aws partner network | competency

Compétences vente au détail AWS

Liste de contrôle de validation des partenaires technologiques

Décembre 2019
Version 1.0

Table des matières

Introduction

L'objectif du programme de compétences AWS est de reconnaître les partenaires du réseau de partenaires AWS (« partenaires APN ») qui font preuve de compétences techniques et démontrent la réussite avérée de leurs clients dans des domaines de solutions spécialisées. La liste de contrôle de validation des partenaires du programme de compétences (la « liste de contrôle ») est destinée aux partenaires APN souhaitant postuler au programme de compétences AWS. Cette liste de contrôle fournit les critères nécessaires pour obtenir cette distinction dans le cadre du programme de compétences AWS. Les partenaires APN sont soumis à un audit de leurs capacités lorsqu'ils postulent pour une compétence spécifique. AWS exploite l'expertise interne et une société tierce pour faciliter l'audit. AWS se réserve le droit d'apporter des modifications à ce document à tout moment.

Attentes des parties

Les partenaires APN doivent examiner ce document en détail avant de postuler pour adhérer au programme de compétences AWS, même si toutes les conditions préalables sont remplies. Si les éléments de ce document ne sont pas clairs et nécessitent des explications supplémentaires, contactez votre agent de développement partenaire (« PDR ») ou votre responsable développement partenaire (PDM) AWS dans un premier temps. Votre PDR/PDM contactera le bureau du programme si une assistance supplémentaire est requise.

Lorsqu'ils sont prêts à soumettre une demande d'adhésion au programme, les partenaires APN doivent remplir la colonne Auto-évaluation du partenaire de la liste de contrôle présentée ci-dessous dans le présent document.

Pour soumettre votre candidature :

1. Connectez-vous à APN Partner Central (https://partnercentral.awspartner.com/) en tant que responsable Alliance
2. Sélectionnez « Afficher mon compte APN » à gauche de la page
3. Faites défiler jusqu'à la section « Détails du programme »
4. Sélectionnez « Mettre à jour » en regard du programme de compétences AWS auquel vous souhaitez postuler
5. Remplissez la demande d'adhésion et cliquez sur « Soumettre »
6. Envoyez votre auto-évaluation complétée par e-mail à l'adresse competency-checklist@amazon.com.
    - L'auto-évaluation doit inclure :
        - la catégorie de la solution (engagement client, merchandising et planification corporate, chaîne logistique et distribution, boutiques physiques, numériques et virtuelles, sciences de données avancées de la vente au détail et applications professionnelles clés de la vente au détail) ;
        - le type de déploiement (SaaS ou déploiement du client sur AWS) ;
        - la documentation pour les études de cas AWS (voir les définitions ci-dessous).

Pour toute question relative aux instructions ci-dessus, contactez votre PDR/PDM.
AWS examinera toutes les questions et s'efforcera d'y répondre dans les cinq jours ouvrés pour lancer la planification de votre audit ou demander des informations complémentaires.

Les partenaires APN doivent se préparer à l'audit en lisant la Liste de contrôle, en réalisant une auto-évaluation à l'aide de la Liste de contrôle, et en rassemblant et en organisant des preuves objectives à communiquer à l'auditeur le jour de l'audit.

AWS recommande aux partenaires APN de disposer de personnes capables de discuter en profondeur des exigences lors de l'audit. La meilleure pratique consiste pour le partenaire APN à mettre à disposition le personnel suivant pour l'audit : un ou plusieurs ingénieurs/architectes certifiés AWS hautement techniques, un directeur des opérations qui est responsable des opérations et des éléments de support, et un responsable du développement commercial en charge de la présentation générale. Les partenaires APN doivent s'assurer qu'ils disposent des autorisations nécessaires pour communiquer à l'auditeur (qu'il s'agisse d'AWS ou d'un tiers) toutes les informations contenues dans les preuves objectives ou les démonstrations avant de programmer l'audit.

Programme de compétences vente au détail AWS

Les partenaires de compétences vente au détail AWS fournissent des solutions de vente au détail via l'engagement client, le merchandising et la planification corporate, la chaîne logistique et la distribution au détail, les boutiques physiques, numériques et virtuelles, les sciences de données avancées de la vente au détail et les applications professionnelles clés de la vente au détail.

Catégories de compétences de vente au détail

Les partenaires APN doivent également identifier la catégorie de segment à laquelle leur solution correspond :

- **Engagement client :** solutions de fidélité, gestion des canaux sociaux, gestion de la relation client (CRM), centre d'appels, publicités (numériques et publipostage), SEO et engagement du public qui permettent aux leaders du marketing au détail d'attirer et de conserver de manière proactive les clients avant et après leurs achats.

- **Merchandising et planification corporate :** solutions de commercialisation, réapprovisionnement, planification d'assortiments, planification d'espaces/planogrammes, optimisation des promotions et des prix, gestion des catégories et collaboration des fournisseurs, mises à profit par les équipes de merchandising et de planification corporate.

- **Chaîne d'approvisionnement et distribution :** solutions de chaîne d'approvisionnement et de distribution couvrant les systèmes de gestion d'entrepôt (WMS), la planification des ressources d'entreprise (ERP), l'automatisation de l'entrepôt, l'import/export, le transport et la logistique.

- **Boutiques physiques, numériques et virtuelles :** solutions qui transforment l'expérience d'achat en ligne ou hors ligne couvrant les points de vente, les systèmes de gestion des commandes (OMS), le commerce unifié, l'e-commerce, la « livraison au dernier kilomètre », l'expérience de magasin illimité (sans friction), les innovations numériques (AR/VR, ESL, IoT, Beacons, vocal, reconnaissance, kiosque numérique, miroirs intelligents, écrans interactifs), gestion des ressources numériques (DAM) et paiements.

- **Sciences des données avancées de la vente au détail :** solutions de Data Lake au détail, IA/ML et analytiques qui améliorent l'efficacité opérationnelle, ainsi que la connaissance et l'engagement des clients.

- **Applications professionnelles clés de vente au détail :** solutions d'entreprise clés de vente au détail pour l'administration, les finances, les achats, les ressources humaines, la gestion des employés, le juridique et l'informatique.

Les partenaires APN doivent également identifier quelle catégorie de livraison s'applique à leur solution :

1. **SaaS :** livre plusieurs clients depuis une infrastructure AWS partagée Tous les comptes AWS sont gérés par le partenaire APN.

2. **Déploiement de clients :** Sont déployés dans un environnement AWS client. Tous les comptes AWS sont gérés par le client.

Prérequis du programme de compétences vente au détail AWS

Les éléments suivants seront validés par le responsable du programme de compétences AWS ; les informations manquantes ou incomplètes doivent être traitées avant la planification de l'examen de validation technologique.

1.0 Adhésion au programme APN		Respecté O/N
1.1 Niveau de partenaire technologique	Le partenaire APN doit lire les directives et les définitions du programme avant de postuler au programme de compétences vente au détail. Cliquez ici pour en savoir plus sur le programme	
1.2 Niveau de partenaire technologique	Le partenaire APN doit être un partenaire technologique de niveau avancé avant d'effectuer une demande d'adhésion au programme de compétences vente au détail AWS.	
1.3 Catégorie de solution	Le partenaire APN doit identifier la catégorie de segment qui correspond à sa solution : ☐ **Engagement client** ☐ **Commercialisation et planification d'entreprise** ☐ **Chaîne d'approvisionnement et distribution** ☐ **Boutiques physiques, numériques et virtuelles** ☐ **Sciences des données avancées de la vente au détail** ☐ **Applications professionnelles clés de la vente au détail** Le partenaire APN doit identifier la catégorie de livraison qui correspond à sa solution : ☐ **SaaS** ☐ **Déploiement de clients**	
1.4 Adoption client	Le partenaire APN doit décrire le nombre total de clients utilisant sa solution.	
2.0 Études de cas		**Respecté O/N**
2.1 Études de cas spécifiques à la vente au détail	Le partenaire APN doit avoir à l'étude quatre études de cas spécifiques à une seule solution de vente au détail. Chacune des quatre études de cas doit porter sur un exemple d'utilisation de la solution partenaire APN dans l'une des six catégories de segments (engagement client, commercialisation et planification d'entreprise, chaîne logistique et distribution, boutiques physiques, numériques et virtuelles, science des données avancées de la vente au détail et applications professionnelles clés de la vente au détail. Les partenaires APN détenant les compétences d'expérience client numérique AWS (DCX), données et analyse, IoT, migration et/ou machine learning peuvent réutiliser jusqu'à quatre études de cas clients pour des projets réalisés avec des solutions très ciblées répondant aux défis du secteur et des pratiques de conseil offrant une connaissance unique du domaine de segment spécifique au secteur de la vente au détail. Pour chaque étude de cas, le partenaire APN doit fournir les informations suivantes : ▪ Nom du client ▪ Site Web du client ▪ Défi client ▪ Comment la solution a été déployée pour relever le défi ▪ Applications ou solutions tierces utilisées ▪ Date à laquelle la référence est entrée en production ▪ Résultat(s) ▪ Schémas d'architecture spécifiques, guides de déploiement et autres supports en fonction du type de solution, tel que décrit dans la section suivante. Ces informations seront demandées dans le cadre du processus de demande d'adhésion au programme dans APN Partner Central. Ces informations fournies dans le cadre de cette étude de cas peuvent être privées et ne seront donc pas publiées. Les quatre études de cas fournies seront examinées lors de la vérification des documents et de la validation technique. L'étude de cas ne sera plus prise en compte pour être incluse dans le programme de compétences si le partenaire APN ne peut pas fournir les documents requis pour évaluer l'étude de cas par rapport à chaque élément de la liste de contrôle, ou si l'un d'eux n'est pas respecté.	

	Les études de cas doivent décrire les déploiements qui ont été effectués au cours des 18 derniers mois et concerner des projets qui sont en production avec des clients, plutôt qu'en phase pilote ou de démonstration de faisabilité.	
2.2 Études de cas accessibles au public	Des études de cas accessibles au public sont utilisées par AWS dès l'approbation de l'adhésion au programme de compétences pour illustrer le succès démontré du partenaire APN sur la base d'indicateurs de performances clés mesurables avec la solution, et donner aux clients l'assurance que le partenaire APN dispose de l'expérience et des connaissances nécessaires pour développer et proposer des solutions répondant à leurs objectifs. Deux des quatre déploiements client associés aux études de cas doivent être publiés par le partenaire APN en tant qu'études de cas accessibles au public. Ces études de cas accessibles au public peuvent se présenter sous la forme d'études de cas formelles, de livres blancs ou d'articles de blog.	
	Les études de cas accessibles au public doivent être facilement consultables depuis le site Internet du partenaire APN. Vous devez, par exemple, pouvoir accéder aux études de cas accessibles au public à partir de la page d'accueil du partenaire APN, et ce partenaire APN doit fournir des liens vers ces études de cas accessibles au public dans leur demande.	
	Les études de cas accessibles au public doivent inclure les éléments suivants : ▪ Références au nom du client, nom du partenaire APN et AWS ▪ Défi client ▪ Comment la solution a été déployée pour relever le défi ▪ Comment les services AWS ont été utilisés dans le cadre de la solution ▪ Résultat(s)	
3.0 Présence sur le Web et leadership d'opinion de vente au détail AWS		**Respecté O/N**
3.1 Page de destination AWS des partenaires APN	La présence sur le web d'un partenaire APN spécifique à ses solutions de vente au détail AWS permet d'accroître la confiance des clients en les capacités et l'expérience de vente au détail du partenaire APN. Le partenaire APN doit disposer d'une page de destination AWS qui décrit sa solution de vente au détail AWS, renvoie vers ses études de cas accessibles au public, répertorie les partenariats technologiques et fournit toute autre information pertinente appuyant l'expertise du partenaire APN en matière de vente au détail, et met en évidence le travail effectué avec AWS. Cette page Vente au détail spécifique à AWS doit être accessible à partir de la page d'accueil du partenaire APN. La page d'accueil elle-même n'est pas acceptable en tant que page de destination AWS, sauf si le partenaire APN est une entreprise technologique de vente au détail dédiée et si la page d'accueil reflète l'attention du partenaire d'APN sur la vente au détail.	
3.2 Leadership orienté sur la vente au détail	Les partenaires du programme de compétences vente au détail AWS sont considérés comme possédant une expertise approfondie du domaine de la gestion de la vente au détail, ayant développé des solutions innovantes qui exploitent les services AWS. Le partenaire APN doit disposer de supports destinés au public (billets de blogs, articles de presse, vidéos, etc.) illustrant l'attention du partenaire APN et son expertise en matière de vente au détail. Des liens vers des exemples de supports publiés au cours des 12 derniers mois doivent être fournis.	
4.0 Exigences de l'entreprise		
4.1 Boîtes à outils accessibles	Le partenaire APN dispose de documents et de boîtes à outils vendeur accessibles y compris une proposition claire des valeurs produits pouvant être articulée selon l'organisation du service commercial AWS avec toutes les informations pertinentes requises pour déterminer s'ils correspondent à une opportunité client (par exemple des supports de ventes, des présentations et de cas d'utilisation client). Les preuves doivent être présentées sous la forme de supports de ventes comprenant une présentation, un bipeur et une liste de contrôle du cas d'utilisation.	

4.2 Support produit/ Service d'assistance	Le partenaire APN propose aux clients un support produit par chat, téléphone ou e-mail. Les preuves doivent être présentées sous la forme d'une description du support proposé aux clients pour son produit ou sa solution.	
4.3 Le produit est répertorié sur AWS Marketplace	Le partenaire APN rend la solution disponible via AWS Marketplace. ☐ Oui ☐ Non Si la réponse est « oui », le partenaire APN doit fournir un lien vers l'offre AWS Marketplace. Si la réponse est « non », aucune information supplémentaire n'est requise.	
4.4 Compensation de ventes pour les offres AWS conjointes	Le partenaire APN obtient des plans de compensation de ventes pour leurs vendeurs sur les opportunités conjointes avec AWS. ☐ Oui ☐ Non ☐ Explication : _____ Les preuves doivent être présentées sous la forme d'une brève description du plan de compensation pour les vendeurs du partenaire APN.	
4.5 Résultats AWS/ partenaire APN conjoints	Le partenaire APN dispose d'un processus pour documenter et promouvoir les résultats conjoints. Les preuves doivent être présentées sous la forme d'une description verbale du processus.	
5.0 Auto-évaluation du partenaire APN		**Respecté O/N**
5.1 Auto-évaluation de la liste de contrôle de validation du programme partenaire de compétences AWS	Le partenaire APN doit procéder à une auto-évaluation de sa conformité aux exigences de la liste de contrôle de validation des partenaires technologiques de la vente au détail AWS. ▪ Il doit compléter toutes les sections de cette liste. ▪ L'auto-évaluation finalisée doit être envoyée par e-mail à l'adresse **competency-checklist@amazon.com**, en utilisant la convention suivante pour l'objet du mail : « [Nom du partenaire APN], Auto-évaluation finalisée du partenaire technologique de compétences en vente au détail ». ▪ Il est recommandé que le partenaire APN demande à son architecte de solutions partenaires, à son agent de développement partenaire (PDR) ou à son responsable développement partenaire (PDM) d'examiner l'auto-évaluation finalisée avant de la soumettre à AWS. L'objectif est de s'assurer que l'équipe AWS du partenaire APN est engagée et s'efforce de formuler des recommandations avant l'examen et de contribuer à une expérience d'examen productive.	

Liste de contrôle de validation des partenaires technologiques du programme de compétences vente au détail

Les éléments suivants seront validés par les auditeurs tiers et/ou des architectes de solutions partenaires AWS ; les informations manquantes ou incomplètes doivent être traitées avant la planification de l'examen de validation technologique.

		S'applique à :		
Validation technique		SaaS	Déploiement de clients sur AWS	Respecté O/N
Diagramme d'architecture	Selon la catégorie de déploiement, un ou plusieurs diagrammes d'architecture sont requis. Chaque diagramme d'architecture doit illustrer : ☐ Les principaux éléments de l'architecture et la manière dont ils sont combinés pour fournir la solution partenaire aux clients. ☐ Tous les services AWS utilisés, à l'aide des icônes de service AWS appropriées. ☐ Comment les services AWS sont déployés, y compris Amazon Virtual Private Cloud (VPC), les zones de disponibilité, les sous-réseaux et les connexions aux systèmes en dehors d'AWS. ☐ Cela inclut les éléments déployés en dehors d'AWS, par exemple des composants sur site ou des périphériques matériels.	Oui - 1 pour la solution complète et 1 pour chaque étude de cas	Oui - 1 pour chaque étude de cas	
Guide de déploiement	Le Guide de déploiement doit fournir les meilleures pratiques pour le déploiement de la solution partenaire sur AWS et inclure toutes les sections décrites dans « Exigences minimales pour les guides de déploiement ».	Non	Oui, 1 pour la solution.	
Liste de contrôle de validation complétée	Pour chacune des quatre études de cas présentées pour la solution partenaire, le partenaire APN doit fournir une version complétée de la liste de contrôle suivante, indiquant les éléments de la liste de contrôle respectés.	Oui	Oui	
1.0 Sécurité **Le pilier sécurité se concentre sur la protection des informations et des systèmes. Les rubriques clés incluent la confidentialité et l'intégrité des données, l'identification et la gestion de ce qu'une personne peut faire via la gestion des privilèges, la protection des systèmes et l'établissement de contrôles pour détecter les événements de sécurité.**				
1.1 L'utilisateur racine du compte AWS n'est pas utilisé pour les activités courantes	L'utilisateur racine du compte AWS ne doit pas être utilisé pour les activités courantes Après la création de votre compte AWS, vous devez immédiatement créer des comptes utilisateur AWS Identity and Access Management (IAM) et les utiliser pour toutes les activités courantes. Une fois vos comptes utilisateurs IAM créés, vous devez stocker de manière sécurisée les informations d'identification du compte racine AWS et les utiliser uniquement pour effectuer les quelques tâches de gestion de compte et de service nécessitant l'utilisateur racine du compte AWS. Pour plus d'informations sur la configuration des comptes et des groupes d'utilisateur IAM pour une utilisation quotidienne, consultez la rubrique Création de votre premier utilisateur et groupe d'administrateur IAM.	Oui	Non	
1.2 La Multi-Factor Authentication (MFA) a été activée pour l'utilisateur racine du compte AWS.	La Multi-Factor Authentication (MFA) doit être activée pour l'utilisateur racine de votre compte AWS. Puisque l'utilisateur racine de votre compte AWS peut effectuer des opérations sensibles sur votre compte AWS, l'ajout d'une couche d'authentification supplémentaire vous aide à mieux sécuriser votre compte. Plusieurs types de MFA sont disponibles, y compris la MFA virtuelle et la MFA matérielle.	Oui	Non	
1.3 Comptes d'utilisateurs IAM utilisés pour toutes	L'utilisateur racine du compte AWS ne doit pas être utilisé pour des tâches qui ne le requièrent pas. Créez plutôt un nouvel utilisateur IAM pour chaque personne nécessitant un accès	Oui	Non	

les activités courantes	administrateur. Puis, faites de ces utilisateurs des administrateurs en les plaçant dans un groupe d'administrateurs auquel vous associez la stratégie gérée Administrator Access. Les utilisateurs du groupe d'administrateurs doivent ensuite configurer les groupes, les utilisateurs, etc., pour le compte AWS. Toutes les interactions futures doivent se faire via les utilisateurs du compte AWS et leurs propres clés au lieu de l'utilisateur racine. Toutefois, pour effectuer certaines tâches de gestion de compte et de service, vous devez vous connecter à l'aide des informations d'identification de l'utilisateur racine.			
1.4 La Multi-Factor Authentication (MFA) est activée pour tous les utilisateurs IAM interactifs	Vous devez activer la MFA pour tous les utilisateurs IAM interactifs. Avec la MFA, les utilisateurs disposent d'un périphérique qui génère un code d'authentification unique (un mot de passe à usage unique). Les utilisateurs doivent fournir leurs informations d'identification standard (nom d'utilisateur et mot de passe) et le mot de passe à usage unique. Le périphérique MFA peut être soit un matériel spécial, soit un périphérique virtuel (par exemple, il peut être exécuté dans une application sur un smartphone).	Oui	Non	
1.5 Les informations d'identification IAM sont soumises à une rotation régulière	Vous devez modifier vos mots de passe et vos clés d'accès régulièrement, et vous assurer que tous les utilisateurs IAM de votre compte le font également. Ainsi, si un mot de passe ou une clé d'accès est compromis(e) à votre insu, vous limitez la durée pendant laquelle les informations d'identification peuvent être utilisées pour accéder à vos ressources. Vous pouvez appliquer une stratégie de mot de passe à votre compte pour obliger tous vos utilisateurs IAM à mettre à jour leurs mots de passe, et choisir la fréquence à laquelle ils doivent le faire. Pour plus d'informations sur la rotation des clés d'accès pour les utilisateurs IAM, consultez la rubrique Rotation des clés d'accès.	Oui	Non	
1.6 Une politique de gestion des mots de passe forts est en place pour les utilisateurs IAM	Vous devez configurer une politique de gestion des mots de passe forts pour vos utilisateurs IAM. Si vous autorisez les utilisateurs à modifier leurs propres mots de passe, demandez-leur de créer des mots de passe forts et de les mettre à jour régulièrement. Sur la page Paramètres du compte de la console IAM, vous pouvez créer une politique de gestion des mots de passe pour votre compte. Vous pouvez utiliser la politique de gestion des mots de passe pour définir les exigences en matière de mot de passe, telles que la longueur minimale, la nécessité ou non d'utiliser des caractères non alphabétiques, la fréquence de rotation requise, etc. Pour plus d'informations, consultez la rubrique Définition d'une stratégie de gestion des mots de passe de compte pour les utilisateurs IAM.	Oui	Non	
1.7 Les informations d'identification IAM ne sont pas partagées entre plusieurs utilisateurs	Vous devez créer un compte utilisateur IAM individuel pour toute personne ayant besoin d'accéder à votre compte AWS. Créez-vous également un utilisateur IAM, accordez-lui des privilèges d'administration et utilisez-le pour l'ensemble de votre tâche. En créant des utilisateurs IAM individuels pour les personnes accédant à votre compte, vous pouvez attribuer à chaque utilisateur IAM un ensemble unique d'informations d'identification de sécurité. Vous pouvez également accorder différentes autorisations à chaque utilisateur IAM. Si nécessaire, vous pouvez modifier ou révoquer les autorisations d'un utilisateur IAM à tout moment. (Si vous divulguez vos informations d'identification d'utilisateur racine, il peut être difficile de les révoquer et il est impossible de limiter leurs autorisations.)	Oui	Non	
1.8 Les stratégies IAM sont basées sur le principe du moindre privilège	Vous devez suivre les conseils de sécurité standard relatifs à l'octroi du moindre privilège. Cela signifie que vous n'accordez que les autorisations requises pour la réalisation d'une tâche. Déterminez ce que les utilisateurs doivent faire, puis élaborez des stratégies leur permettant d'effectuer ces tâches uniquement. Commencez avec un ensemble minimum d'autorisations et accordez des autorisations supplémentaires si nécessaire. Cela est plus sûr que de commencer avec des	Oui	Non	

	autorisations trop indulgentes, puis d'essayer de les restreindre plus tard. Définir le bon ensemble d'autorisations nécessite quelques recherches. Déterminez les éléments requis pour la tâche spécifique, les actions prises en charge par un service donné et les autorisations requises pour effectuer ces actions.			
1.9 Les informations d'identification codées en dur (par exemple, les clés d'accès) ne sont pas utilisées	Vous devez suivre les meilleures pratiques de gestion des clés d'accès AWS et éviter l'utilisation d'informations d'identification codées en dur. Lorsque vous accédez à AWS par programmation, vous utilisez une clé d'accès pour vérifier votre identité et celle de vos applications. Toute personne possédant votre clé d'accès dispose du même niveau d'accès que vous à vos ressources AWS. Par conséquent, AWS met tout en œuvre pour protéger vos clés d'accès et, conformément à notre modèle de responsabilité partagée, vous devriez en faire de même.	Oui	Oui	
1.10 Toutes les informations d'identification sont chiffrées au repos	L'exigence de base est d'assurer le chiffrement de toutes les informations d'identification au repos.	Oui	Oui	
1.11 Clés d'accès AWS utilisées uniquement par les utilisateurs interactifs	Aucune clé d'accès AWS ne doit être utilisée, sauf dans les cas suivants : 1. Utilisée par des individus pour accéder aux services AWS, et stockée en toute sécurité sur un périphérique contrôlé par cet utilisateur. 2. Utilisée par un service pour accéder aux services AWS, mais uniquement dans les cas où : a) il est impossible d'utiliser un rôle d'instance Amazon EC2, un service de conteneur Amazon Elastic, un rôle de tâche Amazon ECS ou un mécanisme similaire, b) les clés d'accès AWS sont mises à jour au moins une fois par semaine, et c) la stratégie IAM est étroitement délimitée de sorte qu'elle : i) autorise uniquement l'accès à des méthodes et cibles spécifiques et ii) limite l'accès aux sous-réseaux sur lesquels les ressources seront accessibles.	Oui	Oui	
1.12 AWS CloudTrail est activé pour tous les comptes AWS dans chaque région.	AWS CloudTrail doit être activé pour tous les comptes AWS et dans toutes les régions. La visibilité de l'activité de votre compte AWS est un aspect essentiel des meilleures pratiques en matière de sécurité et d'exploitation. Vous pouvez utiliser AWS CloudTrail pour afficher, rechercher, télécharger, archiver, analyser et répondre à l'activité du compte sur votre infrastructure AWS. Vous pouvez identifier qui a pris une mesure en particulier, quelles ressources ont été utilisées, quand l'événement s'est produit et d'autres détails pour vous aider à analyser et à répondre aux activités de votre compte AWS.	Oui	Non	
1.13 Les journaux CloudTrail sont stockés dans un compartiment S3 appartenant à un autre compte AWS.	Les journaux AWS CloudTrail doivent être placés dans un compartiment appartenant à un autre compte AWS configuré pour un accès extrêmement limité, tel que l'audit et la récupération uniquement.	Oui	Non	
1.14 La gestion des versions ou la suppression MFA est activée pour le compartiment de journaux CloudTrail S3	Le contenu du compartiment de journaux AWS CloudTrail doit être protégé avec la gestion des versions ou la suppression MFA.	Oui	Non	
1.15 Les groupes de sécurité Amazon EC2 sont étroitement liés.	Tous les groupes de sécurité Amazon EC2 doivent limiter l'accès au maximum. Cela comprend au moins 1. l'implémentation de groupes de sécurité pour limiter le trafic entre Internet et Amazon VPC, 2. l'implémentation de groupes de sécurité pour limiter le trafic dans Amazon VPC, et 3. dans tous les cas, n'autorisez que les paramètres les plus restrictifs possibles.	Oui	Oui	
1.16 Les compartiments Amazon S3 de	Vous devez vous assurer que les contrôles appropriés sont en place pour contrôler l'accès à chaque compartiment Amazon S3. Lorsque vous utilisez AWS, il est recommandé de restreindre	Oui	Oui	

votre compte disposent de niveaux d'accès appropriés.	l'accès à vos ressources aux personnes qui en ont réellement besoin (le principe du moindre privilège).			
1.17 Les compartiments Amazon S3 n'ont pas été mal configurés pour permettre au public d'y accéder	Vous devez vous assurer que les compartiments qui ne doivent pas permettre au public d'y accéder sont correctement configurés pour empêcher cet accès. Par défaut, tous les compartiments Amazon S3 sont privés et ne sont accessibles qu'aux utilisateurs auxquels l'accès a été explicitement accordé. La plupart des cas d'utilisation n'exigent pas un accès public étendu pour lire les fichiers de vos compartiments Amazon S3, sauf si vous utilisez Amazon S3 pour héberger des ressources publiques (par exemple, pour héberger des images à utiliser sur un site Web public), et il est recommandé de ne jamais ouvrir l'accès au public.	Oui	Oui	
1.18 Un mécanisme de surveillance est en place pour détecter à quel moment les objets ou les compartiments S3 deviennent publics.	Une surveillance ou des alertes doivent être en place pour identifier à quel moment les compartiments Amazon S3 deviennent publics. Une option pour cela consiste à utiliser AWS Trusted Advisor. AWS Trusted Advisor vérifie les compartiments dans Amazon S3 dotés d'autorisations d'accès ouvert. Les autorisations de compartiment qui accordent à tous l'accès à la liste peuvent entraîner des frais plus élevés que prévu si les objets du compartiment sont répertoriés fréquemment par des utilisateurs imprévus. Les autorisations de compartiment qui accordent à tous l'accès au chargement/à la suppression créent des vulnérabilités de sécurité potentielles en permettant à quiconque d'ajouter, de modifier ou de supprimer des éléments d'un compartiment. La vérification Trusted Advisor examine les autorisations de compartiment explicites et les stratégies de compartiment associées susceptibles de remplacer les autorisations de compartiment.	Oui	Non	
1.19 Un mécanisme de surveillance est en place pour détecter les modifications apportées aux instances et conteneurs Amazon EC2.	Toute modification apportée à vos instances ou à vos conteneurs Amazon S3 peut indiquer une activité non autorisée et doit au minimum être consignée dans un emplacement durable pour permettre de futures investigations. Le mécanisme utilisé à cette fin doit au moins : 1. détecter toute modification apportée au système d'exploitation ou aux fichiers d'application dans les instances ou les conteneurs Amazon S3 utilisés dans la solution ; 2 stocker des données enregistrant ces modifications dans un emplacement durable, externe à l'instance ou au conteneur Amazon S3. Exemples de mécanismes appropriés : a. Déploiement de la vérification de l'intégrité des fichiers via la gestion de la configuration planifiée (Chef, Puppet, etc.) ou un outil spécialisé (OSSEC, Tripwire ou similaire) ou b. Extension des outils de gestion de la configuration pour valider la configuration de l'hôte Amazon S3 et alerter sur les mises à jour de fichiers de configuration ou packages clés avec des événements « canary » (ineffectifs) configurés pour s'assurer que le service reste opérationnel sur tous les hôtes concernés durant l'exécution, ou c. Déploiement d'un système de détection des intrusions sur l'hôte tel qu'une solution open source de type OSSEC avec ElasticSearch et Kibana ou via une solution partenaire. Notez que le mécanisme suivant ne répond pas à cette exigence : a. Cycles fréquents d'instances ou de conteneurs Amazon S3.	Oui	Non	
1.20 Toutes les données sont classées	Toutes les données client traitées et stockées dans le workload sont prises en compte et classées de sorte à pouvoir déterminer leur sensibilité et les méthodes appropriées à utiliser lors de leur traitement.	Oui	Oui	
1.21 Toutes les données sensibles sont chiffrées	Toutes les données client considérées comme sensibles sont chiffrées en transit et au repos.	Oui	Oui	
1.22 Les clés cryptographiques sont gérées de manière sécurisée	Toutes les clés cryptographiques sont chiffrées au repos et en transit, et l'accès à l'utilisation de ces clés est contrôlé à l'aide d'une solution AWS telle que AWS Key Management Service (KMS) ou d'une solution partenaire telle que HashiCorp Vault.	Oui	Oui	

1.23 Toutes les données en transit sont chiffrées	Toutes les données en transit à travers une limite Amazon Virtual Private Cloud sont chiffrées.	Oui	Oui	
1.24 Le processus de réponse aux incidents de sécurité est défini et répété	Un processus de réponse aux incidents de sécurité doit être défini pour gérer les incidents tels que les compromissions de compte AWS. Ce processus doit être testé en mettant en œuvre des procédures permettant de répéter le processus de réponse aux incidents, par exemple, en effectuant un exercice de jeu de rôle portant sur la sécurité. Une répétition doit avoir eu lieu au cours des 12 derniers mois pour confirmer que : a. les personnes appropriées ont accès à l'environnement ; b. les outils appropriés sont disponibles ; c. Lls personnes appropriées savent comment réagir face aux divers incidents de sécurité décrits dans le plan.	Oui	Non	
1.25 Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) – Certification ou SAQ	Pour les applications d'e-commerce, de commerce unifié et de point de vente, où les données des titulaires de carte sont présentes, un processus est établi pour effectuer une évaluation annuelle de la portée des normes de sécurité des données de l'industrie des cartes de paiement (PCI DSS). Sur la base de l'évaluation de la portée, la certification PCI DSS ou SAQ est effectuée selon les besoins. Les preuves doivent être fournies sous la forme d'un rapport de conformité pour la certification PCI DSS ou d'un questionnaire d'auto-évaluation (SAQ) complété.	Oui	Oui	
1.26 Chiffrement de bout en bout des données PCI	Pour les applications d'e-commerce, de commerce unifié et de point de vente contenant les données des titulaires de carte, les données sont chiffrées en transit, même au sein d'un Amazon VPC.	Oui	Oui	
1.27 Protection mise en place contre les attaques par déni de service distribué (DDoS)	Fournit une infrastructure et un service qui atténuent les attaques par déni de service (DDoS) sur toutes les couches du modèle d'interconnexion de systèmes ouverts (OSI).	Oui	Non	
1.28 Mécanismes mis en place pour atténuer les 10 principales attaques OWASP (Open Web Application Security Project)	Fournissent une infrastructure et un service qui atténuent les vulnérabilités OWASP (Open Web Application Security Project).	Oui	Non	
2.0 Fiabilité Le pilier fiabilité se concentre sur la capacité à prévenir et à remédier rapidement aux défaillances pour répondre à la demande des entreprises et des clients. Les rubriques clés incluent des éléments fondamentaux autour de la configuration, des exigences inter-projets, de la planification de la récupération et de la façon dont nous gérons le changement.				
2.1 La connectivité réseau est hautement disponible	La connectivité réseau à la solution doit être hautement disponible. Si vous utilisez VPN ou AWS Direct Connect pour vous connecter aux réseaux client, la solution doit prendre en charge les connexions redondantes, même si les clients n'implémentent pas toujours cela.	Oui	Oui	
2.2 Les mécanismes de dimensionnement d'infrastructure s'alignent sur les exigences de l'entreprise	Les mécanismes de dimensionnement d'infrastructure doivent s'aligner sur les exigences de l'entreprise : 1. en mettant en œuvre des mécanismes de scalabilité automatique à chaque couche de l'architecture, ou 2. en confirmant que les exigences actuelles de l'entreprise, y compris les exigences en termes de coût et croissance d'utilisateurs anticipée, ne nécessitent pas de mécanismes de scalabilité automatique et que les procédures de dimensionnement manuel sont entièrement documentées et fréquemment testées.	Oui	Oui	
2.3 Les journaux d'application et AWS sont gérés de manière centralisée	Toutes les informations de journaux issues de l'application et de l'infrastructure AWS doivent être regroupées dans un système unique.	Oui	Non	

2.4 La surveillance et les alarmes d'application et AWS sont gérées de manière centralisée	L'application et l'infrastructure AWS doivent être surveillées de manière centralisée, avec des alarmes générées et envoyées au personnel d'exploitation approprié.	Oui	Non	
2.5 La mise en service et la gestion de l'infrastructure sont automatisées	La solution doit utiliser un outil automatisé tel que AWS CloudFormation ou Terraform pour mettre en service et gérer l'infrastructure AWS. La console AWS ne doit pas être utilisée pour apporter des modifications de routine à l'infrastructure AWS de production.	Oui	Oui	
2.6 Des sauvegardes de données régulières sont en cours	Vous devez effectuer des sauvegardes régulières sur un service de stockage durable. Les sauvegardes s'assurent que vous ayez la possibilité de récupérer des scénarios d'erreur administratifs, logiques ou physiques. Amazon S3 et Amazon Glacier sont des services privilégiés pour la sauvegarde et l'archivage. Ce sont des plates-formes de stockage durables et peu coûteuses, qui offrent toutes deux une capacité illimitée et ne nécessitent aucune gestion de volume ou de supports à mesure que les ensembles de données de sauvegarde se développent. Le modèle de paiement à l'utilisation et le faible coût par Go/mois font de ces services un partenaire idéal pour les cas d'utilisation de protection de données.	Oui	Oui	
2.7 Les mécanismes de récupération sont testés régulièrement et à la suite d'importantes modifications architecturales	Vous devez tester les mécanismes et les procédures de récupération, à la fois régulièrement et après avoir apporté des modifications importantes à votre environnement cloud. AWS fournit des ressources substantielles pour vous aider à gérer la sauvegarde et la restauration de vos données.	Oui	Non	
2.8 La solution résiste aux perturbations de zones de disponibilité	La solution doit continuer à fonctionner dans le cas où tous les services d'une même zone de disponibilité ont été perturbés.	Oui	Oui	
2.9 La résistance de la solution a été testée	La résistance de l'infrastructure aux perturbations d'une seule zone de disponibilité a été testée en production, par exemple, au cours d'un exercice de jeu de rôle, au cours des 12 derniers mois.	Oui	Non	
2.10 Le plan de reprise après sinistre a été défini	Un plan de reprise après sinistre bien défini comprend un objectif de point de reprise (RPO) et une durée d'interruption maximale admissible (RTO). Vous devez définir un RPO et un RTO pour tous les services concernés. Les RPO et RTO doivent être alignés sur le contrat de niveau de service que vous proposez à vos clients.	Oui	Oui	
2.11 La durée d'interruption maximale admissible (RTO) est inférieure à 24 heures	L'exigence de base est que le RTO soit inférieur à 24 heures pour les services de base.	Oui	Non	
2.12 Le plan de reprise après sinistre est testé de manière adéquate	Votre plan de reprise après sinistre doit être testé par rapport à votre objectif de point de reprise (RPO) et votre durée d'interruption maximale admissible (RTO), à la fois périodiquement et après d'importantes mises à jour. Au moins un test de reprise après sinistre doit être effectué avant l'approbation de votre application APN AWS de niveau Advanced.	Oui	Non	
2.13 Le plan de reprise après sinistre (DR) inclut la récupération vers une autre région.	Votre plan de reprise après sinistre doit inclure une stratégie de récupération vers une autre région AWS, et vos tests de récupération périodiques doivent tester ce scénario. Vous devez avoir effectué au moins un test complet du plan de reprise après sinistre, y compris au moins une récupération vers une autre région AWS, au cours des 12 derniers mois. Remarque : bien que	Oui	Non	

	la restauration de données dans des environnements de test ou l'exportation de données pour les utilisateurs constituent des moyens utiles de vérifier les sauvegardes, ces processus ne remplissent pas l'obligation d'effectuer un test de restauration complet vers une autre région AWS.			
3.0 Excellence opérationnelle Le pilier excellence opérationnelle se concentre sur le fonctionnement et la surveillance des systèmes afin de générer de la valeur commerciale, ainsi que sur l'amélioration continue des processus et des procédures. Les rubriques clés incluent la gestion et l'automatisation des modifications, la réponse aux événements et la définition de normes pour gérer avec succès les opérations quotidiennes.				
3.1 Le déploiement des modifications de code est automatisé	La solution doit utiliser une méthode automatisée de déploiement de code sur l'infrastructure AWS. Les sessions interactives, SSH ou RDP ne doivent pas être utilisées pour déployer des mises à jour dans l'infrastructure AWS.	Oui	Non	
3.2 Les runbooks et le processus d'acheminement sont définis	Les runbooks doivent être développés pour définir les procédures standard utilisées en réponse à différents événements d'application et AWS. Un processus d'acheminement progressif doit être défini pour traiter les alertes et les alarmes générées par le système et réagir aux incidents signalés par les clients. Le processus d'acheminement doit également inclure un acheminement vers AWS Support, le cas échéant.	Oui	Non	
3.3 Le support commercial AWS est activé pour le compte AWS	Le support commercial doit être activé. Le support commercial (ou supérieur) est une exigence du réseau de partenaires AWS pour les partenaires technologiques de niveau Advanced. Pour bénéficier du niveau Advanced, vous devez activer le support commercial sur au moins un de vos comptes AWS.	Oui	Non	
4.0 Efficacité des performances Le pilier efficacité des performances se concentre sur l'utilisation efficace des ressources informatiques et de calcul. Les rubriques clés incluent la sélection des types et des tailles de ressources appropriés en fonction des exigences de charge de travail, la surveillance des performances et la prise de décisions éclairées pour maintenir l'efficacité à mesure que les besoins de l'entreprise évoluent.				
4.1 Le test de performance est activé après les déploiements	Définissez des objectifs de performance mesurables et effectuez des tests de performance afin de vous assurer que les objectifs de performance sont atteints avant la sortie en production.	Oui	Oui	
4.2 Surveillance des seuils mis en place	Surveillez les performances des applications et mettez en place des mécanismes pour déclencher des alarmes lorsque les seuils sont dépassés.	Oui	Oui	

Ressources AWS :

Titre	Description
Comment créer une page de destination de pratique	Fournit des instructions sur la création d'une page de pratique/solution répondant aux prérequis du programme.
Comment rédiger une étude de cas publique	Fournit des instructions sur la création d'une étude de cas client publique répondant aux prérequis du programme.
Comment créer un diagramme d'architecture	Fournit des instructions sur la création de diagrammes d'architecture répondant aux prérequis du programme.
Doc de préparation du partenaire	Fournit des instructions et des exemples de meilleures pratiques des prérequis du programme.
Site Web AWS Well-Architected	Couvre les meilleures pratiques Well-Architected