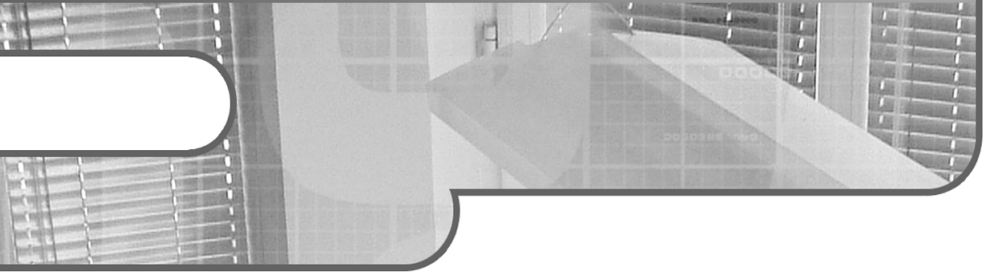


Chapitre 2
La sécurité et la gestion de l'accès

1. Introduction

Les chapitres précédents nous ont permis de faire nos premiers pas dans la compréhension du cloud AWS. À partir de maintenant, nous allons approfondir chacun des concepts et des services mentionnés dans la partie introductive et, pour commencer, nous allons nous attaquer à un sujet central : la sécurité. On va parler de la sécurité en général, de la manière dont AWS implémente un bon nombre des bonnes pratiques liées à la sécurité, aux utilisateurs et rôles et du service IAM (*Identity and Access Management*).

2. La sécurité du cloud

La sécurité est un prérequis fondamental de chaque application, service ou composant logiciel, que ce soit on-premise, dans le datacenter ou sur le cloud. Il est primordial de protéger nos données d'entreprise contre des cyberattaques, brèches de sécurité et pertes de données accidentelles ou délibérées.

De nos jours, les fournisseurs de cloud offrent les mêmes services de sécurité que les datacenters traditionnels. La seule différence consiste dans le fait que, pour ces derniers, on doit prendre en considération les complexités et les coûts de sécurisation des équipements matériels, alors que dans le cloud cette responsabilité est déléguée aux fournisseurs. C'est une différence capitale qui non seulement réduit drastiquement les coûts que l'organisation doit engager, mais qui en plus diminue le temps et l'effort nécessaire pour le monitoring et la protection des ressources.

Une des premières questions à se poser, après avoir créé son compte AWS et avant d'y stocker ses données et exécuter ses applications, est donc de savoir si ce cloud est suffisamment sécurisé. La réponse est clairement oui.

Jetons un coup d'œil aux différents niveaux de sécurité qu'AWS met en place afin de protéger nos ressources :

– La sécurité des datacenters. Toute l'infrastructure AWS, y compris les datacenters, les équipements matériels, les réseaux, les câbles, les volumes de stockage, les processeurs, etc., est conçue en conformité avec les meilleures pratiques de la sécurité. Les datacenters sont hébergés dans des bâtiments banalisés, dont la localisation est secrète et dont l'accès est strictement contrôlé.
– La sécurité des systèmes d'exploitation. Qu'il s'agisse de systèmes d'exploitation natifs ou virtuels, AWS effectue de manière systématique des audits de sécurité et applique tous les patches ou autres corrections de sécurité, afin de réduire à zéro les risques d'attaques comme du DDoS (*Distributed Denial of Services*) ou autres.
– La conformité règlementaire. L'infrastructure AWS est certifiée pour la sécurité et la protection de données en accord avec les normes SOC 1, SOC 2, SOC 3, FISMA, DIACAP, FedRAMP, ISO 27001 et HIPAA.

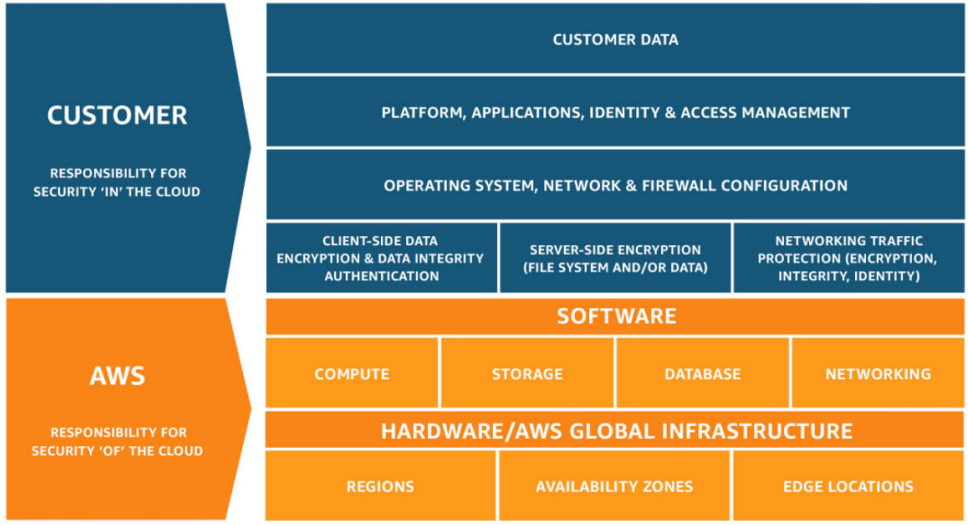
Pour plus de détails sur la sécurité AWS, voir http://aws.amazon.com/security.

© Editions ENI - All rights reserved

3. Le modèle de la responsabilité partagée

On vient de voir de quelle manière AWS protège ses ressources matérielles et logicielles, natives ou virtuelles. Mais qu'en est-il de nos données, applications et services, qui les protègent eux ? C'est là qu'AWS introduit le modèle de la responsabilité partagée.

Selon ce modèle, AWS fournit l'ensemble de l'infrastructure de sécurité, des services et des éléments constitutifs nécessaires, alors que nous, en tant qu'utilisateurs finaux, sommes responsables de la sécurité de nos données, applications et systèmes d'exploitation. La figure ci-dessous montre une représentation schématique de ce modèle.



Le modèle de la responsabilité partagée

AWS fournit un certain nombre d'outils spécifiquement désignés pour nous aider à sécuriser nos applications et services, outils parmi lesquels on mentionne IAM (*Identity Access Management*), MFA (*Multi Factor Authentication*), AWSCloudTrail, et bien d'autres...

Dans la section suivante nous allons examiner IAM, l'outil le plus incontournable pour la sécurité du cloud AWS.

4. IAM (Identity Access Management)

IAM est un service web qui fournit un certain nombre de mécanismes pour le contrôle de l'accès sécurisé destiné à l'ensemble des services AWS. Il est notamment utilisé pour la création des utilisateurs et groupes d'utilisateurs, pour la gestion des permissions et polices de sécurité, etc. Vous l'avez déjà utilisé dans le chapitre introductif lorsque vous avez créé votre compte AWS. Il est complètement gratuit, ce qui ne gâche rien.

Voici un aperçu rapide de ses principales fonctionnalités :

– Accès partagé à un seul compte. Lorsque vous avez effectué le processus d'enregistrement sur AWS, vous avez créé un compte dont vous êtes le seul utilisateur et propriétaire. Mais que se passe-t-il si vous avez besoin de donner accès à votre compte à d'autres utilisateurs de votre organisation ? Hors de question de leur donner vos accréditations, du reste créer autant de comptes que d'utilisateurs serait sans doute une très mauvaise pratique. Avec IAM, vous pouvez créer autant d'utilisateurs que vous voulez et leur accorder l'accès partagé à un seul et unique compte. Ce n'est pas vraiment le cas ici.

– Authentification de type multifacteur. IAM permet l'authentification de type multi-facteur. Cela signifie que, en plus des accréditations classiques basées sur un nom d'utilisateur et un mot de passe, on peut s'authentifier grâce à une clé secrète ou un code stocké sur un périphérique spécial, comme une smart card, un token ou même une application comme, par exemple, Google Authenticator.

– Intégration avec d'autres produits AWS. IAM peut être intégré avec la plupart des produits AWS de manière à fournir un accès granulaire aux services.

– Fédération des identités. Vos utilisateurs et groupes sont déjà stockés au sein d'un annuaire LDAP ou Active Directory on-premise que vous souhaitez continuer d'utiliser ? Aucun problème, vos utilisateurs, groupes et rôles existants peuvent devenir également des utilisateurs, groupes et rôles IAM.

– Disponibilité globale. Vous vous souvenez des notions de zones de disponibilité et régions discutés dans le chapitre introductif ? Eh bien IAM est un des rares services AWS disponible globalement, quelle que soit votre région.

© Editions ENI - All rights reserved

– Mécanismes d'accès. IAM peut être accessible via un certain nombre d'outils différents, le plus fréquemment utilisé étant la console de management AWS. En outre, IAM est accessible via AWS CLI, Terraform, le SDK (*Software Development Kit*) Java ou .NET, des langages de programmation comme Python et Ruby, ou son API REST.

5. Démarrer avec la console IAM

La méthode la plus largement utilisée pour accéder à IAM est de se connecter à la console AWS. Le plus facile est de se rendre dans **Services** et rechercher IAM. En cliquant sur le lien, la page d'accueil du service s'ouvre, comme ci-dessous :

La console IAM

Prenez un moment pour vous familiariser avec la structure visuelle de la console IAM. Comme vous le remarquez, il y a un volet de navigation à gauche de l'écran qui contient des liens vers les fonctions de base, par exemple, la création des utilisateurs, des groupes, etc. Le volet principal, sur le côté droit de l'écran, comporte, quant à lui, des informations diverses et variées sur des ressources et états.

Une des premières choses que l'on remarque dans la partie **Statut de Sécurité** est l'option **Supprimer vos clés racine**. Mais pourquoi voudrait-on faire pareille action avant même d'avoir créé des utilisateurs et des groupes ? Et qu'est-ce donc une clé racine ?

Précédemment, dans le chapitre introductif, lorsque vous aviez créé votre compte AWS, vous vous êtes identifié avec un nom d'utilisateur et un mot de passe. Eh bien, ceci est votre compte racine (root) qui, comme son nom l'indique, possède un accès privilégié et total à tous les services AWS, y compris le service de facturation et de carte de crédit. AWS recommande donc, comme une bonne pratique, de ne pas utiliser ce compte pour quoi que ce soit, mais de créer des utilisateurs séparés et surtout de ne pas utiliser des clés racines. Celles-ci, formées d'un identifiant et d'un secret, peuvent être utilisées de manière programmatique pour accéder à n'importe quel service AWS sous votre compte. D'où l'intérêt de ne pas créer des clés racines, et de les supprimer si vous en avez déjà générées, mais plutôt de dédier des clés à chacun des utilisateurs que vous allez provisionner dans votre infrastructure.

Pour revenir à la console IAM, faisons rapidement le tour des tâches que vous pourriez accomplir. Une des premières choses que l'on remarque est une URL bizarre et incompréhensible pour des humains, tellement elle est longue et illisible. Il s'agit de l'URL que les utilisateurs IAM, que vous allez créer, vont devoir utiliser pour s'authentifier avec la console AWS.

Ainsi, la première chose à faire est de personnaliser cette URL pour pouvoir se le rappeler.

- Cliquez donc sur le bouton **Personnaliser** à droite de l'URL et, dans la boîte de dialogue qui s'affiche, entrez l'alias de votre choix, simple à mémoriser, par exemple "sushi". Vous voilà maintenant prêt à créer des utilisateurs.

© Editions ENI - All rights reserved