Présentation de l'audit de l'utilisation du cloud AWS

Octobre 2015

Mentions légales

Ce document est fourni à titre informatif uniquement. Il présente l'offre de produits et les pratiques actuelles d'AWS à la date de publication de ce document, des informations qui sont susceptibles d'être modifiées sans avis préalable. Il incombe aux clients de procéder à leur propre évaluation indépendante des informations contenues dans ce document et chaque client est responsable de son utilisation des produits ou services AWS, chacun étant fourni « en l'état », sans garantie d'aucune sorte, qu'elle soit explicite ou implicite. Ce document ne crée pas de garanties, représentations, engagements contractuels, conditions ou assurances à l'encontre d'AWS, de ses affiliés, fournisseurs ou donneurs de licence. Les responsabilités et obligations d'AWS vis-à-vis de ses clients sont régies par les contrats AWS. Le présent document ne fait partie d'aucun et ne modifie aucun contrat entre AWS et ses clients.

Table des matières

Résumé 4

Introduction 5

Approches d'utilisation des guides d'audit AWS 6

Auditeurs 6

Preuve fournie par AWS 7

Audit de l'utilisation des concepts AWS 8

Identification des ressources dans AWS 9

Identificateurs de compte AWS 9

1. Gouvernance 10
2. Configuration et gestion du réseau 14
3. Gestion et configuration des ressources 16
4. Contrôle de l'accès logique 17
5. Chiffrement des données 20
6. Journalisation et surveillance de la sécurité 21
7. Réaction aux incidents de sécurité 23
8. Reprise après sinistre 24
9. Contrôles hérités 25

Annexe A : Références et suggestions de lecture 27

Annexe B : Glossaire 28

Annexe C : Appels d'API 29

Résumé

La sécurité chez AWS est une priorité. Tous les clients d'AWS bénéficient d'une architecture réseau et d'un centre de données conçus pour répondre aux besoins des entreprises les plus pointilleuses en termes de sécurité. Afin de satisfaire leurs besoins, la conformité d'AWS permet aux clients d'appréhender les contrôles rigoureux mis en place chez AWS pour assurer la sécurité et la protection des données dans le cloud.

Lorsque des systèmes sont créés sur l'infrastructure de cloud AWS, les responsabilités en termes de conformité sont partagées. En reliant les fonctions de service axées sur la gouvernance, compatibles avec les audits, aux normes de conformité ou d'audit en vigueur, les aides à la conformité AWS s'appuient sur des programmes classiques pour aider les clients à construire et à opérer dans un environnement de contrôle de sécurité AWS.

AWS gère l'infrastructure sous-jacente et il vous incombe de gérer la sécurité de tout ce que vous déployez dans AWS. En tant que plateforme moderne, AWS vous permet de formaliser la conception de la sécurité, ainsi que les contrôles d'audit, grâce à des processus opérationnels et techniques fiables, automatisés et vérifiables, intégrés à tous les comptes client AWS. Le cloud simplifie l'utilisation du système pour les administrateurs et les utilisateurs informatiques, et facilite le contrôle d'un échantillon de test de votre environnement AWS, AWS pouvant transférer les audits vers une vérification à 100 % contrairement aux tests d'échantillon traditionnels.

De plus, les outils spécialisés d'AWS s'adaptent aux exigences du client et aux objectifs d'audit et de dimensionnement, en plus de prendre en charge la vérification en temps réel et la création de rapports à l'aide des outils internes tels que AWS CloudTrail, Config et CloudWatch. Ces outils sont conçus pour vous aider à optimiser la protection de vos services, données et applications. Cela signifie que les clients AWS passent moins de temps sur les opérations de sécurité habituelles et les tâches d'audit, et se concentrent ainsi davantage sur des mesures proactives qui continuent d'améliorer la sécurité et les capacités d'audit de l'environnement client AWS.

Introduction

Comme de plus en plus de clients déploient des charges de travail dans le cloud, les auditeurs doivent maîtriser davantage le fonctionnement du cloud, et trouver comment exploiter la puissance du cloud computing à leur avantage lorsqu'ils mènent des audits. Le cloud AWS permet aux auditeurs de passer d'un test d'échantillon basé sur un pourcentage à une vision d'audit complet en temps réel, qui contrôle 100 % de l'environnement du client et permet ainsi une gestion des risques en temps réel.

Associée à l'interface de ligne de commande (CLI), la console de gestion AWS produit de puissants résultats pour les auditeurs de divers organismes de réglementation, standards et autorités du secteur. En effet, AWS prend en charge une multitude de configurations pour établir des capacités d'audit de sécurité, de conformité dans la conception et d'audit en temps réel par l'utilisation des éléments suivants :

- **Automatisation** : l'infrastructure pouvant contenir des scripts (c'est-à-dire l'infrastructure en tant que Code) vous permet de créer des systèmes de déploiement reproductibles, fiables et sécurisés en exploitant le déploiement de services programmables (pilotés par des API).

- **Architectures pouvant contenir des scripts** : vous pouvez déployer des environnements « finaux » et des images machine Amazon (AMI) pour bénéficier de services fiables pouvant faire l'objet d'un contrôle, et les limiter à la gestion des risques en temps réel.

- **Distribution** : les capacités fournies par AWS CloudFormation permettent aux administrateurs système de créer facilement un ensemble de ressources AWS liées entre elles et de les mettre en service de manière ordonnée et prévisible.

- **Vérifiable** : à l'aide de CloudTrail, Amazon CloudWatch, AWS OpsWorks et AWS CloudHSM vous permettent de bénéficier de fonctions de collecte de preuves d'audit.

Approches d'utilisation des guides d'audit AWS

Auditeurs

Lors de l'évaluation d'une entreprise qui utilise les services AWS, il est essentiel de comprendre le modèle de « responsabilité partagée » entre AWS et le client. Le guide d'audit organise les exigences en points de contrôle et en contrôles de programme de sécurité courant. Chaque contrôle se réfère aux exigences d'audit applicables.

En règle générale, les services AWS sont traités de la même manière que les services d'infrastructure sur site qui ont été traditionnellement utilisés par les clients pour exploiter les services et les applications. Les politiques et les processus qui s'appliquent aux appareils et aux serveurs s'appliquent également quand ces fonctions sont fournies par AWS. Les contrôles relatifs uniquement à la politique ou à la procédure relèvent généralement de l'entière responsabilité du client. De même, la gestion AWS, que ce soit via la console AWS ou la ligne de commande API, doit être traitée comme les autres accès administrateur privilégiés. Pour de plus amples informations, consultez l'annexe et les points référencés.

Preuve fournie par AWS

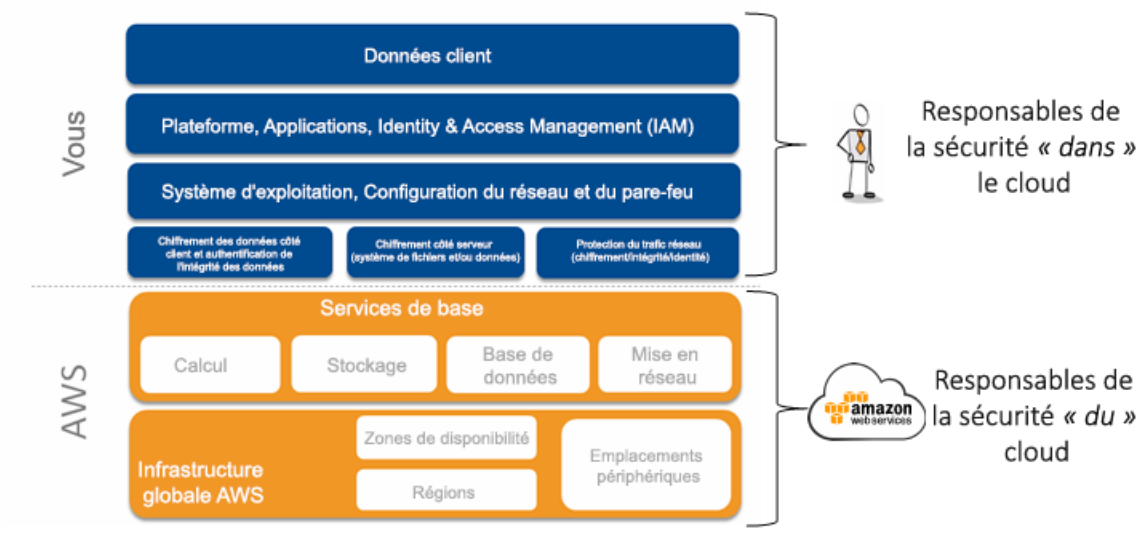
La conformité du cloud AWS permet aux clients d'appréhender les contrôles rigoureux mis en place chez AWS pour assurer la sécurité et la protection des données dans le cloud. Lorsque des systèmes sont créés sur l'infrastructure de cloud AWS, les responsabilités en termes de conformité sont partagées**.** Chaque certification signifie qu'un auditeur a vérifié que les contrôles de sécurité spécifiques sont en place et qu'ils fonctionnent comme prévu. Vous pouvez afficher les rapports de conformité qui s'appliquent en contactant votre représentant AWS. Pour plus d'informations sur les réglementations et les normes de sécurité auxquelles AWS se conforme, consultez la page Web Conformité dans le cloud AWS. Pour vous aider à vous conformer aux réglementations et aux normes de sécurité propres au gouvernement, au secteur et à l'entreprise, AWS fournit des rapports de certification qui décrivent comment l'infrastructure de cloud AWS répond aux exigences d'une longue liste de normes de sécurité mondiales, notamment : la certification ISO 27001, les rapports SOC, la norme PCI DSS, le programme FedRAMP, le manuel de sécurité des informations (ISM) de l'Australian Signals Directorate (ASD) et la norme MTCS SS 584 (Singapore Multi-Tier Cloud Security Standard). Pour plus d'informations sur les réglementations et les normes de sécurité auxquelles AWS se conforme, consultez la page Web Conformité dans le cloud AWS.

Audit de l'utilisation des concepts AWS

Les concepts suivants doivent être pris en considération au cours d'un audit de sécurité des systèmes et des données AWS de l'entreprise :

- Les mesures de sécurité mises en place et gérées par le fournisseur de service de cloud (AWS), c'est-à-dire la « sécurité du cloud »
- Les mesures de sécurité mises en place et gérées par le client, en lien avec la sécurité de contenu et des applications client qui ont recours aux services AWS, à savoir la « sécurité dans le cloud »

AWS gère la sécurité **du** cloud, mais la sécurité **dans** le cloud relève de la responsabilité du client. Les clients gardent le contrôle du type de sécurité qu'ils souhaitent mettre en place afin de protéger leurs propres contenus, plateformes, applications, systèmes et réseaux, de la même manière que s'ils plaçaient leurs applications dans un centre de données sur site.



Pour plus de détails, consultez les pages Sécurité dans le cloud AWS et Conformité dans le cloud AWS et les livres blancs AWS disponibles ici : Livres blancs AWS

Identification des ressources dans AWS

Les ressources AWS d'un client sont des instances, des magasins de données, des applications et des données. L'audit de l'utilisation du cloud AWS commence généralement par l'identification des ressources. Les ressources d'une infrastructure de cloud public *ne sont pas* radicalement différentes de celles d'un environnement sur site, et sont parfois même moins complexes à répertorier car AWS fournit une visibilité des ressources en gestion.

Identificateurs de compte AWS

AWS attribue deux ID uniques à chaque compte AWS : un ID de compte AWS et un ID utilisateur canonique. L'ID de compte AWS comporte 12 chiffres (123456789012, par exemple), qui permet de créer des ARN (Amazon Resource Names). Lorsque vous vous référez aux ressources, comme un utilisateur IAM ou un coffre Amazon Glacier, l'ID de compte distingue vos ressources de celles des autres comptes AWS.

Noms ARN (Amazon Resource Names) et Espaces de nom AWS (AWS Service Namespaces)

Les ARN identifient les ressources AWS de manière unique. L'ARN permet de spécifier une ressource sans aucune ambiguïté sur l'ensemble du cloud AWS, comme par exemple dans les stratégies IAM, les balises Amazon RDS (Amazon Relational Database Service) et les appels d'API.

Exemple de format ARN :

```
    <!-- Elastic Beanstalk application version -->
arn:aws:elasticbeanstalk:us-east-1:123456789012:environment/My App/MyEnvironment

<!-- IAM user name -->
arn:aws:iam::123456789012:user/David

<!-- Amazon RDS tag -->
arn:aws:rds:eu-west-1:001234567890:db:mysql-db

<!-- Amazon S3 bucket (and all objects in it)-->
arn:aws:s3:::my_corporate_bucket/*
```

Outre les identifiants de compte, les ARN (Amazon Resource Names) et les espaces de nom AWS Service Namespaces, chaque service AWS crée un identifiant de service unique (ID d'instance Amazon Elastic Compute Cloud (Amazon EC2) : i-3d68c5cb ou ID de volume Amazon Elastic Block Store (Amazon EBS) : vol-ecd8c122, par exemple) qui permet de créer un inventaire de ressources environnementales et peut être utilisé dans les documents de travail à des fins d'audit et d'inventaire.

Chaque certification signifie qu'un auditeur a vérifié que les contrôles de sécurité spécifiques sont en place et qu'ils fonctionnent comme prévu.

1. Gouvernance

Définition : la gouvernance permet de s'assurer que la direction et les intentions du client apparaissent dans sa posture de sécurité. Pour se faire, il suffit d'utiliser une approche structurée pour mettre en œuvre un programme de sécurité des informations. Dans le cadre de ce programme d'audit, cela signifie qu'il faut comprendre les services AWS qui ont été acquis, savoir quels genres de systèmes et d'information vous envisagez d'utiliser dans le service AWS et quelles politiques, procédures et quels programmes s'appliquent à ces services.

Objet de l'audit principal : identifiez les ressources et les services AWS qui sont utilisés et vérifiez que votre programme de gestion des risques ou de la sécurité a pris en compte l'utilisation de l'environnement de cloud public.

Approche de l'audit : dans le cadre de cet audit, déterminez qui, au sein de votre entreprise, détient une ressource ou un compte AWS, ainsi que les ressources et les services AWS qu'il utilise. Vérifiez les politiques, les programmes et les procédures ainsi que les concepts du cloud, et que le cloud est bien inclus dans le cadre du programme d'audit du client.

Gouvernance - Liste de contrôle

	Elément de la liste de contrôle
☐	Comprendre l'utilisation du cloud AWS au sein de votre entreprise. Les approches peuvent inclure : • Questionnaire ou entretien avec vos équipes en charge de l'informatique et du développement. • Exécution de numérisations réseau ou d'un test d'intrusion plus approfondi. ▪ Etudiez les notes de frais et/ou les paiements des bons de commande (PO) concernant Amazon.com ou AWS pour connaître les services utilisés. Les frais de carte de crédit apparaissent sous « AMAZON WEB SERVICES AWS.AMAZON.CO WA » ou une référence similaire. Remarque : certaines personnes de votre entreprise peuvent avoir souscrit un compte AWS sous leur compte personnel ; par conséquent, demandez-leur si tel est le cas lors du questionnaire ou de l'entretien avec vos équipes informatiques et de développement.
☐	**Identifier les ressources.** Chaque compte AWS dispose d'une adresse e-mail de contact associée qui permet d'identifier les titulaires de compte. Il est important de comprendre que cette adresse e-mail peut être délivrée par un fournisseur de service de messagerie public, selon ce que l'utilisateur a mentionné lors de son enregistrement.

	Elément de la liste de contrôle
	• Vous pouvez organiser une réunion formelle avec chaque titulaire de ressource ou de compte AWS pour connaître les services qui sont déployés sur le cloud AWS, la façon dont ils sont gérés et comment ils sont intégrés dans les politiques, procédures et normes de sécurité de votre entreprise. **Remarque** : le titulaire de compte AWS peut être un membre du service achat ou financier, mais la personne qui *met en œuvre* l'utilisation des ressources AWS de l'entreprise doit faire partie du service informatique. Vous aurez probablement à vous entretenir avec les deux.
☐	**Définir les limites de vérification du cloud AWS.** La vérification doit avoir une étendue définie. Vous devez comprendre les processus métier de votre entreprise et leur adéquation avec l'informatique, sous sa forme non-cloud ainsi que pour des implémentations actuelles ou futures sur le cloud. • Recueillez une description des services AWS utilisés et/ou qu'il est prévu d'utiliser. • Après avoir identifié les types de services AWS utilisés ou à l'étude, déterminez les services et les solutions métier à inclure dans la vérification. • Récupérez et étudiez tous les rapports d'audit précédent, avec les plans de correction. • Identifiez les problèmes ouverts des rapports d'audit précédents et évaluez les mises à jour des documents relatifs à ces problèmes.
☐	**Evaluation des politiques.** Evaluez et étudiez les stratégies de classification de données, de confidentialité et de sécurité de votre entreprise pour identifier les stratégies qui s'appliquent à l'environnement de service AWS. • Vérifiez si un processus et/ou une stratégie d'usage existe autour de l'acquisition de services AWS afin de déterminer dans quelle mesure l'achat de services AWS est autorisé. • Vérifiez si les politiques et les processus de gestion des modifications de votre entreprise prennent en compte les services AWS.
☐	**Identifier les risques.** Déterminez si une évaluation des risques a été menée pour les ressources applicables.
☐	**Vérifier les risques.** Procurez-vous la copie d'un rapport d'évaluation des risques et déterminez si ce rapport reflète l'environnement actuel et s'il décrit précisément l'environnement de risques résiduels.
☐	**Vérifier la documentation sur les risques.** Après chaque élément de votre vérification, vérifiez les plans de traitement des risques et les calendriers/étapes importantes par rapport à vos procédures et politiques de gestion des risques.

	Elément de la liste de contrôle
☐	**Documentation et inventaire.** Vérifiez que votre réseau AWS est entièrement documenté et que tous les systèmes critiques AWS sont inclus dans leur documentation d'inventaire, avec un accès limité à cette documentation. • Vérifiez le paramètre AWS Config de l'inventaire de ressources AWS et de l'historique de configuration des ressources *(Exemple Appel d'API, 1)*. • Assurez-vous que les ressources sont correctement balisées et associées aux données d'application. • Vérifiez l'architecture d'application afin d'identifier les flux de données, la connectivité planifiée entre les composants d'application et les ressources qui contiennent les données. • Vérifiez toutes les connectivités entre votre réseau et la plateforme AWS en examinant les éléments suivants : ▪ Les connexions VPN, où les adresses IP publiques sur site des clients sont mappées aux passerelles client dans n'importe quel VPC appartenant au client. *(Exemple Appel d'API, 2 et 3)*. Les connexions privées Direct Connect, qui peuvent être mappées à un ou plusieurs VPC appartenant au client. *(Exemple Appel d'API, 4)*
☐	**Evaluer les risques.** Evaluez l'importance des données déployées sur le cloud AWS par rapport à la tolérance aux risques et au profil de risque global de l'entreprise. Vérifiez que les ressources AWS sont intégrées au programme d'évaluation officielle des risques de l'entreprise. • Les ressources AWS doivent être identifiées et disposer d'objectifs de protection associés, en fonction de leurs profils de risque.
☐	**Incorporer l'utilisation du cloud AWS dans l'évaluation des risques.** Traitez et/ou intégrez les éléments de service AWS dans vos processus d'évaluation des risques organisationnels. Voici les principaux risques : • Identifiez les risques métier associés à l'utilisation du cloud AWS, ainsi que les propriétaires d'entreprise et les parties prenantes. • Vérifiez que les risques métier sont alignés, ajustés ou classifiés par rapport à votre utilisation des services AWS et vos critères de sécurité organisationnelle pour la protection de la confidentialité, de l'intégrité et de la disponibilité. • Consultez les audits précédents concernant les services AWS (audits associés SOC, PCI, NIST 800-53, etc.).

	Elément de la liste de contrôle
	• Déterminez si les risques identifiés précédemment ont été correctement traités. • Evaluez le facteur de risque global pour l'exécution de la vérification du cloud AWS. • En vous appuyant sur l'évaluation du risque, identifiez les modifications à apporter à l'étendue de votre audit. • Discutez des risques avec les responsables informatiques et ajustez l'évaluation des risques.
☐	**Politique et programme de sécurité informatique.** Vérifiez que le client inclut les services AWS dans ses procédures et politiques de sécurité, y compris les bonnes pratiques au niveau du compte AWS comme souligné dans le service AWS Trusted Advisor qui fournit des conseils et les bonnes pratiques au travers de 4 rubriques : Sécurité, Coûts, Performances et Tolérance aux pannes. • Examinez vos politiques en matière de sécurité des informations et vérifiez qu'elles incluent les services AWS. • Vérifiez que vous avez désigné un ou plusieurs employés comme ayant autorité pour l'utilisation et la sécurité des services AWS et que des rôles ont été définis pour les rôles clés, notamment un poste de Chief Information Security Officer. **Remarque :** toutes les normes de processus de gestion des risques publiées pour la cybersécurité que vous avez utilisées pour élaborer les processus et l'architecture de sécurité des informations. • Assurez-vous de tenir à jour une documentation pour accompagner les audits menés sur les services AWS, notamment son examen des certifications tierces AWS. • Vérifiez que les enregistrements de formation interne comprennent les éléments de sécurité AWS, tels que l'utilisation IAM Amazon, les groupes de sécurité Amazon EC2 et l'accès à distance aux instances Amazon EC2. • Vérifiez qu'une politique de réponse de cybersécurité et que des formations aux services AWS sont disponibles. **Remarque** : toutes les assurances propres à l'utilisation des services AWS par les clients et toutes les réclamations liées aux pertes et dépenses attribuées aux événements de cybersécurité qui en découlent.
☐	**Contrôle du fournisseur de services.** Vérifiez que le contrat avec AWS stipule qu'il est nécessaire d'implémenter et de conserver des protections en termes de confidentialité et de sécurité pour les exigences relatives à la cybersécurité.

2. Configuration et gestion du réseau

Définition : la gestion du réseau dans le cloud AWS est très similaire à la gestion de réseau sur site, à l'exception des composants réseau comme le pare-feu et les routeurs qui sont virtuels. Les clients doivent s'assurer que l'architecture réseau respectent les exigences de sécurité de leur entreprise, notamment l'utilisation de zone démilitarisée (DMZ) pour séparer les ressources publiques et privées (non approuvées et approuvées), la séparation des ressources à l'aide de sous-réseaux et de tables de routage, la configuration sécurisée de DNS, qu'une protection de transmission supplémentaire soit requise ou non sous la forme d'un VPN, ou que ce soit pour limiter le trafic entrant et sortant. Les clients qui doivent effectuer un contrôle de leur réseau peuvent le faire par le biais de la détection d'intrusion basée sur les hôtes, et des systèmes de surveillance.

Objet de l'audit principal : contrôles de sécurité absents ou configurés de façon inappropriée liés à la sécurité réseau/accès externe pouvant entraîner une exposition aux risques de sécurité.

Approche de l'audit : étudiez l'architecture réseau des ressources AWS du client et les ressources qui sont configurées pour permettre l'accès externe depuis le réseau Internet public et les réseaux privés du client. Remarque : AWS Trusted Advisor peut être exploité pour valider et vérifier les paramètres de configuration du cloud AWS.

Configuration et gestion du réseau - Liste de contrôle

	Elément de la liste de contrôle
☐	**Contrôles réseau.** Identifiez la façon dont la segmentation réseau est appliquée au sein de l'environnement de cloud AWS. • Etudiez l'implémentation du groupe de sécurité AWS, les configurations d'AWS Direct Connect et du VPN Amazon afin de mettre en œuvre la segmentation réseau et les paramètres de listes de contrôle d'accès (ACL) et de pare-feu, ou les services AWS *(Exemple Appel d'API, 5 - 8)*. • Vérifiez que vous disposez d'une procédure pour octroyer un accès VPN ou Internet distant aux employés pour accéder à la console AWS et un accès à distance aux systèmes et réseaux Amazon EC2. • Examinez les éléments suivants pour conserver un environnement de test et de développement de logiciels et d'applications distinct de l'environnement d'entreprise :

	▪ L'isolement VPC est en place entre l'environnement d'entreprise et les environnements utilisés pour les tests et le développement. ▪ En contrôlant la connectivité d'appairage VPC entre les VPC pour s'assurer que l'isolement réseau est en place entre les VPC. ▪ L'isolement de sous-réseau est en place entre l'environnement d'entreprise et les environnements utilisés pour les tests et le développement. ▪ En examinant les listes de contrôle d'accès réseau (NACL) associées aux sous-réseaux qui hébergent l'environnement d'entreprise et les environnements de test et de développement pour s'assurer que l'isolement réseau est en place. ▪ L'isolement de l'instance Amazon EC2 est en place entre l'environnement d'entreprise et les environnements utilisés pour les tests et le développement. ▪ En examinant les groupes de sécurité associés à une ou plusieurs instances qui sont associées à l'environnement d'entreprise et aux environnements de test et de développement pour s'assurer que l'isolement réseau est en place entre les instances Amazon EC2. ▪ Vérifiez l'exécution de la solution de défense en couche DDoS qui agit directement sur les composants de révision AWS qui sont exploités dans le cadre de la solution DDoS, tels que : ▪ La configuration d'Amazon CloudFront ▪ La configuration d'Amazon S3 ▪ Amazon Route 53 ▪ La configuration ELB ▪ Remarque : les services ci-dessus n'utilisent pas les adresses IP publiques du client et offrent les fonctions de diminution Dos héritées du DoS AWS. ▪ Utilisation d'Amazon EC2 pour le Proxy ou le WAF Vous trouverez davantage de conseils à la page « AWS Best Practices for DDoS Resiliency Whitepaper » du livre blanc sur la résilience.
☐	**Contrôles des codes malveillants.** Evaluez l'implémentation et la gestion du programme de détection de logiciel malveillant (anti-malware) pour les instances Amazon EC2 de la même manière qu'avec les systèmes physiques.

3. Gestion et configuration des ressources

Définition : les clients du cloud AWS sont responsables de la sécurité de tout ce qui est installé sur les ressources AWS ou connecté aux ressources AWS. Une gestion sécurisée des ressources AWS du client signifie que vous connaissez les ressources que vous utilisez (inventaire des ressources), que vous sécurisez la configuration des applications et des systèmes d'exploitation invité sur vos ressources (paramètres de configuration sécurisés, correctif et anti-malware) et que vous contrôlez les changements de ressources (gestion des modifications).

Objet de l'audit principal : gérez les failles de sécurité de votre système d'exploitation et de vos applications pour protéger la sécurité, la stabilité et l'intégrité des ressources.

Approche de l'audit : confirmez que le système d'exploitation et les applications sont conçus, configurés, corrigés et renforcés conformément à vos normes, procédures et politiques. Toutes les pratiques de gestion d'application et de système d'exploitation peuvent être communes entre les services et les systèmes sur site et sur le cloud AWS.

Configuration et gestion des ressources - Liste de contrôle

	Elément de la liste de contrôle
☐	**Evaluer la gestion de la configuration.** Vérifiez que vos pratiques de gestion de la configuration sont utilisées pour tous les composants du système AWS et confirmez que les normes respectent les configurations de référence. • Vérifiez la procédure pour réaliser une procédure d'effacement spécialisée avant de supprimer le volume, afin d'être conforme à vos exigences définies. • Examinez votre système de gestion IAM (qui peut être utilisé pour autoriser l'accès authentifié aux applications hébergées par dessus les services AWS). • Confirmez que les tests d'intrusion ont été réalisés.

☐	**Contrôles de gestion des modifications.** Assurez-vous que les services AWS suivent les mêmes processus de contrôle des modifications que les séries internes. • Vérifiez que les services AWS sont inclus dans un processus de gestion des correctifs interne. Examinez les processus documentés relatifs à la configuration et aux correctifs des instances Amazon EC2 : ▪ Images machine Amazon (AMI) *(Exemple Appel d'API, 9 - 10)* ▪ Systèmes d'exploitation ▪ Applications • Examinez les appels d'API des services concernés pour la suppression des appels afin de s'assurer que les ressources informatiques sont correctement éliminées.

4. Contrôle de l'accès logique

Définition : les contrôles d'accès logiques déterminent non seulement qui ou ce qui peut avoir accès à une ressource de système spécifique, mais également le type d'actions pouvant être exécuté sur la ressource (lecture, écriture, etc.). Dans le cadre du contrôle d'accès aux ressources AWS, les utilisateurs et les processus doivent présenter des informations d'identification pour confirmer qu'ils sont autorisés à exécuter des fonctions spécifiques ou à avoir accès aux ressources spécifiques. Les informations d'identification requises par le cloud AWS varient selon le type de service et la méthode d'accès, et incluent les mots de passe, les clés cryptographiques et les certificats. L'accès aux ressources AWS peut être activé via le compte AWS, les comptes utilisateur individuels IAM (Identify and Access Management) AWS créés sous le compte AWS ou la fédération d'identité avec l'annuaire d'entreprise du client (authentification unique). AWS Identity et Access Management (IAM) : permet de contrôler l'accès aux services et ressources AWS de façon sécurisée. Avec IAM, vous pouvez créer et gérer des utilisateurs ainsi que des groupes AWS, et configurer des autorisations afin de leur permettre ou non d'accéder aux ressources AWS.

Objet de l'audit principal : cette partie de l'audit a pour but d'identifier la façon dont les configurations et les utilisateurs sont configurés pour les services du cloud AWS. Il est également important de s'assurer que vous gérez de manière sécurisée les informations d'identification associées à tous les comptes AWS.

Approche de l'audit : confirmez que les autorisations d'accès aux ressources AWS sont gérées conformément à vos processus, procédures et politiques organisationnelles. Remarque : AWS Trusted Advisor peut être exploité pour valider et vérifier les configurations des rôles, des groupes et des utilisateurs IAM.

Contrôle de l'accès logique - Liste de contrôle

	Elément de la liste de contrôle
☐	**Gestion de l'accès, authentification et autorisation.** Vérifiez que des procédures et politiques internes sont définies pour la gestion de l'accès aux services AWS et aux instances Amazon EC2. • Vérifiez que vous disposez de la documentation relative à l'utilisation et à la configuration des contrôles d'accès AWS, exemples et options, ci-dessous : ▪ Description du type d'utilisation d'Amazon IAM dans la gestion de l'accès. ▪ Liste des contrôles gérés habituellement par Amazon IAM (Gestion des ressources, Groupes de sécurité, VPN, Autorisations d'objet, etc). ▪ Utilisation des contrôles d'accès AWS natifs ou si l'accès est géré via une authentification fédérée, qui exploite le format ouvert Security Assertion Markup Language (SAML) 2.0. ▪ Liste des comptes, rôles, groupes et utilisateurs, politiques AWS et rattachements de politique aux utilisateurs, groupes et rôles *(Exemple Appel d'API, 11)*. ▪ Une description des comptes et des rôles Amazon IAM, et des méthodes de surveillance. ▪ Une description et une configuration des systèmes dans EC2.

	Elément de la liste de contrôle
☐	**Accès distant.** Assurez-vous qu'un processus d'approbation ou de journalisation, ou que des contrôles existent afin d'éviter tout accès distant non autorisé. Remarque : tous les accès au cloud AWS et aux instances Amazon EC2 sont des « accès distant » par définition sauf si le paramètre Direct Connect a été configuré. • Vérifiez les processus afin d'éviter les accès non autorisés, comme par exemple : ▪ AWS CloudTrail pour la journalisation des appels d'API de niveau de service. ▪ Journaux AWS CloudWatch pour satisfaire les objectifs de journalisation. ▪ Politiques IAM, stratégies de compartiment S3, groupes de sécurité pour effectuer des contrôles afin d'éviter les accès non autorisés. • Examinez la connectivité entre le réseau d'entreprise et AWS : ▪ Connexion VPN entre le VPC et le réseau d'entreprise. ▪ Direct Connect (interfaces privées et connexions transversales) entre l'entreprise et AWS. ▪ Groupes de sécurité définis, listes de contrôle d'accès réseau et tables de routage afin de contrôler l'accès entre AWS et le réseau.
☐	**Contrôle du personnel.** Etablissez des restrictions pour limiter l'accès des utilisateurs uniquement aux services AWS en rapport avec leurs fonctions dans l'entreprise *(Exemple Appel d'API, 12)*. • Examinez le type de contrôle d'accès qui est en place quand il s'agit des services AWS. ▪ Contrôle d'accès AWS au niveau AWS ; à l'aide de l'IAM avec balisage pour contrôler la gestion des instances Amazon EC2 (démarrer/arrêter/mettre fin) dans les réseaux ▪ Contrôle d'accès client ; à l'aide de l'IAM (solution LDAP) pour gérer l'accès aux ressources qui existent sur les réseaux au niveau Système d'exploitation/Application ▪ Contrôle d'accès réseau ; à l'aide des groupes de sécurité AWS (SG), des listes de contrôle d'accès réseau (NACL), des tables de routage, des connexions VPN, de l'appairage de VPC pour contrôler l'accès réseau aux ressources dans un VPC client.

5. Chiffrement des données

Définition : les données stockées dans le cloud AWS sont sécurisées par défaut ; seuls les titulaires de comptes AWS peuvent accéder aux ressources AWS qu'ils ont créées. Toutefois, les clients qui possèdent des données sensibles peuvent nécessiter une protection supplémentaire en chiffrant les données quand elles sont stockées dans le cloud AWS. Aujourd'hui, le service Amazon S3 est le seul à fournir une fonction de chiffrement automatique côté serveur, en plus de permettre aux clients de chiffrer leurs données de leur côté avant de les stocker. Pour les autres options de stockage de données AWS, le client soit effectuer le chiffrement des données.

Objet de l'audit principal : les données au repos doivent être chiffrées de la même manière que les données sont protégées sur site. De même, de nombreuses politiques de sécurité considèrent Internet comme un moyen de communication non sécurisé et requièrent le chiffrement des données en transit. Une mauvaise protection des données risque d'entraîner des expositions aux risques de sécurité.

Approche de l'audit : déterminez l'endroit où les données résident et validez les méthodes utilisées pour protéger les données au repos et en transit (également appelées les « données en cours d'exécution »). Remarque : AWS Trusted Advisor peut être exploité pour valider et vérifier les autorisations et les accès aux ressources de données.

Chiffrement des données - Liste de contrôle

	Elément de la liste de contrôle
☐	**Contrôles du chiffrement.** Vérifiez que les contrôles en place sont appropriés pour protéger les informations confidentielles en cours de transfert lors de l'utilisation des services AWS. ▪ Examinez les méthodes de connexion à la console AWS, à l'API de gestion, au compartiment S3, à Amazon RDS et au VPN Amazon EC2 pour l'application du chiffrement. ▪ Examinez les procédures et politiques internes définies pour la gestion des clés d'accès, notamment aux services AWS et aux instances Amazon EC2. ▪ Vérifiez les méthodes de chiffrement utilisées, le cas échéant, pour protéger les PIN au repos. AWS offre un certain nombre de services de gestion des clés comme KMS, CloudHSM et le chiffrement côté serveur pour les compartiments S3 qui peut aider au chiffrement des données au repos *(Exemple Appel d'API, 13-15)*.

6. Journalisation et surveillance de la sécurité

Définition : les journaux d'audit enregistrent différents événements qui surviennent au sein de vos réseaux et systèmes d'information. Les journaux d'audit permettent d'identifier une activité qui peut avoir un impact sur la sécurité de ces systèmes, que ce soit en temps réel ou une fois l'événement passé. Par conséquent, il est important d'effectuer correctement la configuration et la protection des journaux.

Objet de l'audit principal : les systèmes doivent être consignés et surveillés, comme les systèmes sur site. Si les systèmes AWS ne sont pas inclus dans un programme de sécurité global de l'entreprise, les systèmes stratégiques risquent d'être omis dans les tâches de surveillance.

Approche de l'audit : confirmez que la journalisation de l'audit est réalisée sur le système d'exploitation invité et les applications critiques installées sur les instances Amazon EC2 et que la mise en œuvre est en adéquation avec vos politiques et procédures existantes, tout particulièrement lorsqu'il s'agit du stockage, de la protection et de l'analyse des journaux.

Journalisation et surveillance de la sécurité - Liste de contrôle

	Elément de la liste de contrôle
☐	**Journalisation du suivi d'évaluation et surveillance.** Vérifiez que les procédures et les politiques de journalisation et de surveillance sont en adéquation avec les seuils de conservation définis et qu'elles disposent d'une maintenance sécurisée, tout particulièrement pour détecter une activité non autorisée sur les services AWS. • Vérifiez que les procédures et les politiques de journalisation et de surveillance intègrent bien les services AWS, notamment les instances Amazon EC2 pour la sécurité relative aux événements. • Vérifiez que les mécanismes de journalisation sont configurés pour envoyer les journaux vers un serveur centralisé. Vérifiez également que pour les instances Amazon EC2, le type et le format des journaux, qui sont conservés de manière identique aux systèmes physiques, sont corrects. • Pour les clients qui utilisent AWS CloudWatch, vérifiez le processus et l'enregistrement de l'utilisation de la surveillance du réseau. • Vérifiez que les événements sont bien analysés afin d'améliorer les politiques et les mesures de prévention. • Examinez le rapport sur les informations d'identification AWS IAM des utilisateurs non autorisés, le paramètre AWS Config et le balisage des ressources des appareils non autorisés *(Exemple Appel d'API, 16)*. • Confirmez le regroupement et la corrélation des données d'événement provenant de plusieurs sources à l'aide des services AWS, telles que : ▪ Journaux de flux VPC pour identifier les paquets réseau acceptés/rejetés entrant dans le VPC. ▪ AWS CloudTrail pour identifier les appels d'API authentifiés et non authentifiés vers les services AWS ▪ Journalisation ELB : journalisation Equilibreur de charge. ▪ Journalisation AWS CloudFront : journalisation des distributions CDN.
☐	**Détection d'intrusion et réponse.** Examinez les ID basés sur les hôtes sur les instances Amazon EC2 de la même manière qu'avec les systèmes physiques. • Vérifiez les preuves fournies par AWS relatives à l'endroit où les informations concernant les processus de détection d'intrusion peuvent être examinées.

7. Réaction aux incidents de sécurité

Définition : sous un modèle de responsabilité partagée, les événements de sécurité peuvent être surveillés par l'interaction à la fois du cloud AWS et du client AWS. AWS détecte et réagit aux événements qui affectent l'hyperviseur et l'infrastructure sous-jacente. Le client gère les événements depuis le système d'exploitation invité jusqu'à l'application. Vous devez comprendre les responsabilités de la réaction aux incidents et adapter les processus et outils de surveillance/d'alerte/d'audit de sécurité existant à leurs ressources AWS.

Objet de l'audit principal : les événements de sécurité doivent être surveillés quel que soit l'endroit où résident les ressources. L'auditeur peut évaluer la cohérence du déploiement des contrôles de gestion des incidents à travers tous les environnements, et confirmer une couverture totale via les tests.

Approche de l'audit : évaluez l'existence et l'efficacité opérationnelle des contrôles de gestion des incidents des systèmes qui se trouvent dans l'environnement AWS.

Réaction aux incidents de sécurité - Liste de contrôle

	Elément de la liste de contrôle
☐	**Signalement des incidents.** Vérifiez que le plan de réaction aux incidents et la politique de réponse aux incidents de cybersécurité comprennent les services AWS et gèrent les contrôles qui permettent de limiter les incidents de cybersécurité et d'aider à la récupération. • Assurez-vous d'exploiter les outils de surveillance d'incident existant, ainsi que les outils disponibles dans le cloud AWS pour surveiller l'utilisation des services AWS. • Vérifiez que le plan de réaction aux incidents procède à un contrôle périodique et que les modifications relatives au cloud AWS sont effectuées au besoin. • Indiquez si le plan de réaction aux incidents possède des procédures de notification et la méthode utilisée par le client pour répondre à la responsabilité de pertes associées aux attaques ou aux instructions ayant un impact.

8. Reprise après sinistre

Définition : AWS fournit une infrastructure à haut niveau de disponibilité qui permet aux clients de concevoir des applications résilientes et de répondre rapidement aux principaux incidents ou aux situations de sinistre. Toutefois, les clients doivent s'assurer qu'ils configurent des systèmes qui nécessitent un haut niveau de disponibilité ou des délais de récupération rapide pour tirer le meilleur parti des multiples régions et zones de disponibilité qu'offre AWS.

Objet de l'audit principal : un point de défaillance unique non identifié et/ou une planification inappropriée pour traiter les situations de récupération après sinistre risquent d'avoir un impact considérable. AWS fournit des accords de niveau de service (ou SLA) au niveau du service ou de l'instance individuelle, mais ils ne doivent pas être confondus avec les objectifs de continuité des activités du client (BC) et de reprise après sinistre (DR), tels que l'objectif de durée de récupération (RTO) et l'objectif de point de récupération (RPO). Les paramètres BC/DR sont associés à la conception de la solution. Une conception plus résiliente utilise souvent plusieurs composants dans différentes zones de disponibilité AWS et implique la réplication de données.

Approche de l'audit : examinez le paramètre de reprise après sinistre et déterminez l'architecture tolérante aux défaillances employée pour les ressources critiques. Remarque : AWS Trusted Advisor peut être exploité pour valider et vérifier certains aspects des capacités de résilience du client.

Reprise après sinistre - Liste de contrôle

	Elément de la liste de contrôle
☐	**Plan de continuité des activités (BCP)** Vérifiez qu'un plan de continuité des activités (BCP) complet, utilisé pour les services AWS, permet de limiter les effets des incidents de cybersécurité et/ou de la reprise suite à un tel incident. • Au sein de ce plan, vérifiez que le cloud AWS est bien inclus dans le dispositif de préparation aux urgences et les éléments de gestion de crise, dans les responsabilités de surveillance du responsable senior et dans le programme de test.
☐	**Contrôles de la sauvegarde et du stockage.** Vérifiez les tests périodiques du client concernant son système de sauvegarde des services AWS *(Exemple Appel d'API, 17-18)*. 1. Examinez l'inventaire des données sauvegardées dans les services AWS comme une sauvegarde hors site.

9. Contrôles hérités

Définition : Amazon possède plusieurs années d'expérience dans la conception, l'élaboration et le fonctionnement de centres de données à grande échelle. Cette expérience a été mise à profit pour l'élaboration de la plateforme et de l'infrastructure d'AWS. Les centres de données AWS sont hébergés au sein d'installations anonymes. L'accès physique est strictement contrôlé à la fois dans l'enceinte et aux points d'accès du bâtiment par des professionnels de la sécurité utilisant la vidéosurveillance, des systèmes de détection d'intrusion et d'autres moyens électroniques. Le personnel autorisé doit passer avec succès au moins deux authentifications à deux facteurs pour pouvoir accéder aux étages des centres de données. Tous les visiteurs et sous-traitants sont tenus de présenter une pièce d'identité et sont enregistrés à leur arrivée, puis escortés en permanence par le personnel habilité.

AWS n'autorise l'accès aux centres de données et la diffusion d'informations en la matière qu'au personnel et aux sous-traitants en ayant légitimement besoin dans le cadre de leurs activités professionnelles. Lorsqu'un employé n'a plus besoin de tels privilèges pour remplir ses fonctions, son accès est immédiatement révoqué, même s'il fait toujours partie d'Amazon ou d'Amazon Web Services. L'accès physique aux centres de données par le personnel d'AWS est consigné et audité systématiquement.

Objet de l'audit principal : cette section relative à l'audit a pour but de démontrer toutes les précautions nécessaires à prendre lors de la sélection de vos fournisseurs de services.

Approche de l'audit : étudiez comment demander et évaluer les attestations et certifications émanant d'organismes tiers afin de s'assurer, dans une mesure raisonnable, de l'efficacité de conception et de fonctionnement des objectifs de contrôle et des contrôles eux-mêmes.

Contrôles hérités - Liste de contrôle

	Elément de la liste de contrôle
☐	**Contrôles de l'environnement et de la sécurité physique.** Vérifiez les preuves fournies par AWS pour obtenir des détails sur l'endroit où les informations concernant les processus de détection d'intrusion peuvent être examinées, dont les contrôles concernant la sécurité physique sont gérés par AWS.

Conclusion

De nombreux outils tiers sont à votre disposition pour vous aider dans le cadre de votre processus d'évaluation. Ayant le contrôle total de leurs systèmes d'exploitation, des paramètres réseau et du routage du trafic, les clients AWS peuvent utiliser la majorité des outils utilisés sur site pour leur évaluation et l'audit des ressources dans AWS.

L'outil AWS Trusted Advisor fournit pas AWS est très utile. AWS Trusted Advisor se base sur les meilleures pratiques tirées de l'historique opérationnel agrégé de l'offre AWS fournie à des centaines de milliers de clients AWS. AWS Trusted Advisor effectue plusieurs vérifications importantes sur votre environnement AWS et émet des recommandations dès lors qu'il existe une possibilité de réaliser des économies, d'améliorer les performances du système ou de remédier à certaines failles de sécurité.

Cet outil peut être exploité pour exécuter certains éléments de la liste de contrôle de l'audit afin d'améliorer et de soutenir les processus d'évaluation et d'audit de votre entreprise.

Annexe A : Références et suggestions de lecture

1. Amazon Web Services : Présentation des procédures de sécurité - https://d0.awsstatic.com/whitepapers/Security/AWS%20Security%20Whitepaper.pdf
2. Livre blanc AWS sur les risques et la conformité – https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf
3. Manuel sur la cybersécurité AWS OCIE - https://d0.awsstatic.com/whitepapers/compliance/AWS_SEC_Workbook.pdf
4. Utilisation d'Amazon Web Services pour la reprise après sinistre - http://media.amazonwebservices.com/AWS_Disaster_Recovery.pdf
5. Exemple d'application de la fédération d'identité pour un cas d'utilisation d'Active Directory - http://aws.amazon.com/code/1288653099190193
6. Authentification SSO (Single-Sign-On, authentification unique) avec Windows ADFS auprès des applications Amazon EC2 .NET - http://aws.amazon.com/articles/3698?_encoding=UTF8&queryArg=searchQuery&x=20&y=25&fromSearch=1&searchPath=all&searchQuery=identity%20federation
7. Authentification des utilisateurs des applications mobiles AWS avec un jeton distributeur automatique http://aws.amazon.com/articles/4611615499399490?_encoding=UTF8&queryArg=searchQuery&fromSearch=1&searchQuery=Token%20Vending%20machine
8. Chiffrement de données côté client avec le SDK AWS pour Java et Amazon S3 - http://aws.amazon.com/articles/2850096021478074
9. Interface de ligne de commande AWS – http://docs.aws.amazon.com/cli/latest/userguide/cli-chap-welcome.html
10. Politique d'utilisation acceptable d'AWS - http://aws.amazon.com/aup/

Annexe B : Glossaire

Authentification : l'authentification est le processus consistant à déterminer si quelqu'un ou quelque chose est bien celui ou ce qu'il prétend être.

EC2 : Amazon Elastic Compute Cloud (Amazon EC2) est un service Web fournissant une capacité de calcul redimensionnable dans le cloud. Destiné aux développeurs, il est conçu pour faciliter l'accès aux ressources informatiques du cloud computing à l'échelle du Web.

Hyperviseur : un hyperviseur, également appelé Virtual Machine Monitor (VMM), est un logiciel de virtualisation de plateforme logicielle/matérielle permettant l'exécution simultanée de plusieurs systèmes d'exploitation sur un même ordinateur hôte.

IAM : le service AWS Identity and Access Management (IAM) permet à un client de créer plusieurs utilisateurs et de gérer les autorisations de chacun d'entre eux au sein du compte AWS associé.

Objet : entités fondamentales stockées dans Amazon S3. Les objets sont composés de données et de métadonnées d'objet. La partie données est opaque pour Amazon S3. Les métadonnées sont un ensemble de paires nom-valeur décrivant des objets. Elles incluent certaines métadonnées par défaut comme la date de la dernière modification et des métadonnées HTTP standard comme le type de contenu. Le développeur peut aussi spécifier des métadonnées personnalisées au moment du stockage de l'objet.

Service : fonctionnalité logicielle ou informatique fournie sur un réseau (EC2, S3, VPC, etc.).

Zone de disponibilité : les emplacements Amazon EC2 sont composés de régions et de zones de disponibilité ou AZ (Availability Zone). Les zones de disponibilité sont des lieux distincts qui sont conçus pour être isolés des défaillances survenant dans les autres zones de disponibilité et fournir une connectivité réseau de faible latence et peu coûteuse aux autres zones de disponibilité dans la même région.

Annexe C : Appels d'API

L'interface de ligne de commande AWS est un outil unique vous permettant de gérer vos services AWS.
http://docs.aws.amazon.com/cli/latest/reference/index.html#cli-aws

1. Liste de toutes les ressources avec balises
    - aws ec2 describe-tags

http://docs.aws.amazon.com/cli/latest/reference/ec2/describe-tags.html

2. Liste de toutes les passerelles client sur le compte AWS des clients :
    - aws ec2 describe-customer-gateways –output table
3. Liste de toutes les connexions VPN sur le compte AWS des clients
    - aws ec2 describe-vpn-connections
4. Liste de toutes les connexions Direct Connect client
    - aws directconnect describe-connections
    - aws directconnect describe-interconnects
    - aws directconnect describe-connections-on-interconnect
    - aws directconnect describe-virtual-interfaces
5. Liste de toutes les passerelles client sur le compte AWS des clients :
    - aws ec2 describe-customer-gateways –output table
6. Liste de toutes les connexions VPN sur le compte AWS des clients
    - aws ec2 describe-vpn-connections
7. Liste de toutes les connexions Direct Connect client
    - aws directconnect describe-connections
    - aws directconnect describe-interconnects
    - aws directconnect describe-connections-on-interconnect
    - aws directconnect describe-virtual-interfaces
8. Utilisation également possible de la commande CLI axée sur le groupe de sécurité :
    - aws ec2 describe-security-groups
9. Liste des AMI actuellement détenues/enregistrées par le client
    - aws ec2 describe-images –owners self
10. Liste de toutes les instances lancées avec une AMI spécifique
    - aws ec2-describe-instances --filters “Name=image-id,Values=XXXXX” (où XXXX = image-id value e.g. ami-12345a12

11. Liste des Rôles/Groupes/Utilisateurs IAM
    - aws iam list-roles
    - aws iam list-groups
    - aws iam list-users
12. Liste des politiques attribuées aux Groupes/Rôles/Utilisateurs :
    - aws iam list-attached-role-policies --role-name XXXX
    - aws iam list-attached-group-policies --group-name XXXX
    - aws iam list-attached-user-policies --user-name XXXX où XXXX désigne un nom de ressource dans le compte AWS client
13. Liste des clés KMS
    - aws kms list-aliases
14. Liste de la politique de rotation des clés
    - aws kms get-key-rotation-status –key-id XXX (où XXX = ID de clé du compte AWS
15. Liste des volumes EBS chiffrés à l'aide des clés KMS
    - aws ec2 describe-volumes "Name=encrypted,Values=true"
    - targeted e.g. us-east-1)
16. Rapport sur les informations d'identification
    - aws iam generate-credential-report
    - aws iam get-credential-report
17. Créez un instantané/une sauvegarde du volume EBS
    - aws ec2 create-snapshot --volume-id XXXXXXX
    - (où XXXXXX = ID du volume dans le compte AWS)
18. Confirmation de l'exécution de l'instantané/de la sauvegarde
    - aws ec2 describe-snapshots --filters “Name=volume-id,Values=XXXXXX)