Sécurité à l'échelle : la journalisation dans AWS

Comment AWS CloudTrail peut vous aider à atteindre la conformité en journalisant les appels d'API et les modifications apportées aux ressources

Octobre 2015

(Consultez https://aws.amazon.com/compliance/aws-whitepapers/ pour obtenir la version la plus récente de ce livre blanc)

Table des matières

Résumé

La journalisation et la supervision des appels d'API sont les principaux composants des bonnes pratiques opérationnelles et en matière de sécurité, ainsi que les exigences sectorielles et réglementaires. AWS CloudTrail est un service Web qui enregistre les appels d'API vers les services AWS pris en charge sur votre compte AWS et transmet un fichier journal à votre compartiment Amazon Simple Storage Service (Amazon S3). AWS CloudTrail résout les difficultés apparaissant fréquemment dans un environnement sur site et vous permet également de respecter plus facilement les stratégies ou normes réglementaires, le service vous permet de facilement améliorer votre sécurité et vos processus opérationnels.

Ce document présente les principales exigences en matière de conformité liées à la journalisation et les détails sur la manière dont les fonctions d'AWS CloudTrail peuvent permettre de les appliquer. L'utilisation d'AWS CloudTrail n'implique aucun coût supplémentaire, à l'exception des frais standard pour le stockage des journaux de S3 et pour l'utilisation de SNS pour une notification facultative.

Introduction

Amazon Web Services (AWS) fournit une vaste gamme de services et de ressources informatiques à la demande que vous pouvez lancer et gérer, avec une tarification en fonction de votre utilisation. L'enregistrement des appels d'API AWS et des modifications connexes dans la configuration des ressources est un composant essentiel de la gouvernance, la sécurité et la conformité informatiques. AWS CloudTrail constitue une solution simple pour l'enregistrement d'appels d'API AWS et des modifications des ressources qui permet de résoudre les problèmes d'infrastructure et de stockage sur site, en vous aidant à créer des contrôles de prévention et de sécurité améliorés pour votre environnement AWS. Les solutions de journalisation sur site nécessitent l'installation d'agents, la configuration de fichiers de configuration et de serveurs de journalisation centralisés, et la création et la maintenance de magasins de données onéreux et durables pour le stockage des données. AWS CloudTrail supprime cette configuration d'infrastructure lourde et vous permet d'activer la journalisation en seulement deux clics et d'obtenir une visibilité accrue dans tous les appels d'API de votre compte AWS. CloudTrail reçoit en continu des appels d'API depuis plusieurs serveurs dans un pipeline de traitement hautement disponible. Pour activer CloudTrail, il vous suffit de vous connecter à AWS Management Console, d'accéder à la console CloudTrail et de cliquer pour activer la journalisation. Pour en savoir plus sur les services et régions pouvant être utilisés avec AWS CloudTrail, accédez au site Web d'AWS CloudTrail.

Ce document a été développé en utilisant un ensemble d'exigences de journalisation sur des infrastructures de conformité fréquentes (p. ex. ISO 27001:2005, PCI DSS v2.0, FedRAMP) et en les combinant dans des contrôles généralisés et des domaines de journalisation. Vous pouvez tirer parti de ce document pour un ensemble de cas d'utilisation comme les meilleures pratiques opérationnelles et en termes de sécurité, le respect des stratégies internes, les normes sectorielles, les réglementations légales, etc. Le document est rédigé de manière générique, pour permettre à tous de comprendre comment AWS CloudTrail peut améliorer vos activités existantes de journalisation et de supervision.

Contrôle de l'accès aux fichiers journaux

Pour maintenir l'intégrité de vos données des journaux, il est important de gérer attentivement l'accès autour de la génération et du stockage de vos fichiers journaux. La capacité à consulter ou modifier vos données de journal sera limitée aux utilisateurs autorisés. Un défi fréquent lié à la journalisation pour les environnements sur site est la capacité à démontrer que les régulateurs qui accèdent aux données de journal ne sont que des utilisateurs autorisés. Ce contrôle peut prendre du temps et être compliqué car la majorité des environnements sur site ne présentent pas de solution de journalisation unique ou une sécurité de journalisation cohérente sur tous les systèmes.

Avec AWS CloudTrail, l'accès aux fichiers journaux d'Amazon S3 est contrôlé au niveau central dans AWS, ce qui vous permet de contrôler facilement l'accès à vos fichiers journaux et de démontrer l'intégrité et la confidentialité de vos données de journal.

	Exigences de journalisation fréquentes	Comment AWS CloudTrail peut vous aider à atteindre la conformité aux exigences
Contrôle de l'accès aux fichiers journaux	Des contrôles pour empêcher l'accès non autorisé aux journaux existent.	AWS CloudTrail vous permet de limiter l'accès à vos fichiers journaux. Vous pouvez empêcher et contrôler l'accès pour procéder à des modifications à vos données de fichier journal en configurant vos rôles AWS IAM (Identity and Access Management) et vos stratégies de compartiment Amazon S3 pour permettre un accès en lecture seule à vos fichiers journaux. En savoir plus. De plus, vous pouvez renforcer vos contrôles d'authentification et d'autorisation en activant l'AWS MFA (Multi Factor Authentication) sur votre ou vos compartiments Amazon S3 qui stockent vos journaux AWS CloudTrail. En savoir plus.
	Des contrôles existent pour garantir que l'accès aux fichiers journaux est basé sur les rôles.	AWS CloudTrail vous permet de contrôler l'accès des utilisateurs à vos fichiers journaux sur base d'un provisionnement détaillé sur base des rôles. AWS IAM vous permet de contrôler l'accès en toute sécurité à AWS CloudTrail pour vos utilisateurs. Et à l'aide de rôles IAM et de stratégies de compartiment Amazon S3, vous pouvez garantir un accès en fonction du rôle au compartiment S3 qui stocke vos fichiers de journalisation AWS CloudTrail. En savoir plus.

Obtention d'alertes relatives à la création et à la mauvaise configuration du fichier journal

Des alertes en temps quasi réel pour des problèmes de configuration de journaux détaillant des appels d'API ou des modifications de ressources sont essentielles pour une gouvernance et un respect informatiques efficaces aux exigences internes et externes en termes de conformité. Même d'un point de vue opérationnel, il est impératif de configurer correctement la journalisation pour vous permettre de surveiller les activités de vos utilisateurs et de vos ressources. Toutefois, la variabilité et l'étendue de l'infrastructure de journalisation dans des environnements sur site sont importantes pour une surveillance active et vous alerter en cas de problèmes de configuration ou de changements à votre configuration de journalisation.

Une fois que vous activez AWS CloudTrail pour votre compte, le service fournira des fichiers journaux à votre compartiment S3. En outre, CloudTrail publiera des notifications pour des transferts de fichier journal vers une rubrique SNS, de manière à ce que vous puissiez agir après le transfert. Ces alertes incluent l'adresse du fichier journal de compartiment Amazon S3 pour vous permettre d'accéder rapidement aux métadonnées d'objet relatives à l'événement depuis les fichiers journaux sources. De plus, votre AWS Management Console vous avertira si vos fichiers journaux sont mal configurés. Par conséquent, la journalisation n'a plus lieu.

	Exigences de journalisation fréquentes	Comment AWS CloudTrail peut vous aider à atteindre la conformité aux exigences
Réception d'alertes relatives à la création et à la mauvaise configuration du fichier journal	Fournissez des alertes lorsque des journaux sont créés ou échouent et suivent les actions définies par l'organisation en cas de problème de configuration.	AWS CloudTrail vous avertit immédiatement en cas de problèmes liés à votre configuration de journalisation sur votre AWS Management Console. En savoir plus.
	Les alertes liées au problème de configuration de journal dirigeront les utilisateurs vers les journaux pertinents pour obtenir des détails supplémentaires (et ne présenteront pas de détails inutiles).	AWS CloudTrail enregistre l'adresse du fichier journal du compartiment Amazon S3 à chaque fois qu'un nouveau fichier journal est rédigé. AWS CloudTrail publie des notifications pour la création de fichier journal, de manière à ce que les clients puissent agir en temps quasi réel lorsque des fichiers journaux sont créés. La notification est envoyée à votre compartiment Amazon S3 et apparaît dans AWS Management Console. En outre, des messages Amazon SNS peuvent être envoyés vers des appareils mobiles ou des services distribués, configurés via une API ou AWS Management Console. Le message SNS pour la création de fichiers journaux fournit l'adresse de fichier journal, ce qui limite les informations publiées au strict nécessaire, tout en vous permettant d'établir un lien aisément, pour obtenir des détails supplémentaires sur l'événement. En savoir plus.

Gérer les modifications apportées aux ressources AWS et aux fichiers journaux

La compréhension des modifications apportées à vos ressources est un composant essentiel de la gouvernance et de la sécurité informatiques. Toutefois, le fait d'empêcher les modifications et l'accès non autorisé à ces données de journal a un impact direct sur l'intégrité de vos processus de gestion des modifications et sur votre capacité à respecter les exigences internes, sectorielles et réglementaires en matière de gestion des modifications. L'un des principaux défis dans les environnements sur site est la capacité à journaliser les modifications des ressources ou les modifications des journaux car il ne s'agit que de ressources finies à votre disposition pour surveiller ce qui semble être un volume infini de données.

AWS CloudTrail vous permet de suivre les modifications apportées à une ressource AWS, notamment la création, la modification et la suppression. De plus, en revoyant l'historique de journalisation des appels d'API, AWS CloudTrail vous permet d'enquêter sur un événement pour déterminer si des changements non autorisés ou inattendus sont survenus en analysant qui les a initialisés, quand ils sont survenus et d'où ils proviennent. En outre, CloudTrail publiera des notifications sur une rubrique SNS, de manière à ce que vous puissiez agir après le transfert du nouveau fichier journal sur votre compartiment Amazon S3.

Gérer les modifications apportées aux ressources informatiques et aux fichiers journaux	Exigences de journalisation fréquentes	Comment AWS CloudTrail peut vous aider à atteindre la conformité aux exigences
	Fournissez un journal des modifications apportées aux composants systèmes (notamment la création et la suppression d'objets au niveau du système).	AWS CloudTrail produit des données de journal relatives à des événements de changement système pour permettre le suivi des modifications apportées à vos ressources AWS. AWS CloudTrail fournit une visibilité des modifications apportées à votre ressource AWS de sa création à sa suppression, en journalisant les modifications apportées à l'aide d'appels d'API via AWS Management Console, l'interface ligne de commande (CLI) AWS ou les kits de développement logiciel (SDK) AWS. En savoir plus.
	Des contrôles existent pour empêcher les modifications aux journaux de modifications ou les erreurs associées aux journaux.	Par défaut, les fichiers journaux d'appel d'API sont chiffrés à l'aide du chiffrement côté serveur (SSE) S3 et placés dans votre compartiment S3. Les modifications apportées aux données de journal peuvent être contrôlées via l'utilisation d'IAM et de MFA pour permettre l'accès en lecture seule à votre compartiment Amazon S3 qui stocke vos fichiers journaux AWS CloudTrail. En savoir plus.

Stockage de fichiers journaux

Les normes en vigueur dans le secteur et les réglementations légales peuvent nécessiter que les fichiers journaux soient stockés pour différentes périodes. Par exemple, PCI DSS nécessite le stockage des journaux pendant un an, HIPAA nécessite la conservation des enregistrements pendant au moins six ans et d'autres exigences demandent des périodes de stockage plus longues ou variables en fonction des données journalisées. Ainsi, la gestion des exigences pour le stockage des fichiers journaux pour des données différentes sur des systèmes différents peut représenter un obstacle administratif et technologique. De plus, le stockage et l'archivage de grands volumes de données de journal de manière permanente et sécurisée peuvent être un défi pour de nombreuses organisations.

AWS CloudTrail est conçu pour s'intégrer de manière transparente à Amazon S3 et Amazon Glacier, ce qui permet la personnalisation de compartiments S3 et de règles du cycle de vie pour s'adapter à vos besoins en matière de stockage. AWS CloudTrail offre une période de validité infinie à vos journaux, afin que vous puissiez personnaliser la période de stockage de vos journaux afin de répondre aux exigences de vos régulateurs.

	Exigences de journalisation fréquentes	Comment AWS CloudTrail peut vous aider à atteindre la conformité aux exigences
Stockage de fichiers journaux	Les journaux sont conservés pendant au moins un an.	Pour faciliter le stockage de fichiers journaux, vous pouvez configurer AWS CloudTrail pour regrouper vos fichiers journaux sur toutes les régions ou plusieurs comptes en un compartiment S3 unique. AWS CloudTrail vous permet de personnaliser votre période de stockage de journaux en configurant votre ou vos périodes de validité souhaitées rédigées dans votre compartiment Amazon S3. Vous contrôlez les politiques de rétention pour vos fichiers journaux CloudTrail. Vous pouvez conserver des fichiers journaux pendant une période définie de votre choix ou indéfinies. Par défaut, les fichiers journaux sont stockés indéfiniment. Vous pouvez également déplacer vos données de journal vers Amazon Glacier pour des économies supplémentaires associées au stockage à froid. En savoir plus.
	Stockez des journaux pendant une période définie par l'organisation.	
	Stockez des journaux en temps réel à des fins de résilience.	AWS CloudTrail assure la résilience des fichiers journaux grâce à l'infrastructure de stockage hautement durable d'Amazon S3. Le stockage standard d'Amazon S3 est conçu pour fournir 99,999999999 % de durabilité et 99,99 % de disponibilité des objets sur une année donnée. En savoir plus.

Générer une création de rapport personnalisée de données de journal

Du point de vue opérationnel et de la sécurité, la journalisation des appels d'API fournit les données et le contexte requis pour analyser le comportement des utilisateurs et comprendre certains événements. Les appels d'API et les journaux de modification de ressources informatiques peuvent également être utilisés pour démontrer que seuls les utilisateurs autorisés ont réalisé certaines tâches dans votre environnement conformément aux exigences de conformité. Toutefois, étant donné le volume et la variabilité associés aux journaux de différents systèmes, il peut être difficile, dans un environnement sur site, de comprendre clairement les activités des utilisateurs et les modifications apportées à vos ressources informatiques.

AWS CloudTrail produit des données que vous pouvez utiliser pour détecter les comportements anormaux, récupérer des activités d'événement associées à des objets spécifiques ou fournir une piste d'audit simple pour votre compte. Vous pouvez faire évoluer votre analyse de journalisation actuelle à l'aide de plus de 25 champs différents au cas où les données fournies par AWS CloudTrail pour créer des requêtes ou des rapports personnalisés concernent des enquêtes internes, la conformité externe, etc. AWS CloudTrail vous permet de surveiller les appels d'API pour un ou des comportements spécifiques connus non désirés et d'activer des alarmes à l'aide de vos solutions de gestion des journaux ou de gestion des événements et des incidents en matière de sécurité (SIEM). Les données enrichies fournies par AWS CloudTrail peuvent accélérer votre enquête et diminuer votre temps de réponse à l'incident. En outre, les données fournies par AWS CloudTrail peuvent vous permettre de réaliser une analyse de sécurité plus approfondie des appels d'API afin d'identifier les comportements et modèles latents suspects qui ne génèrent pas d'alarmes immédiates mais qui peuvent constituer un problème de sécurité. Enfin, AWS CloudTrail fonctionne avec de nombreux partenaires présentant des solutions prêtes à l'emploi en termes de sécurité, d'analyse et d'alerte. En savoir plus sur les solutions de nos partenaires sur le site Web d'AWS CloudTrail.

	Exigences de journalisation fréquentes	Comment AWS CloudTrail peut vous aider à atteindre la conformité aux exigences
Générer une création de rapport personnalisée de données de journal	Journalisez l'accès de l'utilisateur aux ressources en fonction du système et des mesures prises. L'accès de l'utilisateur inclut l'accès par les administrateurs système et les opérateurs système. Les ressources incluent des journaux de piste d'audit.	AWS CloudTrail permet de générer des rapports d'appel d'API complets et détaillés en journalisant des activités effectuées par tous les utilisateurs qui accèdent à vos ressources AWS journalisées, notamment la racine, les utilisateurs IAM, les utilisateurs fédérés et tout utilisateur ou service effectuant des activités au nom d'utilisateurs, à l'aide de n'importe quelle méthode d'accès. En savoir plus.
	Produisez des journaux à une fréquence définie par l'organisation.	AWS CloudTrail permet d'utiliser les outils d'analyse de journal pour récupérer des données de fichier journal à des fréquences personnalisées en créant des journaux en temps quasi réel et en fournissant généralement les données de journal à votre compartiment Amazon S3 dans les 15 minutes qui suivent l'appel d'API. Vous pouvez utiliser les fichiers journaux sous forme d'entrée dans vos solutions d'analyse et de gestion des journaux de pointe afin de procéder à l'analyse. En savoir plus.
	Fournissez un journal lorsque l'activité de journalisation a été initiée.	AWS CloudTrail journalise tous les appels d'API, notamment en activant et en désactivant la journalisation d'AWS CloudTrail. Cela vous permet d'effectuer le suivi lorsque CloudTrail est activé ou désactivé. En savoir plus.
	Générez des journaux synchronisés à une seule horloge système interne pour fournir des informations cohérentes sur l'horodatage.	AWS CloudTrail produit des données de journaux depuis une seule horloge système interne en générant des horodatages d'événement en heure universelle coordonnée (UTC), conformément aux normes en matière de format de date et d'heure ISO 8601. En savoir plus.
	Fournissez des journaux qui montrent des activités inappropriées ou inhabituelles.	AWS CloudTrail vous permet de surveiller des appels d'API en registrant des échecs d'autorisation dans votre compte AWS, vous permettant de suivre les tentatives d'accès aux ressources limitées ou les autres activités inhabituelles. En savoir plus.
	Fournissez des journaux avec des détails adéquats sur les événements.	AWS CloudTrail permet des appels d'API avec des informations détaillées comme le type, les données et l'heure, l'emplacement, la source/l'origine, le résultat (notamment des exceptions, défaillances et informations relatives à un événement de sécurité), la ressource affectée (données, système, etc.) et l'utilisateur associé. AWS CloudTrail peut vous aider à identifier l'utilisateur, l'heure de l'événement, l'adresse IP de l'utilisateur, les paramètres de requête fournis par l'utilisateur, les éléments de réponse retournés par le service, le code d'erreur facultatif et le message d'erreur. En savoir plus.

Conclusion

Vous pouvez exécuter sur AWS quasi tous les éléments que vous exécuteriez sur site : sites Web, applications, bases de données, applications mobiles, campagnes d'e-mail, analyse de données distribuées, stockage de média et réseaux privés. Les services fournis par AWS sont conçus pour fonctionner ensemble afin que vous puissiez créer des solutions complètes. AWS CloudTrail offre une solution simple pour enregistrer l'activité des utilisateurs et ne pas avoir à exécuter un système de journalisation complexe. Un autre avantage de la migration de charges de travail vers AWS est la capacité à atteindre un niveau de sécurité plus élevé, à l'échelle, en utilisant les nombreuses fonctions permettant la gouvernance disponibles. Pour les mêmes raisons que la fourniture de l'infrastructure dans le cloud a des avantages par rapport à la fourniture sur site, la gouvernance basée sur le cloud présente des frais d'entrée réduits, des opérations plus aisées et une agilité accrue en fournissant une visibilité, un contrôle de sécurité et une automatisation centrale accrus. AWS CloudTrail est l'un des services que vous pouvez utiliser pour atteindre un niveau élevé de gouvernance de vos ressources informatiques à l'aide d'AWS.

Ressources supplémentaires

Voici des liens en réponse aux questions fréquentes liées à la journalisation dans AWS :

- Que puis-je faire avec AWS ? En savoir plus.
- Comment puis-je commencer à utiliser AWS ? En savoir plus.
- Comment puis-je commencer à utiliser AWS CloudTrail ? En savoir plus.
- AWS CloudTrail a-t-il une liste de FAQ ? En savoir plus.
- Comment puis-je atteindre la conformité en utilisant AWS ? En savoir plus.
- Comment puis-je me préparer à un audit en utilisant AWS ? En savoir plus.

Annexe : index du programme de conformité

Les informations de ce livre blanc ont été présentées en journalisant des domaines d'exigence. À des fins de référence, les exigences de journalisation par cadre de conformité commun sont reprises dans le tableau ci-dessous :

Programme de conformité AWS	Exigence de conformité
Norme PCI (Payment Card Industry) DSS (Data Security Standard) de niveau 1 AWS est conforme au niveau 1 selon la norme PCI DSS. Vous pouvez donc exécuter des applications sur notre infrastructure technologique conforme à la norme PCI pour stocker, traiter et transmettre des informations relatives aux cartes de paiement dans le cloud. En savoir plus.	**PCI 5.2 :** Veillez à ce que tous les mécanismes antivirus soient actuels, en cours d'exécution et génèrent des journaux d'audit.
	PCI 10.1 : Établissez un processus pour la liaison de tous les accès aux composants système (notamment l'accès réalisé à l'aide de privilèges administratifs, comme la racine) pour chaque utilisateur.
	PCI 10.2 : Implémentez les pistes d'audit automatisées pour tous les composants système afin de reconstruire les événements suivants : **10.2.1 :** Tous les accès individuels aux données du titulaire de carte **10.2.2 :** Toutes les actions réalisées par un individu avec des privilèges racines ou administratifs **10.2.3 :** Accès à toutes les pistes d'audit **10.2.4 :** Tentatives d'accès logique non valides **10.2.5 :** Utilisation des mécanismes d'identification et d'authentification **10.2.6 :** Initialisation des journaux d'audit **10.2.7 :** Création et suppression d'objets au niveau système
	PCI 10.3 : Enregistrez au moins les entrées de piste d'audit suivantes pour tous les composants système pour chaque événement : **10.3.1 :** Identification de l'utilisateur **10.3.2 :** Type d'événement **10.3.3 :** Date et heure **10.3.4 :** Indication de réussite ou d'échec **10.3.5 :** Origine de l'événement **10.3.6 :** Identité ou nom des données, du composant système ou de la ressource concernés
	PCI 10.4.2 : Les données d'heure sont protégées.
	PCI 10.5 : Sécurisez toutes les pistes d'audit afin qu'elles ne puissent pas être altérées.
	PCI 10.5.1 : Limitez l'affichage de pistes d'audit aux personnes qui en ont besoin pour leur travail.
	PCI 10.5.2 : Protégez les fichiers de piste d'audit des modifications non autorisées.
	PCI 10.5.3 : Sauvegardez rapidement les fichiers de piste d'audit sur un serveur de journal centralisé ou un support difficile à altérer.

Programme de conformité AWS	Exigence de conformité
Norme PCI (Payment Card Industry) DSS (Data Security Standard) de niveau 1 AWS est conforme au niveau 1 selon la norme PCI DSS. Vous pouvez donc exécuter des applications sur notre infrastructure technologique conforme à la norme PCI pour stocker, traiter et transmettre des informations relatives aux cartes de paiement dans le cloud. En savoir plus.	**PCI 10.5.4 :** Rédigez des journaux pour des technologies externes sur un serveur de journal dans un LAN interne.
	PCI 10.5.5 : Utilisez la supervision de l'intégrité du fichier ou le logiciel de détection des modifications dans des journaux pour s'assurer que les données de journal existantes ne puissent pas être modifiées sans générer d'alertes (bien que les nouvelles données ajoutées ne devraient pas générer d'alerte).
	PCI 10.6 : Consultez les journaux de tous les composants système au moins une fois par jour. Les vérifications de journaux doivent inclure les serveurs qui réalisent des fonctions de sécurité, comme le système de détection des intrusions (IDS) et les serveurs de protocole AAA (par exemple, RADIUS).
	PCI 10.7 : Conservez l'historique des pistes d'audit pendant au moins un an, avec au moins trois mois disponibles immédiatement pour l'analyse (par exemple, en ligne, archivé ou pouvant être restauré depuis la sauvegarde).
	PCI 11.5 : Déployez les outils de supervision d'intégrité de fichier pour alerter le personnel en cas de modification non autorisée de fichiers système critiques, de fichiers de configuration ou de fichiers de contenu ; et configurer le logiciel afin d'effectuer des comparaisons de fichiers critiques au moins chaque semaine.
	PCI 12.2 : Développez des procédures opérationnelles quotidiennes de sécurité qui respectent les exigences de cette spécification (par exemple, procédures de maintenance de compte utilisateur et procédures de vérification de journal).
	PCI A.1.2.d : Limitez l'accès de chaque entité et les privilèges à l'environnement de données de titulaire de carte uniquement.
	PCI A.1.3 : Veillez à ce que la journalisation et les pistes d'audit soient activées et uniques pour l'environnement de données de titulaire de carte de chaque entité et respectent l'exigence PCI DSS 10.
	PCI 11.4 : Utilisez des systèmes de détection d'intrusion et/ou de prévention d'intrusion pour superviser tout le trafic autour de l'environnement de données du titulaire de carte, ainsi qu'à des points critiques de cet environnement, et alerter le personnel en cas de suspicion de compromis. Gardez à jour tous les moteurs de détection et prévention des intrusions, toutes les références et toutes les signatures.

Programme de conformité AWS	Exigence de conformité
Norme PCI (Payment Card Industry) DSS (Data Security Standard) de niveau 1 AWS est conforme au niveau 1 selon la norme PCI DSS. Vous pouvez donc exécuter des applications sur notre infrastructure technologique conforme à la norme PCI pour stocker, traiter et transmettre des informations relatives aux cartes de paiement dans le cloud. En savoir plus.	**PCI 11.5 :** Déployez les outils de supervision d'intégrité de fichier pour alerter le personnel en cas de modification non autorisée de fichiers système critiques, de fichiers de configuration ou de fichiers de contenu ; et configurer le logiciel afin d'effectuer des comparaisons de fichiers critiques au moins chaque semaine.
Service Organization Controls 2 (SOC 2) Le rapport SOC 2 est une attestation qui développe l'évaluation des contrôles par rapport aux critères stipulés par l'AICPA (American Institute of Certified Public Accountants) dans ses principes sur les services de confiance (« Trust Services Principles »). Ces principes définissent des contrôles portant sur les pratiques majeures par rapport à la sécurité, à la disponibilité, à l'intégrité de traitement, à la confidentialité et au respect de la vie privée, et s'appliquent aux prestataires de services tels qu'AWS. En savoir plus.	**SOC 2 Security 3.2.g :** Des procédures existent pour limiter l'accès logique au système défini, notamment, sans s'y limiter, les éléments suivants : restriction de l'accès aux configurations système, fonctionnalité de super utilisateur, mots de passe principaux, utilitaires puissants et appareils de sécurité (par exemple, pare-feu).
	SOC 2 Security 3.3 : Des procédures existent pour limiter l'accès physique au système défini incluant, sans s'y limiter, des infrastructures, des supports de sauvegarde et d'autres composants système comme des pare-feu, des routeurs et des serveurs.
	SOC 2 Security 3.7 : Des procédures existent pour identifier, rapporter et prendre des mesures au niveau de failles de sécurité système et d'autres incidents.
	SOC 2 Availability 3.5.f : Des procédures existent pour limiter l'accès logique au système défini, notamment, sans s'y limiter, les éléments suivants : restriction de l'accès aux configurations système, fonctionnalité de super utilisateur, mots de passe principaux, utilitaires puissants et appareils de sécurité (par exemple, pare-feu).
	SOC 2 Availability 3.6 : Des procédures existent pour limiter l'accès physique au système défini incluant, sans s'y limiter, des infrastructures, des supports de sauvegarde et d'autres composants système comme des pare-feu, des routeurs et des serveurs.

Programme de conformité AWS	Exigence de conformité
Service Organization Controls 2 (SOC 2) Le rapport SOC 2 est une attestation qui développe l'évaluation des contrôles par rapport aux critères stipulés par l'AICPA (American Institute of Certified Public Accountants) dans ses principes sur les services de confiance (« Trust Services Principles »). Ces principes définissent des contrôles portant sur les pratiques majeures par rapport à la sécurité, à la disponibilité, à l'intégrité de traitement, à la confidentialité et au respect de la vie privée, et s'appliquent aux prestataires de services tels qu'AWS. En savoir plus.	**SOC 2 Availability 3.10 :** Des procédures existent pour identifier, rapporter et prendre des mesures au niveau de problèmes de disponibilité et de failles de sécurité et d'autres incidents connexes.
	SOC 2 Confidentiality 3.3 : Les procédures de l'étude liées à la confidentialité du traitement des données sont conformes aux politiques de confidentialité documentées.
	SOC 2 Confidentiality 3.8.1 : Des procédures existent pour limiter l'accès logique au système et aux ressources d'informations confidentielles conservées dans le système, notamment, sans s'y limiter, les éléments suivants : restriction de l'accès aux configurations système, fonctionnalité de super utilisateur, mots de passe principaux, utilitaires puissants et appareils de sécurité (par exemple, pare-feu).
	SOC 2 Confidentiality 3.13 : Des procédures existent pour identifier, rapporter et prendre des mesures au niveau de failles de confidentialité et de sécurité système et d'autres incidents.
	SOC 2 Confidentiality 4.2 : Il existe un processus d'identification et de traitement des dysfonctionnements potentiels de la capacité de l'entité à atteindre ses objectifs conformément aux politiques de confidentialité du système et de sécurité connexes.
	SOC 2 Integrity 3.6.g : Des procédures existent pour limiter l'accès logique au système défini, notamment, sans s'y limiter, les éléments suivants : restriction de l'accès aux configurations système, fonctionnalité de super utilisateur, mots de passe principaux, utilitaires puissants et appareils de sécurité (par exemple, pare-feu).
	SOC 2 Integrity 4.1 : Les performances en matière d'intégrité et de sécurité du traitement du système sont vérifiées régulièrement et comparées aux politiques définies en la matière.
	SOC 2 Integrity 4.2 : Il existe un processus d'identification et de traitement des dysfonctionnements potentiels de la capacité de l'entité à atteindre ses objectifs conformément aux politiques d'intégrité du traitement du système et de sécurité connexes définies.

Programme de conformité AWS	Exigence de conformité
Organisation internationale de normalisation (ISO) 27001 ISO 27001 est une norme de sécurité globale largement adoptée qui souligne les exigences pour les systèmes de gestion de la sécurité des informations. Elle offre une approche systématique de gestion des informations de la société et des clients basée sur des évaluations régulières des risques. En savoir plus.	*En raison des lois sur les droits d'auteur, AWS ne peut pas fournir les descriptions des exigences pour la norme ISO 27001. Vous pouvez acheter une copie de la norme ISO 27001 en ligne à partir de différentes sources, notamment ISO.org*
Federal Risk and Authorization Management Program (FedRAMP) Le programme FedRAMP est un programme gouvernemental qui fournit une approche normalisée de l'évaluation de la sécurité, de l'autorisation et de la surveillance continue pour les produits et services de cloud jusqu'au niveau Modéré. En savoir plus.	**FedRAMP NIST 800-53 Rev 3 AU-2 :** L'organisation : a. Détermine, sur base d'une évaluation des risques et des besoins de la mission/professionnels, que le système d'information doit pouvoir réaliser l'audit des événements suivants : [affectation : liste définie par l'organisation des événements pouvant faire l'objet d'un audit] ; b. Coordonne la fonction de l'audit de sécurité avec d'autres entités organisationnelles nécessitant des informations liées à l'audit pour améliorer la prise en charge mutuelle et guider la sélection des événements pouvant faire l'objet d'un audit ; c. Explique pourquoi la liste des événements pouvant faire l'objet d'un audit est conforme pour la réalisation d'investigations a posteriori d'incidents de sécurité ; et d. Détermine, sur base des informations actuelles sur la menace et de l'évaluation en cours des risques, que les événements suivants doivent faire l'objet d'un audit dans le système d'information : [affectation : sous-ensemble défini par l'organisation des événements pouvant faire l'objet d'un audit définis dans la norme AU-2 a. afin qu'ils fassent l'objet d'un audit, avec la fréquence d'audit (ou la situation nécessitant un audit) pour chaque événement identifié].
	FedRAMP NIST 800-53 Rev 4 AU 2 : L'organisation : a. Détermine que le système d'information doit pouvoir réaliser l'audit des événements suivants : [affectation : événements pouvant faire l'objet d'un audit définis par l'organisation] ; b. Coordonne la fonction de l'audit de sécurité avec d'autres entités organisationnelles nécessitant des informations liées à l'audit pour améliorer la prise en charge mutuelle et guider la sélection des événements pouvant faire l'objet d'un audit ; c. Explique pourquoi les événements pouvant faire l'objet d'un audit sont conformes pour la réalisation d'investigations a posteriori d'incidents de sécurité ; et d. Détermine que les événements suivants doivent faire l'objet d'un audit dans le système d'information : [affectation : sous-ensemble défini par l'organisation des événements pouvant faire l'objet d'un audit définis dans la norme AU-2 a. afin qu'ils fassent l'objet d'un audit, avec la fréquence d'audit (ou la situation nécessitant un audit) pour chaque événement identifié].
	FedRAMP NIST 800-53 Rev 3 AU-3 : Le système d'information produit des enregistrements d'audit qui contiennent suffisamment d'informations pour, au moins, établir quel type d'événement est survenu, quand (date et heure) il est survenu, où il est survenu, la source de l'événement, le résultat (réussite ou échec) et l'identité de tout utilisateur/sujet associé à l'événement.

Programme de conformité AWS	Exigence de conformité
	FedRAMP NIST 800-53 Rev 4 AU-3 : Le système d'information produit des enregistrements d'audit qui contiennent des informations pour, au moins, établir quel type d'événement est survenu, quand (date et heure) il est survenu, où il est survenu, la source de l'événement, le résultat et l'identité de tout utilisateur ou sujet associé à l'événement.
	FedRAMP NIST 800-53 Rev 3 AU-4 : L'organisation attribue une capacité de stockage d'enregistrement d'audit et configure les audits afin de réduire la probabilité de dépasser cette capacité.
	FedRAMP NIST 800-53 Rev 4 AU-4 : L'organisation attribue une capacité de stockage d'enregistrement d'audit conformément à [affectation : exigences de stockage des enregistrements d'audit définies par l'organisation].
Federal Risk and Authorization Management Program (FedRAMP) Le programme FedRAMP est un programme gouvernemental qui fournit une approche normalisée de l'évaluation de la sécurité, de l'autorisation et de la surveillance continue pour les produits et services de cloud jusqu'au niveau Modéré. En savoir plus.	**FedRAMP NIST 800-53 Rev 3 AU-5 :** Le système d'information : a. Alerte les autorités organisationnelles désignées en cas d'échec de traitement d'un audit ; et b. Prend les mesures supplémentaires suivantes : [affectation : actions définies par l'organisation à effectuer (p. ex., arrêter le système d'information, remplacer les enregistrements d'audit les plus anciens, arrêter la génération d'enregistrements d'audit)].
	FedRAMP NIST 800-53 Rev 4 AU-5 : Le système d'information : a. Alerte [affectation : personnel défini par l'organisation] en cas d'échec de traitement d'un audit ; et b. Prend les mesures supplémentaires suivantes : [affectation : actions définies par l'organisation à effectuer (p. ex., arrêter le système d'information, remplacer les enregistrements d'audit les plus anciens, arrêter la génération d'enregistrements d'audit)].
	FedRAMP NIST 800-53 Rev 3 AU-6 : L'organisation : a. Vérifie et analyse les enregistrements d'audit du système d'information [affectation : fréquence définie par l'organisation] pour des indications d'activité inappropriée ou inhabituelle et signale ses découvertes aux autorités organisationnelles désignées ; et b. Ajuste le niveau de contrôle d'audit, d'analyse et de création de rapport dans le système d'information en cas de modification du risque pour des opérations organisationnelles, des ressources organisationnelles, des individus, d'autres organisations ou la Nation en fonction des informations sur l'application de la loi, les connaissances ou d'autres sources d'information crédibles.
	FedRAMP NIST 800-53 Rev 3 AU-6 : L'organisation : a. Vérifie et analyse les enregistrements d'audit du système d'information [affectation : fréquence définie par l'organisation] pour des indications de [affectation : activité inappropriée ou inhabituelle définie par l'organisation] ; et b. Signale les découvertes à [affectation : personnel ou rôles définis par l'organisation].
	FedRAMP NIST 800-53 Rev 3 AU-8 : Le système d'information utilise des horloges système internes pour générer des horodatages pour les enregistrements d'audit.

Programme de conformité AWS	Exigence de conformité
Federal Risk and Authorization Management Program (FedRAMP) Le programme FedRAMP est un programme gouvernemental qui fournit une approche normalisée de l'évaluation de la sécurité, de l'autorisation et de la surveillance continue pour les produits et services de cloud jusqu'au niveau Modéré. En savoir plus.	**FedRAMP NIST 800-53 Rev 4 AU-8 :** Le système d'information : a. Utilise les horloges système internes pour générer des horodatages pour des enregistrements d'audit ; et b. Génère du temps dans les horodatages pouvant être mappé en heure universelle coordonnée (UTC) ou en heure de Greenwich (GMT) et répondant à [affectation : granularité de la mesure du temps définie par l'organisation].
	FedRAMP NIST 800-53 Rev 3 AU-9 : Le système d'information protège les informations de l'audit et les outils de l'audit contre les accès, modifications et suppressions non autorisés.
	FedRAMP NIST 800-53 Rev 4 AU-9 : Le système d'information protège les informations de l'audit et les outils de l'audit contre les accès, modifications et suppressions non autorisés.
	FedRAMP NIST 800-53 Rev 3 AU-10 : Le système d'information protège contre les individus qui nient avoir effectué une action spécifique.
	FedRAMP NIST 800-53 Rev 4 AU-10 : Le système d'information protège contre les individus (ou les processus agissant au nom d'un individu) qui nient avoir effectué [affectation : actions définies par l'organisation à couvrir par la non-répudiation].
	FedRAMP NIST 800-53 Rev 3 AU-11 : L'organisation conserve les enregistrements d'audit pour [affectation : période définie par l'organisation conforme à la politique de conservation des enregistrements] afin d'aider les investigations a posteriori des incidents et sécurité et de respecter les exigences relatives à la conservation des informations organisationnelles et réglementaires.
	FedRAMP NIST 800-53 Rev 4 AU-11 : L'organisation conserve les enregistrements d'audit pour [affectation : période définie par l'organisation conforme à la politique de conservation des enregistrements] afin d'aider les investigations a posteriori des incidents et sécurité et de respecter les exigences relatives à la conservation des informations organisationnelles et réglementaires.