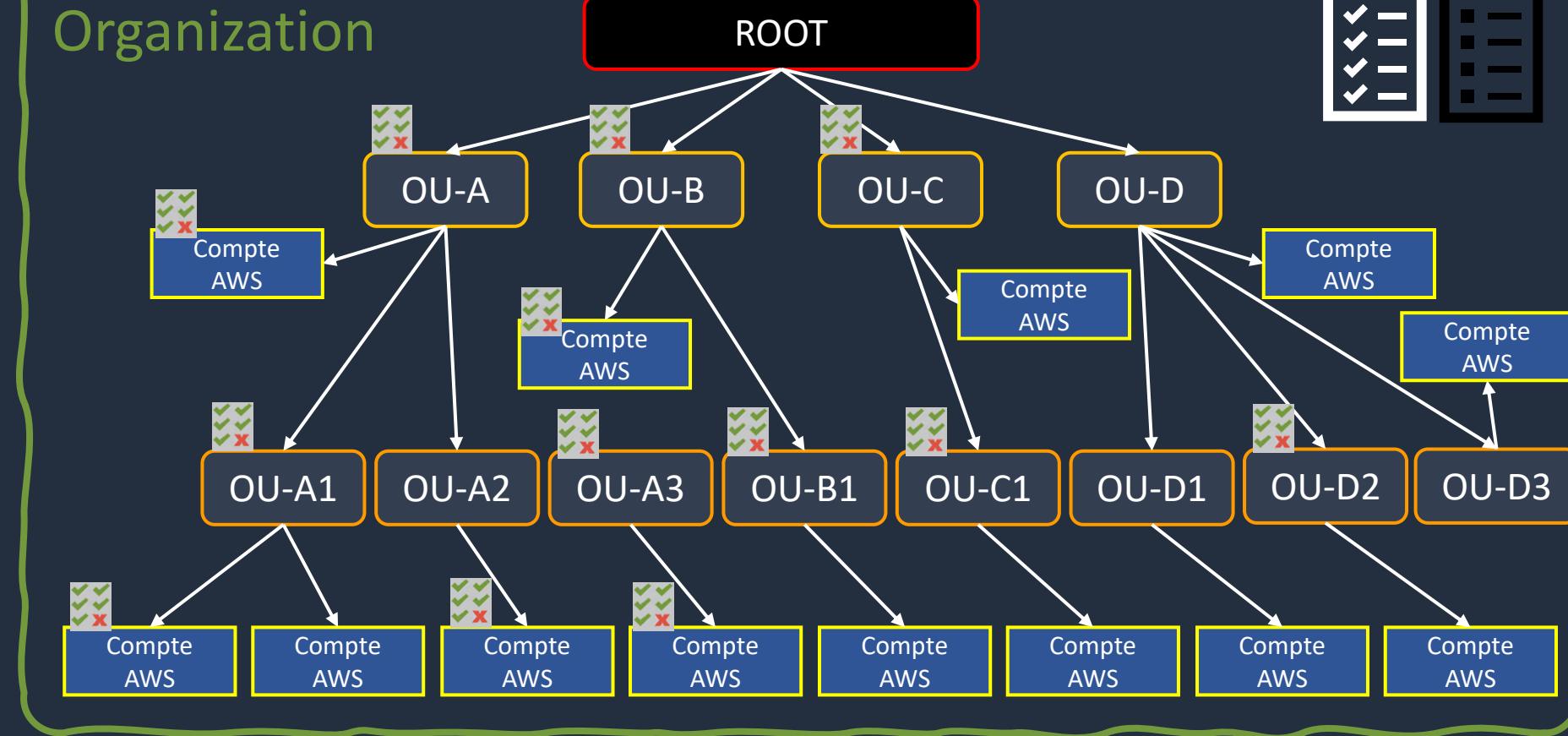
- Gestion des comptes basée sur les politiques
- Gestion des comptes par groupe
- Des API qui automatisent la gestion des comptes
- Facturation consolidée

Amazon Organizations aide à contrôler vos accès, la conformité, la sécurité et la facturation, ainsi qu'à partager des ressources sur vos comptes AWS, et ce de manière centralisée.

- Organization
- Root
- Organization unit (OU)
- Account
- Service control policy (SCP)
- Invitation
- Handshake
- Tag policy
- Allow lists vs. deny lists



IAM + SCP
User, group , root



AWS Organizations

Création et configuration d'une organisation

Étape 1 : Créer votre organisation.

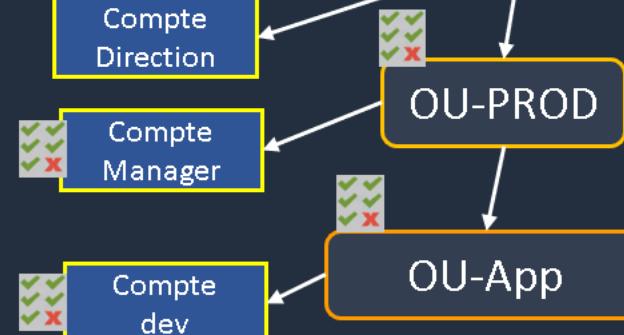
Étape 2 : Créer les unités organisationnelles.

Étape 3 : Créer les politiques de contrôle des services (SCP)

Étape 4 : Tester les politiques de votre organisation

Organization

ROOT (ouprod@mail.org)



```
"Version" "2012-10-17"
"Statement"
  "Sid" "Stmt1234567890123"
  "Effect" "Deny"
  "Action"
    "cloudtrail:AddTags"
    "cloudtrail:CreateTrail"
    "cloudtrail:DeleteTrail"
    "cloudtrail:RemoveTags"
    "cloudtrail:StartLogging"
    "cloudtrail:StopLogging"
    "cloudtrail:UpdateTrail"
  "Resource"
    "arn:aws:cloudtrail:eu-west-1:123456789012:trail/MyCloudTrail"
```

Surveillez les changements importants dans votre organisation

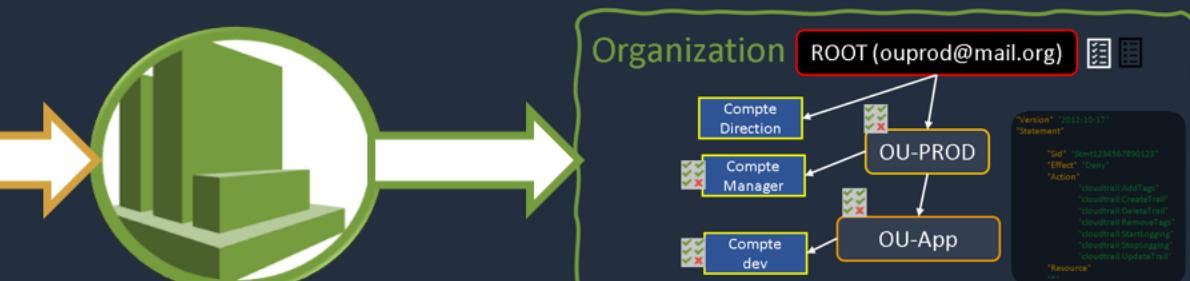
Étape 1 : Configurer un sélecteur d'événements cloudtrail

Étape 2 : Configurer une fonction Lambda

Étape 3 : Créez un sujet SNS Amazon qui envoie des emails ou SMS

Étape 4 : Créez une règle pour les événements CloudWatch

Étape 5 : Testez votre règle pour les événements CloudWatch



AWS Resource Access Manager

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

AWS Resource Access Manager

AWS Resource Access Manager (RAM) est un service qui vous permet de partager facilement et en toute sécurité les ressources AWS avec n'importe quel compte AWS ou au sein de votre organisation AWS.



Amazon Cognito

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

Amazon Cognito

Permet d'ajouter facilement et rapidement l'inscription et la connexion des utilisateurs ainsi que le contrôle d'accès à vos applications Web et mobiles.

User pool (rep util)

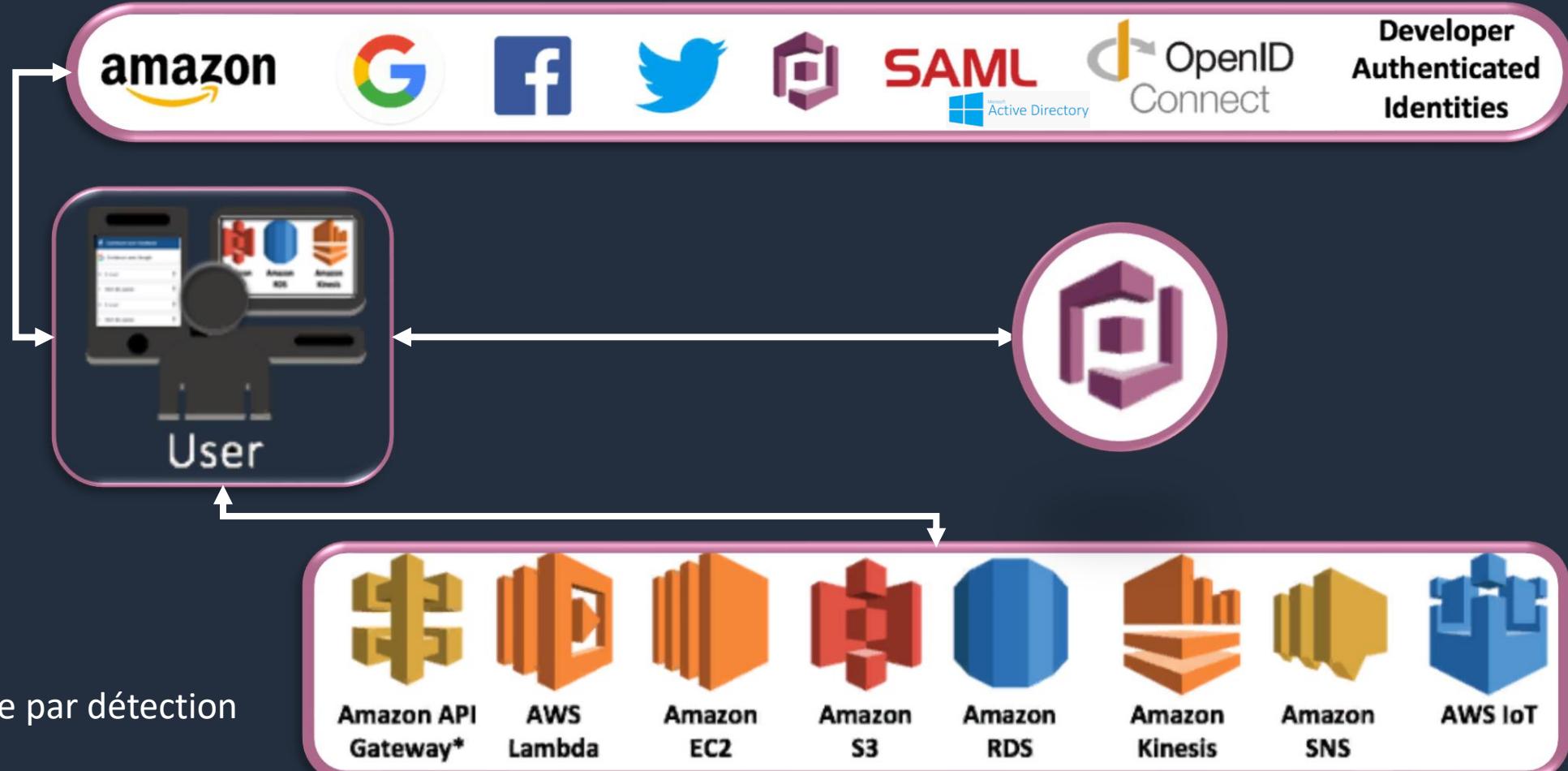
Prénom et nom
E-mail
Mot de passe

Fédération d'identités

Continuer avec Facebook
Continuer avec Google
E-mail
Mot de passe



Sécurité renforcée par détection



AWS Secrets Manager

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

AWS Secrets Manager

Renouvez, gérez et récupérez facilement des informations d'identification de base de données, des clés d'API et d'autres secrets tout au long de leur cycle de vie



Amazon Macie

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

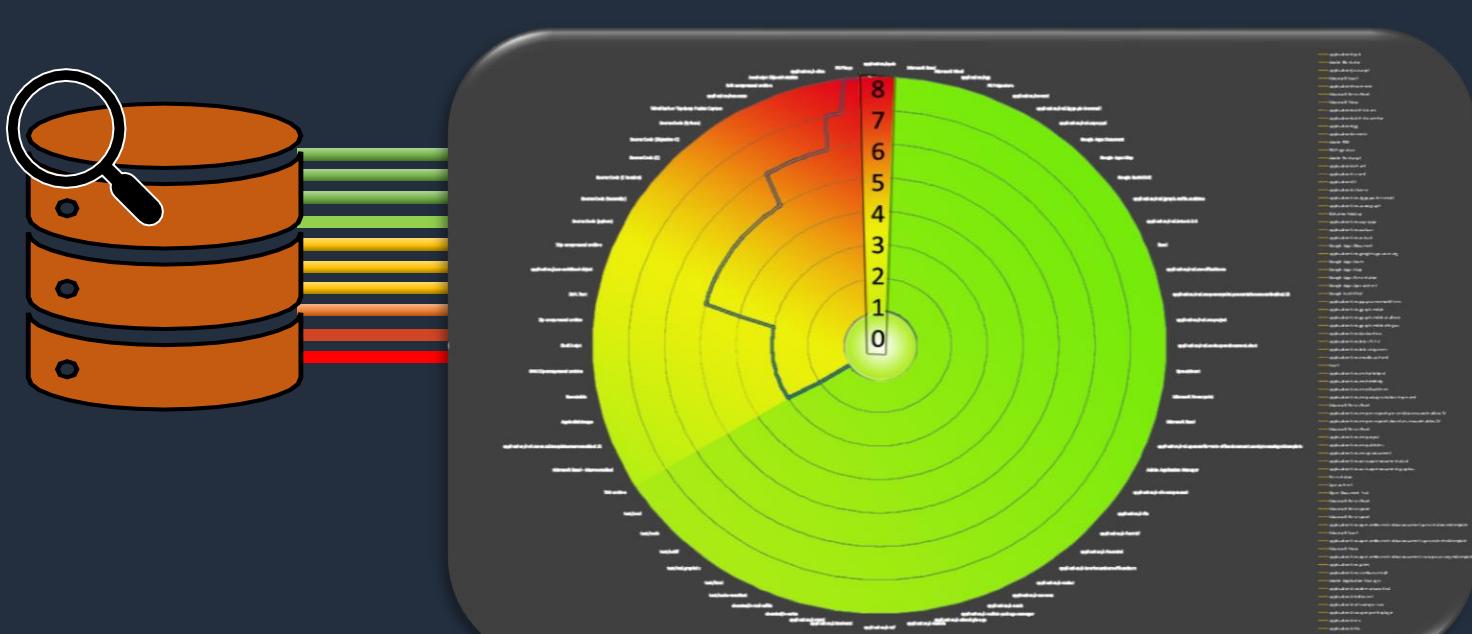
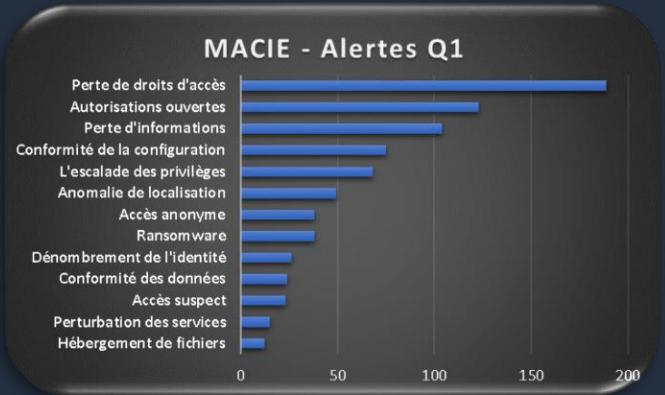
Un service de sécurité optimisé par l'apprentissage machine pour découvrir, classer et protéger les données sensibles.

Détection et classification

- Analyse en permanence des données dans S3
- Analyse les comportements (ML / IA)
- Méthode d'interprétation du langage naturel (NLP)
- Définie la valeur business des données
- Donne un indice de priorité des données
- Priorise les alertes sur les données importantes

Protection des données

- Identifie les données critiques (API Keys – SAKey)
- Identifie les informations personnelles (PII).
- Détectes les modifications des stratégies de sécurité
- Détectes les modifications des Access lists réseaux
- Alerte en cas de comportement anormal détecté
- Assure le maintien en conformité



- un manque de compréhension des contrôles de sécurité clés fournis par le S3
- Un manque de connaissance quant à la sensibilité des données stockées sur S3
- Une simple erreur humaine ou un acte malveillant
- Les données des citoyens de l'UE doivent être protégés et sécurisés en permanences
- Tout défaut peut entraîner 4% du total des revenus et jusqu'à 20M€
- Faire bon usage des bon outils est impératif lorsque l'on stock ses données dans le cloud.

AWS Key Management Service (KMS)

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

AWS Key Management Service (KMS)

SERVER SIDE ENCRYPTION

CLIENT SIDE ENCRYPTION



KMS utilise le **chiffrement** Symétrique pour les données au repos (at rest). RDS EMR EBS S3 (SSE-KMS) AWS n'a pas accès à vos clés et ne pourra en aucun cas restaurer une clé une fois effacée. Tout acte d'administration requiert une double authentification réalisée par deux administrateur AWS. La gestion de KMS est assuré par le client, AWS ne gère que les composants nécessaires pour faire fonctionner le service.



Le **chiffrement** (ou cryptage) est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)**chiffrement**. Ce principe est généralement lié au principe d'accès conditionnel.



Le **chiffrement** symétrique
AES
DES
Triple-DES
Blowfish



Le **chiffrement** Asymétrique
RSA
DH
DSA



jL70zzcXeYDFb406LRe2rIJNA8rlodyEohxa42d7U/4TGuxosoGSPUJHdRhv4VlfP47dmYOC/rFONRzEVsuSvVTCaiLGJ0DSykJUJmztW1BO/LOkCYmWML+Kf1e3RSbQjfTxVoiVOBt6JHMk1MIB41mlG/ooP0WOBxRzrej05AdcwcxDlhgkDFq+2/qROzgBVIFHhQV99KBKod1vldS31P0cFNQjH3Z2kvB4XsID/m/Gi2ovLQ34iK8ORdWEU5iYtQ68yBM1TzIWTTtmzDLHMIrVH8Ry9ENHrjyN+DdACiYyI1+Kx3pugfZCqjx7/298KKMDM486ku5W0eW1CszWXpTzUxX5Dxe3l5voIpBmZLei8/YwNAP0toP7yYS7Om



KMS

Privée - Public



En transit SSL



AWS Certificate Manager

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

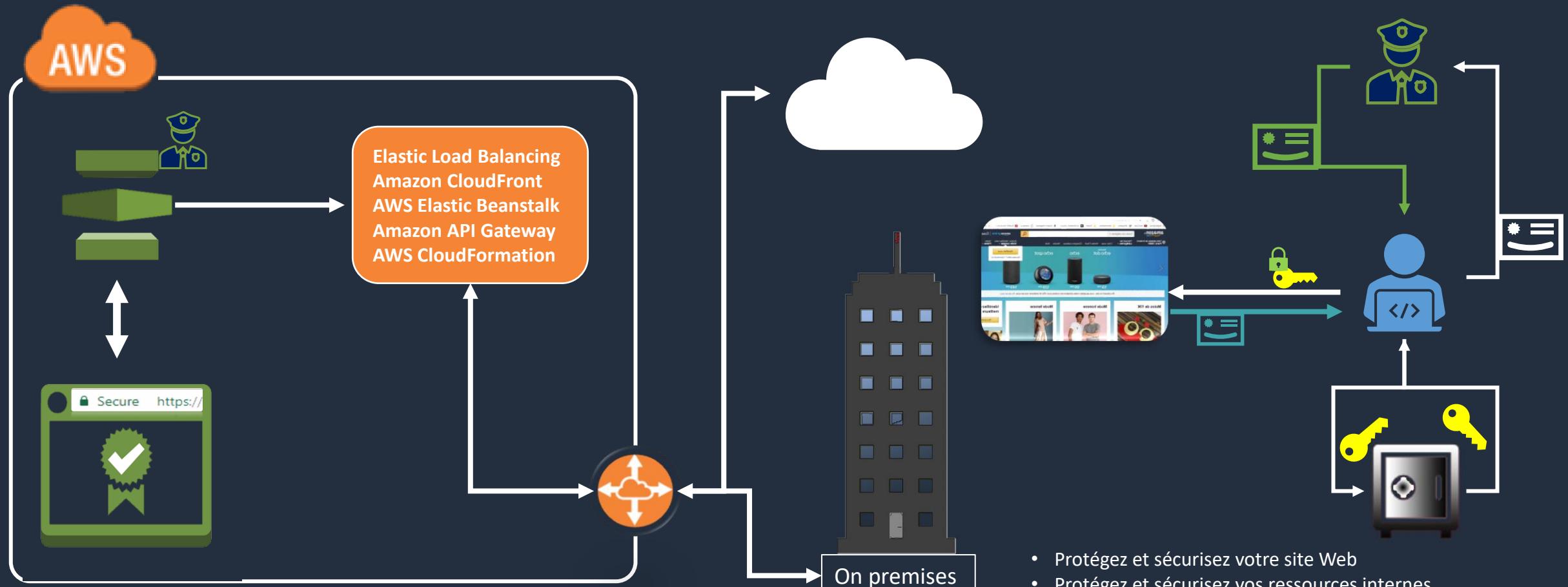
Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

AWS Certificate Manager

- Certificats publics gratuits pour les services intégrés dans ACM
- Gestion du renouvellement des certificats
- Obtenez facilement des certificats



- Protégez et sécurisez votre site Web
- Protégez et sécurisez vos ressources internes
- Respect des exigences en matière de conformité
- Temps de fonctionnement amélioré

AWS CloudHSM

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

AWS CloudHSM

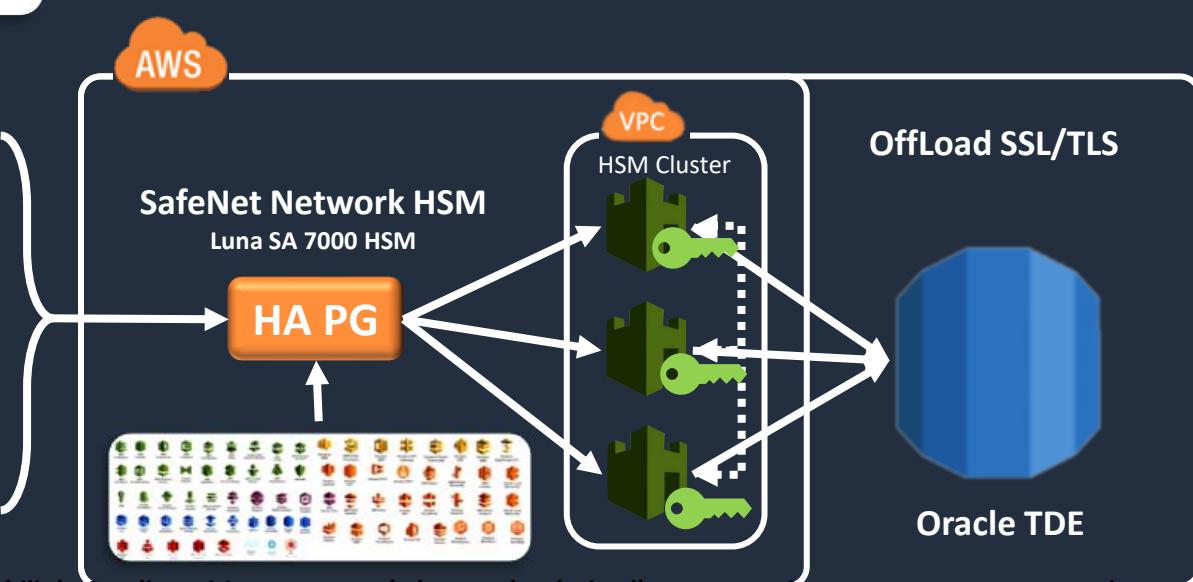
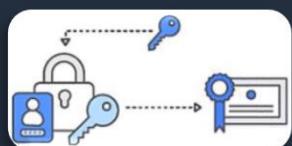
Un HSM (Hardware Security Module) intervient pour faire du double chiffrement c'est-à-dire chiffrer les clés de chiffrement. C'est le cas si on souhaite l'intégrer avec AWS KMS par exemple.

- Protège vos clés de chiffrement grâce à des modules de sécurité matériels sûrs et conformes
 - Accès individuel au matériel validé de niveau 3 de la fips 140-2
 - Prendre en charge les activités sensibles en matière de sécurité, conformément aux règles de la législation en vigueur
- Garder le contrôle total de la gestion de l'accès à vos clés de cryptage
 - AWS n'a pas accès à votre HSM ni aux clés qui s'y trouvent
 - Toutes les communications avec votre HSM sont chiffrées de bout en bout



HMS > 2017

HMS Classic < 08/2017



- ~1024 RSA /sign verify tps
- AES synchrone avec la vitesse du reseau
- ~3500 clés
- Jusqu'à 32 Safenet HSM
- ~32000 tps
- Mise à l'échelle à la demande

AWS Directory Service

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

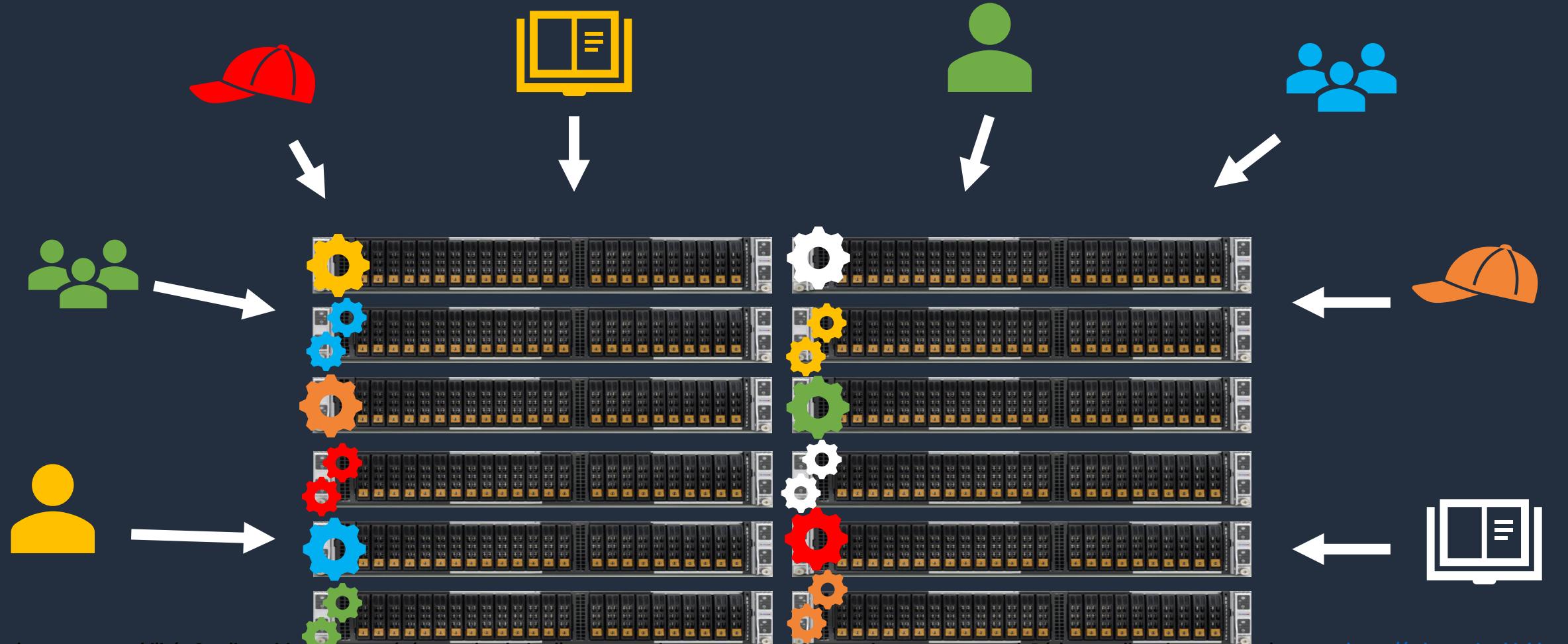
Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

AWS Directory Service

Relation d'approbation (forêt)





AWS Directory Service

Types d'annuaire

- AWS Managed Microsoft AD
- Simple AD
- Connecteur AD
- Groupes d'utilisateurs Amazon Cognito

- AWS Managed Microsoft AD
- Simple AD
- Connecteur AD
- Groupes d'utilisateurs Amazon Cognito

- AWS Managed Microsoft AD
- Simple AD
- Connecteur AD
- Groupes d'utilisateurs Amazon Cognito

- AWS Managed Microsoft AD
- Simple AD
- Connecteur AD
- Groupes d'utilisateurs Amazon Cognito

Grâce à AWS Managed Microsoft AD, vous pouvez facilement permettre à vos charges de travail et ressources AWS compatibles avec Active Directory d'utiliser la version authentique d'Active Directory gérée dans le cloud AWS. Voici quelques exemples de charges de travail : Amazon EC2, Amazon RDS pour SQL Server, applications .NET personnalisées et applications informatiques d'entreprise AWS telles qu'Amazon WorkSpaces.

Simple AD est un annuaire géré et autonome reposant sur un serveur compatible Linux-Samba Active Directory.

AD Connector est un proxy qui redirige les requêtes d'annuaire vers votre annuaire Microsoft Active Directory existant sans mettre d'informations en cache dans le cloud. AD Connector est disponible en deux tailles, petite et grande. Les petits connecteurs AD Connector sont destinés aux petites organisations comptant jusqu'à 500 utilisateurs. Un connecteur AD Connector 5 000 utilisateurs

Les groupes d'utilisateurs vous permettent d'ajouter des fonctions d'inscription et de connexion des utilisateurs à vos applications. Au lieu d'utiliser des fournisseurs d'identité externes comme Facebook ou Google, les utilisateurs peuvent s'inscrire ou se connecter à l'aide d'une adresse e-mail, d'un numéro de téléphone ou un nom d'utilisateur. Vous pouvez également créer des champs d'inscription personnalisés et stocker ces métadonnées dans l'annuaire d'utilisateurs. Quelques lignes de code suffisent pour vous permettre de vérifier les adresses e-mail et les numéros de téléphone, de récupérer des mots de passe et d'activer l'authentification multi-facteurs (MFA).

USA Est (Virginie du Nord) us-east-1

USA Est (Ohio) us-east-2

USA Ouest (Californie du Nord) us-west-1

USA Ouest (Oregon) us-west-2

Asie Pacifique (Hong Kong) ap-east-1

Asie Pacifique (Mumbai) ap-south-1

Asie Pacifique (Séoul) ap-northeast-2

Asie Pacifique (Singapour) ap-southeast-1

Asie Pacifique (Sydney) ap-southeast-2

Asie Pacifique (Tokyo) ap-northeast-1

Canada (Central) ca-central-1

Europe (Francfort) eu-central-1

Europe (Irlande) eu-west-1

Europe (Londres) eu-west-2

Europe (Paris) eu-west-3

Europe (Stockholm) eu-north-1

Moyen-Orient (Bahreïn) me-south-1

Amérique du Sud (São Paulo) sa-east-1

AWS Directory Service

Amazon Cloud Directory permet de créer des annuaires flexibles dans le cloud, afin d'organiser des hiérarchies de données dans plusieurs dimensions. Vous pouvez créer des annuaires destinés à divers cas d'utilisation, tels que des organigrammes, des catalogues de formation ou encore des registres d'appareils.

Sélectionnez une option de schéma correspondant à vos besoins

Schéma géré
Créez instantanément un répertoire.

Exemple de schéma
Choisissez dans une liste d'exemples de schémas AWS.

Schéma personnalisé
Chargez ou choisissez une configuration de schéma précédente.

Exemples de schémas
Applique l'un des exemples de schémas pour les organisations, les personnes et les appareils à votre nouvel annuaire.

Nom	Version (majore/mineure)
device	1.0/-
organization	1.0/-
person	1.0/-

[Prévisualiser le schéma](#)

Amazon Cloud Directory

Magasin de données hiérarchisées, entièrement géré, dans le cloud AWS



AWS Directory Service for Microsoft Active Directory, aussi connu sous le nom d'AWS Managed Microsoft AD, permet à vos charges de travail et ressources AWS prenant en charge les répertoires, d'utiliser Active Directory dans le cloud AWS.

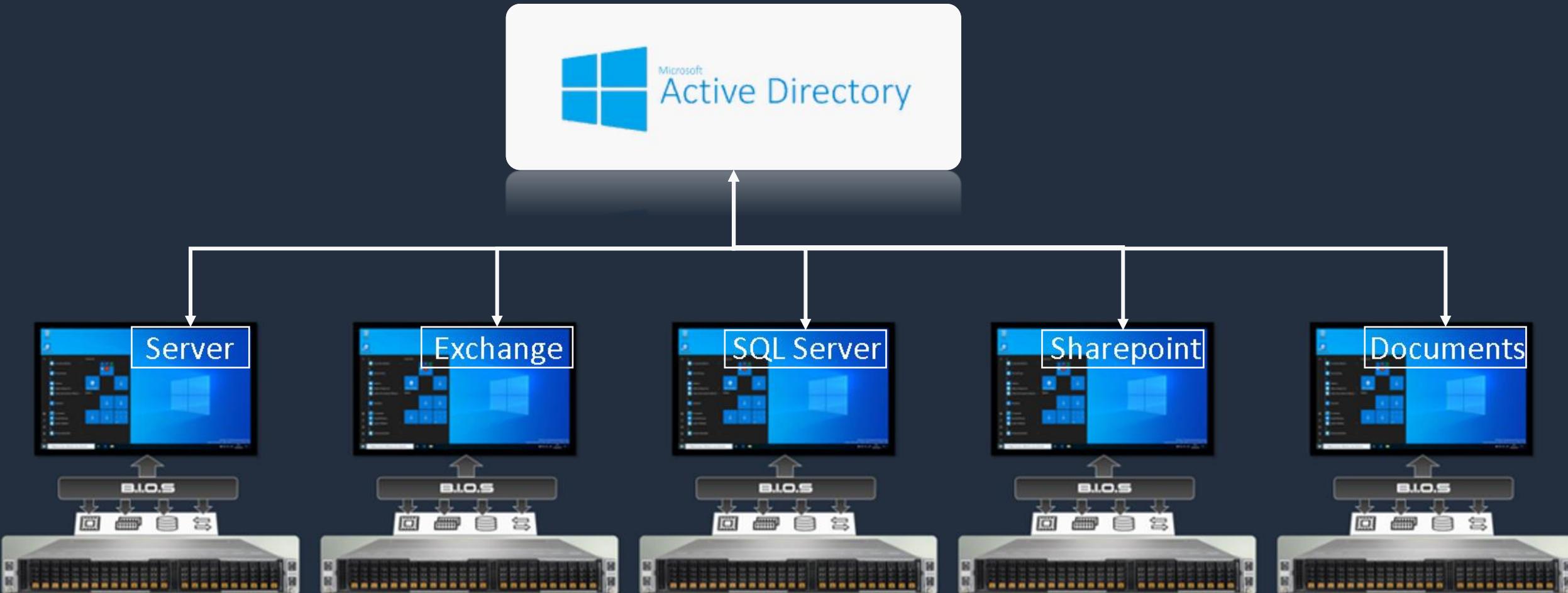
- Version authentique de Microsoft Active Directory
- Haute disponibilité
- Infrastructure gérée par AWS
- Éligibilité HIPAA et PCI
- Prise en charge des approbations
- Stratégies de groupe
- Authentification unique
- Liaison de domaines en toute transparence
- Un répertoire unique pour toutes les charges de travail
- Accès fédéré à AWS Management Console
- Instantanés quotidiens



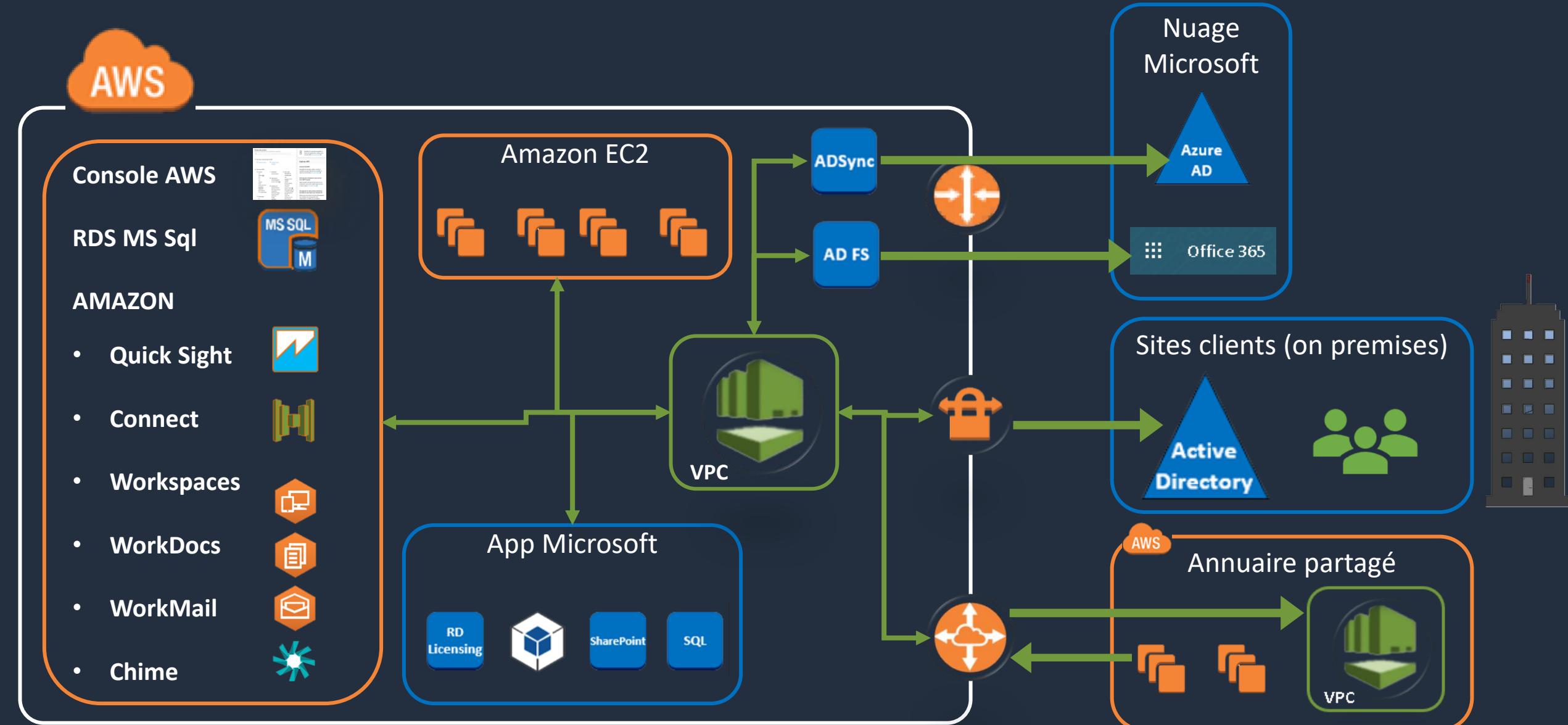
AWS Directory Service

Gestion de Microsoft Active Directory dans le cloud AWS

AWS Directory Service



AWS Directory Service



AWS Shield

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

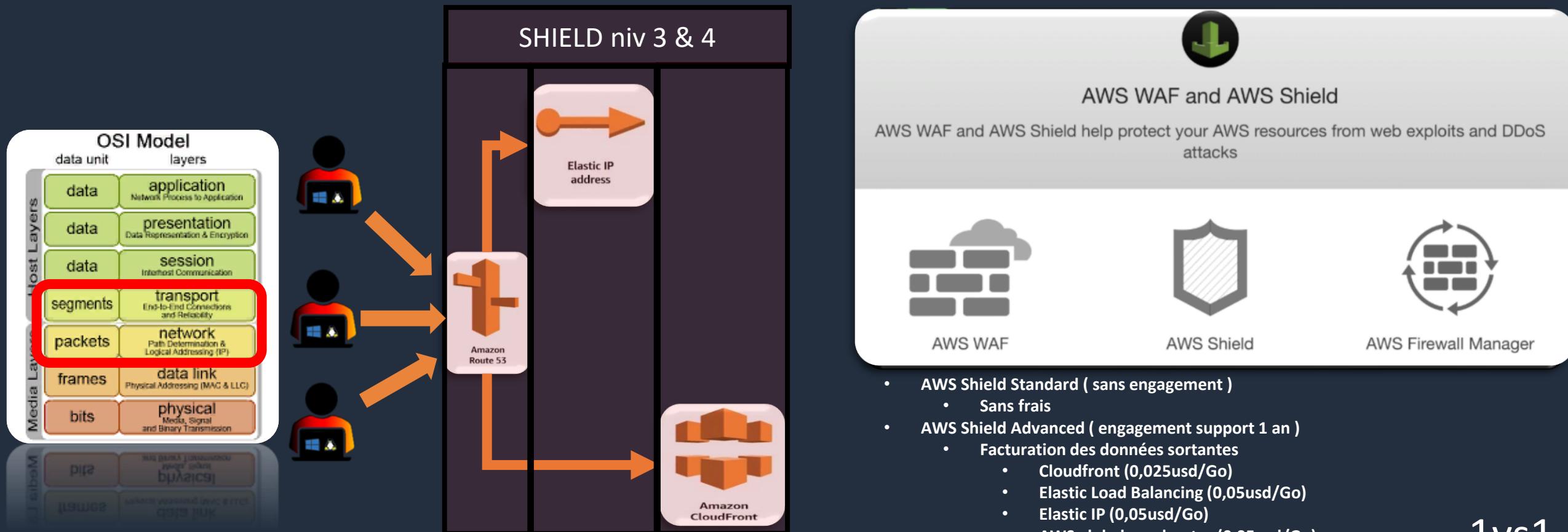
Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

AWS Shield

AWS Shield est un service de protection DDoS (Déni de service distribué) géré qui protège les applications s'exécutant dans AWS

1vsN



AWS WAF : pare-feu d'applications Web

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

AWS WAF - Web Application Firewall

AWS WAF est un pare-feu d'application Web qui aide à protéger les applications Web ou des API contre les failles Web les plus communes susceptibles d'affecter la disponibilité, de compromettre la sécurité ou de provoquer une surconsommation des ressources.



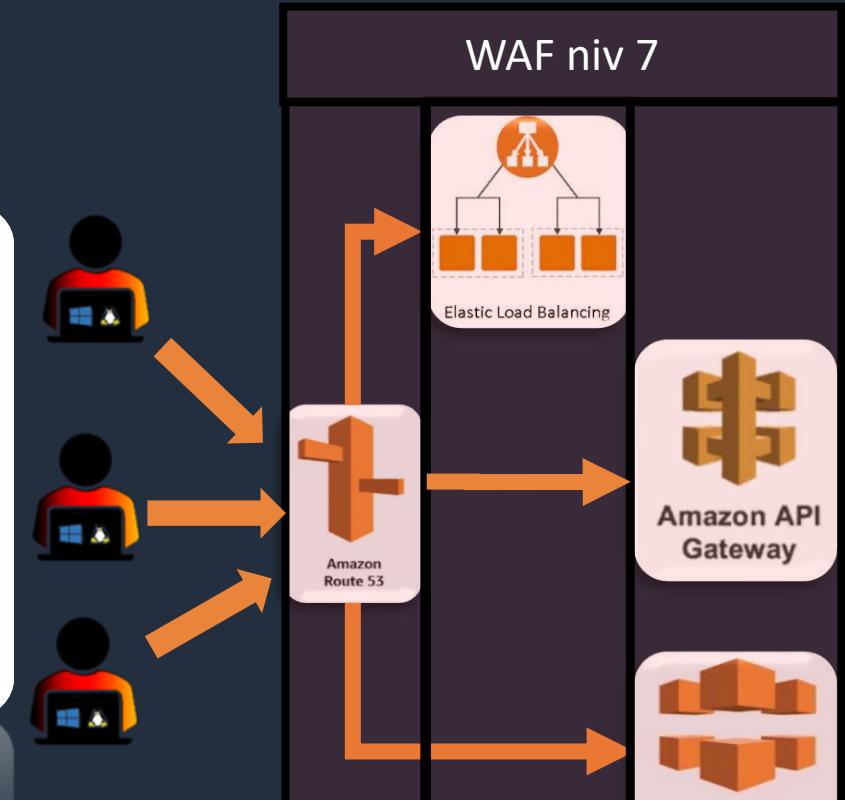
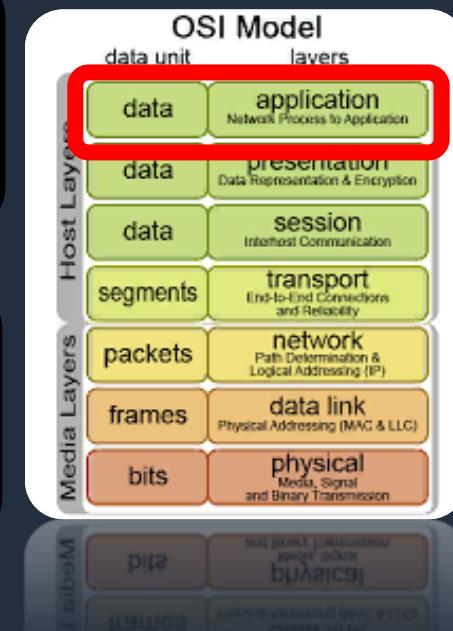
Détection
des attaques courantes



Analyses
les temps de réponses cloudfront



Filtre
Les requêtes http et https

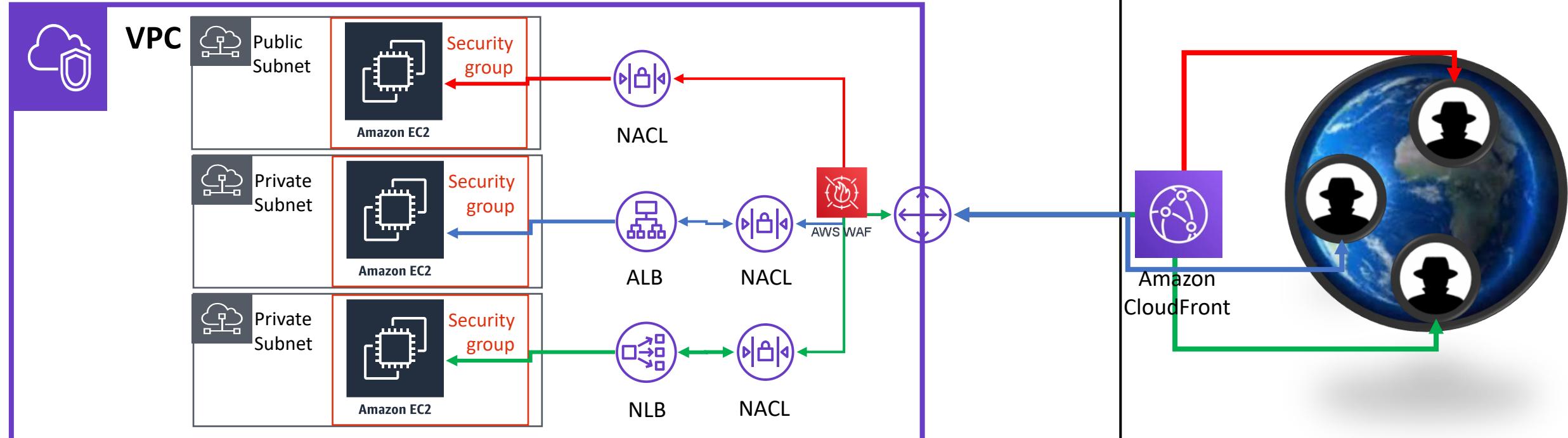




Sécurisation des environnements

En fonction de vos besoins vous n'allez pas utiliser les mêmes services en entrée depuis internet il sera donc important de savoir comment sécuriser en anticipant les attaques, et savoir quoi surveiller.

aws



AWS WAF peut être déployé sur Amazon CloudFront, l'équilibrEUR
de charge d'application (ALB) et Amazon API Gateway.



Amazon Inspector

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

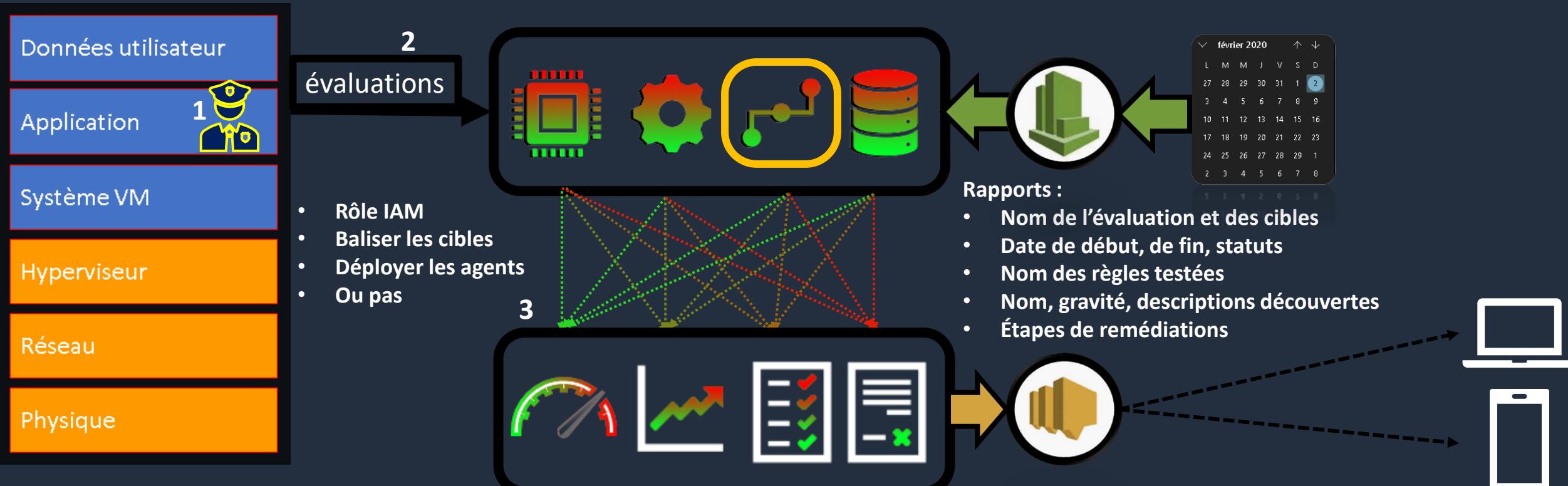
Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

Amazon Inspector

Amazon Inspector évalue les vulnérabilités et permet d'améliorer la sécurité et la conformité des ressources AWS

1. Pré requis (rôle iam, balises, agents)
2. Préparer l'orientation de l'évaluation (packages)
3. Création d'un modèle d'évaluation
4. Lancer l'évaluation
5. Récupérer les rapports => appliquer les recommandations



Déploiement infrastructures & découplage applicatif



AWS CloudFormation

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>



Introduction

Mots clés :

- Simplifie
- Tâches répétitives
- provisionnement



AWS CloudFormation



Introduction

- AWS Management Console
- AWS CLI
- AWS SDK / API



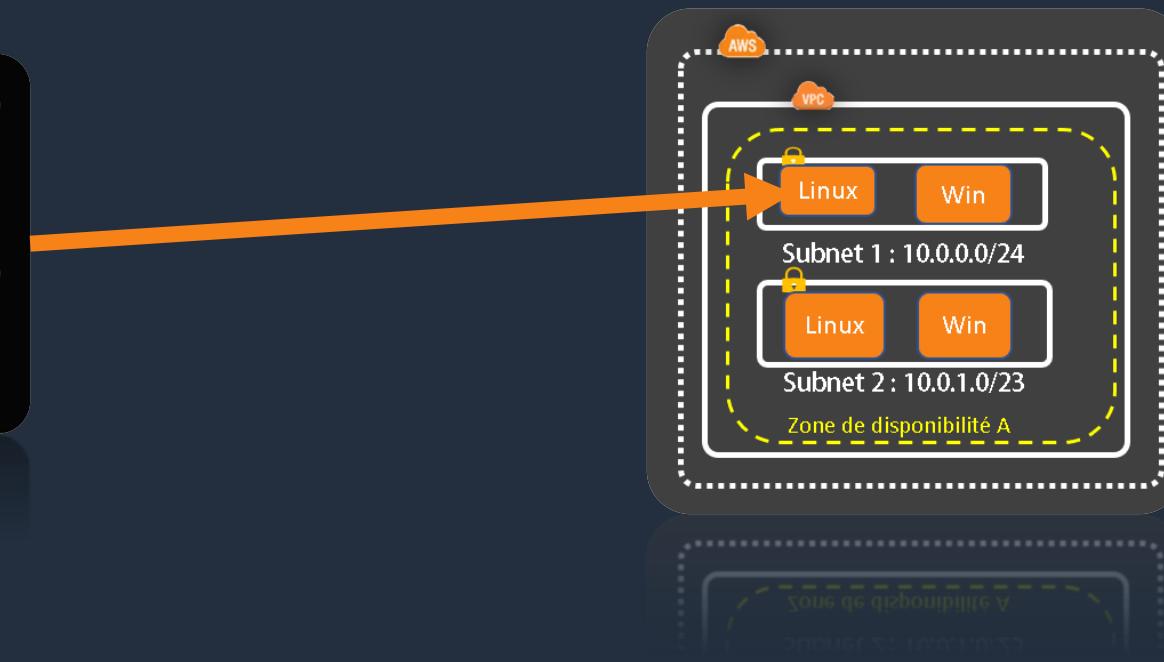
AWS CloudFormation



Introduction

- Modèle (Template)

```
{  
    "AWSTemplateFormatVersion" : "2010-09-09",  
    "Description" : "A simple EC2 instance",  
    "Resources" : {  
        "MyEC2Instance" : {  
            "Type" : "AWS::EC2::Instance",  
            "Properties" : {  
                "ImageId" : "ami-0ff8a91507f77f867",  
                "InstanceType" : "t1.micro"  
            }  
        }  
    }  
}
```

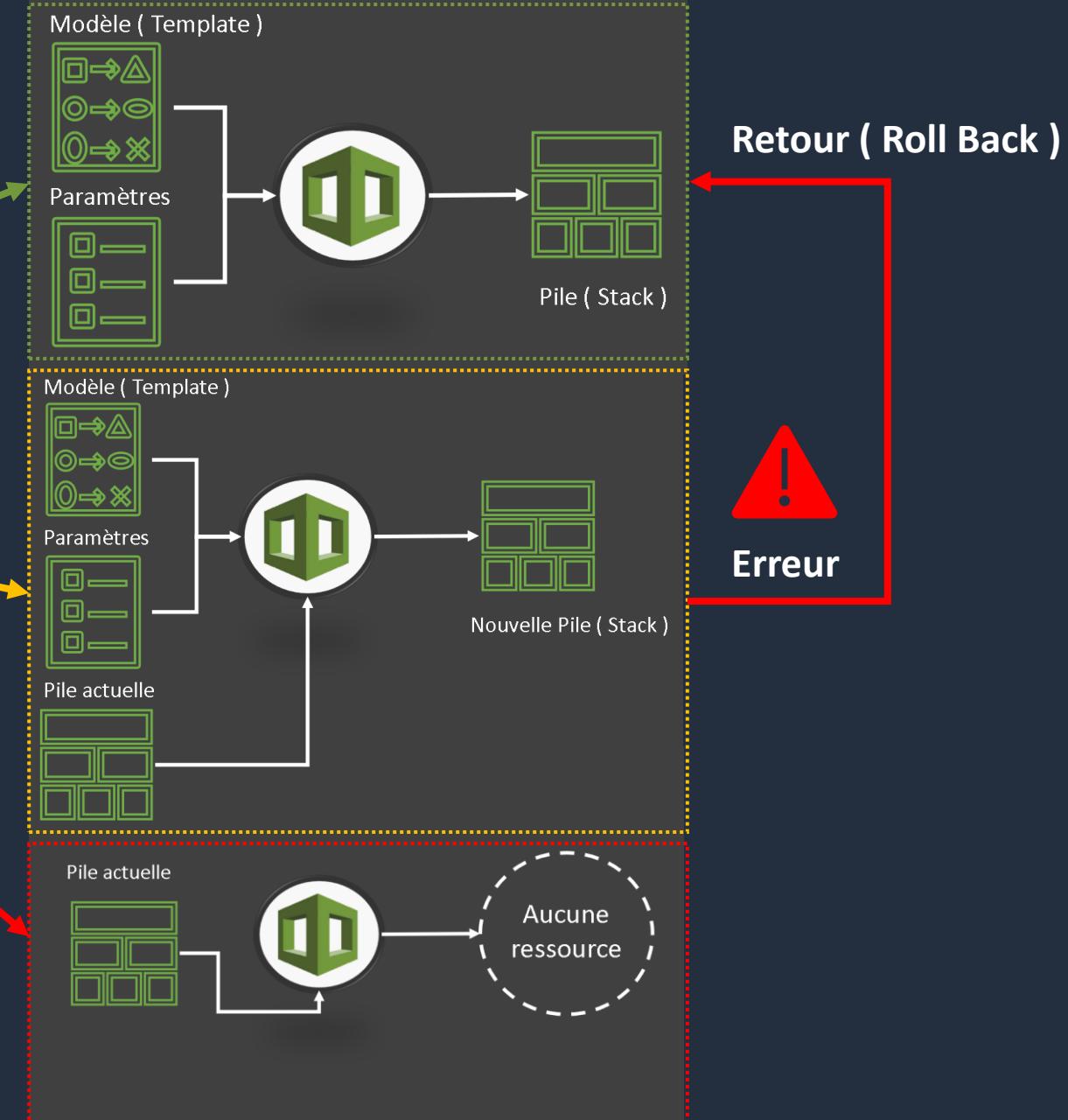


AWS CloudFormation



Fonctionnalités

- Créer
- Mettre à jour
- Supprimer

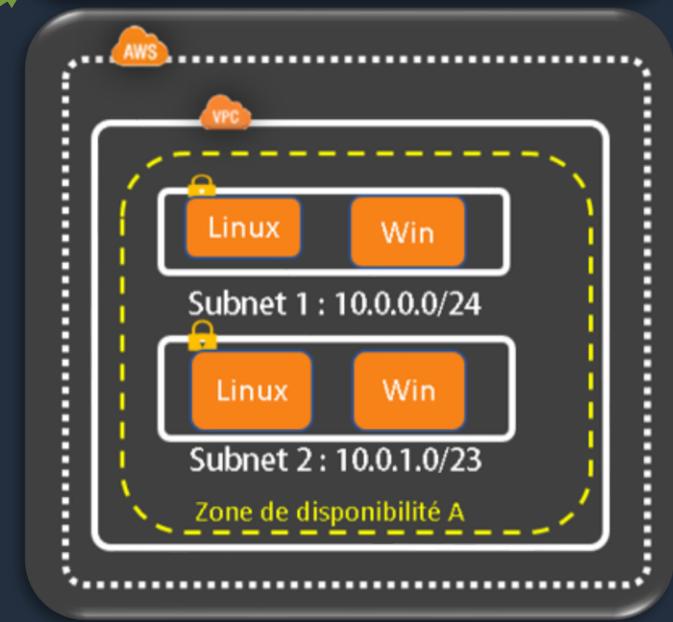
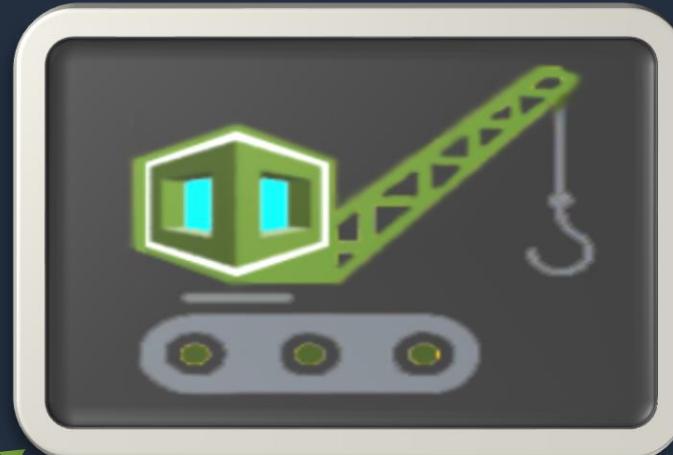


AWS CloudFormation



Sources

```
{  
  "AWSTemplateFormatVersion": "2010-09-09",  
  "Description": "A simple EC2 instance",  
  "Resources": {  
    "MyEC2Instance": {  
      "Type": "AWS::EC2::Instance",  
      "Properties": {  
        "ImageId": "ami-0ff8a91507f77f867",  
        "InstanceType": "t1.micro"  
      }  
    }  
  }  
}
```



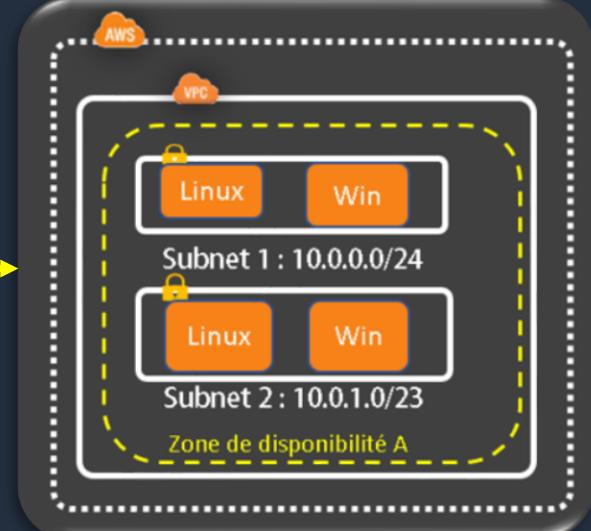
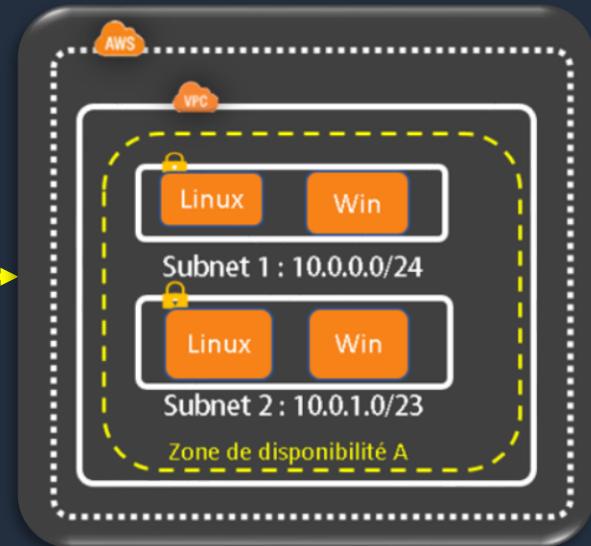
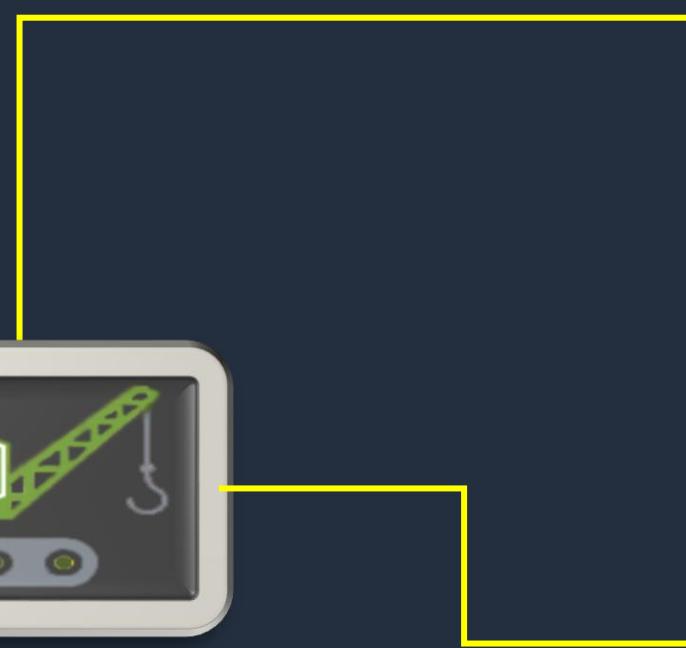
- Créer
- Mettre à jour
- Supprimer

AWS CloudFormation



Cas d'usage

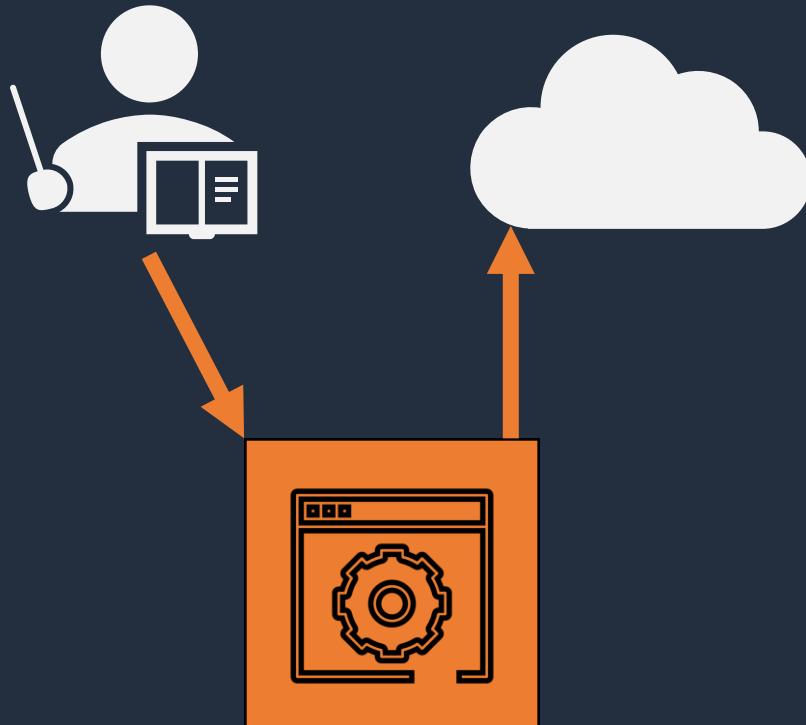
```
{  
  "AWSTemplateFormatVersion": "2010-09-09",  
  "Description": "A simple EC2 instance",  
  "Resources": {  
    "MyEC2Instance": {  
      "Type": "AWS::EC2::Instance",  
      "Properties": {  
        "ImageId": "ami-0ff8a91507f77f867",  
        "InstanceType": "t1.micro"  
      }  
    }  
  }  
}
```



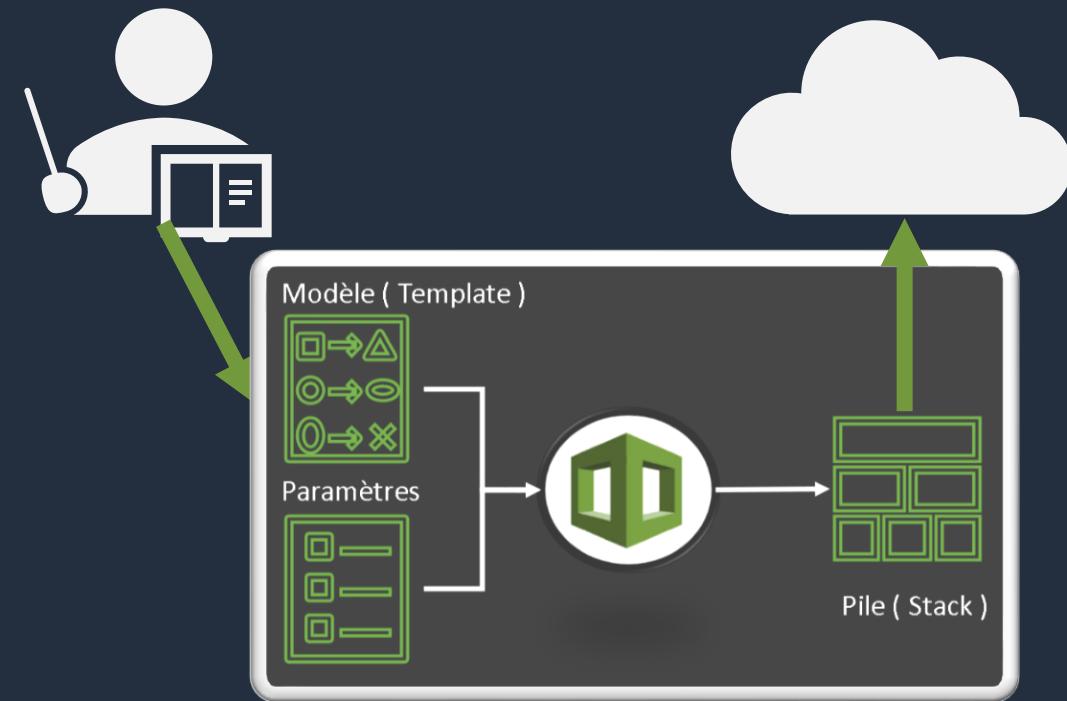
AWS CloudFormation



Cas d'usage



Sans Cloudformation



Avec Cloudformation



AWS CloudFormation

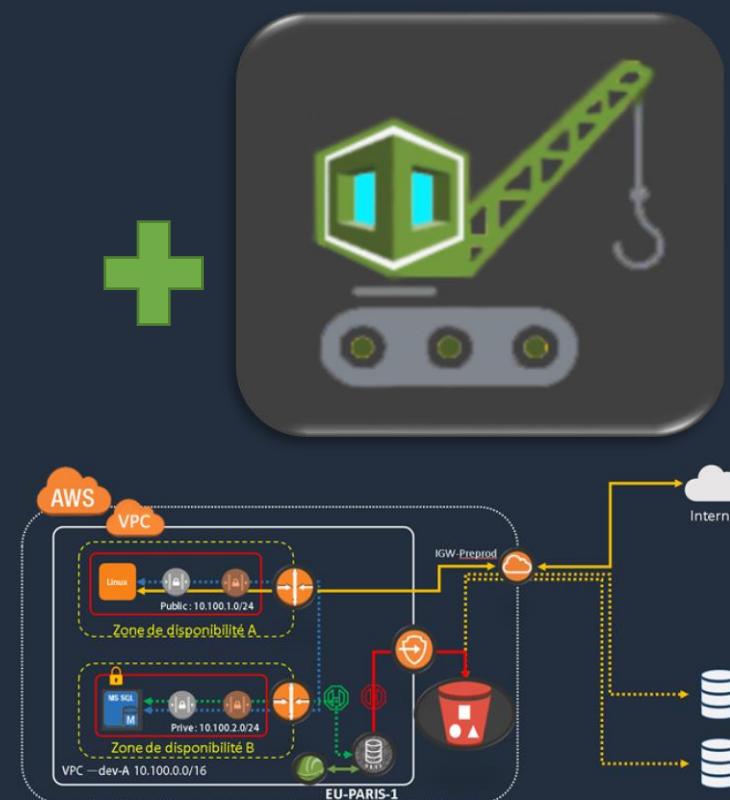


Astuce

The screenshot displays the AWS CloudFormation Quick Start catalog, which contains numerous pre-built stacks categorized by provider and service. The visible sections include:

- Quick Start**: Active Directory, Acqueon Engagement Cloud (AEC), Lac de données avec Talend Big Data Platform.
- CloudStax Cache pour Redis**, Cloudera EDH, HERE Location Suite.
- Enregistrement Compound**, Cluster géré Dynatrace, Drupal.
- Kubernetes par Heptio**, Aviatrix FQDN Egress Filtering sur AWS, Boîte à outils Aria Solutions.
- Hôtes bastions Linux**, Jupiter, Oracle Database.
- DEV STACK**, **TEST STACK**, **PROD STACK** (under NETWORK STACK, SECURITY STACK, DATABASE STACK).

Each stack entry includes a logo, a brief description, and a note indicating it was created by AWS or a partner.





Cloudformation

- Scripter votre environnement (stack)
- Démarrage rapide préconfiguré (quick start aws)
- Déploie votre environnement pour vous
- Supprime l'environnement lors de la suppression d'un stack



Cloudformation

Bénéfices :

- Parfaite parité Dev, Test, Prod
- Déploiement en un click
- Réduction du temps de déploiement
- Rend toutes infrastructures utilisables pour des réaliser des tests
- Milliers de modèles disponibles

AWS CodeDeploy

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

AWS CodeDeploy

Automatiser les déploiements d'application vers divers services de calcul EC2, Fargate, AWS Lambda ou vers des instances s'exécutant sur site (on premise).

- Déploiements automatisés des instances
- Requiert l'installation des instances avec agents
- Déploiements reproductibles sur N instances
- Mise à l'échelle automatique (intégré avec auto scaling)
- Déploiements sur site (on premise) ou dans le cloud AWS
- Indépendant de la plate-forme et du langage
- Limiter les temps d'arrêt (blue / green)
- Contrôle centralisé
- Sans frais

V1 > V2

AWS Systems Manager

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

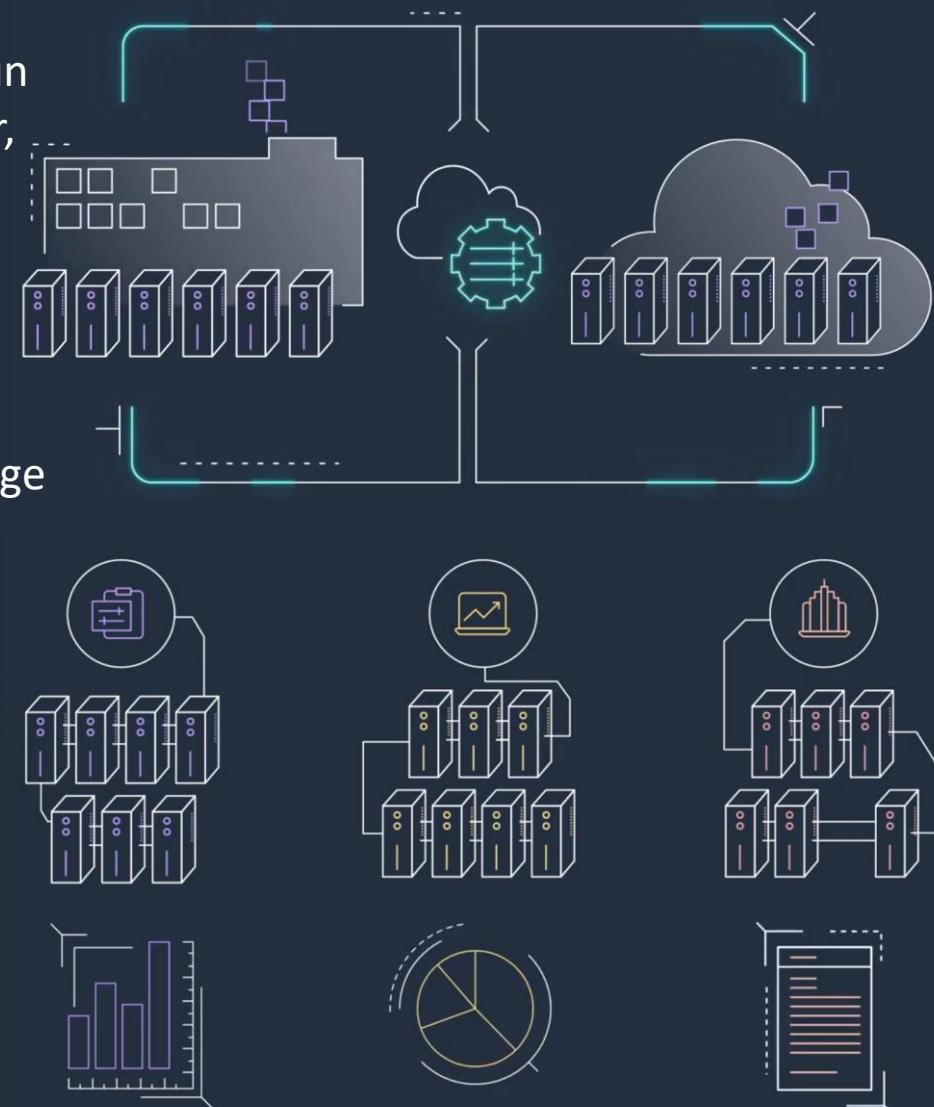
Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

AWS Systems Manager

Simplifie la gestion des ressources et des applications, raccourcit le délai de détection et de résolution des problèmes opérationnels et facilite l'exploitation et la gestion de votre infrastructure de façon sécurisée à grande échelle.

- Suite de services à destination des administrateurs systèmes (OpsCenter, Explorer, resources groups, AppConfig, dashboard Inventory, Automation, Run command, session manager Maintenance window, Distributor, State manager, Parameter store)
- Gestion des ressources on premise et dans le cloud (hybride)
- D'afficher les données opérationnelles de plusieurs services AWS
- D'automatiser les tâches opérationnelles pour vos ressources AWS
- Regrouper des ressources par application, business unit, environnement
- Afficher les données opérationnelles à des fins de surveillance et de dépannage
- Maintenir une configuration cohérente de vos instances
- Support Windows et Linux avec un agent installé
- Connection avec un ITSM comme Jira service desk



The screenshot displays the AWS Systems Manager console with two open tabs: 'Inventory' and 'Compliance'.
The 'Inventory' dashboard provides a summary of managed instances, including a pie chart showing the status of inventory enabled instances (green for Enabled, red for Disabled), and bar charts for inventory coverage per type (AWS/AWB Component, AWS Application, AWS File, instanceDetailedInformation, AWS InstanceInformation).
The 'Compliance' dashboard filtering section allows users to filter results by Compliance type, Patch group, or Resource group. It includes a 'Compliance resources summary' table and a 'Details overview for resources' section.

AWS OpsWorks

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

AWS OpsWorks

Service de gestion des configurations qui fournit des instances gérées de Chef et Puppet.

- Gestion des infrastructures par code (via des cookbooks)
- Dépôt pour le code (cookbook repository)
- Pile Opswork (infrastructure applicative)
- ALB (txt) < configuration + listes des instances
- EC2 (txt) < AMI + bootstrap + EBS volumes + App
- RDS (txt) < instances de base de données
- Fonctionne aussi avec les ressources on premise

The screenshot shows the AWS OpsWorks service page. At the top, there's a brief introduction: "AWS OpsWorks is a configuration management service that helps you build and operate highly dynamic applications, and propagate changes instantly." Below this, it says "AWS OpsWorks provides three solutions to configure your infrastructure:" followed by three options:

- OpsWorks Stacks**: Define, group, provision, deploy, and operate your applications in AWS by using Chef in local mode. Includes a "Go to OpsWorks Stacks" button and a "Learn more about OpsWorks Stacks" link.
- OpsWorks for Chef Automate**: Create Chef servers that include Chef Automate premium features, and use the Chef DK or any Chef tooling to manage them. Includes a "Go to OpsWorks for Chef Automate" button and a "Learn more about OpsWorks for Chef Automate" link.
- OpsWorks for Puppet Enterprise**: Create Puppet servers that include Puppet Enterprise features. Inspect, deliver, update, monitor, and secure your infrastructure. Includes a "Go to OpsWorks for Puppet Enterprise" button and a "Learn more about OpsWorks for Puppet Enterprise" link.



Amazon Simple Notification Service

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

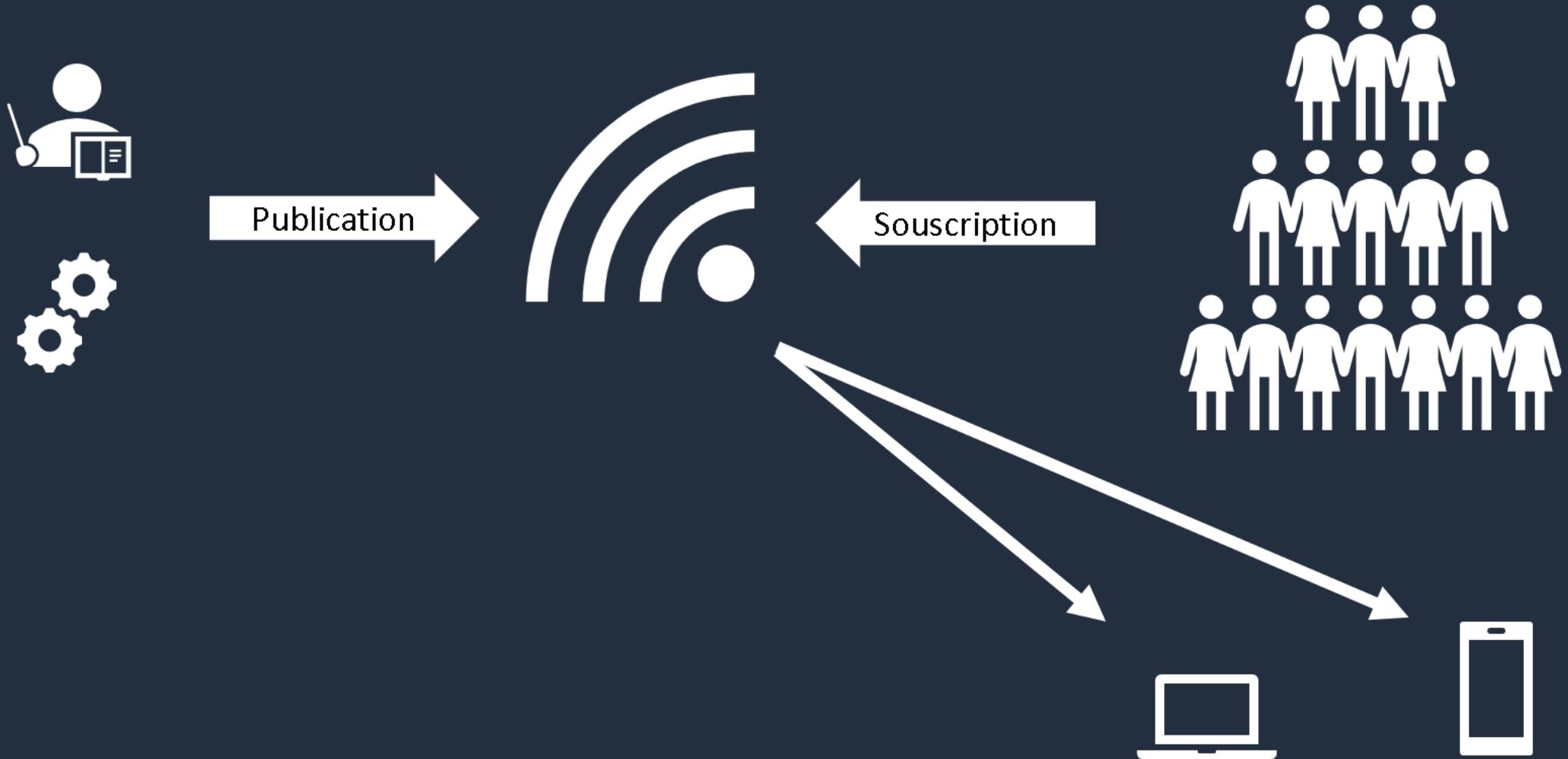
Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>



SNS : Simple Notification Service



Amazon Simple Queue Service

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

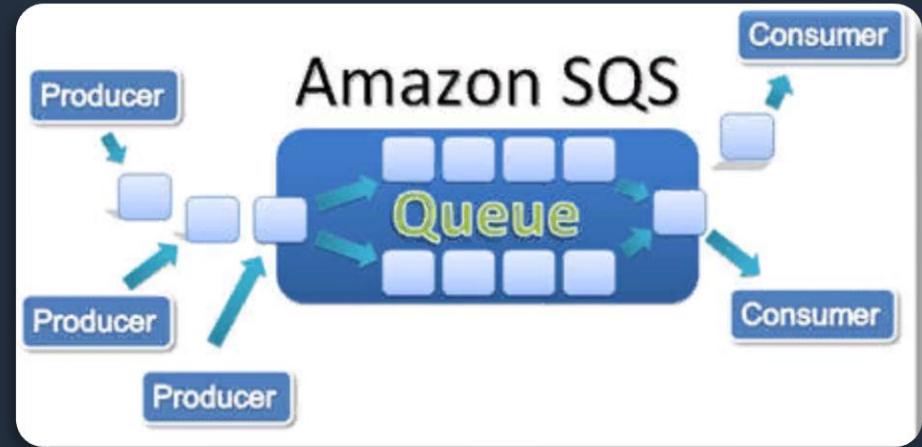
Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

Amazon Simple Queue Service

Propose une file d'attente hébergée fiable et hautement évolutive pour stocker les messages qui transitent entre des applications ou des micro services. (**1^{er} service AWS**)

- Service Web géré par AWS
- Permet de recevoir et de stocker des messages
- 2 intervenants Producteur & Consommateur
- Via le SDK les messages sont traités puis supprimés
- Peut conserver un message pendant 14 jours (4 /default)
- Dispose d'un mode séquentiel (fifo) ou parallèle
- Garantie que le message est transmis au moins une fois





AMAZON Simple Queue Service - SQS

Service de file d'attente de messagerie entièrement géré qui vous permet de **découpler** et mettre à l'échelle des **microservices**, des systèmes décentralisés et des applications sans serveur.

Amazon SQS propose deux types de files d'attente pour différents besoins d'applications :

Files d'attente standard ; Débit illimité ; Remise au moins une fois ; Ordre dans la mesure du possible (Qte illimité)

Files d'attente FIFO ; Haut débit ; Traitement en une seule fois ; Premier entré, premier sorti (Qte 300 tps par défaut)

- Messages : Nombre illimité de files d'attente et de messages dans n'importe quelle région
- Taille du corps des messages : les corps des messages peuvent contenir jusqu'à 256 Ko de texte dans n'importe quel format.
- Lots : Chaque « lot » de 64 Ko de données libres est facturé comme 1 demande.
- Envoyer, recevoir ou supprimer des messages par lots d'un maximum de 10 messages ou 256 Ko.
- Attente longue durée (long polling) permet de réduire le coût d'utilisation de Amazon SQS en éliminant les réponses vides
- Conserver les messages dans les files d'attente jusqu'à 14 jours. (4 jours par défaut)
- Envoyer et lire des messages simultanément
- Verrouillage des messages : lorsqu'un message est reçu, il reste verrouillé pendant toute la durée de son traitement.
- Partage de files d'attente : Amazon SQS de manière anonyme ou avec des comptes AWS spécifiques.
- Chiffrement (SSE) : protéger le contenu des messages présents dans les files d'attente Amazon SQS à l'aide de AWS KMS.



Files d'attente standard



Files d'attente FIFO

Amazon Simple Workflow Service (SWF)

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>



AWS Simple WorkFlow Service - SWF

aide les développeurs à concevoir, exécuter et mettre à l'échelle les travaux en arrière-plan qui présentent des étapes parallèles ou séquentielles. (traitement média, backend webapp, business process, migration)

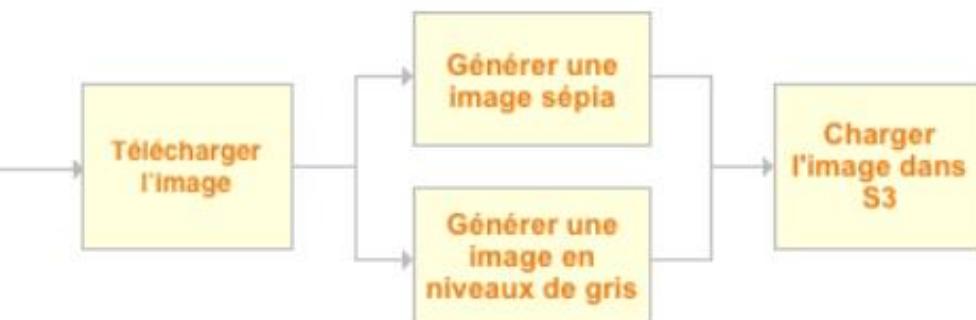
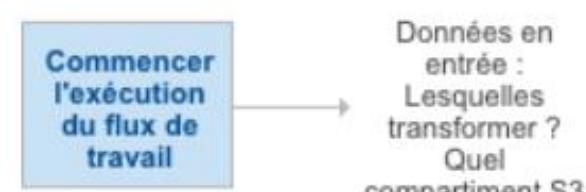
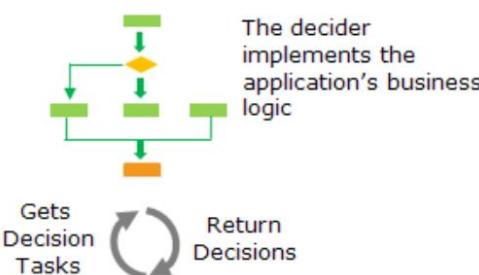
Workflow starters, Deciders, Activity Workers :

- Un workflow est l'automatisation d'un processus d'entreprise
- Un domaine est un ensemble de flux de travail connexes.
- Les actions sont les tâches individuelles entreprises pour exécuter un flux de travail.
- Les travailleurs (workers) d'activité sont les morceaux de code qui mettent réellement en œuvre les tâches.
- Un Décideur met en œuvre la logique de coordination d'un Workflow.

Amazon SWF fait office de plate-forme de coordination pour tous les différents composants de votre application :

- Conservation de l'état de l'application
- Suivi des exécutions des workflows et consignation de leur progression
- Conservation et répartition des tâches
- Contrôle de l'affectation des tâches à exécuter sur vos hôtes d'applications
- Une exécution peut durer jusqu'à un an (vs 14 jours pour SQS)

SQS : decoupled and microservices
SWF : Human action during workflow
Step Function : External signals or child processes return value to the parent



AWS Step Functions

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>



AWS Step Functions

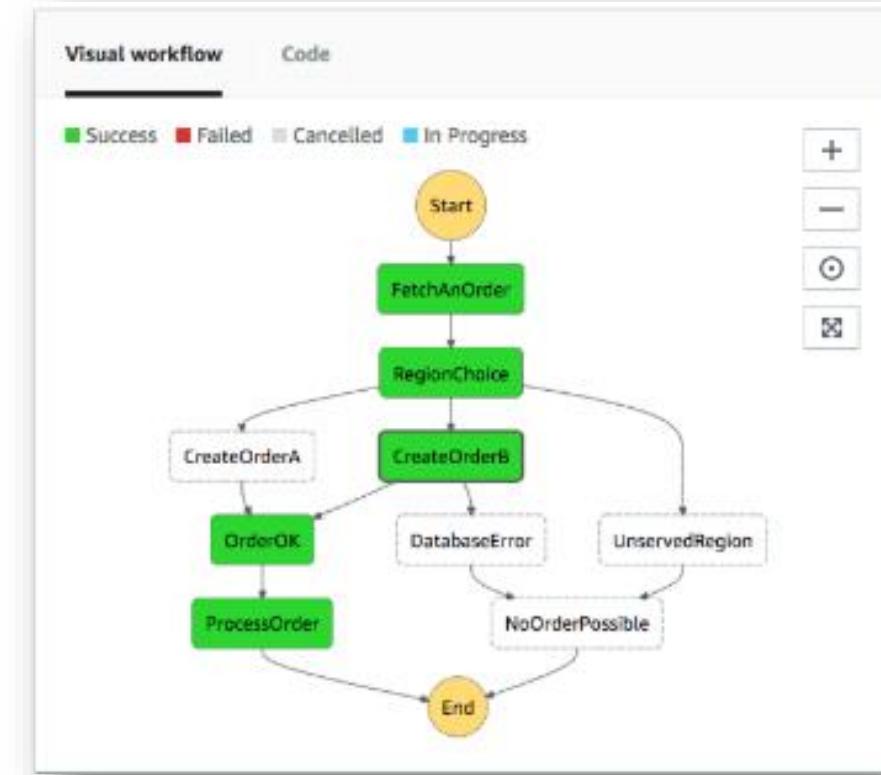
AWS Step Functions est un orchestrateur de fonctions **sans serveur** qui permet de séquencer facilement les fonctions AWS Lambda et les multiples services AWS dans les applications stratégiques de l'entreprise.

Principales caractéristiques d'AWS Step Functions :

- Step Functions repose sur les concepts de tâches et de **machines d'état**.
- Vous définissez les **machines d'état** à l'aide du Langage des états basé sur JSON
- La console Step Functions affiche une vue graphique de la structure de votre machine d'état. Cela permet de vérifier visuellement la logique de votre machine d'état et de surveiller les exécutions.
- États : Pass – Tâches : choice, attente, succeed, Fail, parallel, Map
- Déployer un projet **d'approbation humaine** qui autorise une exécution AWS Step Functions à s'interrompre au cours d'une tâche, et à attendre qu'un utilisateur réponde à un e-mail. (**jusqu'à 1 an**)

Cas d'usage : Moderniser un monolithe, Orchestration d'applications , Traitement de données , Automatiser les tâches

Interagit avec les principaux services : AWS **Lambda**, Amazon ECS, AWS Fargate, Amazon DynamoDB, Amazon SNS and Amazon SQS, AWS Batch and AWS Glue, Amazon EMR, Amazon SageMaker



Amazon API Gateway

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

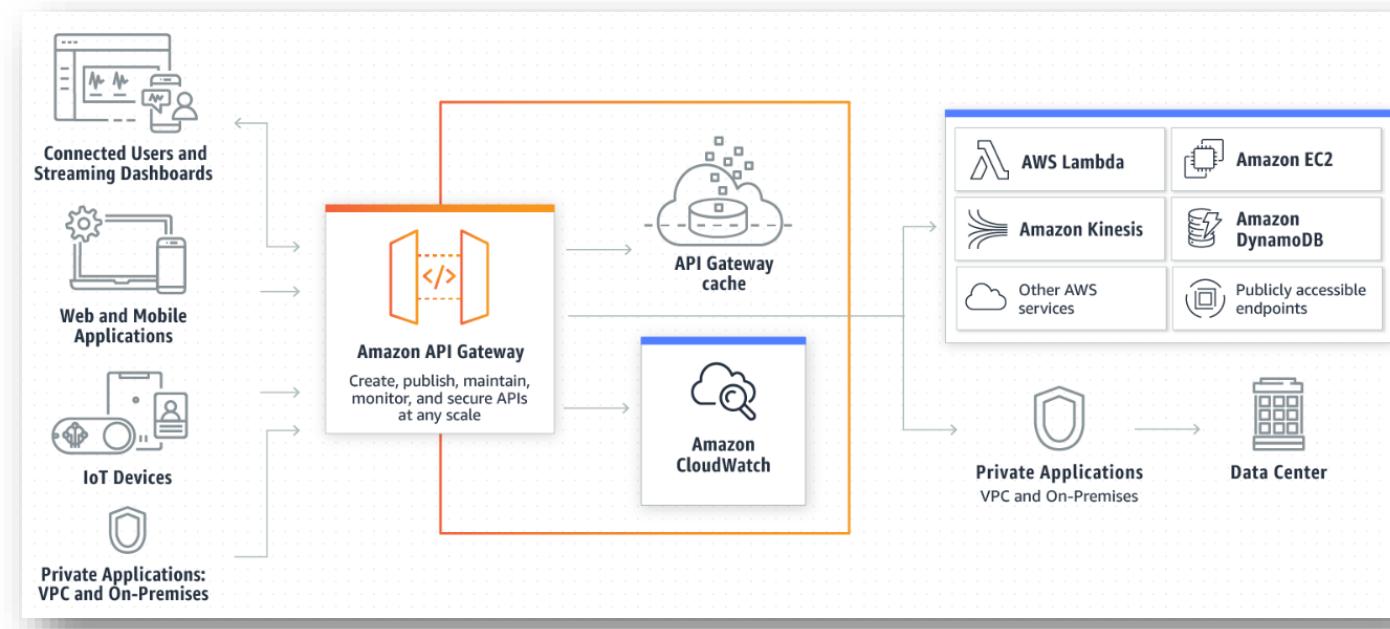


AMAZON API Gateway

Amazon API Gateway est un service entièrement géré, qui permet aux développeurs de créer, publier, gérer, surveiller et sécuriser facilement des API à n'importe quelle échelle.

- API RESTful (stateless) : Le standard REST a été créé en 2000 par Roy Fielding dans sa thèse "Architectural Styles and the Design of Network-based Software Architectures". ("RESTful" en raison du haut niveau de certification)
- API WEBSOCKET (stateful) : Une connexion WebSocket peut s'étendre verticalement sur un seul serveur, tandis que REST, qui est basé sur HTTP, peut s'étendre horizontalement.

- Intégrations privées avec AWS ELB et AWS Cloud Map
- Résilience
- Création et déploiement faciles d'API
- Surveillance du fonctionnement de l'API (cloudwatch)
- Support SSL / TLS certs
- **Support CORS (multiple domaine)**
- **Support Cache (TTL settings)**
- Réduire le nbre d'appels pour prévenir des attaques
- Autorisation AWS
- Clés d'API pour les développeurs tiers
- Génération de kits SDK
- Gestion du cycle de vie d'une API
- **Faible coût et mise à l'échelle automatique**



Extensions API Gateway pour OpenAPI

Gestion dans le cloud



- █ Gestion et gouvernance
 - AWS Organizations
 - CloudWatch
 - AWS Auto Scaling
 - CloudFormation
 - CloudTrail
 - Config
 - OpsWorks
 - Service Catalog
 - Systems Manager
 - AWS AppConfig
- █ Trusted Advisor
 - Control Tower
 - AWS License Manager
 - AWS Well-Architected Tool
 - Personal Health Dashboard ↗
 - AWS Chatbot
 - Launch Wizard
 - AWS Compute Optimizer

Amazon CloudWatch

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

Amazon CloudWatch

Observabilité de vos ressources et applications AWS sur AWS et sur site



AWS CLOUDWATCH

fournit des données et informations exploitables dont vous avez besoin pour surveiller vos applications, réagir aux variations de performance sur l'ensemble du système, optimiser l'utilisation des ressources et avoir une appréciation unifiée de la santé opérationnelle.

BASIC
5 Min

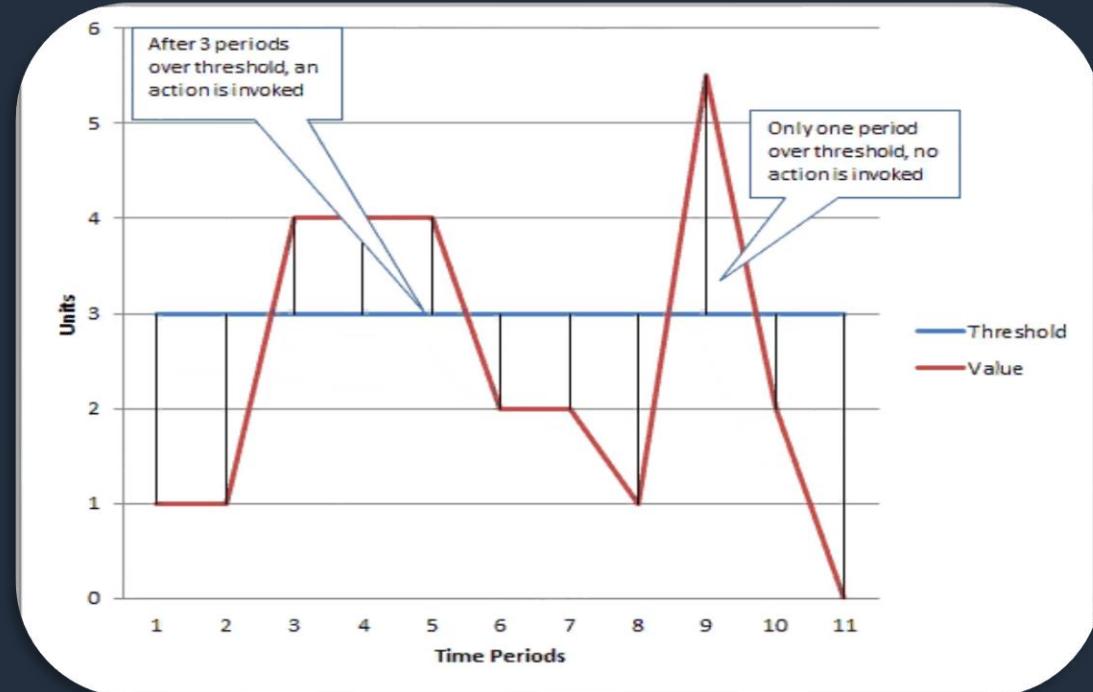
ADVANCED
1 Min

Cas d'usage

- Surveillance et dépannage d'infrastructure
- Amélioration du temps moyen de résolution
- Optimisation proactive des ressources
- Surveillance des applications
- Analyse des journaux

Avantages :

- Le moyen le plus simple de collecter des métriques dans AWS et sur site (on premise)
- Améliorer la performance opérationnelle et l'optimisation des ressources
- Obtenir des informations et gagner en visibilité opérationnelle
- Récupérer des informations exploitables dans des journaux
- Observabilité sur une plate-forme unique sur l'ensemble des applications et de l'infrastructure



AWS CloudTrail

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

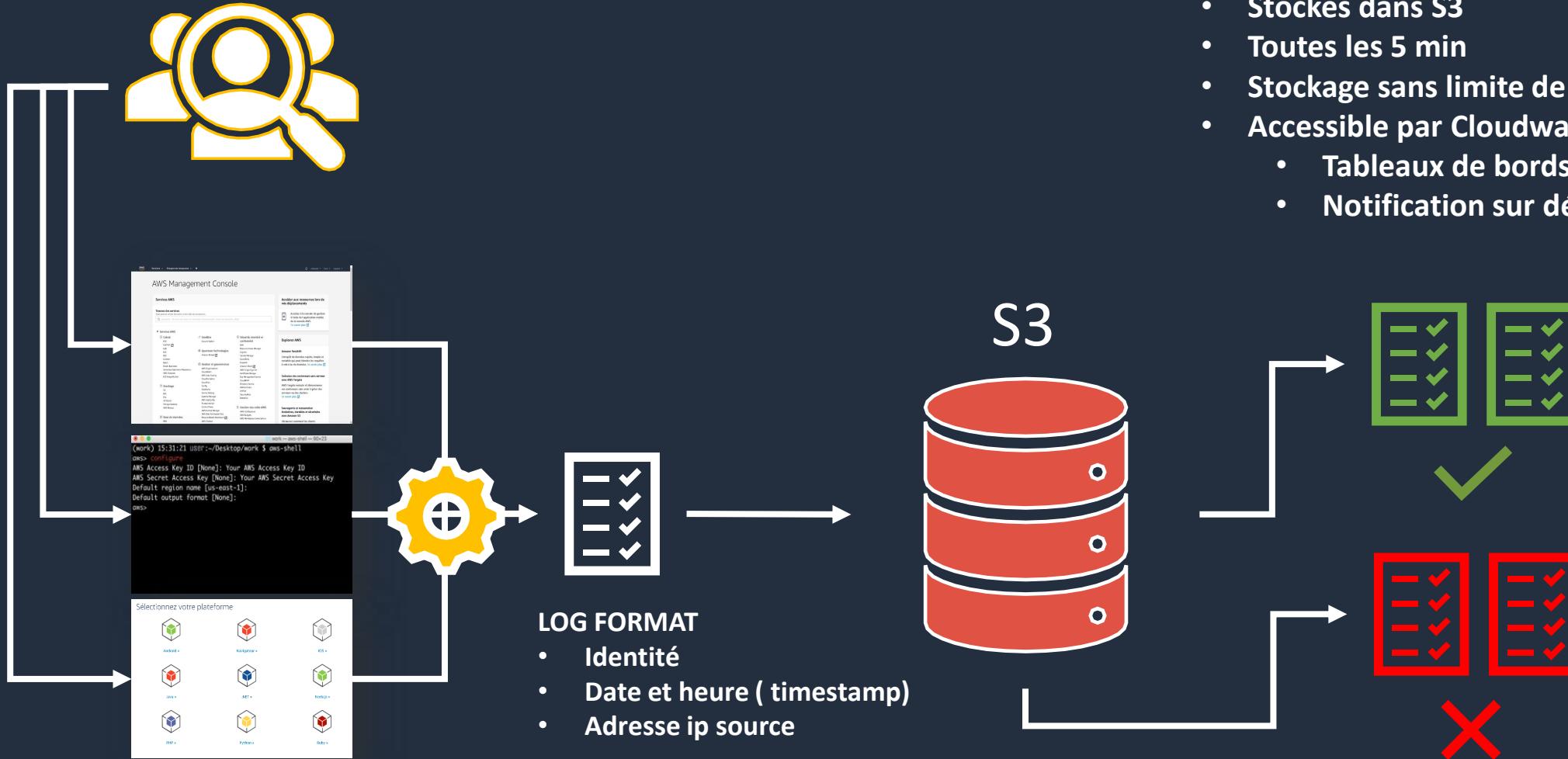
Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

AWS CloudTrail

Suivi de l'activité des utilisateurs et de l'utilisation des API



Journaux CloudTrails (Logs) – service global

- Stockés dans S3
- Toutes les 5 min
- Stockage sans limite de durée imposée
- Accessible par Cloudwatch :
 - Tableaux de bords
 - Notification sur détection via SNS

AWS CLOUDTRAIL

Vous pouvez :

- Enregistrer les événements relatifs à votre compte AWS
- Enregistrer ses informations depuis plusieurs régions
- Surveiller l'intégrité des fichiers logs (modification ou suppression)
- Chiffrer vos fichiers clouptrail
- Accélérer les procédures d'enquête suite aux incidents
- Envoyer des réponses rapides aux demandes des responsables de l'audit.
- Interagir avec cloudwatch logs et events ou Lambda via S3 events
- Créez un journal de suivi pour conserver un enregistrement de ces événements.

Avec ce journal de suivi : (insight)

- créer des métriques d'événement
- déclencher des alertes
- créer des flux de travail d'événement
- créer un journal de suivi pour une organisation (en vous connectant avec le compte principal pour AWS Organizations)

AWS Config

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

AWS CONFIG

AWS Certificate manager	
Cloudtrail	EBS
	EC2
	EC2 system manager
	ELB
	IAM
	Amazon redshift
	RDS
	S3
	VPC

Vous disposez :

- d'une liste exhaustive des ressources que vous utilisez
- d'une liste précise des vulnérabilités potentielles sur ces ressources
- des Inter dépendances entre ces ressources
- d'un historique complet des changements opérés sur ces ressources
- validation de la conformité envers les lois en vigueurs
- de toutes les informations requises à mettre à disposition en cas d'audit

Fonctionnalités :

- Inventaire avec la liste des modifications
- Stock l'historique des configurations (json)
- One click snapshots (delta) instant T
- Notification en cas de changements
- Intégré avec clouptrail, analyse la sécurité
- Conception de règle de conformité



AWS Trusted Advisor

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

AWS Trusted Advisor



Access to 7 core Trusted Advisor checks

Features	Basic Current plan	Developer	Business	Enterprise
Customer service and communities	24x7 access to customer service, documentation, whitepapers, and support forums	24x7 access to customer service, documentation, whitepapers, and support forums	24x7 access to customer service, documentation, whitepapers, and support forums	24x7 access to customer service, documentation, whitepapers, and support forums
Best practices	Access to 7 core Trusted Advisor checks	Access to 7 core Trusted Advisor checks	Access to all Trusted Advisor checks	Access to all Trusted Advisor checks

Access to all Trusted Advisor checks

- Load balancer non utilisé facturé à l'heure
- ENI / elastic ip non associée facturée à l'heure
- Utilisation anormalement haute d'une instance EC2
- MFA non activé
- Gestion des stratégies de mot de passe non actives
- Assurer que vos sauvegardes sont bien actives



Destinataires

- Contact chargé de la facturation: Configurer l'adresse e-mail
- Contact chargé des transactions : Configurer l'adresse e-mail
- Contact chargé de la sécurité: Configurer l'adresse e-mail



AWS Personal Health Dashboard

Est un service de Calcul Stockage Réseau Gestion Sécurité Global Oui Non (region)

Fonctionnalités :

Avantages :

Tarification Oui Non (Gratuit) Non (mais paiement des ressources provisionnées)

Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

AWS Health Dashboard

- Tableau de bord complet
- Tous les services
- Toutes les régions

AWS Personal Health Dashboard

- Tableau de bord personnel
- Uniquement vos services utilisés
- Uniquement dans vos régions
- Listes des incidents en cours
- Changements planifiés
- Autres notifications (update)



Cadre de référence des architectures



Excellence
Opérationnelle



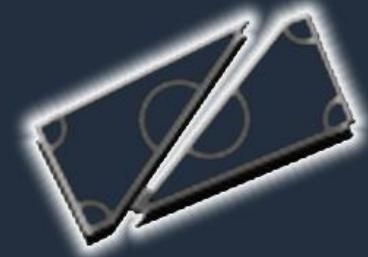
Sécurité



Fiabilité



Efficacité des
performances

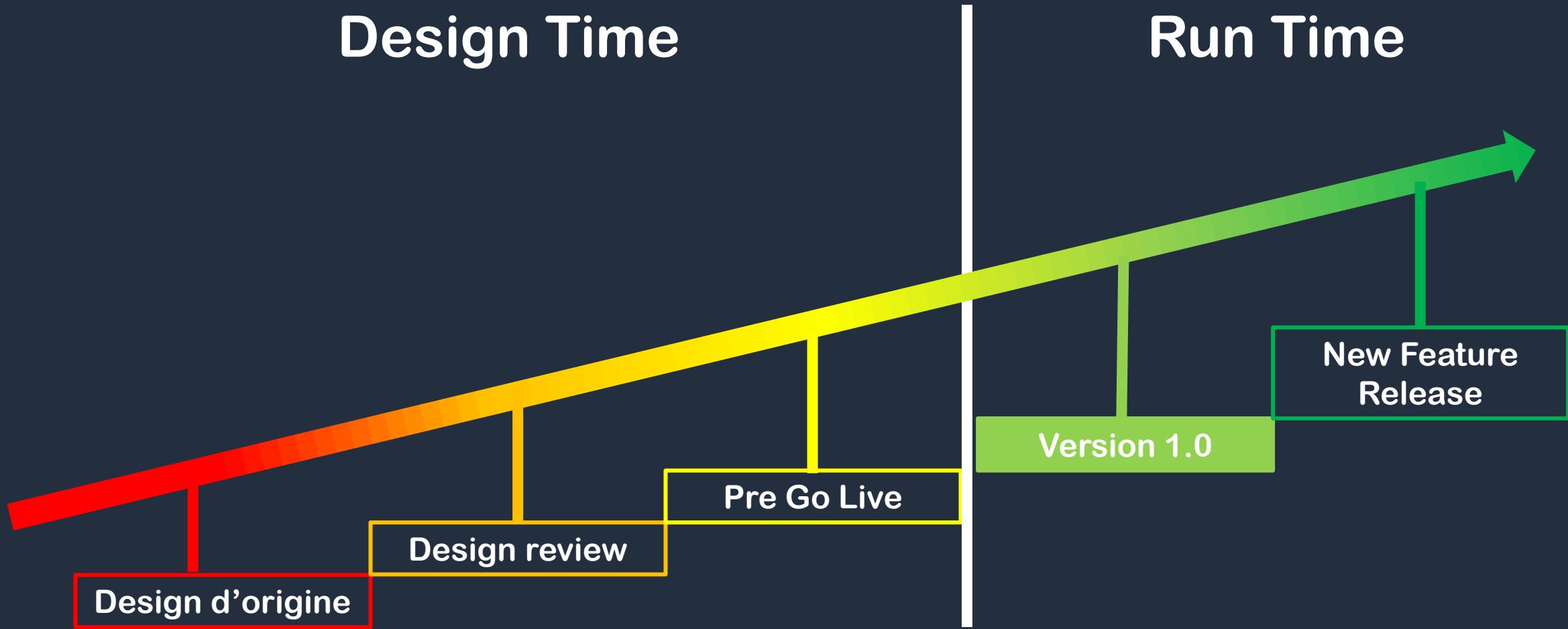


Optimisation
Des coûts



Outils de référence des architectures

Design Time



Run Time

Excellence opérationnelle

Les principes de conception :



- Effectuer des opérations en mode code
- Annoter la documentation
- Effectuer des changements fréquents, petits et réversibles
- Affiner fréquemment les procédures opérationnelles
- Anticiper l'échec
- Tirer les leçons de toutes les défaillances opérationnelles

Improvement Plan
Each day it's Day One

Excellence opérationnelle

Les bonnes pratiques :

- Préparer
- Exploiter
- Évoluer



Improvement Plan
Each day it's Day One

Sécurité



Les principes de conception :

- Mettre en place une identification forte
- Permettre la traçabilité
- Appliquer la sécurité à toutes les couches
- Automatiser les bonnes pratiques de sécurité
- Protéger les données en transit et au repos
- Tenez les gens à l'écart des données.
- Se préparer aux événements de sécurité

Improvement Plan
Each day it's Day One

Sécurité



Les bonnes pratiques :

- Gestion des identités et des accès
- Détection par contrôle
- Protection des infrastructures
- Protection des données
- Réponse sur incidents



Improvement Plan
Each day it's Day One

Fiabilité



Les principes de conception :

- Disposez de procédures de reprise d'activité testées
- Stratégie de récupération automatique après un échec
- Favoriser la mise à l'échelle horizontale (scale horizontally)
- Cessez de deviner la capacité
- Gérer le changement en automatisant les processus

Improvement Plan
Each day it's Day One

Fiabilité



Les bonnes pratiques :

- Adapter les ressources aux besoins
- Monitorer tous les composants
- Déploiements automatisés
- Validation des sauvegardes
- Implémenter la résilience
- Tester la résilience
- PRA

Improvement Plan
Each day it's Day One

Efficacité des performances



Les principes de conception :

- Démocratiser les technologies de pointe
- Passer à l'échelle mondiale en quelques minutes
- Utiliser des architectures « sans serveur » (serverless)
- Expérimenter plus souvent
- Approche technologique

Improvement Plan
Each day it's Day One

Efficacité des performances



Les bonnes pratiques :

- Sélection du type de ressources ad'hoc
- Benchmarking
- Load testing
- Monitoring

Improvement Plan
Each day it's Day One

Optimisation des coûts



Les principes de conception :

- Adopter un modèle de consommation
- Mesurer l'efficacité globale
- Arrêtez de dépenser de l'argent pour les activités liées aux centres de données
- Analyser et attribuer les dépenses aux bénéficiaires des ressources
- Utiliser des services gérés au niveau des applications

Improvement Plan
Each day it's Day One

Optimisation des coûts



Les bonnes pratiques :

- Sensibilisation aux dépenses
- Utilisation de ressources économiquement rentables
- Faire correspondre l'offre et la demande
- Optimiser au fil du temps

Improvement Plan
Each day it's Day One



Plan de reprise d'activité



RPO vs RTO

- Recovery Point Objectif
- Recovery Time Objective



R
P
O



RTO



Types de Plans :

- Backup and restore (8h-24h)
- Pilot light (4h-8h)
- Warm Standby (2h-4h)
- Multi Site (15min-1h)



Developer

Supérieur à 29,00 USD

- ou -

3 % d'utilisation mensuelle d'AWS

Business

Supérieur à 100,00 USD

- ou -

10 % de l'utilisation mensuelle d'AWS pour la première tranche allant de 0 USD à 10 000 USD

7 % de l'utilisation mensuelle d'AWS pour la tranche allant de 10 000 USD à 80 000 USD

5 % de l'utilisation mensuelle d'AWS pour la tranche allant de 80 000 USD à 250 000 USD

3 % d'utilisation mensuelle d'AWS au-delà de 250 000 USD

Enterprise

Supérieur à 15 000,00 USD

- ou -

10 % de l'utilisation mensuelle d'AWS pour la première tranche allant de 0 à 150 000 USD

7 % d'utilisation mensuelle d'AWS pour la tranche de 150 000 USD à 500 000 USD

7 % de l'utilisation mensuelle d'AWS pour la tranche allant de 500 000 USD à 1 000 000 USD

3 % d'utilisation mensuelle d'AWS au-delà de 1 000 000 USD



AWS Support Plans

BASIC

DEVELOPER

BUSINESS

ENTERPRISE

e-mail support
compte et
facturation jours
ouvrés

Conseils d'ordre général : sous 24 heures ouvrables

Système ralenti : sous 12 heures ouvrables

Accès par tél, e-mail et messagerie aux ingénieurs de support
24h/24 et 7j7

Système de production affecté sous 4 heures

Système de production inopérant sous 1 heure

Système vital inopérant
sous 15 minutes

Équipe de support concierge

Autoformation en ligne

gestionnaire technique de
compte

7 vérifications Trusted Advisor

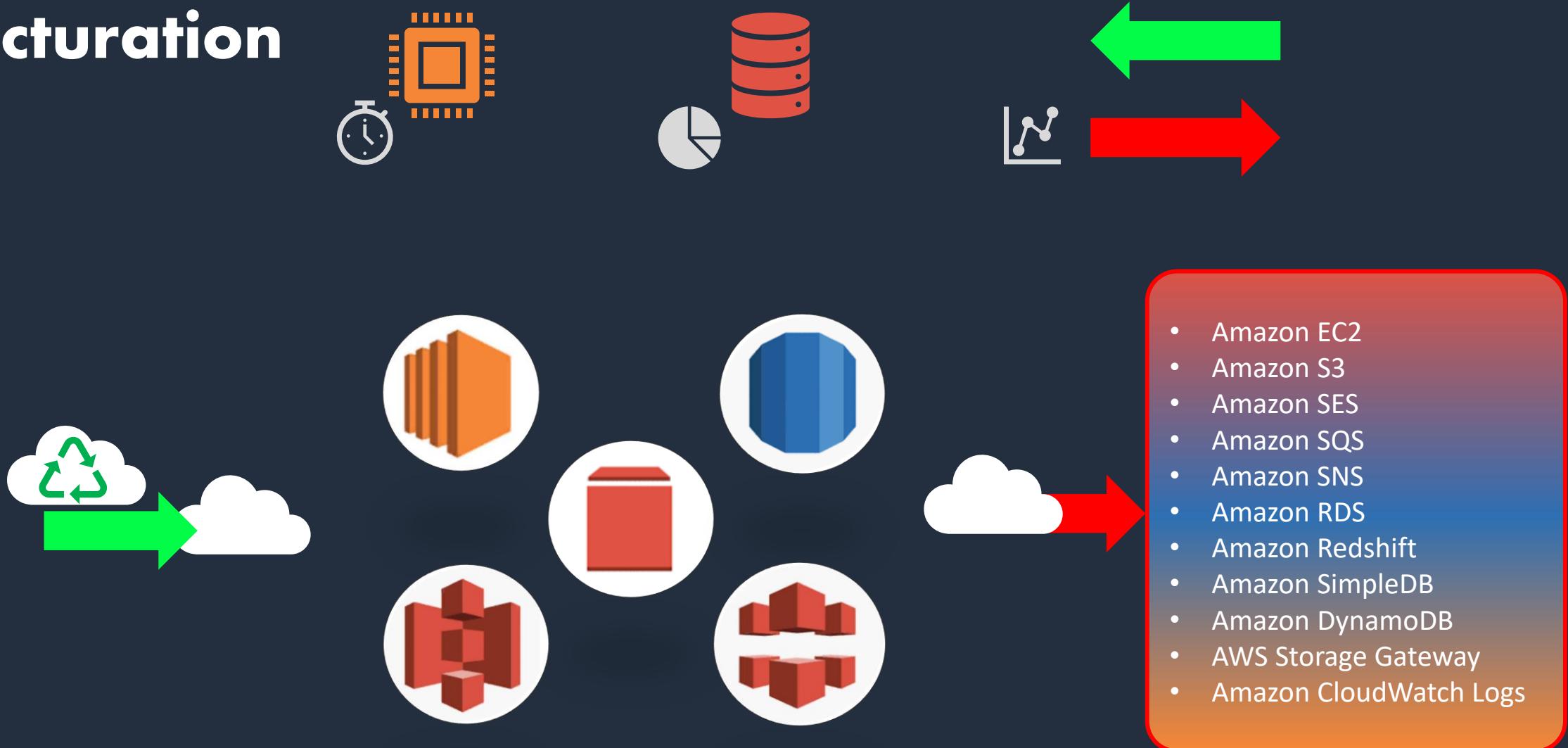
Toutes vérifications Trusted Advisor

Finance & Support



Tarification AWS

Facturation



Les niveaux de tarification prennent en compte votre utilisation totale des transferts de données sortantes vers Internet



Amazon EC2

Capacité de calcul sécurisée et redimensionnable dans le cloud.



Facturé seulement lorsque l'instance est démarrée

- « On demand » pas de frais d'entrée paiement à l'heure ou sec (min 60 sec)
- « Reserved » frais d'entrée paiement à l'heure (-75% vs on demand)
- « Spot » enchères pour obtenir des ressources aws non utilisées

Capacité physique de l'instance

- Processeur, mémoire, disque

Facturation à l'heure consommée

- Dépend de la région, du système, type d'instance, et de la taille

Facturation à la seconde

- Toutes les régions et zones de disponibilité AWS
- À la demande, Réservées et Spot
- Amazon Linux et Ubuntu

Réseau

- **Transfert de données ENTRANTES vers Amazon EC2 depuis Internet**
- **Transfert de données SORTANTES depuis Amazon EC2 vers Internet**



Amazon Elastic Block Store

Stockage par bloc haute performance et simple d'utilisation à n'importe quelle échelle



Facturé en fonction du type de stockage choisi

- Usage général (SSD)
- IOPS provisionnées (SSD)
- Magnétique (HDD)

Options IOPS

- Usage général (gp2) inclus dans le prix
- IOPS provisionnées (io1)
- Magnétique (sc1) inclus dans le prix

Snapshots

- Tarification par GB / Mois pour les données stockées

Transferts de données

- **Transfert de données ENTRANTES vers Amazon EC2 depuis Internet**
- **Transfert de données SORTANTES depuis Amazon EC2 vers Internet**

Les niveaux de tarification prennent en compte votre utilisation totale des transferts de données sortantes vers Internet



Amazon Relational Database Service (RDS)

installer, gérer et mettre à l'échelle facilement une base de données relationnelle dans le cloud



Facturé par heure consommée

- « On demand » (dès la première minute sans minimum)
- « Reserved » (frais de réservation pour 1 an ou 3 ans)
- « Provisionnées » (extensibles)

Facturation à l'heure consommée

- Dépend de la région, du système, type d'instance, et de la taille

Facturation fonction du déploiement

- Mono Zone de disponibilité (une instance)
- Multi Zones de disponibilité (2 instances min)

Facturation des sauvegardes

- Gratuite pour 100% du stockage des bases de données en fonctionnement
- Paiement au Gb / mois pour les sauvegardes d'instance terminée
- **Transfert de données ENTRANTES vers Amazon RDS depuis Internet**
- **Transfert de données SORTANTES depuis Amazon RDS vers Internet**

Les niveaux de tarification prennent en compte votre utilisation totale des transferts de données sortantes vers Internet



Amazon S3

Stockage d'objets conçu pour stocker et récupérer n'importe quelle quantité de données, n'importe où



Facturé en fonction de la classe de stockage

- Standard (durabilité 99,99999999% + 99,99% disponibilité)
- Standard IA (durabilité 99,99999999% + 99,90% disponibilité)

Facturé en fonction de la consommation

- Nombre d'objets
- Tailles des objets
- Type de stockage

Facturé en fonction

- Nombre de requêtes (PUT, COPY, POST, LIST, GET, SELECT, Transition de cycle de vie et Extraction de données)
- Les requêtes DELETE et CANCEL sont gratuites
- Inventaire ou balisage (par quantité d'objets)

Réseau

- Transfert de données ENTRANTES vers Amazon S3 depuis Internet
- Transfert de données SORTANTES depuis une région S3 vers Internet

Les niveaux de tarification prennent en compte votre utilisation totale des transferts de données sortantes vers Internet



Amazon CloudFront

Réseau de diffusion de contenu (CDN) rapide fortement sécurisé et programmable



Facturé en fonction

- La région
- Nombre de requêtes de la part des clients

Réseau

- Transfert de données ENTRANTES vers Amazon CDN depuis Internet
- Transfert de données ENTRANTES vers Amazon S3 depuis CDN depuis une autre région
- Transfert de données SORTANTES depuis Amazon CDN vers Internet
 - Remise au delà de 10To / mois transférés

Les niveaux de tarification prennent en compte votre utilisation totale des transferts de données sortantes vers Internet

BONUS



Révision des bases

- Libre-service à la demande. (On-demand self-service)
- Mise en commun des ressources. (Resource pooling)
- Élasticité rapide. (Rapid elasticity)
- Haute disponibilité = tolérance aux pannes (eliminate spofs)
- Moins de privilège = plus de sécurité (less privilege)
- Service mesuré = surveillance = prise en compte rapide (Measured service)
- Répartition géographique des ressources (World wild access)
- Regions (contain 3 or more AZ)
- Availability zones (IN a region 2 AZ needed to build HA architecture)
- Edge locations (data are cached nearest of final user cloudfont CDN)
- On premise – Cloud – Hybrid cloud architecture
- VPC private network (VPC peering to connect 2 VPC)
- Direct connect up to 10 Gbps dedicated network connection between on premise and VPC
- VPN connect up to 1,25 Gbps establish connection over internet between on premise and VPC
- Route53 DNS routing network between aws services can route and monitor to on premise ressources
- ELB distribute traffic accross EC2, ALB (layer 7) or NLB (Layer 4) (classic load balancer legacy one)
- EC2 instances Select region, AMI OS, az, subnet, storage, SG, balises
- EBS ephemeral data lost if stopped - EBS Volume persistent storage for EC2 instances
- S3 Object storage in buckets (Key + region + object name) and Static Website
- S3 Standard – Standard IA – One Zone IA (instant access)
- Glacier – Glacier Deep archive (up to 4 hours access)
- Snowball (petabyte scale) Snowmobile (exabyte scale) services to move

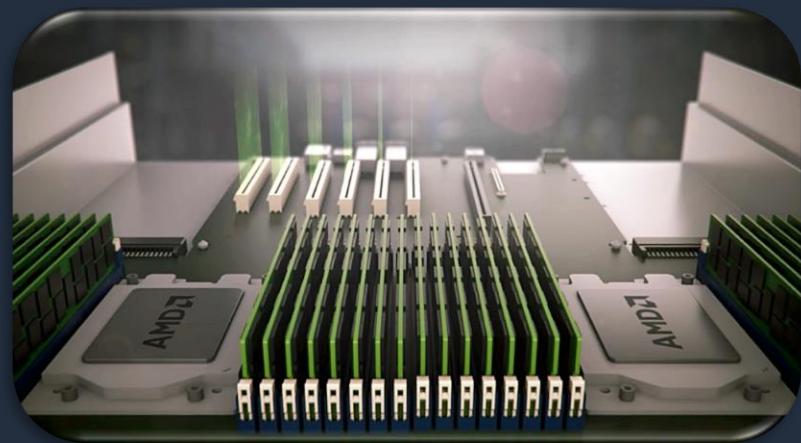
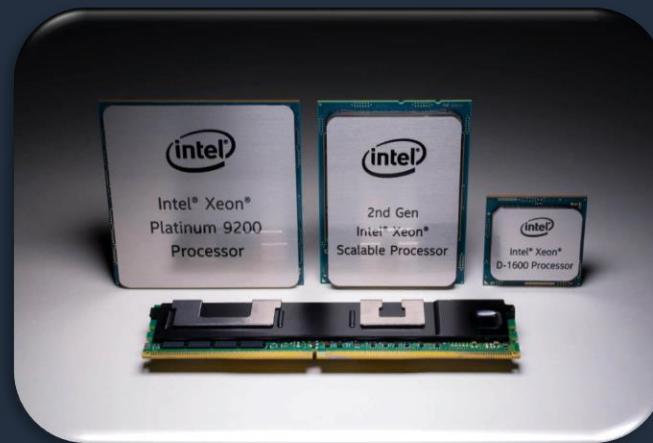
- Shared responsibility model – Aws security **OF** the cloud – You secure data **IN** the cloud
- AWS manage hardware for services, managed services, datacenters, and global network
- Customers, move data, encrypt data at rest and on the fly, os on ec2, firewall configuration
- IAM, user access console with and or Cli with secret accesskey
- Root user must be totally secure with MFA activated
- Users can be in groups, roles are for instances, Policies can be apply on groups to faciliate management
- Security group act as firewalls for EC2 instances
- Network access control list securise (at subnet level) ressources like instances in your VPC
- Trusted advisor for best practices : basic (6/7 checks) , business or enterprise (full checks)
- Important trusted advisor : Cost optimisation, performance, Security, Fault tolerance, services limits
- Cloudtrail certified service records all API perfomed, governance, compliance, auditing
- Cloudtrail control up to 161 services api request, logs can be filtered, who, where, when, what
- Artifact gives you access to compliance documents, to prove compliance to third party under NDA
- **Security breach process**
- Change your AWS account root user password.
- Rotate and delete all root and AWS Identity and Access Management (IAM) access keys.
- Delete any potentially compromised IAM users, and change the password for all other IAM users.
- Delete any resources on your account that you didn't create, such as EC2 instances and AMIs, EBS volumes and snapshots, and IAM users.
- Respond to the notifications that you received from AWS Support through the AWS Support Center.
- Get help from AWS Partner Network (professionnal certified vendors endorsed by AWS)
- **APN Consulting or APN Technology**

- Remember well architected pillars to determine which technology to use for
- Processes : Design – review design – test design – run design – ameliorate design (goto start)
- Deploy = infrastructure as code (CloudFormation use YAML or JSON to describe and deploy infrastructures) – free
- USE native technology services resources (compute EC2, autoscaling, ELB, storage EBS, network VPC are regional service)
- USE region near your customers, and use CloudFront to make it global
- USE native Global DNS Route53 service to route your domain traffic to your AWS resources fast and secure
- USE managed technology services (compute Beanstalk, or storage S3 glacier, automatic scaling and load balancing)
- USE Serverless technology = Lambda (function as a service) (SQS, SNS, SES, DynamoDB)
- CDN content delivery network is like a local cache for app users reduce latency (get or copy data near final customer)
- CloudFront secure by surface app augmentation, protect from DDoS attack, makes app secure and global
- Databases services (managed relational RDS, Redshift) (NoSQL serverless DynamoDB) (in memory ElasticCache)
- Managed service RDS (MySQL, PostgreSQL, MariaDB, Microsoft SQL server, Amazon Aurora, Oracle) (**read replicas**)
- Service management (console, CLI, SDK)
- Remote management on native EC2 Access key / secret access key (ssh tcp22, rdp remote desktop protocol tcp/udp 3389)
- Measure metric to control production (metrics with CloudWatch, analyse CloudWatch logs) (CPU disk, network and others)
- Basic monitoring 5 min / advanced monitoring 1 min
- Personal and AWS Health dashboard to control and be aware about service interruption like geographic service incident
- Amazon Simple Queue Service Fully managed message queues for microservices, distributed systems, and serverless apps
- SQS to create decoupled application architecture (opposing to monolithic software)
- Serverless app use Lambda as compute, S3 as storage, Dynamodb as DB, SQS execution control, SNS for notification
- Developers can use AWS CodeCommit for code versioning control and AWS CodeDeploy
- Docker : container technology to run docker image App Fargate serverless container service
- ECS need you manage EC2 instance for, not with Fargate serverless which one is provisioning resources for you
- ECR Private docker image repository

- USE Organization to consolidated billing, get volume discount, saving money with reserved instances
- EC2 on demand, reserved, spot, dedicated (dedicated host)
- USE free services Cloudformation, IAM, Beanstalk, VPC, Autoscaling, Organization, aws documentation
- Support basic is only for billing and account aspect.
- Live chat and phone support is available only for business and enterprise (with 1h response time)
- USE TCO Calculator to estimate charge for a project and compare with on premise pricing
- TCO include compute, storage AND network data transfert + hours usage services / month
- USE tags to track application expenses
- USE AWS Budget to set custom alerts to control resources consumption
- Import data to aws cloud is free you pay only for storage you use by GB / month
- Pay-as-you-go allows you to easily adapt to changing business needs without overcommitting budgets
- For certain services like Amazon EC2 and Amazon RDS, you can invest in reserved capacity.
- With Reserved Instances, you can save up to 75% over equivalent on-demand capacity.
- you can get volume-based discounts and realize important savings as your usage increases.
- For services such as S3, pricing is tiered, meaning the more you use, the less you pay per GB.
- AWS Database Migration Service you only pay for your replication instances and any additional log storage.
- Migrating databases to Aurora, Redshift, DynamoDB ... you can use DMS free for 6 months.
- AWS Direct Connect has two billing elements: port hours and outbound data transfer.
- In AWS Global Accelerator, you are charged for each accelerator that is provisioned and the amount of traffic.
- VPN Data processing charges apply for each GB processed through the VPC endpoint regardless + h/months 0,01\$ each
- Optimize Costs with Resource and Pricing Recommendations
- AWS Cost Management Services (AWS Resources , AWS Cost Allocation Tags, AWS Cost Explorer , AWS Consolidated Billing , AWS Identity and Access Management, AWS Cost Explorer , AWS Budgets, AWS Free Tier , AWS Instance Scheduler, AWS Cost Explorer)

CALCUL (Compute)

Il s'agit des ressources nécessaires à l'accomplissement des tâches élémentaires sur lesquelles reposent les applications et les systèmes exécutant des processus et des algorithmes

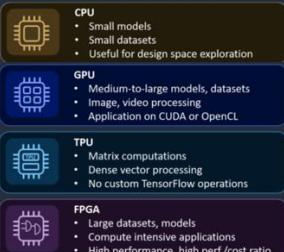




ECC alias EC2

Caractéristiques :

- Types d'instances
- Amazon Machine Image (AMI)
- Location (tenancy shared / dedicated)
- Données utilisateurs (userdata)
- Stockage (éphémère, ebs)
- Réseau (up to 25Gb/s)
- Groupes de Sécurité (accès)
- Monitoring (status check - cloudwatch)



Connexion :

- SSH + keypair (Mac linux)
- Rdp (Windows)
- Session manager
- ACL
- Protocoles ports

Tarification :

- On demand (consommation)
- Reserved (upfront)
- Spot (consommation)
- Dedicated instance (upfront)
- Dedicated Host (upfront)



Elastic Compute Cloud



AMI

EC2 Instances



Type



DEDICATED

- Accès aux contrôles avancés matériel
- Sans engagement (réservation possible)
- Pas de frais initiaux (sauf en cas de réservation)
- Paiement à l'usage
- Facturé à l'heure

Recommandé pour :

- Réduction des coûts en utilisant vos propres licences (-70%)
- Contraintes licences logiciels
- Contraintes sécurité des données ou de conformité

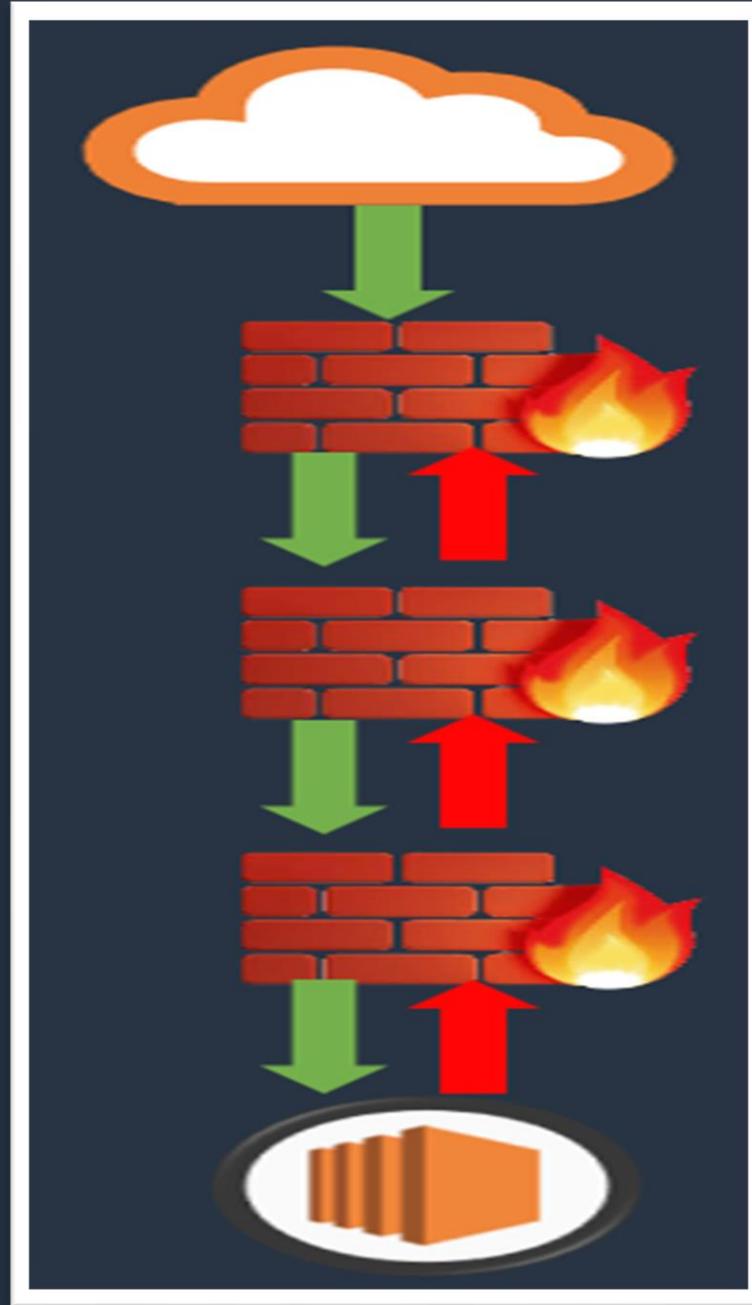
À retenir



Stratégie = format JSON

Appliqué à un
Utilisateur
Groupe
Rôle

Autorisation ou interdiction
d'usage d'un service



EC2 / VPC

GROUPE DE SECURITE
Protocoles / ports

ACCESS CONTROL LIST
Autorisation
Interdiction explicite

SOURCE / DESTINATION
Depuis où
Vers quelles ressources



Elastic Load Balancing

Dirige les requêtes vers les instances EC2 en bonne santé

Équilibreur de charge d'application



7

- osi -

4

Équilibreur de charge réseau



1. Configurer l'équilibreur de charge

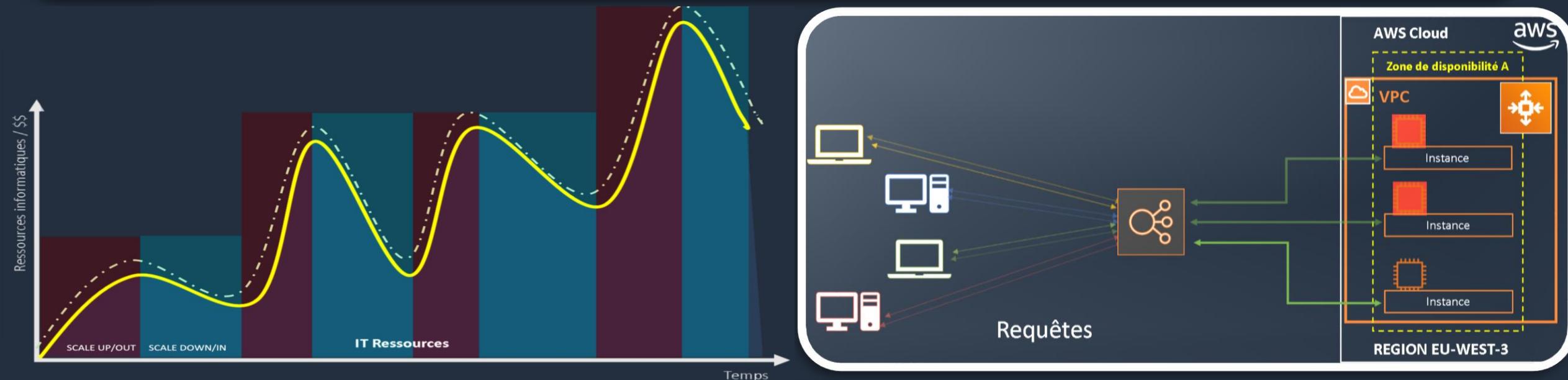
2. Configurer les paramètres de sécurité

3. Configurer les groupes de sécurité

4. Configurer le routage

5. Enregister les cibles

6. Vérification



1. Configurer les détails du groupe Auto Scaling

2. Configurer les stratégies de dimensionnement

3. Configurer des notifications

4. Configurer des balises

5. Vérification



Auto Scaling

Augmente ou diminue les ressources en fonction des besoins



Elastic Beanstalk

Service géré par aws permet de déployer vos applications web

Environnement

Version Application



Configuration d'environnement



Application

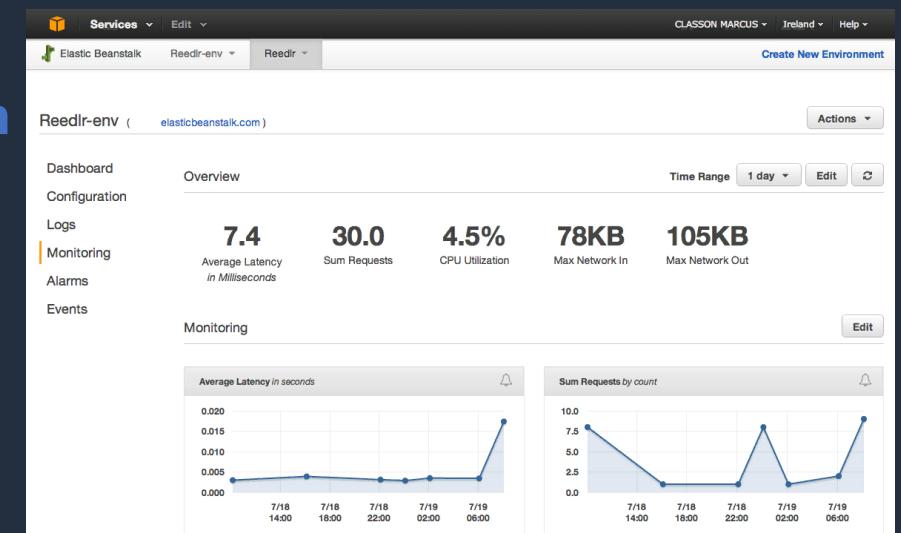


Configuration du modèle (template)



Clause de non-responsabilité : Ces diapositives sont protégées par des droits d'auteur et uniquement pour un usage strictement personnel. Déclarer un lien pirate vers ce document <https://udemy.pirashield.com/home>

1. Créer l'application
2. Téléchargez votre code
3. Lancer l'environnement
4. Gérer l'environnement
5. Superviser jusqu'à deux semaines de rapport



Tarification

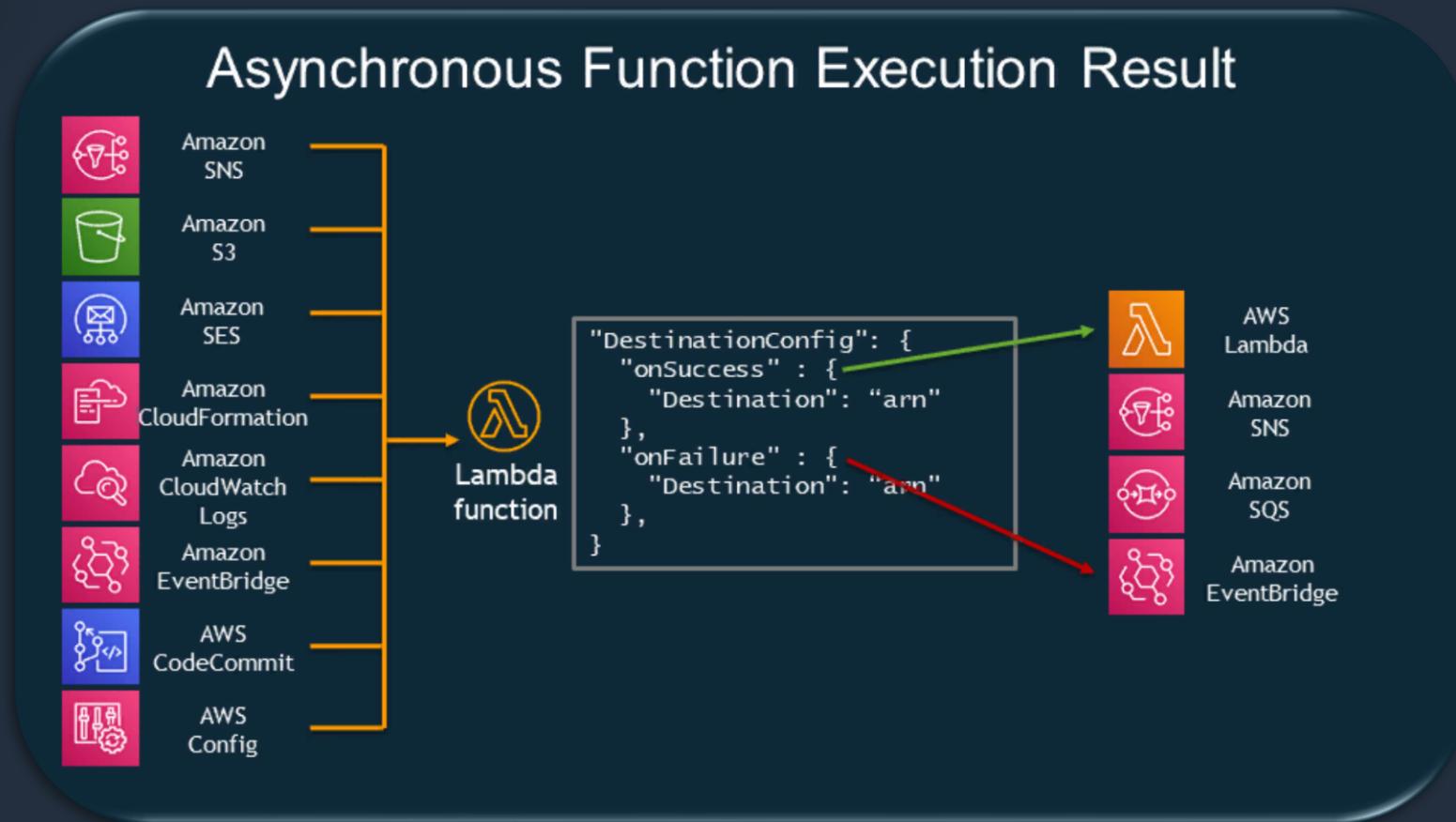
- Il n'y a pas de frais supplémentaires pour EB





Lambda

est un service AWS qui exécute votre propre code en réponse à des événements dans un environnement #Serverless



AWS gère pour vous

- Serveurs
- Capacité
- Déploiement
- Mise à l'échelle
- Administration
- Exécution sur évènement ou un intervalle de temps

Vous gérez

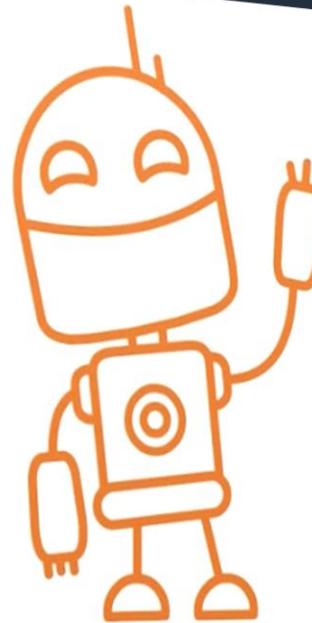
- Code
- Déclencheur
- Destination
- Paiement à l'usage



Lightsail

Est un service de VPS (virtual private server) hébergé par AWS

Imaginez le comme une version allégée et simplifiée du service EC2



Amazon **Lightsail**

- Configuration rapide et ultra simple
- Idéal pour les ingénieurs et développeurs non experts aws
- Service dédié aux petits sites web, blogs ou petites applications
- Les instances lightsail peuvent communiquer avec d'autres ressources aws et « migrer » vers EC2
- Prix de départ à 3.5\$



Amazon **Lightsail**

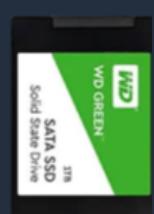
Stockage (Storage)

Le stockage dans le nuage est un modèle de stockage de données informatiques dans lequel les données numériques sont stockées dans des regroupements logiques (blocs, fichiers, objets).

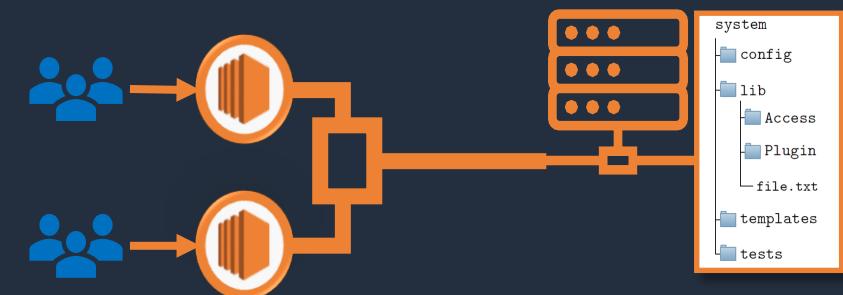
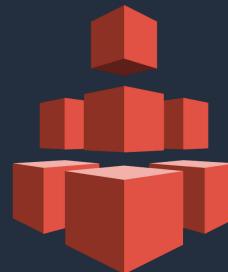


Amazon

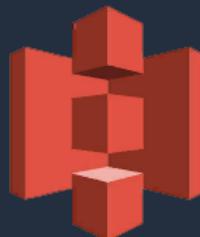
Elastic Block Store



Amazon EFS



Amazon S3



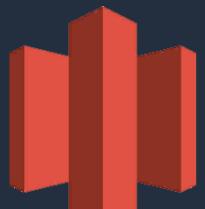
Amazon CloudFront



Amazon RDS

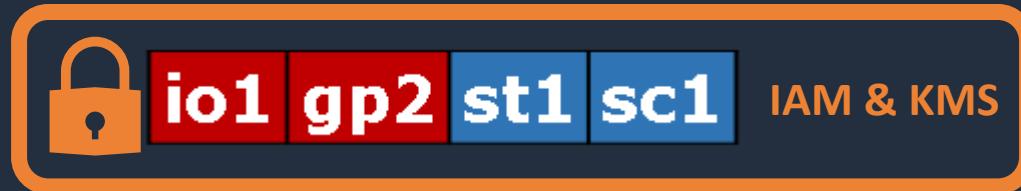


Amazon Glacier





Elastic Block Store (EBS)



Fourni un stockage cloud en mode bloc accessible via des volumes «montés » sur des instances EC2 et répliqués dans une même zone de disponibilité, tolérants aux pannes, procure haute disponibilité et durabilité élevée.

- 2 grandes familles de volume Amazon EBS (SSD / Magnetic)
- 5 Types différents (‘IO1, GP2’ ssd - ‘ST1, SC1’ hdd ‘no boot’ or old magnetic 1To max ‘bootable’)
- Indépendant d'une instance, peut être détaché et attaché à une autre instance à chaud
- Un volume pour une instance, mais plusieurs volumes pour une instance
- Volumes élastiques (changer taille, performance, type volume ,sans coupure ni ralenti)
- Instantanés (snapshots) Amazon EBS (sauvegarde incrémentiel « point in time », migrés, restaurés)
- « Snapshots » manuels ou planifiés, sont stockés dans le service S3, migrations vers autres régions.
- Instances optimisées pour Amazon EBS (D2, H1, I3)
- Disponibilité et durabilité des volumes Amazon EBS (~0,15% vs 4% pour les disques on premise)
- EBS native Encryption AES-256 (clé KMS au repos et en transit, il suffit de cocher l'option)



Availability of 99.999%
Durability (failure rate 0.15%
x20- qu'un disque on premise 4%)
Volume répliqué dans une même AZ

	Solid State Drives (SSD)		Hard Disk Drives (HDD)	
Type de Volume	EBS Provisioned IOPS SSD (io1)	EBS General Purpose SSD (gp2)*	Throughput Optimized HDD (st1)	Cold HDD (sc1) Magnetic last gen
Description	Le volume SSD le plus performant conçu pour les charges de travail transactionnelles sensibles à la latence	Volume de DSS à usage général qui équilibre le rendement des prix pour une grande variété de charges de travail transactionnelles	Volume de disque dur à faible coût conçu pour les charges de travail à haut débit et à accès fréquent	Le volume de disque dur le plus économique conçu pour les charges de travail les moins fréquemment utilisées
Cas d'usages	NoSQL et bases de données relationnelles à forte intensité d'entrées/sorties	Volume d'amorçage (BOOT) , applications à faible latence, développement et test	BIGDATA, datawarehouse, traitement des journaux	Des données plus froides nécessitant moins d'accès par jour
API Name	io1	gp2	st1	sc1
Taille	4 GB - 16 TB	1 GB - 16 TB	500 GB - 16 TB	500 GB - 16 TB -1TB
Max IOPS**/Volume	64000	16000	500	250 (40)
Débit Max**/Volume	1,000 MB/s	250 MB/s	500 MB/s	250 MB/s (40-90 Mo/s)
Prices Without S3 snapshots	\$0.125/GB-month	\$0.10/GB-month	\$0.045/GB-month	\$0.025/GB-month 0,05 USD
	\$0.065/provisioned IOPS			

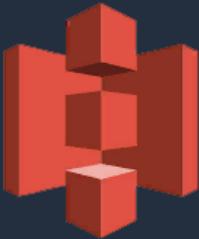


Elastic File System (EFS)

Le stockage de fichiers dans le cloud est une méthode de stockage des données qui permet aux serveurs et aux applications d'accéder aux données via des systèmes de fichiers partagés.

- Service géré par AWS accessible via NFSv4
- Stockage en tant que système de fichier « élastique » capacité illimitée
- Hautement scalable 512 accès simultanés par fichier
- Hautement disponible 7000 opérations par secondes sur le système de fichier entier
- Amazon EFS is **not supported on Windows** instances > **Amazon FSx for Windows File Server**
- “Nfs client for linux” requis pour monter la cible EFS
- Migration avec EFS File sync
- Pas de frais pour l'accès aux données
- Pas de frais pour les requêtes
- Facturation à la consommation en GB / mois

EFS File Sync



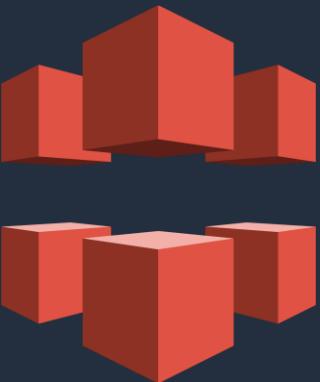
Simple Storage Service (S3)

Le stockage d'objet est idéal pour créer des applications modernes de bout en bout qui exigent mise à l'échelle et flexibilité. S3 permet d'importer des magasins de données existants à des fins d'analyse, de sauvegarde ou d'archivage.

- **S3 est un service de stockage d'objet “Global” dans des compartiments situés en région**
- **Nommage unique pour les compartiments**
- **Objet = Clé, Valeur ,VersionID (Metadata), taille max d'un objet 5To (multi part 5Go)**
- **Pas de limite de stockage, et 99,99999999 % (11 9) de durabilité**
- **S3 Standard et glacier 99,99 % de disponibilité**
- **S3 Standard – IA 99,9 % de disponibilité**
- **S3 One Zone – IA 99,5 % de disponibilité**
- **Données “cohérentes” à la première copie (consistency)**
- **Données “non cohérentes immédiatement” après UPDATE ou un DELETE**
- **S3 Transfer Accélération est conçu pour maximiser les vitesses de transfert**
- **Versioning permet de stocker plusieurs version d'un objet (facturation au volume total occupé)**
- **Gestion avec les balises et S3 inventory**
- **Chiffrement Server Side Encryption (SSE)**
- **Exécution des requêtes sur place (Query in place)**



Storage Class	Designed for	Durability (designed for)	Availability (designed for)	Availability Zones	Min storage duration	Min billable object size	Other Considerations
STANDARD	Frequently accessed data	99.99999999%	99.99%	>= 3	None	None	None
STANDARD_IA	Long-lived, infrequently accessed data	99.99999999%	99.9%	>= 3	30 days	128 KB	Per GB retrieval fees apply.
INTELLIGENT_TIERING	Long-lived data with changing or unknown access patterns	99.99999999%	99.9%	>= 3	30 days	None	Monitoring and automation fees per object apply. No retrieval fees.
ONEZONE_IA	Long-lived, infrequently accessed, non-critical data	99.99999999%	99.5%	1	30 days	128 KB	Per GB retrieval fees apply. Not resilient to the loss of the Availability Zone.
GLACIER	Long-term data archiving with retrieval times ranging from minutes to hours	99.99999999%	99.99% (after you restore objects)	>= 3	90 days	40 KB	Per GB retrieval fees apply. You must first restore archived objects before you can access them. For more information, see Restoring Archived Objects .
DEEP_ARCHIVE	Archiving rarely accessed data with a default retrieval time of 12 hours	99.99999999%	99.99% (after you restore objects)	>= 3	180 days	40 KB	Per GB retrieval fees apply. You must first restore archived objects before you can access them. For more information, see Restoring Archived Objects .
RRS (Not recommended)	Frequently accessed, non-critical data	99.99%	99.99%	>= 3	None	None	None



Amazon CloudFront

Amazon CloudFront est un réseau rapide de diffusion de contenu (CDN)

- Pour fournir du contenu aux utilisateurs finaux avec une latence plus faible
- Amazon CloudFront exploite un réseau mondial de 216 points de présence
- Déployé dans 84 villes de 42 pays
- Protection contre les attaques des couches réseau et application
- Chiffrements SSL/TLS et HTTPS
- Contrôle d'accès avec des URL signées et des cookies signés
- Conformité PCI-DSS Niveau 1, HIPAA et ISO 9001, ISO 27001, SOC (1, 2 et 3)
- Augmenter la disponibilité de l'application
- Activation de la redondance pour les origines
- Optimisations réseau pour des performances optimales
- Contenu statique ou dynamique
- Grandes bibliothèques et ressources multimédias
- API complètes et outils DevOps
- Paiement à l'usage, vous ne payez que ce que vous utilisez



Amazon RDS

Amazon RDS est un service de base de données relationnelle dans le cloud

- Permet de transférer la responsabilité de la plateforme chez le fournisseur **AWS**
- Maintien en conditions opérationnelles en cas de panne matériel
- Mises à jour, Patches management (durant une plage de maintenance pré définie)
- Sauvegarde automatique des instances
- Instantané des bases de données avec choix de rétention des données (jours)
- Déploiement sur plusieurs zones de disponibilité (haute disponibilité)
- Évolution vers du matériel plus performant
- Recevoir des alertes en fonction de critères
- Chiffrement avec gestion des clé via KMS ou CloudHSM
- Gestion des accès avec IAM, groupes, utilisateurs, rôles
- Stockage block SSD, IOPS, Magnétique
- Sécurité des accès aux instances via les groupes de sécurité de base dédiés



Storage Gateway

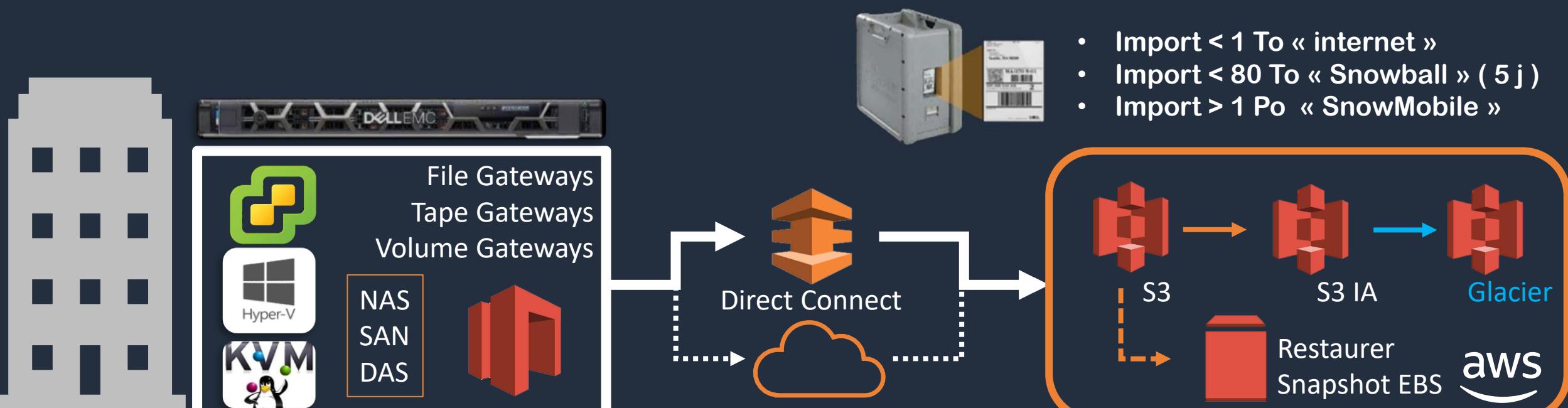


AWS Storage Gateway est un service de stockage dans le cloud hybride, qui connecte vos environnements sur sites existants au cloud AWS.

La passerelle de fichiers propose une interface de fichier qui vous permet de stocker des fichiers en tant qu'objets dans S3.

La passerelle de bande présente à votre application de sauvegarde existante une bibliothèque de bandes virtuelles (VTL).

La passerelle de volume affiche les volumes de stockage par bloc de vos applications à l'aide du protocole iSCSI.

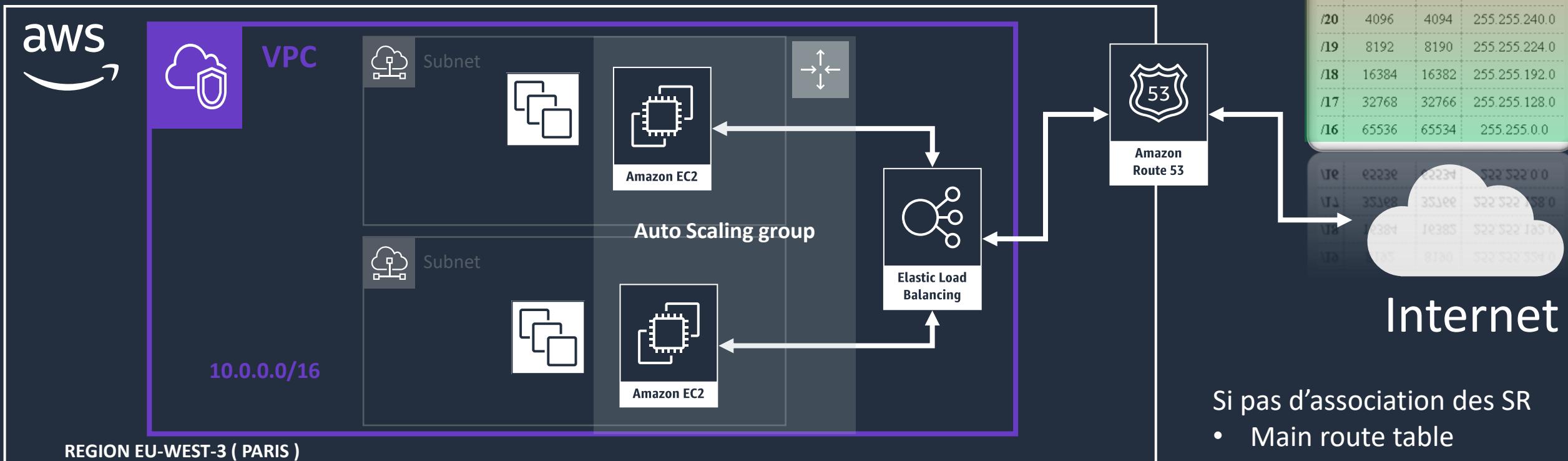




VPC est conçu pour offrir aux services haute disponibilité et tolérance aux pannes.

- Vous disposez d'une « partie » du réseau global AWS isolée logiquement (logiciellement)
- Choisissez la capacité de cette « partie », et combien d'équipements elle pourra accueillir
- La sécurité est assurée par les ACL réseau et les groupes de sécurité
- Contrôle total le nombre d'adresses IP disponibles, de sous réseaux, tables de routages
- Les sous réseaux sont des blocs d'adresses appelés CIDR (ClassLess Inter-Domain Routing)
- Les adresses .0 et .255 sont utilisées par le réseau et .1 à .3 sont réservées par AWS

	Adresses	Hosts	Netmask
/30	4	2	255.255.255.252
/29	8	6	255.255.255.248
/28	16	14	255.255.255.240
/27	32	30	255.255.255.224
/26	64	62	255.255.255.192
/25	128	126	255.255.255.128
/24	256	254	255.255.255.0
/23	512	510	255.255.254.0
/22	1024	1022	255.255.252.0
/21	2048	2046	255.255.248.0
/20	4096	4094	255.255.240.0
/19	8192	8190	255.255.224.0
/18	16384	16382	255.255.192.0
/17	32768	32766	255.255.128.0
/16	65536	65534	255.255.0.0





Route 53

Service DNS Amazon Web Services

- DNS Hautement disponible
- Fournit les URL d'accès aux services
- Politique de routage conditionnelle
 - Routage simple
 - Routage pondéré
 - Routage fonction de la latence
 - Routage bascule en cas de panne
 - Routage géographique
- Surveillance de la disponibilité
- Permet la migration ou l'enregistrement de domaine (mondomaine.com)
- Intégré à Elastic Load Balancing





AWS Virtual Private Network

Etablit une liaison sécurisée via un tunnel privé depuis un réseau d'entreprise avec le réseau global AWS

AWS Site-to-Site VPN

étend votre centre de données ou succursale au cloud via des tunnels IP Security (IPSec) et prend en charge la connexion à la fois à une passerelle réseau privé virtuel et à AWS Transit Gateway.

Vous pouvez éventuellement exécuter Border Gateway Protocol (BGP) sur le tunnel IPSec pour une solution hautement disponible.

AWS Client VPN

fournit une solution VPN entièrement gérée accessible depuis n'importe où avec une connexion Internet. Il est élastique et s'adapte automatiquement aux besoins des utilisateurs qui peuvent se connecter à la fois à AWS et aux réseaux sur site. AWS Client VPN s'intègre à Amazon VPC et AWS Directory Services sans avoir à modifier la topologie réseau.



VPN vs Direct Connect

Liaison à travers internet ou liaison spécialisée directe





Sécurité



Les principes de conception :

- Mettre en place une identification forte
- Permettre la traçabilité
- Appliquer la sécurité à toutes les couches
- Automatiser les bonnes pratiques de sécurité
- Protéger les données en transit et au repos
- Tenez les gens à l'écart des données.
- Se préparer aux événements de sécurité



Sécurité

Les bonnes pratiques :

- Gestion des identités et des accès
- Détection par contrôle
- Protection des infrastructures
- Protection des données
- Réponse sur incidents





Sécurité

Les bonnes pratiques :



- **Gestion des identités et des accès**
 - **Comment gérer les identités et l'authentification ?**



- Définir les exigences en matière de gestion des identités et des accès
- Sécuriser l'utilisateur root AWS
- Appliquer l'utilisation de l'authentification multi-facteurs.
- Automatiser les mesures de contrôle d'accès
- Intégrer une fédération d'identité centralisée
- Faire respecter les exigences relatives aux mots de passe
- Effectuer une rotation régulière mot de passe
- Vérification périodique des Autorisations



Sécurité

Les bonnes pratiques :



- **Gestion des identités et des accès**
 - Comment gérer les identités et l'authentification ?
 - **Comment contrôlez-vous l'accès des personnes ?**
- Définir les conditions d'accès des personnes
- Accorder le moins de privilèges
- Attribuer à chaque individu des identifiants uniques
- Gérer les identifiants en fonction du parcours de l'utilisateur
- Automatiser la gestion des autorisations d'accès
- Autoriser l'accès via les rôles ou la fédération





Sécurité

Les bonnes pratiques :



- **Gestion des identités et des accès**
 - Comment gérer les identités et l'authentification ?
 - Comment contrôlez-vous l'accès des personnes ?
 - **Comment contrôlez-vous les accès programmatiques ?**
- Définir les conditions d'accès programmatiques
- Accorder le moins de privilèges
- Automatiser la gestion des titres de créance
- Attribuer des références uniques pour chaque composant
- Accorder l'accès via les rôles ou la fédération
- Mettre en œuvre l'authentification dynamique





Sécurité

Les bonnes pratiques :



- **Détection par contrôle**
 - **Comment détecter et enquêter sur les événements de sécurité ?**
- Définir les exigences relatives aux registres
- Définir les exigences en matière de mesures
- Définir les exigences relatives aux signalements
- Configurer l'enregistrement des services et des applications
- Analyser les registres de manière centralisée
- Automatiser les alertes sur les indicateurs clés
- Développer les processus d'enquête





Sécurité

Les bonnes pratiques :



- **Détection par contrôle**
 - Comment détecter et enquêter sur les événements de sécurité ?
 - **Comment se défendre contre les nouvelles menaces de sécurité ?**
- Se tenir informé des exigences organisationnelles, juridiques et de conformité
- Se tenir informé des meilleures pratiques en matière de sécurité
- Se tenir informé des menaces pour la sécurité
- Évaluer régulièrement les nouveaux services et caractéristiques de sécurité
- Définir et hiérarchiser les risques à l'aide d'un modèle de menace
- Mettre en œuvre de nouveaux services et fonctionnalités de sécurité





Sécurité

Les bonnes pratiques :

- **Protection des infrastructures**
 - **Comment protéger vos réseaux ?**
 - Comment protéger vos ressources informatiques ?
- Définir les exigences en matière de protection du réseau.
- Limiter l'exposition
- Automatiser la gestion des configurations.
- Automatiser la protection du réseau
- Mettre en œuvre l'inspection et la protection
- Contrôler le trafic à tous les niveaux





Sécurité

Les bonnes pratiques :

- **Protection des infrastructures**
 - Comment protéger vos réseaux ?
 - **Comment protéger vos ressources informatiques ?**
- Définir les exigences en matière de protection informatique
- Cycle de recherche et de correction des vulnérabilités
- Automatiser la gestion des configurations
- Automatiser la protection des ressources informatiques
- Réduire la surface d'attaque
- Prioriser des services managés





Sécurité

Les bonnes pratiques :



- **Protection des données**
 - **Comment classifier vos données ?**
 - Déterminer les exigences en matière de classification des données
 - Définir les contrôles de protection des données
 - Mettre en œuvre l'identification des données
 - Automatiser l'identification et la classification
 - Identifier les types de données





Sécurité

Les bonnes pratiques :



- **Protection des données**
 - Comment classifier vos données ?
 - Comment protéger vos données au repos ?
- Définir les exigences en matière de gestion et de protection des données au repos
- Mettre en place une gestion sécurisée des clés de chiffrement
- Faire appliquer le cryptage au repos
- Faire appliquer le contrôle d'accès
- Fournir des mécanismes permettant de limiter l'accès aux données





Sécurité

Les bonnes pratiques :



- **Protection des données**
 - Comment classifier vos données ?
 - Comment protéger vos données au repos ?
 - **Comment protéger vos données en transit ?**
- Définir les exigences en matière de protection des données en transit
- Mettre en place une gestion sécurisée des clés et des certificats
- Appliquer le chiffrement en transit
- Automatiser la détection des détournements de données
- Authentifier les communications en réseau





Sécurité

Les bonnes pratiques :



- **Réponse sur incidents**
 - Comment réagir à un incident ?
 - Identifier le personnel clé et les ressources externes
 - Identifier l'outillage
 - Élaborer des plans de réaction aux incidents
 - Automatiser la capacité de confinement
 - Identifier les moyens scientifiques disponibles
 - Anticiper les accès requis aux experts
 - Anticiper les déploiements d'outils requis par les experts en sécurité
 - Effectuer des simulations d'incidents de sécurité régulièrement



Improvement Plan
Each day it's Day One



Fiabilité



Les principes de conception :

- Tester les procédures de reprise d'activité
- Récupération automatique après un échec
- Mise à l'échelle horizontale (scale horizontally)
- Cessez de deviner la capacité
- Gérer le changement en automatisant les processus



Fiabilité



Les bonnes pratiques :

- Pré requis fondamentaux
- Gestion du changement
- Gestion des échecs



Fiabilité



Les bonnes pratiques :

- **Pré requis fondamentaux**
 - **Comment gérez-vous les limitations de service ?**
 - Connaître les limites mais ne pas les suivre
 - Surveiller et gérer les limites
 - Automatiser les alertes ou la gestion des limites
 - Adapter les limites de service définies par l'architecture
 - Assurer un écart suffisant entre la limite de service et son taux max d'utilisation pour assurer le basculement
 - Gérer les limites de service pour tous les comptes et régions concernés



Fiabilité



Les bonnes pratiques :

- **Pré requis fondamentaux**
 - **Comment gérez-vous les limitations de service ?**
 - **Comment gérer la topologie réseau ?**
- Utiliser une connectivité hautement disponible entre les adresses privées dans les nuages publics et l'environnement sur site
- Utiliser une connectivité de réseau à haute disponibilité pour les utilisateurs finaux
- Faire respecter les plages d'adresses IP privées pour qu'elles ne se chevauchent pas dans les multiples espaces d'adresses privées où elles sont connectées
- Veiller à ce que l'allocation des sous-réseaux IP tienne compte de l'expansion et de la disponibilité



Fiabilité



Les bonnes pratiques :

- **Gestion du changement**
 - Comment votre système s'adapte-t-il à l'évolution de la demande ?
 - Comment surveillez-vous vos ressources ?
 - Comment mettez-vous en œuvre les changements ?



Fiabilité



Les bonnes pratiques :

- **Gestion du changement**
 - **Comment votre système s'adapte-t-il à l'évolution de la demande ?**
 - Fournir automatiquement des ressources lors de l'augmentation ou de la diminution d'une charge de travail
 - Fournir des ressources en cas de détection d'un manque de service dans le cadre d'une charge de travail
 - Procurer des ressources manuellement lorsqu'on détecte que des ressources supplémentaires pourraient être nécessaires prochainement pour une charge de travail
 - Tester la capacité de charge de travail



Fiabilité



Les bonnes pratiques :

- **Gestion du changement**
 - Comment votre système s'adapte-t-il à l'évolution de la demande ?
 - **Comment surveillez-vous vos ressources ?**
- Surveiller la charge de travail à tous les niveaux
- Envoyer des notifications sur la base de la surveillance
- Effectuer des réponses automatisées sur les événements
- Procéder à des évaluations régulières



Fiabilité



Les bonnes pratiques :

- **Gestion du changement**
 - Comment votre système s'adapte-t-il à l'évolution de la demande ?
 - Comment surveillez-vous vos ressources ?
 - **Comment mettez-vous en œuvre les changements ?**
 - Déployer les changements de manière planifiée
 - Déployer les changements grâce à l'automatisation



Fiabilité



Les bonnes pratiques :

- **Gestion des échecs**
 - **Comment sauvegarder les données ?**
 - Identifier toutes les données qui doivent être sauvegardées et effectuer des sauvegardes ou reproduire les données à partir des sources
 - Réalisation automatique de la sauvegarde des données ou reproduction automatique des données à partir des sources
 - Effectuer une récupération périodique des données pour vérifier l'intégrité et les processus de sauvegarde
 - Sécuriser et chiffrer les sauvegardes ou s'assurer que les données sont disponibles à partir d'une source sûre pour la reproduction



Fiabilité



Les bonnes pratiques :

- **Gestion des échecs**
 - Comment sauvegarder les données ?
 - **Comment votre système résiste-t-il aux défaillances de composants ?**
- Surveiller toutes les couches de la charge de travail pour détecter les défaillances
- Mettre en œuvre des dépendances faiblement couplées
- Mettre en œuvre une approche pragmatique pour transformer les dépendances physiques en dépendances logiques.
- Automatisation complète de la restauration pour cause de contraintes technologiques dans une partie ou dans l'ensemble de la charge de travail n'autorisant qu'un seul emplacement géographique.
- Déployer la charge de travail sur plusieurs sites
- Automatiser la guérison sur toutes les couches
- Envoyer des notifications lors d'événements ayant un impact sur la disponibilité



Fiabilité



Les bonnes pratiques :

- **Gestion des échecs**
 - Comment sauvegarder les données ?
 - Comment votre système résiste-t-il aux défaillances de composants ?
 - **Comment tester la résilience ?**
- Utiliser des "recettes" pour les échecs imprévus
- Effectuer une analyse des causes profondes (RCA) et communiquer les résultats
- créer des défaillances à l'épreuve la résilience en cas d'échec
- Organiser régulièrement des journées de test de résilience



Fiabilité



Les bonnes pratiques :

- **Gestion des échecs**
 - Comment sauvegarder les données ?
 - Comment votre système résiste-t-il aux défaillances de composants ?
 - Comment tester la résilience ?
 - **Comment planifiez-vous la reprise après sinistre ?**
- Définir les objectifs de rétablissement en cas d'interruption de service et de perte de données
- Utiliser des stratégies de reprise définies pour atteindre les objectifs de rétablissement.
- Tester la mise en œuvre de la reprise après sinistre pour valider son implémentation.
- Gérer les différences de configuration à chaque changement.
- Automatiser la récupération



Efficacité des performances



Les principes de conception :

- Démocratiser les technologies de pointe
- Passer à l'échelle mondiale en quelques minutes
- Utiliser des architectures « sans serveur » (serverless)
- Expérimenter plus souvent
- Approche technologique



Efficacité des performances



Les bonnes pratiques :

- Sélection du type de ressources
- Examen
- Supervision
- Compromis



Efficacité des performances



Les bonnes pratiques :

- Sélection du type de ressources
 - Comment sélectionner l'architecture la plus performante ?
 - Comment sélectionner votre solution de calcul ?
 - Comment sélectionner votre solution de stockage ?
 - Comment sélectionner votre solution de base de données ?
 - Comment configurer votre solution de réseau ?



Efficacité des performances



Les bonnes pratiques :

- Sélection du type de ressources
 - Comment sélectionner l'architecture la plus performante ?
 - Comprendre les services et les ressources disponibles.
 - Définir un processus pour les choix architecturaux
 - Prendre en compte le coût ou le budget dans les décisions
 - Utiliser des politiques ou des architectures de référence
 - Utilisez les conseils d'AWS ou d'un partenaire APN
 - Analyse comparative des charges de travail existantes
 - Testez votre charge de travail



Efficacité des performances



Les bonnes pratiques :

- **Sélection du type de ressources**
 - Comment sélectionner l'architecture la plus performante ?
 - **Comment sélectionner votre solution de calcul ?**
- Évaluer les différentes options de ressources de calcul disponibles
- Comprendre les options de configuration des ressources de calcul disponibles
- Collecter les métriques liées au calcul
- Déterminer la configuration souhaitée par un dimensionnement approprié
- Utiliser l'élasticité des ressources de calcul
- Réévaluer les besoins de ressources de calcul en fonction de la métrologie



Efficacité des performances



Les bonnes pratiques :

- **Sélection du type de ressources**
 - Comment sélectionner l'architecture la plus performante ?
 - Comment sélectionner votre solution de calcul ?
 - **Comment sélectionner votre solution de stockage ?**
- Comprendre les caractéristiques de stockage et les besoins en matière
- Évaluer les options de configuration disponibles
- Prendre des décisions basées sur les modèles et la métrologie



Efficacité des performances



Les bonnes pratiques :

- Sélection du type de ressources
 - Comment sélectionner l'architecture la plus performante ?
 - Comment sélectionner votre solution de calcul ?
 - Comment sélectionner votre solution de stockage ?
 - **Comment sélectionner votre solution de base de données ?**
- Comprendre les caractéristiques des données
- Évaluer les options disponibles
- Collecter et enregistrer les mesures de performance de la base de données
- Choisir le stockage des données en fonction des modèles d'accès
- Optimiser le stockage des données en fonction des modèles d'accès et des indicateurs



Efficacité des performances



Les bonnes pratiques :

- **Sélection du type de ressources**
 - Comment sélectionner l'architecture la plus performante ?
 - Comment sélectionner votre solution de calcul ?
 - Comment sélectionner votre solution de stockage ?
 - Comment sélectionner votre solution de base de données ?
 - **Comment configurer votre solution de réseau ?**
 - Comprendre comment la mise en réseau influe sur les performances
 - Comprendre les options de produits disponibles
 - Évaluer les fonctionnalités disponibles
 - Utiliser des ACL minimales
 - Exploiter l'équilibrage des charges pour soulager les opérations de chiffrement
 - Sélectionner les protocoles de réseau pour améliorer les performances
 - Sélectionner la localisation en fonction des exigences du réseau
 - Optimiser la configuration du réseau sur la base de métriques

**Improvement Plan
Each day it's Day One**



Efficacité des performances



Les bonnes pratiques :

- **Examen**
 - **Comment faites-vous évoluer votre charge de travail pour profiter des nouveautés ?**

- Se tenir au courant des nouvelles technologies et des nouveaux services
- Définir un processus en vue d'améliorer la performance de la charge de travail
- Faire évoluer les performances de la charge de travail dans le temps



Efficacité des performances



Les bonnes pratiques :

- **Supervision**
 - **Comment contrôlez vous vos ressources pour vous assurer qu'elles fonctionnent comme prévu ?**
 - Enregistrer les indicateurs de performance
 - Analyser les indicateurs lorsque des événements ou des incidents se produisent
 - Établir des indicateurs clés de performance (KPI) pour mesurer la charge de travail
 - Utiliser la supervision pour générer des notifications sur la base d'alarmes
 - Revoir les indicateurs à intervalles réguliers
 - Surveiller et alerter de manière proactive



Efficacité des performances



Les bonnes pratiques :

- **Compromis**
 - **Comment utiliser les compromis pour améliorer les performances ?**
 - Comprendre les facteurs dans lesquels la performance est la plus critique
 - En savoir plus sur les modèles et services de design
 - Identifier l'impact des compromis sur les clients et sur les performances.
 - Mesurer l'impact de l'amélioration des performances
 - Utiliser plusieurs stratégies orientées vers la performance



Optimisation des coûts



Les principes de conception :

- Adopter un modèle de consommation
- Mesurer l'efficacité globale
- Arrêtez de dépenser de l'argent pour les activités liées aux centres de données
- Analyser et attribuer les dépenses aux bénéficiaires des ressources
- Utiliser des services gérés et au niveau des applications pour réduire le coût de possession



Optimisation des coûts



Les bonnes pratiques :

- Sensibilisation aux dépenses
- Des ressources économiquement rentables
- Faire correspondre l'offre et la demande
- Optimiser au fil du temps



Optimisation des coûts



Les bonnes pratiques :

- **Sensibilisation aux dépenses**
 - **Comment réguler les usages ?**
 - Élaborer des politiques en fonction des besoins de votre organisation
 - Mettre en place une structure de compte
 - Mettre en place des groupes et des rôles
 - Mettre en œuvre des contrôles des coûts
 - Suivre le cycle de vie des projets



Optimisation des coûts



Les bonnes pratiques :

- **Sensibilisation aux dépenses**
 - Comment réguler les usages ?
 - **Comment contrôlez-vous l'utilisation et le coût ?**
- Configurer des rapport de coût et d'utilisation des services AWS
- Identifier les catégories pour la répartition des coûts
- Définir et mettre en œuvre le balisage
- Configurer les outils de facturation et de gestion des coûts
- Faire des rapports et des notifications sur l'optimisation des coûts
- Surveiller les coûts de manière proactive
- Répartir les coûts en fonction de la consommation de ressources



Optimisation des coûts



Les bonnes pratiques :

- **Sensibilisation aux dépenses**
 - Comment réguler les usages ?
 - Comment contrôlez-vous l'utilisation et le coût ?
 - Comment désaffecter les ressources ?
- Suivre les ressources tout au long de leur cycle de vie
- Mettre en œuvre un processus de Décommissionner
- Décommissionner des ressources de manière non planifiée
- Décommissionner automatique des ressources



Optimisation des coûts

Les bonnes pratiques :

- Des ressources économiquement rentables
 - Comment évaluez-vous le coût lorsque vous choisissez des services ?
- Identifier les exigences de l'entreprise en matière de coûts :
- Analyser toutes les constituants de cette charge de travail
- Effectuer une analyse approfondie de chaque constituant.
- Sélectionner les constituants de cette charge de travail pour optimiser les coûts en fonction des priorités de l'organisation
- Effectuer une analyse des coûts pour différentes utilisations au fil du temps



Optimisation des coûts



Les bonnes pratiques :

- Des ressources économiquement rentables
 - Comment évaluez-vous le coût lorsque vous choisissez des services ?
 - **Comment atteindre les objectifs de coût lorsque vous sélectionnez le type et la taille des ressources ?**
- Effectuer une modélisation des coûts
- Sélectionner le type et la taille de la ressource sur la base d'estimations
- Sélectionner le type et la taille de la ressource en fonction de critères métrologiques



Optimisation des coûts

Les bonnes pratiques :

- **Des ressources économiquement rentables**
 - Comment évaluez-vous le coût lorsque vous choisissez des services ?
 - Comment atteindre les objectifs de coût lorsque vous sélectionnez le type et la taille des ressources ?
 - **Comment utilisez-vous les modèles de tarification pour réduire les coûts ?**
- Effectuer une analyse des modèles de tarification
- Mettre en œuvre différents modèles de tarification à faible couts
- Mettre en œuvre les régions en fonction du coût
- Mettre en œuvre des modèles de tarification pour tous les composants d'une charge de travail



Optimisation des coûts

Les bonnes pratiques :

- Des ressources économiquement rentables
 - Comment évaluez-vous le coût lorsque vous choisissez des services ?
 - Comment atteindre les objectifs de coût lorsque vous sélectionnez le type et la taille des ressources ?
 - Comment utilisez-vous les modèles de tarification pour réduire les coûts ?
 - **Comment prévoyez-vous les frais de transfert de données ?**
- Effectuer des modélisations des transferts de données
- Sélectionner les composants pour optimiser le coût du transfert de données
- Mettre en place des services pour réduire les coûts de transfert de données



Optimisation des coûts

Les bonnes pratiques :

- **Faire correspondre l'offre et la demande**
 - **Comment faire correspondre l'offre de ressources à la demande ?**
- Effectuer une analyse de la sollicitation des ressources
- Mettre à disposition des ressources de manière réactive ou non planifiée
- Mettre à disposition des ressources de manière dynamique



Optimisation des coûts



Les bonnes pratiques :

- **Optimiser au fil du temps**
 - **Comment évaluez-vous les nouveaux services ?**
 - Créer un service d'optimisation des coûts
 - Développer un processus de contrôle de la charge de travail
 - Examiner et mettre en œuvre les services de manière non planifiée
 - Examiner et analyser régulièrement les consommation de ressources
 - Tenez-vous au courant des nouvelles versions des services



Excellence opérationnelle



Les principes de conception :

- Effectuer des opérations en mode code
- Annoter la documentation
- Effectuer des changements fréquent, petits et réversibles
- Affiner fréquemment les procédures opérationnelles
- Anticiper l'échec
- Tirer les leçons de toutes les défaillances opérationnelles



Excellence opérationnelle

Les bonnes pratiques :

- Préparer
- Exploiter
- Évoluer





Excellence opérationnelle



Les bonnes pratiques :

- **Préparer**
 - Comment déterminez-vous quelles sont vos priorités ?
 - Comment concevez-vous votre production de manière à pouvoir la comprendre ?
 - Comment réduire les défauts, faciliter la remédiation et améliorer le déroulement de la production ?
 - Comment atténuer les risques liés au déploiement ?
 - Comment savez-vous que vous êtes prêt à passer en production ?



Excellence opérationnelle



Les bonnes pratiques :

- **Préparer**
- **Comment déterminez-vous quelles sont vos priorités ?**
- Évaluer les besoins des clients externes
- Évaluer les besoins des clients internes
- Évaluer les exigences de conformité
- Évaluer le contexte de la menace
- Évaluer les compromis
- Gérer les avantages et les risques



Excellence opérationnelle



Les bonnes pratiques :

- **Préparer**
- Comment déterminez-vous quelles sont vos priorités ?
- Comment concevez-vous votre production de manière à pouvoir la comprendre ?

- Mettre en œuvre la supervision applicative
- Mettre en œuvre et configurer la supervision de la charge de travail
- Mettre en œuvre la supervision de l'activité de l'utilisateur
- Mettre en œuvre la supervision des dépendances
- Mettre en œuvre la supervision des transactions



Excellence opérationnelle



Les bonnes pratiques :

- **Préparer**
 - Comment déterminez-vous quelles sont vos priorités ?
 - Comment concevez-vous votre production de manière à pouvoir la comprendre ?
 - **Comment réduire les défauts, faciliter la remédiation et améliorer le déroulement de la production ?**
- Utiliser un outils de contrôle de version
- Tester et valider les changements
- Utiliser les systèmes de gestion de la configuration
- Utiliser des systèmes de gestion de conception et du déploiement
- Effectuer la gestion des patchs
- Partager les normes de conception
- Mettre en œuvre des pratiques visant à améliorer la qualité du code
- Utiliser des environnements multiples
- Effectuer des changements fréquents, petits et réversibles
- Automatiser entièrement l'intégration et le déploiement

**Improvement Plan
Each day it's Day One**



Excellence opérationnelle



Les bonnes pratiques :

- **Préparer**
 - Comment déterminez-vous quelles sont vos priorités ?
 - Comment concevez-vous votre production de manière à pouvoir la comprendre ?
 - Comment réduire les défauts, faciliter la remédiation et améliorer le déroulement de la production ?
 - **Comment atténuer les risques liés au déploiement ?**
- Avoir une stratégie de retour arrière en cas d'échec
- Tester et valider les changements
- Utiliser des systèmes de gestion du déploiement
- Tester en utilisant des déploiements restreints
- Déployer en utilisant des environnements parallèles
- Déployer des changements fréquents, petits et réversibles
- Automatiser entièrement l'intégration et le déploiement
- Automatiser les tests et le retour en arrière

Improvement Plan
Each day it's Day One



Excellence opérationnelle



Les bonnes pratiques :

- **Préparer**
 - Comment déterminez-vous quelles sont vos priorités ?
 - Comment concevez-vous votre production de manière à pouvoir la comprendre ?
 - Comment réduire les défauts, faciliter la remédiation et améliorer le déroulement de la production ?
 - Comment atténuer les risques liés au déploiement ?
 - **Comment savez-vous que vous êtes prêt à passer en production ?**
- Assurer la disponibilité de personnel qualifiés suffisant
- Assurer un examen cohérent de l'état de préparation opérationnelle
- Utiliser du code et des déclencheurs ("runbooks") pour effectuer des procédures
- Utiliser du code et des déclencheurs ("playbooks") pour résoudre différents problèmes
- Prendre des décisions réfléchies avant déploiement de système ou changements



Excellence opérationnelle



Les bonnes pratiques :

- **Exploiter**
- Comment comprendre l'état de santé de votre charge de travail ?
- Comment comprenez-vous la santé de vos opérations ?
- Comment gérez-vous la charge de travail et les événements liés aux opérations ?



Excellence opérationnelle



Les bonnes pratiques :

- **Exploiter**
 - **Comment comprendre l'état de santé de votre charge de travail ?**
-
- Identifier les indicateurs clés de performance
 - Définir les métriques de la charge de travail
 - Collecter et analyser les métriques de la charge de travail
 - Établir des indicateurs de base de la charge de travail
 - Connaître les modèles d'activité attendus pour la charge de travail
 - Alerte lorsque la production est menacée
 - Alerte en cas d'anomalie de production
 - Valider les résultats opérationnels grâce aux indicateurs de performance clés (KPI) et aux métriques.



Excellence opérationnelle



Les bonnes pratiques :

- **Exploiter**
- Comment comprendre l'état de santé de votre charge de travail ?
- **Comment comprenez-vous la santé de vos opérations ?**

- Identifier les indicateurs clés de performance
- Définir les paramètres des opérations
- Collecter et analyser les mesures des opérations
- Établir les indicateurs de base des opérations
- Connaître les modèles d'activité attendus pour les opérations
- Alerte lorsque les résultats des opérations sont menacés
- Alerte en cas d'anomalies de fonctionnement
- Valider la réalisation des résultats et l'efficacité des ICP et des mesures



Excellence opérationnelle



Les bonnes pratiques :

- **Exploiter**
- Comment comprendre l'état de santé de votre charge de travail ?
- Comment comprenez-vous la santé de vos opérations ?
- **Comment gérez-vous la charge de travail et les événements liés aux opérations ?**
- Utiliser des processus pour la gestion des événements, des incidents et des problèmes
- Utiliser un processus d'analyse des origines de la problématique.
- Disposer d'une procédure par alerte
- Prioriser les événements opérationnels en fonction de l'impact sur l'activités commerciales
- Définir les circuits d'escalade
- Permettre les notifications sur mobile ou application ("push")
- Communiquer le statut par le biais de tableaux de bord
- Automatiser les réponses aux événements



Excellence opérationnelle



Les bonnes pratiques :

- **Évoluer**
 - **Comment faites-vous évoluer les opérations ?**
 - Avoir un processus d'amélioration continue
 - Mettre en place des remontées d'informations
 - Définir les vecteurs d'amélioration
 - Valider les opinions exprimées pour intégrations
 - Effectuer des examens réguliers des métriques liées aux opérations
 - Documenter et partager les expériences acquises
 - Allouer du temps pour apporter des améliorations

Improvement Plan
Each day it's Day One

TOUS MES SOUHAITS DE REUSSITE



ROAD TO SUCCESS