Engineer

AWS

la plateforme cloud d'Amazon

Ce que c’est

AWS, abréviation d’Amazon Web Services, est l’activité d’Amazon qui loue de l’informatique à l’heure et au gigaoctet : serveurs virtuels, stockage de fichiers, bases de données gérées, réseaux privés, files d’attente et un long catalogue d’autres services, activés par une API et facturés à un compte. Amazon la commercialise depuis 2006. Deux des services les plus connus expliquent une grande partie du reste. Amazon EC2 loue des machines virtuelles, qu’AWS appelle instances, et Amazon S3 stocke des fichiers comme objets dans des conteneurs nommés compartiments.

Dans le vocabulaire du NIST, AWS est un cloud public : toute personne munie d’une carte de paiement peut ouvrir un compte, les ressources apparaissent en quelques minutes et chaque seconde ou gigaoctet utilisé est mesuré. On le compare généralement à Azure de Microsoft et à Google Cloud, qui vendent des composants semblables sous d’autres noms. Une instance EC2 correspond à une machine virtuelle Azure ou à une instance Compute Engine de Google Cloud.

Chaque ressource AWS réside à un endroit précis. Le service est divisé en régions, chacune conçue pour être isolée des autres et contenant plusieurs zones de disponibilité. Une zone est constituée d’un ou plusieurs centres de données distincts, avec alimentation, réseau et connectivité redondants, physiquement séparés des autres zones de sa région. Une ressource est créée dans une région, souvent dans une zone unique, et l’équipe choisit le lieu selon latence, droit et prix.

Les accès passent par AWS Identity and Access Management, ou IAM. Un compte commence avec un utilisateur racine capable de tout faire. IAM ajoute utilisateurs, groupes, rôles et politiques indiquant quels appels API sont autorisés

sur quelles ressources et dans quelles conditions. La plupart des questions de sécurité AWS se révèlent être des questions sur ces politiques.

Utilisez le concept pour prendre une décision

Utilisez « Que signifie AWS? » pour éclairer une décision réelle. Nous pouvons vous aider à relier ce concept au système que vous construisez ou achetez. Des serveurs dimensionnés selon vos usages réels, migrés vers le cloud ou hors du cloud, avec une estimation préalable de la facture mensuelle.

Découvrir nos prestations Contactez-nous →

Vérifiez les hypothèses derrière le terme

Appuyez-vous sur l'explication et les réalisations liées pour formuler les questions de votre projet. Nous pouvons examiner les hypothèses avec vous avant le choix d'un outil. 20 applications Docker sur Google Cloud et AWS — 20 applications conteneurisées déployées et surveillées

20 applications Docker sur Google Cloud et AWS Contactez-nous →

Pourquoi c’est important

Les équipes choisissent AWS pour son étendue. Un produit nécessitant PostgreSQL géré, file d’attente, réseau de diffusion de contenu, stockage objet et hébergement de conteneurs peut les réunir sous une facture et un système d’identité, documentés selon un modèle commun. Cette étendue constitue aussi le prix. Chaque service a ses propres dimensions de tarification, limites et partie du langage IAM. Une équipe adoptant dix services maintient donc dix petites intégrations aux interfaces Amazon. Partir plus tard nécessite de remplacer chacune.

Le deuxième choix est ce qui reste au client. Le modèle de responsabilité partagée d’AWS trace la frontière avec deux expressions : AWS répond de la sécurité « du cloud », à savoir « le matériel, les logiciels, les réseaux et les installations qui font fonctionner les services AWS Cloud », tandis que le client répond de la sécurité « dans le cloud ». La frontière varie selon le service. Sur une instance EC2, le client met à jour le système invité, entretient chaque programme et configure le groupe de sécurité, pare-feu en amont de l’instance. Sur S3 ou DynamoDB, AWS exploite système et plateforme. Le client conserve les données, leurs options de chiffrement et les permissions qui déterminent leurs lecteurs.

Le troisième choix est le coût, propriété de la conception plutôt que facture découverte après coup. Le Well-Architected Framework d’Amazon définit six piliers d’examen d’une charge : excellence opérationnelle, sécurité, fiabilité, efficacité des performances, optimisation des coûts et durabilité. Le coût y figure parce que le même système peut devenir bon marché ou cher par des choix de première semaine : tailles d’instances, nombre de zones, volume sortant de la région et services gérés remplaçant un processus sur un simple serveur.

À quoi cela ressemble en pratique

Sur la page des technologies, AWS figure avec Google Cloud parmi les deux clouds de référence, Azure étant ajouté lorsqu'un client l'utilise déjà.

Une mission utilisait les deux clouds simultanément : vingt applications Docker fonctionnaient sur Google Cloud et AWS, dont des applications analytiques fondées sur R. Elles étaient déployées et entretenues avec la même configuration et la même supervision dans chaque cloud, afin qu'aucune ne devienne un cas particulier. Lorsqu'un problème survenait, le diagnostic passait par Podman et celui de l'orchestration par Kubernetes. Les applications analytiques restaient stables et reproductibles en production des deux côtés.

Une autre mission allait dans l'autre sens. Pour un client international, une installation AWS surdimensionnée avait accumulé des services inutilisés, avec un coût devenu disproportionné aux besoins de l'entreprise. Le travail a examiné les services utilisés, supprimé les inutiles, ajusté la capacité restante et déplacé les charges hors d'AWS. Ces changements d'infrastructure sont les travaux livrés décrits par le dossier. Celui-ci n'établit ni ratio de coût à périmètre comparable, ni mesure de productivité, ni migration sans interruption. L'exemple est utile pour sa méthode d'examen de l'installation existante et d'adaptation de ce que l'entreprise doit exploiter, pas comme promesse d'une économie donnée.

Les deux exemples reviennent à la même habitude. Un service payé à l'usage facture tout ce qui a été activé. Un parc AWS reste donc sain lorsque quelqu'un continue à comparer ce qui fonctionne à ce que l'entreprise utilise.

Où les problèmes surviennent

AWS perd rarement des données ou reste indisponible longtemps. Les incidents coûteux commencent généralement dans le compte du client lui-même.

L'utilisateur racine assure le travail quotidien. Chaque compte commence avec un utilisateur racine, associé à l'adresse électronique et au mot de passe utilisés pour l'ouvrir, avec accès illimité à toutes les ressources et tous les réglages, fermeture du compte comprise. Se connecter comme racine pour les tâches ordinaires donne donc accès à tout par un seul mot de passe divulgué. AWS conseille de protéger ces identifiants, d'y ajouter l'authentification multifacteur et de les réserver aux rares opérations nécessaires. Le quotidien passe par connexion fédérée et rôles.

Des clés d'accès durables fuient. Une paire de clés reste valide jusqu'à suppression et se déplace facilement : fichiers cachés d'un ordinateur portable, variable CI, image de conteneur, commit. Les bonnes pratiques IAM partent de l'inverse. Les personnes se connectent par un fournisseur d'identité et reçoivent des identifiants temporaires ; les charges reçoivent ceux d'un rôle IAM attaché à leur environnement de calcul. Lorsqu'une clé durable est réellement nécessaire, renouvelez-la et supprimez les clés, utilisateurs et rôles devenus inutilisés.

Une alerte budgétaire est prise pour un frein. AWS Budgets avertit lorsque les dépenses réelles ou prévues franchissent un seuil, et ses chiffres sont actualisés jusqu'à trois fois par jour : une alerte rapporte donc de l'argent déjà dépensé. Les ressources continuent à fonctionner et à facturer. Budgets peut aussi agir, notamment appliquer une politique IAM ou de contrôle de service empêchant de nouvelles ressources, ou intervenir sur des instances EC2 ou RDS précises. Il ne le fait que si cette action a été configurée à l'avance avec un rôle d'exécution.

Tout réside dans une seule zone de disponibilité. Une instance unique avec un disque unique dans une zone est l'organisation la moins chère, mais partage le destin de ce lieu. Les zones existent pour qu'une panne électrique ou réseau dans l'une laisse les autres fonctionner, et AWS recommande de répartir l'application entre plusieurs. Une base importante reçoit une réplique de secours dans une seconde zone ; la couche Web des instances dans au moins deux zones, derrière un répartiteur couvrant les deux.

Un compartiment ouvert pour une démonstration reste ouvert. Les nouveaux compartiments S3 bloquent l'accès public en l'absence de configuration contraire, mais une politique de compartiment ou une permission d'objet peut changer cela en une minute. Un lien partagé avec un client pour un après-midi reste public un an plus tard. S3 Block Public Access, au niveau du compte ou de l'organisation, prévaut sur ces politiques. Activez-le lorsque le compte n'a aucune raison de publier des fichiers, et servez les fichiers publics depuis un compartiment prévu pour cela.

Pour aller plus loin

- Documentation AWS — index des guides utilisateurs, références d'API et tutoriels pour chaque service AWS.
- Responsabilité partagée — répartition des couches sécurisées par AWS et par le client dans le pilier sécurité.

- Les piliers du cadre — six domaines d'examen d'une charge, notamment coût et fiabilité.
- Régions et zones de disponibilité AWS — isolation des régions et zones et intérêt de répartir une application entre plusieurs zones.
- Bonnes pratiques de sécurité IAM — fédération, rôles, authentification multifacteur, racine et moindre privilège.
- Gérer les coûts avec AWS Budgets — budgets réels et prévisionnels, notifications et actions exécutables.

Glossaire

Choisissez selon vos contraintes réelles

Présentez le parcours de déploiement, les risques opérationnels et les personnes d'astreinte. Nous pouvons définir un changement avec des vérifications, une procédure de reprise et une responsabilité claire.

Consulter les tarifs Contactez-nous →

Rendez la terminologie concrète

Demandez comment « Que signifie AWS? » s'applique à votre organisation. Un exemple concret tiré de votre système actuel suffit pour engager la discussion.

Découvrir nos prestations

welcome@engineer.company +45 50 10 61 84 Copenhague, Danemark

Emportez cette page avec vous

Fiche de contact

Créé avec soin et amour par D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Droit d'auteur © 2025 – aujourd'hui · Engineer ApS · Tous droits réservés.

Imprimé depuis https://engineer.company/fr/glossary/aws/