



Stratégie de modernisation bancaire pour la gestion du cycle de vie des clients
dans le Cloud AWS

AWS Conseils prescriptifs



AWS Conseils prescriptifs: Stratégie de modernisation bancaire pour la gestion du cycle de vie des clients dans le Cloud AWS

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques et la présentation commerciale d'Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n'est pas d'Amazon, d'une manière susceptible de créer une confusion parmi les clients, ou d'une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d'Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Introduction	1
Défis de la modernisation	2
Évolution des attentes et néobanques	2
Problème métier	2
Gestion du cycle de vie client	3
Intégration des clients	4
Parcours d'intégration	6
Intégration sans serveur	7
Solution d'intégration	7
Conformité et sécurité	9
FAQ	11
Comment puis-je être sûr que les AWS services ne stockeront aucune donnée personnelle ?	11
L'architecture est-elle conforme au RGPD ?	11
Comment puis-je garantir la confidentialité des données ?	11
Puis-je intégrer une solution de modernisation bancaire AWS à n'importe quel système bancaire hérité ?	11
Puis-je personnaliser la boîte de dialogue d'intégration ?	12
Étapes suivantes	13
Ressources	14
Historique du document	15
.....	xvi

Stratégie de modernisation bancaire pour la gestion du cycle de vie des clients dans le AWS cloud

Patrick Rotzetter et Florent Batard, Amazon Web Services (AWS)

Juin 2022 ([historique du document](#))

Le secteur des services financiers (FS) est confronté à des bouleversements majeurs. En effet, de plus en plus de clients attendent et préfèrent même les services bancaires en libre-service entièrement numériques proposés par les entreprises de technologie financière (fintechs) et les néobanques (c'est-à-dire les banques exclusivement numériques sans succursales physiques) dans le cadre du processus d'intégration des clients particuliers. Les institutions financières traditionnelles ne peuvent pas suivre le rythme des fintechs et des néobanques. Cela s'explique par le fait que les processus bancaires de la plupart des institutions financières traditionnelles restent manuels ou semi-automatiques.

Aucun cadre standard n'est utilisé pour implémenter les processus bancaires traditionnels, même s'ils sont partagés par toutes les institutions financières. L'absence d'un tel cadre standard freine l'innovation. Par exemple, les institutions financières traditionnelles ne sont pas en mesure de tirer parti de l'une des dernières tendances du secteur bancaire, à savoir la finance intégrée. Il s'agit de la capacité des entités non bancaires à proposer des services similaires à ceux des banques. Pour plus d'informations, voir [Ce que le financement intégré et banking-as-a-service les tendances signifient pour les services financiers](#) de McKinsey & Company. Pour que les institutions financières traditionnelles puissent tirer parti de la finance intégrée, elles doivent exposer leurs capacités métier de manière transparente à d'autres entreprises.

Cette stratégie définit une approche de modernisation pour la mise en œuvre de processus bancaires standard évolutifs et sécurisés en utilisant une architecture sans serveur orientée API basée sur AWS les services cloud. Pour illustrer les défis et les opportunités de cette approche, cette stratégie se concentre sur une étude de cas de gestion du cycle de vie client (CLM). Le public cible de cette stratégie comprend CEOs, CFOs CIOs, et les cadres supérieurs du secteur de la banque de détail et de la gestion de patrimoine.

Défis de la modernisation du secteur bancaire

L'évolution des attentes des clients et l'essor des néobanques

Le secteur des services financiers est confronté à un changement majeur. Les clients s'attendent non seulement à une transition entièrement numérique, mais aussi à une expérience personnalisée. Pour répondre à ces attentes des clients et concurrencer les néobanques, les institutions financières traditionnelles doivent subir une transformation considérable qui exige rapidité, agilité et innovation. Cette transformation obligera les institutions financières traditionnelles à relever les défis à court terme suivants :

1. Les banques traditionnelles doivent suivre le rythme des néobanques, qui sont plus agiles par nature grâce à l'absence de dettes techniques et de processus.
2. Les institutions financières traditionnelles doivent développer et proposer des services bancaires intégrés par le biais du Banking as a Service (BaaS).
3. Les institutions financières traditionnelles doivent développer et proposer des expériences client personnalisables et flexibles qui intègrent des modèles de machine learning de manière rapide et rentable.

Les principaux facteurs stratégiques à prendre en compte au cours des prochaines années sont de tirer parti des services cloud intégrés et des avantages en termes de délais de commercialisation résultant de la collaboration avec les fournisseurs de services et de la transformation agile.

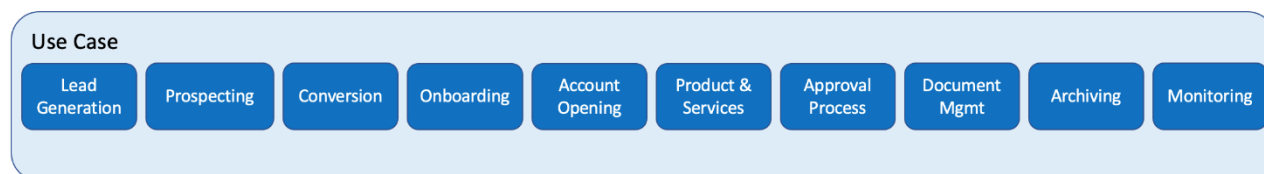
Problème métier

Les institutions financières traditionnelles utilisent toujours des processus manuels ou semi-automatiques. Aucune norme du secteur n'est appliquée aux processus bancaires ordinaires, même si ces processus sont communs à toutes les institutions financières de juridictions similaires. Pour surmonter ces défis, les institutions financières traditionnelles peuvent mettre en œuvre des processus standard évolutifs et sécurisés en utilisant une approche sans serveur basée sur les services AWS cloud. Par exemple [Amazon Lex](#) et [Amazon Rekognition](#) proposent des modèles de machine learning entraînés que vous pouvez intégrer dans des parcours client améliorés. Auparavant, cette innovation était entravée par une intégration complexe et des processus de développement coûteux, mais ces innovations sont désormais disponibles directement pour les applications client via des appels d'API.

AWS Les services cloud apportent non seulement une innovation et une rapidité d'intégration supplémentaires, mais ils tirent également parti des dernières fonctionnalités de sécurité pour garantir la confidentialité et la confidentialité des données. Nous souhaitons mettre en avant cette approche de modernisation du secteur bancaire pour le paysage CLM. Le cycle de vie des clients est au cœur de la relation client, c'est pourquoi il doit être modernisé, voire numérisé de toute urgence. Comme indiqué dans [What the embedded finance and banking-as-a-service trends mean for financial services](#) from McKinsey & Company, les banques qui souhaitent proposer du BaaS devront faire en sorte que cela fonctionne. « Pour que cela fonctionne, il faudra de nouvelles technologies et capacités, car le BaaS est généralement distribué aux clients via des API et nécessite une solide gestion des risques et de la conformité de la part du partenaire financier intégré ». La section Intégration sans serveur de cette stratégie explique comment vous pouvez faire fonctionner une telle stratégie.

Cas d'utilisation de la gestion du cycle de vie client

La CLM est un ensemble de processus librement interdépendants et obligatoires qui définissent l'interaction métier d'un client avec son institution financière ou son assureur. L'illustration suivante donne une vue d'ensemble des étapes de la CLM pour le secteur bancaire et celui de l'assurance :



Tenez compte du fait que ces processus varient selon le segment de clientèle. Par exemple, l'intégration des clients commerciaux est différente de celle des clients particuliers. Les processus peuvent également varier d'un secteur d'activité à l'autre. L'intégration d'un client bancaire est différente de celle d'un client d'assurance. Cette stratégie met l'accent sur l'expérience des clients bancaires particuliers.

Dans le schéma ci-dessus, chaque case (Prospection, par exemple) représente un candidat à la modernisation. Vous pouvez utiliser un diagramme comme celui-ci pour décomposer le cas d'utilisation en cas d'utilisation distincts et indépendants. Par exemple, le cas d'utilisation Prospection peut être décomposé en cas d'utilisation constituants. Vous pouvez ensuite mapper chaque cas d'utilisation indépendant aux fonctionnalités existantes, qu'elles proviennent de fournisseurs de services cloud ou de fournisseurs BaaS. Cet exercice de mappage peut révéler que l'archivage de documents pour le secteur bancaire, par exemple, peut être un service en soi fourni par un

tiers externe. En divisant les cas d'utilisation de la gestion du cycle de vie client en cas d'utilisation distincts et indépendants, vous pouvez concevoir et développer des services ciblés.

Cette stratégie se concentre sur l'exemple de cas d'utilisation d'ouverture d'un nouveau compte bancaire. Pour les clients, il s'agit souvent d'un processus long, très manuel et sujet aux erreurs, à l'origine de frustration et d'insatisfaction. Aujourd'hui, la majeure partie de l'intégration se fait toujours manuellement par le biais d'appels téléphoniques ou de points de contact physiques. Cependant, les recherches indiquent que les clients préfèrent une expérience numérique. Selon l'article [Digital onboarding in finance: a novel model and related cybersecurity risks](#) d'Open Research Europe, 70 % des clients préfèrent contracter leurs produits par voie numérique.

Opportunités d'intégration des clients

À l'ère de la crise post-COVID, les clients des établissements bancaires et des services financiers doivent faire face à des processus lourds et complexes. En réalité, peu de clients peuvent aujourd'hui effectuer l'ensemble du processus d'ouverture d'un compte courant depuis un appareil mobile. La majorité des clients doivent suivre un processus d'intégration manuel pour ouvrir un compte bancaire similaire au suivant :

1. Le client, ou utilisateur final, doit présenter une preuve d'identité, une identification légale et divers autres points de données. Dans de nombreux cas, ces points de données incluent la documentation relative à une adresse physique, à une preuve d'emploi, etc. Souvent, le client doit se rendre dans une succursale pour fournir ces informations ou les envoyer à la banque par courrier standard.
2. Avant même que les clients puissent utiliser leurs comptes bancaires, ils recevront plusieurs documents au format papier. Les clients doivent ensuite signer et renvoyer les documents à la banque (c'est-à-dire des contrats uniques pour chaque produit bancaire, tels que des comptes personnels, des comptes joints, des comptes de trading, des services bancaires en ligne, des cartes de crédit ou des codes de sécurité).
3. La banque numérise tous les documents signés et les lie au compte « en cours d'ouvrage » pour le rendre opérationnel.
4. En fonction du segment de clientèle ou de l'évaluation des risques du demandeur, la banque doit régulièrement répéter partiellement ou totalement ce processus.
5. Si l'adresse, l'état civil ou toute autre donnée du client considérée comme un « changement de circonstances » est mis à jour, le processus est relancé.

L'achèvement de ce processus peut prendre plusieurs jours, voire plusieurs semaines, et il nécessite souvent l'intervention et l'approbation de plusieurs employés de la banque, issus de différents services.

Le parcours d'intégration du client

Un parcours client modernisé pour l'ouverture d'un compte doit inclure les fonctionnalités et capacités suivantes :

- Le client peut accéder au service d'intégration via un site Web, un assistant virtuel ou un centre d'appels. L'assistant virtuel peut être un chatbot orienté texte ou vocal, qui peut être intégré à une page Web ou à une application de messagerie telle que Messenger ou Telegram.
- Les assistants virtuels peuvent interagir avec les clients en utilisant des intentions prédéfinies pour comprendre leurs besoins et leurs attentes. Par exemple, l'assistant virtuel peut demander aux clients de partager leurs centres d'intérêt, de communiquer des informations personnelles pour ouvrir un compte, de scanner leur pièce d'identité et de prendre un selfie, ou de confirmer qu'ils souhaitent procéder à l'ouverture d'un compte.
- Le chatbot sera multilingue.
- Les clients peuvent interagir avec le chatbot à l'aide de la voix ou du texte.
- Après avoir collecté toutes les informations requises auprès du client, vous pouvez les envoyer à la banque pour lancer le processus d'ouverture de compte. Le client recevra une notification par e-mail confirmant que le processus a démarré.
- Vous pouvez fermer la boîte de dialogue une fois le compte ouvert.
- Évitez de stocker les informations des clients dans le cloud. Ces informations doivent être transitoires et n'exister que pendant l'engagement du client. Une fois le processus d'ouverture de compte terminé, vous devez supprimer les données et, si possible, en apporter la preuve. Même si le dialogue est interrompu, vous devez confirmer que toutes les données personnelles sont supprimées (pas de mise en cache).
- Évitez de stocker des journaux contenant des données d'identification personnelle (PII).
- Les clients peuvent être sûrs qu'aucune donnée PII n'est stockée. Si les services utilisés sont sans serveur, il ne reste aucune donnée ni aucun journal contenant des données personnelles.

Intégration sans serveur

Cette section se concentre sur le cas d'utilisation de l'intégration des clients. Elle sert d'exemple pour montrer comment réutiliser des modèles sans serveur afin de moderniser un parcours client clé.

Une solution d'intégration

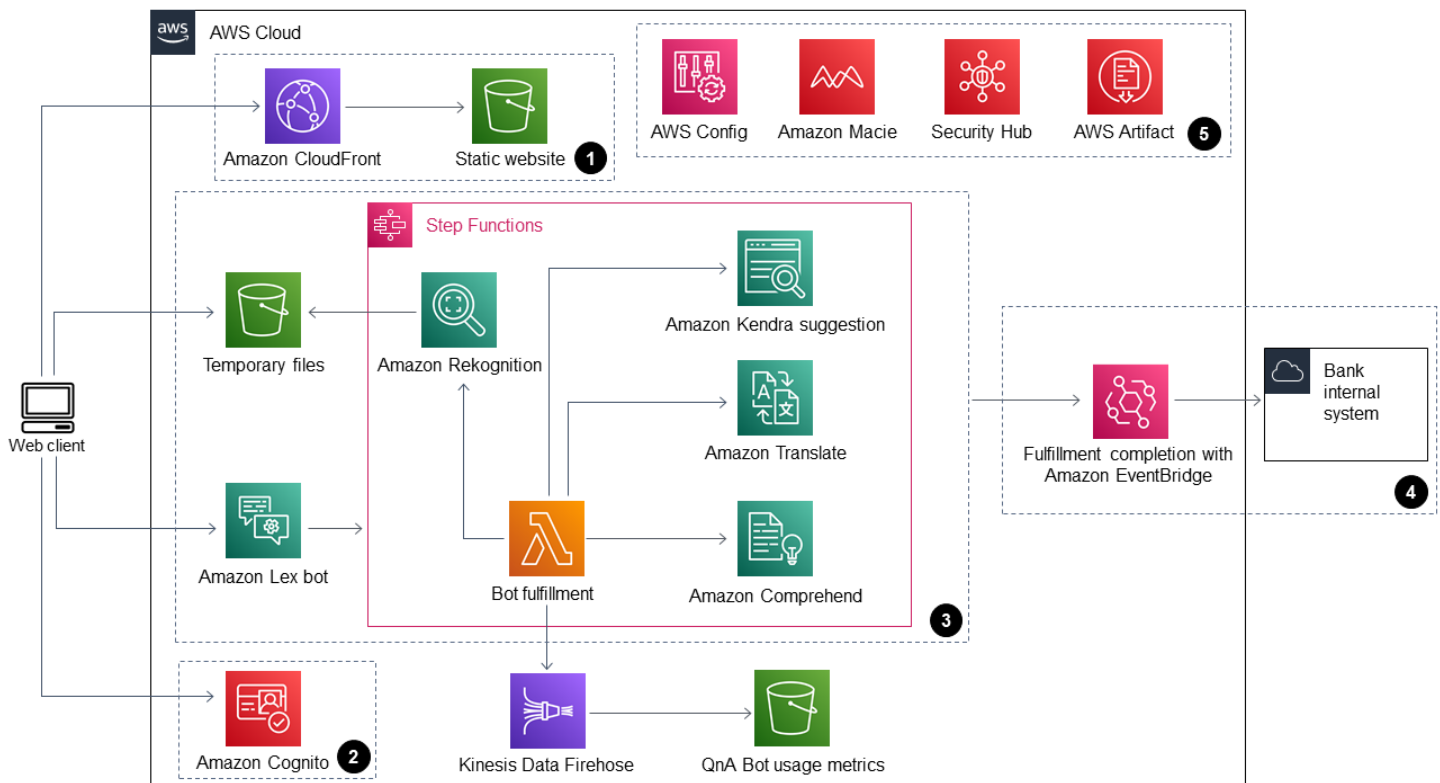
Une solution d'intégration n'est généralement pas isolée, mais s'inscrit dans un contexte plus large. Les composants et services requis pour l'intégration sont les suivants :

1. Génération de prospects (systèmes CRM)
2. Due diligence (AML, risque et conformité)
3. Fichier de données client central (systèmes bancaires de base)
4. Gestion des signatures numériques (à l'aide d'un outil tiers tel que DocuSign)
5. Vérification biométrique
6. Cycle de vie de la gestion numérique des contrats
7. Automatisation de processus et de modèle d'exploitation

Remarque

L'intégration de ces composants à des applications externes n'entre pas dans le cadre de cette stratégie.

Le schéma suivant illustre une architecture sans serveur permettant d'interagir avec les clients par le biais de chatbots dans le AWS cloud :



Remarque

L'architecture est basée sur la AWS solution QnA Bot on et sur les mises à jour d'Amazon Rekognition. Pour plus d'informations, consultez [QnA Bot AWS dans la bibliothèque de AWS solutions](#) et [Amazon Rekognition annonce des mises à jour de ses fonctionnalités de détection, d'analyse et de reconnaissance des visages sur le blog Machine Learning](#). AWS

Le schéma suivant illustre le flux de travail suivant :

1. Les clients accèdent aux composants frontend pour interagir avec le bot. Dans ce cas, la bibliothèque frontend peut être incluse dans les actifs existants de différentes manières. Par exemple, vous pouvez intégrer ces composants au site Web de l'entreprise ou les lier à une application de chat majeure. Ces composants sont fournis JavaScript et servis par le biais d'une gestion statique des actifs à l'aide d'Amazon Simple Storage Service (Amazon S3) et d'Amazon CloudFront

2. Les composants frontend intègrent des connexions aux composants backend pour valider les informations d'identification via Amazon Cognito. Une fois autorisé, le service client peut communiquer avec le service de la solution d'intégration.
3. Les clients interagissent avec le service à l'aide d'un bot Amazon Lex. Un scénario prédéfini pour l'intégration est exécuté en AWS Step Functions appelant les services nécessaires pour terminer le processus. Vous pouvez adapter ce scénario aux besoins du système bancaire (par exemple, pour répondre aux exigences en matière de photographie, de traduction en plusieurs langues et de traitement du langage naturel pour répondre aux intentions du client). Vous pouvez utiliser AWS Lambda des fonctions pour exécuter les actions du bot Amazon Lex avec le client et appeler les services en fonction de la phase d'intégration.
4. Le résultat de Step Functions est envoyé par lots au système interne de la banque via Amazon EventBridge, qui utilise votre méthode préférée pour se connecter au système interne de la banque. Vous pouvez gérer cette communication soit en vous connectant à un autre AWS compte, soit en vous connectant au système bancaire via un réseau privé virtuel (VPN).
5. L'ensemble de l'architecture est conçu pour la sécurité et la conformité en utilisant AWS Config Amazon Macie et AWS Artifact. AWS Security Hub CSPM

Considérations de sécurité et de conformité

La gestion de la sécurité et le traitement d'informations sensibles sont au cœur de l'approche d'intégration sans serveur. L'intégration sans serveur est conçue pour être sans état et ne stocke aucune PII ni aucune donnée métier critique. Pour garantir une sécurité et une conformité continues, vous devez mettre en place les services suivants et les configurer correctement :

- AWS AppConfig garantit l'intégrité et la confidentialité des services grâce à des règles adaptées à la conformité. Les contrôles en place valideront la conformité globale et empêcheront les dérives de la configuration.
- Macie détecte et balise toutes les PII tout au long du processus.
- Security Hub CSPM garantit que tous les services sont définis et utilisés dans le cadre du périmètre de sécurité.
- AWS Artifact fournit des éléments probants attestant de la conformité des AWS services.

Les transactions et les preuves de non-répudiation peuvent être stockées et chiffrées à l'aide de clés gérées par le client ou d'un module de sécurité matériel (HSM) dédié qui est scellé à des fins d'audit.

Vous pouvez également sceller les données à moindre coût tout en garantissant leur intégrité et leur sécurité en utilisant Amazon Glacier.

 Note

Amazon Glacier (service autonome d'origine basé sur un coffre-fort) n'acceptera plus de nouveaux clients à compter du 15 décembre 2025, sans aucune incidence sur les clients existants.

Amazon Glacier est un service autonome doté de ses propres API qui stocke les données dans des coffres-forts. Il est distinct des classes de stockage Amazon S3 et Amazon S3 Glacier. Vos données existantes resteront sécurisées et accessibles indéfiniment dans Amazon Glacier. Aucune migration n'est requise. Pour un stockage d'archivage à long terme et à faible coût AWS, nous recommandons les [classes de stockage Amazon S3 Glacier](#), qui offrent une expérience client supérieure grâce à des API basées sur des compartiments S3, une Région AWS disponibilité totale, des coûts réduits et une intégration. Service AWS Si vous souhaitez des fonctionnalités améliorées, envisagez de migrer vers les classes de stockage Amazon S3 Glacier en suivant nos [conseils relatifs aux AWS solutions pour le transfert de données depuis les coffres-forts Amazon Glacier vers les classes de stockage Amazon S3 Glacier](#).

Seule l'équipe opérationnelle doit être autorisée à accéder à l'environnement. Toutes les activités de développement doivent être rationalisées par le biais d'une prestation continue automatique afin d'empêcher tout accès humain à l'environnement de production. À des fins d'audit, un rôle supplémentaire doit être alloué pour accéder aux artefacts et aux rapports de conformité sur la plateforme.

AWS peut vous aider à garantir que vous respectez les normes réglementaires et de conformité. Pour plus d'informations, consultez le rapport FINMA ISAE 3000 Type 2 dans la AWS documentation. Vous pouvez également télécharger des documents bancaires pertinents directement depuis AWS Artifact, notamment la circulaire FINMA 2008/21, la circulaire FINMA ISAE 3000 type 2, la circulaire 2018/03 FINMA et les principes réglementaires mondiaux des services financiers.

FAQ

Comment puis-je être sûr que les AWS services ne stockeront aucune donnée personnelle ?

Vous pouvez l'utiliser AWS Config pour vérifier la conformité des composants de l'architecture en combinaison avec Macie afin de détecter et de corriger les données personnelles découvertes.

L'architecture est-elle conforme au RGPD ?

Oui, conformément au chapitre 2, [article 5](#) du RGPD, l'architecture est conçue pour ne conserver aucune donnée relative à l'utilisateur à long terme, mais uniquement pour traiter les informations personnelles identifiables. C'est ce que garantissent des mécanismes de conformité continus. En outre, Macie garantit le balisage et la classification de toutes les données personnelles susceptibles de mettre en péril la conformité au RGPD.

Comment puis-je garantir la confidentialité des données ?

La confidentialité est garantie grâce à des modèles de conformité et de sécurité continus grâce à Security Hub AWS Config, CSPM et Macie. Les violations de confidentialité sont immédiatement détectées, corrigées et signalées. Nous vous recommandons également d'ajouter des barrières de protection au cours de la phase de déploiement. Les barrières de protection permettent de garantir qu'aucun changement critique susceptible de mettre la confidentialité en péril n'est répercuté sur l'architecture.

Puis-je intégrer une solution de modernisation bancaire AWS à n'importe quel système bancaire hérité ?

La solution est conçue pour être adaptable et peut s'intégrer à n'importe quel système bancaire hérité capable d'accepter des appels d'API standard.

Puis-je personnaliser la boîte de dialogue d'intégration ?

Oui, vous pouvez personnaliser la boîte de dialogue du chatbot en fonction de votre cas d'utilisation et de la séquence de dialogue ciblée. Pour plus d'informations, consultez [QnA Bot on AWS](#) dans la bibliothèque de AWS solutions.

Étapes suivantes

Il existe d'autres cas d'utilisation du CLM au-delà de l'intégration des clients, et ces cas d'utilisation peuvent être modernisés grâce à des services intégrés. AWS Cloud Les scénarios suivants examinent certains cas d'utilisation potentiels de la modernisation :

1. Intégrez les recommandations de produits dans les produits et services bancaires en utilisant [Amazon Personalize](#) ou d'autres recommandations personnalisées. Bien que les produits FS soient différents des produits vendus au détail, un degré élevé de personnalisation est toujours prévu d'ici 2025, selon l'article [Industry Leaders Predict Massive Changes in Banking by 2025](#) de The Financial Brand. Les clients sont peut-être prêts à payer davantage pour des services hautement personnalisés et contextuels. Cela ne peut être implémenté qu'à l'aide de solutions plus intelligentes basées sur le machine learning.
2. Vous pouvez utiliser [Amazon Fraud Detector](#), un détecteur de fraude en ligne basé sur le machine learning, pour la surveillance des comptes. Vous pouvez également personnaliser d'autres algorithmes intégrés afin de proposer des services de surveillance des comptes normalisés (par exemple, en utilisant la détection d'anomalies).

Note

Amazon Fraud Detector n'est plus ouvert aux nouveaux clients depuis le 7 novembre 2025. Pour des fonctionnalités similaires à Amazon Fraud Detector, explorez Amazon SageMaker AutoGluon, et AWS WAF. Pour plus d'informations, consultez la section [Modification de la disponibilité d'Amazon Fraud Detector](#).

3. Vous pouvez avoir des assistants intelligents qui interagissent directement avec les clients à l'aide d'Amazon Lex et de chatbots basés sur les modèles de langage naturel les plus récents.

Même si les solutions créatives n'ont aucune limite, vous devez toutefois intégrer et déployer de telles solutions rapidement et à grande échelle.

Ressources

- [Ce que le financement intégré et les banking-as-a-service tendances signifient pour les services financiers](#) (McKinsey et l'entreprise)
- [Digital onboarding in finance: a novel model and related cybersecurity risks](#) (Open Research Europe)
- [Industry Leaders Predict Massive Changes in Banking by 2025](#) (The Financial Brand)
- [AWS Guide de l'utilisateur sur les réglementations et directives relatives aux services financiers en Suisse et publications des cahiers de travail de la FINMA \(blog sur AWS la sécurité\)](#)
- [Pleins feux sur les services FSI : Featuring AWS Lambda](#) (article de AWS blog)
- [Amazon Rekognition annonce des mises à jour de ses fonctionnalités de détection, d'analyse et de reconnaissance des visages \(AWS Machine Learning Blog\)](#)
- [QnA Bot activé AWS](#) (bibliothèque de AWS solutions)

Historique du document

Le tableau suivant décrit les modifications importantes apportées à ce guide. Pour être averti des mises à jour à venir, abonnez-vous à un [fil RSS](#).

Modification	Description	Date
Publication initiale	—	8 juin 2022

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.