Documento técnico de AWS

Arquitectura de seguridad de HIPAA y cumplimiento de servicios Amazon Web

Arquitectura de seguridad de HIPAA y cumplimiento de servicios Amazon Web: Documento técnico de AWS

Table of Contents

Arquitectura de seguridad de HIPAA y cumplimiento de servicios Amazon Web

Fecha de publicación: 28 de septiembre de 2022 () Revisiones del documento

En este paper se describe brevemente cómo los clientes pueden utilizar Amazon Web Services (AWS) para ejecutar cargas de trabajo confidenciales reguladas por la Ley de Portabilidad y Responsabilidad de los Seguros de Salud (HIPAA) de EE. UU. Nos centraremos en las normas de privacidad y seguridad de la HIPAA para proteger la información de salud protegida (PHI), cómo utilizar AWS para cifrar los datos en tránsito y en reposo, y cómo se pueden utilizar las funciones de AWS para ejecutar cargas de trabajo que contienen PHI.

Introducción

La Ley de Portabilidad y Responsabilidad de los Seguros Médicos de 1996 (HIPAA) se aplica a las «entidades cubiertas» y a los «socios comerciales». La HIPAA se amplió en 2009 mediante la Ley de Tecnología de la Información Sanitaria para la Salud Económica y Clínica (HITECH).

La HIPAA y la HITECH establecen un conjunto de normas federales destinadas a proteger la seguridad y la privacidad de la PHI. La HIPAA y la HITECH imponen requisitos relacionados con el uso y la divulgación de la información médica protegida (PHI), las salvaguardias adecuadas para proteger la PHI, los derechos individuales y las responsabilidades administrativas. Para obtener más información sobre HIPAA e HITECH, visite la página de inicio de privacidad de la información de salud.

Las entidades cubiertas y sus socios comerciales pueden usar los componentes de TI seguros, escalables y de bajo costo que proporciona Amazon Web Services (AWS) para diseñar aplicaciones de acuerdo con los requisitos de conformidad con la HIPAA y la HITECH. AWS ofrece una plataforma de commercial-off-the-shelf infraestructura con certificaciones y auditorías reconocidas en el sector, como ISO 27001, FedRAMP y los informes de control de la organización de servicios (SOC1, SOC2 y SOC3). Los servicios y centros de datos de AWS tienen varios niveles de seguridad física y operativa para garantizar la integridad y la seguridad de los datos de los clientes. Sin tarifas mínimas, sin necesidad de contratos por plazos y con pay-as-you-use precios, AWS es una solución fiable y eficaz para las crecientes aplicaciones del sector de la salud.

AWS permite a las entidades cubiertas y a sus socios comerciales sujetos a la HIPAA procesar, almacenar y transmitir la PHI de forma segura. Además, a partir de julio de 2013, AWS ofrece un apéndice para socios comerciales (BAA) estandarizado para dichos clientes. Los clientes que ejecuten un BAA de AWS pueden usar cualquier servicio de AWS en una cuenta designada como cuenta HIPAA, pero solo pueden procesar, almacenar y transmitir la PHI mediante los servicios aptos para la HIPAA definidos en el BAA de AWS. Para obtener una lista completa de estos servicios, consulte la página de referencia de servicios aptos para la HIPAA.

AWS mantiene un programa de administración de riesgos basado en estándares para garantizar que los servicios aptos para la HIPAA respalden específicamente las protecciones administrativas, técnicas y físicas de la HIPAA. El uso de estos servicios para almacenar, procesar y transmitir la PHI ayuda a nuestros clientes y a AWS a cumplir los requisitos de la HIPAA aplicables al modelo operativo basado en servicios de AWS.

La BAA de AWS exige que los clientes cifren la PHI almacenada o transmitida mediante servicios que cumplen con los requisitos de la HIPAA, de acuerdo con las directrices del Secretario de Salud y Servicios Humanos (HHS): Guía para hacer que la información de salud protegida no segura sea inutilizable, ilegible o indescifrable para personas no autorizadas («Guía»). Consulte este sitio, ya que podría estar actualizado y estar disponible en un sitio sucesor (o relacionado) designado por el HHS.

AWS ofrece un conjunto completo de funciones y servicios para que la administración de claves y el cifrado de la PHI sean fáciles de administrar y más sencillos de auditar, incluido el AWS Key Management Service (AWS KMS). Los clientes que cumplen los requisitos de conformidad con la HIPAA disponen de una gran flexibilidad a la hora de cumplir los requisitos de cifrado de la PHI.

A la hora de determinar cómo implementar el cifrado, los clientes pueden evaluar y aprovechar las funciones de cifrado propias de los servicios aptos para la HIPAA. O bien, los clientes pueden cumplir los requisitos de cifrado por otros medios, de conformidad con las directrices del HHS.

Cifrado y protección de la PHI en AWS

La norma de seguridad de la HIPAA incluye especificaciones de implementación aplicables para el cifrado de la PHI en la transmisión («en tránsito») y en el almacenamiento («en reposo»). Si bien se trata de una especificación de implementación abordable en la HIPAA, AWS exige que los clientes cifren la PHI almacenada o transmitida mediante servicios que cumplen con los requisitos de la HIPAA, de acuerdo con las directrices del Secretario de Salud y Servicios Humanos (HHS): Guía para hacer que la información de salud protegida no segura sea inutilizable, ilegible o indescifrable para personas no autorizadas («Guía»). Consulte este sitio porque puede estar actualizado y puede estar disponible en un sitio sucesor (o relacionado) designado por el HHS.

AWS ofrece un conjunto completo de funciones y servicios para que la administración de claves y el cifrado de la PHI sean fáciles de administrar y más sencillos de auditar, incluido el AWS Key Management Service (AWS KMS). Los clientes que cumplen los requisitos de conformidad con la HIPAA disponen de una gran flexibilidad a la hora de cumplir los requisitos de cifrado de la PHI.

Al determinar cómo implementar el cifrado, los clientes pueden evaluar y aprovechar las funciones de cifrado propias de los servicios que cumplen con los requisitos de la HIPAA, o pueden cumplir los requisitos de cifrado por otros medios, de acuerdo con las directrices del HHS. En las siguientes secciones se proporcionan detalles de alto nivel sobre el uso de las funciones de cifrado disponibles en cada uno de los servicios que cumplen con los requisitos de la HIPAA y otros patrones para cifrar la PHI, y cómo se puede utilizar AWS KMS para cifrar las claves utilizadas para cifrar la PHI en AWS.

Temas

- Amazon API Gateway
- Amazon AppFlow
- Amazon AppStream 2.0
- Amazon Athena
- Amazon Aurora
- PostgreSQL de Amazon Aurora
- Amazon CloudFront
- Amazon CloudWatch
- CloudWatch Eventos de Amazon
- Amazon CloudWatch Logs

- Amazon Comprehend
- Amazon Comprehend Medical
- Amazon Connect
- Amazon DocumentDB (con compatibilidad con 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 para Redis
- OpenSearch Servicio Amazon
- Amazon EMR
- Amazon EventBridge
- Amazon Forecast
- Amazon FSx
- Amazon GuardDuty
- Amazon HealthLake
- Amazon Inspector
- Amazon Managed Service para 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 para MariaDB
- Amazon RDS para MySQL
- Amazon RDS para Oracle
- Amazon RDS para PostgreSQL
- Amazon RDS para 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 Servicio de migración de aplicaciones
- 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
- Recuperación ante desastres de AWS Elastic
- AWS Fargate
- AWS Firewall Manager
- AWS Global Accelerator
- AWS Glue
- Pegamento AWS DataBrew
- AWS IoT Núcleo y AWS IoT Device Management
- AWS IoT Greengrass
- AWS Lambda
- AWS Managed Services
- AWS OpsWorks para Chef Automate
- AWS OpsWorks para Puppet Enterprise
- AWS OpsWorks Apile
- AWS Organizations

- AWS RoboMaker
- Métricas del SDK de AWS
- AWS Secrets Manager
- AWS Security Hub
- AWS Server Migration Service
- AWS Serverless Application Repository
- Service Catalog
- AWS Shield
- AWS Snowball
- AWS Snowball Edge
- AWS Step Functions
- AWS Storage Gateway
- AWS Systems Manager
- AWS Transfer for SFTP
- AWS WAF: firewall de aplicaciones web
- AWS X-Ray
- Elastic Load Balancing
- FreeRTOS
- Se utiliza para el cifrado de la PHI AWS KMS
- VM Import/Export

Amazon API Gateway

Los clientes pueden usar Amazon API Gateway para procesar y transmitir información de salud protegida (PHI). Si bien Amazon API Gateway utiliza automáticamente los puntos de enlace HTTPS para el cifrado en movimiento, los clientes también pueden optar por cifrar las cargas útiles del lado del cliente. API Gateway pasa todos los datos no almacenados en caché a través de la memoria y no los graba en el disco. Los clientes pueden usar la versión 4 de AWS Signature para la autorización con API Gateway. Para más información, consulte los siguientes temas:

- Preguntas frecuentes sobre Amazon API Gateway: seguridad y autorización
- Control y administración del acceso a una API REST en API Gateway

Los clientes pueden integrarse con cualquier servicio que esté conectado a API Gateway, siempre que, cuando se trate de PHI, el servicio se configure de acuerdo con la Guía y la BAA. Para obtener información sobre la integración de API Gateway con los servicios de backend, consulte Configurar los métodos de API REST en API Gateway.

Los clientes pueden utilizar AWS CloudTrail Amazon CloudWatch para habilitar el registro de forma coherente con sus requisitos de registro. Asegúrese de que cualquier PHI enviada a través de API Gateway (por ejemplo, en encabezados, URL y solicitud/respuesta) solo sea capturada por los servicios aptos para la HIPAA que se hayan configurado de manera coherente con la Guía. Para obtener más información sobre el registro con API Gateway, consulta ¿Cómo habilito CloudWatch los registros para solucionar problemas con mi API REST o API de WebSocket API Gateway?

Amazon AppFlow

Amazon AppFlow es un servicio de integración totalmente gestionado que permite a los clientes transferir datos de forma segura entre aplicaciones oftware-as-a S-Service (SaaS) como Salesforce, Marketo, Slack y ServiceNow servicios de AWS como Amazon S3 y Amazon Redshift. AppFlow puede ejecutar los flujos de datos con la frecuencia que elija el cliente: según un cronograma, en respuesta a un evento empresarial o bajo demanda. Los clientes también pueden configurar las funciones de transformación de datos, como el filtrado y la validación, para generar ready-to-use datos detallados como parte del propio flujo, sin necesidad de realizar pasos adicionales.

Amazon se AppFlow puede utilizar para procesar y transferir datos que contengan PHI. El cifrado de los datos en tránsito entre el origen AppFlow y el destino configurados se proporciona de forma predeterminada mediante TLS 1.2 o una versión posterior. Los datos almacenados en reposo en S3 se cifran automáticamente mediante una AWS KMS clave (anteriormente CMK) especificada por el cliente. En el caso de los datos de PHI transferidos a destinos distintos de S3, los clientes deben asegurarse de que el almacenamiento en reposo del destino elegido satisfaga sus necesidades de seguridad. AppFlow permite la supervisión de aplicaciones al integrarse con AWS CloudTrail las llamadas a la API EventBridge para registrar y Amazon emitir eventos de ejecución de flujos.

Amazon AppStream 2.0

Amazon AppStream 2.0 es un servicio de streaming de aplicaciones totalmente gestionado. Los clientes son dueños de sus datos y deben configurar las aplicaciones de Windows necesarias de manera que cumplan con sus requisitos reglamentarios. Los clientes pueden configurar el almacenamiento persistente a través de Home Folders. Los archivos y carpetas se cifran en tránsito mediante puntos de conexión SSL de Amazon S3. Los archivos y las carpetas se cifran en reposo

mediante claves de cifrado gestionadas por Amazon S3. Para obtener más información, consulte Habilitar y administrar el almacenamiento persistente para sus usuarios de la AppStream versión 2.0. Si los clientes eligen utilizar una solución de almacenamiento de terceros, son responsables de garantizar que la configuración de esa solución sea coherente con las instrucciones. Todas las comunicaciones de la API pública con Amazon AppStream 2.0 se cifran mediante TLS. Para obtener más información, consulta la documentación de Amazon AppStream 2.0.

Amazon AppStream 2.0 está integrado con AWS CloudTrail un servicio que registra las llamadas a la API realizadas por Amazon AppStream 2.0 o en su nombre en la cuenta de AWS del cliente y entrega los archivos de registro al bucket de Amazon S3 especificado. CloudTrail captura las llamadas a la API realizadas desde la consola de Amazon AppStream 2.0 o desde la API de Amazon AppStream 2.0. Los clientes también pueden usar Amazon CloudWatch para registrar las métricas de uso de recursos. Para obtener más información, consulte Monitorización de los recursos de Amazon AppStream 2.0 y Registro de llamadas a la API AppStream 2.0 con AWS CloudTrail.

Amazon Athena

Amazon Athena es un servicio de consultas interactivo que facilita el análisis de datos directamente en Amazon Simple Storage Service (Amazon S3) con SQL estándar. Athena ayuda a los clientes a analizar los datos no estructurados, semiestructurados y estructurados almacenados en Amazon S3. Algunos ejemplos son datos en CSV, JSON o con formatos de columnas, como Apache Parquet y Apache ORC. Los clientes pueden usar Athena para ejecutar consultas ad hoc mediante ANSI SQL, sin necesidad de agregar o cargar los datos en Athena.

Amazon Athena ahora se puede usar para procesar datos que contengan PHI. El cifrado de los datos en tránsito entre Amazon Athena y S3 se proporciona de forma predeterminada mediante SSL/TLS. El cifrado de la PHI mientras está en reposo en S3 debe realizarse de acuerdo con las instrucciones que se proporcionan en la sección S3. El cifrado de los resultados de las consultas desde y dentro de Amazon Athena, incluidos los resultados por etapas, debe habilitarse mediante el cifrado del lado del servidor con claves administradas de Amazon S3 (SSE-S3), claves administradas (AWS KMS SSE-KMS) o el cifrado del lado del cliente con claves administradas (CSE-KMS). AWS KMS Amazon Athena registra todas las AWS CloudTrail llamadas a la API.

Amazon Aurora

Amazon Aurora permite a los clientes cifrar los clústeres de bases de datos y las instantáneas de Aurora en reposo mediante claves que administran. AWS KMS En una instancia de base de datos que se ejecuta con el cifrado Amazon Aurora, los datos almacenados en reposo en el

almacenamiento subyacente se cifran, al igual que las copias de seguridad automatizadas, las réplicas de lectura y las instantáneas.

Como es posible que la Guía se actualice, los clientes deben seguir evaluando y determinando si el cifrado Amazon Aurora cumple con sus requisitos normativos y de conformidad. Para obtener más información sobre el cifrado en reposo con Amazon Aurora, consulte Protección de datos mediante cifrado.

Las conexiones a los clústeres de bases de datos que ejecutan Aurora MySQL deben utilizar el cifrado de transporte, mediante Secure Socket Layer (SSL) o Transport Layer Security (TLS). Para obtener más información sobre la implementación de SSL/TLS, consulte Uso de SSL/TLS con clústeres de bases de datos Aurora MySQL.

PostgreSQL de Amazon Aurora

Amazon Aurora permite a los clientes cifrar los clústeres de bases de datos y las instantáneas de Aurora en reposo mediante claves que administran. AWS KMS En una instancia de base de datos que se ejecuta con el cifrado Amazon Aurora, los datos almacenados en reposo en el almacenamiento subyacente se cifran, al igual que las copias de seguridad automatizadas, las réplicas de lectura y las instantáneas.

Como es posible que la Guía se actualice, los clientes deben seguir evaluando y determinando si el cifrado Amazon Aurora cumple con sus requisitos normativos y de conformidad. Para obtener más información sobre el cifrado en reposo con Amazon Aurora, consulte Protección de datos mediante cifrado.

Las conexiones a los clústeres de bases de datos que ejecutan Aurora PostgreSQL deben utilizar el cifrado de transporte, mediante Secure Socket Layer (SSL) o Transport Layer Security (TLS). Para obtener más información sobre la implementación de SSL/TLS, consulte Proteger los datos de Aurora PostgreSQL con SSL.

Amazon CloudFront

Amazon CloudFront es un servicio de red de entrega de contenido (CDN) global que acelera la entrega de sitios web, API, contenido de vídeo u otros activos web de los clientes. Se integra con otros productos de Amazon Web Services para ofrecer a los desarrolladores y a las empresas una forma sencilla de acelerar el envío de contenido a los usuarios finales sin compromisos de uso mínimo. Para garantizar el cifrado de la PHI durante la transmisión CloudFront, los clientes deben CloudFront configurarla para usar HTTPS end-to-end desde el origen hasta el espectador.

Esto incluye el tráfico entre CloudFront y el espectador, la CloudFront redistribución desde un origen personalizado y la CloudFront distribución desde un origen de Amazon S3. Los clientes también deben asegurarse de que los datos estén cifrados en el origen para garantizar que permanezcan cifrados en reposo mientras se almacenan en caché. CloudFront Si utilizan Amazon S3 como origen, los clientes pueden utilizar las funciones de cifrado de S3 del lado del servidor. Si los clientes distribuyen desde un origen personalizado, deben asegurarse de que los datos estén cifrados en el origen.

Lambda@Edge

Lambda @Edge es un servicio de cómputo que permite la ejecución de funciones de Lambda en ubicaciones de borde de AWS. Lambda @Edge se puede utilizar para personalizar el contenido entregado a través de. CloudFront Al utilizar Lambda @Edge con la PHI, los clientes deben seguir las instrucciones de uso de. CloudFront Todas las conexiones de entrada y salida de Lambda @Edge deben cifrarse mediante HTTPS o SSL/TLS.

Amazon CloudWatch

Amazon CloudWatch es un servicio de supervisión de los recursos de la nube de AWS y las aplicaciones que los clientes ejecutan en AWS. Los clientes pueden usar Amazon CloudWatch para recopilar y rastrear métricas, recopilar y monitorear archivos de registro y configurar alarmas. Amazon CloudWatch por sí misma no produce, almacena ni transmite la PHI. Los clientes pueden monitorear las llamadas a la CloudWatch API con AWS CloudTrail. Para obtener más información, consulte Registrar llamadas a la CloudWatch API de Amazon con AWS CloudTrail.

Para obtener más información sobre los requisitos de configuración, consulta la sección Amazon CloudWatch Logs.

CloudWatch Eventos de Amazon

Amazon CloudWatch Events ofrece una near-real-time secuencia de eventos del sistema que describen los cambios en los recursos de AWS. Los clientes deben asegurarse de que la PHI no fluya hacia CloudWatch los eventos, y cualquier recurso de AWS que emita un CloudWatch evento que almacene, procese o transmita la PHI se configure de acuerdo con la Guía.

Los clientes pueden configurar Amazon CloudWatch Events para que se registre como una llamada a la API de AWS CloudTrail. Para obtener más información, consulte Crear una regla de CloudWatch eventos que se active en una llamada a la API de AWS mediante AWS CloudTrail.

Amazon CloudWatch Logs

Los clientes pueden usar Amazon CloudWatch Logs para monitorear, almacenar y acceder a sus archivos de registro desde instancias de Amazon Elastic Compute Cloud (Amazon EC2) AWS CloudTrail, Amazon Route 53 y otras fuentes. A continuación, pueden recuperar los datos de registro asociados de CloudWatch Logs. Los datos de registro se cifran mientras están en tránsito y mientras están en reposo. Como resultado, no es necesario volver a cifrar la PHI emitida por ningún otro servicio y entregada a Logs. CloudWatch

Amazon Comprehend

Amazon Comprehend utiliza el procesamiento de lenguaje natural para extraer información sobre el contenido de los documentos. Amazon Comprehend procesa cualquier archivo de texto en formato UTF-8. Genera información a partir del reconocimiento de entidades, frases clave, lenguaje, opiniones y otros elementos comunes en un documento. Amazon Comprehend se puede utilizar con datos que contengan PHI. Amazon Comprehend no retiene ni almacena ningún dato y todas las llamadas a la API se cifran con SSL/TLS. Amazon Comprehend registra todas las CloudTrail llamadas a la API.

AWS Identity and Access Management

Las funciones de acceso de seguridad, como la autenticación y la autorización, son necesarias para acceder a Amazon Comprehend y se pueden controlar con AWS Identity and Access Management(IAM), y las credenciales se pueden utilizar para acceder al IAM. Para obtener más información, consulte Autenticación y control de acceso para Amazon Comprehend en la Guía del usuario de Amazon Comprehend.

Administración de cuentas

De forma predeterminada, los usuarios de IAM no tienen permiso para crear o modificar los recursos de Amazon Comprehend ni para realizar tareas mediante la API Amazon Comprehend. Para permitir a los usuarios crear o modificar recursos y realizar tareas, los clientes son responsables de aprovechar las políticas de IAM que otorgan a los usuarios permisos para los recursos específicos (como Amazon Comprehend y las acciones de API) que los usuarios necesitan usar y, a continuación, adjuntar políticas a los usuarios o grupos que requieren permisos específicos.

Con Amazon Comprehend, puede usar AWS Identity and Access Management (IAM) para crear un usuario con una política adjunta para habilitar los permisos de Amazon Comprehend. Si lo

desea, puede optar por crear políticas personalizadas para asociarlas a un rol. A continuación, puede añadir administradores al rol con la posibilidad de invocar las API para la administración de Amazon Comprehend de acuerdo con los principios de acceso basado en roles y privilegios mínimos definidos por la organización.

Identidad y acceso

Con Amazon Comprehend, puede solicitar al usuario que se autentique para AWS utilizar la autenticación multifactorial de acuerdo con sus requisitos organizativos de autenticación.

Con ella AWS Management Console, los administradores de IAM pueden crear una política administrada por el cliente que deniegue todos los permisos excepto los necesarios para que los usuarios administren sus propias credenciales y dispositivos de MFA. Hay una plantilla de política JSON disponible en la página Mis credenciales de seguridad de la consola de IAM.

Si lo desea, puede aprovechar las capacidades de MFA de terceros compatibles con los socios de IAM. Para obtener información adicional, consulte IAM Partners.

Administración

Le recomendamos que Amazon Comprehend seleccione políticas basadas en la identidad en las que los administradores de cuentas puedan adjuntar políticas de permisos a las identidades de IAM (usuarios, grupos y roles) y, de ese modo, conceder permisos para realizar operaciones en los recursos de Amazon Comprehend.

Puede encontrar una lista de acciones de API para Amazon Comprehend en la guía de referencia de API. También debería considerar la posibilidad de autorizar el acceso a las políticas de IAM predefinidas, las políticas de IAM de los clientes y las acciones de API a los usuarios o roles de acuerdo con sus requisitos organizativos de privilegios mínimos y basados en sus roles. Para obtener más información, consulte Uso de la API Amazon Comprehend en la Guía para desarrolladores.

Autenticación externa

Amazon Comprehend es compatible con la federación de identidades mediante funciones de IAM. Esto permite a Amazon Comprehend your usuarios autenticarse AWS asumiendo una función que los administradores han asignado. Los usuarios que acceden AWS con credenciales de su organización o de un tercero asumen una función de forma indirecta.

AWS La compatibilidad con Kerberos y Active Directory ofrece las ventajas del inicio de sesión único y la autenticación centralizada de los usuarios de las bases de datos. AWS los usuarios pueden optar

por administrar y almacenar las credenciales de AWS Directory Service usuario en Microsoft Active Directory o en el Active Directory local del cliente.

Control del flujo de datos

AWS los clientes y los socios de APN, que actúan como controladores o procesadores de datos, son responsables de cualquier dato personal que publiquen en Amazon Comprehend Nube de AWS y en Amazon Comprehend. Usted es responsable de controlar el flujo de entradas y salidas de datos de Amazon Comprehend mediante políticas de IAM.

Protección de datos y gestión de secretos

El modelo de responsabilidad AWS compartida se aplica a la protección de datos en Amazon Comprehend. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecuta toda la AWS nube. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Este contenido incluye las tareas de configuración y administración de la seguridad de AWS los servicios que utiliza. Para obtener más información sobre la privacidad de datos, consulte Preguntas frecuentes sobre la privacidad de datos.

La sección Protección de datos en Amazon Comprehend de la Guía para desarrolladores de Amazon Comprehend proporciona consejos que debe tener en cuenta a la hora de proteger los datos, como el uso de TLS para la transmisión y evitar colocar información confidencial en etiquetas o campos de formato libre.

Cifrado de data-at-rest

Amazon Comprehend trabaja con AWS Key Management Service (AWS KMS) para proporcionar un cifrado mejorado de sus datos. Amazon Simple Storage Service (Amazon S3) ya le permite cifrar los documentos de entrada al crear un análisis de texto, un modelado de temas o un trabajo personalizado de Amazon Comprehend. La integración con AWS KMS le permite cifrar los datos del volumen de almacenamiento para los trabajos de inicio* y creación*, y cifra los resultados de salida de los trabajos de inicio* con su propia clave. AWS KMS

Se recomienda a los usuarios de Amazon Comprehend cifrar los buckets de Amazon S3 utilizados para los documentos de entrada mediante las soluciones de cifrado de S3 disponibles de acuerdo con las políticas de su organización.

El AWS Management Console, cifra los modelos personalizados de Amazon Comprehend con su AWS KMS propia clave. Para ello AWS CLI, Amazon Comprehend puede cifrar modelos

personalizados con su propia AWS KMS clave o con una clave gestionada por el cliente (CMK) proporcionada.

Si selecciona el cifrado al utilizar el AWS Management Console, puede elegir uno de los siguientes métodos opcionales o ambos:

- Cifrado de volumen: garantiza que los datos de un volumen de EBS utilizado por Comprehend estén cifrados durante el entrenamiento o la inferencia (los datos se vacían después del entrenamiento o la inferencia, por lo que esta clave solo es relevante mientras el trabajo está en curso).
- Cifrado de los resultados de salida: permite cifrar los datos de salida almacenados por Comprehend en el depósito del cliente mediante una clave proporcionada por el cliente. AWS KMS

Para obtener más información sobre los tipos de cifrado, como el cifrado por volumen, consulte AWS KMS Cifrado en Amazon Comprehend.

Información de identificación personal

Puede utilizar la consola o las API de Amazon Comprehend para detectar información de identificación personal (PII) en documentos de texto redactados en inglés. Para obtener más información sobre la detección y el etiquetado de las entidades de PII y la ejecución de varios trabajos de análisis de PII, consulte la sección Información de identificación personal de la Guía para desarrolladores de Amazon Comprehend.

Eliminación de datos

Si es cliente de Amazon Comprehend y utiliza Amazon S3 y decide gestionar sus propias AWS KMS claves, debería plantearse la posibilidad de revocar AWS KMS las claves y definir la justificación procesal para hacerlo de acuerdo con sus requisitos organizativos. La revocación de la AWS KMS clave de Amazon S3 hace que los datos sean inutilizables o ilegibles.

Segmentación y endurecimiento de la red

Como servicio gestionado, Amazon Comprehend sigue las prácticas AWS recomendadas en materia de seguridad, identidad y conformidad.

Para ver las medidas de seguridad de red recomendadas, consulte Seguridad de infraestructura en Amazon Comprehend en la Guía para desarrolladores de Amazon Comprehend.

Proteja los trabajos mediante una Amazon Virtual Private Cloud (Amazon VPC)

Amazon Comprehend utiliza diversas medidas de seguridad para garantizar la seguridad de sus datos con nuestros contenedores de trabajos, donde se almacenan mientras Amazon Comprehend los utiliza. Sin embargo, los contenedores de trabajos acceden a AWS los recursos, como los depósitos de Amazon S3 en los que se almacenan datos y modelan artefactos, a través de Internet.

Para controlar el acceso a sus datos, le recomendamos que cree una nube privada virtual (VPC) y que la configure de manera que no se pueda acceder a los datos y a los contenedores por Internet. Para obtener información sobre la creación y configuración de una VPC, consulte Introducción a Amazon VPC en la Guía del usuario de Amazon VPC. Utilizar una VPC ayuda a proteger sus datos, puesto que puede configurar la VPC de manera que no se conecte a Internet. Utilizar una VPC también le permite monitorear todo el tráfico de red dentro y fuera de sus contenedores de trabajos mediante registros de flujo de la VPC. Para obtener más información, consulte Logs de flujo de VPC en la Guía del usuario de Amazon VPC.

Especifique la configuración de la VPC cuando cree un trabajo especificando las subredes y los grupos de seguridad. Cuando especifique las subredes y los grupos de seguridad, Amazon Comprehend creará interfaces de red elásticas (ENI) que se asocian a los grupos de seguridad en una de las subredes. Las ENI permiten que nuestros contenedores de trabajos se conecten a los recursos que hay en la VPC. Para obtener más información sobre las ENI, consulte Interfaces de red elásticas en la Guía del usuario de Amazon VPC.

> **Note**
>
> Para los trabajos, solo pueden configurar subredes con una VPC de tenencia predeterminada en la que la instancia se ejecute en hardware compartido. Para obtener más información sobre el atributo de tenencia de las VPC, consulte Instancias dedicadas en la Guía del usuario de Amazon EC2 para instancias de Linux.

Puede establecer una conexión privada entre la VPC y Amazon Comprehend mediante la creación de un punto de conexión de VPC de interfaz. Para obtener más información, consulte Amazon Comprehend e Interface VPC Endpoints ().AWS PrivateLink

Fortalecimiento del host y de la imagen

Basándose en el modelo de responsabilidad AWS compartida, la protección del servidor y de la imagen del AWS entorno de Amazon Comprehend se AWS gestiona como un servicio prestado.

Tenencia múltiple

Para que su recomendación sea más segura, le recomendamos que implemente las siguientes recomendaciones de seguridad para varios usuarios:

- Use únicamente una dirección de correo electrónico verificada para autorizar el acceso de usuario a un inquilino en función de la coincidencia de dominio. No confíe en las direcciones de correo electrónico y los números de teléfono a menos que su aplicación las verifique o que el IdP externo proporcione una prueba de verificación. Para obtener más detalles sobre la configuración de estos permisos, consulte Permisos y ámbitos de los atributos.
- Utilice atributos inmutables o mutables para los atributos de perfil de usuario que identifican a los inquilinos. Los administradores deben poder cambiar estos atributos. Además, proporcione a los clientes de aplicaciones acceso de solo lectura a los atributos.
- Asegúrese de disponer de una asignación de 1:1 entre el IdP externo y el cliente de la aplicación para evitar el acceso no autorizado entre inquilinos. Un usuario que ha sido autenticado por un IdP externo y que tiene una cookie de sesión de Amazon Cognito válida, puede acceder a otras aplicaciones de inquilino que confían en el mismo IdP.
- Al implementar la lógica de autorización y coincidencia de inquilinos en la aplicación, asegúrese de que los propios usuarios no puedan modificar los criterios utilizados para autorizar el acceso de los usuarios a los inquilinos. Además, si se está utilizando un IdP externo para la federación, restrinja a los administradores de proveedores de identidad de los inquilinos para que no puedan modificar el acceso de usuarios.

Prevención de la sustitución confusa entre servicios

El confuso problema de los suplentes es un problema de seguridad de varios inquilinos, en el que una entidad que no tiene permiso para realizar una acción puede coaccionar a una entidad con más privilegios para que la lleve a cabo. En AWS, la suplantación de identidad entre varios servicios puede provocar el confuso problema de un diputado. La suplantación entre servicios puede producirse cuando un servicio (el servicio que lleva a cabo las llamadas) llama a otro servicio (el servicio al que se llama). El servicio que lleva a cabo las llamadas se puede manipular para utilizar sus permisos a fin de actuar en función de los recursos de otro cliente de una manera en la que no debe tener permiso para acceder. Para evitarlo, AWS proporciona herramientas que pueden ayudarte a proteger los datos de todos los servicios cuyos directores de servicio tengan acceso a los recursos de tu cuenta. Para obtener más información que incluya las medidas de seguridad que

debe tener en cuenta para abordar este problema de seguridad, consulte Cross-service Confused Deputy Prevention en la Guía para desarrolladores de Amazon Comprehend.

Amazon Comprehend Medical

Para obtener orientación, consulte la sección anteriorAmazon Comprehend.

Amazon Connect

Amazon Connect es un servicio de centro de contacto de autoservicio basado en la nube que permite una interacción dinámica, personal y natural con los clientes a cualquier escala. Los clientes no deben incluir ninguna PHI en ningún campo asociado con la gestión de usuarios, perfiles de seguridad y flujos de contactos en Amazon Connect.

Los perfiles de clientes de Amazon Connect, una función de Amazon Connect, proporcionan a los agentes del centro de contacto una vista más unificada del perfil de un cliente con la información más actualizada, a fin de ofrecer un servicio de atención al cliente más personalizado. Los perfiles de clientes están diseñados para reunir automáticamente la información de clientes de múltiples aplicaciones en un perfil de cliente unificado y entregar el perfil directamente al agente tan pronto como comience la llamada de asistencia o la interacción. Los clientes deben abstenerse de nombrar dominios o claves de objetos con datos de PHI. El contenido de los dominios y los objetos está cifrado y protegido, pero los identificadores clave no.

Amazon DocumentDB (con compatibilidad con MongoDB)

Amazon DocumentDB (compatible con MongoDB) (Amazon DocumentDB) ofrece cifrado en reposo durante la creación del clúster mediante, lo AWS KMS que permite a los clientes cifrar bases de datos mediante AWS o claves administradas por el cliente. En una instancia de base de datos que se ejecuta con el cifrado activado, los datos almacenados en reposo se cifran de acuerdo con las directrices vigentes en el momento de la publicación de este documento técnico, al igual que las copias de seguridad automatizadas, las réplicas de lectura y las instantáneas. Dado que la Guía podría actualizarse, los clientes deben seguir evaluando y determinando si el cifrado de Amazon DocumentDB cumple con sus requisitos normativos y de conformidad. Para obtener más información sobre el cifrado en reposo mediante Amazon DocumentDB, consulte Cifrado de datos de Amazon DocumentDB en reposo.

Las conexiones a Amazon DocumentDB que contienen PHI deben utilizar puntos de enlace que acepten el transporte cifrado (HTTPS). De forma predeterminada, un clúster de Amazon

DocumentDB recién creado solo acepta conexiones seguras mediante Transport Layer Security (TLS). Para obtener más información, consulte Cifrado de datos en tránsito. Amazon DocumentDB se utiliza AWS CloudTrail para registrar todas las llamadas a la API. Para obtener más información, consulte Registro y supervisión en Amazon DocumentDB.

En determinadas características de administración, Amazon DocumentDB utiliza una tecnología operativa que comparte con Amazon RDS. Las llamadas a la consola de Amazon DocumentDB, la CLI de AWS y la API se registran como llamadas realizadas a la API de Amazon RDS.

Amazon DynamoDB

Las conexiones a Amazon DynamoDB que contienen PHI deben utilizar puntos de enlace que acepten el transporte cifrado (HTTPS). Para obtener una lista de los puntos de enlace regionales, consulte los puntos de enlace de los servicios de AWS.

Amazon DynamoDB ofrece el cifrado DynamoDB, que permite a los clientes cifrar bases de datos mediante claves que los clientes administran. AWS KMS En una instancia de base de datos que se ejecuta con el cifrado de Amazon DynamoDB, los datos almacenados en reposo en el almacenamiento subyacente se cifran de acuerdo con las directrices vigentes en el momento de la publicación de este documento técnico, al igual que las copias de seguridad automatizadas, las réplicas de lectura y las instantáneas.

Dado que la Guía podría actualizarse, los clientes deben seguir evaluando y determinando si el cifrado de Amazon DynamoDB cumple sus requisitos normativos y de conformidad. Para obtener más información sobre el cifrado en reposo mediante Amazon DynamoDB, consulte Encriptación en reposo de DynamoDB.

Amazon Elastic Block Store

El cifrado en reposo de Amazon EBS es coherente con las directrices vigentes en el momento de la publicación de este documento técnico. Dado que la Guía podría actualizarse, los clientes deben seguir evaluando y determinando si el cifrado de Amazon EBS cumple con sus requisitos normativos y de conformidad. Con el cifrado de Amazon EBS, se genera una clave de cifrado de volumen única para cada volumen de EBS. Los clientes tienen la flexibilidad de elegir qué clave de KMS AWS Key Management Service se utilizará para cifrar cada clave de volumen. Para obtener más información, consulte Amazon EBS encryption (Cifrado de Amazon EBS).

Amazon Elastic Compute Cloud

Amazon EC2 es un servicio informático escalable y configurable por el usuario que admite varios métodos de cifrado de datos en reposo. Por ejemplo, los clientes pueden optar por cifrar la PHI a nivel de aplicación o campo mientras se procesa en una plataforma de aplicaciones o bases de datos alojada en una instancia de Amazon EC2. Los enfoques van desde el cifrado de datos mediante bibliotecas estándar en un marco de aplicaciones como Java o.NET; el aprovechamiento de las funciones de cifrado transparente de datos de Microsoft SQL u Oracle; o la integración de otras soluciones de terceros y basadas en software como servicio (SaaS) en sus aplicaciones.

Los clientes pueden optar por integrar sus aplicaciones que se ejecutan en Amazon EC2 con AWS KMS los SDK, lo que simplifica el proceso de administración y almacenamiento de claves. Los clientes también pueden implementar el cifrado de los datos en reposo mediante el cifrado a nivel de archivos o de disco completo (FDE) mediante software de terceros de AWS Marketplace Partners o herramientas de cifrado de sistemas de archivos nativas (como dm-crypt, LUKS, etc.).

El tráfico de red que contiene PHI debe cifrar los datos en tránsito. Para el tráfico entre fuentes externas (como Internet o un entorno de TI tradicional) y Amazon EC2, los clientes deben utilizar mecanismos de cifrado de transporte estándar y abiertos, como Transport Layer Security (TLS) o redes privadas virtuales (VPN) IPsec, de acuerdo con la Guía. Dentro de una Amazon Virtual Private Cloud (VPC) para los datos que viajan entre instancias de Amazon EC2, el tráfico de red que contiene la PHI también debe estar cifrado; la mayoría de las aplicaciones admiten TLS u otros protocolos que proporcionan un cifrado en tránsito que se puede configurar de forma coherente con la Guía. En el caso de las aplicaciones y protocolos que no admiten el cifrado, las sesiones que transmiten la PHI se pueden enviar a través de túneles cifrados mediante IPsec o implementaciones similares entre instancias.

Amazon Elastic Container Registry

Amazon Elastic Container Registry (Amazon ECR) está integrado con Amazon Elastic Container Service (Amazon ECS) y permite a los clientes almacenar, ejecutar y gestionar fácilmente imágenes de contenedores para aplicaciones que se ejecutan en Amazon ECS. Una vez que los clientes especifiquen el repositorio de Amazon ECR en su definición de tareas, Amazon ECS recuperará las imágenes adecuadas para sus aplicaciones.

No se requieren pasos especiales para usar Amazon ECR con imágenes de contenedores que contienen PHI. Las imágenes de los contenedores se cifran mientras están en tránsito y se

almacenan cifradas mientras están en reposo mediante el cifrado del lado del servidor de Amazon S3 (SSE-S3).

Amazon Elastic Container Service

Amazon Elastic Container Service (Amazon ECS) es un servicio de administración de contenedores altamente escalable y de alto rendimiento que admite contenedores Docker y permite a los clientes ejecutar aplicaciones fácilmente en un clúster gestionado de instancias de Amazon EC2. Amazon ECS elimina la necesidad de que los clientes instalen, operen y escalen su propia infraestructura de administración de clústeres.

Con simples llamadas a la API, los clientes pueden lanzar y detener aplicaciones habilitadas para Docker, consultar el estado completo de su clúster y acceder a muchas funciones conocidas, como los grupos de seguridad, Elastic Load Balancing, los volúmenes de EBS y las funciones de IAM. Los clientes pueden usar Amazon ECS para programar la ubicación de los contenedores en su clúster en función de sus necesidades de recursos y requisitos de disponibilidad.

El uso de ECS con cargas de trabajo que procesan la PHI no requiere ninguna configuración adicional. ECS actúa como un servicio de organización que coordina el lanzamiento de contenedores (cuyas imágenes se almacenan en S3) en EC2 y no funciona con los datos de la carga de trabajo que se está organizando ni sobre ellos. De conformidad con las normas de la HIPAA y el anexo sobre socios AWS comerciales, la PHI debe cifrarse tanto en tránsito como en reposo cuando se accede a ella desde contenedores lanzados con ECS. Hay varios mecanismos de cifrado en reposo disponibles con cada opción de AWS almacenamiento (por ejemplo, S3, EBS y KMS). Garantizar el cifrado completo de la PHI enviada entre contenedores también puede llevar a los clientes a implementar una red superpuesta (como VNS3, Weave Net o similar) para proporcionar una capa de cifrado redundante. No obstante, también debería estar habilitado el registro completo (por ejemplo, mediante CloudTrail) y dirigirse a todos los registros de las instancias del contenedor. CloudWatch

El uso de Firelens y AWS Fluent Bit con cargas de trabajo que procesan la PHI no requiere ninguna configuración adicional, a menos que los registros contengan la PHI. Si los registros contienen PHI, no deben emitirse a los archivos de registro, a menos que el cifrado del disco esté habilitado. En su lugar, configure la aplicación para que emita los registros de salida o error de forma estándar y los recopile automáticamente. FireLens Del mismo modo, no habilite el almacenamiento en búfer de archivos para Fluent Bit, a menos que también esté activado el cifrado del disco. Por último, el destino del registro debe ser compatible encryption-in-transit; todos los complementos de salida del AWS servicio de AWS for Fluent Bit siempre utilizarán el cifrado TLS para exportar los registros.

Amazon Elastic File System (Amazon EFS)

Amazon Elastic File System (Amazon EFS) proporciona un almacenamiento de archivos simple, escalable y elástico para su uso con servicios AWS en la nube y recursos locales. Es fácil de usar y ofrece una interfaz sencilla que permite a los clientes crear y configurar sistemas de archivos de forma rápida y sencilla. Amazon EFS está diseñado para escalar de forma elástica bajo demanda sin interrumpir las aplicaciones, ya que crece y se reduce automáticamente a medida que los clientes añaden y eliminan archivos.

Para cumplir con el requisito de que la PHI esté cifrada en reposo, hay dos rutas disponibles en EFS. EFS admite el cifrado en reposo cuando se crea un nuevo sistema de archivos. Durante la creación, debe seleccionarse la opción «Habilitar el cifrado de datos en reposo». Al seleccionar esta opción, se garantiza que todos los datos colocados en el sistema de archivos EFS se cifrarán mediante el cifrado AES-256 y AWS KMS las claves administradas. Los clientes también pueden optar por cifrar los datos antes de colocarlos en EFS, pero luego son responsables de administrar el proceso de cifrado y la administración de las claves.

La PHI no debe utilizarse total o parcialmente en ningún nombre de archivo o carpeta. El cifrado de la PHI en tránsito para Amazon EFS lo proporciona Transport Layer Security (TLS) entre el servicio de EFS y la instancia que monta el sistema de archivos. EFS ofrece un asistente de montaje para facilitar la conexión a un sistema de archivos mediante TLS. De forma predeterminada, TLS no se utiliza y debe habilitarse al montar el sistema de archivos mediante el asistente de montaje EFS. Asegúrese de que el comando mount contenga la opción «-o tls» para habilitar el cifrado TLS. Como alternativa, los clientes que decidan no utilizar el asistente de montaje de EFS pueden seguir las instrucciones de la documentación de EFS para configurar sus clientes NFS para que se conecten a través de un túnel TLS.

Amazon Elastic Kubernetes Service (Amazon EKS)

Amazon Elastic Kubernetes Service (Amazon EKS) es un servicio gestionado que facilita a los clientes la ejecución de Kubernetes en AWS sin necesidad de instalar o mantener su propio plano de control de Kubernetes. Kubernetes es un sistema de código abierto para automatizar la implementación, escalado y administración de las aplicaciones en contenedores. Para obtener información adicional sobre seguridad y conformidad, consulte el documento técnico Architecting for HIPAA Security and Compliance on Amazon EKS.

Amazon ElastiCache para Redis

Amazon ElastiCache for Redis es un servicio de estructura de datos en memoria compatible con Redis que se puede utilizar como almacén de datos o caché. Para almacenar la PHI, los clientes deben asegurarse de utilizar la versión más reciente del motor de Redis que cumpla con los requisitos de la HIPAA y los tipos de nodos de la generación ElastiCache actual. Amazon ElastiCache for Redis admite el almacenamiento de la PHI para los siguientes tipos de nodos y la versión del motor de Redis:

- Tipos de nodos: solo de la generación actual (por ejemplo, en el momento de la publicación de este documento técnico, M4, M5, R4, R5, T2, T3)
- ElastiCache para la versión del motor Redis: 3.2.6 y 4.0.10 en adelante

Para obtener más información sobre cómo elegir los nodos de la generación actual, consulta los ElastiCache precios de Amazon. Para obtener más información sobre cómo elegir un motor ElastiCache para Redis, consulte ¿Qué es Amazon ElastiCache para Redis?

Los clientes también deben asegurarse de que el clúster y los nodos del clúster estén configurados para cifrar los datos en reposo, habilitar el cifrado de transporte y habilitar la autenticación de los comandos de Redis. Además, los clientes también deben asegurarse en todo momento de que sus clústeres de Redis estén actualizados con las últimas actualizaciones de servicio de tipo «Seguridad» a más tardar en la «fecha de caducidad recomendada» (la fecha en la que se recomienda aplicar la actualización) o antes. Para obtener más información, consulte las secciones siguientes.

Temas

Cifrado en reposo

Amazon ElastiCache for Redis proporciona cifrado de datos para su clúster a fin de ayudar a proteger los datos en reposo. Cuando los clientes habilitan el cifrado en reposo para un clúster en el momento de su creación, Amazon ElastiCache for Redis cifra los datos del disco y automatiza las

copias de seguridad de Redis. Los datos de los clientes en el disco se cifran mediante el estándar de cifrado avanzado (AES) -512 claves simétricas aceleradas por hardware. Las copias de seguridad de Redis se cifran mediante claves de cifrado administradas por Amazon S3 (SSE-S3). Un depósito S3 con el cifrado del lado del servidor activado cifrará los datos mediante 256 claves simétricas del estándar de cifrado avanzado (AES) aceleradas por hardware antes de guardarlos en el depósito.

Para obtener más información sobre las claves de cifrado administradas por Amazon S3 (SSE-S3), consulte Protección de datos mediante el cifrado del lado del servidor con claves de cifrado administradas por Amazon S3 (SSE-S3). En un clúster de ElastiCache Redis (uno o varios nodos) que se ejecute con cifrado, los datos almacenados en reposo se cifran de acuerdo con las directrices vigentes en el momento de la publicación de este documento técnico. Esto incluye los datos en disco y las copias de seguridad automatizadas en un bucket de S3. Dado que la Guía podría actualizarse, los clientes deben seguir evaluando y determinando si el cifrado de Amazon ElastiCache for Redis cumple sus requisitos normativos y de conformidad. Para obtener más información sobre el cifrado en reposo con Amazon ElastiCache for Redis, consulte ¿Qué es Amazon ElastiCache for Redis?

Cifrado en tránsito

Amazon ElastiCache for Redis utiliza TLS para cifrar los datos en tránsito. Las conexiones a ElastiCache Redis que contengan PHI deben utilizar el cifrado de transporte y evaluar la configuración para garantizar su coherencia con las directrices. Para obtener más información, consulte CreateReplicationGroup. Para obtener más información sobre cómo habilitar el cifrado de transporte, consulte ElastiCache Redis In-Transit Encryption (TLS).

Autenticación

Los clústeres de Amazon ElastiCache for Redis (uno o varios nodos) que contienen PHI deben proporcionar un token AUTH de Redis para permitir la autenticación de los comandos de Redis. La autenticación de Redis está disponible cuando están habilitadas tanto el cifrado en reposo como el cifrado en tránsito. Los clientes deben proporcionar un token seguro para Redis AUTH con las siguientes restricciones:

- Deben ser solo caracteres ASCII imprimibles
- Debe tener al menos 16 caracteres y no más de 128 caracteres
- No puede contener ninguno de los siguientes caracteres: '/', "" o «@»

Este token debe configurarse desde el parámetro de solicitud en el momento de la creación del grupo de replicación de Redis (uno o varios nodos) y se puede actualizar más adelante con un nuevo

valor. AWS cifra este token mediante AWS Key Management Service (AWS KMS). Para obtener más información sobre Redis AUTH, consulte Redis In-Transit ElastiCache Encryption (TLS).

Aplicación de actualizaciones de servicio ElastiCache

Los clústeres de Amazon ElastiCache for Redis (uno o varios nodos) que contienen PHI deben actualizarse con las últimas actualizaciones de servicio de tipo «Seguridad» a más tardar en la «Fecha de caducidad recomendada». ElastiCache ofrece esta función de autoservicio que los clientes pueden utilizar para aplicar las actualizaciones en cualquier momento, bajo demanda y en tiempo real. Cada actualización del servicio incluye una «gravedad» y una «fecha de aplicación recomendada» y solo está disponible para los grupos de replicación de Redis correspondientes.

El campo «SLA Cumplido» de la función de actualización del servicio indicará si la actualización se aplicó en la fecha límite recomendada de solicitud o antes. Si los clientes deciden no aplicar las actualizaciones a los grupos de replicación de Redis correspondientes antes de la fecha de solicitud recomendada, no ElastiCache tomarán ninguna medida para aplicarlas. Los clientes pueden utilizar el panel del historial de actualizaciones del servicio para revisar la aplicación de las actualizaciones a sus grupos de replicación de Redis a lo largo del tiempo. Para obtener más información sobre cómo utilizar esta función, consulta Actualizaciones de autoservicio en Amazon ElastiCache.

OpenSearch Servicio Amazon

Amazon OpenSearch Service permite a los clientes ejecutar un clúster de OSS de Elasticsearch heredado OpenSearch o gestionado en una Amazon Virtual Private Cloud (Amazon VPC) dedicada. Al usar OpenSearch Service with PHI, los clientes deben usar Elasticsearch 6.0 OpenSearch o una versión posterior. Los clientes deben asegurarse de que la PHI esté cifrada en reposo y en tránsito dentro de Amazon OpenSearch Service. Los clientes pueden usar el cifrado por AWS KMS clave para cifrar los datos en reposo en sus dominios de OpenSearch servicio, lo que solo está disponible para OpenSearch Elasticsearch 5.1 o versiones posteriores. Para obtener más información sobre cómo cifrar datos en reposo, consulta Cifrado de datos en reposo para Amazon OpenSearch Service.

Cada dominio OpenSearch de servicio se ejecuta en su propia VPC. Los clientes deben habilitar el node-to-node cifrado, que está disponible en todas OpenSearch las versiones, y en Elasticsearch 6.0 o versiones posteriores. Si los clientes envían datos a OpenSearch Service a través de HTTPS, el node-to-node cifrado ayuda a garantizar que sus datos permanezcan cifrados mientras OpenSearch los distribuyen (y redistribuyen) por todo el clúster. Si los datos llegan sin cifrar a través de HTTP, OpenSearch Service los cifra una vez que llegan al clúster. Por lo tanto, cualquier PHI que entre en

un clúster OpenSearch de Amazon Service debe enviarse a través de HTTPS. Para obtener más información, consulta ode-to-node Cifrado N para Amazon OpenSearch Service.

Se pueden capturar los registros de la API de configuración del OpenSearch servicio AWS CloudTrail. Para obtener más información, consulta Cómo monitorizar las llamadas a la API de Amazon OpenSearch Service con AWS CloudTrail.

Amazon EMR

Amazon EMR implementa y administra un clúster de instancias de Amazon EC2 en la cuenta de un cliente. Para obtener información sobre el cifrado con Amazon EMR, consulte Opciones de cifrado.

Amazon EventBridge

Amazon EventBridge (anteriormente Amazon CloudWatch Events) es un bus de eventos sin servidor que le permite crear aplicaciones escalables basadas en eventos. EventBridge ofrece un flujo de datos en tiempo real procedentes de fuentes de eventos, como Zendesk, Datadog o Pagerduty, y dirige esos datos a destinos como los siguientes. AWS Lambda

De forma predeterminada, EventBridge cifra los datos mediante el estándar de cifrado avanzado de 256 bits (AES-256) en virtud de una CMK propiedad de AWS, que ayuda a proteger los datos de los clientes contra el acceso no autorizado. Los clientes deben asegurarse de que cualquier recurso de AWS que emita un evento que almacene, procese o transmita la PHI esté configurado de acuerdo con las prácticas recomendadas.

Amazon EventBridge está integrado AWS CloudTrail y los clientes pueden ver los eventos más recientes de la CloudTrail consola en el Historial de eventos. Para obtener más información, consulta la EventBridge sección Información en CloudTrail.

Amazon Forecast

Amazon Forecast es un servicio totalmente gestionado que utiliza el aprendizaje automático para ofrecer previsiones muy precisas. Basado en la misma tecnología de pronóstico de aprendizaje automático que utiliza Amazon.com. Todas las interacciones que los clientes tienen con Amazon Forecast están protegidas mediante cifrado. Todo el contenido procesado por Amazon Forecast se cifra con las claves de los clientes a través de Amazon Key Management Service y se cifra en reposo en la región de AWS en la que los clientes utilizan el servicio.

Amazon Forecast está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un servicio de AWS en Amazon Forecast. CloudTrail captura todas las llamadas a la API de Amazon Forecast como eventos. Las llamadas capturadas incluyen llamadas desde la consola Amazon Forecast y llamadas en código a las operaciones de la API Amazon Forecast. Si los clientes crean una ruta, pueden habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de Amazon Forecast. Para obtener más información, consulte Registrar llamadas a la API Forecast con AWS CloudTrail.

De forma predeterminada, los archivos de registro que se envían CloudTrail a su bucket se cifran mediante el cifrado del lado del servidor de Amazon con claves de cifrado gestionadas por Amazon S3 (SSE-S3). Para proporcionar una capa de seguridad que se pueda administrar directamente, los clientes pueden utilizar el cifrado del lado del servidor con claves administradas AWS KMS(SSE-KMS) para sus archivos de registro. CloudTrail La habilitación del cifrado del lado del servidor cifra los archivos de registros, pero no los archivos de resumen, con SSE-KMS. Los archivos de resumen se cifran con claves de cifrado administradas por Amazon S3 (SSE-S3).

AWS Forecast importa y exporta datos hacia/desde buckets de S3. Al importar y exportar datos de Amazon S3, los clientes deben asegurarse de que los buckets de S3 estén configurados de manera coherente con las instrucciones. Para obtener más información, consulte Introducción.

Amazon FSx

Amazon FSx es un servicio totalmente gestionado que proporciona sistemas de archivos con muchas funciones y alto rendimiento. Amazon FSx for Windows File Server proporciona un almacenamiento de archivos altamente fiable y escalable, y se puede acceder a él mediante el protocolo Server Message Block (SMB). Amazon FSx for Lustre proporciona almacenamiento de alto rendimiento para cargas de trabajo informáticas y cuenta con la tecnología de Lustre, el sistema de archivos de alto rendimiento más popular del mundo.

Amazon FSx admite dos formas de cifrado para los sistemas de archivos: el cifrado de los datos en tránsito y el cifrado en reposo. Amazon FSx for Windows File Server también admite el registro de todas las llamadas AWS CloudTrail a la API mediante.

Amazon FSx for Windows File Server admite el cifrado de datos en tránsito en instancias informáticas compatibles con el protocolo SMB 3.0 o posterior, y Amazon FSx for Lustre en instancias de Amazon EC2 que admiten el cifrado en tránsito. Como alternativa, los clientes pueden cifrar los datos antes de almacenarlos en Amazon FSx, pero luego son responsables del proceso de cifrado y de la administración de claves.

El cifrado de los datos en reposo se habilita automáticamente al crear un sistema de archivos Amazon FSx mediante el algoritmo de cifrado AES-256 y claves administradas. AWS KMS Los datos y los metadatos se cifran automáticamente antes de escribirse en el sistema de archivos y se descifran automáticamente antes de presentarlos a la aplicación. La PHI no debe usarse en ningún nombre de archivo o carpeta.

Amazon GuardDuty

Amazon GuardDuty es un servicio gestionado de detección de amenazas que monitorea continuamente los comportamientos malintencionados o no autorizados para ayudar a los clientes a proteger sus cuentas y cargas de trabajo de AWS. Supervisa cualquier actividad, como llamadas inusuales a la API o posibles despliegues no autorizados, que indiquen que la cuenta está en peligro. Amazon GuardDuty también detecta instancias potencialmente comprometidas o reconocimientos por parte de los atacantes.

Amazon monitorea y analiza GuardDuty continuamente las siguientes fuentes de datos: registros de flujo de VPC, registros de AWS CloudTrail eventos y registros de DNS. Utiliza fuentes de inteligencia sobre amenazas, como listas de direcciones IP y dominios maliciosos, y aprendizaje automático para identificar actividades inesperadas y potencialmente no autorizadas y maliciosas en un entorno de AWS. Por lo tanto, Amazon no GuardDuty debería encontrar ninguna PHI, ya que estos datos no deben almacenarse en ninguna de las fuentes de datos basadas en AWS enumeradas anteriormente.

Amazon HealthLake

Amazon HealthLake permite a los clientes de los sectores de la salud y las ciencias de la vida almacenar, transformar, consultar y analizar datos de salud a una escala de petabytes. Los clientes pueden usar Amazon HealthLake para transmitir, procesar y almacenar la PHI. Amazon HealthLake cifra los datos en reposo en los almacenes de datos de los clientes de forma predeterminada. Todos los datos y metadatos del servicio se cifran con una clave KMS propiedad del servicio. Según las especificaciones de Fast Healthcare Interoperability Resources (FHIR), si un cliente elimina un recurso del FHIR, solo se ocultará para su recuperación y el servicio lo conservará para el control de versiones. Cuando los clientes utilicen la ImportJob API StartFhir, Amazon HealthLake aplicará el requisito de exportar los datos a un bucket cifrado de Amazon S3.

Amazon HealthLake cifra los datos en tránsito y en reposo. Para el cifrado de los datos en tránsito, puede utilizar las llamadas a la API publicadas por AWS para acceder a HealthLake través de la

red. Los clientes deben ser compatibles con la seguridad de la capa de transporte (TLS) 1.0 o una versión posterior. Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3. Los clientes también deben ser compatibles con conjuntos de cifrado con confidencialidad directa total (PFS) tales como Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos. Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. Como alternativa, los clientes pueden usar el AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes. Para el cifrado de los datos en reposo, Amazon HealthLake cifra los datos de los almacenes de datos del cliente con una clave de AWS KMS propiedad del cliente o mediante una clave de AWS KMS propiedad del servicio de forma predeterminada. Todos los datos y metadatos del servicio se cifran en reposo con una clave de AWS KMS propiedad del servicio.

Amazon HealthLake está integrado con AWS CloudTrail. CloudTrail captura todas las llamadas de API a Amazon HealthLake como eventos, incluidas las llamadas realizadas como resultado de la interacción con AWS Management Console la interfaz de línea de comandos (CLI) y mediante programación mediante el uso del kit de desarrollo de software (SDK).

Amazon Inspector

Amazon Inspector es un servicio de evaluación de seguridad automatizado para los clientes que buscan mejorar la seguridad y el cumplimiento de las aplicaciones implementadas en AWS. Amazon Inspector evalúa automáticamente las aplicaciones en busca de vulnerabilidades o desviaciones respecto a las prácticas recomendadas. Tras realizar una evaluación, Amazon Inspector elabora una lista detallada de los hallazgos de seguridad priorizados por nivel de gravedad. Los clientes pueden ejecutar Amazon Inspector en instancias EC2 que contengan PHI. Amazon Inspector cifra todos los datos transmitidos a través de la red, así como todos los datos de telemetría almacenados en reposo.

Amazon Managed Service para Apache Flink

Amazon Managed Service para Apache Flink permite a los clientes crear rápidamente código SQL que lee, procesa y almacena datos de forma continua casi en tiempo real. Al utilizar consultas SQL estándar en los datos de streaming, los clientes pueden crear aplicaciones que transformen sus datos y les proporcionen información valiosa. El servicio gestionado para Apache Flink admite las entradas de los flujos de entrega de Kinesis Data Streams y Firehose como fuentes para la aplicación de análisis. Si la transmisión está cifrada, Managed Service for Apache Flink accede a

los datos de la transmisión cifrada sin problemas y sin necesidad de realizar más configuraciones. El servicio gestionado para Apache Flink no almacena los datos no cifrados leídos de Kinesis Data Streams. Para obtener más información, consulte Configuración de entrada de la aplicación.

El servicio gestionado para Apache Flink se integra tanto AWS CloudTrail con Amazon Logs como con Amazon CloudWatch Logs para la supervisión de aplicaciones. Para obtener más información, consulte Herramientas de supervisión y Uso de Amazon CloudWatch Logs.

Amazon Data Firehose

Cuando los clientes envían datos de sus productores de datos a su transmisión de datos de Kinesis, Amazon Kinesis Data Streams cifra los datos mediante una AWS KMS clave antes de almacenarlos en reposo. Cuando la transmisión de entrega de Firehose lee datos de la transmisión de Kinesis, Kinesis Data Streams primero descifra los datos y, a continuación, los envía a Firehose. Firehose almacena los datos en la memoria en función de las sugerencias de almacenamiento en búfer especificadas por el cliente.

A continuación, entrega los datos a los destinos sin almacenar los datos no cifrados en reposo. Para obtener más información sobre el cifrado con Firehose, consulte Protección de datos en Amazon Data Firehose.

AWS proporciona varias herramientas que los clientes pueden utilizar para monitorizar Amazon Data Firehose, incluidas CloudWatch las métricas de Amazon, los CloudWatch registros de Amazon Logs, el registro y el historial de Kinesis Agent y API. Para obtener más información, consulte Monitorización de Amazon Data Firehose.

Amazon Kinesis Streams

Amazon Kinesis Streams permite a los clientes crear aplicaciones personalizadas que procesen o analicen los datos de streaming para necesidades específicas. La función de cifrado del lado del servidor permite a los clientes cifrar los datos en reposo. Cuando se habilita el cifrado del lado del servidor, Kinesis Streams utilizará una AWS KMS clave para cifrar los datos antes de almacenarlos en los discos. Para obtener más información, consulte Protección de datos en Amazon Kinesis Data Streams. Las conexiones a Amazon S3 que contienen PHI deben utilizar puntos de enlace que acepten el transporte cifrado (es decir, HTTPS). Para obtener una lista de los puntos de enlace regionales, consulte los puntos de enlace de los servicios de AWS.

Amazon Kinesis Video Streams

Amazon Kinesis Video Streams es un servicio de AWS totalmente gestionado que los clientes pueden utilizar para transmitir vídeo en directo desde los dispositivos a la nube de AWS o crear aplicaciones para el procesamiento de vídeo en tiempo real o el análisis de vídeo orientado a lotes. El cifrado del lado del servidor es una función de Kinesis Video Streams que cifra automáticamente los datos en reposo mediante una AWS KMS clave (anteriormente CMK) especificada por el cliente. Los datos se cifran antes de escribirse en la capa de almacenamiento de transmisiones de Kinesis Video Streams y se descifran una vez recuperados del almacenamiento.

El SDK de Amazon Kinesis Video Streams se puede utilizar para transmitir datos de vídeo en streaming que contengan PHI. De forma predeterminada, el SDK usa TLS para cifrar los fotogramas y fragmentos generados por el dispositivo de hardware en el que está instalado. El SDK no administra ni afecta a los datos almacenados en reposo. Amazon Kinesis Video Streams se AWS CloudTrail utiliza para registrar todas las llamadas a la API.

Amazon Lex

Amazon Lex es un servicio de AWS que permite crear interfaces de conversación para las aplicaciones que usan voz y texto. Con Amazon Lex, el mismo motor conversacional que impulsa Amazon Alexa ahora está disponible para cualquier desarrollador, lo que permite a los clientes crear sofisticados chatbots en lenguaje natural en sus aplicaciones nuevas y existentes. Amazon Lex ofrece la amplia funcionalidad y flexibilidad de la comprensión del lenguaje natural (NLU) y el reconocimiento automático de voz (ASR) para que los clientes puedan crear experiencias de usuario muy atractivas con interacciones conversacionales realistas y crear nuevas categorías de productos.

Lex usa el protocolo HTTPS para comunicarse tanto con los clientes como con otros servicios de AWS. El acceso a Lex se basa en una API y se puede aplicar el mínimo privilegio de IAM adecuado. Para obtener más información, consulte Protección de datos en Amazon Lex.

La supervisión es importante para mantener la fiabilidad, la disponibilidad y el rendimiento de los chatbots Amazon Lex de los clientes. Para realizar un seguimiento del estado de los bots de Amazon Lex, usa Amazon CloudWatch. Con CloudWatch, los clientes pueden obtener métricas de las operaciones individuales de Amazon Lex o de las operaciones globales de Amazon Lex para su cuenta. Los clientes también pueden configurar CloudWatch alarmas para que se les notifique cuando una o más métricas superen un umbral definido por los clientes. Por ejemplo, los clientes pueden controlar la cantidad de solicitudes realizadas a un bot durante un período de tiempo determinado, ver la latencia de las solicitudes aceptadas o activar una alarma cuando los errores

superen un umbral. Lex también está integrado AWS CloudTrail para registrar las llamadas a la API de Lex. Para obtener más información, consulte Supervisión en Amazon Lex.

Amazon Managed Streaming for Apache Kafka (Amazon MSK)

Amazon MSK proporciona funciones de cifrado para los datos en reposo y los datos en tránsito. Para el cifrado de datos en reposo, el clúster de Amazon MSK utiliza el cifrado del lado del servidor de Amazon EBS y AWS KMS las claves para cifrar los volúmenes de almacenamiento. Para los datos en tránsito, los clústeres de Amazon MSK tienen el cifrado habilitado mediante TLS para la comunicación entre intermediarios.

La configuración de cifrado se habilita cuando se crea un clúster. Además, de forma predeterminada, el cifrado en tránsito se establece en TLS para los clústeres creados desde la CLI o AWS la consola. Se requiere una configuración adicional para que los clientes se comuniquen con los clústeres mediante el cifrado TLS. Los clientes pueden cambiar la configuración de cifrado predeterminada seleccionando la configuración de TLS/Plaintext. Para obtener más información, consulte Amazon MSK Encryption.

Los clientes pueden supervisar el rendimiento de los clústeres de los clientes mediante la consola Amazon MSK o la CloudWatch consola Amazon, o pueden acceder a JMX y a las métricas del alojamiento mediante Open Monitoring con Prometheus, una solución de monitoreo de código abierto.

Las herramientas diseñadas para leer datos de los exportadores de Prometheus son compatibles con Open Monitoring, como Datadog, Lenses, New Relic,Sumologic o un servidor Prometheus. Para obtener más información sobre Open Monitoring, consulte la documentación de Amazon MSK Open Monitoring.

Tenga en cuenta que la versión predeterminada de Apache Zookeeper incluida con Apache Kafka no admite el cifrado. Sin embargo, es importante tener en cuenta que las comunicaciones entre los corredores de Apache Zookeeper y Apache Kafka se limitan a la información sobre el corredor, el tema y el estado de la partición. La única forma de generar y consumir datos de un clúster de Amazon MSK es a través de una conexión privada entre sus clientes en su VPC y el clúster de Amazon MSK. Amazon MSK no admite puntos de enlace públicos.

Amazon MQ

Amazon MQ es un servicio gestionado de agentes de mensajes para Apache ActiveMQ que facilita la configuración y el funcionamiento de los agentes de mensajes en la nube. Amazon MQ

funciona con las aplicaciones y los servicios existentes sin necesidad de que el cliente administre, opere o mantenga su propio sistema de mensajería. Para cifrar los datos de la PHI mientras están en tránsito, se deben utilizar los siguientes protocolos con el TLS habilitado para acceder a los intermediarios:

- AMQP
- MQTT
- MQTT ha terminado WebSocket
- OpenWire
- STOMP
- STOMP WebSocket

Amazon MQ cifra los mensajes en reposo y en tránsito mediante claves de cifrado que administra y almacena de forma segura. Amazon MQ registra todas las CloudTrail llamadas a la API.

Amazon Neptune

Amazon Neptune es un servicio de base de datos de gráficos rápido, fiable y completamente administrado que le permite crear y ejecutar fácilmente aplicaciones que funcionen con conjuntos de datos altamente conectados. El núcleo de Amazon Neptune es un motor de base de datos de gráficos de alto rendimiento diseñado específicamente que está optimizado para almacenar miles de millones de relaciones y consultar el gráfico con una latencia de milisegundos. Amazon Neptune es compatible con los populares lenguajes de consulta de gráficos Apache TinkerPop Gremlin y SPARQL del W3C.

Los datos que contienen PHI ahora se pueden conservar en una instancia cifrada de Amazon Neptune. Una instancia cifrada de Amazon Neptune solo se puede especificar en el momento de la creación seleccionando «Enable Encryption» en la consola de Amazon Neptune. Todos los registros, copias de seguridad e instantáneas se cifran para una instancia cifrada de Amazon Neptune. La administración de claves para las instancias cifradas de Amazon Neptune se proporciona a través de. AWS KMS El cifrado de los datos en tránsito se realiza mediante SSL/TLS. Amazon Neptune registra todas las CloudTrail llamadas a la API.

AWS Network Firewall

AWS Network Firewall es un servicio de firewall gestionado que facilita la implementación de las protecciones de red esenciales para todas sus Amazon Virtual Private Cloud (Amazon VPC). El servicio se amplía automáticamente en función del volumen de tráfico de la red para ofrecer protecciones de alta disponibilidad sin necesidad de configurar o mantener la infraestructura subyacente. Tanto las reglas de los clientes como los registros de acceso pueden contener direcciones IP de los usuarios finales, que están cifradas tanto en reposo como en tránsito dentro de la AWS arquitectura. Además, AWS Network Firewall cifra todos los datos en reposo y en tránsito entre los AWS servicios componentes (Amazon S3, Amazon DynamoDB, Amazon Logs CloudWatch , Amazon EBS). El servicio cifra automáticamente los datos sin necesidad de una configuración especial.

Amazon Pinpoint

Amazon Pinpoint ofrece a los desarrolladores una única capa de API, compatibilidad con CLI y compatibilidad con SDK del lado del cliente para ampliar los canales de comunicación de las aplicaciones con los usuarios. Entre los canales aptos se incluyen el correo electrónico, los mensajes de texto SMS, las notificaciones push móviles y los canales personalizados. Amazon Pinpoint también proporciona un sistema de análisis que rastrea el comportamiento de los usuarios de la aplicación y la participación de los usuarios. Con este servicio, los desarrolladores pueden saber cómo prefiere interactuar cada usuario y personalizar la experiencia del usuario para aumentar su satisfacción.

Amazon Pinpoint también ayuda a los desarrolladores a abordar varios casos de uso de la mensajería, como la mensajería directa o transaccional, la mensajería segmentada o de campaña y la mensajería basada en eventos. Al integrar y habilitar todos los canales de participación de los usuarios finales a través de Amazon Pinpoint, los desarrolladores pueden crear una visión integral de la participación de los usuarios en todos los puntos de contacto con los clientes. Amazon Pinpoint almacena datos de usuarios, puntos finales y eventos para que los clientes puedan crear segmentos, enviar mensajes a los destinatarios y capturar datos de participación.

Amazon Pinpoint cifra los datos tanto en reposo como en tránsito. Para obtener más información, consulte las preguntas frecuentes sobre Amazon Pinpoint. Si bien Amazon Pinpoint cifra todos los datos en reposo y en tránsito, es posible que el canal final, como el SMS o el correo electrónico, no esté cifrado, y los clientes deben configurar cualquier canal de forma coherente con sus requisitos.

Además, los clientes que necesiten enviar su PHI a través del canal de SMS deben usar un código corto específico (números de teléfono de origen de 5 o 6 dígitos) con el propósito explícito de enviar la PHI. Para obtener más información sobre cómo solicitar un código corto, consulte Solicitud de códigos cortos dedicados para mensajería SMS con Amazon Pinpoint. Los clientes también pueden optar por no enviar su PHI a través del canal final y, en su lugar, proporcionar un mecanismo para acceder de forma segura a la PHI a través de HTTPS.

Las llamadas de API a Amazon Pinpoint se pueden capturar mediante. AWS CloudTrail Las llamadas capturadas incluyen las de la consola de Amazon Pinpoint y las llamadas en código a las operaciones de la API de Amazon Pinpoint. Si los clientes crean una ruta, pueden habilitar la entrega continua de AWS CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de Amazon Pinpoint. Si los clientes no configuran un registro, pueden seguir viendo los eventos más recientes mediante el historial de eventos de la AWS CloudTrail consola. Con la información recopilada por AWS CloudTrail, los clientes pueden determinar si la solicitud se realizó a Amazon Pinpoint, la dirección IP de la solicitud, quién la realizó, cuándo se realizó la solicitud y detalles adicionales. Para obtener más información, consulte Registrar llamadas a la API de Amazon Pinpoint con. AWS CloudTrail

Amazon Polly

Amazon Polly es un servicio en la nube que convierte el texto en un segmento hablado muy realista. Amazon Polly proporciona operaciones de API sencillas que los clientes pueden integrar fácilmente con las aplicaciones existentes. Amazon Polly usa el protocolo HTTPS para comunicarse con los clientes. El acceso a Amazon Polly se basa en una API y se pueden aplicar los privilegios mínimos de IAM adecuados. Para obtener más información, consulte Protección de datos. Algunos ejemplos de casos de uso que incluyen la PHI:

- El cuidador convierte un informe de texto que contiene la PHI en un discurso sintetizado para que pueda escuchar el informe mientras camina o realiza otras tareas.
- El paciente con discapacidad visual recibe orientación médica y la utiliza en forma de discurso sintetizado.

El canal de entrega final de Amazon Polly podría provocar la reproducción de audio con PHI en un espacio público y se deben tomar precauciones para que la entrega tenga esto en cuenta. La salida de voz sintetizada también se puede enviar de forma asíncrona a un bucket de Amazon S3 con el cifrado activado.

Cuando se produce una actividad de eventos admitida en Amazon Polly, esa actividad se registra en un AWS CloudTrail evento junto con otros eventos de AWS servicio en el Historial de eventos. Para obtener un registro continuo de los eventos en la AWS cuenta de un cliente, incluidos los eventos de Amazon Polly, crea una ruta. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. Con la información recopilada por CloudTrail, los clientes pueden determinar la solicitud que se realizó a Amazon Polly, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Amazon Quantum Ledger Database (Amazon QLDB)

Amazon QLDB es una base de datos de contabilidad completamente administrada en la que se proporciona un registro de transacciones transparente, inmutable y que se puede verificar mediante criptografía, cuya propiedad denota una autoridad central de confianza. Amazon QLDB realiza un seguimiento de todos y cada uno de los cambios en los datos de las aplicaciones y mantiene un historial completo y verificable de los cambios a lo largo del tiempo. Los datos que contienen la PHI ahora se pueden conservar en una instancia de QLDB. De forma predeterminada, todos los datos de Amazon QLDB en tránsito y en reposo están cifrados. Los datos en tránsito se cifran mediante TLS y los datos en reposo se cifran mediante AWS claves administradas. Con fines de protección de datos, recomendamos a los clientes que protejan las credenciales de las AWS cuentas y configuren cuentas de usuario individuales con AWS Identity and Access Management (IAM), de modo que cada usuario solo reciba los permisos necesarios para cumplir con sus obligaciones laborales. Para obtener más información, consulte Protección de datos en Amazon QLDB.

Amazon QLDB está integrado AWS CloudTrail con un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en QLDB. CloudTrail captura todas las llamadas a la API del plano de control para la QLDB como eventos. Las llamadas capturadas incluyen las realizadas desde la consola de QLDB y las llamadas de código a las operaciones de la API de QLDB. Si los clientes crean un registro, pueden habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon Simple Storage Service (Amazon S3), incluidos los eventos de QLDB. Si los clientes no configuran un registro, pueden seguir viendo los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por CloudTrail, los clientes pueden determinar la solicitud que se realizó a la QLDB, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Amazon QuickSight

Amazon QuickSight es un servicio de análisis empresarial que los clientes pueden utilizar para crear visualizaciones, realizar análisis ad hoc y obtener rápidamente información empresarial a partir de sus datos. Amazon QuickSight descubre las fuentes de AWS datos, permite a las organizaciones escalar hasta cientos de miles de usuarios y ofrece un rendimiento con capacidad de respuesta mediante el uso de un sólido motor en memoria (SPICE).

Los clientes solo pueden usar la edición Enterprise de Amazon QuickSight para trabajar con datos que contengan PHI, ya que admite el cifrado de los datos almacenados en reposo en SPICE. El cifrado de datos se realiza mediante claves AWS gestionadas.

Amazon RDS para MariaDB

Amazon RDS for MariaDB permite a los clientes cifrar las bases de datos de MariaDB mediante claves que administran. AWS KMS En una instancia de base de datos que se ejecuta con el cifrado de Amazon RDS, los datos almacenados en reposo en el almacenamiento subyacente se cifran de acuerdo con las directrices vigentes en el momento de la publicación de este documento técnico, al igual que las copias de seguridad automatizadas, las réplicas de lectura y las instantáneas.

Dado que la Guía podría actualizarse, los clientes deben seguir evaluando y determinando si el cifrado Amazon RDS for MariaDB cumple sus requisitos normativos y de conformidad. Para obtener más información sobre el cifrado en reposo mediante Amazon RDS, consulte Cifrar los recursos de Amazon RDS.

Las conexiones a RDS para MariaDB que contienen PHI deben utilizar el cifrado de transporte. Para obtener más información sobre cómo habilitar las conexiones cifradas, consulte Uso de SSL/TLS para cifrar una conexión a una instancia de base de datos.

Amazon RDS para MySQL

Amazon RDS for MySQL permite a los clientes cifrar las bases de datos MySQL mediante claves que los clientes AWS KMS administran. En una instancia de base de datos que se ejecuta con el cifrado de Amazon RDS, los datos almacenados en reposo en el almacenamiento subyacente se cifran de acuerdo con las directrices vigentes en el momento de la publicación de este documento técnico, al igual que las copias de seguridad automatizadas, las réplicas de lectura y las instantáneas.

Dado que la Guía podría actualizarse, los clientes deben seguir evaluando y determinando si el cifrado Amazon RDS for MySQL cumple sus requisitos normativos y de conformidad. Para obtener

más información sobre el cifrado en reposo mediante Amazon RDS, consulte Cifrar los recursos de Amazon RDS.

Las conexiones a RDS para MySQL que contienen PHI deben utilizar el cifrado de transporte. Para obtener más información sobre cómo habilitar las conexiones cifradas, consulte Uso de SSL/TLS para cifrar una conexión a una instancia de base de datos.

Amazon RDS para Oracle

Los clientes disponen de varias opciones para cifrar la PHI en reposo mediante Amazon RDS for Oracle. Los clientes pueden cifrar las bases de datos de Oracle mediante claves que gestionan. AWS KMS En una instancia de base de datos que se ejecuta con el cifrado de Amazon RDS, los datos almacenados en reposo en el almacenamiento subyacente se cifran de acuerdo con las directrices vigentes en el momento de la publicación de este documento técnico, al igual que las copias de seguridad automatizadas, las réplicas de lectura y las instantáneas.

Dado que la Guía podría actualizarse, los clientes deben seguir evaluando y determinando si el cifrado de Amazon RDS for Oracle cumple sus requisitos normativos y de conformidad. Para obtener más información sobre el cifrado en reposo mediante Amazon RDS, consulte Cifrar los recursos de Amazon RDS.

Los clientes también pueden utilizar el cifrado de datos transparente (TDE) de Oracle y deben evaluar la configuración para garantizar su coherencia con las directrices. El TDE de Oracle es una función de la opción Oracle Advanced Security disponible en Oracle Enterprise Edition. Esta característica cifra automáticamente los datos antes de que se escriban en el sistema de almacenamiento y los descifra automáticamente cuando se leen. Los clientes también pueden utilizar AWS CloudHSM para almacenar claves TDE de Oracle de Amazon RDS. Para más información, consulte los siguientes temas:

- Cifrado transparente de datos de Amazon RDS para Oracle: cifrado de datos transparente de Oracle.
- Uso AWS CloudHSM para almacenar claves TDE de Oracle de Amazon RDS: ¿Qué es Amazon Relational Database Service (Amazon RDS)?

Las conexiones a Amazon RDS for Oracle que contengan PHI deben utilizar el cifrado de transporte y evaluar la configuración para garantizar su coherencia con la Guía. Esto se logra mediante el cifrado de red nativo de Oracle y se habilita en los grupos de opciones de Amazon RDS for Oracle. Para obtener información detallada, consulte Oracle Native Network Encryption.

Amazon RDS para PostgreSQL

Amazon RDS for PostgreSQL permite a los clientes cifrar las bases de datos de PostgreSQL mediante claves que los clientes administran. AWS KMS En una instancia de base de datos que se ejecuta con el cifrado de Amazon RDS, los datos almacenados en reposo en el almacenamiento subyacente se cifran de acuerdo con las directrices vigentes en el momento de la publicación de este documento técnico, al igual que las copias de seguridad automatizadas, las réplicas de lectura y las instantáneas.

Dado que la Guía podría actualizarse, los clientes deben seguir evaluando y determinando si el cifrado Amazon RDS for PostgreSQL cumple sus requisitos normativos y de conformidad. Para obtener más información sobre el cifrado en reposo mediante Amazon RDS, consulte Cifrar los recursos de Amazon RDS.

Las conexiones a RDS para PostgreSQL que contienen PHI deben utilizar el cifrado de transporte. Para obtener más información sobre cómo habilitar las conexiones cifradas, consulte Uso de SSL/TLS para cifrar una conexión a una instancia de base de datos.

Amazon RDS para SQL Server

RDS para SQL Server admite el almacenamiento de la PHI para las siguientes combinaciones de versiones y ediciones:

- 2008 R2: solo Enterprise Edition
- 2012, 2014 y 2016: ediciones web, estándar y empresarial

Importante: la edición SQL Server Express no es compatible y nunca debe utilizarse para almacenar la PHI.

Para almacenar la PHI, los clientes deben asegurarse de que la instancia esté configurada para cifrar los datos en reposo y habilitar el cifrado y la auditoría del transporte, como se detalla a continuación.

Cifrado en reposo

Los clientes pueden cifrar las bases de datos de SQL Server mediante claves que administran. AWS KMS En una instancia de base de datos que se ejecuta con el cifrado de Amazon RDS, los datos almacenados en reposo en el almacenamiento subyacente se cifran de acuerdo con las directrices

vigentes en el momento de la publicación de este documento técnico, al igual que las copias de seguridad e instantáneas automatizadas. Dado que la Guía podría actualizarse, los clientes deben seguir evaluando y determinando si el cifrado Amazon RDS for SQL Server cumple sus requisitos normativos y de conformidad. Para obtener más información sobre el cifrado en reposo mediante Amazon RDS, consulte Cifrar los recursos de Amazon RDS.

Si los clientes utilizan SQL Server Enterprise Edition, pueden utilizar el cifrado de datos transparente para servidores (TDE) como alternativa. Esta característica cifra automáticamente los datos antes de que se escriban en el sistema de almacenamiento y los descifra automáticamente cuando se leen. Para obtener más información sobre el cifrado de datos transparente de RDS para SQL Server, consulte Support for Transparent Data Encryption in SQL Server.

Cifrado en tránsito

Las conexiones a Amazon RDS for SQL Server que contengan PHI deben utilizar el cifrado de transporte proporcionado por SQL Server Forced SSL. El SSL forzado se habilita desde el grupo de parámetros de Amazon RDS SQL Server. Para obtener más información sobre RDS para SSL forzado de SQL Server, consulte Uso de SSL con una instancia de base de datos de Microsoft SQL Server.

Auditoría

Las instancias de RDS para SQL Server que contienen PHI deben tener habilitada la auditoría. La auditoría se habilita desde el grupo de parámetros de Amazon RDS SQL Server. Para obtener más información sobre la auditoría de RDS para SQL Server, consulte Compliance Program Support for Microsoft SQL Server DB Instances.

Amazon Redshift

Amazon Redshift proporciona cifrado de bases de datos para sus clústeres a fin de proteger los datos en reposo. Cuando los clientes habilitan el cifrado de un clúster, Amazon Redshift cifra todos los datos, incluidas las copias de seguridad, mediante claves simétricas del Estándar de cifrado avanzado (AES) -256 aceleradas por hardware. Amazon Redshift usa una arquitectura de cuatro niveles basada en claves para el cifrado. Estas claves se componen de claves de cifrado de datos, una clave de base de datos, una clave de clúster y una clave KMS.

La clave del clúster cifra la clave de base de datos del clúster de Amazon Redshift. Los clientes pueden usar uno AWS KMS o varios AWS CloudHSM (módulos de seguridad de hardware) para

administrar la clave del clúster. El cifrado en reposo de Amazon Redshift es coherente con las directrices vigentes en el momento de la publicación de este documento técnico. Dado que la Guía podría actualizarse, los clientes deben seguir evaluando y determinando si el cifrado de Amazon Redshift cumple sus requisitos normativos y de conformidad. Para obtener más información, consulte Cifrado de base de datos de Amazon Redshift.

Las conexiones a Amazon Redshift que contienen PHI deben utilizar el cifrado de transporte y los clientes deben evaluar la configuración para garantizar su coherencia con las directrices. Para obtener más información, consulte Configuración de las opciones de seguridad para las conexiones. Amazon Redshift Spectrum permite a los clientes ejecutar consultas SQL de Amazon Redshift en exabytes de datos en Amazon S3. Redshift Spectrum es una función de Amazon Redshift y, por lo tanto, también está incluida en el ámbito de aplicación de la HIPAA BAA.

Amazon Rekognition

Amazon Rekognition facilita la adición de análisis de imágenes y vídeos a las aplicaciones de los clientes. Un cliente solo necesita proporcionar una imagen o un vídeo a la API Amazon Rekognition, y el servicio puede identificar los objetos, las personas, el texto, las escenas y las actividades, así como detectar cualquier contenido inapropiado. Amazon Rekognition también ofrece análisis y reconocimiento facial de alta precisión.

Amazon Rekognition cumple los requisitos para operar con imágenes o vídeos que contengan PHI. Amazon Rekognition funciona como un servicio gestionado y no presenta ninguna opción configurable para la gestión de datos. Amazon Rekognition solo usa, divulga y conserva la PHI según lo permitido por los términos de la BAA. AWS Todos los datos en reposo y en tránsito se cifran con Amazon Rekognition. Amazon AWS CloudTrail Rekognition registra todas las llamadas a la API.

Amazon Route 53

Amazon Route 53 es un servicio de DNS administrado que ofrece a los clientes la posibilidad de registrar nombres de dominio, enrutar el tráfico de Internet, los recursos de dominio de los clientes y comprobar el estado de esos recursos. Si bien Amazon Route 53 es un servicio que cumple con los requisitos de la HIPAA, no se debe almacenar ninguna PHI en los nombres o etiquetas de los recursos de Amazon Route 53, ya que no se admite el cifrado de dichos datos. En cambio, Amazon Route 53 se puede utilizar para proporcionar acceso a los recursos del dominio del cliente que transmiten o almacenan la PHI, como los servidores web que se ejecutan en Amazon EC2 o el almacenamiento, como Amazon S3.

Amazon S3 Glacier

Amazon S3 Glacier cifra automáticamente los datos en reposo mediante claves simétricas AES de 256 bits y admite la transferencia segura de los datos de los clientes a través de protocolos seguros. Las conexiones a Amazon S3 Glacier que contienen PHI deben utilizar puntos de enlace que acepten el transporte cifrado (HTTPS). Para obtener una lista de los puntos de enlace regionales, consulte los puntos de enlace del AWS servicio.

No utilice la PHI en los nombres o metadatos de los archivos y almacenes, ya que estos datos no se cifran mediante el cifrado del lado del servidor de Amazon S3 Glacier y, por lo general, no se cifran en las arquitecturas de cifrado del lado del cliente.

Amazon S3 Transfer Acceleration

Amazon S3 Transfer Acceleration (S3TA) permite transferencias de archivos rápidas, fáciles y seguras a largas distancias entre el cliente de un cliente y un bucket de S3. Transfer Acceleration aprovecha las ubicaciones CloudFront perimetrales distribuidas por todo el mundo de Amazon. A medida que los datos llegan a una ubicación de borde, se redirigen a Amazon S3 a través de una ruta de red optimizada. Los clientes deben asegurarse de que todos los datos que contengan PHI transferidos mediante AWS S3TA estén cifrados tanto en tránsito como en reposo. Consulte la Guía de Amazon S3 para conocer las opciones de cifrado disponibles.

Amazon SageMaker

Amazon SageMaker es un servicio de aprendizaje automático totalmente gestionado. Con Amazon SageMaker, los científicos de datos y los desarrolladores pueden crear y entrenar modelos de aprendizaje automático de forma rápida y sencilla y, a continuación, implementarlos directamente en un entorno hospedado listo para la producción. Proporciona una instancia de cuaderno de creación de Jupyter integrada para acceder fácilmente a las fuentes de datos para su exploración y análisis. Amazon SageMaker también proporciona algoritmos de aprendizaje automático comunes que están optimizados para ejecutarse de manera eficiente con datos extremadamente grandes en un entorno distribuido.

Con soporte bring-your-own-algorithms y marcos nativos, Amazon SageMaker ofrece opciones de formación distribuidas y flexibles que se ajustan a los flujos de trabajo específicos del cliente. Amazon SageMaker cumple los requisitos para operar con datos que contengan PHI. El cifrado de los datos en tránsito lo proporciona SSL/TLS y se utiliza tanto en la comunicación con la interfaz

front-end de SageMaker Amazon (al portátil) como siempre que SageMaker Amazon interactúa con cualquier AWS otro servicio (por ejemplo, al extraer datos de Amazon S3).

Para cumplir con el requisito de que la PHI esté cifrada en reposo, se habilita el cifrado de los datos almacenados con la instancia que ejecuta modelos con Amazon SageMaker mediante AWS Key Management Service (KMS) al configurar el punto final (DescribeEndpointConfig: KmsKey ID). El cifrado de los resultados del entrenamiento de los modelos (artefactos) se habilita mediante el uso AWS KMS y las claves deben especificarse mediante el KmsKey ID que aparece en la OutputDataConfig descripción. Si no se proporciona un ID de clave de KMS, se utilizará la clave KMS de Amazon S3 predeterminada para la cuenta del rol. Amazon SageMaker suele AWS CloudTrail registrar todas las llamadas a la API.

Amazon Simple Notification Service (Amazon SNS)

Los clientes deben comprender el siguiente requisito de cifrado de claves para poder utilizar Amazon Simple Notification Service (SNS) con Protected Health Information (PHI). Los clientes deben usar el punto de enlace de la API HTTPS que proporciona SNS en cada AWS región. El punto final HTTPS aprovecha las conexiones cifradas y protege la privacidad y la integridad de los datos a los que se envían. AWS Para obtener una lista de todos los puntos de enlace de la API HTTPS, consulta los puntos de enlace del AWS servicio.

Además, Amazon SNS utiliza CloudTrail un servicio que captura las llamadas a la API realizadas por Amazon SNS o en su nombre en la cuenta AWS del cliente y entrega los archivos de registro a un bucket de Amazon S3 que especifique. CloudTrail captura las llamadas a la API realizadas desde la consola de Amazon SNS o desde la API de Amazon SNS. Con la información recopilada por CloudTrail, los clientes pueden determinar qué solicitud se realizó a Amazon SNS, la dirección IP de origen desde la que se realizó la solicitud, quién la hizo y cuándo se hizo. Para obtener más información sobre el registro de las operaciones de SNS, consulte Registrar las llamadas a la API de Amazon SNS mediante. CloudTrail

Amazon Simple Email Service (Amazon SES)

Amazon Simple Email Service (Amazon SES) es un servicio de envío y recepción de correo electrónico flexible y altamente escalable. Es compatible con los protocolos S/MIME y PGP para cifrar los mensajes y lograr un end-to-end cifrado completo, y todas las comunicaciones con Amazon SES se protegen mediante SSL (TLS 1.2). Los clientes tienen la opción de almacenar los mensajes cifrados en reposo configurando Amazon SES para recibir y cifrar los mensajes antes de

almacenarlos en un bucket de Amazon S3. Para obtener más información, consulte Cómo AWS KMS utiliza Amazon Simple Email Service (Amazon SES) para obtener más información sobre el cifrado de mensajes para su almacenamiento. Los mensajes se protegen en tránsito a Amazon SES a través de un punto de conexión HTTPS o de una conexión SMTP cifrada.

En el caso de los mensajes enviados desde Amazon SES a un receptor, Amazon SES intentará primero establecer una conexión segura con el servidor de correo receptor, pero si no se puede establecer una conexión segura, enviará el mensaje sin cifrar. Para requerir el cifrado para la entrega a un destinatario, los clientes deben crear un conjunto de configuración en Amazon SES y usar el AWS CLI para establecer la TlsPolicy propiedad en Requerido. Para obtener más información, consulte Amazon SES y los protocolos de seguridad. Amazon SES se integra AWS CloudTrail para supervisar todas las llamadas a la API. Con la información recopilada por AWS CloudTrail, los clientes pueden determinar si la solicitud se realizó a Amazon SES, la dirección IP de la solicitud, quién la realizó, cuándo se realizó la solicitud y detalles adicionales. Para obtener más información, consulte Registrar llamadas a la API de Amazon SES con AWS CloudTrail. Amazon SES también proporciona métodos para supervisar la actividad de envío, como los envíos, los rechazos, las tasas de rebote, las entregas, las aperturas y los clics. Para obtener más información, consulte Supervisión de la actividad de envío de Amazon SES.

Amazon Simple Queue Service (Amazon SQS)

Los clientes deben comprender los siguientes requisitos de cifrado de claves para poder utilizar Amazon SQS con PHI.

- La comunicación con Amazon SQS Queue a través de la solicitud de consulta debe cifrarse con HTTPS. Para obtener más información sobre cómo realizar solicitudes de SQS, consulte Realizar solicitudes a la API de Query.
- Amazon SQS admite el cifrado del lado del servidor integrado con el AWS KMS para proteger los datos en reposo. La incorporación del cifrado del lado del servidor permite a los clientes transmitir y recibir datos confidenciales con la mayor seguridad que supone el uso de colas cifradas. El cifrado del lado del servidor de Amazon SQS utiliza el estándar de cifrado avanzado de 256 bits (algoritmo AES-256 GCM) para cifrar el cuerpo de cada mensaje. La integración con AWS KMS permite a los clientes gestionar de forma centralizada las claves que protegen los mensajes de Amazon SQS junto con las claves que protegen sus demás AWS recursos. AWS KMS registra cada uso de las claves de cifrado para ayudar AWS CloudTrail a satisfacer las necesidades normativas y de conformidad. Para obtener más información y comprobar la disponibilidad de SSE para Amazon SQS en la región, consulte Encryption at Rest.

- Si no se utiliza el cifrado del lado del servidor, la carga útil del mensaje en sí debe cifrarse antes de enviarse a SQS. Una forma de cifrar la carga útil del mensaje consiste en utilizar el Amazon SQS Extended Client junto con el cliente de cifrado Amazon S3. Para obtener más información sobre el uso del cifrado del lado del cliente, consulte Cifrado de cargas útiles de mensajes mediante Amazon SQS Extended Client y Amazon S3 Encryption Client.

Amazon SQS utiliza CloudTrail un servicio que registra las llamadas a la API realizadas por Amazon SQS o en su nombre en la cuenta de un cliente y entrega los archivos AWS de registro al bucket de Amazon S3 especificado. CloudTrail captura las llamadas a la API realizadas desde la consola de Amazon SQS o desde la API de Amazon SQS. Los clientes pueden usar la información recopilada CloudTrail para determinar qué solicitudes se realizan a Amazon SQS, la dirección IP de origen desde la que se realiza la solicitud, quién la realizó, cuándo se realizó, etc. Para obtener más información sobre el registro de las operaciones de SQS, consulte Registrar las llamadas a la API de Amazon SQS mediante. AWS CloudTrail

Amazon Simple Storage Service (Amazon S3)

Los clientes disponen de varias opciones para cifrar los datos en reposo cuando utilizan Amazon S3, que incluyen el cifrado del lado del servidor y del lado del cliente, y varios métodos de administración de claves. Para obtener más información, consulte Protección de datos mediante cifrado.

Las conexiones a Amazon S3 que contienen PHI deben utilizar puntos de enlace que acepten el transporte cifrado (HTTPS). Para obtener una lista de los puntos de enlace regionales, consulte los puntos de enlace del AWS servicio.

No utilice la PHI en los nombres de los cubos, los nombres de los objetos o los metadatos, ya que estos datos no se cifran mediante el cifrado S3 del lado del servidor y, por lo general, no se cifran en las arquitecturas de cifrado del lado del cliente.

Amazon Simple Workflow Service

Amazon Simple Workflow Service (Amazon SWF) ayuda a los desarrolladores a crear, ejecutar y escalar trabajos en segundo plano que tienen pasos paralelos o secuenciales. Amazon SWF puede considerarse como un rastreador de estado y un coordinador de tareas totalmente gestionado en la nube.

El Amazon Simple Workflow Service se utiliza para organizar los flujos de trabajo y no puede almacenar ni transmitir datos. La PHI no debe incluirse en los metadatos de Amazon SWF ni en

ninguna descripción de tarea. Amazon SWF se utiliza AWS CloudTrail para registrar todas las llamadas a la API.

Amazon Textract

Amazon Textract utiliza tecnologías de aprendizaje automático para extraer automáticamente el texto y los datos de los documentos escaneados, algo que va más allá del simple reconocimiento óptico de caracteres (OCR) para identificar, comprender y extraer datos de formularios y tablas. Por ejemplo, los clientes pueden usar Amazon Textract para extraer datos automáticamente y procesar formularios con información de salud protegida (PHI) sin intervención humana para cumplir con las reclamaciones médicas.

Amazon Textract también se puede utilizar para mantener la conformidad en los archivos de documentos. Por ejemplo, los clientes pueden usar Amazon Textract para extraer datos de reclamaciones de seguros o recetas médicas y reconocer automáticamente los pares clave-valor de esos documentos para poder redactar los confidenciales.

Amazon Textract admite el cifrado del lado del servidor (SSE-S3 y SSE-KMS) para los documentos de entrada y el cifrado TLS para los datos en tránsito entre el servicio y el agente. Los clientes pueden usar Amazon CloudWatch para realizar un seguimiento de las métricas de uso de recursos y AWS CloudTrail capturar las llamadas de API a Amazon Textract.

Amazon Transcribe

Amazon Transcribe utiliza tecnologías avanzadas de aprendizaje automático para reconocer el habla en los archivos de audio y transcribirlos en texto. Por ejemplo, los clientes pueden usar Amazon Transcribe para convertir audio en texto en inglés estadounidense y español mexicano y crear aplicaciones que incorporen el contenido de los archivos de audio. Amazon Transcribe se puede utilizar con datos que contengan PHI. Amazon Transcribe no retiene ni almacena ningún dato y todas las llamadas a la API se cifran con SSL/TLS. Amazon Transcribe se utiliza CloudTrail para registrar todas las llamadas a la API.

Amazon Translate

Amazon Translate utiliza tecnologías avanzadas de aprendizaje automático para ofrecer traducciones bajo demanda de alta calidad. Los clientes pueden usar Amazon Translate para traducir documentos de texto no estructurados o para crear aplicaciones que funcionen en varios idiomas.

Los documentos que contienen PHI se pueden procesar con Amazon Translate. No se requiere ninguna configuración adicional al traducir documentos que contienen PHI. El cifrado de los datos en tránsito se realiza mediante SSL/TLS y Amazon Translate no deja ningún dato en reposo. Amazon Translate registra todas las llamadas CloudTrail a la API.

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud (Amazon VPC) ofrece un conjunto de funciones de seguridad de red perfectamente adaptadas a la arquitectura de las cargas de trabajo reguladas por la HIPAA. Características como las listas de control de acceso a la red sin estado y la reasignación dinámica de instancias en grupos de seguridad con estado ofrecen flexibilidad a la hora de proteger las instancias contra el acceso no autorizado a la red.

Amazon VPC también permite a los clientes ampliar su propio espacio AWS de direcciones de red y ofrece varias formas de conectar sus centros de datos. AWS Los registros de flujo de VPC proporcionan un registro de auditoría de las conexiones aceptadas y rechazadas a las instancias que procesan, transmiten o almacenan la PHI.

AWS Transit Gateway actúa como un centro de red y simplifica la conectividad entre las VPC de Amazon y las redes locales. AWS Transit Gateway también proporciona capacidades de interconexión interregional con otras pasarelas de tránsito para establecer una red global utilizando la red troncal. AWS Para obtener más información sobre Amazon VPC, consulte Amazon Virtual Private Cloud.

Amazon WorkDocs

Amazon WorkDocs es un servicio empresarial de almacenamiento e intercambio de archivos seguro y totalmente gestionado con sólidos controles administrativos y capacidades de retroalimentación que mejoran la productividad de los usuarios. Amazon WorkDocs los archivos se cifran en reposo mediante claves que los clientes gestionan mediante AWS Key Management Service (AWS KMS). Todos los datos en tránsito se cifran mediante SSL/TLS. AWS Las aplicaciones web y móviles y los clientes de sincronización de escritorio transmiten los archivos directamente mediante SSL/TLS. Amazon WorkDocs

Con la consola Amazon WorkDocs de administración, WorkDocs los administradores pueden ver los registros de auditoría para realizar un seguimiento de la actividad de los archivos y los usuarios por tiempo y elegir si permiten a los usuarios compartir archivos con otras personas ajenas a su

organización. Amazon WorkDocs también está integrado con CloudTrail (un servicio que captura las llamadas a la API realizadas por la AWS cuenta del cliente o Amazon WorkDocs en su nombre) y entrega los archivos de CloudTrail registro a un bucket de Amazon S3 que los clientes especifiquen.

La autenticación multifactor (MFA) mediante un servidor RADIUS está disponible y puede proporcionar a los clientes una capa de seguridad adicional durante el proceso de autenticación. Los usuarios inician sesión introduciendo su nombre de usuario y contraseña seguidos de un OTP (código de acceso de un solo uso) suministrado mediante un token de hardware o software.

Para obtener más información, consulte:

- Amazon WorkDocs feature
- Registrar Amazon WorkDocs las llamadas a la API mediante AWS CloudTrail

Los clientes no deben almacenar la PHI en los nombres de archivos o directorios.

Amazon WorkSpaces

Amazon WorkSpaces es una solución de esktop-as-a servicio D (DaaS) totalmente gestionada y segura que se ejecuta en. AWS Con Amazon WorkSpaces, los clientes pueden aprovisionar fácilmente escritorios Microsoft Windows virtuales basados en la nube para sus usuarios, proporcionándoles acceso a los documentos, las aplicaciones y los recursos que necesitan, en cualquier lugar, en cualquier momento y desde cualquier dispositivo compatible.

Amazon WorkSpaces almacena los datos en volúmenes de Amazon Elastic Block Store. Los clientes pueden cifrar los volúmenes de WorkSpaces almacenamiento de los clientes mediante claves que los clientes administran. AWS Key Management Service Cuando el cifrado está activado en a WorkSpace, tanto los datos almacenados en reposo en el almacenamiento subyacente como las copias de seguridad automatizadas (instantáneas de EBS) del almacenamiento en disco se cifran de acuerdo con la Guía. La comunicación entre los WorkSpace clientes y los clientes WorkSpace está protegida mediante SSL/TLS. Para obtener más información sobre el cifrado en reposo con Amazon WorkSpaces, consulta Encrypted WorkSpaces.

AWS App Mesh

AWS App Mesh es una malla de servicios que proporciona redes a nivel de aplicación para facilitar que sus servicios se comuniquen entre sí a través de varios tipos de infraestructura informática,

como los servicios de Amazon ECS, Amazon EKS o Amazon EC2. App Mesh configura los proxies de Envoy para recopilar y transmitir datos de observabilidad a los conjuntos de monitoreo que configure, a fin de brindarle visibilidad. end-to-end Puede enrutar el tráfico en función de las políticas de enrutamiento y tráfico configuradas para garantizar la alta disponibilidad de sus aplicaciones. El tráfico entre aplicaciones se puede configurar para que utilice TLS. App Mesh se puede utilizar mediante el AWS SDK o el controlador App Mesh para Kubernetes. Si bien AWS App Mesh es un servicio que cumple con los requisitos de la HIPAA, no se debe almacenar ninguna PHI en los nombres o atributos de los recursos, AWS App Mesh ya que no existe ningún soporte para proteger dichos datos. En cambio, se AWS App Mesh puede usar para monitorear, controlar y proteger los recursos del dominio del cliente que transmiten o almacenan la PHI.

AWS Servicio de migración de aplicaciones

AWS El servicio de migración de aplicaciones (AWS MGN) le permite migrar rápidamente sus servidores y aplicaciones AWS, sin cambios y con un tiempo de inactividad mínimo. AWS MGN es el principal servicio de migración recomendado para realizar migraciones temporales a. AWS

AWS MGN utiliza la replicación de datos a nivel de bloques para copiar los discos de origen directamente a los volúmenes de EBS de la cuenta del cliente; los datos nunca se transmiten a través de un entorno de nube controlado por AWS MGN. De forma predeterminada, los datos replicados se cifran en tránsito. Los datos de los volúmenes de EBS del cliente se cifran de forma predeterminada mediante las propias claves del cliente.

AWS Auto Scaling

AWS Auto Scaling permite a los clientes configurar el escalado automático de AWS los recursos que forman parte de la aplicación del cliente en cuestión de minutos. Los clientes pueden usar AWS Auto Scaling para varios servicios que involucran PHI, como Amazon DynamoDB, Amazon ECS, réplicas Aurora de Amazon RDS e instancias de Amazon EC2 en un grupo de Auto Scaling.

AWS Auto Scaling es un servicio de organización que no procesa, almacena ni transmite directamente el contenido del cliente; por esa razón, los clientes pueden usar este servicio con contenido cifrado. El modelo de responsabilidad AWS compartida se aplica a la protección de datos en AWS Auto Scaling: AWS es responsable de los procedimientos de seguridad de la AWS red, mientras que el cliente es responsable de mantener el control sobre el contenido del cliente que está alojado en esta infraestructura. Este contenido incluye las tareas de configuración y administración de la seguridad de los AWS servicios que utilizan los clientes. Con fines de protección de datos,

recomendamos a los clientes que protejan las credenciales de las AWS cuentas y configuren cuentas de usuario individuales con AWS Identity and Access Management (IAM). De esta manera, cada usuario recibe únicamente los permisos necesarios para cumplir con sus obligaciones laborales.

Recomendamos encarecidamente a los clientes que nunca coloquen información de identificación confidencial, como los números de cuenta de los clientes, en campos de formato libre, como el campo de nombre. Esto incluye cuando los clientes trabajan con AWS Auto Scaling u otros AWS servicios mediante la AWS Management Console API o AWS los SDK. AWS CLI

Todos los datos que los clientes introduzcan en AWS Auto Scaling u otros servicios podrían recogerse para incluirlos en los registros de diagnóstico. Cuando los clientes proporcionan una URL a un servidor externo, no deben incluir la información sobre las credenciales en la URL para validar su solicitud a ese servidor. AWS también recomienda a los clientes que protejan sus datos de las siguientes maneras:

- Utilice autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Recomendamos TLS 1.2 o una versión posterior
- Configure la API y el registro de actividad de los usuarios con AWS CloudTrail.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados de AWS los servicios.
- Utilice avanzados servicios de seguridad administrados, como Amazon Macie, que lo ayuden a detectar y proteger los datos personales almacenados en Amazon S3.

AWS Backup

AWS Backup ofrece un servicio centralizado, totalmente gestionado y basado en políticas para proteger los datos de los clientes y garantizar el cumplimiento de todos los AWS servicios con fines de continuidad empresarial. Con AWS Backup, los clientes pueden configurar de forma centralizada las políticas de protección de datos (backup) y supervisar la actividad de backup en todos AWS los recursos del cliente, incluidos los volúmenes de Amazon EBS, las bases de datos de Amazon Relational Database Service (Amazon RDS) (incluidos los clústeres de Aurora), las tablas de Amazon DynamoDB, el Amazon Elastic File System (Amazon EFS), los sistemas de archivos Amazon FSx, las instancias y los volúmenes de Amazon EC2. AWS Storage Gateway

AWS Backup cifra los datos de los clientes en tránsito y en reposo. Las copias de seguridad de los servicios con capacidades de instantáneas existentes se cifran mediante la metodología de cifrado

de instantáneas del servicio de origen. Por ejemplo, las instantáneas de EBS se cifran con la clave de cifrado del volumen a partir del cual se creó la instantánea.

Las copias de seguridad de AWS los servicios más recientes que incorporan una funcionalidad de copia de seguridad integrada AWS Backup, como Amazon EFS, se cifran en tránsito y en reposo independientemente de los servicios de origen, lo que proporciona a las copias de seguridad de los clientes un nivel adicional de protección. El cifrado se configura en el nivel de Backup Vault. El almacén predeterminado está cifrado. Cuando los clientes crean una nueva bóveda, deben seleccionar una clave de cifrado.

AWS Batch

AWS Batch permite a los desarrolladores, científicos e ingenieros ejecutar cientos de miles de trabajos de computación por lotes de manera fácil y eficiente AWS. AWS Batch aprovisiona de forma dinámica la cantidad y el tipo óptimos de recursos informáticos (como instancias optimizadas para la CPU o la memoria) en función del volumen y los requisitos de recursos específicos de los trabajos por lotes enviados. AWS Batch planifica, programa y ejecuta cargas de trabajo de computación por lotes en toda la gama de funciones y servicios AWS informáticos.

Al igual que las directrices de Amazon ECS, la PHI no debe incluirse directamente en la definición del trabajo, la cola de trabajos o las etiquetas correspondientes AWS Batch. En cambio, los trabajos programados y ejecutados con ellos AWS Batch pueden funcionar con una PHI cifrada. La información que se devuelva por etapas de un trabajo tampoco AWS Batch debe contener ninguna PHI. Siempre que los trabajos que se estén ejecutando AWS Batch deban transmitir o recibir PHI, esa conexión debe cifrarse mediante HTTPS o SSL/TLS.

AWS Certificate Manager

AWS Certificate Manager es un servicio que permite a los clientes aprovisionar, administrar e implementar fácilmente certificados SSL/TLS públicos y privados para usarlos con los servicios y sus recursos internos conectados. AWS AWS Certificate Manager se utiliza para registrar todas CloudTrail las llamadas a la API.

Los usuarios necesitan acceso programático si quieren interactuar con personas AWS ajenas a. AWS Management Console La forma de conceder el acceso programático depende del tipo de usuario que acceda. AWS

Para conceder acceso programático a los usuarios, seleccione una de las siguientes opciones.

¿Qué usuario necesita acceso programático?	Para	Mediante
Identidad del personal (Usuarios administrados en el Centro de identidades de IAM)	Usa credenciales temporales para firmar las solicitudes programáticas a los AWS CLI AWS SDK o las API. AWS	Siga las instrucciones de la interfaz que desea utilizar: • Para ello AWS CLI, consulte Configuración del uso AWS IAM Identity Center en AWS CLI la Guía del AWS Command Line Interface usuario. • Para obtener AWS información sobre los SDK, las herramientas y AWS las API, consulte la autenticación del IAM Identity Center en la Guía de referencia de AWS los SDK y las herramientas.
IAM	Utilice credenciales temporales para firmar las solicitudes programáticas a los AWS SDK o las AWS CLI API. AWS	Siga las instrucciones de Uso de credenciales temporales con AWS recursos de la Guía del usuario de IAM.
IAM	(No recomendado) Utilice credenciales de larga duración para firmar las solicitudes programáticas a los AWS CLI AWS SDK o las API. AWS	Siga las instrucciones de la interfaz que desea utilizar: • Para ello AWS CLI, consulte Autenticación con credenciales de usuario de IAM en la Guía del usuario.AWS Command Line Interface • Para obtener información AWS sobre los SDK y las herramientas, consulte

¿Qué usuario necesita acceso programático?	Para	Mediante
		Autenticarse con credencia les de larga duración en la Guía de referencia de los AWS SDK y las herramien tas. • Para obtener informaci ón AWS sobre las API, consulte Administrar las claves de acceso para los usuarios de IAM en la Guía del usuario de IAM.

AWS Cloud Map

AWS Cloud Map es un servicio de descubrimiento de recursos en la nube. Con AWS Cloud Map, los clientes pueden definir nombres personalizados para los recursos de la aplicación, como las tareas de Amazon ECS, las instancias de Amazon EC2, los buckets de Amazon S3, las tablas de Amazon DynamoDB, las colas de Amazon SQS o cualquier otro recurso en la nube. Luego, los clientes pueden usar estos nombres personalizados para descubrir la ubicación y los metadatos de los recursos en la nube de sus aplicaciones mediante el SDK de AWS y las consultas de API autenticadas. Si bien AWS Cloud Map es un servicio que cumple con los requisitos de la HIPAA, no se debe almacenar ninguna PHI en los nombres o atributos de los recursos de AWS Cloud Map, ya que no existe soporte para proteger dichos datos. En su lugar, AWS Cloud Map se puede utilizar para descubrir los recursos del dominio del cliente que transmiten o almacenan la PHI.

AWS CloudFormation

AWS CloudFormation permite a los clientes crear y aprovisionar despliegues de infraestructura de AWS de forma predecible y repetida. Ayuda a los clientes a aprovechar los productos de AWS, como Amazon EC2, Amazon Elastic Block Store, Amazon SNS, Elastic Load Balancing y Auto Scaling, para crear aplicaciones altamente fiables, escalables y rentables en la nube sin preocuparse por crear y configurar la infraestructura de AWS subyacente. AWS CloudFormation permite a los clientes

utilizar un archivo de plantilla para crear y eliminar un conjunto de recursos en una sola unidad (una pila).

AWS CloudFormation no almacena, transmite ni procesa por sí mismo la PHI. En su lugar, se utiliza para crear e implementar arquitecturas que utilizan otros servicios de AWS que pueden almacenar, transmitir o procesar la PHI. Con la PHI, solo se deben utilizar los servicios que cumplen con los requisitos de la HIPAA. Consulte las entradas correspondientes a esos servicios en este documento técnico para obtener orientación sobre el uso de la PHI con esos servicios. AWS CloudFormation se utiliza AWS CloudTrail para registrar todas las llamadas a la API.

AWS CloudHSM

AWS CloudHSM es un módulo de seguridad de hardware (HSM) basado en la nube que permite a los clientes generar y utilizar fácilmente sus propias claves de cifrado en la nube de AWS. Con CloudHSM, los clientes pueden gestionar sus propias claves de cifrado mediante HSM validados por FIPS 140-2 de nivel 3. CloudHSM ofrece a los clientes la flexibilidad de integrarse con sus aplicaciones mediante API de estándares abiertos, como PKCS #11, Java Cryptography Extensions (JCE) y bibliotecas Microsoft CryptoNG (CNG).

CloudHSM también cumple con los estándares y permite a los clientes exportar todas sus claves a la mayoría de los demás HSM disponibles en el mercado. Como AWS CloudHSM es un servicio de administración de claves para dispositivos de hardware, no puede almacenar ni transmitir la PHI. Los clientes no deben almacenar la PHI en etiquetas (metadatos). No se requiere ninguna otra orientación especial.

AWS CloudTrail

AWS CloudTrail es un servicio que permite la gobernanza, el cumplimiento, la auditoría operativa y la auditoría de riesgos de las cuentas de AWS. Con ello CloudTrail, los clientes pueden registrar, supervisar de forma continua y conservar la actividad de la cuenta relacionada con las acciones en toda su infraestructura de AWS. CloudTrail proporciona el historial de eventos de la actividad de sus cuentas de AWS, incluidas las acciones realizadas a través de los SDK de AWS AWS Management Console, las herramientas de línea de comandos y otros servicios de AWS. Este historial de eventos simplifica el análisis de seguridad, el seguimiento de los cambios en los recursos y la solución de problemas.

AWS CloudTrail está habilitado para su uso con todas las cuentas de AWS y se puede usar para el registro de auditorías, según lo exige la BAA de AWS. Las rutas específicas se deben crear mediante

la CloudTrail consola o la interfaz de línea de comandos de AWS. CloudTrail cifra todo el tráfico en tránsito y en reposo cuando se crea una ruta cifrada. Se debe crear un registro cifrado cuando exista la posibilidad de registrar la PHI.

De forma predeterminada, un Trail cifrado almacena las entradas en Amazon S3 mediante el cifrado del lado del servidor con claves administradas por Amazon S3 (SSE-S3). Si se desea una administración adicional de las claves, también se puede configurar con claves AWS KMS administradas (SSE-KMS). Como CloudTrail es el destino final de las entradas de registro de AWS y, por lo tanto, un componente fundamental de cualquier arquitectura que gestione la PHI, la validación de la integridad de los archivos de CloudTrail registro debe estar habilitada y los archivos de CloudTrail resumen asociados deben revisarse periódicamente. Una vez habilitada, se puede establecer una afirmación positiva de que los archivos de registro no se han modificado ni alterado.

AWS CodeBuild

AWS CodeBuild es un servicio de compilación en la nube totalmente gestionado. AWS CodeBuild compila el código fuente, ejecuta pruebas unitarias y produce artefactos que están listos para su despliegue. AWS CodeBuild utiliza una AWS KMS clave para cifrar los artefactos de salida de la compilación. Se debe crear y configurar una clave KMS antes de crear artefactos que contengan PHI, secretos/contraseñas, certificados, etc. AWS CloudTrail para registrar todas las AWS CodeBuild llamadas a la API.

AWS CodeDeploy

AWS CodeDeploy es un servicio de implementación totalmente gestionado que automatiza las implementaciones de software en una variedad de servicios informáticos AWS Fargate AWS Lambda, incluidos Amazon EC2 y servidores locales. Los clientes suelen AWS CodeDeploy lanzar rápidamente nuevas funciones de la carga de trabajo contenerizada y gestionar la complejidad que supone actualizar las aplicaciones.

AWS CodeDeploy admite el cifrado del lado del servidor (SSE-S3) para los artefactos de despliegue y el cifrado TLS para los datos en tránsito entre el servicio y el agente. Los clientes pueden usar Amazon CloudWatch Events para realizar un seguimiento de las implementaciones y capturar AWS CloudTrail las llamadas a AWS CodeDeploy las API.

AWS CodeCommit

AWS CodeCommit es un servicio de control de código fuente gestionado, seguro y altamente escalable que aloja repositorios Git privados. AWS CodeCommit elimina la necesidad de que los clientes administren su propio sistema de control de código fuente o se preocupen por escalar su infraestructura.

AWS CodeCommit cifra todo el tráfico y la información almacenada mientras está en tránsito y en reposo. De forma predeterminada, cuando se crea un repositorio en él AWS CodeCommit, se crea una clave gestionada por AWS con AWS KMS ese repositorio, que solo la utiliza para cifrar todos los datos almacenados en reposo. AWS CodeCommit se utiliza AWS CloudTrail para registrar todas las llamadas a la API.

AWS CodePipeline

AWS CodePipeline es un servicio de entrega continua totalmente gestionado que ayuda a los clientes a automatizar los procesos de publicación de los clientes para obtener actualizaciones rápidas y fiables de las aplicaciones y la infraestructura. Los clientes permiten AWS CodePipeline a los investigadores procesar automáticamente los datos de los ensayos clínicos; los resultados de laboratorio y los datos genómicos son algunos ejemplos de los flujos de trabajo utilizados por los clientes.

AWS CodePipeline admite el cifrado del lado del servidor (SSE-S3 y SSE-KMS) para los artefactos de código y el cifrado TLS para los datos en tránsito entre el servicio y el agente. Los clientes pueden usar Amazon CloudWatch Events para realizar un seguimiento de los cambios en la canalización y AWS CloudTrail capturar las llamadas a las API AWS CodePipeline.

AWS Config

AWS Config proporciona una vista detallada de los recursos asociados a la cuenta de AWS de un cliente, incluida la forma en que están configurados, cómo se relacionan entre sí y cómo han cambiado las configuraciones y sus relaciones a lo largo del tiempo.

AWS Config no se puede utilizar por sí solo para almacenar o transmitir la PHI.

En su lugar, se puede aprovechar para supervisar y evaluar las arquitecturas creadas con otros servicios de AWS, incluidas las arquitecturas que gestionan la PHI, a fin de determinar si siguen

cumpliendo con el objetivo de diseño previsto. Las arquitecturas que gestionan la PHI solo deben crearse con servicios que cumplan con los requisitos de la HIPAA. AWS Config Se utiliza AWS CloudTrail para registrar todos los resultados.

AWS Data Exchange

AWS Data Exchange facilita la búsqueda, la suscripción y el uso de datos de terceros en la nube. Una vez suscritos a un producto de datos, los clientes pueden usar la API de AWS Data Exchange para cargar datos directamente en Amazon S3 y analizarlos con una amplia variedad de servicios de análisis y aprendizaje automático de AWS. Para los proveedores de datos, AWS Data Exchange facilita el acceso a los millones de clientes de AWS que migran a la nube al eliminar la necesidad de crear y mantener una infraestructura para el almacenamiento, la entrega, la facturación y la autorización de los datos.

AWS Data Exchange siempre cifra todos los productos de datos almacenados en el servicio en reposo sin necesidad de ninguna configuración adicional. Este cifrado se realiza automáticamente mediante una clave KMS administrada por el servicio. AWS Data Exchange utiliza Transport Layer Security (TLS) y el cifrado del lado del cliente para el cifrado en tránsito. La comunicación con AWS Data Exchange siempre se realiza a través de HTTPS, por lo que los datos del cliente siempre están cifrados en tránsito. Este cifrado se configura de forma predeterminada cuando los clientes utilizan AWS Data Exchange. Para obtener más información, consulte Protección de datos en AWS Data Exchange.

AWS Data Exchange está integrado con AWS CloudTrail. AWS CloudTrail captura todas las llamadas a las API de AWS Data Exchange como eventos, incluidas las llamadas desde la consola de AWS Data Exchange y las llamadas en código a las operaciones de la API de AWS Data Exchange. Algunas de las acciones que los clientes pueden realizar son acciones que solo pueden realizar desde la consola. No hay una API correspondiente en el AWS SDK ni en la AWS CLI. Se trata de acciones que dependen de AWS Marketplace la funcionalidad, como publicar un producto o suscribirse a él. AWS Data Exchange proporciona CloudTrail registros para un subconjunto de estas acciones exclusivas de la consola. Para obtener más información, consulte Registrar llamadas a la API de AWS Data Exchange con AWS CloudTrail.

Tenga en cuenta que todos los listados que utilicen AWS Data Exchange deben cumplir las directrices de publicación de AWS Data Exchange y las preguntas frecuentes sobre AWS Data Exchange para AWS Marketplace proveedores, que restringen determinadas categorías de datos. Para obtener más información, consulte las preguntas frecuentes sobre AWS Data Exchange.

AWS Database Migration Service

AWS Database Migration Service (AWS DMS) ayuda a los clientes a migrar las bases de datos a AWS de forma fácil y segura. Los clientes pueden migrar sus datos hacia y desde las bases de datos comerciales y de código abierto más utilizadas, como Oracle, MySQL y PostgreSQL. Este servicio admite migraciones homogéneas como de Oracle a Oracle, así como migraciones heterogéneas entre diferentes plataformas de bases de datos, como de Oracle a PostgreSQL o de MySQL a Oracle.

Las bases de datos que se ejecutan en las instalaciones y que se migran a la nube con AWS DMS pueden contener datos de PHI. AWS DMS cifra los datos mientras están en tránsito y cuando los datos se están preparando para la migración final a la base de datos de destino en AWS. AWS DMS cifra el almacenamiento utilizado por una instancia de replicación y la información de conexión del punto final. Para cifrar el almacenamiento que utiliza una instancia de replicación, AWS DMS utiliza una AWS KMS clave que es exclusiva de la cuenta de AWS. Consulte la guía de la base de datos de destino adecuada para asegurarse de que los datos permanezcan cifrados una vez finalizada la migración. AWS DMS registra todas las llamadas CloudTrail a la API.

AWS DataSync

AWS DataSync es un servicio de transferencia en línea que simplifica, automatiza y acelera la transferencia de datos entre el almacenamiento local y AWS. Los clientes pueden usar AWS DataSync para conectar sus fuentes de datos a Amazon S3 o Amazon EFS. Los clientes deben asegurarse de que Amazon S3 y Amazon EFS estén configurados de forma coherente con las directrices. De forma predeterminada, los datos de los clientes se cifran en tránsito mediante TLS 1.2. Para obtener más información sobre el cifrado y AWS DataSync, consulte DataSyncCaracterísticas de AWS. Los clientes pueden monitorizar DataSync la actividad mediante AWS CloudTrail. Para obtener más información sobre cómo iniciar sesión con CloudTrail, consulte Registrar llamadas a la DataSync API de AWS con AWS CloudTrail.

AWS Directory Service

AWS Directory Service para Microsoft AD

AWS Directory Service para Microsoft Active Directory (Enterprise Edition), también conocido como AWS Microsoft AD, permite que las cargas de trabajo con reconocimiento de directorios y los recursos de AWS utilicen Active Directory administrado en la nube de AWS. AWS Microsoft AD

almacena el contenido del directorio (incluido el contenido que contiene PHI) en volúmenes cifrados de Amazon Elastic Block Store mediante claves de cifrado que administra AWS. Para obtener más información, consulte Cifrado de Amazon EBS.

Los datos en tránsito hacia y desde los clientes de Active Directory se cifran cuando viajan a través del Protocolo ligero de acceso a directorios (LDAP) a través de la red Amazon Virtual Private Cloud (VPC) del cliente. Si un cliente de Active Directory reside en una red local, el tráfico viaja a la VPC del cliente mediante un enlace de red privada virtual o AWS Direct Connect un enlace.

Amazon Cloud Directory

Amazon Cloud Directory permite a los clientes crear directorios flexibles nativos de la nube para organizar jerarquías de datos en múltiples dimensiones. Los clientes también pueden crear directorios para una variedad de casos de uso, como organigramas, catálogos de cursos y registros de dispositivos. Por ejemplo, los clientes pueden crear un organigrama en el que se pueda navegar a través de jerarquías independientes para determinar la estructura jerárquica, la ubicación y el centro de costes. Amazon Cloud Directory cifra automáticamente los datos en reposo y en tránsito mediante claves de cifrado de 256 bits gestionadas por (). AWS Key Management Service AWS KMS

AWS Elastic Beanstalk

Con AWS Elastic Beanstalk, los clientes pueden implementar y administrar aplicaciones rápidamente en la nube de AWS sin tener que conocer la infraestructura en la que se ejecutan esas aplicaciones. Los clientes solo tienen que cargar el código y gestionar AWS Elastic Beanstalk automáticamente la implementación, desde el aprovisionamiento de la capacidad, el equilibrio de carga y el escalado automático hasta la supervisión del estado de las aplicaciones. Al mismo tiempo, los clientes mantienen el control total sobre los recursos de AWS que impulsan su aplicación y pueden acceder a los recursos subyacentes en cualquier momento.

AWS Elastic Beanstalk no almacena, transmite ni procesa por sí mismo la PHI. En su lugar, los clientes pueden utilizarla para crear e implementar arquitecturas con otros servicios de AWS que puedan almacenar, transmitir o procesar la PHI. Al elegir los servicios que van a implementar, los clientes deben asegurarse de utilizar únicamente los servicios aptos AWS Elastic Beanstalk para la HIPAA con la PHI. Consulte las entradas correspondientes a esos servicios en este documento técnico para obtener orientación sobre el uso de la PHI con esos servicios.

Los clientes no deben incluir la PHI en ningún campo de formato libre AWS Elastic Beanstalk , como el campo Nombre. AWS Elastic Beanstalk se utiliza AWS CloudTrail para registrar todas las llamadas a la API.

Recuperación ante desastres de AWS Elastic

AWS Elastic Disaster Recovery (AWS DRS) minimiza el tiempo de inactividad y la pérdida de datos con una recuperación rápida y fiable de aplicaciones locales y basadas en la nube mediante un almacenamiento asequible, un cálculo y point-in-time una recuperación mínimos.

Los clientes pueden configurar AWS Elastic Disaster Recovery en sus servidores de origen para iniciar la replicación segura de los datos. Sus datos se replican en una subred de área de ensayo de su cuenta de AWS, en la región de AWS que seleccionen. El diseño del área de almacenamiento reduce los costos al utilizar un almacenamiento asequible y recursos de cómputo mínimos para mantener una replicación continua. Los datos de los clientes replicados por AWS Elastic Disaster Recovery se cifran en tránsito mediante TLS 1.2 y se transfieren directamente desde sus servidores de origen a su VPC. Los clientes pueden aprovechar la conectividad privada, como AWS Direct Connect o VPN, para configurar la ruta de replicación. Los datos de los clientes también se pueden cifrar en reposo en AWS mediante el cifrado de Amazon EBS.

Los clientes pueden realizar pruebas no disruptivas para confirmar que la implementación se ha completado. Durante el funcionamiento normal, manténgase preparado supervisando la replicación y realizando periódicamente simulacros de recuperación y conmutación por error no disruptivos. Si los clientes necesitan recuperar aplicaciones, pueden lanzar instancias de recuperación en AWS en cuestión de minutos, utilizando el estado máximo up-to-date del servidor o un momento anterior. Una vez que las aplicaciones de los clientes se ejecutan en AWS, pueden optar por mantenerlas allí o iniciar la replicación de datos en su sitio principal cuando se resuelva el problema. Los clientes pueden volver a su sitio principal por defecto cuando estén preparados.

AWS Fargate

AWS Fargate es una tecnología que permite al cliente ejecutar contenedores sin tener que administrar servidores o clústeres. Con AWS Fargate ello, los clientes ya no tienen que aprovisionar, configurar ni escalar clústeres de máquinas virtuales para ejecutar contenedores. Esto elimina la necesidad de elegir los tipos de servidores, decidir cuándo escalar los clústeres u optimizar el empaquetado de los clústeres. AWS Fargate elimina la necesidad de que los clientes interactúen con servidores o clústeres o piensen en ellos. Con Fargate, los clientes se centran en diseñar y crear sus aplicaciones en lugar de gestionar la infraestructura que las ejecuta.

Fargate no requiere ninguna configuración adicional para funcionar con cargas de trabajo que procesan la PHI. Los clientes pueden ejecutar cargas de trabajo de contenedores en Fargate mediante servicios de organización de contenedores como Amazon ECS. Fargate solo administra

la infraestructura subyacente y no opera con los datos ni sobre ellos dentro de la carga de trabajo que se está organizando. De acuerdo con los requisitos de la HIPAA, la PHI debe seguir cifrándose cuando esté en tránsito o en reposo cuando se acceda a ella desde contenedores lanzados con Fargate. Hay varios mecanismos de cifrado en reposo disponibles con cada opción de almacenamiento de AWS descrita en este paper. Para obtener información adicional sobre la seguridad y la configuración de la HIPAA, consulte el documento técnico Architecting for HIPAA Security and Compliance on Amazon EKS.

AWS Firewall Manager

AWS Firewall Manager es un servicio de administración de seguridad que permite a los clientes configurar y administrar de forma centralizada las reglas de firewall en todas las cuentas y aplicaciones de los clientes en. AWS Organizations A medida que se crean nuevas aplicaciones, Firewall Manager facilita el cumplimiento de las nuevas aplicaciones y recursos mediante la aplicación de un conjunto común de reglas de seguridad. Ahora los clientes disponen de un único servicio para crear reglas de firewall, crear políticas de seguridad y aplicarlas de manera coherente y jerárquica en toda su infraestructura, desde una cuenta de administrador central.

AWS Firewall Manager es un servicio de organización que no procesa, almacena ni transmite directamente los datos de los usuarios. El servicio no cifra el contenido del cliente, pero los servicios subyacentes que lo AWS Firewall Manager utiliza, como DynamoDB, cifran los datos de los usuarios.

AWS Global Accelerator

AWS Global Accelerator es un servicio de equilibrio de carga global que mejora la disponibilidad y la latencia de las aplicaciones multirregionales. Para garantizar que la PHI permanezca cifrada en tránsito y en reposo durante su uso AWS Global Accelerator, las arquitecturas en las que Global Accelerator equilibra la carga deben utilizar un protocolo cifrado, como HTTPS o SSL/TLS. Consulte la guía de Amazon EC2, Elastic Load Balancing y otros servicios de AWS para comprender mejor las opciones de cifrado disponibles para los recursos de backend. AWS Global Accelerator se utiliza AWS CloudTrail para registrar todas las llamadas a la API.

AWS Glue

AWS Glue es un servicio ETL (extracción, transformación y carga) totalmente gestionado que permite a los clientes clasificar sus datos, limpiarlos, enriquecerlos y moverlos de forma fiable entre varios almacenes de datos de forma sencilla y rentable. Para garantizar el cifrado de los datos que

contienen PHI mientras están en tránsito, AWS Glue debe configurarse para utilizar conexiones JDBC a los almacenes de datos con SSL/TLS. Además, para mantener el cifrado mientras están en tránsito, la configuración del cifrado del lado del servidor (SSE-S3) debe pasarse como parámetro a los trabajos de ETL que se ejecuten con ellos. AWS Glue Todos los datos almacenados en reposo en el catálogo de datos AWS Glue se cifran mediante claves administradas AWS KMS cuando el cifrado está activado al crear un objeto del catálogo de datos. AWS Glue se utiliza CloudTrail para registrar todas las llamadas a la API.

Pegamento AWS DataBrew

AWS Glue DataBrew es un servicio de preparación visual de datos totalmente gestionado que facilita a los analistas y científicos de datos la limpieza y normalización de los datos para prepararlos para el análisis y el aprendizaje automático. Para garantizar el cifrado de los datos que contienen PHI mientras están en tránsito, DataBrew debe configurarse para utilizar conexiones JDBC a los almacenes de datos con SSL/TLS. Al conectarse a fuentes de datos JDBC, DataBrew utiliza la configuración de su conexión AWS Glue, incluida la opción «Requerir conexión SSL». Además, para mantener el cifrado mientras está en reposo en los depósitos de S3, la configuración del cifrado del lado del servidor (SSE-S3 o SSE-KMS) debe transferirse como parámetro a jobs. DataBrew

AWS IoT Núcleo y AWS IoT Device Management

AWS IoT Centralice y AWS IoT Device Management proporcione una comunicación bidireccional segura entre los dispositivos conectados a Internet, como sensores, actuadores, microcontroladores integrados o dispositivos inteligentes, y la nube de AWS. AWS IoT Core y ahora AWS IoT Device Management puede adaptarse a dispositivos que transmiten datos que contienen PHI. Toda la comunicación con AWS IoT Core AWS IoT Device Management está cifrada mediante TLS. AWS IoT Núcleo y AWS IoT Device Management utilícelo AWS CloudTrail para registrar todas las llamadas a la API.

AWS IoT Greengrass

AWS IoT Greengrass permite a los clientes ejecutar funciones locales de procesamiento, mensajería, almacenamiento en caché de datos, sincronización e inferencia de aprendizaje automático para los dispositivos conectados de forma segura. AWS IoT Greengrass utiliza certificados X.509, suscripciones gestionadas, AWS IoT políticas y políticas y funciones de IAM para garantizar la seguridad de las aplicaciones Greengrass del cliente. AWS IoT Greengrass utiliza el modelo

de seguridad del AWS IoT transporte para cifrar la comunicación con la nube mediante TLS. Además, AWS IoT Greengrass los datos se cifran cuando están en reposo (en la nube). Para obtener más información sobre la seguridad de Greengrass, consulte Descripción general de la AWS IoT Greengrass seguridad.

Los clientes pueden registrar las acciones AWS IoT Greengrass de la API mediante AWS CloudTrail. Para obtener más información, consulte Registrar llamadas a la AWS IoT Greengrass API con AWS CloudTrail.

AWS Lambda

AWS Lambda permite a los clientes ejecutar código sin aprovisionar ni administrar los servidores por sí mismos. AWS Lambda utiliza una flota informática de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en varias zonas de disponibilidad de una región, lo que proporciona la alta disponibilidad, seguridad, rendimiento y escalabilidad de la infraestructura de AWS.

Para garantizar que la PHI permanezca cifrada durante su uso AWS Lambda, las conexiones a recursos externos deben utilizar un protocolo cifrado, como HTTPS o SSL/TLS. Por ejemplo, cuando se accede a S3 desde un procedimiento Lambda, debe abordarse con https://bucket.s3-aws-region.amazonaws.com.

Si alguna PHI permanece inactiva o inactiva dentro de un procedimiento en ejecución, debe cifrarse en el lado del cliente o en el servidor con claves obtenidas de o. AWS KMS AWS CloudHSM Siga las instrucciones relacionadas con Amazon API Gateway cuando active AWS Lambda funciones a través del servicio. Cuando se utilizan eventos de otros servicios de AWS para activar AWS Lambda funciones, los datos del evento no deben contener (por sí solos) la PHI. Por ejemplo, cuando se desencadena un procedimiento Lambda a partir de un evento de S3, como la llegada de un objeto a S3, el nombre del objeto que se transmite a Lambda no debe tener ningún PHI, aunque el propio objeto puede contener dichos datos.

AWS Managed Services

AWS Managed Services proporciona una administración continua de las infraestructuras de AWS. Al implementar las mejores prácticas para mantener la infraestructura de un cliente, AWS Managed Services ayuda a reducir sus gastos operativos y sus riesgos. AWS Managed Services automatiza las actividades habituales, como las solicitudes de cambios, la supervisión, la administración de parches, la seguridad y los servicios de respaldo, y proporciona servicios durante todo el ciclo de vida para aprovisionar, ejecutar y dar soporte a las infraestructuras.

Los clientes pueden utilizarlas AWS Managed Services para gestionar las cargas de trabajo de AWS que funcionan con datos que contienen PHI. El uso de AWS Managed Services no altera los servicios de AWS aptos para su uso con la PHI. Las herramientas y la automatización proporcionadas por AWS Managed Services no se pueden utilizar para almacenar o transmitir la PHI.

AWS OpsWorks para Chef Automate

AWS OpsWorks for Chef Automate es un servicio de gestión de la configuración totalmente gestionado que aloja Chef Automate, un conjunto de herramientas de automatización de Chef para la gestión de infraestructuras y aplicaciones. El servicio en sí no contiene, transmite ni gestiona ninguna PHI ni información confidencial, pero los clientes deben asegurarse de que todos los recursos configurados OpsWorks por Chef Automate estén configurados de conformidad con las directrices. Las llamadas a la API se capturan con AWS CloudTrail. Para obtener más información, consulta Cómo registrar las llamadas a la API de AWS OpsWorks Stacks con AWS CloudTrail.

AWS OpsWorks para Puppet Enterprise

AWS OpsWorks for Puppet Enterprise es un servicio de gestión de la configuración totalmente gestionado que aloja Puppet Enterprise, un conjunto de herramientas de automatización de Puppet para la gestión de infraestructuras y aplicaciones. El servicio en sí no contiene, transmite ni gestiona ninguna PHI ni información confidencial, pero los clientes deben asegurarse de que todos los recursos configurados OpsWorks por Puppet Enterprise estén configurados de conformidad con las directrices. Las llamadas a la API se capturan con AWS CloudTrail. Para obtener más información, consulta Cómo registrar las llamadas a la API de AWS OpsWorks Stacks con AWS CloudTrail.

AWS OpsWorks Apile

AWS OpsWorks Stacks proporciona una forma sencilla y flexible de crear y gestionar pilas y aplicaciones. Los clientes pueden usar AWS OpsWorks Stacks para implementar y monitorear las aplicaciones en sus stacks.

AWS OpsWorks Stacks cifra todo el tráfico mientras está en tránsito. Sin embargo, las bolsas de datos cifrados (un mecanismo de almacenamiento de datos de Chef) no están disponibles y cualquier activo que deba almacenarse de forma segura, como la PHI, los secretos/contraseñas, los certificados, etc., debe almacenarse en un depósito cifrado en Amazon S3. AWS OpsWorks Stack se utiliza AWS CloudTrail para registrar todas las llamadas a la API.

AWS Organizations

AWS Organizations ayuda a los clientes a gestionar y gobernar su entorno de forma centralizada a medida que crecen y escalan sus recursos de AWS. Con AWS Organizationsél, pueden crear nuevas cuentas de AWS y asignar recursos mediante programación, agrupar cuentas para organizar sus flujos de trabajo, aplicar políticas a las cuentas o grupos para la gobernanza y simplificar la facturación mediante el uso de un único método de pago para todas sus cuentas.

Además, AWS Organizations está integrado con otros servicios de AWS para que los clientes puedan definir configuraciones centrales, mecanismos de seguridad, requisitos de auditoría y uso compartido de recursos entre las cuentas de su organización. AWS Organizations está disponible para todos los clientes de AWS sin coste adicional.

AWS Organizations es un servicio de organización que no procesa, almacena ni transmite directamente los datos de los usuarios. El servicio no cifra el contenido de los clientes, pero los servicios subyacentes que se lanzan en AWS Organizationsél sí cifran los datos de los usuarios. AWS Organizations está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un servicio de AWS en AWS Organizations.

AWS RoboMaker

AWS RoboMaker permite a los clientes ejecutar código en la nube para el desarrollo de aplicaciones y proporciona un servicio de simulación robótica para acelerar las pruebas de aplicaciones. AWS RoboMaker también ofrece un servicio de administración de flotas robóticas para la implementación, actualización y administración remotas de aplicaciones.

El tráfico de red que contiene PHI debe cifrar los datos en tránsito. Todas las comunicaciones de administración con el servidor de simulación se realizan a través de TLS y los clientes deben utilizar mecanismos de cifrado de transporte estándar abierto para las conexiones a otros servicios de AWS. AWS RoboMaker también se integra CloudTrail para registrar todas las llamadas a la API en un bucket de Amazon S3 específico.

RoboMaker Los registros de AWS no contienen PHI y los volúmenes de EBS que utiliza el servidor de simulación están cifrados. Al transferir datos que puedan contener PHI a otros servicios, como Amazon S3, los clientes deben seguir las instrucciones del servicio receptor para almacenar la PHI. En el caso de los despliegues en robots, los clientes deben asegurarse de que el cifrado de los datos en tránsito y en reposo sea coherente con su interpretación de la Guía.

Métricas del SDK de AWS

Los clientes empresariales pueden usar el CloudWatch agente de AWS con AWS SDK Metrics for Enterprise Support (SDK Metrics) para recopilar métricas de los SDK de AWS en sus hosts y clientes. Estas métricas se comparten con AWS Enterprise Support. SDK Metrics puede ayudar a los clientes a recopilar métricas y datos de diagnóstico relevantes sobre las conexiones de sus aplicaciones a los servicios de AWS sin añadir instrumentación personalizada a su código, y reduce el trabajo manual necesario para compartir registros y datos. AWS Support

Tenga en cuenta que SDK Metrics solo está disponible para los clientes de AWS con una suscripción a Enterprise Support. Los clientes pueden usar SDK Metrics con cualquier aplicación que llame directamente a los servicios de AWS y que se haya creado con un SDK de AWS que sea una de las versiones que se indican en la documentación de AWS Metrics.

SDK Metrics supervisa las llamadas que realiza el SDK de AWS y usa el CloudWatch agente que se ejecuta en el mismo entorno que una aplicación cliente.

El CloudWatch agente cifra los datos en tránsito desde la máquina local hasta su entrega en el grupo de registros de destino. El grupo de registros se puede configurar para que se cifre siguiendo las instrucciones que se indican en Cómo cifrar los datos de registro en CloudWatch los registros mediante. AWS KMS

AWS Secrets Manager

AWS Secrets Manager es un servicio de AWS que facilita a los clientes la administración de los «secretos». Los secretos pueden ser credenciales de bases de datos, contraseñas, claves de API de terceros e incluso texto arbitrario. AWS Secrets Manager puede usarse para almacenar la PHI si dicha información está contenida en «secretos». Todos los secretos almacenados por AWS Secrets Manager se cifran en reposo mediante el Sistema de administración de claves (KMS) de AWS. Los usuarios pueden seleccionar la AWS KMS clave utilizada al crear un secreto nuevo. Si no se selecciona ninguna clave, se utilizará la clave predeterminada de la cuenta. AWS Secrets Manager se utiliza AWS CloudTrail para registrar todas las llamadas a la API.

AWS Security Hub

AWS Security Hub recopila y consolida los hallazgos de los servicios de seguridad de AWS habilitados en el entorno de un cliente, como los hallazgos de detección de intrusiones de Amazon

GuardDuty, los escaneos de vulnerabilidades de Amazon Inspector, los hallazgos de las políticas de bucket de Amazon S3 de Amazon Macie, los recursos de acceso público y multicuenta de IAM Access Analyzer y los recursos que no están cubiertos por WAF. AWS Firewall Manager AWS Security Hub también consolida los hallazgos de las soluciones de seguridad integradas de la Red de socios de AWS (APN).

AWS Security Hub se integra con Amazon CloudWatch Events, lo que permite a los clientes crear flujos de trabajo personalizados de respuesta y corrección. Los clientes pueden enviar fácilmente sus conclusiones a los SIEM, a las herramientas de chat, a los sistemas de emisión de tickets, a las herramientas de automatización y respuesta de la organización de la seguridad (SOAR) y a las plataformas de gestión de llamadas. Las acciones de respuesta y corrección se pueden automatizar por completo o se pueden activar manualmente en la consola. Los clientes también pueden usar los documentos y AWS Lambda las funciones de AWS Systems Manager automatización para crear flujos de trabajo de remediación automatizados desde los que puedan iniciarse. AWS Step Functions AWS Security Hub

Para garantizar la protección de los datos, AWS Security Hub cifra los datos en reposo y los datos en tránsito entre los servicios componentes. Los auditores externos evalúan la seguridad y la conformidad AWS Security Hub como parte de varios programas de conformidad de AWS. AWS Security Hub forma parte de los programas de conformidad con las normas SOC, ISO, PCI e HIPAA de AWS.

AWS Server Migration Service

AWS Server Migration Service (AWS SMS) automatiza la migración de máquinas virtuales VMware vSphere o Microsoft Hyper-V/SCVMM locales a la nube de AWS. AWS SMS replica de forma incremental las máquinas virtuales del servidor como Amazon Machine Images (AMI) alojadas en la nube y listas para su implementación en Amazon EC2.

Los servidores que se ejecutan en las instalaciones y que se migran a la nube con (AWS SMS) pueden contener datos de PHI. AWS SMS cifra los datos mientras están en tránsito y cuando las imágenes de la máquina virtual del servidor se están preparando para su ubicación final en EC2. Consulte la guía de EC2 y la configuración de volúmenes de almacenamiento cifrados al migrar una máquina virtual de servidor que contenga PHI con AWS SMS. AWS SMS se utiliza CloudTrail para registrar todas las llamadas a la API.

AWS Serverless Application Repository

El AWS Serverless Application Repository (SAR) es un repositorio administrado para aplicaciones sin servidor. Permite a los equipos, las organizaciones y los desarrolladores individuales almacenar y compartir aplicaciones reutilizables, y ensamblar e implementar fácilmente arquitecturas sin servidor de formas nuevas y poderosas. Las aplicaciones son AWS CloudFormation plantillas que contienen definiciones de la infraestructura de la aplicación y archivos binarios compilados del código de las funciones de la aplicación AWS Lambda .

Si bien es posible que las aplicaciones incluidas en el sistema AWS Serverless Application Repository procesen la PHI, solo lo harán después de haberla desplegado en la cuenta del cliente y no como parte del propio SAR. AWS Serverless Application Repository Cifra los archivos que cargan los clientes, incluidos los paquetes de implementación y los archivos en capas. En el caso de los datos en tránsito, AWS Serverless Application Repository utiliza TLS para cifrar los datos entre el servicio y el agente. AWS Serverless Application Repository está integrado con AWS CloudTrail, que es un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un servicio de AWS en el AWS Serverless Application Repository.

Service Catalog

Service Catalog permite a los administradores de TI crear, administrar y distribuir carteras de productos aprobados a los usuarios finales, quienes pueden acceder a los productos que necesitan en un portal personalizado. Service Catalog se usa para catalogar, compartir e implementar soluciones de autoservicio en AWS y no se puede usar para almacenar, transmitir ni procesar la PHI. La PHI no debe incluirse en ningún metadato de los elementos del Service Catalog ni en la descripción de ningún elemento. Service Catalog se utiliza AWS CloudTrail para registrar todas las llamadas a la API.

AWS Shield

AWS Shield es un servicio de protección gestionado contra la denegación de servicio distribuido (DDoS) que protege las aplicaciones web que se ejecutan en AWS. AWS Shield proporciona una detección permanente y mitigaciones automáticas integradas que minimizan el tiempo de inactividad y la latencia de las aplicaciones, por lo que no es necesario recurrir AWS Support a ellos para beneficiarse de la protección contra DDoS.

AWS Shield no se puede utilizar para almacenar o transmitir la PHI, sino que se puede utilizar para proteger las aplicaciones web que sí funcionan con la PHI. Por lo tanto, no se necesita ninguna configuración especial cuando se activa AWS Shield.

Todos los clientes de AWS se benefician de las protecciones automáticas de AWS Shield Standard, sin coste adicional. AWS Shield Standard se defiende contra los ataques DDoS más comunes y frecuentes en la capa de red y transporte que tienen como objetivo su sitio web o sus aplicaciones. Para obtener niveles más altos de protección contra los ataques dirigidos a sus aplicaciones web que se ejecutan en los recursos de Elastic Load Balancing (ELB) CloudFront, Amazon y Amazon Route 53, los clientes pueden suscribirse a AWS Shield Advanced.

AWS Snowball

Con AWS Snowball (Snowball), los clientes pueden transferir cientos de terabytes o petabytes de datos entre sus centros de datos locales y Amazon Simple Storage Service (Amazon S3). La PHI almacenada AWS Snowball debe cifrarse en reposo de acuerdo con las directrices. Al crear un trabajo de importación, los clientes deben especificar el ARN de la AWS KMS clave que se utilizará para proteger los datos de Snowball. Además, durante la creación del trabajo de importación, los clientes deben elegir un depósito S3 de destino que cumpla con los estándares de cifrado establecidos en la Guía.

Si bien Snowball no admite actualmente el cifrado del lado del servidor con claves AWS KMS administradas (SSE-KMS) ni el cifrado del lado del servidor con claves proporcionadas por el cliente (SSE-C), Snowball sí admite el cifrado del lado del servidor con claves de cifrado administradas por Amazon S3 (SSE-S3). Para obtener más información, consulte Protección de datos con el cifrado del lado del servidor con claves de cifrado administradas por Amazon S3 (SSE-S3).

Como alternativa, los clientes pueden utilizar la metodología de cifrado que prefieran para cifrar la PHI antes de almacenar los datos. AWS Snowball

En la actualidad, los clientes pueden utilizar el AWS Snowball dispositivo estándar como parte de nuestro BAA.

AWS Snowball Edge

AWS Snowball Edge se conecta a las aplicaciones y la infraestructura existentes de los clientes mediante interfaces de almacenamiento estándar, lo que agiliza el proceso de transferencia de datos y minimiza la configuración y la integración. Snowball Edge puede agruparse para formar un nivel

de almacenamiento local y procesar los datos de los clientes in situ, lo que ayuda a los clientes a garantizar que sus aplicaciones sigan ejecutándose incluso cuando no puedan acceder a la nube.

Para garantizar que la PHI permanezca cifrada mientras utilizan Snowball Edge, los clientes deben asegurarse de utilizar un protocolo de conexión cifrada, como HTTPS o SSL/TLS, cuando utilicen AWS Lambda procedimientos con tecnología AWS IoT Greengrass para transmitir la PHI hacia/desde recursos externos a Snowball Edge. Además, la PHI debe cifrarse mientras se almacena en los volúmenes locales de Snowball Edge, ya sea mediante acceso local o mediante NFS. El cifrado se aplica automáticamente a los datos colocados en Snowball Edge mediante la consola de administración y la API de Snowball para el transporte masivo a S3. Para obtener más información sobre el transporte de datos a S3, consulte la guía relacionada para. the section called “AWS Snowball”

AWS Step Functions

AWS Step Functions facilita la coordinación de los componentes de las aplicaciones distribuidas y los microservicios mediante flujos de trabajo visuales. AWS Step Functions no puede almacenar, transmitir ni procesar la PHI. La PHI no debe incluirse en los metadatos AWS Step Functions ni dentro de ninguna tarea o definición de máquina estatal. AWS Step Functions AWS CloudTrail se utiliza para registrar todas las llamadas a la API.

AWS Storage Gateway

AWS Storage Gateway es un servicio de almacenamiento híbrido que permite a las aplicaciones locales de los clientes utilizar sin problemas el almacenamiento en la nube de AWS. La puerta de enlace utiliza protocolos de almacenamiento estándar abiertos para conectar las aplicaciones y los flujos de trabajo de almacenamiento existentes a los servicios de almacenamiento en la nube de AWS para reducir al mínimo la interrupción del proceso.

Gateway de archivos

La puerta de enlace de archivos es un tipo AWS Storage Gateway que admite una interfaz de archivos en Amazon S3 y que se suma al volumen actual basado en bloques y al almacenamiento VTL. La puerta de enlace de archivos utiliza HTTPS para comunicarse con S3 y almacena todos los objetos cifrados mientras se está en S3 mediante el SSE-S3, de forma predeterminada, o mediante el cifrado del lado del cliente con las claves almacenadas. AWS KMS Los metadatos de los archivos, como los nombres de los archivos, permanecen sin cifrar y no deben contener ninguna PHI.

Volume Gateway

Volume Gateway proporciona volúmenes de almacenamiento respaldados en la nube que los clientes pueden montar como dispositivos de interfaz de sistemas de ordenadores pequeños (iSCSI) de Internet desde servidores de aplicaciones locales. Los clientes deben conectar los discos locales como búferes de carga y caché a la máquina virtual Volume Gateway de acuerdo con sus requisitos normativos y de conformidad internos. Se recomienda que, en el caso de la PHI, estos discos sean capaces de proporcionar cifrado en reposo. La comunicación entre la máquina virtual de Volume Gateway y AWS se cifra mediante TLS 1.2 para proteger la PHI durante el transporte.

Gateway de cinta

Tape Gateway proporciona una interfaz VTL (biblioteca de cintas virtuales) para aplicaciones de respaldo de terceros que se ejecutan en las instalaciones. Los clientes deben habilitar el cifrado de la PHI en la aplicación de respaldo de terceros al configurar un trabajo de respaldo en cinta. La comunicación entre la máquina virtual de Tape Gateway y AWS se cifra mediante TLS 1.2 para proteger la PHI durante el transporte. Los clientes que utilicen cualquiera de las configuraciones de Storage Gateway con PHI deben habilitar el registro completo. Para obtener más información, consulte ¿Qué es AWS Storage Gateway?

AWS Systems Manager

AWS Systems Manager es una interfaz unificada que permite a los clientes centralizar fácilmente los datos operativos, automatizar las tareas en todos sus recursos de AWS y acortar el tiempo necesario para detectar y resolver problemas operativos en su infraestructura. Systems Manager proporciona una visión completa del rendimiento y la configuración de la infraestructura del cliente, simplifica la administración de recursos y aplicaciones y facilita el funcionamiento y la administración de su infraestructura a escala.

Al enviar datos que puedan contener PHI a otros servicios, como Amazon S3, los clientes deben seguir las instrucciones del servicio receptor para almacenar la PHI. Los clientes no deben incluir la PHI en los metadatos o identificadores, como los nombres de los documentos y los nombres de los parámetros.

AWS Transfer for SFTP

AWS Transfer for SFTP proporciona acceso mediante el Protocolo seguro de transferencia de archivos (SFTP) a los recursos de S3 del cliente. Los clientes disponen de un servidor virtual,

al que se accede mediante el protocolo SFTP estándar en un punto final de servicio regional. Desde el punto de vista del cliente de AWS y del cliente de SFTP, la puerta de enlace de SFTP tiene el aspecto de un servidor SFTP estándar de alta disponibilidad. Si bien el servicio en sí no almacena, procesa ni transmite la PHI, los recursos a los que accede el cliente en Amazon S3 deben configurarse de forma coherente con las directrices. Los clientes también pueden utilizarlo AWS CloudTrail para registrar las llamadas a la API realizadas a AWS Transfer for SFTP.

AWS WAF: firewall de aplicaciones web

AWS WAF es un firewall de aplicaciones web que ayuda a proteger las aplicaciones web de los clientes de las vulnerabilidades web más comunes que podrían afectar a la disponibilidad de las aplicaciones, comprometer la seguridad o consumir recursos excesivos. Los clientes pueden colocar AWS WAF entre sus aplicaciones web alojadas en AWS que funcionan con PHI o la intercambian, y sus usuarios finales. Al igual que ocurre con la transmisión de cualquier PHI en AWS, los datos que contengan PHI deben cifrarse mientras estén en tránsito. Consulte la guía de Amazon EC2 para comprender mejor las opciones de cifrado disponibles.

AWS X-Ray

AWS X-Ray es un servicio que recopila datos sobre las solicitudes que atiende la aplicación de un cliente y proporciona herramientas que pueden utilizar para ver, filtrar y obtener información sobre esos datos a fin de identificar problemas y oportunidades de optimización. Para cualquier solicitud rastreada hasta la aplicación de un cliente, pueden ver información detallada no solo sobre la solicitud y la respuesta, sino también sobre las llamadas que su aplicación realiza a los recursos, microservicios, bases de datos y API web HTTP descendentes de AWS. AWS X-Ray no debe usarse para almacenar o procesar la PHI. La información que se transmite desde y hacia donde AWS X-Ray se envía está cifrada de forma predeterminada. Cuando la utilice AWS X-Ray, no coloque ninguna PHI en las anotaciones de los segmentos o en los metadatos de los segmentos.

Elastic Load Balancing

Los clientes pueden usar Elastic Load Balancing para finalizar y procesar sesiones que contengan PHI. Los clientes pueden elegir entre Classic Load Balancer o Application Load Balancer. Como todo el tráfico de red que contiene PHI debe cifrarse en tránsito end-to-end, los clientes tienen la flexibilidad de implementar dos arquitecturas diferentes:

Los clientes pueden cancelar HTTPS, HTTP/2 a través de TLS (para aplicaciones) o SSL/TLS en Elastic Load Balancing creando un balanceador de cargas que utilice un protocolo cifrado para las conexiones. Esta función permite cifrar el tráfico entre el balanceador de cargas y los clientes que inician sesiones HTTPS, HTTP/2 sobre TLS o SSL/TLS, y para las conexiones entre el balanceador de cargas y las instancias de backend del cliente. Las sesiones que contienen PHI deben cifrar tanto a los oyentes frontales como a los de backend para el cifrado del transporte. Los clientes deben evaluar sus políticas de certificación y negociación de sesiones y mantenerlas de acuerdo con la Guía. Para obtener más información, consulta HTTPS Listeners for Your Classic Load Balancer.

Como alternativa, los clientes pueden configurar Amazon ELB en el modo TCP básico (para la versión clásica) o superior WebSockets (para la aplicación) y transferir las sesiones cifradas a las instancias de back-end en las que finaliza la sesión cifrada. En esta arquitectura, los clientes administran sus propios certificados y políticas de negociación de TLS en aplicaciones que se ejecutan en sus propias instancias. Para obtener más información, consulte Listeners for Your Classic Load Balancer. En ambas arquitecturas, los clientes deben implementar un nivel de registro que, a su juicio, sea coherente con los requisitos de la HIPAA y la HITECH.

FreeRTOS

Freertos es un sistema operativo para microcontroladores que hace que los dispositivos periféricos pequeños y de bajo consumo sean fáciles de programar, implementar, proteger, conectar y administrar. FreeRTOS se basa en el núcleo FreeRTOS, un popular sistema operativo de código abierto para microcontroladores, y lo amplía con bibliotecas de software que facilitan la conexión segura de dispositivos pequeños y de bajo consumo a los servicios en la nube de AWS, como AWS IoT Core, o a dispositivos periféricos más potentes que se estén ejecutando. AWS IoT Greengrass

Los datos que contienen PHI ahora se pueden cifrar en tránsito y en reposo cuando se utiliza un dispositivo compatible con FreeRTOS. Freertos proporciona dos bibliotecas para proporcionar seguridad a la plataforma: TLS y PKCS #11. La API TLS debe usarse para cifrar y autenticar todo el tráfico de red que contiene PHI. El PKCS #11 proporciona una interfaz estándar para las operaciones criptográficas de software y debe usarse para cifrar cualquier PHI almacenada en un dispositivo apto que ejecute Freertos.

Se utiliza para el cifrado de la PHI AWS KMS

Las claves de KMS se pueden usar para cifrar o descifrar las claves de cifrado de datos que se utilizan para cifrar la PHI en las aplicaciones de un cliente o en los servicios de AWS que la utilizan.

AWS KMS AWS KMS se puede usar junto con una cuenta de la HIPAA, pero la PHI solo se puede procesar, almacenar o transmitir en los servicios que cumplen con los requisitos de la HIPAA. AWS KMS normalmente se usa para generar y administrar claves para aplicaciones que se ejecutan en otros servicios que cumplen con los requisitos de la HIPAA.

Por ejemplo, una aplicación que procese la PHI en Amazon EC2 podría utilizar la llamada a la GenerateDataKey API para generar claves de cifrado de datos para cifrar y descifrar la PHI en la aplicación. Las claves de cifrado de datos estarían protegidas por las claves de KMS del cliente almacenadas en ellas AWS KMS, lo que crearía una jerarquía de claves altamente auditable a medida que se inicien sesión en las llamadas a la AWS KMS API. AWS CloudTrail La PHI no debe almacenarse en las etiquetas (metadatos) de ninguna clave almacenada en AWS KMS ellas.

VM Import/Export

VM Import/Export permite a los clientes importar fácilmente imágenes de máquinas virtuales del entorno existente a las instancias de Amazon EC2 y exportarlas de nuevo a su entorno local. Esta oferta permite a los clientes aprovechar las inversiones existentes en las máquinas virtuales que ha creado para cumplir con sus requisitos de seguridad de TI, administración de la configuración y conformidad al incorporar esas máquinas virtuales a Amazon ready-to-use EC2 como instancias. Los clientes también pueden exportar las instancias importadas a su infraestructura de virtualización local, lo que les permite implementar cargas de trabajo en toda su infraestructura de TI.

VM Import/Export está disponible sin cargo adicional, aparte de los cargos por uso estándar para Amazon EC2 y Amazon S3.

Para importar imágenes de clientes, los clientes pueden usar estas AWS CLI u otras herramientas de desarrollador para importar una imagen de máquina virtual (VM) desde su entorno de VMware. Si los clientes utilizan la plataforma de virtualización VMware vSphere, también pueden utilizar el AWS Management Portal for vCenter para importar sus máquinas virtuales. Como parte del proceso de importación, VM Import convertirá la máquina virtual del cliente en una AMI de Amazon EC2, que podrá utilizar para ejecutar instancias de Amazon EC2. Una vez importada su máquina virtual, pueden aprovechar la elasticidad, escalabilidad y monitoreo de Amazon a través de ofertas como Auto Scaling y Elastic Load Balancing y CloudWatch para soportar sus imágenes importadas.

Los clientes pueden exportar instancias de Amazon EC2 previamente importadas mediante las herramientas de la API de Amazon EC2. Solo tiene que especificar la instancia de destino, el formato de archivo de la máquina virtual y un bucket de Amazon S3 de destino, y VM Import/Export exportará automáticamente la instancia al depósito de Amazon S3 junto con opciones de cifrado para proteger

la transmisión y el almacenamiento de las imágenes de sus máquinas virtuales. A continuación, los clientes pueden descargar e iniciar la máquina virtual exportada dentro de su infraestructura de virtualización local.

Los clientes pueden importar máquinas virtuales Windows y Linux que utilicen los formatos de virtualización VMware ESX o Workstation, Microsoft Hyper-V y Citrix Xen. Además, los clientes pueden exportar instancias de Amazon EC2 previamente importadas a los formatos VMware ESX, Microsoft Hyper-V o Citrix Xen. Para obtener una lista completa de los sistemas operativos, versiones y formatos compatibles, consulte Requisitos de importación y exportación de máquinas virtuales. AWS planea añadir soporte para sistemas operativos, versiones y formatos adicionales en el futuro.

Auditoría, copias de seguridad y recuperación ante desastres

La norma de seguridad de la HIPAA contiene requisitos detallados relacionados con las capacidades de auditoría exhaustiva, los procedimientos de copia de seguridad de los datos y los mecanismos de recuperación ante desastres. Los servicios de AWS contienen muchas características que ayudan a los clientes a cumplir sus requisitos. Por ejemplo, los clientes deberían considerar la posibilidad de establecer capacidades de auditoría que permitan a los analistas de seguridad examinar los registros o informes de actividad detallados para ver quién tuvo acceso, la dirección IP ingresada, a qué datos se accedió, etc.

En caso de una auditoría, estos datos deben rastrearse, registrarse y almacenarse en una ubicación central durante períodos prolongados. Con Amazon EC2, los clientes pueden ejecutar archivos de registro de actividad y auditorías hasta la capa de paquetes de sus servidores virtuales, tal como lo hacen en el hardware tradicional. También pueden rastrear cualquier tráfico IP que llegue a su instancia de servidor virtual. Los administradores del cliente pueden hacer copias de seguridad de los archivos de registro en Amazon S3 para un almacenamiento fiable a largo plazo.

La HIPAA también establece requisitos detallados relacionados con el mantenimiento de un plan de contingencia para proteger los datos en caso de emergencia y debe crear y mantener copias exactas y recuperables de la PHI electrónica. Para implementar un plan de respaldo de datos en AWS, Amazon EBS ofrece almacenamiento persistente para las instancias de servidores virtuales Amazon EC2. Estos volúmenes se pueden exponer como dispositivos de bloques estándar y ofrecen almacenamiento fuera de la instancia que persiste independientemente de la vida útil de la instancia. Para cumplir con las directrices de la HIPAA, los clientes pueden crear point-in-time instantáneas de los volúmenes de Amazon EBS que se almacenan automáticamente en Amazon S3 y se replican en varias zonas de disponibilidad, que son ubicaciones distintas diseñadas para aislarlas de los fallos en otras zonas de disponibilidad.

Se puede acceder a estas instantáneas en cualquier momento y pueden proteger los datos para garantizar una durabilidad a largo plazo. Amazon S3 también proporciona una solución de alta disponibilidad para el almacenamiento de datos y las copias de seguridad automatizadas. Con solo cargar un archivo o una imagen en Amazon S3, se crean automáticamente varias copias redundantes y se almacenan en centros de datos independientes. Se puede acceder a estos archivos en cualquier momento y desde cualquier lugar (según los permisos) y se almacenan hasta que se eliminen intencionalmente.

Además, AWS ofrece de forma inherente una variedad de mecanismos de recuperación ante desastres. La recuperación ante desastres, el proceso de proteger los datos y la infraestructura de TI de una organización en caso de desastre, implica mantener los sistemas de alta disponibilidad, mantener tanto los datos como el sistema replicados fuera de las instalaciones y permitir el acceso continuo a ambos.

Con Amazon EC2, los administradores pueden iniciar instancias de servidor muy rápidamente y pueden usar una dirección IP elástica (una dirección IP estática para el entorno de computación en nube) para realizar una conmutación por error sin problemas de una máquina a otra. Amazon EC2 también ofrece zonas de disponibilidad. Los administradores pueden lanzar instancias de Amazon EC2 en varias zonas de disponibilidad para crear sistemas tolerantes a errores y geográficamente diversos que sean altamente resilientes en caso de fallos de red, desastres naturales y la mayoría de las otras fuentes probables de tiempo de inactividad.

Con Amazon S3, los datos de un cliente se replican y almacenan automáticamente en centros de datos independientes para ofrecer un almacenamiento de datos fiable diseñado para ofrecer una disponibilidad del 99,99%.

Con AWS Elastic Disaster Recovery (AWS DRS), los clientes pueden recuperar rápidamente las aplicaciones en AWS, ya sea en el up-to-date estado más avanzado de las aplicaciones o desde un momento anterior.

Revisiones del documento

Para recibir notificaciones sobre las actualizaciones de este documento técnico, suscríbase a la fuente RSS.

Cambio	Descripción	Fecha
Actualización menor	Actualización menor	12 de mayo de 2023
Actualización menor	Se actualizó el documento técnico para ampliar el contenido disponible en los servicios.	28 de septiembre de 2022
Actualización menor	Corrija el lenguaje no inclusivo .	6 de abril de 2022
Documento técnico actualizado	Se agregó información sobre el Servicio de migración de AWS aplicaciones e información actualizada sobre Amazon ECS	6 de diciembre de 2021
Documento técnico actualizado	Información actualizada en las secciones de Amazon Healthlake y Amazon VPC	9 de noviembre de 2021
Documento técnico actualizado	Se agregó información sobre AWS Network Firewall	9 de septiembre de 2021
Documento técnico actualizado	Información actualizada sobre los perfiles de clientes de Amazon Connect	26 de agosto de 2021
Documento técnico actualizado	Se agregaron las secciones Amazon AppFlow y AWS Glue DataBrew	22 de julio de 2021

Documento técnico actualizado	Navegación y organización actualizadas.	26 de abril de 2021
Documento técnico actualizado	Se agregaron las siguientes secciones: 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 AWS Serverless Application Repository, Amazon. HealthLake EventBridge Sección Amazon Aurora actualizada.	31 de marzo de 2021
Documento técnico actualizado	Se agregó una sección sobre AWS App Mesh y se actualizó el contenido de AWS System Manager	25 de agosto de 2020
Documento técnico actualizado	Se agregaron las secciones Amazon Appstream 2.0, AWS SDK Metrics, AWS Data Exchange, Amazon MSK, Amazon Pinpoint, Amazon Lex, Amazon SES y Amazon Forecast, Amazon Quantum Ledger Database (QLDB),. AWS Cloud Map	7 de mayo de 2020

Documento técnico actualizado	Se agregaron secciones sobre Amazon CloudWatch, Amazon CloudWatch Events, Amazon Data Firehose, Amazon Managed Service for Apache Flink, Amazon OpenSearch Service, Amazon DocumentDB (compatible con MongoDB), AWS Mobile Hub, AWS OpsWorks Chef Automate, Puppet Enterprise, AWS AWS IoT Greengrass Transfer for SFTP, AWS AWS Global Accelerator, Amazon Comprehend Medical y DataSync AWS. AWS OpsWorks RoboMaker	1 de enero de 2020
Documento técnico actualizado	Se agregaron secciones sobre Amazon Comprehend, Amazon Transcribe, Amazon Translate y AWS Certificate Manager.	1 de enero de 2019
Documento técnico actualizado	Se agregaron secciones sobre Amazon Athena, Amazon EKS, AWS IoT Core y Amazon FreeRTOS AWS IoT Device Management, GuardDuty Amazon, Amazon Neptune, AWS Server Migration Service AWS Database Migration Service, Amazon MQ y. AWS Glue	1 de noviembre de 2018

Documento técnico actualizado	Se agregaron secciones sobre Amazon Elastic File System (EFS), Amazon Kinesis Video Streams, Amazon Rekogniti on, Amazon, SageMaker Amazon Simple Workflow, AWS Secrets Manage, Service Catalog y. AWS Step Functions	1 de junio de 2018
Documento técnico actualizado	Se agregaron secciones sobre AWS CloudFormation, AWS X-Ray, AWS CloudTrail AWS CodeBuild AWS CodeCommi t, AWS Config y Stack. AWS OpsWorks	1 de abril de 2018
Documento técnico actualizado	Se agregó una sección sobre AWS Fargate.	1 de enero de 2018

Actualizaciones realizadas antes de 2018:

Date	Descripción
Noviembre de 2017	Se agregaron secciones en Amazon EC2 Container Registry, Amazon Macie, QuickSight Amazon y. AWS Managed Services
Noviembre de 2017	Se agregaron secciones en Amazon ElastiCac he para Redis y Amazon CloudWatch.
de octubre de 2017	Se agregaron secciones en Amazon SNS, Amazon Route 53 y AWS Storage Gateway. AWS CloudHSM Sección actualizada sobre. AWS Key Management Service

Date	Descripción
Septiembre de 2017	Se agregaron secciones sobre Amazon Connect, Amazon Kinesis Streams, Amazon RDS (Maria) DB, Amazon RDS SQL Server AWS Batch AWS Lambda AWS Snowball , Edge y la función Lambda @Edge de Amazon. CloudFront
Agosto de 2017	Se han añadido secciones sobre Amazon EC2 Systems Manager y Amazon Inspector.
Julio de 2017	Se agregaron secciones sobre Amazon WorkSpaces WorkDocs, Amazon, AWS Directory Service y Amazon ECS.
Junio de 2017	Se agregaron secciones sobre Amazon CloudFront, AWS WAF y Amazon S3 Transfer Acceleration. AWS Shield
2017 de mayo	Se eliminó el requisito de instancias dedicadas o hosts dedicados para procesar la PHI en EC2 y EMR.
Marzo de 2017	Se actualizó la lista de servicios para que apunte a la página Servicios de AWS incluidos en el ámbito del programa de conformidad. Se agregó una descripción para Amazon API Gateway.
Enero de 2017	Se ha actualizado a la plantilla más reciente.
Octubre de 2016	Publicación inicial

Avisos

Es responsabilidad de los clientes realizar su propia evaluación independiente de la información que contiene este documento. El presente documento: (a) tiene solo fines informativos, (b) representa las ofertas y prácticas actuales de los productos de AWS, que están sujetas a cambios sin previo aviso, y (c) no supone ningún compromiso ni garantía por parte de AWS y sus filiales, proveedores o licenciantes. Los productos o servicios de AWS se proporcionan “tal cual” sin garantías, declaraciones ni condiciones de ningún tipo, ya sean expresas o implícitas. Las responsabilidades y obligaciones de AWS con respecto a sus clientes se controlan mediante los acuerdos de AWS y este documento no forma parte ni modifica ningún acuerdo entre AWS y sus clientes.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.