aws

Livre blanc AWS

Architecting for HIPAA Security and Compliance on Amazon Web Services

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

Architecting for HIPAA Security and Compliance on Amazon Web Services: Livre blanc 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

Résumé i
Introduction 2
Chiffrement et protection des PHI dans AWS 4
Amazon API Gateway 8
Amazon AppFlow 9
Amazon AppStream 2.0 10
Amazon Athena 10
Amazon Aurora 11
Amazon Aurora PostgreSQL 11
Amazon CloudFront 12
Lambda@Edge 12
Amazon CloudWatch 12
CloudWatch Événements Amazon 13
Amazon CloudWatch Logs 13
Amazon Comprehend 13
Gestion des identités et des accès AWS 13
Protection des données et gestion des secrets 15
Segmentation et renforcement du réseau 17
Renforcement de l'hôte et de l'image 18
Multilocataire 18
Prévention du problème de l’adjoint confus entre services 19
Amazon Comprehend Medical 19
Amazon Connect 19
Amazon DocumentDB (compatible avec MongoDB) 20
Amazon DynamoDB 20
Amazon Elastic Block Store 21
Amazon EC2 21
Amazon Elastic Container Registry 22
Amazon ECS 22
Amazon EFS 23
Amazon EKS 24
Amazon ElastiCache pour Redis 24
Chiffrement au repos 25
Chiffrement de transport 25

Authentification 26
Appliquer les mises à jour ElastiCache de service 26
Amazon OpenSearch Service 27
Amazon EMR 27
Amazon EventBridge 27
Amazon Forecast 28
Amazon FSx 29
Amazon GuardDuty 29
Amazon HealthLake 30
Amazon Inspector 31
Service géré Amazon pour Apache Flink 31
Amazon Data Firehose 31
Amazon Kinesis Streams 32
Amazon Kinesis Video Streams 32
Amazon Lex 32
Amazon Managed Streaming for Apache Kafka (Amazon MSK) 33
Amazon MQ 34
Amazon Neptune 34
AWS Network Firewall 35
Amazon Pinpoint 35
Amazon Polly 36
Amazon Quantum Ledger Database (Amazon QLDB) 37
Amazon QuickSight 38
Amazon RDS for MariaDB 38
Amazon RDS for MySQL 39
Amazon RDS for Oracle 39
Amazon RDS for PostgreSQL 40
Amazon RDS for SQL Server 40
Chiffrement au repos 41
Chiffrement de transport 41
Audit 41
Amazon Redshift 41
Amazon Rekognition 42
Amazon Route 53 42
Amazon S3 Glacier 43
Amazon S3 Transfer Acceleration 43

Amazon SageMaker 43
Amazon SNS 44
Amazon Simple Email Service (Amazon SES) 45
Amazon SQS 45
Amazon S3 46
Amazon Simple Workflow Service 47
Amazon Textract 47
Amazon Transcribe 47
Amazon Translate 48
Amazon Virtual Private Cloud 48
Amazon WorkDocs 48
Amazon WorkSpaces 49
AWS App Mesh 50
AWS Service de migration d'applications 50
AWS Auto Scaling 50
AWS Backup 51
AWS Batch 52
AWS Certificate Manager 52
AWS Cloud Map 54
AWS CloudFormation 55
AWS CloudHSM 55
AWS CloudTrail 55
AWS CodeBuild 56
AWS CodeDeploy 56
AWS CodeCommit 57
AWS CodePipeline 57
AWS Config 57
AWS Data Exchange 58
AWS Database Migration Service 59
AWS DataSync 59
AWS Directory Service 60
AWS Directory Service pour Microsoft AD 60
Amazon Cloud Directory 60
AWS Elastic Beanstalk 60
AWS Elastic Disaster Recovery 61
AWS Fargate 62

AWS Firewall Manager 62
AWS Global Accelerator 63
AWS Glue 63
AWS Glue DataBrew 63
AWS IoT Core et AWS IoT Device Management 64
AWS IoT Greengrass 64
AWS Lambda 64
AWS Managed Services 65
AWS OpsWorks pour Chef Automate 65
AWS OpsWorks pour Puppet Enterprise 65
AWS OpsWorks Empilez 66
AWS Organizations 66
AWS RoboMaker 67
Métriques du SDK AWS 67
AWS Secrets Manager 68
AWS Security Hub CSPM 68
AWS Server Migration Service 69
AWS Serverless Application Repository 69
Service Catalog 70
AWS Shield 70
AWS Snowball Edge 70
AWS Snowball Edge Bord 71
AWS Step Functions 71
AWS Storage Gateway 72
Passerelle de fichier 72
Passerelle de volume 72
Passerelle de bande 72
AWS Systems Manager 73
AWS Transfer for SFTP 73
AWS WAF — Pare-feu pour applications Web 73
AWS X-Ray 74
Elastic Load Balancing 74
FreeRTOS 75
Utilisation AWS KMS pour le chiffrement de PHI 75
VM Import/Export 75
Audit, sauvegardes et reprise après sinistre 77

Révisions du document 79
Avis 84
..... lxxxv

Architecting for HIPAA Security and Compliance on Amazon Web Services

Date de publication : 28 septembre 2022 (Révisions du document)

Ce paper explique brièvement comment les clients peuvent utiliser Amazon Web Services (AWS) pour exécuter des charges de travail sensibles réglementées par le Health Insurance Portability and Accountability Act (HIPAA) des États-Unis. Nous nous concentrerons sur les règles de confidentialité et de sécurité HIPAA pour protéger les informations de santé protégées (PHI), sur la manière d'utiliser AWS pour chiffrer les données en transit et au repos, et sur la manière dont les fonctionnalités d'AWS peuvent être utilisées pour exécuter des charges de travail contenant des PHI.

Introduction

La Health Insurance Portability and Accountability Act de 1996 (HIPAA) s'applique aux « entités couvertes » et aux « partenaires commerciaux ». La loi HIPAA a été étendue en 2009 par la loi HITECH (Health Information Technology for Economic and Clinical Health).

HIPAA et HITECH établissent un ensemble de normes fédérales destinées à protéger la sécurité et la confidentialité des PHI. HIPAA et HITECH imposent des exigences relatives à l'utilisation et à la divulgation des informations de santé protégées (PHI), des garanties appropriées pour protéger les PHI, les droits individuels et les responsabilités administratives. Pour plus d'informations sur les lois HIPAA et HITECH, rendez-vous sur le site Health Information Privacy Home.

Les entités couvertes et leurs partenaires commerciaux peuvent utiliser les composants informatiques sécurisés, évolutifs et peu coûteux fournis par Amazon Web Services (AWS) pour concevoir des applications conformément aux exigences de conformité HIPAA et HITECH. AWS propose une plate-forme d' commercial-off-the-shelfinfrastructure dotée de certifications et d'audits reconnus par le secteur, tels que ISO 27001, FedRAMP et les rapports de contrôle de l'organisation des services (SOC1, SOC2 et SOC3). Les services et les centres de données AWS comportent plusieurs niveaux de sécurité opérationnelle et physique pour garantir l'intégrité et la sécurité des données des clients. Sans frais minimaux, sans contrat à durée déterminée ni pay-as-you-use tarification, AWS est une solution fiable et efficace pour les applications croissantes du secteur de la santé.

AWS permet aux entités couvertes et à leurs partenaires commerciaux soumis à la loi HIPAA de traiter, de stocker et de transmettre des PHI en toute sécurité. En outre, depuis juillet 2013, AWS propose un addendum Business Associate (BAA) standardisé pour ces clients. Les clients qui exécutent un AWS BAA peuvent utiliser n'importe quel service AWS sur un compte désigné comme compte HIPAA, mais ils ne peuvent traiter, stocker et transmettre des PHI qu'en utilisant les services éligibles à la loi HIPAA définis dans le BAA AWS. Pour une liste complète de ces services, consultez la page de référence des services éligibles à la loi HIPAA.

AWS gère un programme de gestion des risques basé sur des normes afin de garantir que les services éligibles à la loi HIPAA prennent spécifiquement en charge les garanties administratives, techniques et physiques HIPAA. L'utilisation de ces services pour stocker, traiter et transmettre des PHI aide nos clients et AWS à répondre aux exigences de la loi HIPAA applicables au modèle d'exploitation basé sur les utilitaires AWS.

Le BAA d'AWS oblige les clients à chiffrer les PHI stockés ou transmis à l'aide de services conformes à la loi HIPAA conformément aux directives du secrétaire à la Santé et aux Services sociaux (HHS) :

Guidance to Render Unsecure Protected Health Information unusable, illisible ou indéchiffrable pour les personnes non autorisées (« Guidance »). Veuillez consulter ce site car il est susceptible d'être mis à jour et peut être mis à disposition sur un site successeur (ou apparenté) désigné par le HHS.

AWS propose un ensemble complet de fonctionnalités et de services destinés à faciliter la gestion des clés et le chiffrement des PHI et à en simplifier l'audit, notamment le AWS Key Management Service (AWS KMS). Les clients soumis à des exigences de conformité à la loi HIPAA disposent d'une grande flexibilité dans la manière dont ils répondent aux exigences de chiffrement des PHI.

Lorsqu'ils déterminent comment implémenter le chiffrement, les clients peuvent évaluer et tirer parti des fonctionnalités de chiffrement propres aux services conformes à la loi HIPAA. Les clients peuvent également satisfaire aux exigences de cryptage par d'autres moyens conformément aux directives du HHS.

Chiffrement et protection des PHI dans AWS

La règle de sécurité HIPAA inclut des spécifications d'implémentation adressables pour le chiffrement des PHI en transmission (« en transit ») et en stockage (« au repos »). Bien qu'il s'agisse d'une spécification d'implémentation applicable dans la loi HIPAA, AWS demande aux clients de chiffrer les PHI stockés ou transmis à l'aide de services éligibles à la loi HIPAA conformément aux directives du secrétaire à la Santé et aux Services sociaux (HHS) : Guidance to Render Unsecure Protected Health Information unusable, Unreadable, or Indechiffrable to Unauthorized Individuals (« Guidance »). Veuillez consulter ce site car il est susceptible d'être mis à jour et peut être mis à disposition sur un successeur (ou un site connexe) désigné par le HHS.

AWS propose un ensemble complet de fonctionnalités et de services destinés à faciliter la gestion des clés et le chiffrement des PHI et à en simplifier l'audit, notamment le AWS Key Management Service (AWS KMS). Les clients soumis à des exigences de conformité à la loi HIPAA disposent d'une grande flexibilité dans la manière dont ils répondent aux exigences de chiffrement des PHI.

Lorsqu'ils déterminent comment implémenter le chiffrement, les clients peuvent évaluer et tirer parti des fonctionnalités de chiffrement natives des services éligibles à la loi HIPAA, ou ils peuvent satisfaire aux exigences de cryptage par d'autres moyens conformément aux directives du HHS. Les sections suivantes fournissent des informations détaillées sur l'utilisation des fonctionnalités de chiffrement disponibles dans chacun des services éligibles à la loi HIPAA et d'autres modèles de chiffrement des PHI, ainsi que sur la manière dont AWS KMS peut être utilisé pour chiffrer les clés utilisées pour le chiffrement des PHI sur AWS.

Rubriques

- Amazon API Gateway
- Amazon AppFlow
- Amazon AppStream 2.0
- Amazon Athena
- Amazon Aurora
- Amazon Aurora PostgreSQL
- Amazon CloudFront
- Amazon CloudWatch
- CloudWatch Événements Amazon

- Amazon CloudWatch Logs
- Amazon Comprehend
- Amazon Comprehend Medical
- Amazon Connect
- Amazon DocumentDB (compatible avec MongoDB)
- Amazon DynamoDB
- Amazon Elastic Block Store
- Amazon Elastic Compute Cloud
- Amazon Elastic Container Registry
- Amazon Elastic Container Service
- Amazon Elastic File System (Amazon EFS)
- Amazon Elastic Kubernetes Service (Amazon EKS)
- Amazon ElastiCache pour Redis
- Amazon OpenSearch Service
- Amazon EMR
- Amazon EventBridge
- Amazon Forecast
- Amazon FSx
- Amazon GuardDuty
- Amazon HealthLake
- Amazon Inspector
- Service géré Amazon pour Apache Flink
- Amazon Data Firehose
- Amazon Kinesis Streams
- Amazon Kinesis Video Streams
- Amazon Lex
- Amazon Managed Streaming for Apache Kafka (Amazon MSK)
- Amazon MQ
- Amazon Neptune

- AWS Network Firewall
- Amazon Pinpoint
- Amazon Polly
- Amazon Quantum Ledger Database (Amazon QLDB)
- Amazon QuickSight
- Amazon RDS for MariaDB
- Amazon RDS for MySQL
- Amazon RDS for Oracle
- Amazon RDS for PostgreSQL
- Amazon RDS for SQL Server
- Amazon Redshift
- Amazon Rekognition
- Amazon Route 53
- Amazon S3 Glacier
- Amazon S3 Transfer Acceleration
- Amazon SageMaker
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Email Service (Amazon SES)
- Amazon Simple Queue Service (Amazon SQS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon Simple Workflow Service
- Amazon Textract
- Amazon Transcribe
- Amazon Translate
- Amazon Virtual Private Cloud
- Amazon WorkDocs
- Amazon WorkSpaces
- AWS App Mesh
- AWS Service de migration d'applications

- AWS Auto Scaling
- AWS Backup
- AWS Batch
- AWS Certificate Manager
- AWS Cloud Map
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- AWS CodeBuild
- AWS CodeDeploy
- AWS CodeCommit
- AWS CodePipeline
- AWS Config
- AWS Data Exchange
- AWS Database Migration Service
- AWS DataSync
- AWS Directory Service
- AWS Elastic Beanstalk
- AWS Elastic Disaster Recovery
- AWS Fargate
- AWS Firewall Manager
- AWS Global Accelerator
- AWS Glue
- AWS Glue DataBrew
- AWS IoT Core et AWS IoT Device Management
- AWS IoT Greengrass
- AWS Lambda
- AWS Managed Services
- AWS OpsWorks pour Chef Automate

- AWS OpsWorks pour Puppet Enterprise
- AWS OpsWorks Empilez
- AWS Organizations
- AWS RoboMaker
- Métriques du SDK AWS
- AWS Secrets Manager
- AWS Security Hub CSPM
- AWS Server Migration Service
- AWS Serverless Application Repository
- Service Catalog
- AWS Shield
- AWS Snowball Edge
- AWS Snowball Edge Bord
- AWS Step Functions
- AWS Storage Gateway
- AWS Systems Manager
- AWS Transfer for SFTP
- AWS WAF — Pare-feu pour applications Web
- AWS X-Ray
- Elastic Load Balancing
- FreeRTOS
- Utilisation AWS KMS pour le chiffrement de PHI
- VM Import/Export

Amazon API Gateway

Les clients peuvent utiliser Amazon API Gateway pour traiter et transmettre des informations de santé protégées (PHI). Amazon API Gateway utilise automatiquement les points de terminaison HTTPS pour le chiffrement en cours de route, mais les clients peuvent également choisir de chiffrer les charges utiles côté client. API Gateway transmet toutes les données non mises en cache en mémoire et ne les écrit pas sur le disque. Les clients peuvent utiliser AWS Signature version 4 pour

obtenir une autorisation avec API Gateway. Pour plus d'informations, consultez les ressources suivantes :

- FAQ sur Amazon API Gateway : sécurité et autorisation
- Contrôle et gestion de l'accès à une API REST dans API Gateway

Les clients peuvent intégrer n'importe quel service connecté à API Gateway, à condition que, lorsque PHI est impliqué, le service soit configuré conformément aux directives et au BAA. Pour plus d'informations sur l'intégration d'API Gateway aux services principaux, consultez la section Configurer les méthodes d'API REST dans API Gateway.

Les clients peuvent utiliser AWS CloudTrail Amazon CloudWatch pour activer la journalisation conformément à leurs exigences en matière de journalisation. Assurez-vous que tous les PHI envoyés via API Gateway (tels que les en-têtes, les URL et les requêtes/réponses) ne sont capturés que par les services éligibles à la loi HIPAA qui ont été configurés conformément aux directives. Pour plus d'informations sur la journalisation avec API Gateway, consultez Comment activer les CloudWatch journaux pour résoudre les problèmes liés à mon API REST ou à mon API WebSocket API Gateway ?

Amazon AppFlow

Amazon AppFlow est un service d'intégration entièrement géré qui permet aux clients de transférer des données en toute sécurité entre des applications oftware-as-a S-Service (SaaS) telles que Salesforce, Marketo, Slack ServiceNow et des services AWS tels qu'Amazon S3 et Amazon Redshift. AppFlow peut exécuter des flux de données à la fréquence choisie par le client : selon un calendrier, en réponse à un événement professionnel ou à la demande. Les clients peuvent également configurer des fonctionnalités de transformation des données, telles que le filtrage et la validation, afin de générer des ready-to-use données riches dans le cadre du flux lui-même, sans étapes supplémentaires.

Amazon AppFlow peut être utilisé pour traiter et transférer des données contenant des PHI. Le chiffrement des données pendant leur transit entre la source/destination configurée AppFlow et la source configurée est fourni par défaut à l'aide de TLS 1.2 ou version ultérieure. Les données stockées au repos dans S3 sont automatiquement cryptées à l'aide d'une AWS KMS clé (anciennement CMK) spécifiée par le client. Pour les données PHI transférées vers des destinations autres que S3, les clients doivent s'assurer que le stockage au repos pour la destination choisie répond à leurs besoins de sécurité. AppFlow permet de surveiller les applications en s'intégrant AWS

CloudTrail à Amazon pour enregistrer les appels d'API et EventBridge d'émettre des événements d'exécution de flux.

Amazon AppStream 2.0

Amazon AppStream 2.0 est un service de streaming d'applications entièrement géré. Les clients sont propriétaires de leurs données et doivent configurer les applications Windows nécessaires conformément à leurs exigences réglementaires. Les clients peuvent configurer le stockage persistant via Home Folders. Les fichiers et les dossiers sont chiffrés en transit à l'aide des points de terminaison SSL Amazon S3. Les fichiers et les dossiers sont chiffrés au repos à l'aide de clés de chiffrement gérées par Amazon S3. Pour plus d'informations, voir Activer et administrer le stockage persistant pour vos utilisateurs AppStream 2.0. Si les clients choisissent d'utiliser une solution de stockage tierce, il leur incombe de s'assurer que la configuration de cette solution est conforme aux instructions. Toutes les communications d'API publiques avec Amazon AppStream 2.0 sont cryptées à l'aide du protocole TLS. Pour plus d'informations, consultez la documentation Amazon AppStream 2.0.

Amazon AppStream 2.0 est intégré à AWS CloudTrail un service qui enregistre les appels d'API effectués par ou pour le compte d'Amazon AppStream 2.0 dans le compte AWS du client et envoie les fichiers journaux dans le compartiment Amazon S3 spécifié. CloudTrail capture les appels d'API effectués depuis la console Amazon AppStream 2.0 ou depuis l'API Amazon AppStream 2.0. Les clients peuvent également utiliser Amazon CloudWatch pour enregistrer les statistiques d'utilisation des ressources. Pour plus d'informations, consultez Surveillance des ressources Amazon AppStream 2.0 et journalisation des appels d'API AppStream 2.0 avec AWS CloudTrail.

Amazon Athena

Amazon Athena est un service de requêtes interactif qui facilite l'analyse de données directe dans Amazon Simple Storage Service (Amazon S3) via la syntaxe SQL standard. Athena aide les clients à analyser les données non structurées, semi-structurées et structurées stockées dans Amazon S3. Par exemple, des formats de données CSV ou JSON, ou des formats en colonnes, tels qu'Apache Parquet et Apache ORC. Les clients peuvent utiliser Athena pour exécuter des requêtes ad hoc à l'aide du SQL ANSI, sans avoir à agréger ou à charger les données dans Athena.

Amazon Athena peut désormais être utilisé pour traiter des données contenant des PHI. Le chiffrement des données pendant leur transit entre Amazon Athena et S3 est fourni par défaut à l'aide du protocole SSL/TLS. Le chiffrement des PHI au repos sur S3 doit être effectué conformément aux instructions fournies dans la section S3. Le chiffrement des résultats des requêtes depuis et au

sein d'Amazon Athena, y compris les résultats intermédiaires, doit être activé à l'aide du chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3), des clés gérées (SSE-KMS) ou un chiffrement côté client avec des clés AWS KMS gérées (CSE-KMS). AWS KMS Amazon Athena enregistre tous les AWS CloudTrail appels d'API.

Amazon Aurora

Amazon Aurora permet aux clients de chiffrer les clusters de bases de données Aurora et les instantanés au repos à l'aide de clés qu'ils gèrent. AWS KMS Sur une instance de base de données exécutée avec le chiffrement Amazon Aurora, les données stockées au repos dans le stockage sous-jacent sont chiffrées, tout comme les sauvegardes automatisées, les répliques en lecture et les instantanés.

Les directives étant susceptibles d'être mises à jour, les clients doivent continuer à évaluer et à déterminer si le chiffrement Amazon Aurora répond à leurs exigences réglementaires et de conformité. Pour plus d'informations sur le chiffrement au repos à l'aide d'Amazon Aurora, consultez la section Protection des données à l'aide du chiffrement.

Les connexions aux clusters de base de données exécutant Aurora MySQL doivent utiliser le chiffrement de transport, à l'aide du protocole SSL (Secure Socket Layer) ou du protocole TLS (Transport Layer Security). Pour plus d'informations sur l'implémentation de SSL/TLS, consultez la section Utilisation de SSL/TLS avec des clusters de base de données Aurora MySQL.

Amazon Aurora PostgreSQL

Amazon Aurora permet aux clients de chiffrer les clusters de bases de données Aurora et les instantanés au repos à l'aide de clés qu'ils gèrent. AWS KMS Sur une instance de base de données exécutée avec le chiffrement Amazon Aurora, les données stockées au repos dans le stockage sous-jacent sont chiffrées, tout comme les sauvegardes automatisées, les répliques en lecture et les instantanés.

Les directives étant susceptibles d'être mises à jour, les clients doivent continuer à évaluer et à déterminer si le chiffrement Amazon Aurora répond à leurs exigences réglementaires et de conformité. Pour plus d'informations sur le chiffrement au repos à l'aide d'Amazon Aurora, consultez la section Protection des données à l'aide du chiffrement.

Les connexions aux clusters de bases de données exécutant Aurora PostgreSQL doivent utiliser le chiffrement de transport, à l'aide du protocole SSL (Secure Socket Layer) ou du protocole TLS

(Transport Layer Security). Pour plus d'informations sur la mise en œuvre du protocole SSL/TLS, consultez la section Sécurisation des données Aurora PostgreSQL avec SSL.

Amazon CloudFront

Amazon CloudFront est un service de réseau mondial de diffusion de contenu (CDN) qui accélère la diffusion des sites Web des clients, des API, du contenu vidéo ou d'autres ressources Web. Il s'intègre à d'autres produits Amazon Web Services pour offrir aux développeurs et aux entreprises un moyen simple d'accélérer la diffusion de contenu aux utilisateurs finaux, sans engagement d'utilisation minimale. Pour garantir le chiffrement des PHI lors de leur transfert CloudFront, les clients doivent configurer leur système de manière CloudFront à utiliser le protocole HTTPS end-to-end depuis l'origine jusqu'au lecteur.

Cela inclut le trafic entre CloudFront et le spectateur, la CloudFront redistribution à partir d'une origine personnalisée et la CloudFront distribution à partir d'une origine Amazon S3. Les clients doivent également s'assurer que les données sont cryptées à l'origine afin de garantir qu'elles restent cryptées au repos lorsqu'elles sont mises en cache. CloudFront S'ils utilisent Amazon S3 comme origine, les clients peuvent utiliser les fonctionnalités de chiffrement côté serveur de S3. Si les clients distribuent à partir d'une origine personnalisée, ils doivent s'assurer que les données sont cryptées à l'origine.

Lambda@Edge

Lambda @Edge est un service de calcul qui permet d'exécuter des fonctions Lambda sur des sites périphériques AWS. Lambda @Edge peut être utilisé pour personnaliser le contenu diffusé via. CloudFront Lorsqu'ils utilisent Lambda @Edge avec PHI, les clients doivent suivre les instructions d'utilisation de. CloudFront Toutes les connexions entrantes et sortantes de Lambda @Edge doivent être chiffrées à l'aide du protocole HTTPS ou SSL/TLS.

Amazon CloudWatch

Amazon CloudWatch est un service de surveillance des ressources du cloud AWS et des applications que les clients exécutent sur AWS. Les clients peuvent utiliser Amazon CloudWatch pour collecter et suivre les métriques, collecter et surveiller les fichiers journaux et définir des alarmes. Amazon CloudWatch lui-même ne produit, ne stocke ni ne transmet de PHI. Les clients peuvent surveiller les appels CloudWatch d'API avec AWS CloudTrail. Pour plus d'informations, consultez la section Journalisation des appels CloudWatch d'API Amazon avec AWS CloudTrail.

Pour plus de détails sur les exigences de configuration, consultez la section Amazon CloudWatch Logs.

CloudWatch Événements Amazon

Amazon CloudWatch Events fournit un near-real-time flux d'événements système qui décrivent les modifications apportées aux ressources AWS. Les clients doivent s'assurer que les PHI ne sont pas intégrés aux CloudWatch événements, et que toute ressource AWS émettant un CloudWatch événement qui stocke, traite ou transmet des PHI est configurée conformément aux directives.

Les clients peuvent configurer Amazon CloudWatch Events pour s'enregistrer en tant qu'appel d'API AWS CloudTrail. Pour plus d'informations, consultez Création d'une règle d' CloudWatch événements qui se déclenche lors d'un appel d'API AWS à l'aide de AWS CloudTrail.

Amazon CloudWatch Logs

Les clients peuvent utiliser Amazon CloudWatch Logs pour surveiller, stocker et accéder à leurs fichiers journaux à partir d'instances Amazon Elastic Compute Cloud (Amazon EC2) AWS CloudTrail, d'Amazon Route 53 et d'autres sources. Ils peuvent ensuite récupérer les données de journal associées dans CloudWatch Logs. Les données du journal sont cryptées pendant leur transit et pendant qu'elles sont au repos. Par conséquent, il n'est pas nécessaire de rechiffrer les PHI émis par un autre service et transmis à CloudWatch Logs.

Amazon Comprehend

Amazon Comprehend utilise le traitement du langage naturel pour extraire des informations sur le contenu des documents. Amazon Comprehend traite n'importe quel fichier texte au format UTF-8. Il développe des informations en reconnaissant les identités, les phrases clés, le langage, les sentiments et d'autres éléments courants dans un document. Amazon Comprehend peut être utilisé avec des données contenant des PHI. Amazon Comprehend ne conserve ni ne stocke aucune donnée et tous les appels à l'API sont chiffrés avec SSL/TLS. Amazon Comprehend enregistre tous CloudTrail les appels d'API.

Gestion des identités et des accès AWS

Les fonctions d'accès de sécurité telles que l'authentification et l'autorisation sont requises pour accéder à Amazon Comprehend et peuvent être contrôlées avec Gestion des identités et des accès

AWS(IAM), et les informations d'identification peuvent être utilisées pour accéder à l'IAM. Pour plus d'informations, consultez Authentification et contrôle d'accès pour Amazon Comprehend dans le guide de l'utilisateur d'Amazon Comprehend.

Gestion du compte

Par défaut, les utilisateurs IAM ne sont pas autorisés à créer ou à modifier des ressources Amazon Comprehend, ni à effectuer des tâches à l'aide de l'API Amazon Comprehend. Pour permettre aux utilisateurs de créer ou de modifier des ressources et d'effectuer des tâches, les clients sont tenus de tirer parti des politiques IAM qui accordent aux utilisateurs des autorisations pour les ressources spécifiques (telles qu'Amazon Comprehend et les actions d'API) que les utilisateurs doivent utiliser, puis d'associer des politiques aux utilisateurs ou aux groupes qui nécessitent des autorisations spécifiques.

Avec Amazon Comprehend, vous pouvez utiliser Gestion des identités et des accès AWS (IAM) pour créer un utilisateur auquel est attachée une politique afin d'activer les autorisations Amazon Comprehend. Vous pouvez éventuellement choisir de créer des politiques personnalisées à associer à un rôle. Vous pouvez ensuite ajouter des administrateurs au rôle avec la possibilité d'invoquer des API pour l'administration d'Amazon Comprehend conformément aux principes d'accès basé sur les rôles et de moindre privilège définis par l'organisation.

Identité et accès

Avec Amazon Comprehend, vous pouvez demander à l'utilisateur de s'authentifier à AWS l'aide de l'authentification multifactorielle conformément aux exigences organisationnelles en matière d'authentification.

À l'aide de Console de gestion AWS, les administrateurs IAM peuvent créer une politique gérée par le client qui refuse toutes les autorisations, à l'exception de celles requises pour que les utilisateurs puissent gérer leurs propres informations d'identification et leurs appareils MFA. Un modèle de politique JSON est disponible sur la page My Security Credential de la console IAM.

Vous pouvez éventuellement tirer parti des fonctionnalités MFA tierces compatibles avec les partenaires IAM. Pour plus d'informations, consultez IAM Partners.

Administration

Nous recommandons à Amazon Comprehend de sélectionner des politiques basées sur l'identité dans lesquelles les administrateurs de comptes peuvent associer des politiques d'autorisation aux

identités IAM (utilisateurs, groupes et rôles) et ainsi accorder des autorisations pour effectuer des opérations sur les ressources Amazon Comprehend.

Une liste des actions d'API pour Amazon Comprehend se trouve dans le guide de référence des API. Vous devez également envisager d'autoriser l'accès aux politiques IAM prédéfinies, aux politiques IAM des clients et aux actions d'API aux utilisateurs ou aux rôles conformément à leurs exigences organisationnelles basées sur le moindre privilège et les rôles. Pour plus d'informations, consultez la section Utilisation de l'API Amazon Comprehend dans le manuel du développeur.

Authentification externe

Amazon Comprehend est compatible avec la fédération d'identité à l'aide de rôles IAM. Cela permet à vos utilisateurs d'Amazon Comprehend de s'authentifier AWS en assumant un rôle attribué par les administrateurs. Les utilisateurs accédant à AWS l'aide des informations d'identification de leur organisation ou d'un tiers assument un rôle indirectement.

AWS la prise en charge de Kerberos et d'Active Directory offre les avantages de l'authentification unique et de l'authentification centralisée des utilisateurs de bases de données. AWS les utilisateurs peuvent choisir de gérer et de stocker les informations d'identification AWS Directory Service des utilisateurs dans Microsoft Active Directory ou dans l'Active Directory local du client.

Application du flux de données

AWS les clients et les partenaires APN, agissant en tant que contrôleurs ou sous-traitants de données, sont responsables de toutes les données personnelles qu'ils saisissent dans Amazon AWS Cloud Comprehend. Vous êtes responsable du contrôle du flux vers les entrées et sorties de données pour Amazon Comprehend à l'aide des politiques IAM.

Protection des données et gestion des secrets

Le modèle de responsabilité AWS partagée s'applique à la protection des données dans Amazon Comprehend. Comme décrit dans ce modèle, AWS est responsable de la protection de l'infrastructure mondiale qui gère l'ensemble du AWS cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Ce contenu inclut la configuration de la sécurité et les tâches de gestion pour les AWS services que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez les FAQ sur la confidentialité des données.

La section Protection des données dans Amazon Comprehend du guide du développeur Amazon Comprehend fournit des conseils à prendre en compte pour protéger les données, par exemple en

utilisant le protocole TLS pour la transmission et en évitant de placer des informations sensibles dans des balises ou des champs de forme libre.

Chiffrement de data-at-rest

Amazon Comprehend travaille avec AWS Key Management Service(AWS KMS) pour fournir un chiffrement amélioré de vos données. Amazon Simple Storage Service (Amazon S3) vous permet déjà de chiffrer vos documents d'entrée lors de la création d'une analyse de texte, d'une modélisation de sujets ou d'une tâche Amazon Comprehend personnalisée. L'intégration avec vous AWS KMS permet de chiffrer les données du volume de stockage pour les tâches start* et create*, et de chiffrer les résultats de sortie des tâches start* à l'aide de votre propre clé. AWS KMS

Il est recommandé aux utilisateurs d'Amazon Comprehend de chiffrer les compartiments Amazon S3 utilisés pour saisir des documents à l'aide des solutions de chiffrement S3 disponibles conformément à leurs politiques organisationnelles.

Le chiffre Console de gestion AWS les modèles personnalisés Amazon Comprehend avec sa AWS KMS propre clé. Dans ce cas AWS CLI, Amazon Comprehend peut chiffrer des modèles personnalisés à l'aide de sa propre AWS KMS clé ou d'une clé gérée par le client (CMK) fournie.

Si vous sélectionnez le chiffrement lors de l'utilisation du Console de gestion AWS, vous pouvez choisir l'une des méthodes facultatives suivantes ou les deux :

- Chiffrement des volumes : garantit que les données d'un volume EBS utilisé par Comprehend sont cryptées pendant l'entraînement/l'inférence (les données sont vidées après l'entraînement/l'inférence, de sorte que cette clé n'est pertinente que pendant le travail en cours).
- Chiffrement des résultats de sortie : pour chiffrer les résultats stockés par Comprehend dans le compartiment du client à l'aide d'une clé fournie AWS KMS par le client.

Pour plus d'informations sur les types de chiffrement tels que le chiffrement de volume, consultez la section AWS KMS Chiffrement dans Amazon Comprehend.

Informations personnelles identifiables

Vous pouvez utiliser la console Amazon Comprehend ou les API pour détecter les informations personnelles identifiables (PII) dans les documents texte en anglais. Pour plus d'informations sur la détection et l'étiquetage des entités PII et sur l'exécution de différentes tâches d'analyse d'informations personnelles, consultez la section Informations personnelles du manuel Amazon Comprehend Developer Guide.

Suppression de données

Si vous êtes un client d'Amazon Comprehend qui utilise Amazon S3 et que vous choisissez de gérer vos propres AWS KMS clés, vous devez envisager de révoquer AWS KMS les clés et de définir la justification procédurale pour ce faire conformément aux exigences organisationnelles. La révocation de la AWS KMS clé pour Amazon S3 rend toutes les données inutilisables/illisibles.

Segmentation et renforcement du réseau

En tant que service géré, Amazon Comprehend adhère aux AWS meilleures pratiques en matière de sécurité, d'identité et de conformité.

Pour connaître les mesures de sécurité réseau recommandées, consultez la section Sécurité de l'infrastructure dans Amazon Comprehend dans le manuel Amazon Comprehend Developers Guide.

Protégez les emplois à l'aide d'un Amazon Virtual Private Cloud (Amazon VPC)

Amazon Comprehend utilise diverses mesures de sécurité pour garantir la sécurité de vos données grâce à nos conteneurs de tâches dans lesquels elles sont stockées pendant leur utilisation par Amazon Comprehend. Cependant, les conteneurs de tâches accèdent à des AWS ressources, telles que les compartiments Amazon S3 dans lesquels vous stockez des données et des artefacts de modèles, via Internet.

Pour contrôler l'accès à vos données, nous vous recommandons de créer un cloud privé virtuel (VPC) et de le configurer de manière à ce que les données et les conteneurs ne soient pas accessibles via Internet. Pour plus d’informations sur la création et la configuration d’un VPC, consultez Démarrer avec Amazon VPC dans le Guide de l’utilisateur Amazon VPC. L'utilisation d'un VPC permet de protéger vos données, car vous pouvez configurer votre VPC de manière à ce qu'il ne soit pas connecté à Internet. L'utilisation d'un VPC vous permet également de surveiller l'ensemble du trafic réseau entrant et sortant de nos conteneurs de tâches à l'aide des journaux de flux VPC. Pour plus d’informations, consultez la rubrique Journaux de flux VPC dans le Guide de l’utilisateur Amazon VPC.

Vous spécifiez la configuration de votre VPC lorsque vous créez une tâche, en spécifiant les sous-réseaux et les groupes de sécurité. Lorsque vous spécifiez les sous-réseaux et les groupes de sécurité, Amazon Comprehend crée des interfaces réseau élastiques (ENI) associées à vos groupes de sécurité dans l'un des sous-réseaux. Les ENI permettent à nos conteneurs de tâches de se connecter aux ressources de votre VPC. Pour plus d’informations sur les interfaces réseau Elastic, consultez Interfaces réseau Elastic dans le Guide de l’utilisateur Amazon VPC.

> **Note**
>
> Pour les tâches, vous pouvez uniquement configurer des sous-réseaux avec un VPC de location par défaut dans lequel votre instance s'exécute sur du matériel partagé. Pour plus d'informations sur l'attribut de location pour les VPC, consultez la section Instances dédiées du guide de l'utilisateur Amazon EC2 pour les instances Linux.

Vous pouvez établir une connexion privée entre votre VPC et Amazon Comprehend en créant un point de terminaison VPC d'interface. Pour plus d'informations, consultez Amazon Comprehend and Interface VPC Endpoints ().AWS PrivateLink

Renforcement de l'hôte et de l'image

Sur la base du modèle de responsabilité AWS partagée, le renforcement des hôtes et des images de l' AWS environnement pour Amazon Comprehend est géré AWS en tant que service fourni.

Multilocataire

Pour renforcer la sécurité de votre recommandation, nous vous recommandons de mettre en œuvre les recommandations de sécurité mutuelles suivantes :

- Utilisez uniquement une adresse e-mail vérifiée pour autoriser l'accès utilisateur à un locataire sur la base d'une correspondance de domaine. Ne faites pas confiance aux adresses e-mail et aux numéros de téléphone à moins que votre application ne les ait vérifiés ou que le fournisseur d'identité externe n'ait fourni une preuve de vérification. Pour plus d'informations sur la définition de ces autorisations, consultez Attribuer des autorisations et des périmètres.
- Utilisez des attributs inaltérables ou réversibles pour les attributs de profil utilisateur qui identifient les locataires. Les administrateurs doivent être en mesure de modifier ces attributs. De plus, accordez aux clients d'application un accès en lecture seule à ces attributs.
- Utilisez un mappage 1:1 entre le fournisseur d'identité externe et le client d'application pour empêcher tout accès non autorisé entre locataires. Un utilisateur authentifié par un fournisseur d'identité externe et doté d'un cookie de session Amazon Cognito valide peut accéder aux applications d'autres locataires qui font confiance au même fournisseur d'identité.
- Quand vous implémentez la logique d'autorisation et de correspondance de locataire dans votre application, limitez les utilisateurs afin qu'ils ne puissent pas modifier les critères utilisés pour autoriser l'accès des utilisateurs aux locataires. De plus, si un fournisseur d'identité externe est

utilisé pour la fédération, limitez les administrateurs du fournisseur d'identité du locataire afin qu'ils ne puissent pas modifier l'accès utilisateur.

Prévention du problème de l’adjoint confus entre services

Le problème des adjoints confus est un problème de sécurité multilocataire dans lequel une entité qui n'est pas autorisée à effectuer une action peut contraindre une entité plus privilégiée à effectuer l'action. En AWS, l'usurpation d'identité interservices peut entraîner la confusion des adjoints. L’usurpation d’identité entre services peut se produire lorsqu’un service (le service appelant) appelle un autre service (le service appelé). Le service appelant peut être manipulé et ses autorisations utilisées pour agir sur les ressources d’un autre client auxquelles on ne serait pas autorisé d’accéder autrement. Pour éviter cela, AWS fournit des outils qui peuvent vous aider à protéger vos données pour tous les services dont les responsables ont obtenu l'accès aux ressources de votre compte. Pour plus d'informations concernant les mesures de protection à prendre en compte pour résoudre ce problème de sécurité, consultez Cross-service Confused Deputy Prevention dans le manuel Amazon Comprehend Developer Guide.

Amazon Comprehend Medical

Pour obtenir des conseils, consultez la Amazon Comprehend section précédente.

Amazon Connect

Amazon Connect est un service de centre d'appels en libre-service basé sur le cloud qui permet un engagement client dynamique, personnel et naturel à n'importe quelle échelle. Les clients ne doivent inclure aucun PHI dans les champs associés à la gestion des utilisateurs, des profils de sécurité et des flux de contacts au sein d'Amazon Connect.

Amazon Connect Customer Profiles, une fonctionnalité d'Amazon Connect, fournit aux agents des centres de contact une vue plus unifiée du profil d'un client avec les informations les plus récentes, afin de fournir un service client plus personnalisé. Les profils clients sont conçus pour rassembler automatiquement les informations clients provenant de plusieurs applications dans un profil client unifié, en fournissant le profil directement à l'agent dès le début de l'appel d'assistance ou de l'interaction. Les clients doivent s'abstenir de nommer des domaines ou des clés d'objet avec des données PHI. Le contenu des domaines et des objets est crypté et protégé, mais pas les identifiants clés.

Amazon DocumentDB (compatible avec MongoDB)

Amazon DocumentDB (compatible avec MongoDB) (Amazon DocumentDB) propose un chiffrement au repos lors de la création de clusters via AWS KMS, ce qui permet aux clients de chiffrer des bases de données à l'aide d'AWS ou de clés gérées par le client. Sur une instance de base de données exécutée avec le chiffrement activé, les données stockées au repos sont chiffrées conformément aux directives en vigueur au moment de la publication de ce livre blanc, tout comme les sauvegardes automatisées, les répliques en lecture et les instantanés. Le guide étant susceptible d'être mis à jour, les clients doivent continuer à évaluer et à déterminer si le chiffrement Amazon DocumentDB répond à leurs exigences réglementaires et de conformité. Pour plus d'informations sur le chiffrement au repos à l'aide d'Amazon DocumentDB, consultez la section Chiffrement des données Amazon DocumentDB au repos.

Les connexions à Amazon DocumentDB contenant des PHI doivent utiliser des points de terminaison qui acceptent le transport crypté (HTTPS). Par défaut, un cluster Amazon DocumentDB nouvellement créé accepte uniquement les connexions sécurisées utilisant le protocole TLS (Transport Layer Security). Pour plus d'informations, consultez la section Chiffrement des données en transit. Amazon DocumentDB enregistre tous AWS CloudTrail les appels d'API. Pour plus d'informations, consultez la section Journalisation et surveillance dans Amazon DocumentDB.

Pour certaines fonctionnalités de gestion, Amazon DocumentDB utilise une technologie opérationnelle partagée avec Amazon RDS. Les appels de la console Amazon DocumentDB, de l'interface de ligne de commande AWS et de l'API sont enregistrés en tant qu'appels effectués vers l'API Amazon RDS.

Amazon DynamoDB

Les connexions à Amazon DynamoDB contenant des PHI doivent utiliser des points de terminaison qui acceptent le transport crypté (HTTPS). Pour obtenir la liste des points de terminaison régionaux, consultez la section Points de terminaison des services AWS.

Amazon DynamoDB propose le chiffrement DynamoDB, qui permet aux clients de chiffrer des bases de données à l'aide de clés gérées par les clients. AWS KMS Sur une instance de base de données exécutée avec le chiffrement Amazon DynamoDB, les données stockées au repos dans le stockage sous-jacent sont chiffrées conformément aux directives en vigueur au moment de la publication de ce livre blanc, tout comme les sauvegardes automatisées, les répliques de lecture et les instantanés.

Le guide étant susceptible d'être mis à jour, les clients doivent continuer à évaluer et à déterminer si le chiffrement Amazon DynamoDB répond à leurs exigences réglementaires et de conformité. Pour plus d'informations sur le chiffrement au repos à l'aide d'Amazon DynamoDB, consultez DynamoDB Encryption at Rest.

Amazon Elastic Block Store

Le chiffrement au repos d'Amazon EBS est conforme aux directives en vigueur au moment de la publication de ce livre blanc. Le guide étant susceptible d'être mis à jour, les clients doivent continuer à évaluer et à déterminer si le chiffrement Amazon EBS répond à leurs exigences réglementaires et de conformité. Avec le chiffrement Amazon EBS, une clé de chiffrement de volume unique est générée pour chaque volume EBS. Les clients ont la possibilité de choisir la AWS Key Management Service clé KMS à utiliser pour chiffrer chaque clé de volume. Pour en savoir plus, consultez la page Chiffrement Amazon EBS.

Amazon Elastic Compute Cloud

Amazon EC2 est un service de calcul évolutif et configurable par l'utilisateur qui prend en charge plusieurs méthodes de chiffrement des données au repos. Par exemple, les clients peuvent choisir de chiffrer les PHI au niveau de l'application ou du champ lorsqu'ils sont traités au sein d'une application ou d'une plate-forme de base de données hébergée dans une instance Amazon EC2. Les approches vont du chiffrement des données à l'aide de bibliothèques standard dans un framework applicatif tel que Java ou .NET, à l'exploitation des fonctionnalités de chiffrement transparent des données de Microsoft SQL ou Oracle, ou à l'intégration d'autres solutions tierces et basées sur le logiciel en tant que service (SaaS) dans leurs applications.

Les clients peuvent choisir d'intégrer leurs applications exécutées dans Amazon EC2 avec des AWS KMS SDK, ce qui simplifie le processus de gestion et de stockage des clés. Les clients peuvent également implémenter le chiffrement des données au repos à l'aide du chiffrement au niveau des fichiers ou du disque complet (FDE) à l'aide de logiciels tiers fournis par des AWS Marketplace partenaires ou d'outils de chiffrement de systèmes de fichiers natifs (tels que dm-crypt, LUKS, etc.).

Le trafic réseau contenant des PHI doit chiffrer les données en transit. Pour le trafic entre des sources externes (telles qu'Internet ou un environnement informatique traditionnel) et Amazon EC2, les clients doivent utiliser des mécanismes de chiffrement de transport standard ouverts tels que le protocole TLS (Transport Layer Security) ou les réseaux privés virtuels (VPN) IPSec, conformément au guide. En interne à un Amazon Virtual Private Cloud (VPC) pour les données transitant entre

les instances Amazon EC2, le trafic réseau contenant des PHI doit également être chiffré ; la plupart des applications prennent en charge le protocole TLS ou d'autres protocoles fournissant un chiffrement en transit qui peut être configuré conformément aux directives. Pour les applications et les protocoles qui ne prennent pas en charge le chiffrement, les sessions transmettant des PHI peuvent être envoyées via des tunnels chiffrés utilisant IPsec ou des implémentations similaires entre les instances.

Amazon Elastic Container Registry

Amazon Elastic Container Registry (Amazon ECR) est intégré à Amazon Elastic Container Service (Amazon ECS) et permet aux clients de stocker, exécuter et gérer facilement des images de conteneurs pour les applications exécutées sur Amazon ECS. Une fois que les clients ont spécifié le référentiel Amazon ECR dans leur définition de tâche, Amazon ECS récupère les images appropriées pour leurs applications.

Aucune étape particulière n'est requise pour utiliser Amazon ECR avec des images de conteneur contenant des PHI. Les images de conteneur sont chiffrées pendant le transport et stockées cryptées lorsqu'elles sont au repos à l'aide du chiffrement côté serveur Amazon S3 (SSE-S3).

Amazon Elastic Container Service

Amazon Elastic Container Service (Amazon ECS) est un service de gestion de conteneurs hautement évolutif et performant qui prend en charge les conteneurs Docker et permet aux clients d'exécuter facilement des applications sur un cluster géré d'instances Amazon EC2. Amazon ECS évite aux clients d'installer, d'exploiter et de faire évoluer leur propre infrastructure de gestion de clusters.

À l'aide de simples appels d'API, les clients peuvent lancer et arrêter des applications compatibles Docker, demander l'état complet de leur cluster et accéder à de nombreuses fonctionnalités familières telles que les groupes de sécurité, Elastic Load Balancing, les volumes EBS et les rôles IAM. Les clients peuvent utiliser Amazon ECS pour planifier le placement des conteneurs dans leur cluster en fonction de leurs besoins en ressources et de leurs exigences de disponibilité.

L'utilisation d'ECS avec des charges de travail traitant des PHI ne nécessite aucune configuration supplémentaire. ECS agit comme un service d'orchestration qui coordonne le lancement de conteneurs (dont les images sont stockées dans S3) sur EC2, et il ne fonctionne pas avec ou sur les données de la charge de travail orchestrée. Conformément aux réglementations HIPAA et au AWS Business Associate Addendum, les PHI doivent être chiffrés en transit et au repos lorsqu'ils sont

accessibles par des conteneurs lancés avec ECS. Différents mécanismes de chiffrement au repos sont disponibles avec chaque option de AWS stockage (par exemple, S3, EBS et KMS). Garantir le chiffrement complet des PHI envoyés entre les conteneurs peut également amener les clients à déployer un réseau superposé (tel que VNS3, Weave Net ou similaire), afin de fournir une couche de chiffrement redondante. Néanmoins, la journalisation complète doit également être activée (par exemple, via CloudTrail), et tous les journaux des instances de conteneur doivent être dirigés vers CloudWatch.

L'utilisation de Firelens et AWS de Fluent Bit avec des charges de travail traitant des PHI ne nécessite aucune configuration supplémentaire, sauf si les journaux contiennent des PHI. Si les journaux contiennent des données PHI, ils ne doivent pas être envoyés dans des fichiers journaux, sauf si le chiffrement du disque est activé. Configurez plutôt votre application pour qu'elle émette des journaux en sortie standard ou en erreur, qui seront automatiquement collectés par. FireLens De même, n'activez pas la mise en mémoire tampon des fichiers pour Fluent Bit, sauf si le chiffrement du disque est également activé. Enfin, la destination des journaux doit être compatible encryption-in-transit ; tous les plug-ins de sortie de AWS service d'AWS pour Fluent Bit utiliseront toujours le chiffrement TLS pour exporter les journaux.

Amazon Elastic File System (Amazon EFS)

Amazon Elastic File System (Amazon EFS) fournit un stockage de fichiers simple, évolutif et élastique à utiliser avec les services AWS cloud et les ressources sur site. Il est facile à utiliser et offre une interface simple qui permet aux clients de créer et de configurer des systèmes de fichiers rapidement et facilement. Amazon EFS est conçu pour évoluer de manière élastique à la demande sans perturber les applications, en augmentant et en diminuant automatiquement au fur et à mesure que les clients ajoutent et suppriment des fichiers.

Pour satisfaire à l'exigence selon laquelle les PHI doivent être chiffrés au repos, deux chemins sont disponibles sur EFS. L'EFS prend en charge le chiffrement au repos lorsqu'un nouveau système de fichiers est créé. Lors de la création, l'option « Activer le chiffrement des données au repos » doit être sélectionnée. La sélection de cette option garantit que toutes les données placées sur le système de fichiers EFS seront cryptées à l'aide du chiffrement AES-256 et AWS KMS de clés gérées. Les clients peuvent également choisir de chiffrer les données avant qu'elles ne soient placées sur EFS, mais ils sont ensuite responsables de la gestion du processus de chiffrement et de la gestion des clés.

PHI ne doit pas être utilisé en totalité ou en partie comme nom de fichier ou de dossier. Le chiffrement des PHI en transit pour Amazon EFS est assuré par le protocole TLS (Transport Layer Security) entre le service EFS et l'instance qui monte le système de fichiers. EFS propose un

assistant de montage pour faciliter la connexion à un système de fichiers à l'aide du protocole TLS. Par défaut, le protocole TLS n'est pas utilisé et doit être activé lors du montage du système de fichiers à l'aide de l'assistant de montage EFS. Assurez-vous que la commande mount contient l'option « -o tls » pour activer le chiffrement TLS. Les clients qui choisissent de ne pas utiliser l'assistant de montage EFS peuvent également suivre les instructions de la documentation EFS pour configurer leurs clients NFS afin qu'ils se connectent via un tunnel TLS.

Amazon Elastic Kubernetes Service (Amazon EKS)

Amazon Elastic Kubernetes Service (Amazon EKS) est un service géré qui permet aux clients d'exécuter facilement Kubernetes sur AWS sans avoir à configurer ou à gérer leur propre plan de contrôle Kubernetes. Kubernetes est un système open source destiné à l'automatisation du déploiement, la mise à l'échelle et la gestion d'applications conteneurisées. Pour plus d'informations sur la sécurité et la conformité, consultez le livre blanc Architecting for HIPAA Security and Compliance on Amazon EKS.

Amazon ElastiCache pour Redis

Amazon ElastiCache pour Redis est un service de structure de données en mémoire compatible avec Redis qui peut être utilisé comme magasin de données ou cache. Afin de stocker des PHI, les clients doivent s'assurer qu'ils utilisent la dernière version du moteur Redis conforme à la norme HIPAA et ElastiCache les types de nœuds de génération actuelle. Amazon ElastiCache pour Redis prend en charge le stockage des PHI pour les types de nœuds et les versions du moteur Redis suivants :

- Types de nœuds : génération actuelle uniquement (par exemple, au moment de la publication de ce livre blanc, M4, M5, R4, R5, T2, T3)
- ElastiCache pour les versions du moteur Redis : 3.2.6 et 4.0.10 et suivantes

Pour plus d'informations sur le choix des nœuds de génération actuelle, consultez ElastiCache les tarifs Amazon. Pour plus d'informations sur le choix d'un moteur ElastiCache pour Redis, consultez Qu'est-ce qu'Amazon ElastiCache pour Redis ?

Les clients doivent également s'assurer que le cluster et les nœuds du cluster sont configurés pour chiffrer les données au repos, activer le chiffrement du transport et activer l'authentification des commandes Redis. En outre, les clients doivent également s'assurer que leurs clusters Redis sont mis à jour avec les dernières mises à jour du service de type « Sécurité » au plus tard à la « Date

limite d'application recommandée » (date à laquelle il est recommandé d'appliquer la mise à jour) à tout moment. Consultez les sections ci-dessous pour en savoir plus.

Rubriques

- Chiffrement au repos
- Chiffrement de transport
- Authentification
- Appliquer les mises à jour ElastiCache de service

Chiffrement au repos

Amazon ElastiCache for Redis fournit un chiffrement des données pour son cluster afin de protéger les données au repos. Lorsque les clients activent le chiffrement au repos pour un cluster au moment de sa création, Amazon ElastiCache for Redis chiffre les données sur disque et automatise les sauvegardes Redis. Les données client sur disque sont chiffrées à l'aide de clés symétriques AES (Advanced Encryption Standard) -512 accélérées par le matériel. Les sauvegardes Redis sont chiffrées via des clés de chiffrement gérées par Amazon S3 (SSE-S3). Un compartiment S3 sur lequel le chiffrement côté serveur est activé cryptera les données à l'aide de clés symétriques AES (Advanced Encryption Standard) accélérées par le matériel, à 256 clés symétriques avant de les enregistrer dans le compartiment.

Pour plus de détails sur les clés de chiffrement gérées par Amazon S3 (SSE-S3), consultez Protection des données à l'aide du chiffrement côté serveur avec les clés de chiffrement gérées par Amazon S3 (SSE-S3). Sur un cluster ElastiCache Redis (à un ou plusieurs nœuds) fonctionnant avec chiffrement, les données stockées au repos sont cryptées conformément aux directives en vigueur au moment de la publication de ce livre blanc. Cela inclut les données sur disque et les sauvegardes automatisées dans le compartiment S3. Le guide étant susceptible d'être mis à jour, les clients doivent continuer à évaluer et à déterminer si le chiffrement Amazon ElastiCache pour Redis répond à leurs exigences réglementaires et de conformité. Pour plus d'informations sur le chiffrement au repos à l'aide d'Amazon ElastiCache pour Redis, consultez Qu'est-ce qu'Amazon ElastiCache pour Redis ?

Chiffrement de transport

Amazon ElastiCache pour Redis utilise le protocole TLS pour chiffrer les données en transit. Les connexions vers ElastiCache Redis contenant des PHI doivent utiliser le cryptage du transport et

évaluer la cohérence de la configuration avec les directives. Pour plus d'informations, consultez CreateReplicationGroup. Pour plus d'informations sur l'activation du chiffrement des transports, consultez ElastiCache Redis In-Transit Encryption (TLS).

Authentification

Les clusters Amazon ElastiCache for Redis (à un ou plusieurs nœuds) contenant des PHI doivent fournir un jeton Redis AUTH pour permettre l'authentification des commandes Redis. Redis AUTH est disponible lorsque le chiffrement au repos et le chiffrement en transit sont activés. Les clients doivent fournir un jeton fort pour Redis AUTH avec les contraintes suivantes :

- Doit contenir uniquement des caractères ASCII imprimables
- Doit comporter au moins 16 caractères et pas plus de 128 caractères
- Ne peut contenir aucun des caractères suivants : '/', "" ou « @ »

Ce jeton doit être défini dans le paramètre de demande au moment de la création du groupe de réplication Redis (à un ou plusieurs nœuds) et peut être mis à jour ultérieurement avec une nouvelle valeur. AWS chiffre ce jeton à l'aide de AWS Key Management Service (AWS KMS). Pour plus d'informations sur Redis AUTH, consultez ElastiCache Redis In-Transit Encryption (TLS).

Appliquer les mises à jour ElastiCache de service

Les clusters Amazon ElastiCache pour Redis (à un ou plusieurs nœuds) contenant des PHI doivent être mis à jour avec les dernières mises à jour du service de type « Sécurité » au plus tard à la « Date limite de candidature recommandée ». ElastiCache propose cette fonctionnalité en libre-service que les clients peuvent utiliser pour appliquer les mises à jour à tout moment, à la demande et en temps réel. Chaque mise à jour de service est assortie d'une « gravité » et d'une « date limite d'application recommandée » et n'est disponible que pour les groupes de réplication Redis applicables.

Le champ « SLA atteint » dans la fonction de mise à jour du service indiquera si la mise à jour a été appliquée à la date limite d'application recommandée ou avant. Si les clients choisissent de ne pas appliquer les mises à jour aux groupes de réplication Redis applicables avant la date limite d'application recommandée, ils ne ElastiCache prendront aucune mesure pour les appliquer. Les clients peuvent utiliser le tableau de bord de l'historique des mises à jour du service pour examiner l'application des mises à jour apportées à leurs groupes de réplication Redis au fil du temps. Pour plus d'informations sur l'utilisation de cette fonctionnalité, consultez la section Mises à jour en libre-service sur Amazon ElastiCache.

Amazon OpenSearch Service

Amazon OpenSearch Service permet aux clients d'exécuter un cluster Elasticsearch OSS géré OpenSearch ou hérité dans un Amazon Virtual Private Cloud (Amazon VPC) dédié. Lors de l'utilisation OpenSearch du Service avec PHI, les clients doivent utiliser OpenSearch Elasticsearch 6.0 ou version ultérieure. Les clients doivent s'assurer que les PHI sont chiffrés au repos et en transit au sein d'Amazon OpenSearch Service. Les clients peuvent utiliser le chiffrement par AWS KMS clé pour chiffrer les données au repos dans leurs domaines de OpenSearch service, qui n'est disponible que pour OpenSearch Elasticsearch 5.1 ou version ultérieure. Pour plus d'informations sur le chiffrement des données au repos, consultez la section Chiffrement des données au repos pour Amazon OpenSearch Service.

Chaque domaine OpenSearch de service s'exécute dans son propre VPC. Les clients doivent activer node-to-node le chiffrement, qui est disponible dans toutes les OpenSearch versions, ainsi que dans Elasticsearch 6.0 ou version ultérieure. Si les clients envoient des données au OpenSearch Service via HTTPS, le node-to-node chiffrement permet de garantir que leurs données restent cryptées lorsqu'elles OpenSearch sont distribuées (et redistribuées) dans l'ensemble du cluster. Si les données arrivent non chiffrées via HTTP, le OpenSearch service chiffre les données une fois qu'elles ont atteint le cluster. Par conséquent, tout PHI qui entre dans un cluster Amazon OpenSearch Service doit être envoyé via HTTPS. Pour plus d'informations, consultez la section ode-to-node Chiffrement N pour Amazon OpenSearch Service.

Les journaux de l'API de configuration du OpenSearch service peuvent être capturés AWS CloudTrail. Pour plus d'informations, consultez la section Surveillance des appels d'API Amazon OpenSearch Service avec AWS CloudTrail.

Amazon EMR

Amazon EMR déploie et gère un cluster d'instances Amazon EC2 sur le compte d'un client. Pour plus d'informations sur le chiffrement avec Amazon EMR, consultez la section Options de chiffrement.

Amazon EventBridge

Amazon EventBridge (anciennement Amazon CloudWatch Events) est un bus d'événements sans serveur qui vous permet de créer des applications évolutives pilotées par des événements. EventBridge fournit un flux de données en temps réel provenant de sources d'événements, telles que Zendesk, Datadog ou Pagerduty, et achemine ces données vers des cibles telles que. AWS Lambda

Par défaut, EventBridge chiffre les données à l'aide de la norme de chiffrement avancée 256 bits (AES-256) sous une clé CMK appartenant à AWS, ce qui permet de protéger les données des clients contre tout accès non autorisé. Les clients doivent s'assurer que toute ressource AWS émettant un événement stockant, traitant ou transmettant des PHI est configurée conformément aux meilleures pratiques.

Amazon EventBridge est intégré à la CloudTrail console AWS CloudTrail et les clients peuvent consulter les événements les plus récents dans l'historique des événements. Pour plus d'informations, consultez la section EventBridge Informations dans CloudTrail.

Amazon Forecast

Amazon Forecast est un service entièrement géré qui utilise le machine learning pour fournir des prévisions très précises. Basé sur la même technologie de prévision basée sur l'apprentissage automatique utilisée par Amazon.com. Chaque interaction des clients avec Amazon Forecast est protégée par un chiffrement. Tout le contenu traité par Amazon Forecast est chiffré à l'aide des clés client via Amazon Key Management Service, et chiffré au repos dans la région AWS où les clients utilisent le service.

Amazon Forecast est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un service AWS dans Amazon Forecast. CloudTrail capture tous les appels d'API pour Amazon Forecast sous forme d'événements. Les appels capturés incluent des appels provenant de la console Amazon Forecast et des appels de code vers les opérations de l'API Amazon Forecast. Si les clients créent un suivi, ils peuvent activer la diffusion continue des CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour Amazon Forecast. Pour plus d'informations, consultez Logging Forecast API Calls with AWS CloudTrail.

Par défaut, les fichiers journaux fournis par CloudTrail leur compartiment sont chiffrés par chiffrement côté serveur Amazon avec des clés de chiffrement gérées par Amazon S3 (SSE-S3). Pour fournir une couche de sécurité directement gérable, les clients peuvent plutôt utiliser le chiffrement côté serveur avec des clés AWS KMS gérées (SSE-KMS) pour leurs fichiers journaux. CloudTrail L'activation du chiffrement côté serveur chiffre les fichiers journaux, mais pas les fichiers de valeur de hachage avec SSE-KMS. Les fichiers de valeur de hachage sont chiffrés avec des Amazon S3-managed encryption keys (SSE-S3) (clés de chiffrement gérées par Amazon S3 (SSE-S3)).

AWS Forecast importe et exporte des données vers/depuis des compartiments S3. Lors de l'importation et de l'exportation de données depuis Amazon S3, les clients doivent s'assurer que les compartiments S3 sont configurés conformément aux instructions. Pour plus d'informations, consultez Mise en route avec .

Amazon FSx

Amazon FSx est un service entièrement géré fournissant des systèmes de fichiers riches en fonctionnalités et très performants. Amazon FSx for Windows File Server fournit un stockage de fichiers hautement fiable et évolutif et est accessible via le protocole SMB (Server Message Block). Amazon FSx for Lustre fournit un stockage haute performance pour les charges de travail informatiques et est alimenté par Lustre, le système de fichiers hautes performances le plus populaire au monde.

Amazon FSx prend en charge deux formes de chiffrement pour les systèmes de fichiers : le chiffrement des données en transit et le chiffrement au repos. Amazon FSx for Windows File Server prend également en charge la journalisation de tous les appels AWS CloudTrail d'API à l'aide de.

Le chiffrement des données en transit est pris en charge par Amazon FSx for Windows File Server sur les instances de calcul prenant en charge le protocole SMB 3.0 ou version ultérieure, et par Amazon FSx for Lustre sur les instances Amazon EC2 qui prennent en charge le chiffrement en transit. Les clients peuvent également chiffrer les données avant de les stocker sur Amazon FSx, mais ils sont ensuite responsables du processus de chiffrement et de la gestion des clés.

Le chiffrement des données au repos est automatiquement activé lors de la création d'un système de fichiers Amazon FSx, à l'aide de l'algorithme de chiffrement AES-256 et de clés gérées. AWS KMS Les données et les métadonnées sont automatiquement cryptées avant d'être écrites dans le système de fichiers, et automatiquement déchiffrées avant d'être présentées à l'application. PHI ne doit être utilisé dans aucun nom de fichier ou de dossier.

Amazon GuardDuty

Amazon GuardDuty est un service géré de détection des menaces qui surveille en permanence les comportements malveillants ou non autorisés afin d'aider les clients à protéger leurs comptes et leurs charges de travail AWS. Il surveille les activités telles que les appels d'API inhabituels ou les déploiements potentiellement non autorisés indiquant une possible compromission du compte. Amazon détecte GuardDuty également les instances potentiellement compromises ou les opérations de reconnaissance effectuées par des attaquants.

Amazon surveille et analyse GuardDuty en permanence les sources de données suivantes : journaux de flux VPC, journaux d' AWS CloudTrail événements et journaux DNS. Il utilise des flux de renseignements sur les menaces, tels que des listes d'adresses IP et de domaines malveillants, et

l'apprentissage automatique pour identifier les activités inattendues, potentiellement non autorisées et malveillantes au sein d'un environnement AWS. Amazon ne GuardDuty devrait donc pas rencontrer de PHI, car ces données ne doivent être stockées dans aucune des sources de données AWS répertoriées ci-dessus.

Amazon HealthLake

Amazon HealthLake permet aux clients des secteurs de la santé et des sciences de la vie de stocker, transformer, interroger et analyser des données de santé à l'échelle du pétaoctet. Les clients peuvent utiliser Amazon HealthLake pour transmettre, traiter et stocker des PHI. Amazon HealthLake chiffre les données inactives dans les magasins de données du client par défaut. Toutes les données et métadonnées du service sont chiffrées à l'aide d'une clé KMS appartenant au service. Conformément aux spécifications de Fast Healthcare Interoperability Resources (FHIR), si un client supprime une ressource FHIR, elle sera uniquement masquée et sera conservée par le service à des fins de gestion des versions. Lorsque les clients utilisent l'ImportJob API StartFHIR, Amazon HealthLake impose l'obligation d'exporter les données vers un compartiment Amazon S3 chiffré.

Amazon HealthLake chiffre les données en transit et au repos. Pour le chiffrement des données en transit, vous pouvez utiliser les appels d'API publiés par AWS pour y accéder HealthLake via le réseau. Les clients doivent supporter le protocole TLS (Sécurité de la couche transport) 1.0 ou une version ultérieure. Nous exigeons TLS 1.2 et recommandons TLS 1.3. Les clients doivent aussi prendre en charge les suites de chiffrement PFS (Perfect Forward Secrecy) comme Ephemeral Diffie-Hellman (DHE) ou Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes. En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Les clients peuvent également utiliser l'AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires afin de signer les demandes. Pour le chiffrement des données au repos, Amazon HealthLake chiffre les données stockées dans les magasins de données du client à l'aide d'une clé AWS KMS appartenant au client ou d'une clé AWS KMS appartenant au service par défaut. Toutes les données et métadonnées du service sont chiffrées au repos à l'aide d'une clé AWS KMS détenue par le service.

Amazon HealthLake est intégré à AWS CloudTrail. CloudTrail capture tous les appels d'API adressés à Amazon HealthLake sous forme d'événements, y compris les appels effectués à la suite d'une interaction avec Console de gestion AWS l'interface de ligne de commande (CLI) et de manière programmatique à l'aide d'un kit de développement logiciel (SDK).

Amazon Inspector

Amazon Inspector est un service d'évaluation automatique de la sécurité destiné aux clients qui souhaitent améliorer la sécurité et la conformité des applications déployées sur AWS. Amazon Inspector évalue automatiquement les applications pour détecter les vulnérabilités ou les écarts par rapport aux meilleures pratiques. Après avoir effectué une évaluation, Amazon Inspector produit une liste détaillée des résultats de sécurité classés par niveau de gravité. Les clients peuvent exécuter Amazon Inspector sur des instances EC2 contenant des PHI. Amazon Inspector chiffre toutes les données transmises sur le réseau ainsi que toutes les données de télémétrie stockées au repos.

Service géré Amazon pour Apache Flink

Amazon Managed Service pour Apache Flink permet aux clients de créer rapidement du code SQL qui lit, traite et stocke les données en continu quasiment en temps réel. À l'aide de requêtes SQL standard sur les données de streaming, les clients peuvent créer des applications qui transforment leurs données et fournissent des informations sur celles-ci. Le service géré pour Apache Flink prend en charge les entrées provenant des flux de diffusion Kinesis Data Streams et Firehose en tant que sources pour les applications d'analyse. Si le flux est chiffré, le service géré pour Apache Flink accède aux données du flux crypté de manière fluide, sans qu'aucune autre configuration ne soit nécessaire. Le service géré pour Apache Flink ne stocke pas les données non chiffrées lues depuis Kinesis Data Streams. Pour plus d'informations, consultez Configuration de l'entrée de l'application.

Le service géré pour Apache Flink s'intègre à la fois à Amazon Logs AWS CloudTrail et à Amazon CloudWatch Logs pour la surveillance des applications. Pour plus d'informations, consultez les sections Outils de surveillance et Utilisation d'Amazon CloudWatch Logs.

Amazon Data Firehose

Lorsque les clients envoient des données de leurs producteurs de données vers leur flux de données Kinesis, Amazon Kinesis Data Streams chiffre les données à l'aide d'une AWS KMS clé avant de les stocker au repos. Lorsque le flux de diffusion Firehose lit les données du flux Kinesis, Kinesis Data Streams déchiffre d'abord les données, puis les envoie à Firehose. Firehose met en mémoire tampon les données en mémoire en fonction des indications de mise en mémoire tampon spécifiées par le client.

Il fournit ensuite les données aux destinations sans stocker les données non cryptées au repos. Pour plus d'informations sur le chiffrement avec Firehose, consultez la section Protection des données dans Amazon Data Firehose.

AWS fournit différents outils que les clients peuvent utiliser pour surveiller Amazon Data Firehose, notamment Amazon CloudWatch Metrics, Amazon CloudWatch Logs, Kinesis Agent, ainsi que la journalisation et l'historique des API. Pour plus d'informations, consultez Monitoring Amazon Data Firehose.

Amazon Kinesis Streams

Amazon Kinesis Streams permet aux clients de créer des applications personnalisées qui traitent ou analysent les données de streaming pour des besoins spécifiques. La fonction de chiffrement côté serveur permet aux clients de chiffrer les données au repos. Lorsque le chiffrement côté serveur est activé, Kinesis Streams utilise une AWS KMS clé pour chiffrer les données avant de les stocker sur des disques. Pour plus d'informations, consultez Protection des données dans Amazon Kinesis Data Streams. Les connexions à Amazon S3 contenant des PHI doivent utiliser des points de terminaison qui acceptent le transport crypté (c'est-à-dire HTTPS). Pour obtenir la liste des points de terminaison régionaux, consultez la section Points de terminaison des services AWS.

Amazon Kinesis Video Streams

Amazon Kinesis Video Streams est un service AWS entièrement géré que les clients peuvent utiliser pour diffuser des vidéos en direct depuis des appareils vers le cloud AWS, ou créer des applications de traitement vidéo en temps réel ou d'analyse vidéo par lots. Le chiffrement côté serveur est une fonctionnalité de Kinesis Video Streams qui chiffre automatiquement les données au repos à l'aide d'une AWS KMS clé (anciennement CMK) spécifiée par le client. Les données sont chiffrées avant d'être écrites sur la couche de stockage des flux Kinesis Video Streams, et elles sont déchiffrées une fois extraites du stockage.

Le SDK Amazon Kinesis Video Streams peut être utilisé pour transmettre des données vidéo en streaming contenant des PHI. Par défaut, le SDK utilise le protocole TLS pour chiffrer les cadres et les fragments générés par le périphérique matériel sur lequel il est installé. Le SDK ne gère ni n'affecte les données stockées au repos. Amazon Kinesis Video Streams enregistre AWS CloudTrail tous les appels d'API.

Amazon Lex

Amazon Lex est un service AWS permettant de créer des interfaces conversationnelles pour les applications utilisant la voix et le texte. Avec Amazon Lex, le même moteur de conversation qui alimente Amazon Alexa est désormais accessible à tous les développeurs, permettant aux clients de

créer des chatbots sophistiqués en langage naturel dans leurs applications nouvelles et existantes. Amazon Lex fournit les fonctionnalités avancées et la flexibilité de la compréhension du langage naturel (NLU) et de la reconnaissance vocale automatique (ASR) afin que les clients puissent créer des expériences utilisateur très engageantes grâce à des interactions conversationnelles réalistes et créer de nouvelles catégories de produits.

Lex utilise le protocole HTTPS pour communiquer à la fois avec les clients et avec les autres services AWS. L'accès à Lex est piloté par une API, et le moindre privilège IAM approprié peut être appliqué. Pour plus d'informations, consultez la section Protection des données dans Amazon Lex.

La surveillance est importante pour garantir la fiabilité, la disponibilité et les performances des chatbots Amazon Lex du client. Pour suivre l'état de santé des robots Amazon Lex, utilisez Amazon CloudWatch. Les clients peuvent ainsi obtenir des statistiques pour les opérations Amazon Lex individuelles ou pour les opérations Amazon Lex mondiales pour leur compte. CloudWatch Les clients peuvent également configurer des CloudWatch alarmes pour être avertis lorsqu'une ou plusieurs mesures dépassent un seuil défini par les clients. Par exemple, les clients peuvent surveiller le nombre de demandes adressées à un bot sur une période donnée, voir le temps de latence des demandes réussies ou déclencher une alarme lorsque les erreurs dépassent un certain seuil. Lex est également intégré AWS CloudTrail pour enregistrer les appels de l'API Lex. Pour plus d'informations, consultez la section Surveillance dans Amazon Lex.

Amazon Managed Streaming for Apache Kafka (Amazon MSK)

Amazon MSK fournit des fonctionnalités de chiffrement pour les données au repos et pour les données en transit. Pour le chiffrement des données au repos, le cluster Amazon MSK utilise le chiffrement côté serveur Amazon EBS et les AWS KMS clés pour chiffrer les volumes de stockage. Pour les données en transit, le chiffrement des clusters Amazon MSK est activé via TLS pour les communications entre courtiers.

Le paramètre de configuration du chiffrement est activé lors de la création d'un cluster. De plus, par défaut, le chiffrement en transit est défini sur TLS pour les clusters créés à partir de la CLI ou AWS de la console. Une configuration supplémentaire est requise pour que les clients puissent communiquer avec les clusters à l'aide du chiffrement TLS. Les clients peuvent modifier le paramètre de chiffrement par défaut en sélectionnant les paramètres TLS/Plaintext. Pour plus d'informations, consultez Amazon MSK Encryption.

Les clients peuvent surveiller les performances de leurs clusters à l'aide de la console Amazon MSK, de la CloudWatch console Amazon, ou les clients peuvent accéder à JMX et aux métriques de l'hôte à l'aide d'Open Monitoring avec Prometheus, une solution de surveillance open source.

Les outils conçus pour lire à partir des exportateurs Prometheus sont compatibles avec Open Monitoring, tels que Datadog, Lenses, New Relic,Sumologic ou un serveur Prometheus. Pour en savoir plus sur l'Open Monitoring, consultez la documentation Amazon MSK Open Monitoring.

Veuillez noter que la version par défaut d'Apache Zookeeper fournie avec Apache Kafka ne prend pas en charge le chiffrement. Cependant, il est important de noter que les communications entre Apache Zookeeper et les courtiers Apache Kafka sont limitées aux informations relatives aux courtiers, aux sujets et à l'état des partitions. Les données ne peuvent être produites et consommées à partir d'un cluster Amazon MSK que via une connexion privée entre leurs clients dans leur VPC et le cluster Amazon MSK. Amazon MSK ne prend pas en charge les points de terminaison publics.

Amazon MQ

Amazon MQ est un service de messagerie géré pour Apache ActiveMQ qui facilite la configuration et le fonctionnement des courtiers de messages dans le cloud. Amazon MQ fonctionne avec les applications et services existants sans que le client n'ait besoin de gérer, d'exploiter ou de maintenir son propre système de messagerie. Pour chiffrer les données PHI en transit, les protocoles suivants avec TLS activé doivent être utilisés pour accéder aux courtiers :

- AMQP
- MQTT
- MQTT terminé WebSocket
- OpenWire
- STOMP
- STOMP over WebSocket

Amazon MQ chiffre les messages au repos et en transit à l'aide de clés de chiffrement qu'il gère et stocke en toute sécurité. Amazon MQ enregistre tous les CloudTrail appels d'API.

Amazon Neptune

Amazon Neptune est un service de base de données orientée graphe entièrement géré et fiable, qui facilite la création et l'exécution d'applications fonctionnant avec des jeux de données hautement connectés. Le cœur d'Amazon Neptune est un moteur de base de données de graphes hautes performances spécialement conçu, optimisé pour stocker des milliards de relations et interroger le

graphe avec une latence de quelques millisecondes. Amazon Neptune prend en charge les langages de requête graphique populaires Apache TinkerPop Gremlin et SPARQL du W3C.

Les données contenant des PHI peuvent désormais être conservées dans une instance cryptée d'Amazon Neptune. Une instance chiffrée d'Amazon Neptune ne peut être spécifiée qu'au moment de sa création en choisissant « Activer le chiffrement » dans la console Amazon Neptune. Tous les journaux, sauvegardes et instantanés sont chiffrés pour une instance cryptée Amazon Neptune. La gestion des clés pour les instances chiffrées d'Amazon Neptune est assurée par le biais du. AWS KMS Le chiffrement des données en transit est assuré par le biais du protocole SSL/TLS. Amazon Neptune enregistre tous les CloudTrail appels d'API.

AWS Network Firewall

AWS Network Firewall est un service de pare-feu géré qui facilite le déploiement des protections réseau essentielles pour tous vos Amazon Virtual Private Cloud (Amazon VPC). Le service s'adapte automatiquement au volume du trafic réseau pour fournir des protections à haute disponibilité sans qu'il soit nécessaire de configurer ou de maintenir l'infrastructure sous-jacente. Les règles du client et les journaux d'accès peuvent contenir les adresses IP des utilisateurs finaux, qui sont chiffrées à la fois au repos et en transit au sein de l' AWS architecture. En outre, AWS Network Firewall chiffre toutes les données au repos et en transit entre les AWS services des composants (Amazon S3, Amazon DynamoDB, Amazon Logs CloudWatch , Amazon EBS). Le service chiffre automatiquement les données sans nécessiter de configuration particulière.

Amazon Pinpoint

Amazon Pinpoint offre aux développeurs une couche d'API unique, une prise en charge des CLI et une prise en charge du SDK côté client pour étendre les canaux de communication entre les applications et les utilisateurs. Les canaux éligibles incluent : les e-mails, les SMS, les notifications push mobiles et les canaux personnalisés. Amazon Pinpoint fournit également un système d'analyse qui suit le comportement et l'engagement des utilisateurs de l'application. Grâce à ce service, les développeurs peuvent découvrir comment chaque utilisateur préfère s'engager et personnaliser l'expérience de l'utilisateur afin d'accroître sa satisfaction.

Amazon Pinpoint aide également les développeurs à répondre à de multiples cas d'utilisation de la messagerie, tels que la messagerie directe ou transactionnelle, la messagerie ciblée ou de campagne et la messagerie basée sur des événements. En intégrant et en activant tous les canaux d'engagement des utilisateurs finaux via Amazon Pinpoint, les développeurs peuvent créer une vue à

360 degrés de l'engagement des utilisateurs sur tous les points de contact avec les clients. Amazon Pinpoint stocke les données relatives aux utilisateurs, aux terminaux et aux événements afin que les clients puissent créer des segments, envoyer des messages aux destinataires et recueillir des données d'engagement.

Amazon Pinpoint chiffre les données au repos et en transit. Pour plus d'informations, consultez les FAQ Amazon Pinpoint. Amazon Pinpoint chiffre toutes les données au repos et en transit, mais le canal final, tel que les SMS ou les e-mails, peut ne pas être crypté, et les clients doivent configurer tous les canaux conformément à leurs besoins.

En outre, les clients qui doivent envoyer des PHI par SMS doivent utiliser un code court dédié (numéros de téléphone d'origine à 5 ou 6 chiffres) dans le but explicite d'envoyer des PHI. Pour plus d'informations sur la procédure à suivre pour demander un code abrégé, consultez la section Demande de codes abrégés dédiés pour la messagerie SMS avec Amazon Pinpoint. Les clients peuvent également choisir de ne pas envoyer de PHI par le canal final et de fournir à la place un mécanisme permettant d'accéder aux PHI en toute sécurité via HTTPS.

Les appels d'API à Amazon Pinpoint peuvent être capturés à l'aide de. AWS CloudTrail Les appels capturés incluent ceux provenant de la console Amazon Pinpoint et les appels de code vers les opérations de l'API Amazon Pinpoint. Si les clients créent un suivi, ils peuvent activer la diffusion continue des AWS CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour Amazon Pinpoint. Si les clients ne configurent pas de suivi, ils peuvent toujours consulter les événements les plus récents en utilisant l'historique des événements sur la AWS CloudTrail console. À l'aide des informations collectées par AWS CloudTrail, les clients peuvent déterminer si la demande a été envoyée à Amazon Pinpoint, l'adresse IP de la demande, l'auteur de la demande, la date à laquelle elle a été faite et des informations supplémentaires. Pour plus d'informations, consultez la section Journalisation des appels d'API Amazon Pinpoint avec. AWS CloudTrail

Amazon Polly

Amazon Polly est un service cloud qui convertit le texte en un enregistrement audio réaliste. Amazon Polly fournit des opérations d'API simples que les clients peuvent facilement intégrer aux applications existantes. Amazon Polly utilise le protocole HTTPS pour communiquer avec les clients. L'accès à Amazon Polly est piloté par une API, et le moindre privilège IAM approprié peut être appliqué. Pour plus d'informations, consultez la section Protection des données. Voici quelques exemples de cas d'utilisation qui incluent PHI :

- Le soignant convertit un rapport texte contenant des PHI en synthèse vocale afin qu'il puisse écouter le rapport en marchant ou en accomplissant d'autres tâches.
- Le patient malvoyant reçoit des conseils médicaux et utilise les conseils sous forme de synthèse vocale.

Le canal de diffusion final d'Amazon Polly peut entraîner la diffusion de fichiers audio avec PHI dans un espace public et des précautions doivent être prises pour que la livraison en tienne compte. La sortie vocale synthétisée peut également être envoyée de manière asynchrone vers un compartiment Amazon S3 avec le chiffrement activé.

Lorsqu'une activité événementielle prise en charge se produit sur Amazon Polly, cette activité est enregistrée dans un AWS CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Pour un enregistrement continu des événements enregistrés dans un AWS compte client, y compris des événements liés à Amazon Polly, créez un historique. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. À l'aide des informations collectées par CloudTrail, les clients peuvent déterminer la demande qui a été faite à Amazon Polly, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des informations supplémentaires.

Amazon Quantum Ledger Database (Amazon QLDB)

Amazon QLDB est une base de données de registre entièrement gérée qui fournit un journal des transactions transparent, immuable et vérifiable par cryptographie, appartenant à une autorité centrale de confiance. Amazon QLDB suit chaque modification des données d'application et conserve un historique complet et vérifiable des modifications au fil du temps. Les données contenant des PHI peuvent désormais être conservées dans une instance QLDB. Par défaut, toutes les données Amazon QLDB en transit et au repos sont cryptées. Les données en transit sont cryptées à l'aide du protocole TLS et les données au repos sont chiffrées à l'aide de clés AWS gérées. À des fins de protection des données, nous recommandons aux clients de protéger les informations d'identification des AWS comptes et de configurer des comptes utilisateur individuels avec Gestion des identités et des accès AWS (IAM), afin que chaque utilisateur ne dispose que des autorisations nécessaires à l'accomplissement de ses tâches. Pour plus d'informations, consultez la section Protection des données dans Amazon QLDB.

Amazon QLDB est intégré AWS CloudTrailà un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans QLDB. CloudTrail capture tous les appels d'API du plan de contrôle pour QLDB sous forme d'événements. Les appels capturés incluent

les appels provenant de la console QLDB et les appels de code vers les opérations de l'API QLDB. Si les clients créent un suivi, ils peuvent activer la diffusion continue des CloudTrail événements vers un bucket Amazon Simple Storage Service (Amazon S3), y compris les événements pour QLDB. Si les clients ne configurent pas de suivi, ils peuvent toujours consulter les événements les plus récents sur la CloudTrail console dans l'historique des événements. À l'aide des informations collectées par CloudTrail, les clients peuvent déterminer la demande qui a été faite à QLDB, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires.

Amazon QuickSight

Amazon QuickSight est un service d'analyse commerciale que les clients peuvent utiliser pour créer des visualisations, effectuer des analyses ad hoc et obtenir rapidement des informations commerciales à partir de leurs données. Amazon QuickSight découvre AWS les sources de données, permet aux entreprises de s'adapter à des centaines de milliers d'utilisateurs et fournit des performances réactives grâce à un moteur en mémoire robuste (SPICE).

Les clients ne peuvent utiliser l'édition Enterprise d'Amazon que QuickSight pour travailler avec des données contenant des PHI, car elle prend en charge le chiffrement des données stockées au repos dans SPICE. Le chiffrement des données est effectué à l'aide de clés AWS gérées.

Amazon RDS for MariaDB

Amazon RDS for MariaDB permet aux clients de chiffrer les bases de données MariaDB à l'aide de clés qu'ils gèrent. AWS KMS Sur une instance de base de données exécutée avec le chiffrement Amazon RDS, les données stockées au repos dans le stockage sous-jacent sont chiffrées conformément aux directives en vigueur au moment de la publication de ce livre blanc, tout comme les sauvegardes automatisées, les répliques en lecture et les instantanés.

Le guide étant susceptible d'être mis à jour, les clients doivent continuer à évaluer et à déterminer si le chiffrement Amazon RDS for MariaDB répond à leurs exigences réglementaires et de conformité. Pour plus d'informations sur le chiffrement au repos à l'aide d'Amazon RDS, consultez la section Chiffrement des ressources Amazon RDS.

Les connexions à RDS pour MariaDB contenant des PHI doivent utiliser le cryptage du transport. Pour plus d'informations sur l'activation des connexions chiffrées, voir Utilisation du protocole SSL/TLS pour chiffrer une connexion à une instance de base de données.

Amazon RDS for MySQL

Amazon RDS for MySQL permet aux clients de chiffrer les bases de données MySQL à l'aide de clés gérées par les clients AWS KMS. Sur une instance de base de données exécutée avec le chiffrement Amazon RDS, les données stockées au repos dans le stockage sous-jacent sont chiffrées conformément aux directives en vigueur au moment de la publication de ce livre blanc, tout comme les sauvegardes automatisées, les répliques en lecture et les instantanés.

Le guide étant susceptible d'être mis à jour, les clients doivent continuer à évaluer et à déterminer si le chiffrement Amazon RDS for MySQL répond à leurs exigences réglementaires et de conformité. Pour plus d'informations sur le chiffrement au repos à l'aide d'Amazon RDS, consultez la section Chiffrement des ressources Amazon RDS.

Les connexions à RDS pour MySQL contenant des données PHI doivent utiliser le chiffrement de transport. Pour plus d'informations sur l'activation des connexions chiffrées, voir Utilisation du protocole SSL/TLS pour chiffrer une connexion à une instance de base de données.

Amazon RDS for Oracle

Les clients disposent de plusieurs options pour chiffrer les PHI au repos à l'aide d'Amazon RDS for Oracle. Les clients peuvent chiffrer les bases de données Oracle à l'aide de clés qu'ils gèrent. AWS KMS Sur une instance de base de données exécutée avec le chiffrement Amazon RDS, les données stockées au repos dans le stockage sous-jacent sont chiffrées conformément aux directives en vigueur au moment de la publication de ce livre blanc, tout comme les sauvegardes automatisées, les répliques en lecture et les instantanés.

Les directives étant susceptibles d'être mises à jour, les clients doivent continuer à évaluer et à déterminer si le chiffrement Amazon RDS for Oracle répond à leurs exigences réglementaires et de conformité. Pour plus d'informations sur le chiffrement au repos à l'aide d'Amazon RDS, consultez la section Chiffrement des ressources Amazon RDS.

Les clients peuvent également utiliser Oracle Transparent Data Encryption (TDE), et ils doivent évaluer la cohérence de la configuration avec les directives. Oracle TDE est une fonctionnalité de l'option Oracle Advanced Security disponible dans Oracle Enterprise Edition. Cette fonction chiffre automatiquement les données avant qu'elles ne soient écrites dans le stockage et déchiffre automatiquement les données lorsqu'elles sont lues depuis le stockage. Les clients peuvent également les utiliser AWS CloudHSM pour stocker les clés Oracle TDE d'Amazon RDS. Pour plus d'informations, consultez les ressources suivantes :

- Chiffrement transparent des données Amazon RDS pour Oracle : chiffrement transparent des données Oracle.
- Utilisation AWS CloudHSM pour stocker les clés Oracle TDE d'Amazon RDS : qu'est-ce qu'Amazon Relational Database Service (Amazon RDS) ?

Les connexions à Amazon RDS for Oracle contenant des PHI doivent utiliser le chiffrement du transport et évaluer la cohérence de la configuration avec les directives. Ceci est réalisé à l'aide d'Oracle Native Network Encryption et activé dans les groupes d'options Amazon RDS for Oracle. Pour des informations détaillées, voir Oracle Native Network Encryption.

Amazon RDS for PostgreSQL

Amazon RDS for PostgreSQL permet aux clients de chiffrer les bases de données PostgreSQL à l'aide de clés gérées par les clients. AWS KMS Sur une instance de base de données exécutée avec le chiffrement Amazon RDS, les données stockées au repos dans le stockage sous-jacent sont chiffrées conformément aux directives en vigueur au moment de la publication de ce livre blanc, tout comme les sauvegardes automatisées, les répliques en lecture et les instantanés.

Le guide étant susceptible d'être mis à jour, les clients doivent continuer à évaluer et à déterminer si le chiffrement Amazon RDS for PostgreSQL répond à leurs exigences réglementaires et de conformité. Pour plus d'informations sur le chiffrement au repos à l'aide d'Amazon RDS, consultez la section Chiffrement des ressources Amazon RDS.

Les connexions à RDS pour PostgreSQL contenant des données PHI doivent utiliser le chiffrement du transport. Pour plus d'informations sur l'activation des connexions chiffrées, voir Utilisation du protocole SSL/TLS pour chiffrer une connexion à une instance de base de données.

Amazon RDS for SQL Server

RDS pour SQL Server prend en charge le stockage de PHI pour les combinaisons de versions et d'éditions suivantes :

- 2008 R2 - Édition Enterprise uniquement
- 2012, 2014 et 2016 - Éditions Web, Standard et Enterprise

Important : l'édition SQL Server Express n'est pas prise en charge et ne doit jamais être utilisée pour le stockage de PHI.

Pour stocker des données PHI, les clients doivent s'assurer que l'instance est configurée pour chiffrer les données au repos et activer le chiffrement et l'audit du transport, comme indiqué ci-dessous.

Chiffrement au repos

Les clients peuvent chiffrer les bases de données SQL Server à l'aide de clés qu'ils gèrent. AWS KMS Sur une instance de base de données exécutée avec le chiffrement Amazon RDS, les données stockées au repos dans le stockage sous-jacent sont chiffrées conformément aux directives en vigueur au moment de la publication de ce livre blanc, tout comme les sauvegardes automatisées et les instantanés. Le guide étant susceptible d'être mis à jour, les clients doivent continuer à évaluer et à déterminer si le chiffrement Amazon RDS for SQL Server répond à leurs exigences réglementaires et de conformité. Pour plus d'informations sur le chiffrement au repos à l'aide d'Amazon RDS, consultez la section Chiffrement des ressources Amazon RDS.

Si les clients utilisent SQL Server Enterprise Edition, ils peuvent utiliser le chiffrement transparent des données (TDE) comme alternative. Cette fonction chiffre automatiquement les données avant qu'elles ne soient écrites dans le stockage et déchiffre automatiquement les données lorsqu'elles sont lues depuis le stockage. Pour plus d'informations sur le chiffrement transparent des données RDS pour SQL Server, consultez Support pour le chiffrement transparent des données dans SQL Server.

Chiffrement de transport

Les connexions à Amazon RDS for SQL Server contenant des PHI doivent utiliser le chiffrement de transport fourni par le protocole SSL forcé de SQL Server. Le SSL forcé est activé depuis le groupe de paramètres pour Amazon RDS SQL Server. Pour plus d'informations sur le protocole SSL forcé RDS pour SQL Server, consultez la section Utilisation du protocole SSL avec une instance de base de données Microsoft SQL Server.

Audit

L'audit doit être activé pour les instances de RDS pour SQL Server contenant des données PHI. L'audit est activé depuis le groupe de paramètres pour Amazon RDS SQL Server. Pour plus d'informations sur l'audit RDS pour SQL Server, consultez la section Support du programme de conformité pour les instances de base de données Microsoft SQL Server.

Amazon Redshift

Amazon Redshift fournit un chiffrement de base de données pour ses clusters afin de protéger les données au repos. Lorsque les clients activent le chiffrement d'un cluster, Amazon Redshift

chiffre toutes les données, y compris les sauvegardes, à l'aide de clés symétriques AES (Advanced Encryption Standard) à 256 clés symétriques accélérées par le matériel. Amazon Redshift utilise une architecture à quatre niveaux de clés pour le chiffrement. Ces clés se composent de clés de chiffrement des données, d'une clé de base de données, d'une clé de cluster et d'une clé KMS.

La clé de cluster chiffre la clé de base de données du cluster Amazon Redshift. Les clients peuvent utiliser l'un AWS KMS ou l'autre AWS CloudHSM (module de sécurité matérielle) pour gérer la clé de cluster. Le chiffrement au repos d'Amazon Redshift est conforme aux directives en vigueur au moment de la publication de ce livre blanc. Le guide étant susceptible d'être mis à jour, les clients doivent continuer à évaluer et à déterminer si le chiffrement Amazon Redshift répond à leurs exigences réglementaires et de conformité. Pour plus d'informations, consultez Chiffrement de base de données Amazon Redshift.

Les connexions à Amazon Redshift contenant des PHI doivent utiliser le chiffrement du transport et les clients doivent évaluer la cohérence de la configuration avec les directives. Pour plus d'informations, consultez la section Configuration des options de sécurité pour les connexions. Amazon Redshift Spectrum permet aux clients d'exécuter des requêtes SQL Amazon Redshift sur des exaoctets de données dans Amazon S3. Redshift Spectrum est une fonctionnalité d'Amazon Redshift et est donc également couverte par le HIPAA BAA.

Amazon Rekognition

Amazon Rekognition permet d'ajouter facilement des analyses d'images et de vidéos aux applications des clients. Un client doit uniquement fournir une image ou une vidéo à l'API Amazon Rekognition, et le service peut identifier les objets, les personnes, le texte, les scènes et les activités, ainsi que détecter tout contenu inapproprié. Amazon Rekognition fournit également une analyse faciale et une reconnaissance faciale très précises.

Amazon Rekognition peut fonctionner avec des images ou des vidéos contenant des PHI. Amazon Rekognition fonctionne comme un service géré et ne propose aucune option configurable pour le traitement des données. Amazon Rekognition utilise, divulgue et gère les PHI uniquement conformément aux termes de la BAA. AWS Toutes les données sont cryptées au repos et en transit avec Amazon Rekognition. Amazon AWS CloudTrail Rekognition enregistre tous les appels d'API.

Amazon Route 53

Amazon Route 53 est un service DNS géré qui permet aux clients d'enregistrer des noms de domaine, d'acheminer le trafic Internet, les ressources du domaine des clients et de vérifier l'état de

ces ressources. Bien qu'Amazon Route 53 soit un service éligible à la loi HIPAA, aucun PHI ne doit être stocké dans les noms de ressources ou les balises d'Amazon Route 53, car le chiffrement de ces données n'est pas pris en charge. Amazon Route 53 peut plutôt être utilisé pour fournir un accès aux ressources du domaine client qui transmettent ou stockent des PHI, telles que les serveurs Web exécutés sur Amazon EC2 ou le stockage tel qu'Amazon S3.

Amazon S3 Glacier

Amazon S3 Glacier chiffre automatiquement les données au repos à l'aide de clés symétriques AES 256 bits et prend en charge le transfert sécurisé des données des clients via des protocoles sécurisés. Les connexions à Amazon S3 Glacier contenant des PHI doivent utiliser des points de terminaison qui acceptent le transport crypté (HTTPS). Pour obtenir la liste des points de terminaison régionaux, consultez la section Points de terminaison AWS de service.

N'utilisez pas PHI dans les noms d'archives et de coffres-forts ou dans les métadonnées, car ces données ne sont pas chiffrées à l'aide du chiffrement côté serveur Amazon S3 Glacier et ne sont généralement pas chiffrées dans les architectures de chiffrement côté client.

Amazon S3 Transfer Acceleration

Amazon S3 Transfer Acceleration (S3TA) permet des transferts rapides, faciles et sécurisés de fichiers sur de longues distances entre le client d'un client et un compartiment S3. Transfer Acceleration tire parti des emplacements périphériques distribués dans le monde entier d'Amazon CloudFront. Lorsque les données arrivent dans un emplacement périphérique, elles sont transférées vers Amazon S3 sur un chemin de réseau optimisé. Les clients doivent s'assurer que toutes les données contenant des PHI transférées via AWS S3TA sont cryptées en transit et au repos. Reportez-vous au guide destiné à Amazon S3 pour comprendre les options de chiffrement disponibles.

Amazon SageMaker

Amazon SageMaker est un service d'apprentissage automatique entièrement géré. Avec Amazon SageMaker, les data scientists et les développeurs peuvent rapidement et facilement créer et entraîner des modèles d'apprentissage automatique, puis les déployer directement dans un environnement hébergé prêt pour la production. Il fournit une instance de bloc-notes de création Jupyter intégrée pour un accès facile aux sources de données à des fins d'exploration et d'analyse.

Amazon fournit SageMaker également des algorithmes d'apprentissage automatique courants optimisés pour fonctionner efficacement sur des données extrêmement volumineuses dans un environnement distribué.

Grâce à un support bring-your-own-algorithms et à des frameworks natifs, Amazon SageMaker propose des options de formation distribuées flexibles qui s'adaptent aux flux de travail spécifiques du client. Amazon SageMaker est éligible pour opérer avec des données contenant des PHI. Le chiffrement des données en transit est fourni par SSL/TLS et est utilisé à la fois lors de la communication avec l'interface frontale d'Amazon SageMaker (vers le Notebook) et chaque fois qu'Amazon SageMaker interagit avec un autre AWS service (par exemple, pour extraire des données d'Amazon S3).

Pour satisfaire à l'exigence selon laquelle les PHI doivent être chiffrés au repos, le chiffrement des données stockées avec l'instance exécutant des modèles avec Amazon SageMaker est activé à l'aide de AWS Key Management Service (KMS) lors de la configuration du point de terminaison (DescribeEndpointConfig: KmsKey ID). Le chiffrement des résultats d'entraînement des modèles (artefacts) est activé à l'aide de AWS KMS et les clés doivent être spécifiées à l'aide de l' KmsKeyID indiqué dans la OutputDataConfig description. Si aucun ID de clé KMS n'est fourni, la clé KMS Amazon S3 par défaut pour le compte du rôle sera utilisée. Amazon SageMaker enregistre AWS CloudTrail tous les appels d'API.

Amazon Simple Notification Service (Amazon SNS)

Les clients doivent comprendre les exigences de chiffrement des clés suivantes afin d'utiliser Amazon Simple Notification Service (SNS) avec Protected Health Information (PHI). Les clients doivent utiliser le point de terminaison de l'API HTTPS fourni par SNS dans chaque AWS région. Le point de terminaison HTTPS utilise des connexions cryptées et protège la confidentialité et l'intégrité des données envoyées AWS. Pour obtenir la liste de tous les points de terminaison de l'API HTTPS, consultez la section Points de terminaison AWS du service.

En outre, Amazon SNS utilise CloudTrail un service qui capture les appels d'API effectués par ou pour le compte d'Amazon SNS dans le compte AWS du client et envoie les fichiers journaux dans un compartiment Amazon S3 spécifié par ce dernier. CloudTrail capture les appels d'API effectués depuis la console Amazon SNS ou depuis l'API Amazon SNS. À l'aide des informations collectées par CloudTrail, les clients peuvent déterminer quelle demande a été envoyée à Amazon SNS, l'adresse IP source à partir de laquelle la demande a été faite, qui l'a faite et quand elle a été faite. Pour plus d'informations sur la journalisation des opérations SNS, consultez la section Journalisation des appels d'API Amazon SNS à l'aide de. CloudTrail

Amazon Simple Email Service (Amazon SES)

Amazon Simple Email Service (Amazon SES) est un service d'envoi et de réception d'e-mails flexible et hautement évolutif. Il prend en charge les protocoles S/MIME et PGP pour chiffrer les messages pour un end-to-end chiffrement complet, et toutes les communications avec Amazon SES sont sécurisées à l'aide du protocole SSL (TLS 1.2). Les clients ont la possibilité de stocker les messages chiffrés au repos en configurant Amazon SES pour recevoir et chiffrer les messages avant de les stocker dans un compartiment Amazon S3. Pour plus d'informations, consultez Comment AWS KMS utilise Amazon Simple Email Service (Amazon SES) pour en savoir plus sur le chiffrement des messages à des fins de stockage. Les messages sont sécurisés lors de leur transfert vers Amazon SES via un point de terminaison HTTPS ou une connexion SMTP cryptée.

Pour les messages envoyés par Amazon SES à un destinataire, Amazon SES essaiera d'abord d'établir une connexion sécurisée avec le serveur de messagerie de réception, mais si une connexion sécurisée ne peut pas être établie, il enverra le message non chiffré. Pour exiger le chiffrement lors de la livraison à un destinataire, les clients doivent créer un ensemble de configuration dans Amazon SES et utiliser le AWS CLI pour définir la TlsPolicy propriété sur Require. Pour plus d'informations, consultez Amazon SES et protocoles de sécurité. Amazon SES s'intègre AWS CloudTrail pour surveiller tous les appels d'API. À l'aide des informations collectées par AWS CloudTrail, les clients peuvent déterminer si la demande a été envoyée à Amazon SES, l'adresse IP de la demande, l'auteur de la demande, la date à laquelle elle a été faite et des informations supplémentaires. Pour plus d'informations, consultez la section Journalisation des appels d'API Amazon SES avec AWS CloudTrail. Amazon SES propose également des méthodes pour surveiller les activités d'envoi telles que les envois, les rejets, les taux de rebond, les livraisons, les ouvertures et les clics. Pour plus d'informations, consultez Surveillance de votre activité d'envoi sur Amazon SES.

Amazon Simple Queue Service (Amazon SQS)

Les clients doivent comprendre les exigences de chiffrement des clés suivantes afin d'utiliser Amazon SQS avec PHI.

- La communication avec la file d'attente Amazon SQS via la demande de requête doit être cryptée avec HTTPS. Pour plus d'informations sur les requêtes SQS, consultez la section Création de requêtes API.
- Amazon SQS prend en charge le chiffrement côté serveur intégré au AWS KMS pour protéger les données au repos. L'ajout du chiffrement côté serveur permet aux clients de transmettre et de recevoir des données sensibles avec une sécurité accrue grâce à l'utilisation de files d'attente

cryptées. Le chiffrement côté serveur Amazon SQS utilise la norme de chiffrement avancée 256 bits (algorithme AES-256 GCM) pour chiffrer le corps de chaque message. L'intégration AWS KMS permet aux clients de gérer de manière centralisée les clés qui protègent les messages Amazon SQS ainsi que les clés qui protègent leurs autres AWS ressources. AWS KMS enregistre chaque utilisation de clés de chiffrement AWS CloudTrail afin de répondre aux exigences réglementaires et de conformité. Pour plus d'informations et pour vérifier la disponibilité de SSE pour Amazon SQS par région, consultez Encryption at Rest.

- Si le chiffrement côté serveur n'est pas utilisé, la charge utile du message elle-même doit être chiffrée avant d'être envoyée à SQS. L'un des moyens de chiffrer la charge utile des messages consiste à utiliser le client Amazon SQS Extended avec le client de chiffrement Amazon S3. Pour plus d'informations sur l'utilisation du chiffrement côté client, consultez Chiffrer les charges utiles des messages à l'aide du client Amazon SQS Extended et du client de chiffrement Amazon S3.

Amazon SQS utilise CloudTrail un service qui enregistre les appels d'API effectués par ou pour le compte d'Amazon SQS dans le compte d'un AWS client et envoie les fichiers journaux dans le compartiment Amazon S3 spécifié. CloudTrail capture les appels d'API effectués depuis la console Amazon SQS ou depuis l'API Amazon SQS. Les clients peuvent utiliser les informations collectées par CloudTrail pour déterminer quelles demandes sont adressées à Amazon SQS, l'adresse IP source à partir de laquelle la demande est faite, qui a fait la demande, quand elle est faite, etc. Pour plus d'informations sur la journalisation des opérations SQS, consultez la section Journalisation des appels d'API Amazon SQS à l'aide de. AWS CloudTrail

Amazon Simple Storage Service (Amazon S3)

Les clients disposent de plusieurs options pour le chiffrement des données au repos lorsqu'ils utilisent Amazon S3, notamment le chiffrement côté serveur et côté client, et plusieurs méthodes de gestion des clés. Pour plus d'informations, consultez la section Protection des données à l'aide du chiffrement.

Les connexions à Amazon S3 contenant des PHI doivent utiliser des points de terminaison qui acceptent le transport crypté (HTTPS). Pour obtenir la liste des points de terminaison régionaux, consultez la section Points de terminaison AWS de service.

N'utilisez pas PHI dans les noms de compartiments, les noms d'objets ou les métadonnées, car ces données ne sont pas chiffrées à l'aide du chiffrement côté serveur S3 et ne sont généralement pas chiffrées dans les architectures de chiffrement côté client.

Amazon Simple Workflow Service

Amazon Simple Workflow Service (Amazon SWF) aide les développeurs à créer, exécuter et dimensionner des tâches d'arrière-plan comportant des étapes parallèles ou séquentielles. Amazon SWF peut être considéré comme un outil de suivi d'état entièrement géré et un coordinateur de tâches dans le cloud.

Le service Amazon Simple Workflow est utilisé pour orchestrer les flux de travail et n'est pas en mesure de stocker ou de transmettre des données. Le PHI ne doit pas être placé dans les métadonnées d'Amazon SWF ni dans la description d'une tâche. Amazon SWF enregistre tous les AWS CloudTrail appels d'API.

Amazon Textract

Amazon Textract utilise des technologies d'apprentissage automatique pour extraire automatiquement le texte et les données des documents numérisés. Cela va au-delà de la simple reconnaissance optique de caractères (OCR) pour identifier, comprendre et extraire les données des formulaires et des tableaux. Par exemple, les clients peuvent utiliser Amazon Textract pour extraire automatiquement des données et traiter des formulaires contenant des informations médicales protégées (PHI) sans intervention humaine pour traiter les demandes de remboursement de frais médicaux.

Amazon Textract peut également être utilisé pour garantir la conformité des archives de documents. Par exemple, les clients peuvent utiliser Amazon Textract pour extraire des données provenant de réclamations d'assurance ou de prescriptions médicales, et reconnaître automatiquement les paires clé-valeur dans ces documents afin que les documents sensibles puissent être expurgés.

Amazon Textract prend en charge le chiffrement côté serveur (SSE-S3 et SSE-KMS) pour les documents d'entrée et le chiffrement TLS pour les données en transit entre le service et l'agent. Les clients peuvent utiliser Amazon CloudWatch pour suivre les statistiques d'utilisation des ressources et AWS CloudTrail pour capturer les appels d'API vers Amazon Textract.

Amazon Transcribe

Amazon Transcribe utilise des technologies avancées d'apprentissage automatique pour reconnaître la parole dans les fichiers audio et la transcrire en texte. Par exemple, les clients peuvent utiliser Amazon Transcribe pour convertir des fichiers audio en anglais américain et en espagnol mexicain en texte et pour créer des applications intégrant le contenu de fichiers audio. Amazon Transcribe

peut être utilisé avec des données contenant des PHI. Amazon Transcribe ne conserve ni ne stocke aucune donnée et tous les appels à l'API sont chiffrés avec SSL/TLS. Amazon Transcribe enregistre tous CloudTrail les appels d'API.

Amazon Translate

Amazon Translate utilise des technologies avancées d'apprentissage automatique pour fournir des traductions de haute qualité à la demande. Les clients peuvent utiliser Amazon Translate pour traduire des documents texte non structurés ou pour créer des applications qui fonctionnent dans plusieurs langues. Les documents contenant des PHI peuvent être traités avec Amazon Translate. Aucune configuration supplémentaire n'est requise lors de la traduction de documents contenant des données PHI. Le chiffrement des données en transit est assuré par le protocole SSL/TLS et aucune donnée n'est conservée avec Amazon Translate. Amazon Translate CloudTrail enregistre tous les appels d'API.

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud (Amazon VPC) propose un ensemble de fonctionnalités de sécurité réseau parfaitement adaptées à l'architecture des charges de travail réglementées par la loi HIPAA. Des fonctionnalités telles que les listes de contrôle d'accès réseau sans état et la réaffectation dynamique des instances dans des groupes de sécurité dynamiques offrent une certaine flexibilité dans la protection des instances contre tout accès réseau non autorisé.

Amazon VPC permet également aux clients d'étendre leur propre espace d'adressage réseau et de proposer un certain nombre de méthodes pour connecter leurs centres de données à. AWS AWS Les journaux de flux VPC fournissent une piste d'audit des connexions acceptées et rejetées aux instances traitant, transmettant ou stockant des PHI.

AWS Transit Gateway agit comme un hub réseau et simplifie la connectivité entre les Amazon VPC et les réseaux sur site. AWS Transit Gateway fournit également des capacités de peering interrégionales à d'autres passerelles de transit afin d'établir un réseau mondial utilisant le backbone. AWS Pour plus d'informations sur Amazon VPC, consultez Amazon Virtual Private Cloud.

Amazon WorkDocs

Amazon WorkDocs est un service de stockage et de partage de fichiers d'entreprise entièrement géré et sécurisé, doté de contrôles administratifs stricts et de fonctionnalités de feedback qui améliorent la productivité des utilisateurs. Amazon WorkDocs les fichiers sont chiffrés au repos à l'aide de clés que

les clients gèrent via AWS Key Management Service (AWS KMS). Toutes les données en transit sont cryptées à l'aide du protocole SSL/TLS. AWS les applications Web et mobiles, ainsi que les clients de synchronisation de bureau, transmettent les fichiers directement Amazon WorkDocs via SSL/TLS.

À l'aide de la console de Amazon WorkDocs gestion, WorkDocs les administrateurs peuvent consulter les journaux d'audit pour suivre l'activité des fichiers et des utilisateurs dans le temps, et choisir d'autoriser ou non les utilisateurs à partager des fichiers avec d'autres personnes extérieures à leur organisation. Amazon WorkDocs est également intégré à CloudTrail (un service qui capture les appels d'API effectués par le compte du Amazon WorkDocs client ou pour le AWS compte de celui-ci) et fournit des fichiers CloudTrail journaux à un compartiment Amazon S3 spécifié par les clients.

L'authentification multifactorielle (MFA) à l'aide d'un serveur RADIUS est disponible et peut fournir aux clients un niveau de sécurité supplémentaire pendant le processus d'authentification. Les utilisateurs se connectent en saisissant leur nom d'utilisateur et leur mot de passe suivis d'un OTP (code à usage unique) fourni par un jeton matériel ou logiciel.

Pour plus d’informations, consultez :

- Amazon WorkDocs fonctionnalité
- Enregistrement des appels Amazon WorkDocs d'API à l'aide de AWS CloudTrail

Les clients ne doivent pas stocker de PHI dans des noms de fichiers ou de répertoires.

Amazon WorkSpaces

Amazon WorkSpaces est une solution esktop-as-a D-Service (DaaS) entièrement gérée et sécurisée qui fonctionne sur. AWS Avec Amazon WorkSpaces, les clients peuvent facilement fournir des bureaux Microsoft Windows virtuels basés sur le cloud à leurs utilisateurs, leur permettant ainsi d'accéder aux documents, aux applications et aux ressources dont ils ont besoin, n'importe où, n'importe quand, depuis n'importe quel appareil compatible.

Amazon WorkSpaces stocke les données dans les volumes Amazon Elastic Block Store. Les clients peuvent chiffrer leurs volumes de WorkSpaces stockage à l'aide de clés qu'ils utilisent pour les gérer. AWS Key Management Service Lorsque le chiffrement est activé sur un WorkSpace, les données stockées au repos dans le stockage sous-jacent et les sauvegardes automatisées (instantanés EBS) du stockage sur disque sont chiffrées conformément au guide. La communication entre les WorkSpace clients WorkSpace est sécurisée à l'aide du protocole SSL/TLS. Pour plus d'informations sur le chiffrement au repos à l'aide d'Amazon WorkSpaces, consultez Encrypted WorkSpaces.

AWS App Mesh

AWS App Mesh est un maillage de services qui fournit un réseau au niveau des applications afin de permettre à vos services de communiquer facilement entre eux via plusieurs types d'infrastructures informatiques, tels que les services Amazon ECS, Amazon EKS ou Amazon EC2. App Mesh configure les proxys Envoy pour collecter et transmettre des données d'observabilité aux vices du set de surveillance que vous configurez, afin de vous donner de la visibilité. end-to-end Il peut acheminer le trafic en fonction du routage et des politiques de trafic configurées pour garantir la haute disponibilité de vos applications. Le trafic entre les applications peut être configuré pour utiliser le protocole TLS. App Mesh peut être utilisé à l'aide du AWS SDK ou du contrôleur App Mesh pour Kubernetes. Bien qu' AWS App Mesh il s'agisse d'un service éligible à la loi HIPAA, aucun PHI ne doit être stocké dans aucun nom/attribut de ressource, AWS App Mesh car il n'existe aucun support pour protéger ces données. Il AWS App Mesh peut plutôt être utilisé pour surveiller, contrôler et sécuriser les ressources du domaine client qui transmettent ou stockent des PHI.

AWS Service de migration d'applications

AWS Le service de migration des applications (AWS MGN) vous permet de migrer rapidement vos serveurs et applications AWS, sans modifications et avec un temps d'arrêt minimal. AWS MGN est le principal service de migration recommandé pour les migrations par levage et transfert vers AWS.

AWS MGN utilise la réplication des données au niveau des blocs pour copier les disques sources directement sur les volumes EBS du compte client. Les données ne sont jamais transmises via un environnement cloud contrôlé par AWS MGN. Les données répliquées sont chiffrées en transit par défaut. Les données des volumes EBS du client sont chiffrées par défaut à l'aide des propres clés du client.

AWS Auto Scaling

AWS Auto Scaling permet aux clients de configurer le dimensionnement automatique des AWS ressources faisant partie de leur application en quelques minutes. Les clients peuvent utiliser AWS Auto Scaling pour un certain nombre de services impliquant des PHI, tels qu'Amazon DynamoDB, Amazon ECS, les répliques Amazon RDS Aurora et les instances Amazon EC2 au sein d'un groupe Auto Scaling.

AWS Auto Scaling est un service d'orchestration qui ne traite, ne stocke ni ne transmet directement le contenu des clients ; les clients peuvent donc utiliser ce service avec du contenu crypté. Le modèle

de responsabilité AWS partagée s'applique à la protection des données dans AWS Auto Scaling : AWS il est responsable des procédures de sécurité du AWS réseau, tandis que le client est chargé de garder le contrôle sur le contenu du client hébergé sur cette infrastructure. Ce contenu inclut la configuration de la sécurité et les tâches de gestion pour les AWS services utilisés par les clients. À des fins de protection des données, nous recommandons aux clients de protéger les informations d'identification des AWS comptes et de configurer des comptes utilisateur individuels avec Gestion des identités et des accès AWS (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches.

Nous recommandons vivement aux clients de ne jamais saisir d'informations d'identification sensibles, telles que les numéros de compte des clients, dans des champs libres tels que le champ Nom. Cela inclut lorsque les clients travaillent avec AWS Auto Scaling ou d'autres AWS services à l' Console de gestion AWS aide de l' AWS CLI API ou AWS des SDK.

Toutes les données saisies par les clients dans AWS Auto Scaling ou dans d'autres services peuvent être récupérées pour être incluses dans les journaux de diagnostic. Lorsque les clients fournissent une URL vers un serveur externe, ils ne doivent pas inclure d'informations d'identification dans l'URL pour valider leur demande auprès de ce serveur. AWS recommande également aux clients de sécuriser leurs données de la manière suivante :

- Utilisez l’authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous recommandons le protocole TLS 1.2 ou version ultérieure
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut au sein AWS des services.
- Utilisez des services de sécurité gérés avancés tels qu’Amazon Macie, qui contribuent à la découverte et à la sécurisation des données personnelles stockées dans Amazon S3.

AWS Backup

AWS Backup propose un service centralisé, entièrement géré et basé sur des règles pour protéger les données des clients et garantir la conformité des AWS services à des fins de continuité des activités. Les clients peuvent configurer de manière centralisée les politiques de protection des données (sauvegarde) et surveiller les activités de sauvegarde sur l'ensemble des AWS ressources du client, notamment les volumes Amazon EBS, les bases de données Amazon Relational Database Service (Amazon RDS) (y compris les clusters Aurora), les tables Amazon DynamoDB, les tables

Amazon Elastic File System (Amazon EFS), les systèmes de fichiers Amazon FSx, les instances Amazon EC2. AWS Backup AWS Storage Gateway

AWS Backup chiffre les données des clients en transit et au repos. Les sauvegardes provenant de services dotés de fonctionnalités de capture instantanée existantes sont chiffrées à l'aide de la méthodologie de chiffrement des instantanés du service source. Par exemple, les instantanés EBS sont chiffrés à l'aide de la clé de chiffrement du volume à partir duquel ils ont été créés.

Les sauvegardes provenant de nouveaux AWS services intégrant des fonctionnalités de sauvegarde intégrées AWS Backup, tels qu'Amazon EFS, sont chiffrées en cours de transfert et au repos indépendamment des services sources, offrant ainsi aux sauvegardes des clients un niveau de protection supplémentaire. Le chiffrement est configuré au niveau du Backup Vault. Le coffre-fort par défaut est crypté. Lorsque les clients créent un nouveau coffre-fort, une clé de chiffrement doit être sélectionnée.

AWS Batch

AWS Batch permet aux développeurs, aux scientifiques et aux ingénieurs d'exécuter facilement et efficacement des centaines de milliers de tâches de calcul par lots AWS. AWS Batch fournit dynamiquement la quantité et le type optimaux de ressources de calcul (telles que les instances optimisées pour le processeur ou la mémoire) en fonction du volume et des besoins en ressources spécifiques des tâches par lots soumises. AWS Batch planifie, planifie et exécute des charges de travail informatiques par lots sur l'ensemble de la gamme de services et de fonctionnalités AWS informatiques.

À l'instar des instructions pour Amazon ECS, les PHI ne doivent pas être placés directement dans la définition de la tâche, dans la file d'attente des tâches ou dans les balises pour AWS Batch. Au lieu de cela, les tâches planifiées et exécutées avec AWS Batch peuvent fonctionner sur des PHI chiffrés. Toute information renvoyée par les étapes d'une tâche ne AWS Batch doit pas non plus contenir de PHI. Chaque fois que des tâches exécutées par AWS Batch doivent transmettre ou recevoir des PHI, cette connexion doit être cryptée à l'aide du protocole HTTPS ou SSL/TLS.

AWS Certificate Manager

AWS Certificate Manager est un service qui permet aux clients de fournir, de gérer et de déployer facilement des certificats SSL/TLS publics et privés à utiliser avec les AWS services et leurs ressources internes connectées. AWS Certificate Manager utilise CloudTrail pour enregistrer tous les appels d'API.

Les utilisateurs ont besoin d'un accès programmatique s'ils souhaitent interagir avec AWS l'extérieur du Console de gestion AWS. La manière d'accorder un accès programmatique dépend du type d'utilisateur qui y accède AWS.

Pour accorder aux utilisateurs un accès par programmation, choisissez l’une des options suivantes.

Quel utilisateur a besoin d’un accès par programmation ?	Pour	Méthode
Identité de la main-d’œuvre (Utilisateurs gérés dans IAM Identity Center)	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées aux AWS CLI AWS SDK ou AWS aux API.	Suivez les instructions pour l’interface que vous souhaitez utiliser. • Pour le AWS CLI, voir Configuration du AWS CLI à utiliser AWS IAM Identity Center dans le guide de AWS Command Line Interface l'utilisateur. • Pour les AWS SDK, les outils et les AWS API, consultez la section Authentification IAM Identity Center dans le Guide de référence AWS des SDK et des outils.
IAM	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées aux AWS CLI AWS SDK ou AWS aux API.	Suivez les instructions de la section Utilisation d'informations d'identification temporaires avec AWS les ressources du Guide de l'utilisateur IAM.
IAM	(Non recommandé) Utilisez des informations d'identification à long terme pour signer les AWS CLI	Suivez les instructions pour l’interface que vous souhaitez utiliser.

Quel utilisateur a besoin d'un accès par programmation ?	Pour	Méthode
	demandes programmatiques adressées aux AWS SDK ou AWS aux API.	• Pour le AWS CLI, voir Authentification à l'aide des informations d'identification utilisateur IAM dans le Guide de l'AWS Command Line Interface utilisateur. • Pour les AWS SDK et les outils, voir Authentifier à l'aide d'informations d'identification à long terme dans le Guide de AWS référence des SDK et des outils. • Pour les AWS API, consultez la section Gestion des clés d'accès pour les utilisateurs IAM dans le guide de l'utilisateur IAM.

AWS Cloud Map

AWS Cloud Map est un service de découverte de ressources cloud. Avec AWS Cloud Map, les clients peuvent définir des noms personnalisés pour les ressources des applications, telles que les tâches Amazon ECS, les instances Amazon EC2, les compartiments Amazon S3, les tables Amazon DynamoDB, les files d'attente Amazon SQS ou toute autre ressource cloud. Les clients peuvent ensuite utiliser ces noms personnalisés pour découvrir l'emplacement et les métadonnées des ressources cloud de leurs applications à l'aide du SDK AWS et de requêtes d'API authentifiées. Bien qu'AWS Cloud Map soit un service éligible à la loi HIPAA, aucun PHI ne doit être stocké dans aucun nom/attribut de ressource dans AWS Cloud Map, car il n'existe aucun support pour protéger ces données. AWS Cloud Map peut plutôt être utilisé pour découvrir les ressources du domaine client qui transmettent ou stockent des PHI.

AWS CloudFormation

AWS CloudFormation permet aux clients de créer et de provisionner des déploiements d'infrastructure AWS de manière prévisible et répétée. Il aide les clients à tirer parti des produits AWS tels qu'Amazon EC2, Amazon Elastic Block Store, Amazon SNS, Elastic Load Balancing et Auto Scaling pour créer des applications hautement fiables, hautement évolutives et économiques dans le cloud sans se soucier de créer et de configurer l'infrastructure AWS sous-jacente. AWS CloudFormation permet aux clients d'utiliser un fichier modèle pour créer et supprimer un ensemble de ressources en une seule unité (une pile).

AWS CloudFormation ne stocke, ne transmet ni ne traite lui-même les PHI. Il est plutôt utilisé pour créer et déployer des architectures qui utilisent d'autres services AWS susceptibles de stocker, de transmettre et/ou de traiter des PHI. Seuls les services éligibles à la loi HIPAA doivent être utilisés avec PHI. Reportez-vous aux entrées relatives à ces services dans ce livre blanc pour obtenir des conseils sur l'utilisation des PHI avec ces services. AWS CloudFormation utilise AWS CloudTrail pour enregistrer tous les appels d'API.

AWS CloudHSM

AWS CloudHSM est un module de sécurité matérielle (HSM) basé sur le cloud qui permet aux clients de générer et d'utiliser facilement leurs propres clés de chiffrement sur le cloud AWS. Avec CloudHSM, les clients peuvent gérer leurs propres clés de chiffrement à l'aide de HSM validés par la norme FIPS 140-2 de niveau 3. CloudHSM offre aux clients la flexibilité nécessaire pour intégrer leurs applications à l'aide d'API standard ouvertes, telles que les bibliothèques PKCS #11, Java Cryptography Extensions (JCE) et Microsoft CryptoNG (CNG).

CloudHSM est également conforme aux normes et permet aux clients d'exporter toutes leurs clés vers la plupart des autres HSM disponibles dans le commerce. Tout comme AWS CloudHSM le service de gestion des clés d'une appliance matérielle, il n'est pas en mesure de stocker ou de transmettre des PHI. Les clients ne doivent pas stocker de PHI dans des balises (métadonnées). Aucune autre directive particulière n'est requise.

AWS CloudTrail

AWS CloudTrail est un service qui permet la gouvernance, la conformité, l'audit opérationnel et l'audit des risques des comptes AWS. Les clients peuvent ainsi enregistrer, surveiller en permanence et conserver l'activité de leur compte liée aux actions menées au sein de leur infrastructure AWS. CloudTrail CloudTrail fournit un historique des événements relatifs à l'activité de leur compte AWS, y

compris les actions entreprises par le biais des kits SDK AWS Console de gestion AWS, des outils de ligne de commande et d'autres services AWS. Cet historique des événements simplifie l'analyse de sécurité, le suivi des modifications des ressources et le dépannage.

AWS CloudTrail est activé pour être utilisé avec tous les comptes AWS et peut être utilisé pour la journalisation des audits, comme l'exige le BAA AWS. Des sentiers spécifiques doivent être créés à l'aide de la CloudTrail console ou de l'interface de ligne de commande AWS. CloudTrail chiffre tout le trafic en transit et au repos lorsqu'un Trail chiffré est créé. Une trace cryptée doit être créée lorsqu'il est possible de consigner des PHI.

Par défaut, un Trail chiffré stocke les entrées dans Amazon S3 à l'aide du chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3). Si une gestion supplémentaire des clés est souhaitée, elle peut également être configurée avec AWS KMS-managed keys (SSE-KMS). Comme CloudTrail c'est la destination finale des entrées de journal AWS, et donc un composant essentiel de toute architecture qui gère les PHI, la validation de l'intégrité des fichiers CloudTrail journaux doit être activée et les fichiers de CloudTrail résumé associés doivent être revus périodiquement. Une fois activé, une affirmation positive indiquant que les fichiers journaux n'ont pas été modifiés ou altérés peut être établie.

AWS CodeBuild

AWS CodeBuild est un service de création entièrement géré dans le cloud. AWS CodeBuild compile le code source, exécute des tests unitaires et produit des artefacts prêts à être déployés. AWS CodeBuild utilise une AWS KMS clé pour chiffrer les artefacts de sortie de build. Une clé KMS doit être créée et configurée avant de créer des artefacts contenant des données PHI, des secrets/mots de passe, des certificats, etc. AWS CodeBuild utilisés AWS CloudTrail pour enregistrer tous les appels d'API.

AWS CodeDeploy

AWS CodeDeploy est un service de déploiement entièrement géré qui automatise les déploiements de logiciels vers divers services informatiques, notamment Amazon EC2 AWS Fargate, AWS Lambda, et les serveurs sur site. Les clients ont l' AWS CodeDeploy habitude de lancer rapidement de nouvelles fonctionnalités de charge de travail conteneurisée et de gérer la complexité de la mise à jour des applications.

AWS CodeDeploy prend en charge le chiffrement côté serveur (SSE-S3) pour les artefacts de déploiement et le chiffrement TLS pour les données en transit entre le service et l'agent. Les clients

peuvent utiliser Amazon CloudWatch Events pour suivre les déploiements et AWS CloudTrail capturer les appels d'API adressés à AWS CodeDeploy.

AWS CodeCommit

AWS CodeCommit est un service de contrôle de source géré, sécurisé et hautement évolutif qui héberge des référentiels Git privés. AWS CodeCommit élimine la nécessité pour les clients de gérer leur propre système de contrôle de source ou de se soucier de la mise à l'échelle de son infrastructure.

AWS CodeCommit chiffre tout le trafic et les informations stockées pendant le transport et au repos. Par défaut, lorsqu'un référentiel est créé dans ce référentiel AWS CodeCommit, une clé gérée par AWS est créée avec ce référentiel AWS KMS et n'est utilisée que par celui-ci pour chiffrer toutes les données stockées au repos. AWS CodeCommit utilise AWS CloudTrail pour enregistrer tous les appels d'API.

AWS CodePipeline

AWS CodePipeline est un service de livraison continue entièrement géré qui aide les clients à automatiser les pipelines de publication des clients pour des mises à jour rapides et fiables des applications et de l'infrastructure. Le pipeline de flux de travail utilisé par les clients pour permettre AWS CodePipeline aux chercheurs de traiter automatiquement les données des essais cliniques, les résultats de laboratoire et les données génomiques ne sont que quelques exemples de pipeline de flux de travail utilisés par les clients.

AWS CodePipeline prend en charge le chiffrement côté serveur (SSE-S3 et SSE-KMS) pour les artefacts de code et le chiffrement TLS pour les données en transit entre le service et l'agent. Les clients peuvent utiliser Amazon CloudWatch Events pour suivre les modifications du pipeline et AWS CloudTrail pour capturer les appels d'API vers AWS CodePipeline.

AWS Config

AWS Config fournit une vue détaillée des ressources associées au compte AWS d'un client, notamment de leur configuration, de leur relation entre elles et de l'évolution des configurations et de leurs relations au fil du temps.

AWS Config ne peut pas être utilisé lui-même pour stocker ou transmettre des données PHI.

Il peut plutôt être utilisé pour surveiller et évaluer les architectures créées avec d'autres services AWS, y compris les architectures qui gèrent les PHI, afin de déterminer si elles restent conformes à l'objectif de conception prévu. Les architectures qui gèrent les PHI ne doivent être créées qu'avec des services éligibles à la loi HIPAA. AWS Config utilise AWS CloudTrail pour enregistrer tous les résultats.

AWS Data Exchange

AWS Data Exchange facilite la recherche, l'abonnement et l'utilisation de données tierces dans le cloud. Une fois abonnés à un produit de données, les clients peuvent utiliser l'API AWS Data Exchange pour charger des données directement dans Amazon S3, puis les analyser à l'aide d'un large éventail de services d'analyse et d'apprentissage automatique AWS. Pour les fournisseurs de données, AWS Data Exchange permet d'atteindre facilement les millions de clients AWS qui migrent vers le cloud en éliminant le besoin de créer et de maintenir une infrastructure pour le stockage, la livraison, la facturation et les droits des données.

AWS Data Exchange chiffre toujours tous les produits de données stockés dans le service au repos sans nécessiter de configuration supplémentaire. Ce chiffrement est automatiquement effectué via une clé KMS gérée par le service. AWS Data Exchange utilise le protocole TLS (Transport Layer Security) et le chiffrement côté client pour le chiffrement en transit. La communication avec AWS Data Exchange se fait toujours via HTTPS, de sorte que les données du client sont toujours cryptées pendant le transfert. Ce chiffrement est configuré par défaut lorsque les clients utilisent AWS Data Exchange. Pour plus d'informations, consultez la section Protection des données dans AWS Data Exchange.

AWS Data Exchange est intégré à AWS CloudTrail. AWS CloudTrail capture tous les appels aux API AWS Data Exchange sous forme d'événements, y compris les appels depuis la console AWS Data Exchange et les appels de code vers les opérations de l'API AWS Data Exchange. Certaines actions que les clients peuvent effectuer concernent uniquement la console. Il n'existe aucune API correspondante dans le SDK AWS ou dans l'interface de ligne de commande AWS. Il s'agit d'actions qui reposent sur des AWS Marketplace fonctionnalités, telles que la publication ou l'abonnement à un produit. AWS Data Exchange fournit des CloudTrail journaux pour un sous-ensemble de ces actions réservées à la console. Pour plus d'informations, consultez la section Journalisation des appels d'API AWS Data Exchange avec AWS CloudTrail.

Veuillez noter que toutes les offres utilisant AWS Data Exchange doivent respecter les directives de publication d'AWS Data Exchange et les FAQ AWS Data Exchange pour les AWS Marketplace

fournisseurs, qui limitent certaines catégories de données. Pour plus d'informations, consultez les FAQ d'AWS Data Exchange.

AWS Database Migration Service

AWS Database Migration Service (AWS DMS) aide les clients à migrer des bases de données vers AWS facilement et en toute sécurité. Les clients peuvent migrer leurs données vers et depuis les bases de données commerciales et open source les plus utilisées, telles qu'Oracle, MySQL et PostgreSQL. Ce service prend en charge les migrations homogènes, par exemple d'Oracle vers Oracle, mais aussi les migrations hétérogènes entre différentes plateformes de bases de données, par exemple d'Oracle vers PostgreSQL ou de MySQL vers Oracle.

Les bases de données exécutées sur site et migrées vers le cloud avec AWS DMS peuvent contenir des données PHI. AWS DMS chiffre les données en transit et lors du transfert des données en vue de leur migration finale vers la base de données cible sur AWS. AWS DMS chiffre le stockage utilisé par une instance de réplication et les informations de connexion du point de terminaison. Pour chiffrer le stockage utilisé par une instance de réplication, AWS DMS utilise une AWS KMS clé propre au compte AWS. Reportez-vous aux instructions relatives à la base de données cible appropriée pour vous assurer que les données restent cryptées une fois la migration terminée. AWS DMS enregistre CloudTrail tous les appels d'API.

AWS DataSync

AWS DataSync est un service de transfert en ligne qui simplifie, automatise et accélère le transfert de données entre le stockage sur site et AWS. Les clients peuvent utiliser AWS DataSync pour connecter leurs sources de données à Amazon S3 ou Amazon EFS. Les clients doivent s'assurer qu'Amazon S3 et Amazon EFS sont configurés conformément aux directives. Par défaut, les données des clients sont cryptées en transit à l'aide du protocole TLS 1.2. Pour plus d'informations sur le chiffrement et AWS DataSync, consultez la section DataSyncFonctionnalités d'AWS. Les clients peuvent surveiller leur DataSync activité en utilisant AWS CloudTrail. Pour plus d'informations sur la journalisation avec CloudTrail, consultez la section Journalisation des appels DataSync d'API AWS avec AWS CloudTrail.

AWS Directory Service

AWS Directory Service pour Microsoft AD

AWS Directory Service pour Microsoft Active Directory (Enterprise Edition), également connu sous le nom d'AWS Microsoft AD, permet aux charges de travail sensibles aux annuaires et aux ressources AWS d'utiliser Active Directory géré dans le cloud AWS. AWS Microsoft AD stocke le contenu du répertoire (y compris le contenu contenant des PHI) dans des volumes Amazon Elastic Block Store chiffrés à l'aide de clés de chiffrement gérées par AWS. Pour en savoir plus, consultez la page Chiffrement Amazon EBS.

Les données en transit vers et depuis les clients Active Directory sont chiffrées lorsqu'elles transitent via le protocole LDAP (Lightweight Directory Access Protocol) sur le réseau Amazon Virtual Private Cloud (VPC) du client. Si un client Active Directory réside dans un réseau local, le trafic est acheminé vers le VPC du client par un lien réseau privé virtuel ou AWS Direct Connect un lien.

Amazon Cloud Directory

Amazon Cloud Directory permet aux clients de créer des annuaires cloud natifs flexibles pour organiser des hiérarchies de données selon plusieurs dimensions. Les clients peuvent également créer des annuaires pour divers cas d'utilisation, tels que des organigrammes, des catalogues de cours et des registres d'appareils. Par exemple, les clients peuvent créer un organigramme qui peut être parcouru dans des hiérarchies distinctes pour la structure hiérarchique, l'emplacement et le centre de coûts. Amazon Cloud Directory chiffre automatiquement les données au repos et en transit à l'aide de clés de chiffrement 256 bits gérées par le AWS Key Management Service ().AWS KMS

AWS Elastic Beanstalk

Les clients peuvent ainsi déployer et gérer rapidement des applications dans le cloud AWS sans avoir à se renseigner sur l'infrastructure qui exécute ces applications. AWS Elastic Beanstalk Les clients peuvent simplement télécharger du code et gérer AWS Elastic Beanstalk automatiquement le déploiement, qu'il s'agisse du provisionnement des capacités, de l'équilibrage de charge, du dimensionnement automatique ou de la surveillance de l'état de santé des applications. Dans le même temps, les clients gardent le contrôle total des ressources AWS qui alimentent leur application et peuvent accéder aux ressources sous-jacentes à tout moment.

AWS Elastic Beanstalk ne stocke, ne transmet ni ne traite lui-même les PHI. Les clients peuvent plutôt l'utiliser pour créer et déployer des architectures avec d'autres services AWS susceptibles de

stocker, de transmettre et/ou de traiter des PHI. Les clients doivent s'assurer, lorsqu'ils choisissent les services déployés par, de n'utiliser que les services éligibles AWS Elastic Beanstalk à la loi HIPAA avec PHI. Reportez-vous aux entrées relatives à ces services dans ce livre blanc pour obtenir des conseils sur l'utilisation des PHI avec ces services.

Les clients ne doivent pas inclure de PHI dans les champs de forme libre AWS Elastic Beanstalk tels que le champ Nom. AWS Elastic Beanstalk utilise AWS CloudTrail pour enregistrer tous les appels d'API.

AWS Elastic Disaster Recovery

AWS Elastic Disaster Recovery (AWS DRS) minimise les temps d'arrêt et les pertes de données grâce à une restauration rapide et fiable des applications sur site et dans le cloud à l'aide d'un stockage abordable, d'un calcul et point-in-time d'une restauration minimaux.

Les clients peuvent configurer AWS Elastic Disaster Recovery sur leurs serveurs sources afin de lancer une réplication sécurisée des données. Leurs données sont répliquées sur un sous-réseau de zone de transit de votre compte AWS, dans la région AWS sélectionnée. La conception de la zone de transit réduit les coûts en utilisant un stockage abordable et des ressources de calcul minimales pour assurer une réplication continue. Les données des clients répliquées par AWS Elastic Disaster Recovery sont chiffrées en transit à l'aide du protocole TLS 1.2 et sont transférées directement de leurs serveurs sources vers leur VPC. Les clients peuvent tirer parti d'une connectivité privée telle qu'AWS Direct Connect ou un VPN pour configurer l'itinéraire de réplication. Les données des clients peuvent également être chiffrées au repos sur AWS à l'aide du chiffrement Amazon EBS.

Les clients peuvent effectuer des tests sans interruption pour confirmer que la mise en œuvre est terminée. Pendant le fonctionnement normal, maintenez l'état de préparation en surveillant la réplication et en effectuant régulièrement des exercices de restauration et de restauration sans interruption de service. Si les clients ont besoin de récupérer des applications, ils peuvent lancer des instances de restauration sur AWS en quelques minutes, en utilisant l'état up-to-date du serveur le plus élevé ou à un moment antérieur. Une fois que les applications des clients sont exécutées sur AWS, ils peuvent choisir de les conserver ou de lancer la réplication des données vers leur site principal une fois le problème résolu. Les clients peuvent revenir sur leur site principal dès qu'ils sont prêts.

AWS Fargate

AWS Fargate est une technologie qui permet aux clients d'exécuter des conteneurs sans avoir à gérer de serveurs ou de clusters. Ainsi AWS Fargate, les clients n'ont plus à provisionner, configurer et dimensionner des clusters de machines virtuelles pour exécuter des conteneurs. Il n'est donc plus nécessaire de choisir les types de serveurs, de décider quand dimensionner les clusters ou d'optimiser le regroupement des clusters. AWS Fargate les clients n'ont plus besoin d'interagir avec des serveurs ou des clusters ou de penser à ces derniers. Avec Fargate, les clients se concentrent sur la conception et le développement de leurs applications plutôt que sur la gestion de l'infrastructure qui les exécute.

Fargate ne nécessite aucune configuration supplémentaire pour fonctionner avec les charges de travail qui traitent des PHI. Les clients peuvent exécuter des charges de travail de conteneurs sur Fargate à l'aide de services d'orchestration de conteneurs tels qu'Amazon ECS. Fargate gère uniquement l'infrastructure sous-jacente et ne fonctionne pas avec ou sur les données de la charge de travail orchestrée. Conformément aux exigences de la loi HIPAA, les PHI doivent toujours être chiffrés lorsqu'ils sont en transit ou au repos lorsqu'ils sont accessibles par des conteneurs lancés avec Fargate. Différents mécanismes de chiffrement au repos sont disponibles avec chaque option de stockage AWS décrite dans ce paper. Pour obtenir des informations supplémentaires sur la sécurité et la configuration HIPAA, consultez le livre blanc Architecting for HIPAA Security and Compliance on Amazon EKS.

AWS Firewall Manager

AWS Firewall Manager est un service de gestion de la sécurité qui permet aux clients de configurer et de gérer de manière centralisée les règles de pare-feu pour les comptes clients et les applications dans AWS Organizations. À mesure que de nouvelles applications sont créées, Firewall Manager facilite la mise en conformité des nouvelles applications et ressources en appliquant un ensemble commun de règles de sécurité. Les clients disposent désormais d'un service unique pour établir des règles de pare-feu, créer des politiques de sécurité et les appliquer de manière cohérente et hiérarchique sur l'ensemble de leur infrastructure, à partir d'un compte d'administrateur central.

AWS Firewall Manager est un service d'orchestration qui ne traite, ne stocke ni ne transmet directement les données des utilisateurs. Le service ne chiffre pas le contenu du client, mais les services sous-jacents qui l' AWS Firewall Manager utilisent, tels que DynamoDB, cryptent les données utilisateur.

AWS Global Accelerator

AWS Global Accelerator est un service mondial d'équilibrage de charge qui améliore la disponibilité et la latence des applications multirégionales. Pour garantir que le PHI reste crypté en transit et au repos pendant son utilisation AWS Global Accelerator, les architectures équilibrées par Global Accelerator doivent utiliser un protocole crypté, tel que HTTPS ou SSL/TLS. Reportez-vous aux instructions relatives à Amazon EC2, à Elastic Load Balancing et aux autres services AWS afin de mieux comprendre les options de chiffrement disponibles pour les ressources principales. AWS Global Accelerator utilise AWS CloudTrail pour enregistrer tous les appels d'API.

AWS Glue

AWS Glue est un service ETL (extraction, transformation et chargement) entièrement géré qui permet aux clients de classer leurs données de manière simple et rentable, de les nettoyer, de les enrichir et de les déplacer de manière fiable entre différents magasins de données. Afin de garantir le chiffrement des données contenant des PHI pendant leur transit, vous AWS Glue devez être configuré pour utiliser des connexions JDBC aux magasins de données avec SSL/TLS. En outre, pour maintenir le chiffrement pendant le transit, le paramètre de chiffrement côté serveur (SSE-S3) doit être transmis en tant que paramètre aux tâches ETL exécutées avec. AWS Glue Toutes les données stockées au repos dans le catalogue de données de AWS Glue sont cryptées à l'aide de clés gérées AWS KMS lorsque le chiffrement est activé lors de la création d'un objet du catalogue de données. AWS Glue utilise CloudTrail pour enregistrer tous les appels d'API.

AWS Glue DataBrew

AWS Glue DataBrew est un service de préparation visuelle des données entièrement géré qui permet aux analystes de données et aux data scientists de nettoyer et de normaliser facilement les données afin de les préparer à des fins d'analyse et d'apprentissage automatique. Afin de garantir le chiffrement des données contenant des PHI pendant leur transit, vous DataBrew devez être configuré pour utiliser des connexions JDBC aux magasins de données avec SSL/TLS. Lorsque vous vous connectez à des sources de données JDBC, DataBrew utilisez les paramètres de votre connexion AWS Glue, notamment l'option « Exiger une connexion SSL ». En outre, pour maintenir le chiffrement au repos dans les compartiments S3, le paramètre de chiffrement côté serveur (SSE-S3 ou SSE-KMS) doit être transmis en tant que paramètre aux tâches. DataBrew

AWS IoT Core et AWS IoT Device Management

AWS IoT Établissez et AWS IoT Device Management assurez une communication bidirectionnelle sécurisée entre les appareils connectés à Internet, tels que les capteurs, les actionneurs, les microcontrôleurs intégrés ou les appareils intelligents, et le cloud AWS. AWS IoT Core et AWS IoT Device Management peut désormais accueillir des appareils qui transmettent des données contenant des PHI. Toutes les communications avec AWS IoT Core sont cryptées à l'aide du protocole TLS. AWS IoT Device Management AWS IoT Core et AWS IoT Device Management utilisation AWS CloudTrail pour enregistrer tous les appels d'API.

AWS IoT Greengrass

AWS IoT Greengrass permet aux clients d'exécuter des fonctionnalités locales de calcul, de messagerie, de mise en cache des données, de synchronisation et d'inférence ML pour les appareils connectés de manière sécurisée. AWS IoT Greengrass utilise des certificats X.509, des abonnements gérés, des AWS IoT politiques, ainsi que des politiques et des rôles IAM pour garantir la sécurité des applications Greengrass du client. AWS IoT Greengrass utilise le modèle de sécurité du AWS IoT transport pour chiffrer les communications avec le cloud à l'aide du protocole TLS. De plus, AWS IoT Greengrass les données sont cryptées lorsqu'elles sont au repos (dans le cloud). Pour plus d'informations sur la sécurité de Greengrass, consultez la section Présentation de la AWS IoT Greengrass sécurité.

Les clients peuvent enregistrer les actions de AWS IoT Greengrass l'API à l'aide de AWS CloudTrail. Pour plus d'informations, consultez la section Journalisation des appels d' AWS IoT Greengrass API avec AWS CloudTrail.

AWS Lambda

AWS Lambda permet aux clients d'exécuter du code sans provisionner ni gérer eux-mêmes les serveurs. AWS Lambda utilise un parc informatique d'instances Amazon Elastic Compute Cloud (Amazon EC2) réparties dans plusieurs zones de disponibilité d'une région, ce qui garantit la haute disponibilité, la sécurité, les performances et l'évolutivité de l'infrastructure AWS.

Pour garantir que le PHI reste crypté pendant son utilisation AWS Lambda, les connexions aux ressources externes doivent utiliser un protocole crypté tel que HTTPS ou SSL/TLS. Par exemple, lorsque S3 est accessible à partir d'une procédure Lambda, il doit être traité avec https://bucket.s3-aws-region.amazonaws.com.

Si un PHI est mis au repos ou inactif dans une procédure en cours d'exécution, il doit être chiffré côté client ou côté serveur avec des clés obtenues à partir de ou. AWS KMS AWS CloudHSM Suivez les instructions associées pour Amazon API Gateway lorsque vous déclenchez AWS Lambda des fonctions via le service. Lorsque vous utilisez des événements provenant d'autres services AWS pour déclencher AWS Lambda des fonctions, les données des événements ne doivent pas contenir (en elles-mêmes) de PHI. Par exemple, lorsqu'une procédure Lambda est déclenchée par un événement S3, tel que l'arrivée d'un objet dans S3, le nom de l'objet transmis à Lambda ne doit pas comporter de PHI, bien que l'objet lui-même puisse contenir de telles données.

AWS Managed Services

AWS Managed Services assure la gestion continue des infrastructures AWS. La mise en œuvre des meilleures pratiques pour maintenir l'infrastructure d'un client AWS Managed Services contribue à réduire ses frais opérationnels et ses risques. AWS Managed Services automatise les activités courantes telles que les demandes de modification, la surveillance, la gestion des correctifs, la sécurité et les services de sauvegarde, et fournit des services de cycle de vie complet pour fournir, exécuter et soutenir les infrastructures.

Les clients peuvent l'utiliser AWS Managed Services pour gérer les charges de travail AWS qui fonctionnent avec des données contenant des PHI. L'utilisation de AWS Managed Services ne modifie pas les services AWS éligibles à l'utilisation avec PHI. L'outillage et l'automatisation fournis par AWS Managed Services ne peuvent pas être utilisés pour le stockage ou la transmission de PHI.

AWS OpsWorks pour Chef Automate

AWS OpsWorks for Chef Automate est un service de gestion de configuration entièrement géré qui héberge Chef Automate, un ensemble d'outils d'automatisation de Chef pour la gestion de l'infrastructure et des applications. Le service lui-même ne contient, ne transmet ni ne gère aucune information PHI ou sensible, mais les clients doivent s'assurer que toutes les ressources configurées par OpsWorks Chef Automate sont configurées conformément aux directives. Les appels d'API sont capturés avec AWS CloudTrail. Pour plus d'informations, consultez Logging AWS OpsWorks Stacks API Calls with AWS CloudTrail.

AWS OpsWorks pour Puppet Enterprise

AWS OpsWorks for Puppet Enterprise est un service de gestion de configuration entièrement géré qui héberge Puppet Enterprise, un ensemble d'outils d'automatisation de Puppet pour la gestion

de l'infrastructure et des applications. Le service lui-même ne contient, ne transmet ni ne gère aucune information PHI ou sensible, mais les clients doivent s'assurer que toutes les ressources configurées par OpsWorks pour Puppet Enterprise sont configurées conformément aux directives. Les appels d'API sont capturés avec AWS CloudTrail. Pour plus d'informations, consultez Logging AWS OpsWorks Stacks API Calls with AWS CloudTrail.

AWS OpsWorks Empilez

AWS OpsWorks Stacks fournit un moyen simple et flexible de créer et de gérer des piles et des applications. Les clients peuvent utiliser AWS OpsWorks Stacks pour déployer et surveiller les applications qu'ils contiennent.

AWS OpsWorks Stacks chiffre tout le trafic en transit. Cependant, les sacs de données chiffrés (un mécanisme de stockage de données Chef) ne sont pas disponibles et tous les actifs devant être stockés de manière sécurisée, tels que les PHI, les secrets/mots de passe, les certificats, etc., doivent être stockés dans un compartiment chiffré dans Amazon S3. AWS OpsWorks Stack AWS CloudTrail enregistre tous les appels d'API.

AWS Organizations

AWS Organizations aide les clients à gérer et à gouverner leur environnement de manière centralisée à mesure qu'ils développent et font évoluer leurs ressources AWS. Ils peuvent ainsi créer par programmation de nouveaux comptes AWS et allouer des ressources, regrouper des comptes pour organiser leurs flux de travail, appliquer des politiques aux comptes ou aux groupes à des fins de gouvernance et simplifier la facturation en utilisant un mode de paiement unique pour tous leurs comptes. AWS Organizations

En outre, AWS Organizations il est intégré à d'autres services AWS afin que les clients puissent définir des configurations centralisées, des mécanismes de sécurité, des exigences d'audit et le partage des ressources entre les comptes de leur organisation. AWS Organizations est disponible pour tous les clients AWS sans frais supplémentaires.

AWS Organizations est un service d'orchestration qui ne traite, ne stocke ni ne transmet directement les données des utilisateurs. Le service ne chiffre pas le contenu des clients, mais les services sous-jacents qui y sont lancés chiffrent AWS Organizations les données des utilisateurs.
AWS Organizations est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un service AWS dans AWS Organizations.

AWS RoboMaker

AWS RoboMaker permet aux clients d'exécuter du code dans le cloud pour le développement d'applications et fournit un service de simulation robotique pour accélérer les tests d'applications. AWS fournit RoboMaker également un service de gestion de flotte robotique pour le déploiement, la mise à jour et la gestion d'applications à distance.

Le trafic réseau contenant des PHI doit chiffrer les données en transit. Toutes les communications de gestion avec le serveur de simulation se font via le protocole TLS, et les clients doivent utiliser des mécanismes de chiffrement de transport standard ouverts pour les connexions aux autres services AWS. AWS s'intègre RoboMaker également CloudTrail à un compartiment Amazon S3 spécifique pour consigner tous les appels d'API.

RoboMaker Les journaux AWS ne contiennent pas de PHI et les volumes EBS utilisés par le serveur de simulation sont chiffrés. Lors du transfert de données susceptibles de contenir des PHI vers d'autres services, tels qu'Amazon S3, les clients doivent suivre les instructions du service de réception concernant le stockage des PHI. Pour les déploiements sur des robots, les clients doivent s'assurer que le chiffrement des données en transit et au repos est conforme à leur interprétation des directives.

Métriques du SDK AWS

Les entreprises clientes peuvent utiliser l' CloudWatch agent AWS associé à AWS SDK Metrics for Enterprise Support (SDK Metrics) pour collecter des métriques à partir des SDK AWS sur leurs hôtes et leurs clients. Ces statistiques sont partagées avec AWS Enterprise Support. Les métriques du SDK peuvent aider les clients à collecter des métriques et des données de diagnostic pertinentes concernant les connexions de leur application aux services AWS sans ajouter d'instrumentation personnalisée à leur code, et réduisent le travail manuel nécessaire pour partager les journaux et les données avec AWS Support.

Notez que SDK Metrics n'est disponible que pour les clients AWS disposant d'un abonnement Enterprise Support. Les clients peuvent utiliser les métriques du SDK avec n'importe quelle application qui appelle directement les services AWS et qui a été créée à l'aide d'un SDK AWS dont la version est répertoriée dans la documentation AWS Metrics.

SDK Metrics surveille les appels effectués par le SDK AWS et utilise l' CloudWatch agent exécuté dans le même environnement qu'une application cliente.

L' CloudWatch agent chiffre les données en transit entre la machine locale et la livraison dans le groupe de journaux de destination. Le groupe de journaux peut être configuré pour être chiffré en suivant les instructions de la section Chiffrer les données du journal dans les CloudWatch journaux à l'aide AWS KMS.

AWS Secrets Manager

AWS Secrets Manager est un service AWS qui permet aux clients de gérer plus facilement les « secrets ». Les secrets peuvent être des informations d'identification de base de données, des mots de passe, des clés d'API tierces et même du texte arbitraire. AWS Secrets Manager peut être utilisé pour stocker des données PHI si ces informations sont contenues dans des « secrets ». Tous les secrets stockés par AWS Secrets Manager sont chiffrés au repos à l'aide du système de gestion des clés (KMS) AWS. Les utilisateurs peuvent sélectionner la AWS KMS clé utilisée lors de la création d'un nouveau secret. Si aucune clé n'est sélectionnée, la clé par défaut du compte sera utilisée. AWS Secrets Manager AWS CloudTrail enregistre tous les appels d'API.

AWS Security Hub CSPM

AWS Security Hub CSPM collecte et consolide les résultats des services de sécurité AWS activés dans l'environnement d'un client, tels que les résultats de détection d'intrusion d'Amazon, les scans de vulnérabilité d'Amazon Inspector GuardDuty, les résultats de la politique relative aux compartiments Amazon S3 d'Amazon Macie, les ressources accessibles au public et multicomptes d'IAM Access Analyzer, et les ressources non couvertes par le WAF par. AWS Firewall Manager AWS Security Hub CSPM consolide également les résultats des solutions de sécurité intégrées du réseau de partenaires AWS (APN).

AWS Security Hub CSPM s'intègre à Amazon CloudWatch Events, permettant aux clients de créer des flux de travail de réponse et de correction personnalisés. Les clients peuvent facilement envoyer leurs résultats aux SIEM, aux outils de chat, aux systèmes de billetterie, aux outils SOAR (Security Orchestration Automation and Response) et aux plateformes de gestion des appels. Les actions de réponse et de correction peuvent être entièrement automatisées ou peuvent être déclenchées manuellement dans la console. Les clients peuvent également utiliser des documents et des AWS Lambda fonctions d' AWS Systems Manager automatisation pour créer des flux de travail de correction automatisés pouvant être initiés à partir de AWS Security Hub CSPM. AWS Step Functions

Pour garantir la protection des données, AWS Security Hub CSPM chiffre les données au repos et les données en transit entre les services des composants. Des auditeurs tiers évaluent la sécurité et

la conformité dans AWS Security Hub CSPM le cadre de plusieurs programmes de conformité AWS. AWS Security Hub CSPM fait partie des programmes de conformité SOC, ISO, PCI et HIPAA d'AWS.

AWS Server Migration Service

AWS Server Migration Service (AWS SMS) automatise la migration des machines virtuelles VMware vSphere ou Microsoft Hyper-V/SCVMM sur site vers le cloud AWS. AWS SMS réplique de manière incrémentielle les machines virtuelles du serveur sous forme d'Amazon Machine Images (AMI) hébergées dans le cloud, prêtes à être déployées sur Amazon EC2.

Les serveurs exécutés sur site et migrés vers le cloud avec (AWS SMS) peuvent contenir des données PHI. AWS SMS chiffre les données en transit et lorsque les images des machines virtuelles du serveur sont préparées pour être placées définitivement sur EC2. Reportez-vous aux instructions relatives à EC2 et à la configuration de volumes de stockage chiffrés lors de la migration d'une machine virtuelle de serveur contenant des PHI avec AWS SMS. AWS SMS enregistre CloudTrail tous les appels d'API.

AWS Serverless Application Repository

Le AWS Serverless Application Repository (SAR) est un référentiel géré pour les applications sans serveur. Il permet aux équipes, aux organisations et aux développeurs individuels de stocker et de partager des applications réutilisables, ainsi que d'assembler et de déployer facilement des architectures sans serveur de nouvelles manières puissantes. Les applications sont des CloudFormation modèles qui contiennent des définitions de l'infrastructure de l'application et des fichiers binaires compilés du code de AWS Lambda fonction de l'application.

Bien qu'il soit possible pour les applications incluses de AWS Serverless Application Repository traiter les PHI, elles ne le feront qu'après avoir été déployées sur le compte d'un client et non dans le cadre du SAR lui-même. Le AWS Serverless Application Repository chiffre les fichiers que les clients téléchargent, y compris les packages de déploiement et les archives de couches. Pour les données en transit, le protocole TLS est AWS Serverless Application Repository utilisé pour chiffrer les données entre le service et l'agent. AWS Serverless Application Repository est intégré à AWS CloudTrail, qui est un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un service AWS dans le AWS Serverless Application Repository.

Service Catalog

Service Catalog permet aux administrateurs informatiques de créer, de gérer et de distribuer des portefeuilles de produits approuvés aux utilisateurs finaux, qui peuvent ensuite accéder aux produits dont ils ont besoin sur un portail personnalisé. Service Catalog est utilisé pour cataloguer, partager et déployer des solutions en libre-service sur AWS et ne peut pas être utilisé pour stocker, transmettre ou traiter des PHI. Les PHI ne doivent pas être placés dans les métadonnées des éléments du Service Catalog ni dans les descriptions des éléments. Service Catalog AWS CloudTrail enregistre tous les appels d'API.

AWS Shield

AWS Shield est un service géré de protection par déni de service distribué (DDoS) qui protège les applications Web exécutées sur AWS. AWS Shield fournit une détection permanente et des mesures d'atténuation automatiques en ligne qui minimisent les temps d'arrêt et la latence des applications. Il n'est donc pas nécessaire de s'engager pour bénéficier de la protection contre les attaques AWS Support DDoS.

AWS Shield ne peut pas être utilisé pour stocker ou transmettre des PHI, mais peut être utilisé pour protéger les applications Web qui fonctionnent avec des PHI. Ainsi, aucune configuration particulière n'est requise lors de l'engagement AWS Shield.

Tous les clients AWS bénéficient des protections automatiques de AWS Shield Standard, sans frais supplémentaires. AWS Shield Standard se défend contre les attaques DDoS les plus courantes et fréquentes au niveau du réseau et de la couche de transport qui ciblent leur site Web ou leurs applications. Pour bénéficier de niveaux de protection supérieurs contre les attaques ciblant leurs applications Web exécutées sur les ressources Elastic Load Balancing (ELB) CloudFront, Amazon et Amazon Route 53, les clients peuvent s'abonner à AWS Shield Advanced.

AWS Snowball Edge

Avec AWS Snowball Edge (Snowball), les clients peuvent transférer des centaines de téraoctets ou de pétaoctets de données entre leurs centres de données sur site et Amazon Simple Storage Service (Amazon S3). Les PHI stockés AWS Snowball Edge doivent être chiffrés au repos conformément au guide. Lors de la création d'une tâche d'importation, les clients doivent spécifier l'ARN de la AWS KMS clé à utiliser pour protéger les données dans le Snowball. En outre, lors de la création de la tâche d'importation, les clients doivent choisir un compartiment S3 de destination conforme aux normes de chiffrement définies dans le guide.

Alors que Snowball ne prend actuellement pas en charge le chiffrement côté serveur avec des clés AWS KMS gérées (SSE-KMS) ou le chiffrement côté serveur avec des clés fournies par le client (SSE-C), Snowball prend en charge le chiffrement côté serveur avec des clés de chiffrement gérées par Amazon S3 (SSE-S3). Pour plus d'informations, consultez Protection des données à l'aide du chiffrement côté serveur avec les clés de chiffrement Amazon S3 (SSE-S3).

Les clients peuvent également utiliser la méthodologie de chiffrement de leur choix pour chiffrer les PHI avant d'y stocker les AWS Snowball Edge données.

Actuellement, les clients peuvent utiliser l' AWS Snowball Edge appareil standard dans le cadre de notre BAA.

AWS Snowball Edge Bord

AWS Snowball Edge Edge se connecte aux applications et infrastructures clients existantes à l'aide d'interfaces de stockage standard, rationalisant ainsi le processus de transfert de données et minimisant la configuration et l'intégration. Snowball Edge peut se regrouper pour former un niveau de stockage local et traiter les données des clients sur site, aidant ainsi les clients à garantir que leurs applications continuent de fonctionner même lorsqu'ils ne sont pas en mesure d'accéder au cloud.

Pour garantir que les PHI restent chiffrés lorsqu'ils utilisent Snowball Edge, les clients doivent s'assurer d'utiliser un protocole de connexion crypté tel que HTTPS ou SSL/TLS lorsqu'ils utilisent des AWS Lambda procédures basées sur la transmission de PHI vers/depuis des ressources externes AWS IoT Greengrass à Snowball Edge. En outre, les PHI doivent être chiffrés lorsqu'ils sont stockés sur les volumes locaux de Snowball Edge, soit via un accès local, soit via NFS. Le chiffrement est automatiquement appliqué aux données placées dans Snowball Edge à l'aide de la console de gestion Snowball et de l'API pour le transport en masse vers S3. Pour plus d'informations sur le transport de données vers S3, consultez les instructions associées pourthe section called “AWS Snowball Edge”.

AWS Step Functions

AWS Step Functions facilite la coordination des composants des applications distribuées et des microservices à l'aide de flux de travail visuels. AWS Step Functions n'est pas en mesure de stocker, de transmettre ou de traiter les PHI. Le PHI ne doit pas être placé dans les métadonnées pour AWS Step Functions ou dans une définition de tâche ou de machine à états. AWS Step Functions utilise AWS CloudTrail pour enregistrer tous les appels d'API.

AWS Storage Gateway

AWS Storage Gateway est un service de stockage hybride qui permet aux applications sur site des clients d'utiliser de manière fluide le stockage dans le cloud AWS. La passerelle utilise des protocoles de stockage standard ouverts pour connecter les applications de stockage et les flux de travail existants aux services de stockage dans le cloud AWS pour une interruption minimale des processus.

Passerelle de fichier

La passerelle de fichiers est un type de passerelle AWS Storage Gateway qui prend en charge une interface de fichiers dans Amazon S3 et qui s'ajoute au volume basé sur des blocs et au stockage VTL actuels. La passerelle de fichiers utilise le protocole HTTPS pour communiquer avec S3 et stocke tous les objets chiffrés sur S3 en utilisant SSE-S3, par défaut, ou en utilisant le chiffrement côté client avec des clés stockées dans. AWS KMS Les métadonnées des fichiers, telles que les noms de fichiers, restent non chiffrées et ne doivent contenir aucun PHI.

Passerelle de volume

Volume Gateway fournit des volumes de stockage basés sur le cloud que les clients peuvent monter en tant que périphériques iSCSI (Internet Small Computer System Interface) à partir de serveurs d'applications sur site. Les clients doivent connecter des disques locaux en tant que tampons de téléchargement et cache à la machine virtuelle Volume Gateway conformément à leurs exigences internes en matière de conformité et de réglementation. Pour les PHI, il est recommandé que ces disques soient capables de fournir un chiffrement au repos. Les communications entre la machine virtuelle Volume Gateway et AWS sont chiffrées à l'aide du protocole TLS 1.2 afin de sécuriser les PHI pendant le transport.

Passerelle de bande

Tape Gateway fournit une interface VTL (bibliothèque de bandes virtuelles) aux applications de sauvegarde tierces exécutées sur site. Les clients doivent activer le chiffrement des données PHI dans l'application de sauvegarde tierce lors de la configuration d'une tâche de sauvegarde sur bande. Les communications entre la machine virtuelle Tape Gateway et AWS sont chiffrées à l'aide du protocole TLS 1.2 afin de sécuriser les PHI pendant le transport. Les clients utilisant l'une des configurations Storage Gateway avec PHI doivent activer la journalisation complète. Pour de plus amples informations, veuillez consulter la documentation relative à la présentation d' AWS Storage Gateway.

AWS Systems Manager

AWS Systems Manager est une interface unifiée qui permet aux clients de centraliser facilement les données opérationnelles, d'automatiser les tâches sur l'ensemble de leurs ressources AWS et de réduire le temps nécessaire pour détecter et résoudre les problèmes opérationnels dans leur infrastructure. Systems Manager fournit une vue complète des performances et de la configuration de l'infrastructure d'un client, simplifie la gestion des ressources et des applications, et facilite le fonctionnement et la gestion de leur infrastructure à grande échelle.

Lorsqu'ils transmettent des données susceptibles de contenir des PHI à d'autres services, tels qu'Amazon S3, les clients doivent suivre les instructions du service de réception concernant le stockage des PHI. Les clients ne doivent pas inclure de PHI dans les métadonnées ou les identifiants, tels que les noms de documents et les noms de paramètres.

AWS Transfer for SFTP

AWS Transfer for SFTP fournit un accès au protocole SFTP (Secure File Transfer Protocol) aux ressources S3 d'un client. Les clients disposent d'un serveur virtuel accessible via le protocole SFTP standard sur un point de terminaison de service régional. Du point de vue du client AWS et du client SFTP, la passerelle SFTP ressemble à un serveur SFTP standard à haute disponibilité. Bien que le service lui-même ne stocke, ne traite ni ne transmette de PHI, les ressources auxquelles le client accède sur Amazon S3 doivent être configurées conformément au guide. Les clients peuvent également l'utiliser AWS CloudTrail pour consigner les appels d'API effectués vers AWS Transfer for SFTP.

AWS WAF — Pare-feu pour applications Web

AWS WAF est un pare-feu d'applications Web qui aide à protéger les applications Web des clients contre les exploits Web courants susceptibles d'affecter la disponibilité des applications, de compromettre la sécurité ou de consommer des ressources excessives. Les clients peuvent placer AWS WAF entre leurs applications Web hébergées sur AWS qui fonctionnent avec ou échangent des PHI, et leurs utilisateurs finaux. Comme pour la transmission de tout PHI sur AWS, les données contenant des PHI doivent être cryptées pendant leur transit. Reportez-vous aux instructions destinées à Amazon EC2 pour mieux comprendre les options de chiffrement disponibles.

AWS X-Ray

AWS X-Ray est un service qui collecte des données sur les demandes traitées par l'application d'un client et fournit des outils que celui-ci peut utiliser pour visualiser, filtrer et mieux comprendre ces données afin d'identifier les problèmes et les opportunités d'optimisation. Pour toute demande retracée envoyée à l'application d'un client, celui-ci peut consulter des informations détaillées non seulement sur la demande et la réponse, mais également sur les appels que son application envoie aux ressources AWS, aux microservices, aux bases de données et aux API Web HTTP en aval. AWS X-Ray ne doit pas être utilisé pour stocker ou traiter des PHI. Les informations transmises vers et depuis AWS X-Ray sont cryptées par défaut. Lors de l'utilisation AWS X-Ray, ne placez aucun PHI dans les annotations ou les métadonnées des segments.

Elastic Load Balancing

Les clients peuvent utiliser Elastic Load Balancing pour terminer et traiter des sessions contenant des PHI. Les clients peuvent choisir entre le Classic Load Balancer ou l'Application Load Balancer. Étant donné que tout le trafic réseau contenant des PHI doit être chiffré en transit end-to-end, les clients ont la possibilité de mettre en œuvre deux architectures différentes :

Les clients peuvent mettre fin au protocole HTTPS, au HTTP/2 via TLS (pour les applications) ou au protocole SSL/TLS sur Elastic Load Balancing en créant un équilibreur de charge qui utilise un protocole chiffré pour les connexions. Cette fonctionnalité permet le chiffrement du trafic entre l'équilibreur de charge et les clients qui initient des sessions HTTPS, HTTP/2 sur TLS ou SSL/TLS, ainsi que pour les connexions entre l'équilibreur de charge et les instances de backend du client. Les sessions contenant des PHI doivent chiffrer à la fois les écouteurs frontaux et principaux pour le chiffrement du transport. Les clients doivent évaluer leurs certificats et leurs politiques de négociation de sessions et les maintenir conformes aux directives. Pour plus d'informations, consultez la section HTTPS Listeners for Your Classic Load Balancer.

Les clients peuvent également configurer Amazon ELB en mode TCP de base (pour Classic) ou sur WebSockets (pour Application) et transmettre les sessions chiffrées aux instances principales où la session cryptée est interrompue. Dans cette architecture, les clients gèrent leurs propres certificats et politiques de négociation TLS dans les applications exécutées dans leurs propres instances. Pour plus d'informations, consultez Listeners for Your Classic Load Balancer. Dans les deux architectures, les clients doivent implémenter un niveau de journalisation qu'ils jugent conforme aux exigences HIPAA et HITECH.

FreeRTOS

FreeRTOS est un système d'exploitation pour microcontrôleurs qui facilite la programmation, le déploiement, la sécurisation, la connexion et la gestion des petits appareils périphériques à faible consommation d'énergie. FreeRTOS est basé sur le noyau FreeRTOS, un système d'exploitation open source populaire pour les microcontrôleurs, et l'étend avec des bibliothèques de logiciels qui facilitent la connexion sécurisée de petits appareils à faible consommation aux services AWS IoT cloud AWS tels que Core ou à des appareils périphériques plus puissants fonctionnant en cours d'exécution. AWS IoT Greengrass

Les données contenant des PHI peuvent désormais être cryptées en transit et au repos lorsque vous utilisez un appareil qualifié exécutant FreeRTOS. FreeRTOS fournit deux bibliothèques pour assurer la sécurité de la plateforme : TLS et PKCS #11. L'API TLS doit être utilisée pour chiffrer et authentifier tout le trafic réseau contenant des PHI. PKCS #11 fournit une interface standard pour les opérations cryptographiques logicielles et doit être utilisé pour chiffrer tout PHI stocké sur un appareil qualifié exécutant FreeRTOS.

Utilisation AWS KMS pour le chiffrement de PHI

Les clés KMS peuvent être utilisées pour crypter/déchiffrer les clés de chiffrement des données utilisées pour chiffrer les PHI dans les applications d'un client ou dans les services AWS qui les utilisent. AWS KMS AWS KMS peut être utilisé conjointement avec un compte HIPAA, mais les PHI ne peuvent être traités, stockés ou transmis que dans le cadre des services éligibles à la HIPAA. AWS KMS est normalement utilisé pour générer et gérer des clés pour les applications exécutées dans d'autres services éligibles à la loi HIPAA.

Par exemple, une application traitant des PHI dans Amazon EC2 peut utiliser l'appel d' GenerateDataKey API pour générer des clés de chiffrement de données afin de chiffrer et de déchiffrer les PHI dans l'application. Les clés de chiffrement des données seraient protégées par les clés KMS du client stockées AWS KMS, créant ainsi une hiérarchie de clés hautement contrôlable lorsque les appels d'API AWS KMS sont connectés. AWS CloudTrail Les PHI ne doivent pas être stockés dans les balises (métadonnées) pour les clés stockées dans AWS KMS.

VM Import/Export

VM Import/Export permet aux clients d'importer facilement des images de machines virtuelles depuis un environnement existant vers des instances Amazon EC2 et de les réexporter vers votre

environnement sur site. Cette offre permet aux clients de tirer parti des investissements existants dans les machines virtuelles que vous avez créées pour répondre à leurs exigences en matière de sécurité informatique, de gestion de configuration et de conformité en intégrant ces machines virtuelles dans Amazon ready-to-use EC2 en tant qu'instances. Les clients peuvent également réexporter les instances importées vers leur infrastructure de virtualisation sur site, ce qui leur permet de déployer des charges de travail sur l'ensemble de votre infrastructure informatique.

VM Import/Export est disponible sans frais supplémentaires au-delà des frais d'utilisation standard pour Amazon EC2 et Amazon S3.

Pour importer des images de clients, les clients peuvent utiliser les outils de développement AWS CLI ou d'autres outils de développement pour importer une image de machine virtuelle (VM) depuis leur environnement VMware. Si les clients utilisent la plate-forme de virtualisation VMware vSphere, ils peuvent également utiliser le AWS Management Portal for vCenter vCenter pour importer leur machine virtuelle. Dans le cadre du processus d'importation, VM Import convertira la machine virtuelle du client en une AMI Amazon EC2, qu'il pourra utiliser pour exécuter des instances Amazon EC2. Une fois leur machine virtuelle importée, ils peuvent tirer parti de l'élasticité, de l'évolutivité et de la surveillance d'Amazon grâce à des offres telles que Auto Scaling, Elastic Load Balancing et CloudWatch pour prendre en charge leurs images importées.

Les clients peuvent exporter des instances Amazon EC2 précédemment importées à l'aide des outils d'API Amazon EC2. Spécifiez simplement l'instance cible, le format de fichier de la machine virtuelle et un compartiment Amazon S3 de destination, et VM Import/Export exportera automatiquement l'instance vers le compartiment Amazon S3 ainsi que les options de chiffrement pour sécuriser la transmission et le stockage de leurs images de machine virtuelle. Les clients peuvent ensuite télécharger et lancer la machine virtuelle exportée au sein de leur infrastructure de virtualisation sur site.

Les clients peuvent importer des machines virtuelles Windows et Linux qui utilisent les formats de virtualisation VMware ESX ou Workstation, Microsoft Hyper-V et Citrix Xen. Les clients peuvent également exporter des instances Amazon EC2 précédemment importées aux formats VMware ESX, Microsoft Hyper-V ou Citrix Xen. Pour obtenir la liste complète des systèmes d'exploitation, des versions et des formats pris en charge, consultez la section Exigences relatives à l'importation/exportation des machines virtuelles. AWS prévoit d'ajouter la prise en charge de systèmes d'exploitation, de versions et de formats supplémentaires à l'avenir.

Audit, sauvegardes et reprise après sinistre

La règle de sécurité de l'HIPAA contient des exigences détaillées relatives aux capacités d'audit approfondies, aux procédures de sauvegarde des données et aux mécanismes de reprise après sinistre. Les services d'AWS contiennent de nombreuses fonctionnalités qui aident les clients à répondre à leurs besoins. Par exemple, les clients devraient envisager de mettre en place des fonctionnalités d'audit pour permettre aux analystes de sécurité d'examiner les journaux d'activité ou les rapports détaillés afin de déterminer qui y avait accès, la saisie de l'adresse IP, les données consultées, etc.

Ces données doivent être suivies, enregistrées et stockées dans un emplacement central pendant de longues périodes, en cas d'audit. Grâce à Amazon EC2, les clients peuvent exécuter des fichiers journaux d'activité et des audits jusqu'à la couche de paquets de leurs serveurs virtuels, comme ils le font sur du matériel traditionnel. Ils peuvent également suivre tout trafic IP qui atteint leur instance de serveur virtuel. Les administrateurs d'un client peuvent sauvegarder les fichiers journaux dans Amazon S3 pour un stockage fiable à long terme.

L'HIPAA a également des exigences détaillées liées à la mise à jour d'un plan d'urgence pour protéger les données en cas d'urgence et doit créer et maintenir des copies exactes récupérables des PHI électroniques. Pour mettre en œuvre un plan de sauvegarde des données sur AWS, Amazon EBS propose un stockage persistant pour les instances de serveur virtuel Amazon EC2. Ces volumes peuvent être exposés sous forme de périphériques de blocs standard, et ils offrent un stockage hors instance qui persiste indépendamment de la durée de vie d'une instance. Conformément aux directives HIPAA, les clients peuvent créer point-in-time des instantanés des volumes Amazon EBS qui sont stockés automatiquement dans Amazon S3 et répliqués sur plusieurs zones de disponibilité, qui sont des emplacements distincts conçus pour être isolés des défaillances dans d'autres zones de disponibilité.

Ces instantanés sont accessibles à tout moment et peuvent protéger les données pour une durabilité à long terme. Amazon S3 fournit également une solution hautement disponible pour le stockage de données et les sauvegardes automatisées. En chargeant simplement un fichier ou une image dans Amazon S3, plusieurs copies redondantes sont automatiquement créées et stockées dans des centres de données distincts. Ces fichiers sont accessibles à tout moment, de n'importe où (en fonction des autorisations) et sont conservés jusqu'à leur suppression intentionnelle.

En outre, AWS propose par nature une variété de mécanismes de reprise après sinistre. La reprise après sinistre, le processus de protection des données et de l'infrastructure informatique d'une

entreprise en cas de sinistre, implique de maintenir des systèmes hautement disponibles, de conserver les données et le système répliqués hors site et de permettre un accès continu aux deux.

Avec Amazon EC2, les administrateurs peuvent démarrer des instances de serveur très rapidement et utiliser une adresse IP élastique (adresse IP statique pour l'environnement de cloud computing) pour basculer en douceur d'une machine à l'autre. Amazon EC2 propose également des zones de disponibilité. Les administrateurs peuvent lancer des instances Amazon EC2 dans plusieurs zones de disponibilité afin de créer des systèmes tolérants aux pannes, géographiquement diversifiés et hautement résilients en cas de défaillance du réseau, de catastrophes naturelles et de la plupart des autres sources probables de temps d'arrêt.

À l'aide d'Amazon S3, les données d'un client sont répliquées et stockées automatiquement dans des centres de données distincts afin de fournir un stockage de données fiable conçu pour garantir une disponibilité de 99,99 %.

Grâce à AWS Elastic Disaster Recovery (AWS DRS), les clients peuvent restaurer rapidement des applications sur AWS, soit à leur up-to-date état maximal, soit à une date antérieure.

Révisions du document

Pour être informé des mises à jour de ce livre blanc, abonnez-vous au flux RSS.

Modification	Description	Date
Mise à jour mineure	Mise à jour mineure	12 mai 2023
Mise à jour mineure	Livre blanc mis à jour pour étendre le contenu disponible sur les services.	28 septembre 2022
Mise à jour mineure	Corrigez le langage non inclusif.	6 avril 2022
Livre blanc mis à jour	Ajout d'informations sur le service de migration d' AWS applications et informations mises à jour pour Amazon ECS	6 décembre 2021
Livre blanc mis à jour	Informations mises à jour dans les sections Amazon Healthlake et Amazon VPC	9 novembre 2021
Livre blanc mis à jour	Ajout d'informations sur AWS Network Firewall	9 septembre 2021
Livre blanc mis à jour	Informations mises à jour sur les profils clients Amazon Connect	26 août 2021
Livre blanc mis à jour	Sections ajoutées : Amazon AppFlow et AWS Glue DataBrew	22 juillet 2021
Livre blanc mis à jour	Navigation et organisation mises à jour.	26 avril 2021

Livre blanc mis à jour	Les sections suivantes ont été ajoutées : AWS CodeDeploy, AWS CodePipeline, Amazon Aurora, Aurora PostgreSQL, Amazon Textract, Amazon Polly, Amazon FSx, AWS AWS Backup AWS Elastic Beanstalk Auto Scaling,, ,,,,, VM Import/Export AWS Firewall Manager, Amazon AWS Organizations AWS Security Hub CSPM AWS Serverless Applicati on Repository, Amazon. HealthLake EventBridge Section Amazon Aurora mise à jour.	31 mars 2021
Livre blanc mis à jour	Ajout d'une section sur AWS App Mesh et mise à jour du contenu d'AWS System Manager	25 août 2020
Livre blanc mis à jour	Ajout de sections Amazon Appstream 2.0, AWS SDK Metrics, AWS Data Exchange, Amazon MSK, Amazon Pinpoint, Amazon Lex, Amazon SES et Amazon Forecast, Amazon Quantum Ledger Database (QLDB),. AWS Cloud Map	7 mai 2020

Livre blanc mis à jour	Des sections ont été ajoutées sur Amazon CloudWatch, Amazon CloudWatch Events, Amazon Data Firehose, Amazon Managed Service pour Apache Flink, Amazon OpenSearch Service, Amazon DocumentDB (compatible avec MongoDB), AWS Mobile Hub, pour Chef Automate AWS IoT Greengrass, AWS OpsWorks pour Puppet Enterprise AWS OpsWorks , AWS Transfer pour SFTP, AWS DataSync, AWS Global Accelerator Amazon Comprehend Medical et AWS. RoboMaker	1er janvier 2020
Livre blanc mis à jour	Des sections ont été ajoutées sur Amazon Comprehend, Amazon Transcribe, Amazon Translate et AWS Certificate Manager.	1er janvier 2019
Livre blanc mis à jour	Ajout de sections sur Amazon Athena, Amazon EKS, AWS IoT Core et Amazon FreeRTOS AWS IoT Device Management, Amazon, Amazon GuardDuty Neptune, AWS Server Migration Service, Amazon MQ et. AWS Database Migration Service AWS Glue	1 novembre 2018

Livre blanc mis à jour	Des sections ont été ajoutées sur Amazon Elastic File System (EFS), Amazon Kinesis Video Streams, Amazon Rekognition, Amazon, SageMaker Amazon Simple Workflow, AWS Secrets Manage, Service Catalog et. AWS Step Functions	1er juin 2018
Livre blanc mis à jour	Ajout de sections sur AWS CloudFormation AWS X-Ray, AWS CloudTrail,, AWS CodeBuild, AWS CodeCommi t AWS Config, et AWS OpsWorks Stack.	1er avril 2018
Livre blanc mis à jour	Ajout d'une section sur AWS Fargate.	1er janvier 2018

Mises à jour effectuées avant 2018 :

Date	Description
novembre 2017	Des sections ont été ajoutées sur Amazon EC2 Container Registry, Amazon Macie, QuickSight Amazon et. AWS Managed Services
novembre 2017	Ajout de sections sur Amazon ElastiCache pour Redis et Amazon CloudWatch.
octobre 2017	Des sections ont été ajoutées sur Amazon SNS AWS Storage Gateway, Amazon Route 53 et. AWS CloudHSM Section mise à jour sur AWS Key Management Service.

Date	Description
Septembre 2017	Des sections ont été ajoutées sur Amazon Connect, Amazon Kinesis Streams, Amazon RDS (Maria) DB, Amazon RDS SQL Server AWS Batch AWS Lambda AWS Snowball Edge , Edge et la fonctionnalité Lambda @Edge d'Amazon. CloudFront
Août 2017	Des sections ont été ajoutées sur Amazon EC2 Systems Manager et Amazon Inspector.
juillet 2017	Des sections ont été ajoutées sur Amazon WorkSpaces WorkDocs, Amazon, AWS Directory Service et Amazon ECS.
Juin 2017	Ajout de sections sur Amazon CloudFront, AWS WAF et Amazon S3 Transfer Accelerat ion. AWS Shield
2017 mai	Suppression de l'exigence d'instances dédiées ou d'hôtes dédiés pour le traitement des PHI dans EC2 et EMR.
Mars 2017	Liste des services mise à jour pour pointer vers la page Services AWS concernés par le programme de conformité. Ajout d'une descripti on pour Amazon API Gateway.
Janvier 2017	Mise à jour vers le modèle le plus récent.
Octobre 2016	Première publication

Avis

Il incombe aux clients de procéder à une évaluation indépendante des informations contenues dans le présent document. Ce document : (a) est fourni à titre informatif uniquement, (b) représente les offres de produits et les pratiques actuelles d'AWS, qui sont susceptibles d'être modifiées sans préavis, et (c) ne crée aucun engagement ni aucune garantie de la part d'AWS et de ses filiales, fournisseurs ou concédants de licence. Les produits ou services AWS sont fournis « tels quels » sans garanties, déclarations ou conditions d'aucune sorte, qu'elles soient explicites ou implicites. Les responsabilités et obligations d'AWS vis-à-vis de ses clients sont régies par les contrats AWS. Le présent document ne fait partie d'aucun, et ne modifie aucun, contrat entre AWS et ses clients.

© 2023 Amazon Web Services, Inc. ou ses filiales. Tous droits réservés.

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.