Whitepaper da AWS

Arquitetando para Segurança HIPAA e Conformidade no Amazon Web Services

Arquitetando para Segurança HIPAA e Conformidade no Amazon Web Services: Whitepaper da AWS

Table of Contents

Arquitetando para Segurança HIPAA e Conformidade no Amazon Web Services

Data de publicação: 28 de setembro de 2022 (Revisões do documento)

Este paper descreve brevemente como os clientes podem usar a Amazon Web Services (AWS) para executar cargas de trabalho confidenciais regulamentadas pela Lei de Portabilidade e Responsabilidade de Seguros de Saúde dos EUA (HIPAA). Vamos nos concentrar nas regras de privacidade e segurança da HIPAA para proteger informações de saúde protegidas (PHI), como usar a AWS para criptografar dados em trânsito e em repouso e como os recursos da AWS podem ser usados para executar cargas de trabalho contendo PHI.

Introdução

A Lei de Portabilidade e Responsabilidade de Seguros de Saúde de 1996 (HIPAA) se aplica a “entidades cobertas” e “parceiros de negócios”. A HIPAA foi expandida em 2009 pela Lei de Tecnologia da Informação em Saúde para Saúde Econômica e Clínica (HITECH).

A HIPAA e a HITECH estabelecem um conjunto de padrões federais destinados a proteger a segurança e a privacidade das PHI. A HIPAA e a HITECH impõem requisitos relacionados ao uso e divulgação de informações de saúde protegidas (PHI), salvaguardas apropriadas para proteger as PHI, direitos individuais e responsabilidades administrativas. Para obter mais informações sobre HIPAA e HITECH, acesse o Health Information Privacy Home.

As entidades cobertas e seus parceiros comerciais podem usar os componentes de TI seguros, escaláveis e de baixo custo fornecidos pela Amazon Web Services (AWS) para arquitetar aplicativos alinhados aos requisitos de conformidade da HIPAA e da HITECH. A AWS oferece uma plataforma de commercial-off-the-shelf infraestrutura com certificações e auditorias reconhecidas pelo setor, como ISO 27001, FedRAMP e os Relatórios de Controle da Organização de Serviços (SOC1, SOC2 e SOC3). Os serviços e datacenters da AWS têm várias camadas de segurança operacional e física para ajudar a garantir a integridade e a segurança dos dados dos clientes. Sem taxas mínimas, sem contratos baseados em prazos e pay-as-you-use preços, a AWS é uma solução confiável e eficaz para o crescimento de aplicativos do setor de saúde.

A AWS permite que entidades cobertas e seus parceiros comerciais sujeitos à HIPAA processem, armazenem e transmitam PHI com segurança. Além disso, a partir de julho de 2013, a AWS oferece um Adendo de Associado Comercial (BAA) padronizado para esses clientes. Os clientes que executam um BAA da AWS podem usar qualquer serviço da AWS em uma conta designada como conta da HIPAA, mas só podem processar, armazenar e transmitir PHI usando os serviços elegíveis para a HIPAA definidos no BAA da AWS. Para obter uma lista completa desses serviços, consulte a página de referência de serviços qualificados pela HIPAA.

A AWS mantém um programa de gerenciamento de riscos baseado em padrões para garantir que os serviços qualificados pela HIPAA ofereçam suporte específico às proteções administrativas, técnicas e físicas da HIPAA. O uso desses serviços para armazenar, processar e transmitir PHI ajuda nossos clientes e a AWS a atender aos requisitos da HIPAA aplicáveis ao modelo operacional baseado em utilitários da AWS.

O BAA da AWS exige que os clientes criptografem as PHI armazenadas ou transmitidas usando serviços qualificados pela HIPAA, de acordo com a orientação do Secretary of Health and Human

Services (HHS): Orientação para tornar inutilizáveis, ilegíveis ou indecifráveis informações de saúde protegidas não seguras para indivíduos não autorizados (“Orientação”). Consulte este site porque ele pode ser atualizado e disponibilizado em um site sucessor (ou relacionado) designado pelo HHS.

A AWS oferece um conjunto abrangente de recursos e serviços para tornar o gerenciamento de chaves e a criptografia de PHI fáceis de gerenciar e simplificar a auditoria, incluindo o AWS Key Management Service ()AWS KMS. Os clientes com requisitos de conformidade com a HIPAA têm muita flexibilidade na forma como atendem aos requisitos de criptografia para PHI.

Ao determinar como implementar a criptografia, os clientes podem avaliar e aproveitar os recursos de criptografia nativos dos serviços qualificados pela HIPAA. Ou os clientes podem satisfazer os requisitos de criptografia por outros meios consistentes com as orientações do HHS.

Criptografia e proteção de PHI na AWS

A regra de segurança da HIPAA inclui especificações de implementação endereçáveis para a criptografia de PHI na transmissão (“em trânsito”) e no armazenamento (“em repouso”). Embora essa seja uma especificação de implementação endereçável na HIPAA, a AWS exige que os clientes criptografem as PHI armazenadas ou transmitidas usando serviços qualificados pela HIPAA, de acordo com a orientação da Secretaria de Saúde e Serviços Humanos (HHS): Orientação para tornar inutilizáveis, ilegíveis ou indecifráveis informações de saúde protegidas não seguras para indivíduos não autorizados (“Orientação”). Consulte este site porque ele pode ser atualizado e disponibilizado em um sucessor (ou site relacionado) designado pelo HHS.

A AWS oferece um conjunto abrangente de recursos e serviços para tornar o gerenciamento de chaves e a criptografia de PHI fáceis de gerenciar e simplificar a auditoria, incluindo o AWS Key Management Service ()AWS KMS. Os clientes com requisitos de conformidade com a HIPAA têm muita flexibilidade na forma como atendem aos requisitos de criptografia para PHI.

Ao determinar como implementar a criptografia, os clientes podem avaliar e aproveitar os recursos de criptografia nativos dos serviços qualificados pela HIPAA, ou podem satisfazer os requisitos de criptografia por outros meios consistentes com as orientações do HHS. As seções a seguir fornecem detalhes de alto nível sobre o uso dos recursos de criptografia disponíveis em cada um dos serviços qualificados pela HIPAA e outros padrões para criptografar PHI, e como o AWS KMS pode ser usado para criptografar as chaves usadas para criptografia de PHI na AWS.

Tópicos

- Amazon API Gateway
- Amazon AppFlow
- Amazon AppStream 2.0
- Amazon Athena
- Amazon Aurora
- Amazon Aurora PostgreSQL
- Amazon CloudFront
- Amazon CloudWatch
- CloudWatch Eventos da Amazon
- CloudWatch Registros da Amazon

- Amazon Comprehend
- Amazon Comprehend Medical
- Amazon Connect
- Amazon DocumentDB (compatível com 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 Serviço Amazon
- Amazon EMR
- Amazon EventBridge
- Amazon Forecast
- Amazon FSx
- Amazon GuardDuty
- Amazon HealthLake
- Amazon Inspector
- Amazon Managed Service for 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 Firewall de rede

- 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 Serviço de migração de aplicativos
- 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
- Recuperação elástica de desastres da AWS
- AWS Fargate
- AWS Firewall Manager
- AWS Global Accelerator
- AWS Glue
- AWS Glue DataBrew
- AWS IoT Núcleo e AWS IoT Device Management
- AWS IoT Greengrass
- AWS Lambda
- AWS Managed Services
- AWS OpsWorks para Chef Automate
- AWS OpsWorks para Puppet Enterprise
- AWS OpsWorks Pilha
- AWS Organizations

- AWS RoboMaker
- Métricas do AWS SDK
- AWS Secrets Manager
- AWS Security Hub
- AWS Server Migration Service
- AWS Serverless Application Repository
- Service Catalog
- AWS Shield
- AWS Snowball
- AWS Snowball Borda
- AWS Step Functions
- AWS Storage Gateway
- AWS Systems Manager
- AWS Transfer for SFTP
- AWS WAF — Firewall de aplicativos web
- AWS X-Ray
- Elastic Load Balancing
- FreeRTOS
- Usando AWS KMS para criptografia de PHI
- VM Import/Export

Amazon API Gateway

Os clientes podem usar o Amazon API Gateway para processar e transmitir informações de saúde protegidas (PHI). Embora o Amazon API Gateway use automaticamente endpoints HTTPS para criptografia em andamento, os clientes também podem optar por criptografar cargas no lado do cliente. O API Gateway passa todos os dados não armazenados em cache pela memória e não os grava no disco. Os clientes podem usar o AWS Signature versão 4 para autorização com o API Gateway. Para obter mais informações, consulte:

- Perguntas frequentes sobre o Amazon API Gateway: Segurança e autorização
- Controle e gerenciamento do acesso a uma API REST no API Gateway

Os clientes podem se integrar a qualquer serviço conectado ao API Gateway, desde que, quando a PHI esteja envolvida, o serviço seja configurado de acordo com o Guidance e o BAA. Para obter informações sobre a integração do API Gateway com serviços de back-end, consulte Configurar métodos da API REST no API Gateway.

Os clientes podem usar AWS CloudTrail a Amazon CloudWatch para habilitar o registro que seja consistente com seus requisitos de registro. Certifique-se de que qualquer PHI enviada pelo API Gateway (como em cabeçalhos, URLs e solicitação/resposta) seja capturada somente por serviços qualificados pela HIPAA que tenham sido configurados para serem consistentes com a Orientação. Para obter mais informações sobre o registro com o API Gateway, consulte Como habilito CloudWatch os registros para solucionar problemas com minha API REST ou WebSocket API do API Gateway?

Amazon AppFlow

AppFlow A Amazon é um serviço de integração totalmente gerenciado que permite aos clientes transferir dados com segurança entre aplicativos S oftware-as-a -Service (SaaS), como Salesforce, Marketo, Slack e, e serviços da ServiceNow AWS, como Amazon S3 e Amazon Redshift. AppFlow pode executar fluxos de dados na frequência que o cliente escolher — em um cronograma, em resposta a um evento comercial ou sob demanda. Os clientes também podem configurar recursos de transformação de dados, como filtragem e validação, para gerar ready-to-use dados ricos como parte do próprio fluxo, sem etapas adicionais.

A Amazon AppFlow pode ser usada para processar e transferir dados contendo PHI. A criptografia de dados em trânsito entre AppFlow a origem/destino configurada é fornecida por padrão usando o TLS 1.2 ou posterior. Os dados armazenados em repouso no S3 são criptografados automaticamente usando uma AWS KMS chave (antiga CMK) especificada pelo cliente. Para dados PHI transferidos para destinos que não sejam do S3, os clientes devem garantir que o armazenamento em repouso para o destino escolhido atenda às suas necessidades de segurança. AppFlow permite o monitoramento de aplicativos por meio da integração com AWS CloudTrail o registro de chamadas de API e EventBridge a Amazon para emitir eventos de execução de fluxo.

Amazon AppStream 2.0

O Amazon AppStream 2.0 é um serviço de streaming de aplicativos totalmente gerenciado. Os clientes são proprietários de seus dados e devem configurar os aplicativos Windows necessários de uma forma que atenda aos requisitos normativos. Os clientes podem configurar o armazenamento persistente por meio de pastas pessoais. Os arquivos e as pastas são criptografados em trânsito

usando endpoints SSL do Amazon S3. Arquivos e pastas são criptografados em repouso usando chaves de criptografia gerenciadas pelo Amazon S3. Para obter mais informações, consulte Habilitar e administrar armazenamento persistente para seus usuários AppStream 2.0. Se os clientes optarem por usar uma solução de armazenamento de terceiros, eles são responsáveis por garantir que a configuração dessa solução seja consistente com a orientação. Toda comunicação pública da API com a Amazon AppStream 2.0 é criptografada usando TLS. Para obter mais informações, consulte a documentação da Amazon AppStream 2.0.

O Amazon AppStream 2.0 é integrado com AWS CloudTrail um serviço que registra chamadas de API feitas por ou em nome da Amazon AppStream 2.0 na conta da AWS do cliente e entrega os arquivos de log ao bucket especificado do Amazon S3. CloudTrail captura chamadas de API feitas a partir do console da Amazon AppStream 2.0 ou da API da Amazon AppStream 2.0. Os clientes também podem usar CloudWatch a Amazon para registrar métricas de uso de recursos. Para obter mais informações, consulte Monitoramento de recursos da Amazon AppStream 2.0 e Registro de chamadas de API AppStream 2.0 com AWS CloudTrail.

Amazon Athena

O Amazon Athena é um serviço de consultas interativas que facilita a análise de dados diretamente no Amazon Simple Storage Service (Amazon S3) usando SQL padrão. O Athena ajuda os clientes a analisar dados não estruturados, semiestruturados e estruturados armazenados no Amazon S3. Entre os exemplos estão formatos de dados CSV, JSON ou colunares, como Apache Parquet e Apache ORC. Os clientes podem usar o Athena para executar consultas ad hoc usando ANSI SQL, sem a necessidade de agregar ou carregar os dados no Athena.

O Amazon Athena agora pode ser usado para processar dados contendo PHI. A criptografia de dados em trânsito entre o Amazon Athena e o S3 é fornecida por padrão usando SSL/TLS. A criptografia de PHI em repouso no S3 deve ser executada de acordo com as orientações fornecidas na seção S3. A criptografia dos resultados da consulta de e dentro do Amazon Athena, incluindo resultados em estágios, deve ser habilitada usando criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3), chaves gerenciadas (SSE-KMS) ou criptografia do lado do cliente com chaves gerenciadas (CSE-KMS) AWS KMS. AWS KMS O Amazon Athena usa AWS CloudTrail para registrar todas as chamadas de API.

Amazon Aurora

O Amazon Aurora permite que os clientes criptografem clusters e snapshots do banco de dados do Aurora em repouso usando chaves que eles gerenciam. AWS KMS Em uma instância de banco

de dados executada com a criptografia do Amazon Aurora, os dados armazenados em repouso no armazenamento subjacente são criptografados, assim como os backups automatizados, as réplicas de leitura e os snapshots.

Como a orientação pode ser atualizada, os clientes devem continuar avaliando e determinando se a criptografia do Amazon Aurora satisfaz seus requisitos regulatórios e de conformidade. Para obter mais informações sobre criptografia em repouso usando o Amazon Aurora, consulte Proteção de dados usando criptografia.

As conexões com clusters de banco de dados que executam o Aurora MySQL devem usar criptografia de transporte, utilizando Secure Socket Layer (SSL) ou Transport Layer Security (TLS). Para obter mais informações sobre a implementação de SSL/TLS, consulte Como usar SSL/TLS com clusters de banco de dados Aurora MySQL.

Amazon Aurora PostgreSQL

O Amazon Aurora permite que os clientes criptografem clusters e snapshots do banco de dados do Aurora em repouso usando chaves que eles gerenciam. AWS KMS Em uma instância de banco de dados executada com a criptografia do Amazon Aurora, os dados armazenados em repouso no armazenamento subjacente são criptografados, assim como os backups automatizados, as réplicas de leitura e os snapshots.

Como a orientação pode ser atualizada, os clientes devem continuar avaliando e determinando se a criptografia do Amazon Aurora satisfaz seus requisitos regulatórios e de conformidade. Para obter mais informações sobre criptografia em repouso usando o Amazon Aurora, consulte Proteção de dados usando criptografia.

As conexões com clusters de banco de dados que executam o Aurora PostgreSQL devem usar criptografia de transporte, utilizando Secure Socket Layer (SSL) ou Transport Layer Security (TLS). Para obter mais informações sobre a implementação de SSL/TLS, consulte Como proteger dados do Aurora PostgreSQL com SSL.

Amazon CloudFront

CloudFront A Amazon é um serviço global de rede de entrega de conteúdo (CDN) que acelera a entrega de sites, APIs, conteúdo de vídeo ou outros ativos da web para clientes. Ele se integra a outros produtos da Amazon Web Services para oferecer aos desenvolvedores e às empresas uma maneira fácil de acelerar o conteúdo para os usuários finais sem compromissos mínimos de

uso. Para garantir a criptografia da PHI durante o trânsito CloudFront, os clientes devem configurar CloudFront para usar HTTPS end-to-end da origem até o visualizador.

Isso inclui o tráfego entre CloudFront e o visualizador, a CloudFront redistribuição a partir de uma origem personalizada e a CloudFront distribuição a partir de uma origem do Amazon S3. Os clientes também devem garantir que os dados sejam criptografados na origem para garantir que permaneçam criptografados em repouso enquanto estão em cache. CloudFront Ao usar o Amazon S3 como origem, os clientes podem usar os recursos de criptografia do lado do servidor do S3. Se os clientes distribuírem de uma origem personalizada, eles devem garantir que os dados sejam criptografados na origem.

Lambda@Edge

O Lambda @Edge é um serviço de computação que permite a execução de funções do Lambda nos pontos de presença da AWS. O Lambda @Edge pode ser usado para personalizar o conteúdo entregue por meio do. CloudFront Ao usar o Lambda @Edge com PHI, os clientes devem seguir a orientação para o uso do. CloudFront Todas as conexões de entrada e saída do Lambda @Edge devem ser criptografadas usando HTTPS ou SSL/TLS.

Amazon CloudWatch

CloudWatch A Amazon é um serviço de monitoramento dos recursos da nuvem da AWS e dos aplicativos que os clientes executam na AWS. Os clientes podem usar CloudWatch a Amazon para coletar e rastrear métricas, coletar e monitorar arquivos de log e definir alarmes. A CloudWatch própria Amazon não produz, armazena ou transmite PHI. Os clientes podem monitorar as chamadas de CloudWatch API com AWS CloudTrail. Para obter mais informações, consulte Registrar chamadas de CloudWatch API da Amazon com AWS CloudTrail.

Para obter mais detalhes sobre os requisitos de configuração, consulte a seção Amazon CloudWatch Logs.

CloudWatch Eventos da Amazon

A Amazon CloudWatch Events fornece um near-real-time fluxo de eventos do sistema que descrevem as mudanças nos recursos da AWS. Os clientes devem garantir que a PHI não flua para CloudWatch os Eventos, e que qualquer recurso da AWS que emita um CloudWatch evento que esteja armazenando, processando ou transmitindo PHI seja configurado de acordo com a Orientação.

Os clientes podem configurar o Amazon CloudWatch Events para se registrarem como uma chamada de API da AWS CloudTrail. Para obter mais informações, consulte Criação de uma regra de CloudWatch eventos que é acionada em uma chamada de API da AWS usando. AWS CloudTrail

CloudWatch Registros da Amazon

Os clientes podem usar o Amazon CloudWatch Logs para monitorar, armazenar e acessar seus arquivos de log das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) AWS CloudTrail, do Amazon Route 53 e de outras fontes. Em seguida, eles podem recuperar os dados de registro associados do CloudWatch Logs. Os dados de registro são criptografados enquanto estão em trânsito e em repouso. Como resultado, não é necessário recriptografar a PHI emitida por nenhum outro serviço e entregue ao Logs. CloudWatch

Amazon Comprehend

O Amazon Comprehend usa o processamento de linguagem natural para extrair insights sobre o conteúdo dos documentos. O Amazon Comprehend processa qualquer arquivo de texto no formato UTF-8. O serviço desenvolve insights por meio do reconhecimento de entidades, frases importantes, linguagem, sentimentos e outros elementos comuns de um documento. O Amazon Comprehend pode ser usado com dados contendo PHI. O Amazon Comprehend não retém nem armazena nenhum dado e todas as chamadas para a API são criptografadas com SSL/TLS. O Amazon Comprehend CloudTrail usa para registrar todas as chamadas de API.

AWS Identity and Access Management

Funções de acesso de segurança, como autenticação e autorização, são necessárias para acessar o Amazon Comprehend e podem ser controladas AWS Identity and Access Managementcom (IAM), e as credenciais podem ser usadas para acessar o IAM. Para obter mais informações, consulte Autenticação e controle de acesso para o Amazon Comprehend no Guia do usuário do Amazon Comprehend.

Gerenciamento de contas

Por padrão, os usuários do IAM não têm permissão para criar ou modificar recursos do Amazon Comprehend nem realizar tarefas usando a API do Amazon Comprehend. Para permitir que os usuários criem ou modifiquem recursos e executem tarefas, os clientes são responsáveis por aproveitar as políticas do IAM que concedem aos usuários permissões para os recursos específicos

(como o Amazon Comprehend e as ações de API) que os usuários precisam usar e, em seguida, anexar políticas aos usuários ou grupos que exigem permissões específicas.

Com o Amazon Comprehend, você pode AWS Identity and Access Management usar (IAM) para criar um usuário com uma política anexada para habilitar as permissões do Amazon Comprehend. Opcionalmente, você pode optar por criar políticas personalizadas para anexar a uma função. Em seguida, você pode adicionar administradores à função com a capacidade de invocar APIs para a administração do Amazon Comprehend de acordo com os princípios de acesso baseado em funções e privilégios mínimos definidos pela organização.

Identidade e acesso

Com o Amazon Comprehend, você pode exigir que o usuário se autentique usando a autenticação AWS multifatorial de acordo com seus requisitos organizacionais de autenticação.

Usando o AWS Management Console, os administradores do IAM podem criar uma política gerenciada pelo cliente que nega todas as permissões, exceto aquelas necessárias para que os usuários gerenciem suas próprias credenciais e dispositivos de MFA. Um modelo de política JSON está disponível na página Minha credencial de segurança no console do IAM.

Opcionalmente, você pode aproveitar recursos de MFA de terceiros compatíveis com parceiros do IAM. Para obter mais informações, consulte Parceiros do IAM.

Administração

Recomendamos que o Amazon Comprehend selecione políticas baseadas em identidade nas quais os administradores da conta possam anexar políticas de permissões às identidades do IAM (usuários, grupos e funções) e, assim, conceder permissões para realizar operações nos recursos do Amazon Comprehend.

Uma lista de ações de API para o Amazon Comprehend pode ser encontrada no Guia de referência de APIs. Você também deve considerar autorizar o acesso a políticas predefinidas de IAM, políticas de IAM de clientes e ações de API para usuários ou funções de acordo com seus menores privilégios e requisitos organizacionais baseados em funções. Para obter mais informações, consulte Como usar a API Amazon Comprehend no Guia do desenvolvedor.

Autenticação externa

O Amazon Comprehend é compatível com a federação de identidades usando funções do IAM. Isso permite que seus usuários se autentiquem no Amazon Comprehend assumindo uma função AWS

provisionada pelos administradores. Os usuários que acessam AWS usando credenciais de sua organização ou de terceiros assumem uma função indiretamente.

AWS o suporte para Kerberos e Active Directory oferece os benefícios do login único e da autenticação centralizada dos usuários do banco de dados. AWS os usuários podem optar por gerenciar e armazenar as credenciais do usuário no AWS Directory Service Microsoft Active Directory ou no Active Directory local do cliente.

Aplicação do fluxo de dados

AWS clientes e parceiros da APN, atuando como controladores ou processadores de dados, são responsáveis por quaisquer dados pessoais que eles coloquem no Amazon Nuvem AWS Comprehend. Você é responsável por controlar o fluxo para entradas e saídas de dados para o Amazon Comprehend usando políticas do IAM.

Proteção de dados e gerenciamento de segredos

O modelo de responsabilidade AWS compartilhada se aplica à proteção de dados no Amazon Comprehend. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa toda a AWS nuvem. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Esse conteúdo inclui as tarefas de configuração e gerenciamento de segurança dos AWS serviços que você usa. Para obter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados.

A seção Proteção de dados no Amazon Comprehend no Guia do desenvolvedor do Amazon Comprehend fornece dicas que você deve considerar para proteger dados, como usar TLS para transmissão e evitar a colocação de informações confidenciais em tags ou campos de formato livre.

Criptografia de data-at-rest

O Amazon Comprehend trabalha com o AWS Key Management Service (AWS KMS) para fornecer criptografia aprimorada para seus dados. O Amazon Simple Storage Service (Amazon S3) já permite que você criptografe seus documentos de entrada ao criar uma análise de texto, modelagem de tópicos ou trabalho personalizado do Amazon Comprehend. A integração com AWS KMS permite que você criptografe os dados no volume de armazenamento para iniciar* e criação* e criptografa os resultados de saída dos trabalhos iniciais* usando sua própria chave. AWS KMS

É uma prática recomendada para os usuários do Amazon Comprehend criptografar os buckets do Amazon S3 usados para inserir documentos usando as soluções de criptografia do S3 disponíveis de acordo com suas políticas organizacionais.

O AWS Management Console, criptografa os modelos personalizados do Amazon Comprehend com sua própria chave. AWS KMS Para o AWS CLI, o Amazon Comprehend pode criptografar modelos personalizados usando sua AWS KMS própria chave ou uma chave gerenciada pelo cliente (CMK) fornecida.

Se selecionar a criptografia ao usar o AWS Management Console, você poderá escolher um ou os dois métodos opcionais a seguir:

- Criptografia de volume - garante que os dados em um volume do EBS usado pelo Comprehend sejam criptografados durante o treinamento/inferência (os dados são liberados após o treinamento/inferência, portanto, essa chave é relevante somente enquanto o trabalho está em andamento).
- Criptografia do resultado de saída - para criptografar a saída armazenada pelo comprehend no bucket do cliente usando uma chave fornecida pelo cliente. AWS KMS

Para obter mais informações sobre tipos de criptografia, como criptografia de volume, consulte AWS KMS Criptografia no Amazon Comprehend.

Informações de identificação pessoal

Você pode usar o console ou as APIs do Amazon Comprehend para detectar informações de identificação pessoal (PII) em documentos com texto em inglês. Para obter mais informações sobre como detectar e rotular entidades de PII e operar vários trabalhos de análise de PII, consulte a seção Informações de identificação pessoal no Guia do desenvolvedor do Amazon Comprehend.

Exclusão de dados

Se você for um cliente do Amazon Comprehend usando o Amazon S3 e optar por gerenciar suas AWS KMS próprias chaves, considere AWS KMS revogar as chaves e definir a justificativa processual para fazer isso de acordo com seus requisitos organizacionais. A revogação da AWS KMS chave para o Amazon S3 torna todos os dados inutilizáveis/ilegíveis.

Segmentação e fortalecimento da rede

Como um serviço gerenciado, o Amazon Comprehend segue AWS as melhores práticas de segurança, identidade e conformidade.

Para obter as proteções de segurança de rede recomendadas, consulte Segurança da infraestrutura no Amazon Comprehend no Guia de desenvolvedores do Amazon Comprehend.

Proteja trabalhos usando uma Amazon Virtual Private Cloud (Amazon VPC)

O Amazon Comprehend usa uma variedade de medidas de segurança para garantir a segurança de seus dados com nossos contêineres de trabalho, onde eles são armazenados enquanto são usados pelo Amazon Comprehend. No entanto, os contêineres de trabalho acessam AWS recursos, como os buckets do Amazon S3, onde você armazena dados e artefatos de modelo, pela Internet.

Para controlar o acesso aos seus dados, recomendamos a criação de uma nuvem privada virtual (VPC) e a sua configuração para que os dados e os contêineres não sejam acessíveis pela internet. Para obter informações sobre como criar e configurar uma VPC, consulte Conceitos básicos da Amazon VPC no Guia do usuário da Amazon VPC. Usar uma VPC ajuda a proteger seus dados, pois é possível configurá-la para não se conectar à internet. Usar uma VPC também permite monitorar todo o tráfego de rede de entrada e saída de seus contêineres de trabalho, com os logs de fluxo da VPC. Para obter mais informações, consulte Logs de fluxo da VPC no Guia do usuário do Amazon Virtual Private Cloud.

Especifique a configuração de sua VPC ao criar um trabalho. Basta especificar as sub-redes e grupos de segurança. Quando você especifica sub-redes e grupos de segurança, o Amazon Comprehend cria interfaces de rede elástica (ENIs) que são associadas aos seus grupos de segurança em uma das sub-redes. ENIs permitem que nossos contêineres de trabalho se conectem a recursos na sua VPC. Para obter informações sobre as ENIs, consulte Interfaces de rede elástica no Guia do usuário da Amazon VPC.

> **Note**
>
> Para trabalhos, você pode configurar apenas sub-redes com uma VPC de locação padrão em que sua instância é executada em hardware compartilhado. Para obter mais informações sobre a locação de atributos das VPCs, consulte Instâncias dedicadas no Guia do usuário do Amazon EC2 para instâncias do Linux.

É possível estabelecer uma conexão privada entre a VPC e o Amazon Comprehend criando um endpoint da VPC de interface. Para obter mais informações, consulte Amazon Comprehend and Interface VPC Endpoints ().AWS PrivateLink

Fortalecimento do host e da imagem

Com base no modelo de responsabilidade AWS compartilhada, o fortalecimento do AWS ambiente de hospedagem e imagem do Amazon Comprehend é gerenciado AWS como um serviço fornecido.

Multilocação

Para ajudar a tornar sua recomendação mais segura, recomendamos que você implemente as seguintes recomendações de segurança de multilocação:

- Use apenas um endereço de e-mail verificado para autorizar o acesso do usuário a um locatário com base na correspondência de domínio. Não confie em endereços de e-mail e números de telefone, a menos que sua aplicação os verifique ou o IdP externo forneça uma prova de verificação. Para obter mais detalhes sobre como configurar essas permissões, consulte Permissões e escopos de atributos.
- Use atributos imutáveis ou mutáveis para os atributos de perfil de usuário que identificam locatários. Os administradores devem ter autonomia para alterar esses atributos. Além disso, conceda aos clientes da aplicação acesso somente leitura aos atributos.
- Use mapeamento 1:1 entre o IdP externo e o cliente da aplicação para impedir o acesso não autorizado entre locatários. Um usuário autenticado por um IdP externo e que tenha um cookie de sessão válido do Amazon Cognito pode acessar outras aplicações de locatários que confiam no mesmo IdP.
- Ao implementar a lógica de correspondência e autorização de locatário em sua aplicação, restrinja os usuários de modo que eles não possam modificar os critérios que autorizam o acesso do usuário aos locatários. Além disso, se um IdP externo estiver sendo usado para federação, restrinja os administradores do provedor de identidade do locatário para que não possam modificar o acesso do usuário.

Prevenção do problema do “confused deputy” entre serviços

O problema confuso do deputado é um problema de segurança de multilocação em que uma entidade que não tem permissão para realizar uma ação pode coagir uma entidade mais privilegiada a realizar a ação. Em AWS, a falsificação de identidade entre serviços pode resultar em um problema confuso de delegado. A imitação entre serviços pode ocorrer quando um serviço (o serviço de chamada) chama outro serviço (o serviço chamado). O serviço de chamada pode ser manipulado para utilizar as suas permissões para atuar nos recursos de outro cliente em que, de outra forma, ele não teria permissão para acessar. Para evitar isso, AWS fornece ferramentas que podem ajudar você a proteger seus dados em todos os serviços com diretores de serviços que receberam acesso aos recursos em sua conta. Para obter mais informações, incluindo proteções que você deve considerar para resolver esse problema de segurança, consulte Cross-service Confused Deputy Prevention no Amazon Comprehend Developer Guide.

Amazon Comprehend Medical

Para obter orientação, consulte a Amazon Comprehend seção anterior.

Amazon Connect

O Amazon Connect é um serviço de central de atendimento de autoatendimento baseado em nuvem que permite um engajamento dinâmico, pessoal e natural do cliente em qualquer escala. Os clientes não devem incluir nenhuma PHI em nenhum campo associado ao gerenciamento de usuários, perfis de segurança e fluxos de contato no Amazon Connect.

O Amazon Connect Customer Profiles, um recurso do Amazon Connect, fornece aos agentes da central de atendimento uma visão mais unificada do perfil do cliente com as informações mais atualizadas, para oferecer um atendimento mais personalizado. O Customer Profiles foi projetado para reunir automaticamente as informações do cliente de vários aplicativos em um perfil de cliente unificado, entregando o perfil diretamente ao agente assim que a chamada de suporte ou a interação começarem. Os clientes devem evitar nomear domínios ou chaves de objetos com dados PHI. O conteúdo de Domínios e Objetos é criptografado e protegido, mas os identificadores de chave não.

Amazon DocumentDB (compatível com MongoDB)

O Amazon DocumentDB (com compatibilidade com o MongoDB) (Amazon DocumentDB) oferece criptografia em repouso durante a criação do cluster via, o AWS KMS que permite aos clientes criptografar bancos de dados usando a AWS ou chaves gerenciadas pelo cliente. Em uma instância de banco de dados executada com a criptografia ativada, os dados armazenados em repouso são criptografados de acordo com a orientação em vigor no momento da publicação deste whitepaper, assim como backups automatizados, réplicas de leitura e instantâneos. Como a orientação pode ser atualizada, os clientes devem continuar avaliando e determinando se a criptografia do Amazon DocumentDB satisfaz seus requisitos regulatórios e de conformidade. Para obter mais informações sobre criptografia em repouso usando o Amazon DocumentDB, consulte Criptografar dados do Amazon DocumentDB em repouso.

As conexões com o Amazon DocumentDB contendo PHI devem usar endpoints que aceitem transporte criptografado (HTTPS). Por padrão, um cluster Amazon DocumentDB recém-criado só aceita conexões seguras usando Transport Layer Security (TLS). Para obter mais informações, consulte Criptografar dados em trânsito. O Amazon DocumentDB usa AWS CloudTrail para registrar todas as chamadas de API. Para obter mais informações, consulte Registro e monitoramento no Amazon DocumentDB.

Para determinados atributos de gerenciamento, o Amazon DocumentDB usa a tecnologia operacional que é compartilhada com o Amazon RDS. As chamadas do console do Amazon DocumentDB, da AWS CLI e da API são registradas como chamadas feitas para a API do Amazon RDS.

Amazon DynamoDB

As conexões com o Amazon DynamoDB contendo PHI devem usar endpoints que aceitem transporte criptografado (HTTPS). Para obter uma lista de endpoints regionais, consulte os endpoints de serviços da AWS.

O Amazon DynamoDB oferece criptografia do DynamoDB, que permite aos clientes criptografar bancos de dados usando chaves que os clientes gerenciam. AWS KMS Em uma instância de banco de dados executada com a criptografia do Amazon DynamoDB, os dados armazenados em repouso no armazenamento subjacente são criptografados de acordo com a orientação em vigor no momento da publicação deste whitepaper, assim como backups automatizados, réplicas de leitura e snapshots.

Como a orientação pode ser atualizada, os clientes devem continuar avaliando e determinando se a criptografia do Amazon DynamoDB satisfaz seus requisitos regulatórios e de conformidade. Para obter mais informações sobre criptografia em repouso usando o Amazon DynamoDB, consulte DynamoDB Encryption at Rest.

Amazon Elastic Block Store

A criptografia em repouso do Amazon EBS é consistente com a orientação em vigor no momento da publicação deste whitepaper. Como a orientação pode ser atualizada, os clientes devem continuar avaliando e determinando se a criptografia do Amazon EBS satisfaz seus requisitos regulatórios e de conformidade. Com a criptografia do Amazon EBS, uma chave de criptografia de volume exclusiva é gerada para cada volume do EBS. Os clientes têm a flexibilidade de escolher qual chave KMS AWS Key Management Service é usada para criptografar cada chave de volume. Para obter mais informações, consulte Criptografia do Amazon EBS.

Amazon Elastic Compute Cloud

O Amazon EC2 é um serviço computacional escalável e configurável pelo usuário que oferece suporte a vários métodos para criptografar dados em repouso. Por exemplo, os clientes podem optar

por realizar a criptografia em nível de aplicativo ou campo da PHI à medida que ela é processada em uma plataforma de aplicativo ou banco de dados hospedada em uma instância do Amazon EC2. As abordagens vão desde a criptografia de dados usando bibliotecas padrão em uma estrutura de aplicativo, como Java ou .NET; a utilização de recursos de criptografia transparente de dados no Microsoft SQL ou Oracle; ou a integração de outras soluções de terceiros e baseadas em software como serviço (SaaS) em seus aplicativos.

Os clientes podem optar por integrar seus aplicativos executados no Amazon EC2 com AWS KMS SDKs, simplificando o processo de gerenciamento e armazenamento de chaves. Os clientes também podem implementar a criptografia de dados em repouso usando criptografia em nível de arquivo ou de disco inteiro (FDE) usando software de terceiros de AWS Marketplace parceiros ou ferramentas nativas de criptografia de sistemas de arquivos (como dm-crypt, LUKS etc.).

O tráfego de rede contendo PHI deve criptografar os dados em trânsito. Para tráfego entre fontes externas (como a Internet ou um ambiente de TI tradicional) e o Amazon EC2, os clientes devem usar mecanismos de criptografia de transporte de padrão aberto, como Transport Layer Security (TLS) ou redes privadas virtuais (VPNs) IPsec, consistentes com a orientação. Interno de uma Amazon Virtual Private Cloud (VPC) para dados que trafegam entre instâncias do Amazon EC2, o tráfego de rede contendo PHI também deve ser criptografado; a maioria dos aplicativos suporta TLS ou outros protocolos que fornecem criptografia em trânsito que pode ser configurada para ser consistente com a orientação. Para aplicativos e protocolos que não oferecem suporte à criptografia, as sessões que transmitem PHI podem ser enviadas por meio de túneis criptografados usando IPsec ou implementações similares entre instâncias.

Amazon Elastic Container Registry

O Amazon Elastic Container Registry (Amazon ECR) é integrado ao Amazon Elastic Container Service (Amazon ECS) e permite que os clientes armazenem, executem e gerenciem facilmente imagens de contêineres para aplicativos executados no Amazon ECS. Depois que os clientes especificarem o repositório do Amazon ECR em sua definição de tarefas, o Amazon ECS recuperará as imagens apropriadas para seus aplicativos.

Nenhuma etapa especial é necessária para usar o Amazon ECR com imagens de contêiner que contenham PHI. As imagens do contêiner são criptografadas enquanto estão em trânsito e armazenadas criptografadas enquanto estão em repouso usando a criptografia do lado do servidor do Amazon S3 (SSE-S3).

Amazon Elastic Container Service

O Amazon Elastic Container Service (Amazon ECS) é um serviço de gerenciamento de contêineres altamente escalável e de alto desempenho que oferece suporte a contêineres Docker e permite que os clientes executem facilmente aplicativos em um cluster gerenciado de instâncias do Amazon EC2. O Amazon ECS elimina a necessidade de os clientes instalarem, operarem e escalarem sua própria infraestrutura de gerenciamento de clusters.

Com chamadas de API simples, os clientes podem iniciar e interromper aplicativos habilitados para Docker, consultar o estado completo do cluster e acessar muitos recursos conhecidos, como grupos de segurança, Elastic Load Balancing, volumes do EBS e funções do IAM. Os clientes podem usar o Amazon ECS para programar a colocação de contêineres em seu cluster com base em suas necessidades de recursos e requisitos de disponibilidade.

O uso do ECS com cargas de trabalho que processam PHI não requer configuração adicional. O ECS atua como um serviço de orquestração que coordena o lançamento de contêineres (imagens armazenadas no S3) no EC2 e não opera com ou sobre dados dentro da carga de trabalho que está sendo orquestrada. Consistente com os regulamentos da HIPAA e com o Adendo de Associado AWS Comercial, as PHI devem ser criptografadas em trânsito e em repouso quando acessadas por contêineres lançados com o ECS. Vários mecanismos para criptografia em repouso estão disponíveis com cada opção AWS de armazenamento (por exemplo, S3, EBS e KMS). Garantir a criptografia completa das PHI enviadas entre contêineres também pode levar os clientes a implantar uma rede de sobreposição (como VNS3, Weave Net ou similar), a fim de fornecer uma camada redundante de criptografia. No entanto, o registro completo também deve ser ativado (por exemplo, por meio de CloudTrail), e todos os registros de instâncias do contêiner devem ser direcionados para CloudWatch.

O uso do Firelens e AWS do Fluent Bit com cargas de trabalho que processam PHI não requer configuração adicional, a menos que os registros contenham PHI. Se os registros contiverem PHI, eles não devem ser emitidos para arquivos de log, a menos que a criptografia de disco esteja ativada. Em vez disso, configure seu aplicativo para emitir registros de saída/erro padrão, que serão coletados automaticamente pelo. FireLens Da mesma forma, não ative o buffer de arquivos para o Fluent Bit, a menos que a criptografia de disco também esteja ativada. Por fim, o destino do log deve ser compatível encryption-in-transit; todos os plug-ins de saída de AWS serviços no AWS para Fluent Bit sempre usarão criptografia TLS para exportar registros.

Amazon Elastic File System (Amazon EFS)

O Amazon Elastic File System (Amazon EFS) fornece armazenamento de arquivos simples, escalável e elástico para uso com serviços AWS em nuvem e recursos locais. É fácil de usar e oferece uma interface simples que permite aos clientes criar e configurar sistemas de arquivos com rapidez e facilidade. O Amazon EFS foi criado para escalar elasticamente sob demanda sem interromper os aplicativos, crescendo e diminuindo automaticamente à medida que os clientes adicionam e removem arquivos.

Para satisfazer a exigência de que a PHI seja criptografada em repouso, dois caminhos estão disponíveis no EFS. O EFS oferece suporte à criptografia em repouso quando um novo sistema de arquivos é criado. Durante a criação, a opção “Ativar criptografia de dados em repouso” deve ser selecionada. Selecionar essa opção garante que todos os dados colocados no sistema de arquivos EFS sejam criptografados usando criptografia AES-256 e AWS KMS chaves gerenciadas. Como alternativa, os clientes podem optar por criptografar os dados antes que eles sejam colocados no EFS, mas eles são responsáveis por gerenciar o processo de criptografia e o gerenciamento de chaves.

O PHI não deve ser usado como todo ou parte de qualquer nome de arquivo ou nome de pasta. A criptografia de PHI em trânsito para o Amazon EFS é fornecida pelo Transport Layer Security (TLS) entre o serviço EFS e a instância que monta o sistema de arquivos. O EFS oferece um auxiliar de montagem para facilitar a conexão a um sistema de arquivos usando TLS. Por padrão, o TLS não é usado e deve ser habilitado ao montar o sistema de arquivos usando o auxiliar de montagem do EFS. Certifique-se de que o comando mount contenha a opção “-o tls” para ativar a criptografia TLS. Como alternativa, os clientes que optarem por não usar o auxiliar de montagem do EFS podem seguir as instruções na documentação do EFS para configurar seus clientes NFS para se conectarem por meio de um túnel TLS.

Amazon Elastic Kubernetes Service (Amazon EKS)

O Amazon Elastic Kubernetes Service (Amazon EKS) é um serviço gerenciado que facilita aos clientes a execução do Kubernetes na AWS sem precisar instalar ou manter seu próprio plano de controle do Kubernetes. O Kubernetes é um sistema de código aberto para automatizar a implantação, a escalabilidade e o gerenciamento de aplicações em contêineres. Para obter informações adicionais sobre segurança e conformidade, consulte o whitepaper Architecting for HIPAA Security and Compliance on Amazon EKS.

Amazon ElastiCache para Redis

O Amazon ElastiCache for Redis é um serviço de estrutura de dados em memória compatível com o Redis que pode ser usado como armazenamento de dados ou cache. Para armazenar PHI, os clientes devem garantir que estejam executando a versão mais recente do mecanismo Redis qualificada ElastiCache para a HIPAA e os tipos de nós da geração atual. O Amazon ElastiCache for Redis oferece suporte ao armazenamento de PHI para os seguintes tipos de nós e versões do mecanismo Redis:

- Tipos de nós: somente na geração atual (por exemplo, no momento da publicação deste whitepaper, M4, M5, R4, R5, T2, T3)
- ElastiCache para a versão do motor Redis: 3.2.6 e 4.0.10 em diante

Para obter mais informações sobre como escolher os nós da geração atual, consulte os ElastiCache preços da Amazon. Para obter mais informações sobre como escolher um mecanismo ElastiCache para Redis, consulte O que é o Amazon ElastiCache for Redis?

Os clientes também devem garantir que o cluster e os nós dentro do cluster estejam configurados para criptografar dados em repouso, habilitar a criptografia de transporte e habilitar a autenticação de comandos do Redis. Além disso, os clientes também devem garantir que seus clusters Redis sejam atualizados com as atualizações mais recentes do serviço do tipo “Segurança” em ou antes da “Data de aplicação recomendada” (a data em que é recomendável que a atualização seja aplicada) em todos os momentos. Para obter mais informações, consulte as seções abaixo.

Tópicos

Criptografia em repouso

O Amazon ElastiCache for Redis fornece criptografia de dados para seu cluster para ajudar a proteger os dados em repouso. Quando os clientes habilitam a criptografia em repouso para um cluster no momento da criação, o Amazon ElastiCache for Redis criptografa os dados em disco e os backups automatizados do Redis. Os dados do cliente em disco são criptografados usando chaves

simétricas do Advanced Encryption Standard (AES) -512 aceleradas por hardware. Os backups do Redis são criptografados por meio de chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3). Um bucket S3 com criptografia do lado do servidor ativada criptografará os dados usando chaves simétricas Advanced Encryption Standard (AES) -256 aceleradas por hardware antes de salvá-los no bucket.

Para obter mais detalhes sobre as chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3), consulte Proteção de dados usando criptografia do lado do servidor com chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3). Em um cluster ElastiCache Redis (de um ou vários nós) executado com criptografia, os dados armazenados em repouso são criptografados de acordo com a orientação em vigor no momento da publicação deste whitepaper. Isso inclui dados em disco e backups automatizados no bucket do S3. Como a orientação pode ser atualizada, os clientes devem continuar avaliando e determinando se a criptografia do Amazon ElastiCache for Redis satisfaz seus requisitos regulatórios e de conformidade. Para obter mais informações sobre criptografia em repouso usando o Amazon ElastiCache for Redis, consulte O que é o Amazon ElastiCache for Redis?

Criptografia de transporte

O Amazon ElastiCache for Redis usa TLS para criptografar os dados em trânsito. As conexões ElastiCache para o Redis contendo PHI devem usar criptografia de transporte e avaliar a consistência da configuração com o Guidance. Para obter mais informações, consulte CreateReplicationGroup. Para obter mais informações sobre como habilitar a criptografia de transporte, consulte ElastiCache Redis In-Transit Encryption (TLS).

Autenticação

Os clusters Amazon ElastiCache for Redis (de um ou vários nós) que contêm PHI devem fornecer um token Redis AUTH para permitir a autenticação dos comandos do Redis. O Redis AUTH está disponível quando a criptografia em repouso e a criptografia em trânsito estão habilitadas. Os clientes devem fornecer um token forte para o Redis AUTH com as seguintes restrições:

- Devem conter somente caracteres ASCII imprimíveis
- Deve ter pelo menos 16 caracteres e não mais que 128 caracteres
- Não pode conter nenhum dos seguintes caracteres: '/', "" ou “@”

Esse token deve ser definido a partir do Parâmetro de Solicitação no momento da criação do grupo de replicação do Redis (um ou vários nós) e pode ser atualizado posteriormente com um novo valor.

A AWS criptografa esse token usando AWS Key Management Service (AWS KMS). Para obter mais informações sobre o Redis AUTH, consulte ElastiCache Redis In-Transit Encryption (TLS).

Aplicando atualizações ElastiCache de serviço

Os clusters Amazon ElastiCache for Redis (de um ou vários nós) que contêm PHI devem ser atualizados com as atualizações mais recentes do serviço do tipo “Segurança” até a “Data de inscrição recomendada”. ElastiCache oferece isso como um recurso de autoatendimento que os clientes podem usar para aplicar as atualizações a qualquer momento, sob demanda e em tempo real. Cada atualização de serviço vem com uma “Gravidade” e uma “Data de aplicação recomendada” e está disponível somente para os grupos de replicação do Redis aplicáveis.

O campo “SLA Met” no recurso de atualização do serviço indicará se a atualização foi aplicada em ou antes da opção “Aplicar por data recomendada”. Se os clientes optarem por não aplicar as atualizações aos grupos de replicação do Redis aplicáveis até a “Data de aplicação recomendada”, não ElastiCache tomarão nenhuma ação para aplicá-las. Os clientes podem usar o painel do histórico de atualizações do serviço para analisar a aplicação de atualizações em seus grupos de replicação do Redis ao longo do tempo. Para obter mais informações sobre como usar esse recurso, consulte Atualizações de autoatendimento na Amazon ElastiCache.

OpenSearch Serviço Amazon

O Amazon OpenSearch Service permite que os clientes executem um cluster OSS Elasticsearch gerenciado OpenSearch ou legado em uma Amazon Virtual Private Cloud (Amazon VPC) dedicada. Ao usar o OpenSearch Service com PHI, os clientes devem usar o Elasticsearch 6.0 OpenSearch ou posterior. Os clientes devem garantir que a PHI seja criptografada em repouso e em trânsito no Amazon Service. OpenSearch Os clientes podem usar criptografia de AWS KMS chave para criptografar dados em repouso em seus domínios OpenSearch de serviço, que só está disponível para OpenSearch o Elasticsearch 5.1 ou posterior. Para obter mais informações sobre como criptografar dados em repouso, consulte Criptografia de dados em repouso para o Amazon OpenSearch Service.

Cada domínio OpenSearch de serviço é executado em sua própria VPC. Os clientes devem habilitar a node-to-node criptografia, que está disponível em todas as OpenSearch versões e no Elasticsearch 6.0 ou posterior. Se os clientes enviarem dados para o OpenSearch Serviço via HTTPS, a node-to-node criptografia ajuda a garantir que seus dados permaneçam criptografados enquanto OpenSearch os distribuem (e redistribuem) por todo o cluster. Se os dados chegarem sem criptografia via HTTP, o OpenSearch Service criptografará os dados depois que eles chegarem ao

cluster. Portanto, qualquer PHI que entre em um cluster do Amazon OpenSearch Service deve ser enviada por HTTPS. Para obter mais informações, consulte ode-to-node Criptografia N para Amazon OpenSearch Service.

Os registros da API OpenSearch de configuração do serviço podem ser capturados em AWS CloudTrail. Para obter mais informações, consulte Monitoramento de chamadas OpenSearch de API do Amazon Service com AWS CloudTrail.

Amazon EMR

O Amazon EMR implanta e gerencia um cluster de instâncias do Amazon EC2 na conta de um cliente. Para obter informações sobre criptografia com o Amazon EMR, consulte Opções de criptografia.

Amazon EventBridge

O Amazon EventBridge (antigo Amazon CloudWatch Events) é um barramento de eventos sem servidor que permite criar aplicativos escaláveis orientados a eventos. EventBridge fornece um fluxo de dados em tempo real de fontes de eventos, como Zendesk, Datadog ou Pagerduty, e encaminha esses dados para alvos como. AWS Lambda

Por padrão, EventBridge criptografa dados usando o Advanced Encryption Standard (AES-256) de 256 bits sob uma CMK de propriedade da AWS, que ajuda a proteger os dados do cliente contra acesso não autorizado. Os clientes devem garantir que qualquer recurso da AWS que emita um evento que esteja armazenando, processando ou transmitindo PHI seja configurado de acordo com as melhores práticas.

EventBridge A Amazon está integrada AWS CloudTrail e os clientes podem ver os eventos mais recentes no CloudTrail console no histórico de eventos. Para obter mais informações, consulte EventBridge Informações em CloudTrail.

Amazon Forecast

O Amazon Forecast é um serviço totalmente gerenciado que usa aprendizado de máquina para fornecer previsões altamente precisas. Com base na mesma tecnologia de previsão de aprendizado de máquina usada pela Amazon.com. Cada interação que os clientes têm com o Amazon Forecast é protegida por criptografia. Qualquer conteúdo processado pelo Amazon Forecast é criptografado

com chaves de clientes por meio do Amazon Key Management Service e criptografado em repouso na região da AWS em que os clientes estão usando o serviço.

O Amazon Forecast é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou serviço da AWS no Amazon Forecast. CloudTrail captura todas as chamadas de API para o Amazon Forecast como eventos. As chamadas capturadas incluem chamadas do console do Amazon Forecast e chamadas de código para as operações da API Amazon Forecast. Se os clientes criarem uma trilha, eles poderão permitir a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para o Amazon Forecast. Para obter mais informações, consulte Logging Forecast API Calls with AWS CloudTrail.

Por padrão, os arquivos de log entregues pelo CloudTrail bucket são criptografados pela criptografia do lado do servidor da Amazon com chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3). Para fornecer uma camada de segurança que seja diretamente gerenciável, os clientes podem usar criptografia do lado do servidor com chaves AWS KMS gerenciadas (SSE-KMS) para seus arquivos de log. CloudTrail A ativação da criptografia no servidor criptografa os arquivos de log com o SSE-KMS, mas não os arquivos de compilação. Os arquivos de compilação são criptografados com chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3).

O AWS Forecast importa e exporta dados de/para buckets S3. Ao importar e exportar dados do Amazon S3, os clientes devem garantir que os buckets do S3 sejam configurados de forma consistente com a orientação. Para obter mais informações, consulte Conceitos básicos do .

Amazon FSx

O Amazon FSx é um serviço totalmente gerenciado que fornece sistemas de arquivos ricos em recursos e de alto desempenho. O Amazon FSx for Windows File Server fornece armazenamento de arquivos altamente confiável e escalável e pode ser acessado pelo protocolo Server Message Block (SMB). O Amazon FSx for Lustre fornece armazenamento de alto desempenho para cargas de trabalho computacionais e é desenvolvido pelo Lustre, o sistema de arquivos de alto desempenho mais popular do mundo.

O Amazon FSx oferece suporte a duas formas de criptografia para sistemas de arquivos: criptografia de dados em trânsito e criptografia em repouso. O Amazon FSx for Windows File Server também suporta o registro de todas as chamadas AWS CloudTrail de API usando.

A criptografia de dados em trânsito é suportada pelo Amazon FSx for Windows File Server em instâncias computacionais compatíveis com o protocolo SMB 3.0 ou mais recente, e pelo Amazon

FSx for Lustre em instâncias do Amazon EC2 que oferecem suporte à criptografia em trânsito. Como alternativa, os clientes podem criptografar dados antes de armazená-los no Amazon FSx, mas são responsáveis pelo processo de criptografia e pelo gerenciamento de chaves.

A criptografia de dados em repouso é ativada automaticamente ao criar um sistema de arquivos Amazon FSx, usando o algoritmo de criptografia AES-256 e chaves gerenciadas. AWS KMS Os dados e metadados são criptografados automaticamente antes de serem gravados no sistema de arquivos e automaticamente descriptografados antes de serem apresentados ao aplicativo. O PHI não deve ser usado em nenhum nome de arquivo ou pasta.

Amazon GuardDuty

GuardDuty A Amazon é um serviço gerenciado de detecção de ameaças que monitora continuamente comportamentos maliciosos ou não autorizados para ajudar os clientes a proteger suas contas e cargas de trabalho da AWS. Ele monitora atividades como chamadas de API incomuns ou implantações potencialmente não autorizadas que indicam um possível comprometimento da conta. A Amazon GuardDuty também detecta instâncias potencialmente comprometidas ou reconhecimento por atacantes.

A Amazon monitora e analisa GuardDuty continuamente as seguintes fontes de dados: registros de fluxo de VPC AWS CloudTrail , registros de eventos e registros de DNS. Ele usa feeds de inteligência de ameaças, como listas de IPs e domínios maliciosos, e aprendizado de máquina para identificar atividades inesperadas, potencialmente não autorizadas e maliciosas em um ambiente da AWS. Dessa forma, a Amazon não GuardDuty deve encontrar nenhuma PHI, pois esses dados não devem ser armazenados em nenhuma das fontes de dados baseadas na AWS listadas acima.

Amazon HealthLake

A Amazon HealthLake permite que clientes dos setores de saúde e ciências biológicas armazenem, transformem, consultem e analisem dados de saúde em escala de petabytes. Os clientes podem usar HealthLake a Amazon para transmitir, processar e armazenar PHI. Por padrão, a Amazon HealthLake criptografa dados em repouso nos armazenamentos de dados do cliente. Todos os dados e metadados do serviço são criptografados com uma chave KMS de propriedade do serviço. De acordo com as especificações da Fast Healthcare Interoperability Resources (FHIR), se um cliente excluir o recurso FHIR, ele só ficará oculto para recuperação e será retido pelo serviço para controle de versão. Quando os clientes usam a API StartFhirImportJob , a Amazon HealthLake impõe a exigência de exportar dados para um bucket criptografado do Amazon S3.

A Amazon HealthLake criptografa dados em trânsito e em repouso. Para a criptografia de dados em trânsito, você pode usar chamadas de API publicadas pela AWS para acessar HealthLake por meio da rede. Os clientes devem oferecer suporte a Transport Layer Security (TLS) 1.0 ou posterior. Exigimos TLS 1.2 e recomendamos TLS 1.3. Os clientes também devem ter suporte a conjuntos de criptografia com perfect forward secrecy (PFS) como Ephemeral Diffie-Hellman (DHE) ou Ephemeral Elliptic Curve Diffie-Hellman (ECDHE). A maioria dos sistemas modernos como Java 7 e versões posteriores oferece suporte a esses modos. Além disso, as solicitações devem ser assinadas utilizando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Como alternativa, os clientes podem usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações. Para a criptografia de dados em repouso, a Amazon HealthLake criptografa os dados nos armazenamentos de dados do cliente com uma chave AWS KMS de propriedade do cliente ou por uma chave AWS KMS de propriedade do serviço, por padrão. Todos os dados e metadados do serviço são criptografados em repouso com uma chave AWS KMS de propriedade do serviço.

A Amazon HealthLake está integrada com AWS CloudTrail. CloudTrail captura todas as chamadas de API para a Amazon HealthLake como eventos, incluindo chamadas feitas como resultado da interação com AWS Management Console a interface de linha de comando (CLI) e usando programaticamente o kit de desenvolvimento de software (SDK).

Amazon Inspector

O Amazon Inspector é um serviço automatizado de avaliação de segurança para clientes que buscam melhorar a segurança e a conformidade dos aplicativos implantados na AWS. O Amazon Inspector avalia os aplicativos automaticamente para detectar vulnerabilidades ou desvios das melhores práticas. Depois de realizar uma avaliação, o Amazon Inspector produz uma lista detalhada de descobertas de segurança priorizadas por nível de severidade. Os clientes podem executar o Amazon Inspector em instâncias do EC2 que contêm PHI. O Amazon Inspector criptografa todos os dados transmitidos pela rede, bem como todos os dados de telemetria armazenados em repouso.

Amazon Managed Service for Apache Flink

O Amazon Managed Service para Apache Flink permite que os clientes criem rapidamente um código SQL que lê, processa e armazena dados continuamente quase em tempo real. Usando consultas SQL padrão nos dados de streaming, os clientes podem criar aplicativos que transformam e fornecem insights sobre seus dados. O Managed Service for Apache Flink suporta entradas dos streams de entrega do Kinesis Data Streams e Firehose como fontes para aplicativos de análise.

Se o stream for criptografado, o Managed Service for Apache Flink acessa os dados no stream criptografado sem necessidade de configuração adicional. O Managed Service for Apache Flink não armazena dados não criptografados lidos do Kinesis Data Streams. Para obter mais informações, consulte Configuração de entrada do aplicativo.

O Managed Service for Apache Flink se integra tanto com o Amazon Logs quanto com o AWS CloudTrail Amazon CloudWatch Logs para monitoramento de aplicativos. Para obter mais informações, consulte Ferramentas de monitoramento e Trabalho com Amazon CloudWatch Logs.

Amazon Data Firehose

Quando os clientes enviam dados de seus produtores de dados para o stream de dados do Kinesis, o Amazon Kinesis Data Streams criptografa os dados usando AWS KMS uma chave antes de armazená-los em repouso. Quando o stream de entrega do Firehose lê os dados do stream do Kinesis, o Kinesis Data Streams primeiro descriptografa os dados e depois os envia para o Firehose. O Firehose armazena os dados na memória com base nas dicas de buffer especificadas pelo cliente.

Em seguida, ele entrega os dados aos destinos sem armazenar os dados não criptografados em repouso. Para obter mais informações sobre criptografia com o Firehose, consulte Proteção de dados no Amazon Data Firehose.

A AWS fornece várias ferramentas que os clientes podem usar para monitorar o Amazon Data Firehose, incluindo CloudWatch métricas da Amazon, Amazon CloudWatch Logs, Kinesis Agent e registro e histórico de APIs. Para obter mais informações, consulte Monitoramento do Amazon Data Firehose.

Amazon Kinesis Streams

O Amazon Kinesis Streams permite que os clientes criem aplicativos personalizados que processam ou analisam dados de streaming para necessidades específicas. O recurso de criptografia do lado do servidor permite que os clientes criptografem dados em repouso. Quando a criptografia do lado do servidor estiver ativada, o Kinesis Streams usará uma AWS KMS chave para criptografar os dados antes de armazená-los em discos. Para obter mais informações, consulte Proteção de dados no Amazon Kinesis Data Streams. As conexões com o Amazon S3 contendo PHI devem usar endpoints que aceitem transporte criptografado (ou seja, HTTPS). Para obter uma lista de endpoints regionais, consulte os endpoints de serviços da AWS.

Amazon Kinesis Video Streams

O Amazon Kinesis Video Streams é um serviço da AWS totalmente gerenciado que os clientes podem usar para transmitir vídeo ao vivo de dispositivos para a nuvem da AWS ou criar aplicativos para processamento de vídeo em tempo real ou análise de vídeo orientada por lotes. A criptografia do lado do servidor é um recurso do Kinesis Video Streams que criptografa automaticamente os dados em repouso usando AWS KMS uma chave (antiga CMK) especificada pelo cliente. Os dados são criptografados antes de serem gravados na camada de armazenamento de streams do Kinesis Video Streams e são descriptografados após serem recuperados do armazenamento.

O SDK do Amazon Kinesis Video Streams pode ser usado para transmitir dados de streaming de vídeo contendo PHI. Por padrão, o SDK usa TLS para criptografar quadros e fragmentos gerados pelo dispositivo de hardware no qual está instalado. O SDK não gerencia nem afeta os dados armazenados em repouso. O Amazon Kinesis Video AWS CloudTrail Streams usa para registrar todas as chamadas de API.

Amazon Lex

O Amazon Lex é um serviço da AWS para a criação de interfaces de conversa em qualquer aplicação que usa voz e texto. Com o Amazon Lex, o mesmo mecanismo de conversação que alimenta o Amazon Alexa agora está disponível para qualquer desenvolvedor, permitindo que os clientes criem chatbots sofisticados de linguagem natural em seus aplicativos novos e existentes. O Amazon Lex fornece a profunda funcionalidade e flexibilidade da compreensão da linguagem natural (NLU) e do reconhecimento automático de fala (ASR) para que os clientes possam criar experiências de usuário altamente envolventes com interações conversacionais realistas e criar novas categorias de produtos.

Lex usa o protocolo HTTPS para se comunicar tanto com clientes quanto com outros serviços da AWS. O acesso ao Lex é orientado por API, e o menor privilégio apropriado do IAM pode ser aplicado. Para obter mais informações, consulte Proteção de dados no Amazon Lex.

O monitoramento é importante para manter a confiabilidade, a disponibilidade e o desempenho dos chatbots Amazon Lex do cliente. Para monitorar a integridade dos bots do Amazon Lex, use a Amazon CloudWatch. Com CloudWatch, os clientes podem obter métricas para operações individuais do Amazon Lex ou para operações globais do Amazon Lex para suas contas. Os clientes também podem configurar CloudWatch alarmes para serem notificados quando uma ou mais métricas excederem um limite definido pelos clientes. Por exemplo, os clientes podem monitorar o número de solicitações feitas a um bot em um determinado período de tempo, visualizar a latência

das solicitações bem-sucedidas ou acionar um alarme quando os erros excederem um limite. O Lex também está integrado AWS CloudTrail para registrar as chamadas da API Lex. Para obter mais informações, consulte Monitoramento no Amazon Lex.

Amazon Managed Streaming for Apache Kafka (Amazon MSK)

O Amazon MSK fornece recursos de criptografia para dados em repouso e para dados em trânsito. Para criptografia de dados em repouso, o cluster Amazon MSK usa criptografia e AWS KMS chaves do lado do servidor do Amazon EBS para criptografar volumes de armazenamento. Para dados em trânsito, os clusters do Amazon MSK têm criptografia habilitada via TLS para comunicação entre agentes.

A configuração de criptografia é ativada quando um cluster é criado. Além disso, por padrão, a criptografia em trânsito é definida como TLS para clusters criados a partir da CLI ou do console. AWS É necessária uma configuração adicional para que os clientes se comuniquem com clusters usando criptografia TLS. Os clientes podem alterar a configuração de criptografia padrão selecionando as configurações de TLS/Texto sem formatação. Para obter mais informações, consulte Amazon MSK Encryption.

Os clientes podem monitorar o desempenho dos clusters do cliente usando o console Amazon MSK, o console da Amazon CloudWatch , ou os clientes podem acessar o JMX e hospedar métricas usando o Open Monitoring with Prometheus, uma solução de monitoramento de código aberto.

As ferramentas projetadas para ler os exportadores do Prometheus são compatíveis com o Open Monitoring, como: Datadog, Lenses, New Relic, Sumologic ou um servidor Prometheus. Para obter detalhes sobre o Open Monitoring, consulte a documentação do Amazon MSK Open Monitoring.

Observe que a versão padrão do Apache Zookeeper fornecida com o Apache Kafka não suporta criptografia. No entanto, é importante observar que as comunicações entre os corretores Apache Zookeeper e Apache Kafka são limitadas às informações do corretor, do tópico e do estado da partição. A única maneira pela qual os dados podem ser produzidos e consumidos de um cluster Amazon MSK é por meio de uma conexão privada entre seus clientes em sua VPC e o cluster Amazon MSK. O Amazon MSK não oferece suporte a endpoints públicos.

Amazon MQ

O Amazon MQ é um serviço gerenciado de agente de mensagens para o Apache ActiveMQ que facilita a configuração e a operação de agentes de mensagens na nuvem. O Amazon MQ funciona com aplicativos e serviços existentes sem a necessidade de um cliente gerenciar, operar ou manter

seu próprio sistema de mensagens. Para fornecer a criptografia de dados PHI em trânsito, os seguintes protocolos com o TLS habilitado devem ser usados para acessar os corretores:

- AMQP
- MQTT
- Acabou o MQTT WebSocket
- OpenWire
- STOMP
- STOMP over WebSocket

O Amazon MQ criptografa mensagens em repouso e em trânsito usando chaves de criptografia que ele gerencia e armazena com segurança. O Amazon MQ usa CloudTrail para registrar todas as chamadas de API.

Amazon Neptune

O Amazon Neptune é um serviço de banco de dados de grafos rápido, confiável e totalmente gerenciado que facilita a criação e a execução de aplicações que trabalham com conjuntos de dados altamente conectados. O núcleo do Amazon Neptune é um mecanismo de banco de dados gráfico de alto desempenho, criado especificamente para armazenar bilhões de relacionamentos e consultar o gráfico com latência de milissegundos. O Amazon Neptune oferece suporte às populares linguagens de consulta gráfica TinkerPop Apache Gremlin e SPARQL do W3C.

Os dados contendo PHI agora podem ser retidos em uma instância criptografada do Amazon Neptune. Uma instância criptografada do Amazon Neptune só pode ser especificada no momento da criação, escolhendo “Ativar criptografia” no console do Amazon Neptune. Todos os logs, backups e snapshots são criptografados para uma instância criptografada do Amazon Neptune. O gerenciamento de chaves para instâncias criptografadas do Amazon Neptune é fornecido por meio do. AWS KMS A criptografia dos dados em trânsito é fornecida por meio de SSL/TLS. O Amazon Neptune CloudTrail usa para registrar todas as chamadas de API.

AWS Firewall de rede

AWS O Network Firewall é um serviço gerenciado de firewall que facilita a implantação de proteções de rede essenciais para toda a sua Amazon Virtual Private Cloud (Amazon VPC). O serviço se expande automaticamente de acordo com o volume de tráfego da rede para fornecer proteções de

alta disponibilidade sem a necessidade de configurar ou manter a infraestrutura subjacente. Tanto as regras do cliente quanto os registros de acesso podem conter endereços IP do usuário final, que são criptografados tanto em repouso quanto em trânsito dentro da AWS arquitetura. Além disso, o AWS Network Firewall criptografa todos os dados em repouso e em trânsito entre os AWS serviços de componentes (Amazon S3, Amazon DynamoDB, Amazon Logs, Amazon CloudWatch EBS). O serviço criptografa automaticamente os dados sem exigir uma configuração especial.

Amazon Pinpoint

O Amazon Pinpoint oferece aos desenvolvedores uma única camada de API, suporte à CLI e suporte ao SDK do lado do cliente para ampliar os canais de comunicação do aplicativo com os usuários. Os canais elegíveis incluem: e-mail, mensagens de texto SMS, notificações push móveis e canais personalizados. O Amazon Pinpoint também fornece um sistema de análise que rastreia o comportamento do usuário do aplicativo e o engajamento do usuário. Com esse serviço, os desenvolvedores podem aprender como cada usuário prefere se envolver e personalizar a experiência do usuário para aumentar a satisfação do usuário.

O Amazon Pinpoint também ajuda os desenvolvedores a lidar com vários casos de uso de mensagens, como mensagens diretas ou transacionais, mensagens direcionadas ou de campanha e mensagens baseadas em eventos. Ao integrar e habilitar todos os canais de engajamento do usuário final por meio do Amazon Pinpoint, os desenvolvedores podem criar uma visão de 360 graus do engajamento do usuário em todos os pontos de contato com o cliente. O Amazon Pinpoint armazena dados de usuários, endpoints e eventos para que os clientes possam criar segmentos, enviar mensagens aos destinatários e capturar dados de engajamento.

O Amazon Pinpoint criptografa dados em repouso e em trânsito. Para obter mais informações, consulte as perguntas frequentes do Amazon Pinpoint. Embora o Amazon Pinpoint criptografe todos os dados em repouso e em trânsito, o canal final, como SMS ou e-mail, pode não ser criptografado, e os clientes devem configurar qualquer canal de forma consistente com seus requisitos.

Além disso, os clientes que precisam enviar PHI pelo canal SMS devem usar um código curto dedicado (números de telefone de origem de 5 e 6 dígitos) com a finalidade explícita de enviar PHI. Para obter mais informações sobre como solicitar um código curto, consulte Solicitação de códigos curtos dedicados para mensagens SMS com o Amazon Pinpoint. Os clientes também podem optar por não enviar PHI pelo canal final e, em vez disso, fornecer um mecanismo para acessar com segurança a PHI por HTTPS.

As chamadas de API para o Amazon Pinpoint podem ser capturadas usando. AWS CloudTrail As chamadas capturadas incluem aquelas do console do Amazon Pinpoint e chamadas de código

para as operações da API do Amazon Pinpoint. Se os clientes criarem uma trilha, eles poderão permitir a entrega contínua de AWS CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para o Amazon Pinpoint. Se os clientes não configurarem uma trilha, eles ainda poderão ver os eventos mais recentes usando o histórico de eventos no AWS CloudTrail console. Usando as informações coletadas por AWS CloudTrail, os clientes podem determinar se a solicitação foi feita ao Amazon Pinpoint, o endereço IP da solicitação, quem fez a solicitação, quando a solicitação foi feita e detalhes adicionais. Para obter mais informações, consulte Registrar chamadas de API do Amazon Pinpoint com. AWS CloudTrail

Amazon Polly

O Amazon Polly é um serviço na nuvem que converte texto em fala realista. O Amazon Polly fornece operações de API simples que os clientes podem integrar facilmente aos aplicativos existentes. O Amazon Polly usa o protocolo HTTPS para se comunicar com os clientes. O acesso ao Amazon Polly é orientado por API, e o privilégio mínimo apropriado do IAM pode ser aplicado. Para obter mais informações, consulte Proteção de dados. Alguns exemplos de casos de uso que incluem PHI:

- O cuidador converte um relatório de texto contendo PHI em fala sintetizada para que possa ouvir o relatório enquanto caminha ou realiza outras tarefas.
- O paciente com deficiência visual recebe orientação médica e consome a orientação na forma de fala sintetizada.

O canal de entrega final do Amazon Polly pode resultar na reprodução de áudio com PHI em um espaço público, e deve-se tomar precauções para que a entrega leve isso em consideração. A saída de fala sintetizada também pode ser enviada de forma assíncrona para um bucket do Amazon S3 com criptografia ativada.

Quando uma atividade de evento suportada ocorre no Amazon Polly, essa atividade é registrada em um AWS CloudTrail evento junto com outros eventos de AWS serviço no Histórico de eventos. Para um registro contínuo de eventos em uma AWS conta de cliente, incluindo eventos do Amazon Polly, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Usando as informações coletadas pelo CloudTrail, os clientes podem determinar a solicitação que foi feita à Amazon Polly, o endereço IP a partir do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Amazon Quantum Ledger Database (Amazon QLDB)

O Amazon QLDB é um banco de dados ledger totalmente gerenciado que fornece um log de transações transparente, imutável e criptograficamente verificável pertencente a uma autoridade central confiável. O Amazon QLDB rastreia toda e qualquer alteração nos dados do aplicativo e mantém um histórico completo e verificável das alterações ao longo do tempo. Os dados contendo PHI agora podem ser retidos em uma instância do QLDB. Por padrão, todos os dados do Amazon QLDB em trânsito e em repouso são criptografados. Os dados em trânsito são criptografados usando TLS e os dados em repouso são criptografados usando chaves AWS gerenciadas. Para fins de proteção de dados, recomendamos que os clientes protejam as credenciais da AWS conta e configurem contas de usuário individuais com AWS Identity and Access Management (IAM), para que cada usuário receba somente as permissões necessárias para cumprir suas tarefas. Para obter mais informações, consulte Proteção de dados no Amazon QLDB.

O Amazon QLDB é integrado AWS CloudTrail com, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no QLDB. CloudTrail captura todas as chamadas de API do plano de controle para QLDB como eventos. As chamadas capturadas incluem as chamadas do console do QLDB e as chamadas de código para as operações de API do QLDB. Se os clientes criarem uma trilha, eles poderão habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon Simple Storage Service (Amazon S3), incluindo eventos para QLDB. Se os clientes não configurarem uma trilha, eles ainda poderão ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, os clientes podem determinar a solicitação que foi feita ao QLDB, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Amazon QuickSight

QuickSight A Amazon é um serviço de análise de negócios que os clientes podem usar para criar visualizações, realizar análises ad hoc e obter rapidamente insights de negócios a partir de seus dados. A Amazon QuickSight descobre fontes de AWS dados, permite que as organizações escalem para centenas de milhares de usuários e oferece desempenho responsivo usando um mecanismo robusto em memória (SPICE).

Os clientes só podem usar a edição Enterprise da Amazon QuickSight para trabalhar com dados contendo PHI, pois ela fornece suporte para criptografia de dados armazenados em repouso no SPICE. A criptografia de dados é realizada usando chaves AWS gerenciadas.

Amazon RDS para MariaDB

O Amazon RDS for MariaDB permite que os clientes criptografem bancos de dados MariaDB usando chaves que eles gerenciam. AWS KMS Em uma instância de banco de dados executada com a criptografia do Amazon RDS, os dados armazenados em repouso no armazenamento subjacente são criptografados de acordo com a orientação em vigor no momento da publicação deste whitepaper, assim como backups automatizados, réplicas de leitura e snapshots.

Como a orientação pode ser atualizada, os clientes devem continuar avaliando e determinando se a criptografia do Amazon RDS for MariaDB satisfaz seus requisitos regulatórios e de conformidade. Para obter mais informações sobre criptografia em repouso usando o Amazon RDS, consulte Criptografando recursos do Amazon RDS.

As conexões com o RDS for MariaDB contendo PHI devem usar criptografia de transporte. Para obter mais informações sobre como habilitar conexões criptografadas, consulte Usando SSL/TLS para criptografar uma conexão com uma instância de banco de dados.

Amazon RDS para MySQL

O Amazon RDS for MySQL permite que os clientes criptografem bancos de dados MySQL usando chaves que os clientes gerenciam. AWS KMS Em uma instância de banco de dados executada com a criptografia do Amazon RDS, os dados armazenados em repouso no armazenamento subjacente são criptografados de acordo com a orientação em vigor no momento da publicação deste whitepaper, assim como backups automatizados, réplicas de leitura e snapshots.

Como a orientação pode ser atualizada, os clientes devem continuar avaliando e determinando se a criptografia do Amazon RDS for MySQL satisfaz seus requisitos regulatórios e de conformidade. Para obter mais informações sobre criptografia em repouso usando o Amazon RDS, consulte Criptografando recursos do Amazon RDS.

As conexões com o RDS para MySQL contendo PHI devem usar criptografia de transporte. Para obter mais informações sobre como habilitar conexões criptografadas, consulte Usando SSL/TLS para criptografar uma conexão com uma instância de banco de dados.

Amazon RDS para Oracle

Os clientes têm várias opções para criptografar PHI em repouso usando o Amazon RDS for Oracle. Os clientes podem criptografar bancos de dados Oracle usando chaves que eles gerenciam AWS

KMS. Em uma instância de banco de dados executada com a criptografia do Amazon RDS, os dados armazenados em repouso no armazenamento subjacente são criptografados de acordo com a orientação em vigor no momento da publicação deste whitepaper, assim como backups automatizados, réplicas de leitura e snapshots.

Como a orientação pode ser atualizada, os clientes devem continuar avaliando e determinando se a criptografia do Amazon RDS for Oracle satisfaz seus requisitos regulatórios e de conformidade. Para obter mais informações sobre criptografia em repouso usando o Amazon RDS, consulte Criptografando recursos do Amazon RDS.

Os clientes também podem usar o Oracle Transparent Data Encryption (TDE) e devem avaliar a consistência da configuração com a Orientação. O Oracle TDE é um recurso da opção Oracle Advanced Security disponível no Oracle Enterprise Edition. Esse recurso criptografa os dados automaticamente antes de gravá-los no armazenamento e os descriptografa automaticamente quando os são lidos. Os clientes também podem usar AWS CloudHSM para armazenar chaves Oracle TDE do Amazon RDS. Para obter mais informações, consulte:

- Amazon RDS for Oracle Transparent Data Encryption: Oracle Transparent Data Encryption.
- Usando AWS CloudHSM para armazenar chaves Oracle TDE do Amazon RDS: O que é o Amazon Relational Database Service (Amazon RDS)?

As conexões com o Amazon RDS for Oracle contendo PHI devem usar criptografia de transporte e avaliar a consistência da configuração com a orientação. Isso é feito usando o Oracle Native Network Encryption e habilitado no Amazon RDS for Oracle para grupos de opções. Para obter informações detalhadas, consulte Oracle Native Network Encryption.

Amazon RDS para PostgreSQL

O Amazon RDS for PostgreSQL permite que os clientes criptografem bancos de dados PostgreSQL usando chaves que os clientes gerenciam. AWS KMS Em uma instância de banco de dados executada com a criptografia do Amazon RDS, os dados armazenados em repouso no armazenamento subjacente são criptografados de acordo com a orientação em vigor no momento da publicação deste whitepaper, assim como backups automatizados, réplicas de leitura e snapshots.

Como a orientação pode ser atualizada, os clientes devem continuar avaliando e determinando se a criptografia do Amazon RDS for PostgreSQL satisfaz seus requisitos regulatórios e de conformidade. Para obter mais informações sobre criptografia em repouso usando o Amazon RDS, consulte Criptografando recursos do Amazon RDS.

As conexões com o RDS para PostgreSQL contendo PHI devem usar criptografia de transporte. Para obter mais informações sobre como habilitar conexões criptografadas, consulte Usando SSL/TLS para criptografar uma conexão com uma instância de banco de dados.

Amazon RDS para SQL Server

O RDS para SQL Server oferece suporte ao armazenamento de PHI para as seguintes combinações de versão e edição:

- 2008 R2 - Somente edição empresarial
- 2012, 2014 e 2016 - Edições Web, Standard e Enterprise

Importante: a edição SQL Server Express não é suportada e nunca deve ser usada para o armazenamento de PHI.

Para armazenar PHI, os clientes devem garantir que a instância esteja configurada para criptografar dados em repouso e habilitar a criptografia e a auditoria de transporte, conforme detalhado abaixo.

Criptografia em repouso

Os clientes podem criptografar bancos de dados do SQL Server usando chaves que eles gerenciam AWS KMS. Em uma instância de banco de dados executada com a criptografia do Amazon RDS, os dados armazenados em repouso no armazenamento subjacente são criptografados de acordo com a orientação em vigor no momento da publicação deste whitepaper, assim como backups e snapshots automatizados. Como a orientação pode ser atualizada, os clientes devem continuar avaliando e determinando se a criptografia do Amazon RDS for SQL Server satisfaz seus requisitos regulatórios e de conformidade. Para obter mais informações sobre criptografia em repouso usando o Amazon RDS, consulte Criptografando recursos do Amazon RDS.

Se os clientes usarem o SQL Server Enterprise Edition, eles poderão usar o Server Transparent Data Encryption (TDE) como alternativa. Esse recurso criptografa os dados automaticamente antes de gravá-los no armazenamento e os descriptografa automaticamente quando os são lidos. Para obter mais informações sobre o RDS for SQL Server Transparent Data Encryption, consulte Support for Transparent Data Encryption in SQL Server.

Criptografia de transporte

As conexões com o Amazon RDS for SQL Server contendo PHI devem usar a criptografia de transporte fornecida pelo SQL Server Forced SSL. O SSL forçado é habilitado de dentro do grupo de

parâmetros do Amazon RDS SQL Server. Para obter mais informações sobre RDS para SSL forçado do SQL Server, consulte Usando SSL com uma instância de banco de dados Microsoft SQL Server.

Auditoria

As instâncias do RDS para SQL Server que contêm PHI devem ter a auditoria habilitada. A auditoria é habilitada de dentro do grupo de parâmetros do Amazon RDS SQL Server. Para obter mais informações sobre a auditoria do RDS para SQL Server, consulte Compliance Program Support for Microsoft SQL Server DB Instances.

Amazon Redshift

O Amazon Redshift fornece criptografia de banco de dados para seus clusters para ajudar a proteger dados em repouso. Quando os clientes habilitam a criptografia para um cluster, o Amazon Redshift criptografa todos os dados, incluindo backups, usando chaves simétricas Advanced Encryption Standard (AES) -256 aceleradas por hardware. O Amazon Redshift usa para criptografia uma arquitetura de quatro níveis baseada em chaves. Essas chaves consistem em chaves de criptografia de dados, uma chave de banco de dados, uma chave de cluster e uma chave KMS.

A chave do cluster criptografa a chave do banco de dados do cluster do Amazon Redshift. Os clientes podem usar um AWS KMS ou um AWS CloudHSM (Módulo de Segurança de Hardware) para gerenciar a chave do cluster. A criptografia em repouso do Amazon Redshift é consistente com a orientação em vigor no momento da publicação deste whitepaper. Como a orientação pode ser atualizada, os clientes devem continuar avaliando e determinando se a criptografia do Amazon Redshift satisfaz seus requisitos regulatórios e de conformidade. Para obter mais informações, consulte Criptografia de bancos de dados no Amazon Redshift.

As conexões com o Amazon Redshift contendo PHI devem usar criptografia de transporte e os clientes devem avaliar a configuração para verificar a consistência com a orientação. Para obter mais informações, consulte Configurar as opções de segurança para conexões. O Amazon Redshift Spectrum permite que os clientes executem consultas SQL do Amazon Redshift em exabytes de dados no Amazon S3. O Redshift Spectrum é um recurso do Amazon Redshift e, portanto, também está no escopo do HIPAA BAA.

Amazon Rekognition

O Amazon Rekognition facilita a adição de análises de imagens e vídeos aos aplicativos do cliente. O cliente só precisa fornecer uma imagem ou um vídeo para a API do Amazon Rekognition, e o serviço

pode identificar objetos, pessoas, textos, cenas e atividades, bem como detectar qualquer conteúdo impróprio. O Amazon Rekognition também fornece análise facial e reconhecimento facial altamente precisos.

O Amazon Rekognition está qualificado para operar com imagens ou vídeos contendo PHI. O Amazon Rekognition opera como um serviço gerenciado e não apresenta nenhuma opção configurável para o tratamento de dados. O Amazon Rekognition só usa, divulga e mantém a PHI conforme permitido pelos termos do BAA. AWS Todos os dados são criptografados em repouso e em trânsito com o Amazon Rekognition. O Amazon AWS CloudTrail Rekognition usa para registrar todas as chamadas de API.

Amazon Route 53

O Amazon Route 53 é um serviço de DNS gerenciado que oferece aos clientes a capacidade de registrar nomes de domínio, rotear recursos de domínio de clientes com tráfego de internet e verificar a integridade desses recursos. Embora o Amazon Route 53 seja um serviço qualificado pela HIPAA, nenhuma PHI deve ser armazenada em nenhum nome de recurso ou tag no Amazon Route 53, pois não há suporte para criptografar esses dados. Em vez disso, o Amazon Route 53 pode ser usado para fornecer acesso aos recursos de domínio do cliente que transmitem ou armazenam PHI, como servidores web executados no Amazon EC2 ou armazenamento, como o Amazon S3.

Amazon S3 Glacier

O Amazon S3 Glacier criptografa automaticamente os dados em repouso usando chaves simétricas AES de 256 bits e oferece suporte à transferência segura de dados do cliente por meio de protocolos seguros. As conexões com o Amazon S3 Glacier contendo PHI devem usar endpoints que aceitem transporte criptografado (HTTPS). Para obter uma lista de endpoints regionais, consulte endpoints AWS de serviço.

Não use PHI em nomes ou metadados de arquivos e cofres porque esses dados não são criptografados usando a criptografia do lado do servidor do Amazon S3 Glacier e geralmente não são criptografados nas arquiteturas de criptografia do lado do cliente.

Amazon S3 Transfer Acceleration

O Amazon S3 Transfer Acceleration (S3TA) permite transferências rápidas, fáceis e seguras de arquivos por longas distâncias entre o cliente do cliente e um bucket do S3. O Transfer Acceleration

aproveita os pontos CloudFront de presença distribuídos globalmente da Amazon. Conforme os dados chegam em um ponto de presença, eles são roteados para o Amazon S3 por um caminho de rede otimizado. Os clientes devem garantir que todos os dados contendo PHI transferidos usando o AWS S3TA sejam criptografados em trânsito e em repouso. Consulte a orientação do Amazon S3 para entender as opções de criptografia disponíveis.

Amazon SageMaker

A Amazon SageMaker é um serviço de aprendizado de máquina totalmente gerenciado. Com a Amazon SageMaker, cientistas de dados e desenvolvedores podem criar e treinar modelos de aprendizado de máquina com rapidez e facilidade e, em seguida, implantá-los diretamente em um ambiente hospedado pronto para produção. Ele fornece uma instância integrada do notebook de criação do Jupyter para facilitar o acesso às fontes de dados para exploração e análise. A Amazon SageMaker também fornece algoritmos comuns de aprendizado de máquina que são otimizados para serem executados com eficiência em dados extremamente grandes em um ambiente distribuído.

Com suporte bring-your-own-algorithms e estruturas nativos, a Amazon SageMaker oferece opções flexíveis de treinamento distribuído que se ajustam aos fluxos de trabalho específicos do cliente. A Amazon SageMaker está qualificada para operar com dados contendo PHI. A criptografia dos dados em trânsito é fornecida por SSL/TLS e é usada na comunicação com a interface front-end da Amazon (com o Notebook) e sempre que a SageMaker SageMaker Amazon interage com qualquer AWS outro serviço (por exemplo, obtendo dados do Amazon S3).

Para satisfazer a exigência de que a PHI seja criptografada em repouso, a criptografia dos dados armazenados com a instância executando modelos com a Amazon SageMaker é habilitada usando AWS Key Management Service (KMS) ao configurar o endpoint (DescribeEndpointConfig: ID). KmsKey A criptografia dos resultados do treinamento do modelo (artefatos) é habilitada usando AWS KMS e as chaves devem ser especificadas usando o KmsKey ID na OutputDataConfig descrição. Se um ID de chave KMS não for fornecido, a chave KMS padrão do Amazon S3 para a conta da função será usada. A Amazon SageMaker usa AWS CloudTrail para registrar todas as chamadas de API.

Amazon Simple Notification Service (Amazon SNS)

Os clientes devem entender o seguinte requisito de criptografia de chave para usar o Amazon Simple Notification Service (SNS) com Protected Health Information (PHI). Os clientes devem usar o endpoint da API HTTPS que o SNS fornece em cada AWS região. O endpoint HTTPS aproveita

conexões criptografadas e protege a privacidade e a integridade dos dados enviados para ele. AWS Para ver uma lista de todos os endpoints da API HTTPS, consulte endpoints AWS de serviço.

Além disso, o Amazon SNS usa CloudTrail um serviço que captura chamadas de API feitas por ou em nome do Amazon SNS na AWS conta do cliente e entrega os arquivos de log em um bucket do Amazon S3 que eles especificam. CloudTrail captura chamadas de API feitas a partir do console do Amazon SNS ou da API do Amazon SNS. Usando as informações coletadas pelo CloudTrail, os clientes podem determinar qual solicitação foi feita ao Amazon SNS, o endereço IP de origem a partir do qual a solicitação foi feita, quem fez a solicitação e quando ela foi feita. Para obter mais informações sobre como registrar operações do SNS, consulte Registro de chamadas de API do Amazon SNS usando. CloudTrail

Amazon Simple Email Service (Amazon SES)

O Amazon Simple Email Service (Amazon SES) é um serviço de envio e recebimento de e-mails flexível e altamente escalável. Ele suporta os protocolos S/MIME e PGP para criptografar mensagens com end-to-end criptografia total, e toda a comunicação com o Amazon SES é protegida usando SSL (TLS 1.2). Os clientes têm a opção de armazenar mensagens criptografadas em repouso configurando o Amazon SES para receber e criptografar mensagens antes de armazená-las em um bucket do Amazon S3. Para obter mais informações, consulte Como o Amazon Simple Email Service (Amazon SES) AWS KMS usa para descobrir mais informações sobre a criptografia de mensagens para armazenamento. As mensagens são protegidas em trânsito para o Amazon SES por meio de um endpoint HTTPS ou de uma conexão SMTP criptografada.

Para mensagens enviadas do Amazon SES para um destinatário, o Amazon SES primeiro tentará estabelecer uma conexão segura com o servidor de e-mail receptor, mas se uma conexão segura não puder ser estabelecida, ele enviará a mensagem sem criptografia. Para exigir criptografia para entrega a um destinatário, os clientes devem criar um conjunto de configurações no Amazon SES e usá-lo AWS CLI para definir a TlsPolicy propriedade como Exigir. Para obter mais informações, consulte Amazon SES e protocolos de segurança. O Amazon SES se integra AWS CloudTrail para monitorar todas as chamadas de API. Usando as informações coletadas por AWS CloudTrail, os clientes podem determinar se a solicitação foi feita ao Amazon SES, o endereço IP da solicitação, quem fez a solicitação, quando a solicitação foi feita e detalhes adicionais. Para obter mais informações, consulte Registrar chamadas de API do Amazon SES com AWS CloudTrail. O Amazon SES também fornece métodos para monitorar atividades de envio, como envios, rejeições, taxas de rejeição, entregas, aberturas e cliques. Para obter mais informações, consulte Monitorando sua atividade de envio do Amazon SES.

Amazon Simple Queue Service (Amazon SQS)

Os clientes devem compreender os seguintes requisitos de criptografia chave para usar o Amazon SQS com PHI.

- A comunicação com a fila do Amazon SQS por meio da solicitação de consulta deve ser criptografada com HTTPS. Para obter mais informações sobre como fazer solicitações de SQS, consulte Como fazer solicitações da API Query.
- O Amazon SQS oferece suporte à criptografia do lado do servidor integrada ao AWS KMS para proteger dados em repouso. A adição da criptografia do lado do servidor permite que os clientes transmitam e recebam dados confidenciais com a maior segurança do uso de filas criptografadas. A criptografia do lado do servidor do Amazon SQS usa o Advanced Encryption Standard de 256 bits (algoritmo AES-256 GCM) para criptografar o corpo de cada mensagem. A integração com AWS KMS permite que os clientes gerenciem centralmente as chaves que protegem as mensagens do Amazon SQS junto com as chaves que protegem seus AWS outros recursos. AWS KMS registra cada uso de chaves de criptografia AWS CloudTrail para ajudar a atender às necessidades regulatórias e de conformidade. Para obter mais informações e verificar a disponibilidade do SSE na região para o Amazon SQS, consulte Encryption at Rest.
- Se a criptografia do lado do servidor não for usada, a carga útil da mensagem em si deverá ser criptografada antes de ser enviada ao SQS. Uma forma de criptografar a carga útil da mensagem é usando o Amazon SQS Extended Client junto com o cliente de criptografia Amazon S3. Para obter mais informações sobre o uso da criptografia do lado do cliente, consulte Criptografando cargas de mensagens usando o Amazon SQS Extended Client e o Amazon S3 Encryption Client.

O Amazon SQS usa CloudTrail um serviço que registra chamadas de API feitas por ou em nome do Amazon SQS na conta de um cliente e entrega os arquivos AWS de log ao bucket especificado do Amazon S3. CloudTrail captura chamadas de API feitas a partir do console do Amazon SQS ou da API do Amazon SQS. Os clientes podem usar as informações coletadas pelo CloudTrail para determinar quais solicitações são feitas ao Amazon SQS, o endereço IP de origem a partir do qual a solicitação é feita, quem fez a solicitação, quando ela é feita e assim por diante. Para obter mais informações sobre o registro de operações do SQS, consulte Registro de chamadas de API do Amazon SQS usando. AWS CloudTrail

Amazon Simple Storage Service (Amazon S3)

Os clientes têm várias opções para criptografia de dados em repouso ao usar o Amazon S3, incluindo criptografia do lado do servidor e do lado do cliente, além de vários métodos de gerenciamento de chaves. Para obter mais informações, consulte Proteção de dados usando criptografia.

As conexões com o Amazon S3 contendo PHI devem usar endpoints que aceitem transporte criptografado (HTTPS). Para obter uma lista de endpoints regionais, consulte endpoints AWS de serviço.

Não use PHI em nomes de buckets, nomes de objetos ou metadados porque esses dados não são criptografados usando a criptografia do lado do servidor S3 e geralmente não são criptografados nas arquiteturas de criptografia do lado do cliente.

Amazon Simple Workflow Service

O Amazon Simple Workflow Service (Amazon SWF) ajuda os desenvolvedores a criar, executar e escalar trabalhos em segundo plano que tenham etapas paralelas ou sequenciais. O Amazon SWF pode ser considerado um rastreador de estado totalmente gerenciado e coordenador de tarefas na nuvem.

O Amazon Simple Workflow Service é usado para orquestrar fluxos de trabalho e não é capaz de armazenar ou transmitir dados. A PHI não deve ser colocada nos metadados do Amazon SWF ou em nenhuma descrição de tarefa. O Amazon SWF usa AWS CloudTrail para registrar todas as chamadas de API.

Amazon Textract

O Amazon Textract usa tecnologias de aprendizado de máquina para extrair automaticamente texto e dados de documentos digitalizados que vão além do simples reconhecimento óptico de caracteres (OCR) para identificar, entender e extrair dados de formulários e tabelas. Por exemplo, os clientes podem usar o Amazon Textract para extrair dados automaticamente e processar formulários com informações de saúde protegidas (PHI) sem intervenção humana para atender solicitações médicas.

O Amazon Textract também pode ser usado para manter a conformidade em arquivos de documentos. Por exemplo, os clientes podem usar o Amazon Textract para extrair dados de pedidos de seguro ou prescrições médicas e reconhecer automaticamente pares de valores-chave nesses documentos para que os confidenciais possam ser editados.

O Amazon Textract oferece suporte à criptografia do lado do servidor (SSE-S3 e SSE-KMS) para documentos de entrada e criptografia TLS para dados em trânsito entre o serviço e o agente. Os clientes podem usar CloudWatch a Amazon para rastrear métricas de uso de recursos e AWS CloudTrail capturar chamadas de API para o Amazon Textract.

Amazon Transcribe

O Amazon Transcribe usa tecnologias avançadas de aprendizado de máquina para reconhecer a fala em arquivos de áudio e transcrevê-los em texto. Por exemplo, os clientes podem usar o Amazon Transcribe para converter áudio em inglês dos EUA e espanhol mexicano em texto e criar aplicativos que incorporem o conteúdo de arquivos de áudio. O Amazon Transcribe pode ser usado com dados contendo PHI. O Amazon Transcribe não retém nem armazena nenhum dado e todas as chamadas para a API são criptografadas com SSL/TLS. O Amazon Transcribe CloudTrail usa para registrar todas as chamadas de API.

Amazon Translate

O Amazon Translate usa tecnologias avançadas de aprendizado de máquina para fornecer tradução de alta qualidade sob demanda. Os clientes podem usar o Amazon Translate para traduzir documentos de texto não estruturados ou criar aplicativos que funcionem em vários idiomas. Documentos contendo PHI podem ser processados com o Amazon Translate. Nenhuma configuração adicional é necessária ao traduzir documentos que contenham PHI. A criptografia dos dados em trânsito é fornecida por SSL/TLS e nenhum dado permanece em repouso com o Amazon Translate. O Amazon Translate usa CloudTrail para registrar todas as chamadas de API.

Amazon Virtual Private Cloud

A Amazon Virtual Private Cloud (Amazon VPC) oferece um conjunto de recursos de segurança de rede bem alinhados à arquitetura de cargas de trabalho regulamentadas pela HIPAA. Recursos como listas de controle de acesso à rede sem estado e reatribuição dinâmica de instâncias em grupos de segurança com estado oferecem flexibilidade na proteção das instâncias contra acesso não autorizado à rede.

A Amazon VPC também permite que os clientes ampliem seu próprio espaço de endereço de rede AWS, além de fornecer várias maneiras de conectar seus datacenters a. AWS Os registros de fluxo da VPC fornecem uma trilha de auditoria de conexões aceitas e rejeitadas com instâncias que processam, transmitem ou armazenam PHI.

AWS Transit Gateway atua como um hub de rede e simplifica a conectividade entre Amazon VPCs e redes locais. AWS Transit Gateway também fornece recursos de emparelhamento entre regiões para outros Transit Gateways para estabelecer uma rede global usando o backbone. AWS Para obter mais informações sobre a Amazon VPC, consulte Amazon Virtual Private Cloud.

Amazon WorkDocs

Amazon WorkDocs é um serviço de armazenamento e compartilhamento de arquivos corporativos totalmente gerenciado e seguro, com fortes controles administrativos e recursos de feedback que melhoram a produtividade do usuário. Amazon WorkDocs os arquivos são criptografados em repouso usando chaves que os clientes gerenciam por meio de AWS Key Management Service (AWS KMS). Todos os dados em trânsito são criptografados usando SSL/TLS. AWS aplicativos web e móveis e clientes de sincronização de desktop transmitem arquivos diretamente para o Amazon WorkDocs uso de SSL/TLS.

Usando o Amazon WorkDocs Management Console, WorkDocs os administradores podem visualizar os registros de auditoria para rastrear a atividade do arquivo e do usuário por tempo e escolher se desejam permitir que os usuários compartilhem arquivos com outras pessoas fora da organização. Amazon WorkDocs também está integrado com CloudTrail (um serviço que captura chamadas de API feitas por ou em nome da AWS conta do Amazon WorkDocs cliente) e entrega arquivos de CloudTrail log para um bucket do Amazon S3 que os clientes especificam.

A autenticação multifator (MFA) usando um servidor RADIUS está disponível e pode fornecer aos clientes uma camada adicional de segurança durante o processo de autenticação. Os usuários fazem login inserindo seu nome de usuário e senha seguidos por um OTP (One-Time Passcode) fornecido por um token de hardware ou software.

Para obter mais informações, consulte:

- Amazon WorkDocs feature
- Registrando chamadas de Amazon WorkDocs API usando AWS CloudTrail

Os clientes não devem armazenar PHI em nomes de arquivos ou nomes de diretórios.

Amazon WorkSpaces

A Amazon WorkSpaces é uma solução D esktop-as-a -Service (DaaS) totalmente gerenciada e segura que funciona em. AWS Com a Amazon WorkSpaces, os clientes podem provisionar

facilmente desktops Microsoft Windows virtuais baseados em nuvem para seus usuários, fornecendo acesso aos documentos, aplicativos e recursos de que precisam, em qualquer lugar, a qualquer hora, de qualquer dispositivo compatível.

A Amazon WorkSpaces armazena dados em volumes do Amazon Elastic Block Store. Os clientes podem criptografar os volumes de WorkSpaces armazenamento do cliente usando chaves que os clientes gerenciam AWS Key Management Service. Quando a criptografia é ativada em um WorkSpace, tanto os dados armazenados em repouso no armazenamento subjacente quanto os backups automatizados (instantâneos do EBS) do armazenamento em disco são criptografados de acordo com a Orientação. A comunicação dos WorkSpace clientes para WorkSpace é protegida usando SSL/TLS. Para obter mais informações sobre criptografia em repouso usando a Amazon WorkSpaces, consulte WorkSpacesCriptografado.

AWS App Mesh

AWS O App Mesh é uma malha de serviços que fornece rede em nível de aplicativo para facilitar a comunicação entre seus serviços em vários tipos de infraestrutura computacional, como Amazon ECS, Amazon EKS ou Amazon EC2. O App Mesh configura os proxies Envoy para coletar e transmitir dados de observabilidade aos conjuntos de monitoramento que você configura, para lhe dar visibilidade. end-to-end Ele pode rotear o tráfego com base em políticas de roteamento e tráfego configuradas para garantir a alta disponibilidade de seus aplicativos. O tráfego entre aplicativos pode ser configurado para usar TLS. O App Mesh pode ser usado usando o AWS SDK ou o controlador App Mesh para Kubernetes. Embora AWS App Mesh seja um serviço qualificado pela HIPAA, nenhuma PHI deve ser armazenada em nenhum nome/atributo de recurso, AWS App Mesh pois não há suporte para proteger esses dados. Em vez disso, AWS App Mesh pode ser usado para monitorar, controlar e proteger recursos de domínio do cliente que transmitem ou armazenam PHI.

AWS Serviço de migração de aplicativos

AWS O Serviço de Migração de Aplicativos (AWS MGN) permite que você migre rapidamente seus servidores e aplicativos para AWS, sem alterações e com o mínimo de tempo de inatividade. AWS O MGN é o principal serviço de migração recomendado para migrações de elevador e deslocamento para o. AWS

AWS A MGN usa replicação de dados em nível de bloco para copiar discos de origem diretamente para volumes do EBS na conta do cliente — os dados nunca são transmitidos por meio de um ambiente de nuvem controlado pela AWS MGN. Por padrão, os dados replicados são criptografados

em trânsito. Os dados nos volumes do EBS do cliente são criptografados por padrão usando as chaves do próprio cliente.

AWS Auto Scaling

AWS O Auto Scaling permite que os clientes configurem o escalonamento automático para os AWS recursos que fazem parte do aplicativo do cliente em questão de minutos. Os clientes podem usar o AWS Auto Scaling para vários serviços que envolvem PHI, como Amazon DynamoDB, Amazon ECS, réplicas Aurora do Amazon RDS e instâncias do Amazon EC2 em um grupo de Auto Scaling.

AWS O Auto Scaling é um serviço de orquestração que não processa, armazena ou transmite diretamente o conteúdo do cliente; por esse motivo, os clientes podem usar esse serviço com conteúdo criptografado. O modelo de responsabilidade AWS compartilhada se aplica à proteção de dados no AWS Auto Scaling: AWS é responsável pelos procedimentos de segurança da AWS rede, enquanto o cliente é responsável por manter o controle sobre o conteúdo do cliente hospedado nessa infraestrutura. Esse conteúdo inclui as tarefas de configuração e gerenciamento de segurança dos AWS serviços que os clientes usam. Para fins de proteção de dados, recomendamos que os clientes protejam as credenciais da AWS conta e configurem contas de usuário individuais com AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho.

É altamente recomendável que os clientes nunca coloquem informações de identificação confidenciais, como números de contas de clientes, em campos de formato livre, como o campo Nome. Isso inclui quando os clientes trabalham com o AWS Auto Scaling ou outros AWS serviços usando a AWS Management Console API ou AWS os AWS CLI SDKs.

Todos os dados que os clientes inserem no AWS Auto Scaling ou em outros serviços podem ser coletados para inclusão nos registros de diagnóstico. Quando os clientes fornecem uma URL para um servidor externo, eles não devem incluir informações de credenciais na URL para validar sua solicitação para esse servidor. AWS também recomenda que os clientes protejam seus dados das seguintes maneiras:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Recomendamos o TLS 1.2 ou posterior
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções AWS de criptografia, juntamente com todos os controles de segurança padrão nos AWS serviços.

- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados pessoais armazenados no Amazon S3.

AWS Backup

AWS Backup oferece um serviço centralizado, totalmente gerenciado e baseado em políticas para proteger os dados do cliente e garantir a conformidade entre os AWS serviços para fins de continuidade de negócios. Com AWS Backup, os clientes podem configurar centralmente as políticas de proteção de dados (backup) e monitorar a atividade de backup em todos AWS os recursos do cliente, incluindo volumes do Amazon EBS, bancos de dados do Amazon Relational Database Service (Amazon RDS) (incluindo clusters Aurora), tabelas do Amazon DynamoDB, Amazon Elastic File System (Amazon EFS), sistemas de arquivos Amazon FSx e instâncias do Amazon EC2 e volumes. AWS Storage Gateway

AWS Backup criptografa os dados do cliente em trânsito e em repouso. Os backups de serviços com recursos de snapshot existentes são criptografados usando a metodologia de criptografia de snapshot do serviço de origem. Por exemplo, os snapshots do EBS são criptografados usando a chave de criptografia do volume a partir do qual o snapshot foi criado.

Os backups de AWS serviços mais novos que introduzem a funcionalidade de backup incorporada AWS Backup, como o Amazon EFS, são criptografados em trânsito e em repouso, independentemente dos serviços de origem, oferecendo aos backups dos clientes uma camada adicional de proteção. A criptografia é configurada no nível do Backup Vault. O cofre padrão é criptografado. Quando os clientes criam um novo cofre, uma chave de criptografia deve ser selecionada.

AWS Batch

AWS Batch permite que desenvolvedores, cientistas e engenheiros executem com facilidade e eficiência centenas de milhares de trabalhos de computação em lotes no AWS. AWS Batch provisiona dinamicamente a quantidade e o tipo ideais de recursos computacionais (como CPU ou instâncias otimizadas para memória) com base no volume e nos requisitos de recursos específicos dos trabalhos em lote enviados. AWS Batch planeja, agenda e executa cargas de trabalho de computação em lote em toda a gama de serviços AWS e recursos de computação.

Semelhante à orientação do Amazon ECS, a PHI não deve ser colocada diretamente na definição do trabalho, na fila de trabalhos ou nas tags para. AWS Batch Em vez disso, trabalhos agendados e executados com AWS Batch podem operar em PHI criptografada. Qualquer informação retornada

por etapas de um trabalho também não AWS Batch deve conter nenhuma PHI. Sempre que os trabalhos executados AWS Batch devem transmitir ou receber PHI, essa conexão deve ser criptografada usando HTTPS ou SSL/TLS.

AWS Certificate Manager

AWS Certificate Manager é um serviço que permite aos clientes provisionar, gerenciar e implantar com facilidade certificados SSL/TLS públicos e privados para uso com AWS serviços e seus recursos internos conectados. AWS Certificate Manager usa CloudTrail para registrar todas as chamadas de API.

Os usuários precisam de acesso programático se quiserem interagir com pessoas AWS fora do AWS Management Console. A forma de conceder acesso programático depende do tipo de usuário que está acessando AWS.

Para conceder acesso programático aos usuários, selecione uma das seguintes opções:

Qual usuário precisa de acesso programático?	Para	Por
Identificação da força de trabalho (Usuários gerenciados no Centro de Identidade do IAM)	Use credenciais temporári as para assinar solicitações programáticas para AWS SDKs ou APIs. AWS CLI AWS	Siga as instruções da interface que deseja utilizar. • Para o AWS CLI, consulte Configurando o AWS CLI para uso AWS IAM Identity Center no Guia do AWS Command Line Interface usuário. • Para AWS SDKs, ferrament as e AWS APIs, consulte a autenticação do IAM Identity Center no Guia de referência de AWS SDKs e ferramentas.
IAM	Use credenciais temporári as para assinar solicitações	Siga as instruções em Como usar credenciais temporárias

Qual usuário precisa de acesso programático?	Para	Por
	programáticas para AWS SDKs ou APIs. AWS CLI AWS	com AWS recursos no Guia do usuário do IAM.
IAM	(Não recomendado) Use credenciais de longo prazo para assinar solicitaç ões programáticas para AWS SDKs AWS CLI ou APIs. AWS	Siga as instruções da interface que deseja utilizar. • Para isso AWS CLI, consulte Autenticação usando credenciais de usuário do IAM no Guia do AWS Command Line Interface usuário. • Para AWS SDKs e ferramentas, consulte Autenticar usando credencia is de longo prazo no Guia de referência de AWS SDKs e ferramentas. • Para AWS APIs, consulte Gerenciamento de chaves de acesso para usuários do IAM no Guia do usuário do IAM.

AWS Cloud Map

O AWS Cloud Map é um serviço de descoberta de recursos na nuvem. Com o AWS Cloud Map, os clientes podem definir nomes personalizados para recursos de aplicativos, como tarefas do Amazon ECS, instâncias do Amazon EC2, buckets do Amazon S3, tabelas do Amazon DynamoDB, filas do Amazon SQS ou qualquer outro recurso na nuvem. Os clientes podem então usar esses nomes personalizados para descobrir a localização e os metadados dos recursos de nuvem de seus aplicativos usando o AWS SDK e consultas de API autenticadas. Embora o AWS Cloud Map seja um serviço qualificado pela HIPAA, nenhuma PHI deve ser armazenada em nenhum nome/atributo

de recurso no AWS Cloud Map, pois não há suporte para proteger esses dados. Em vez disso, o AWS Cloud Map pode ser usado para descobrir recursos de domínio do cliente que transmitem ou armazenam PHI.

AWS CloudFormation

AWS CloudFormation permite que os clientes criem e provisionem implantações de infraestrutura da AWS de forma previsível e repetida. Ele ajuda os clientes a aproveitar produtos da AWS, como Amazon EC2, Amazon Elastic Block Store, Amazon SNS, Elastic Load Balancing e Auto Scaling, para criar aplicativos altamente confiáveis, escaláveis e econômicos na nuvem sem se preocupar em criar e configurar a infraestrutura subjacente da AWS. AWS CloudFormation permite que os clientes usem um arquivo de modelo para criar e excluir uma coleção de recursos juntos como uma única unidade (uma pilha).

AWS CloudFormation não armazena, transmite ou processa PHI por si só. Em vez disso, ele é usado para criar e implantar arquiteturas que usam outros serviços da AWS que podem armazenar, transmitir e/ou processar PHI. Somente os serviços qualificados pela HIPAA devem ser usados com PHI. Consulte as entradas desses serviços neste Whitepaper para obter orientação sobre o uso de PHI com esses serviços. AWS CloudFormation usa AWS CloudTrail para registrar todas as chamadas de API.

AWS CloudHSM

AWS CloudHSM é um módulo de segurança de hardware (HSM) baseado em nuvem que permite que os clientes gerem e usem facilmente suas próprias chaves de criptografia na nuvem da AWS. Com o CloudHSM, os clientes podem gerenciar suas próprias chaves de criptografia usando HSMs validados pelo FIPS 140-2 de nível 3. O CloudHSM oferece aos clientes a flexibilidade de se integrarem com seus aplicativos usando APIs de padrão aberto, como as bibliotecas PKCS #11, Java Cryptography Extensions (JCE) e Microsoft CryptoNG (CNG).

O CloudHSM também está em conformidade com os padrões e permite que os clientes exportem todas as suas chaves para a maioria dos outros HSMs disponíveis comercialmente. Como AWS CloudHSM é um serviço de gerenciamento de chaves de um dispositivo de hardware, ele não consegue armazenar ou transmitir PHI. Os clientes não devem armazenar PHI em tags (metadados). Nenhuma outra orientação especial é necessária.

AWS CloudTrail

AWS CloudTrail é um serviço que permite governança, conformidade, auditoria operacional e auditoria de risco das contas da AWS. Com CloudTrail isso, os clientes podem registrar, monitorar continuamente e reter as atividades da conta relacionadas às ações em toda a infraestrutura da AWS. CloudTrail fornece o histórico de eventos de suas atividades na conta da AWS, incluindo ações realizadas por meio de SDKs da AWS AWS Management Console, ferramentas de linha de comando e outros serviços da AWS. Esse histórico de eventos simplifica a análise de segurança, o rastreamento de alterações de recursos e a solução de problemas.

AWS CloudTrail está habilitado para uso com todas as contas da AWS e pode ser usado para registro em log de auditoria, conforme exigido pelo BAA da AWS. Trilhas específicas devem ser criadas usando o CloudTrail console ou a interface de linha de comando da AWS. CloudTrail criptografa todo o tráfego em trânsito e em repouso quando uma trilha criptografada é criada. Uma trilha criptografada deve ser criada quando existe a possibilidade de registrar PHI.

Por padrão, uma trilha criptografada armazena entradas no Amazon S3 usando criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3). Se um gerenciamento adicional de chaves for desejado, ele também poderá ser configurado com chaves AWS KMS gerenciadas (SSE-KMS). Como CloudTrail é o destino final das entradas de log da AWS e, portanto, um componente essencial de qualquer arquitetura que lida com PHI, a validação da integridade do arquivo de CloudTrail log deve ser habilitada e os arquivos de CloudTrail resumo associados devem ser revisados periodicamente. Uma vez ativada, uma afirmação positiva de que os arquivos de log não foram alterados ou alterados pode ser estabelecida.

AWS CodeBuild

AWS CodeBuild é um serviço de criação totalmente gerenciado na nuvem. AWS CodeBuild compila o código-fonte, executa testes unitários e produz artefatos prontos para serem implantados. AWS CodeBuild usa uma AWS KMS chave para criptografar artefatos de saída de compilação. Uma chave KMS deve ser criada e configurada antes de criar artefatos que contenham PHI, segredos/senhas, certificados etc. AWS CloudTrail para registrar todas as chamadas de AWS CodeBuild API.

AWS CodeDeploy

AWS CodeDeploy é um serviço de implantação totalmente gerenciado que automatiza implantações de software em uma variedade de serviços computacionais, incluindo Amazon EC2,, AWS Fargate,

AWS Lambda e servidores locais. Os clientes costumam AWS CodeDeploy lançar rapidamente novos recursos de carga de trabalho em contêineres e lidar com a complexidade da atualização de aplicativos.

AWS CodeDeploy suporta criptografia do lado do servidor (SSE-S3) para artefatos de implantação e criptografia TLS para dados em trânsito entre o serviço e o agente. Os clientes podem usar o Amazon CloudWatch Events para rastrear implantações e AWS CloudTrail capturar chamadas de API para AWS CodeDeploy.

AWS CodeCommit

AWS CodeCommit é um serviço de controle de fonte gerenciado, seguro e altamente escalável que hospeda repositórios Git privados. AWS CodeCommit elimina a necessidade de os clientes gerenciarem seu próprio sistema de controle de origem ou se preocuparem com a escalabilidade de sua infraestrutura.

AWS CodeCommit criptografa todo o tráfego e as informações armazenadas em trânsito e em repouso. Por padrão, quando um repositório é criado nele AWS CodeCommit, uma chave gerenciada pela AWS é criada AWS KMS e usada somente por esse repositório para criptografar todos os dados armazenados em repouso. AWS CodeCommit usa AWS CloudTrail para registrar todas as chamadas de API.

AWS CodePipeline

AWS CodePipeline é um serviço de entrega contínua totalmente gerenciado que ajuda os clientes a automatizar os canais de lançamento para atualizações rápidas e confiáveis de aplicativos e infraestrutura. O que os clientes usam AWS CodePipeline para permitir que os pesquisadores processem automaticamente dados de ensaios clínicos, resultados de laboratório e dados genômicos são alguns exemplos de fluxo de trabalho usado pelos clientes.

AWS CodePipeline suporta criptografia do lado do servidor (SSE-S3 e SSE-KMS) para artefatos de código e criptografia TLS para dados em trânsito entre o serviço e o agente. Os clientes podem usar o Amazon CloudWatch Events para rastrear alterações no pipeline e AWS CloudTrail capturar chamadas de API para AWS CodePipeline.

AWS Config

AWS Config fornece uma visão detalhada dos recursos associados à conta da AWS de um cliente, incluindo como eles estão configurados, como estão relacionados entre si e como as configurações e seus relacionamentos mudaram ao longo do tempo.

AWS Config não pode ser usado por si só para armazenar ou transmitir PHI.

Em vez disso, ele pode ser utilizado para monitorar e avaliar arquiteturas criadas com outros serviços da AWS, incluindo arquiteturas que lidam com PHI, para ajudar a determinar se elas permanecem em conformidade com a meta de design pretendida. Arquiteturas que lidam com PHI só devem ser construídas com serviços qualificados pela HIPAA. AWS Config usa AWS CloudTrail para registrar todos os resultados.

AWS Data Exchange

O AWS Data Exchange facilita a localização, a assinatura e o uso de dados de terceiros na nuvem. Depois de assinar um produto de dados, os clientes podem usar a API AWS Data Exchange para carregar dados diretamente no Amazon S3 e depois analisá-los com uma ampla variedade de serviços de análise e aprendizado de máquina da AWS. Para provedores de dados, o AWS Data Exchange facilita o alcance de milhões de clientes da AWS que estão migrando para a nuvem, eliminando a necessidade de criar e manter uma infraestrutura para armazenamento, entrega, cobrança e titulação de dados.

O AWS Data Exchange sempre criptografa todos os produtos de dados armazenados no serviço em repouso sem exigir nenhuma configuração adicional. Essa criptografia é feita automaticamente por meio de uma chave KMS gerenciada pelo serviço. O AWS Data Exchange usa Transport Layer Security (TLS) e criptografia do lado do cliente para criptografia em trânsito. A comunicação com o AWS Data Exchange é sempre feita por HTTPS para que os dados do cliente sejam sempre criptografados em trânsito. Essa criptografia é configurada por padrão quando os clientes usam o AWS Data Exchange. Para obter mais informações, consulte Proteção de dados no AWS Data Exchange.

O AWS Data Exchange é integrado com AWS CloudTrail o. AWS CloudTrail captura todas as chamadas para as APIs do AWS Data Exchange como eventos, incluindo chamadas do console do AWS Data Exchange e de chamadas de código para as operações da API do AWS Data Exchange. Algumas ações que os clientes podem realizar são ações somente do console. Não há API correspondente no AWS SDK ou no AWS CLI. Essas são ações que dependem da AWS

Marketplace funcionalidade, como publicar ou assinar um produto. O AWS Data Exchange fornece CloudTrail registros para um subconjunto dessas ações somente para console. Para obter mais informações, consulte Registrar chamadas de API do AWS Data Exchange com AWS CloudTrail.

Observe que todas as listagens que usam o AWS Data Exchange devem seguir as diretrizes de publicação do AWS Data Exchange e as perguntas frequentes do AWS Data Exchange para AWS Marketplace provedores, que restringem determinadas categorias de dados. Para obter mais informações, consulte as perguntas frequentes do AWS Data Exchange.

AWS Database Migration Service

AWS Database Migration Service (AWS DMS) ajuda os clientes a migrar bancos de dados para a AWS com facilidade e segurança. Os clientes podem migrar seus dados de e para os bancos de dados comerciais e de código aberto mais usados, como Oracle, MySQL e PostgreSQL. O serviço é compatível com migrações homogêneas, como de Oracle para Oracle, e migrações heterogêneas, entre plataformas de banco de dados diferentes, como de Oracle para PostgreSQL ou de MySQL para Oracle.

Bancos de dados executados localmente e migrados para a nuvem com o AWS DMS podem conter dados de PHI. O AWS DMS criptografa dados enquanto estão em trânsito e quando os dados estão sendo preparados para a migração final para o banco de dados de destino na AWS. O AWS DMS criptografa o armazenamento usado por uma instância de replicação e as informações de conexão do endpoint. Para criptografar o armazenamento usado por uma instância de replicação, o AWS DMS usa uma AWS KMS chave exclusiva para a conta da AWS. Consulte a orientação do banco de dados de destino apropriado para garantir que os dados permaneçam criptografados após a conclusão da migração. O AWS DMS usa CloudTrail para registrar todas as chamadas de API.

AWS DataSync

DataSync A AWS é um serviço de transferência on-line que simplifica, automatiza e acelera a movimentação de dados entre o armazenamento local e a AWS. Os clientes podem usar DataSync a AWS para conectar suas fontes de dados ao Amazon S3 ou ao Amazon EFS. Os clientes devem garantir que o Amazon S3 e o Amazon EFS estejam configurados de forma consistente com a orientação. Por padrão, os dados do cliente são criptografados em trânsito usando o TLS 1.2. Para obter mais informações sobre criptografia e AWS DataSync, consulte os DataSyncrecursos da AWS. Os clientes podem monitorar DataSync a atividade usando AWS CloudTrail. Para obter mais informações sobre como fazer login com CloudTrail, consulte Registrar chamadas de DataSync API da AWS com AWS CloudTrail.

AWS Directory Service

AWS Directory Service para o Microsoft AD

O AWS Directory Service for Microsoft Active Directory (Enterprise Edition), também conhecido como AWS Microsoft AD, permite que cargas de trabalho com reconhecimento de diretório e recursos da AWS usem o Active Directory gerenciado na nuvem da AWS. O AWS Microsoft AD armazena o conteúdo do diretório (incluindo conteúdo contendo PHI) em volumes criptografados do Amazon Elastic Block Store usando chaves de criptografia gerenciadas pela AWS. Para obter mais informações, consulte Criptografia do Amazon EBS.

Os dados em trânsito de e para os clientes do Active Directory são criptografados quando trafegam pelo Lightweight Directory Access Protocol (LDAP) pela rede Amazon Virtual Private Cloud (VPC) do cliente. Se um cliente do Active Directory residir em uma rede local, o tráfego viaja para a VPC do cliente por meio de um link de rede virtual privada ou um link. AWS Direct Connect

Amazon Cloud Directory

O Amazon Cloud Directory permite que os clientes criem diretórios flexíveis nativos da nuvem para organizar hierarquias de dados em várias dimensões. Os clientes também podem criar diretórios para diversos casos de uso, como organogramas, catálogos de cursos e registros de dispositivos. Por exemplo, os clientes podem criar um organograma que pode ser navegado por hierarquias separadas para estrutura de relatórios, localização e centro de custos. O Amazon Cloud Directory criptografa automaticamente os dados em repouso e em trânsito usando chaves de criptografia de 256 bits que são gerenciadas pelo AWS Key Management Service ().AWS KMS

AWS Elastic Beanstalk

Com isso AWS Elastic Beanstalk, os clientes podem implantar e gerenciar rapidamente aplicativos na nuvem da AWS sem precisar aprender sobre a infraestrutura que executa esses aplicativos. Os clientes podem simplesmente carregar o código e gerenciar AWS Elastic Beanstalk automaticamente a implantação, desde o provisionamento da capacidade, balanceamento de carga, escalabilidade automática até o monitoramento da integridade do aplicativo. Ao mesmo tempo, os clientes mantêm controle total sobre os recursos da AWS que alimentam seus aplicativos e podem acessar os recursos subjacentes a qualquer momento.

AWS Elastic Beanstalk não armazena, transmite ou processa PHI por si só. Em vez disso, os clientes podem usá-lo para criar e implantar arquiteturas com outros serviços da AWS que possam

armazenar, transmitir e/ou processar PHI. Os clientes devem garantir que, ao escolher os serviços que são implantados pela, usem apenas os serviços qualificados pela AWS Elastic Beanstalk HIPAA com PHI. Consulte as entradas desses serviços neste whitepaper para obter orientação sobre o uso de PHI com esses serviços.

Os clientes não devem incluir PHI em nenhum campo de formato livre AWS Elastic Beanstalk , como o campo Nome. AWS Elastic Beanstalk usa AWS CloudTrail para registrar todas as chamadas de API.

Recuperação elástica de desastres da AWS

O AWS Elastic Disaster Recovery (AWS DRS) minimiza o tempo de inatividade e a perda de dados com a recuperação rápida e confiável de aplicativos locais e baseados na nuvem usando armazenamento acessível, computação e recuperação mínimas. point-in-time

Os clientes podem configurar o AWS Elastic Disaster Recovery em seus servidores de origem para iniciar a replicação segura de dados. Seus dados são replicados em uma sub-rede da área de armazenamento em sua conta da AWS, na região da AWS que eles selecionarem. O design da área de armazenamento reduz os custos usando armazenamento acessível e recursos computacionais mínimos para manter a replicação contínua. Os dados do cliente replicados pelo AWS Elastic Disaster Recovery são criptografados em trânsito usando o TLS 1.2 e transferidos diretamente dos servidores de origem para a VPC. Os clientes podem aproveitar a conectividade privada, como o AWS Direct Connect ou a VPN, para configurar a rota de replicação. Os dados do cliente também podem ser criptografados em repouso na AWS usando a criptografia do Amazon EBS.

Os clientes podem realizar testes sem interrupções para confirmar que a implementação foi concluída. Durante a operação normal, mantenha a prontidão monitorando a replicação e realizando periodicamente exercícios de recuperação e failback sem interrupções. Se os clientes precisarem recuperar aplicativos, eles poderão iniciar instâncias de recuperação na AWS em minutos, usando a maior parte do estado do up-to-date servidor ou um momento anterior. Depois que os aplicativos do cliente estiverem em execução na AWS, eles poderão optar por mantê-los lá ou iniciar a replicação de dados de volta ao site principal quando o problema for resolvido. Os clientes podem retornar ao site principal sempre que estiverem prontos.

AWS Fargate

AWS Fargate é uma tecnologia que permite ao cliente executar contêineres sem precisar gerenciar servidores ou clusters. Com AWS Fargate isso, os clientes não precisam mais provisionar, configurar

e escalar clusters de máquinas virtuais para executar contêineres. Isso elimina a necessidade de escolher tipos de servidor, decidir quando escalar clusters ou otimizar o empacotamento de clusters. AWS Fargate elimina a necessidade de os clientes interagirem ou pensarem em servidores ou clusters. Com o Fargate, os clientes se concentram em projetar e criar seus aplicativos em vez de gerenciar a infraestrutura que os executa.

O Fargate não exige nenhuma configuração adicional para trabalhar com cargas de trabalho que processam PHI. Os clientes podem executar cargas de trabalho de contêineres no Fargate usando serviços de orquestração de contêineres como o Amazon ECS. O Fargate gerencia apenas a infraestrutura subjacente e não opera com ou sobre dados dentro da carga de trabalho que está sendo orquestrada. De acordo com os requisitos da HIPAA, as PHI ainda devem ser criptografadas sempre que estiverem em trânsito ou em repouso quando acessadas por contêineres lançados com o Fargate. Vários mecanismos para criptografia em repouso estão disponíveis com cada opção de armazenamento da AWS descrita neste paper. Para obter informações adicionais sobre segurança e configuração da HIPAA, consulte o whitepaper Architecting for HIPAA Security and Compliance on Amazon EKS.

AWS Firewall Manager

AWS Firewall Manager é um serviço de gerenciamento de segurança que permite aos clientes configurar e gerenciar centralmente as regras de firewall em todas as contas de clientes e aplicativos em AWS Organizations. À medida que novos aplicativos são criados, o Firewall Manager facilita a conformidade de novos aplicativos e recursos ao impor um conjunto comum de regras de segurança. Agora, os clientes têm um único serviço para criar regras de firewall, criar políticas de segurança e aplicá-las de maneira consistente e hierárquica em toda a infraestrutura, a partir de uma conta de administrador central.

AWS Firewall Manager é um serviço de orquestração que não processa, armazena ou transmite diretamente os dados do usuário. O serviço não criptografa o conteúdo do cliente, mas os serviços subjacentes que AWS Firewall Manager usa, como o DynamoDB, criptografam os dados do usuário.

AWS Global Accelerator

AWS Global Accelerator é um serviço global de balanceamento de carga que melhora a disponibilidade e a latência de aplicativos multirregionais. Para garantir que a PHI permaneça criptografada em trânsito e em repouso durante o uso AWS Global Accelerator, as arquiteturas com balanceamento de carga do Global Accelerator devem usar um protocolo criptografado, como

HTTPS ou SSL/TLS. Consulte a orientação do Amazon EC2, do Elastic Load Balancing e de outros serviços da AWS para entender melhor as opções de criptografia disponíveis para recursos de back-end. AWS Global Accelerator usa AWS CloudTrail para registrar todas as chamadas de API.

AWS Glue

AWS Glue é um serviço de ETL (extração, transformação e carregamento) totalmente gerenciado que torna simples e econômico para os clientes categorizar seus dados, limpá-los, enriquecê-los e movê-los de forma confiável entre vários armazenamentos de dados. Para garantir a criptografia de dados contendo PHI em trânsito, AWS Glue deve ser configurado para usar conexões JDBC com armazenamentos de dados com SSL/TLS. Além disso, para manter a criptografia em trânsito, a configuração da criptografia do lado do servidor (SSE-S3) deve ser passada como um parâmetro para as tarefas de ETL executadas com. AWS Glue Todos os dados armazenados em repouso no Catálogo de Dados do AWS Glue são criptografados usando chaves gerenciadas por AWS KMS quando a criptografia é ativada na criação de um objeto do Catálogo de Dados. AWS Glue usa CloudTrail para registrar todas as chamadas de API.

AWS Glue DataBrew

DataBrew O AWS Glue é um serviço visual de preparação de dados totalmente gerenciado que facilita para analistas e cientistas de dados limpar e normalizar dados para prepará-los para análise e aprendizado de máquina. Para garantir a criptografia de dados contendo PHI em trânsito, DataBrew deve ser configurado para usar conexões JDBC com armazenamentos de dados com SSL/TLS. Ao se conectar às fontes de dados do JDBC, DataBrew usa as configurações da sua conexão do AWS Glue, incluindo a opção “Exigir conexão SSL”. Além disso, para manter a criptografia em repouso nos buckets do S3, a configuração da criptografia do lado do servidor (SSE-S3 ou SSE-KMS) deve ser passada como um parâmetro para os trabalhos. DataBrew

AWS IoT Núcleo e AWS IoT Device Management

AWS IoT Faça o núcleo e AWS IoT Device Management forneça comunicação segura e bidirecional entre dispositivos conectados à Internet, como sensores, atuadores, microcontroladores incorporados ou dispositivos inteligentes, e a nuvem da AWS. AWS IoT Core e agora AWS IoT Device Management pode acomodar dispositivos que transmitem dados contendo PHI. Toda comunicação com o AWS IoT Core AWS IoT Device Management é criptografada usando TLS. AWS IoT AWS IoT Device Management Núcleo e use AWS CloudTrail para registrar todas as chamadas de API.

AWS IoT Greengrass

AWS IoT Greengrass permite que os clientes executem recursos locais de computação, mensagens, armazenamento em cache de dados, sincronização e inferência de ML para dispositivos conectados de forma segura. AWS IoT Greengrass usa certificados X.509, assinaturas gerenciadas, AWS IoT políticas e políticas e funções do IAM para garantir que os aplicativos Greengrass do cliente estejam seguros. AWS IoT Greengrass usa o modelo de segurança de AWS IoT transporte para criptografar a comunicação com a nuvem usando TLS. Além disso, AWS IoT Greengrass os dados são criptografados quando estão em repouso (na nuvem). Para obter mais informações sobre a segurança do Greengrass, consulte Visão geral da AWS IoT Greengrass segurança.

Os clientes podem registrar as ações AWS IoT Greengrass da API usando AWS CloudTrail o. Para obter mais informações, consulte Registrar chamadas de AWS IoT Greengrass API com AWS CloudTrail.

AWS Lambda

AWS Lambda permite que os clientes executem códigos sem provisionar ou gerenciar servidores sozinhos. AWS Lambda usa uma frota computacional de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em várias zonas de disponibilidade em uma região, o que fornece a alta disponibilidade, segurança, desempenho e escalabilidade da infraestrutura da AWS.

Para garantir que a PHI permaneça criptografada durante o uso AWS Lambda, as conexões com recursos externos devem usar um protocolo criptografado, como HTTPS ou SSL/TLS. Por exemplo, quando o S3 é acessado a partir de um procedimento Lambda, ele deve ser tratado com https://bucket.s3-aws-region.amazonaws.com.

Se alguma PHI for colocada em repouso ou ociosa em um procedimento em execução, ela deverá ser criptografada no lado do cliente ou no lado do servidor com as chaves obtidas de ou. AWS KMS AWS CloudHSM Siga as orientações relacionadas ao Amazon API Gateway ao acionar AWS Lambda funções por meio do serviço. Ao usar eventos de outros serviços da AWS para acionar AWS Lambda funções, os dados do evento não devem conter (por si só) PHI. Por exemplo, quando um procedimento do Lambda é acionado a partir de um evento do S3, como a chegada de um objeto no S3, o nome do objeto que é retransmitido para o Lambda não deve ter nenhuma PHI, embora o objeto em si possa conter esses dados.

AWS Managed Services

AWS Managed Services fornece gerenciamento contínuo das infraestruturas da AWS. Ao implementar as melhores práticas para manter a infraestrutura do cliente, AWS Managed Services ajuda a reduzir a sobrecarga e o risco operacionais. AWS Managed Services automatiza atividades comuns, como solicitações de mudança, monitoramento, gerenciamento de patches, segurança e serviços de backup, e fornece serviços de ciclo de vida completo para provisionar, executar e dar suporte a infraestruturas.

Os clientes podem usar AWS Managed Services para gerenciar cargas de trabalho da AWS que operam com dados contendo PHI. O uso de AWS Managed Services não altera os Serviços da AWS elegíveis para uso com PHI. As ferramentas e a automação fornecidas pela AWS Managed Services não podem ser usadas para o armazenamento ou transmissão de PHI.

AWS OpsWorks para Chef Automate

AWS OpsWorks for Chef Automate é um serviço de gerenciamento de configuração totalmente gerenciado que hospeda o Chef Automate, um conjunto de ferramentas de automação do Chef para gerenciamento de infraestrutura e aplicativos. O serviço em si não contém, transmite ou manipula nenhuma PHI ou informação confidencial, mas os clientes devem garantir que todos os recursos configurados OpsWorks pelo Chef Automate sejam configurados de acordo com a orientação. As chamadas de API são capturadas com AWS CloudTrail. Para obter mais informações, consulte Logging AWS OpsWorks Stacks API Calls with AWS CloudTrail.

AWS OpsWorks para Puppet Enterprise

AWS OpsWorks for Puppet Enterprise é um serviço de gerenciamento de configuração totalmente gerenciado que hospeda o Puppet Enterprise, um conjunto de ferramentas de automação do Puppet para gerenciamento de infraestrutura e aplicativos. O serviço em si não contém, transmite ou manipula nenhuma PHI ou informações confidenciais, mas os clientes devem garantir que qualquer recurso configurado OpsWorks pelo Puppet Enterprise seja configurado de acordo com a Orientação. As chamadas de API são capturadas com AWS CloudTrail. Para obter mais informações, consulte Logging AWS OpsWorks Stacks API Calls with AWS CloudTrail.

AWS OpsWorks Pilha

AWS OpsWorks O Stacks fornece uma maneira simples e flexível de criar e gerenciar pilhas e aplicativos. Os clientes podem usar o AWS OpsWorks Stacks para implantar e monitorar aplicativos em suas pilhas.

AWS OpsWorks O Stacks criptografa todo o tráfego em trânsito. No entanto, pacotes de dados criptografados (um mecanismo de armazenamento de dados do Chef) não estão disponíveis e quaisquer ativos que devam ser armazenados com segurança, como PHI, segredos/senhas, certificados, etc., devem ser armazenados em um bucket criptografado no Amazon S3. O AWS OpsWorks Stack usa AWS CloudTrail para registrar todas as chamadas de API.

AWS Organizations

AWS Organizations ajuda os clientes a gerenciar e governar centralmente seu ambiente à medida que crescem e escalam seus recursos da AWS. Usando AWS Organizations, eles podem criar programaticamente novas contas da AWS e alocar recursos, agrupar contas para organizar seus fluxos de trabalho, aplicar políticas a contas ou grupos para fins de governança e simplificar o faturamento usando um único método de pagamento para todas as suas contas.

Além disso, AWS Organizations é integrado a outros serviços da AWS para que os clientes possam definir configurações centrais, mecanismos de segurança, requisitos de auditoria e compartilhamento de recursos entre contas em sua organização. AWS Organizations está disponível para todos os clientes da AWS sem custo adicional.

AWS Organizations é um serviço de orquestração que não processa, armazena ou transmite diretamente os dados do usuário. O serviço não criptografa o conteúdo do cliente, mas os serviços subjacentes lançados nele criptografam AWS Organizations os dados do usuário. AWS Organizations é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, uma função ou um serviço da AWS no AWS Organizations.

AWS RoboMaker

A AWS RoboMaker permite que os clientes executem código na nuvem para desenvolvimento de aplicativos e fornece um serviço de simulação robótica para acelerar os testes de aplicativos. A AWS RoboMaker também fornece um serviço de gerenciamento de frotas de robótica para implantação, atualização e gerenciamento remotos de aplicativos.

O tráfego de rede contendo PHI deve criptografar os dados em trânsito. Toda comunicação de gerenciamento com o servidor de simulação é via TLS, e os clientes devem usar mecanismos de criptografia de transporte de padrão aberto para conexões com outros serviços da AWS. A AWS RoboMaker também se integra CloudTrail para registrar todas as chamadas de API em um bucket específico do Amazon S3.

RoboMaker Os registros da AWS não contêm PHI, e os volumes do EBS usados pelo servidor de simulação são criptografados. Ao transferir dados que possam conter PHI para outros serviços, como o Amazon S3, os clientes devem seguir as orientações do serviço de recebimento para armazenar PHI. Para implantações em robôs, os clientes devem garantir que a criptografia dos dados em trânsito e em repouso seja consistente com sua interpretação da Orientação.

Métricas do AWS SDK

Clientes corporativos podem usar o CloudWatch agente da AWS com o AWS SDK Metrics for Enterprise Support (SDK Metrics) para coletar métricas dos SDKs da AWS em seus hosts e clientes. Essas métricas são compartilhadas com o AWS Enterprise Support. O SDK Metrics pode ajudar os clientes a coletar métricas e dados de diagnóstico relevantes sobre as conexões de seus aplicativos aos serviços da AWS sem adicionar instrumentação personalizada ao código, além de reduzir o trabalho manual necessário para compartilhar registros e dados com eles. AWS Support

Observe que o SDK Metrics só está disponível para clientes da AWS com uma assinatura do Enterprise Support. Os clientes podem usar o SDK Metrics com qualquer aplicativo que chame diretamente os serviços da AWS e que tenha sido criado usando um SDK da AWS que é uma das versões listadas na documentação do AWS Metrics.

O SDK Metrics monitora as chamadas feitas pelo SDK da AWS e usa o CloudWatch agente em execução no mesmo ambiente de um aplicativo cliente.

O CloudWatch agente criptografa os dados em trânsito da máquina local até a entrega no grupo de registros de destino. O grupo de registros pode ser configurado para ser criptografado seguindo as instruções em Criptografar dados de log em CloudWatch Registros usando AWS KMS.

AWS Secrets Manager

AWS O Secrets Manager é um serviço da AWS que facilita o gerenciamento de “segredos” pelos clientes. Os segredos podem ser credenciais de banco de dados, senhas, chaves de API de terceiros e até mesmo texto arbitrário. AWS O Secrets Manager pode ser usado para armazenar PHI se essas informações estiverem contidas em “segredos”. Todos os segredos armazenados pelo AWS

Secrets Manager são criptografados em repouso usando o AWS Key Management System (KMS). Os usuários podem selecionar a AWS KMS chave usada ao criar um novo segredo. Se nenhuma chave for selecionada, a chave padrão da conta será usada. AWS O Secrets Manager usa AWS CloudTrail para registrar todas as chamadas de API.

AWS Security Hub

AWS Security Hub coleta e consolida descobertas dos serviços de segurança da AWS habilitados no ambiente de um cliente, como descobertas de detecção de intrusões da Amazon, escaneamentos de vulnerabilidade do Amazon Inspector GuardDuty, descobertas de políticas de bucket do Amazon S3 do Amazon Macie, recursos acessíveis ao público e entre contas do IAM Access Analyzer e recursos sem cobertura de WAF do. AWS Firewall Manager AWS Security Hub também consolida descobertas de soluções de segurança integradas da AWS Partner Network (APN).

AWS Security Hub se integra ao Amazon CloudWatch Events, permitindo que os clientes criem fluxos de trabalho personalizados de resposta e remediação. Os clientes podem enviar facilmente as descobertas para SIEMs, ferramentas de bate-papo, sistemas de emissão de tíquetes, ferramentas de automação e resposta de orquestração de segurança (SOAR) e plataformas de gerenciamento de plantão. As ações de resposta e remediação podem ser totalmente automatizadas ou acionadas manualmente no console. Os clientes também podem usar documentos e AWS Lambda funções de AWS Systems Manager automação para criar fluxos de trabalho de remediação automatizados que podem ser iniciados a partir de. AWS Step Functions AWS Security Hub

Para garantir a proteção dos dados, AWS Security Hub criptografa os dados em repouso e os dados em trânsito entre os serviços de componentes. Auditores terceirizados avaliam a segurança e a conformidade AWS Security Hub como parte de vários programas de conformidade da AWS. AWS Security Hub faz parte dos programas de conformidade com SOC, ISO, PCI e HIPAA da AWS.

AWS Server Migration Service

O AWS Server Migration Service (AWS SMS) automatiza a migração de máquinas virtuais locais VMware vSphere ou Microsoft Hyper-V/SCVMM para a nuvem da AWS. O AWS SMS replica incrementalmente as VMs do servidor como Amazon Machine Images (AMIs) hospedadas na nuvem, prontas para implantação no Amazon EC2.

Servidores executados localmente e migrados para a nuvem com o (AWS SMS) podem conter dados de PHI. O AWS SMS criptografa dados enquanto estão em trânsito e quando as imagens da VM do servidor estão sendo preparadas para colocação final no EC2. Consulte a orientação para EC2 e a

configuração de volumes de armazenamento criptografados ao migrar uma VM de servidor contendo PHI com o AWS SMS. O AWS SMS usa CloudTrail para registrar todas as chamadas de API.

AWS Serverless Application Repository

O AWS Serverless Application Repository (SAR) é um repositório gerenciado para aplicativos sem servidor. Ele permite que equipes, organizações e desenvolvedores individuais armazenem e compartilhem aplicativos reutilizáveis e montem e implantem facilmente arquiteturas sem servidor de novas maneiras poderosas. Os aplicativos são AWS CloudFormation modelos que contêm definições da infraestrutura do aplicativo e binários compilados do código da AWS Lambda função do aplicativo.

Embora seja possível que os aplicativos que estão no AWS Serverless Application Repository processem PHI, eles só fariam isso depois de serem implantados na conta do cliente e não como parte do próprio SAR. Ele AWS Serverless Application Repository criptografa os arquivos que os clientes carregam, incluindo pacotes de implantação e arquivos em camadas. Para dados em trânsito, o AWS Serverless Application Repository usa TLS para criptografar dados entre o serviço e o agente. AWS Serverless Application Repository está integrado com AWS CloudTrail, que é um serviço que fornece um registro das ações realizadas por um usuário, função ou serviço da AWS no AWS Serverless Application Repository.

Service Catalog

O Service Catalog permite que os administradores de TI criem, gerenciem e distribuam portfólios de produtos aprovados para usuários finais, que podem então acessar os produtos de que precisam em um portal personalizado. O Service Catalog é usado para catalogar, compartilhar e implantar soluções de autoatendimento na AWS e não pode ser usado para armazenar, transmitir ou processar PHI. A PHI não deve ser colocada em nenhum metadado para itens do Service Catalog ou em qualquer descrição do item. O Service Catalog usa AWS CloudTrail para registrar todas as chamadas de API.

AWS Shield

AWS Shield é um serviço gerenciado de proteção contra negação de serviço distribuído (DDoS) que protege aplicativos web executados na AWS. AWS Shield fornece detecção sempre ativa e mitigações automáticas em linha que minimizam o tempo de inatividade e a latência do aplicativo, portanto, não há necessidade de se engajar para se beneficiar da proteção contra DDoS. AWS Support

AWS Shield não pode ser usado para armazenar ou transmitir PHI, mas, em vez disso, pode ser usado para proteger aplicativos da web que operam com PHI. Dessa forma, nenhuma configuração especial é necessária durante o engate AWS Shield.

Todos os clientes da AWS se beneficiam das proteções automáticas do AWS Shield Standard, sem custo adicional. AWS Shield Standard defende-se contra os ataques de DDoS mais comuns e frequentes na camada de rede e transporte que têm como alvo seus sites ou aplicativos. Para obter níveis mais altos de proteção contra ataques direcionados a seus aplicativos web executados nos recursos do Elastic Load Balancing (ELB) CloudFront, Amazon e Amazon Route 53, os clientes podem se inscrever. AWS Shield Advanced

AWS Snowball

Com o AWS Snowball (Snowball), os clientes podem transferir centenas de terabytes ou petabytes de dados entre seus datacenters locais e o Amazon Simple Storage Service (Amazon S3). As PHI armazenadas AWS Snowball devem ser criptografadas em repouso, de acordo com a Orientação. Ao criar um trabalho de importação, os clientes devem especificar o ARN da AWS KMS chave a ser usada para proteger os dados no Snowball. Além disso, durante a criação do trabalho de importação, os clientes devem escolher um bucket S3 de destino que atenda aos padrões de criptografia definidos pela Orientação.

Embora o Snowball atualmente não ofereça suporte à criptografia do lado do servidor com chaves AWS KMS gerenciadas (SSE-KMS) ou criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C), o Snowball oferece suporte à criptografia do lado do servidor com chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3). Para obter mais informações, consulte Proteção de dados usando criptografia no lado do servidor com chaves de criptografia gerenciadas do Amazon S3 (SSE-S3).

Como alternativa, os clientes podem usar a metodologia de criptografia de sua escolha para criptografar a PHI antes de armazenar os dados. AWS Snowball

Atualmente, os clientes podem usar o AWS Snowball dispositivo padrão como parte do nosso BAA.

AWS Snowball Borda

AWS Snowball O Edge se conecta aos aplicativos e à infraestrutura existentes do cliente usando interfaces de armazenamento padrão, simplificando o processo de transferência de dados e

minimizando a configuração e a integração. O Snowball Edge pode se agrupar para formar um nível de armazenamento local e processar os dados do cliente no local, ajudando os clientes a garantir que seus aplicativos continuem em execução mesmo quando não conseguem acessar a nuvem.

Para garantir que a PHI permaneça criptografada ao usar o Snowball Edge, os clientes devem usar um protocolo de conexão criptografado, como HTTPS ou SSL/TLS, ao AWS Lambda usar procedimentos habilitados para transmitir PHI de/para recursos externos AWS IoT Greengrass ao Snowball Edge. Além disso, a PHI deve ser criptografada enquanto armazenada nos volumes locais do Snowball Edge, seja por meio de acesso local ou via NFS. A criptografia é aplicada automaticamente aos dados colocados no Snowball Edge usando o Snowball Management Console e a API para transporte em massa para o S3. Para obter mais informações sobre transporte de dados para o S3, consulte a orientação relacionada parathe section called “AWS Snowball”.

AWS Step Functions

AWS Step Functions facilita a coordenação dos componentes de aplicativos distribuídos e microsserviços usando fluxos de trabalho visuais. AWS Step Functions não é capaz de armazenar, transmitir ou processar PHI. A PHI não deve ser colocada nos metadados AWS Step Functions ou em nenhuma definição de máquina de estado ou tarefa. AWS Step Functions usa AWS CloudTrail para registrar todas as chamadas de API.

AWS Storage Gateway

AWS Storage Gateway é um serviço de armazenamento híbrido que permite que os aplicativos locais dos clientes usem perfeitamente o armazenamento em nuvem da AWS. O gateway usa protocolos de armazenamento de padrão aberto para conectar aplicativos e fluxos de trabalho de armazenamento existentes aos serviços de armazenamento em nuvem da AWS para minimizar a interrupção do processo.

Gateway de arquivos

O gateway de arquivos é um tipo AWS Storage Gateway que oferece suporte a uma interface de arquivos no Amazon S3 e que aumenta o volume atual baseado em blocos e o armazenamento VTL. O gateway de arquivos usa HTTPS para se comunicar com o S3 e armazena todos os objetos criptografados enquanto estiver no S3 usando SSE-S3, por padrão, ou usando criptografia do lado do cliente com chaves armazenadas. AWS KMS Os metadados do arquivo, como nomes de arquivos, permanecem não criptografados e não devem conter nenhuma PHI.

Gateway de volumes

O gateway de volume fornece volumes de armazenamento baseados em nuvem que os clientes podem montar como dispositivos iSCSI (Small Computer System Interface) da Internet a partir de servidores de aplicativos locais. Os clientes devem conectar discos locais como buffers de upload e cache à VM do Volume Gateway de acordo com seus requisitos normativos e de conformidade internos. É recomendável que, para PHI, esses discos sejam capazes de fornecer criptografia em repouso. A comunicação entre a VM do Volume Gateway e a AWS é criptografada usando o TLS 1.2 para proteger a PHI no transporte.

Gateway de fitas

O gateway de fita fornece uma interface VTL (biblioteca virtual de fitas) para aplicativos de backup de terceiros executados localmente. Os clientes devem habilitar a criptografia para PHI no aplicativo de backup de terceiros ao configurar uma tarefa de backup em fita. A comunicação entre a VM do Tape Gateway e a AWS é criptografada usando o TLS 1.2 para proteger a PHI no transporte. Os clientes que usam qualquer uma das configurações do Storage Gateway com PHI devem habilitar o registro completo. Para obter mais informações, consulte O que é o AWS Storage Gateway?

AWS Systems Manager

AWS Systems Manager é uma interface unificada que permite aos clientes centralizar facilmente os dados operacionais, automatizar tarefas em seus recursos da AWS e reduzir o tempo para detectar e resolver problemas operacionais em sua infraestrutura. O Systems Manager fornece uma visão completa do desempenho e da configuração da infraestrutura do cliente, simplifica o gerenciamento de recursos e aplicativos e facilita a operação e o gerenciamento de sua infraestrutura em grande escala.

Ao enviar dados que possam conter PHI para outros serviços, como o Amazon S3, os clientes devem seguir as orientações do serviço de recebimento para armazenar PHI. Os clientes não devem incluir PHI em metadados ou identificadores, como nomes de documentos e nomes de parâmetros.

AWS Transfer for SFTP

O AWS Transfer for SFTP fornece acesso ao Secure File Transfer Protocol (SFTP) aos recursos do S3 do cliente. Os clientes recebem um servidor virtual, que é acessado usando o protocolo SFTP padrão em um endpoint de serviço regional. Do ponto de vista do cliente da AWS e do cliente SFTP,

o gateway SFTP parece um servidor SFTP padrão e altamente disponível. Embora o serviço em si não armazene, processe ou transmita PHI, os recursos que o cliente está acessando no Amazon S3 devem ser configurados de forma consistente com a orientação. Os clientes também podem usar AWS CloudTrail para registrar as chamadas de API feitas para o AWS Transfer for SFTP.

AWS WAF — Firewall de aplicativos web

O AWS WAF é um firewall de aplicativos web que ajuda a proteger os aplicativos web dos clientes contra explorações comuns da web que podem afetar a disponibilidade dos aplicativos, comprometer a segurança ou consumir recursos excessivos. Os clientes podem colocar o AWS WAF entre seus aplicativos web hospedados na AWS que operam com ou trocam PHI e seus usuários finais. Assim como acontece com a transmissão de qualquer PHI na AWS, os dados que contêm PHI devem ser criptografados enquanto estão em trânsito. Consulte a orientação do Amazon EC2 para entender melhor as opções de criptografia disponíveis.

AWS X-Ray

AWS X-Ray é um serviço que coleta dados sobre solicitações atendidas pelo aplicativo de um cliente e fornece ferramentas que eles podem usar para visualizar, filtrar e obter informações sobre esses dados para identificar problemas e oportunidades de otimização. Para qualquer solicitação rastreada até o aplicativo de um cliente, eles podem ver informações detalhadas não apenas sobre a solicitação e a resposta, mas também sobre as chamadas que o aplicativo faz para recursos, microsserviços, bancos de dados e APIs web HTTP da AWS. AWS X-Ray não deve ser usado para armazenar ou processar PHI. As informações transmitidas de e para AWS X-Ray lá são criptografadas por padrão. Ao usar AWS X-Ray, não coloque nenhuma PHI nas anotações do segmento ou nos metadados do segmento.

Elastic Load Balancing

Os clientes podem usar o Elastic Load Balancing para encerrar e processar sessões contendo PHI. Os clientes podem escolher o Classic Load Balancer ou o Application Load Balancer. Como todo o tráfego de rede contendo PHI deve ser criptografado em trânsito end-to-end, os clientes têm a flexibilidade de implementar duas arquiteturas diferentes:

Os clientes podem encerrar HTTPS, HTTP/2 por TLS (para aplicativo) ou SSL/TLS no Elastic Load Balancing criando um balanceador de carga que usa um protocolo criptografado para conexões.

Esse recurso permite a criptografia de tráfego entre o balanceador de carga e os clientes que iniciam sessões HTTPS, HTTP/2 sobre TLS ou SSL/TLS e para conexões entre o balanceador de carga e as instâncias de back-end do cliente. As sessões contendo PHI devem criptografar os ouvintes front-end e back-end para criptografia de transporte. Os clientes devem avaliar seus certificados e políticas de negociação de sessões e mantê-los consistentes com a Orientação. Para obter mais informações, consulte HTTPS Listeners for Your Classic Load Balancer.

Como alternativa, os clientes podem configurar o Amazon ELB no modo TCP básico (para Classic) ou mais WebSockets (para Application) e passar sessões criptografadas para instâncias de back-end em que a sessão criptografada é encerrada. Nessa arquitetura, os clientes gerenciam seus próprios certificados e políticas de negociação de TLS em aplicativos executados em suas próprias instâncias. Para obter mais informações, consulte Listeners for Your Classic Load Balancer. Em ambas as arquiteturas, os clientes devem implementar um nível de registro que eles determinem ser consistente com os requisitos da HIPAA e da HITECH.

FreeRTOS

O FreeRTOS é um sistema operacional para microcontroladores que facilita a programação, implantação, proteção, conexão e gerenciamento de dispositivos de ponta pequenos e de baixo consumo de energia. O FreeRTOS é baseado no kernel do FreeRTOS, um popular sistema operacional de código aberto para microcontroladores, e o estende com bibliotecas de software que facilitam a conexão segura de dispositivos pequenos e de baixo consumo de energia aos serviços da nuvem da AWS, como o Core, ou a dispositivos de ponta mais poderosos em execução. AWS IoT AWS IoT Greengrass

Os dados contendo PHI agora podem ser criptografados em trânsito e em repouso ao usar um dispositivo qualificado executando FreeRTOS. O FreeRTOS fornece duas bibliotecas para fornecer segurança à plataforma: TLS e PKCS #11. A API TLS deve ser usada para criptografar e autenticar todo o tráfego de rede que contém PHI. O PKCS #11 fornece uma interface padrão para operações criptográficas de software e deve ser usado para criptografar qualquer PHI armazenada em um dispositivo qualificado executando FreeRTOS.

Usando AWS KMS para criptografia de PHI

As chaves KMS podem ser usadas para criptografar/descriptografar chaves de criptografia de dados usadas para criptografar PHI nos aplicativos de um cliente ou nos serviços da AWS que usam. AWS KMS AWS KMS podem ser usadas em conjunto com uma conta HIPAA, mas as PHI só podem

ser processadas, armazenadas ou transmitidas em serviços qualificados pela HIPAA. AWS KMS normalmente é usado para gerar e gerenciar chaves para aplicativos executados em outros serviços qualificados pela HIPAA.

Por exemplo, um aplicativo que processa PHI no Amazon EC2 poderia usar GenerateDataKey a chamada de API para gerar chaves de criptografia de dados para criptografar e descriptografar PHI no aplicativo. As chaves de criptografia de dados seriam protegidas pelas chaves KMS do cliente armazenadas AWS KMS, criando uma hierarquia de chaves altamente auditável à medida que as chamadas de API fossem AWS KMS registradas. AWS CloudTrail A PHI não deve ser armazenada nas tags (metadados) de nenhuma chave armazenada em. AWS KMS

VM Import/Export

O VM Import/Export permite que os clientes importem facilmente imagens de máquinas virtuais do ambiente existente para as instâncias do Amazon EC2 e as exportem de volta para seu ambiente local. Essa oferta permite que os clientes aproveitem os investimentos existentes nas máquinas virtuais que você criou para atender à segurança de TI, ao gerenciamento de configurações e aos requisitos de conformidade, trazendo essas máquinas virtuais para o Amazon ready-to-use EC2 como instâncias. Os clientes também podem exportar instâncias importadas de volta para sua infraestrutura de virtualização local, permitindo que implantem cargas de trabalho em toda a sua infraestrutura de TI.

O VM Import/Export está disponível sem custo adicional além das taxas de uso padrão para Amazon EC2 e Amazon S3.

Para importar imagens de clientes, os clientes podem usar a AWS CLI ou outras ferramentas de desenvolvedor para importar uma imagem de máquina virtual (VM) de seu ambiente VMware. Se os clientes usarem a plataforma de virtualização VMware vSphere, eles também poderão usar o AWS Management Portal for vCenter para importar sua VM. Como parte do processo de importação, o VM Import converterá a VM do cliente em uma AMI do Amazon EC2, que eles podem usar para executar instâncias do Amazon EC2. Depois que a VM for importada, eles poderão aproveitar a elasticidade, a escalabilidade e o monitoramento da Amazon por meio de ofertas como Auto Scaling, Elastic Load Balancing e dar suporte às imagens importadas. CloudWatch

Os clientes podem exportar instâncias do Amazon EC2 importadas anteriormente usando as ferramentas de API do Amazon EC2. Basta especificar a instância de destino, o formato de arquivo da máquina virtual e um bucket Amazon S3 de destino, e o VM Import/Export exportará automaticamente a instância para o bucket do Amazon S3 junto com as opções de criptografia para

proteger a transmissão e o armazenamento de suas imagens de VM. Em seguida, os clientes podem baixar e iniciar a VM exportada em sua infraestrutura de virtualização local.

Os clientes podem importar VMs Windows e Linux que usam os formatos de virtualização VMware ESX ou Workstation, Microsoft Hyper-V e Citrix Xen. E os clientes podem exportar instâncias do Amazon EC2 importadas anteriormente para os formatos VMware ESX, Microsoft Hyper-V ou Citrix Xen. Para obter uma lista completa dos sistemas operacionais, versões e formatos compatíveis, consulte Requisitos de importação/exportação da VM. A AWS planeja adicionar suporte para sistemas operacionais, versões e formatos adicionais no futuro.

Auditoria, backups e recuperação de desastres

A regra de segurança da HIPAA tem requisitos detalhados relacionados a recursos de auditoria aprofundada, procedimentos de backup de dados e mecanismos de recuperação de desastres. Os serviços na AWS contêm muitos recursos que ajudam os clientes a atender às suas necessidades. Por exemplo, os clientes devem considerar o estabelecimento de recursos de auditoria para permitir que os analistas de segurança examinem registros ou relatórios detalhados de atividades para ver quem teve acesso, entrada de endereço IP, quais dados foram acessados etc.

Esses dados devem ser rastreados, registrados e armazenados em um local central por longos períodos de tempo, no caso de uma auditoria. Usando o Amazon EC2, os clientes podem executar arquivos de registro de atividades e auditorias até a camada de pacotes em seus servidores virtuais, assim como fazem no hardware tradicional. Eles também podem rastrear qualquer tráfego IP que chegue à instância do servidor virtual. Os administradores do cliente podem fazer backup dos arquivos de log no Amazon S3 para armazenamento confiável a longo prazo.

A HIPAA também tem requisitos detalhados relacionados à manutenção de um plano de contingência para proteger os dados em caso de emergência e deve criar e manter cópias exatas recuperáveis do PHI eletrônico. Para implementar um plano de backup de dados na AWS, o Amazon EBS oferece armazenamento persistente para instâncias de servidores virtuais do Amazon EC2. Esses volumes podem ser expostos como dispositivos de bloco padrão e oferecem armazenamento fora da instância que persiste independentemente da vida útil de uma instância. Para se alinhar às diretrizes da HIPAA, os clientes podem criar point-in-time snapshots dos volumes do Amazon EBS que são armazenados automaticamente no Amazon S3 e replicados em várias zonas de disponibilidade, que são locais distintos projetados para serem isolados de falhas em outras zonas de disponibilidade.

Esses instantâneos podem ser acessados a qualquer momento e podem proteger os dados para durabilidade a longo prazo. O Amazon S3 também fornece uma solução altamente disponível para armazenamento de dados e backups automatizados. Com o simples carregamento de um arquivo ou imagem no Amazon S3, várias cópias redundantes são automaticamente criadas e armazenadas em datacenters separados. Esses arquivos podem ser acessados a qualquer momento, de qualquer lugar (com base nas permissões) e são armazenados até serem excluídos intencionalmente.

Além disso, a AWS oferece inerentemente uma variedade de mecanismos de recuperação de desastres. A recuperação de desastres, o processo de proteger os dados e a infraestrutura de TI de uma organização em tempos de desastre, envolve manter sistemas altamente disponíveis, manter os dados e o sistema replicados externamente e permitir o acesso contínuo a ambos.

Com o Amazon EC2, os administradores podem iniciar instâncias de servidor muito rapidamente e usar um endereço IP elástico (um endereço IP estático para o ambiente de computação em nuvem) para um failover fácil de uma máquina para outra. O Amazon EC2 também oferece zonas de disponibilidade. Os administradores podem iniciar instâncias do Amazon EC2 em várias zonas de disponibilidade para criar sistemas geograficamente diversos e tolerantes a falhas que sejam altamente resilientes em caso de falhas de rede, desastres naturais e a maioria das outras fontes prováveis de tempo de inatividade.

Usando o Amazon S3, os dados de um cliente são replicados e armazenados automaticamente em datacenters separados para fornecer armazenamento de dados confiável projetado para fornecer disponibilidade de 99,99%.

Usando o AWS Elastic Disaster Recovery (AWS DRS), os clientes podem recuperar rapidamente aplicativos na AWS, no up-to-date estado mais elevado dos aplicativos ou em um momento anterior.

Revisões do documento

Para ser notificado sobre atualizações desse whitepaper, inscreva-se no feed RSS.

Alteração	Descrição	Data
Atualização secundária	Atualização secundária	12 de maio de 2023
Atualização secundária	Whitepaper atualizado para expandir o conteúdo disponível nos serviços.	28 de setembro de 2022
Atualização secundária	Corrija o idioma não inclusivo.	6 de abril de 2022
Whitepaper atualizado	Informações adicionadas sobre o AWS Application Migration Service e informações atualizadas para o Amazon ECS	6 de dezembro de 2021
Whitepaper atualizado	Informações atualizadas nas seções Amazon Healthlake e Amazon VPC	9 de novembro de 2021
Whitepaper atualizado	Informações adicionadas sobre o AWS Network Firewall	9 de setembro de 2021
Whitepaper atualizado	Informações atualizadas sobre os perfis de clientes do Amazon Connect	26 de agosto de 2021
Whitepaper atualizado	Seções adicionadas Amazon AppFlow e AWS Glue DataBrew	22 de julho de 2021
Whitepaper atualizado	Navegação e organização atualizadas.	26 de abril de 2021

Whitepaper atualizado	Foram adicionadas as seguintes seções: AWS CodeDeploy, AWS CodePipeline, Amazon Aurora, Aurora PostgreSQL, Amazon Textract, Amazon Polly, Amazon FSx, AWS Auto Scaling AWS Backup,,,,,,,, VM Import/Export, Amazon, Amazon. AWS Elastic Beanstalk AWS Firewall Manager AWS Organizations AWS Security Hub AWS Serverless Application Repository HealthLake EventBridge Seção Amazon Aurora atualizada.	31 de março de 2021
Whitepaper atualizado	Seção adicionada sobre o AWS App Mesh e conteúdo atualizado do AWS System Manager	25 de agosto de 2020
Whitepaper atualizado	Foram adicionadas seções Amazon Appstream 2.0, AWS SDK Metrics, AWS Data Exchange, Amazon MSK, Amazon Pinpoint, Amazon Lex, Amazon SES e Amazon Forecast, Amazon Quantum Ledger Database (QLDB),. AWS Cloud Map	7 de maio de 2020

Whitepaper atualizado	Seções adicionadas sobre Amazon CloudWatch, Amazon CloudWatch Events, Amazon Data Firehose, Amazon Managed Service para Apache Flink, Amazon Service, OpenSearch Amazon DocumentDB (com compatibi lidade com MongoDB), AWS Mobile Hub, AWS OpsWorks Chef Automate, Puppet Enterprise, AWS AWS IoT Greengrass Transfer for SFTP, AWS, Amazon Comprehend Medical e AWS AWS. AWS OpsWorks DataSync AWS Global Accelerator RoboMaker	1º de janeiro de 2020
Whitepaper atualizado	Seções adicionadas no Amazon Comprehend, Amazon Transcribe, Amazon Translate e AWS Certificate Manager.	1º de janeiro de 2019
Whitepaper atualizado	Seções adicionadas sobre Amazon Athena, Amazon EKS, AWS IoT Core e Amazon FreeRTOS AWS IoT Device Management, Amazon, Amazon GuardDuty Neptune, AWS Server Migration Service, Amazon MQ e. AWS Database Migration Service AWS Glue	1 de novembro de 2018

Whitepaper atualizado	Seções adicionadas sobre Amazon Elastic File System (EFS), Amazon Kinesis Video Streams, Amazon Rekognition, Amazon, Amazon Simple Workflow, SageMaker AWS Secrets Manage, Service Catalog e. AWS Step Functions	1º de junho de 2018
Whitepaper atualizado	Seções adicionadas em AWS CloudFormation AWS X-Ray, AWS CloudTrail, AWS CodeBuild, AWS CodeCommit, AWS Config, e AWS OpsWorks Stack.	1 de abril de 2018
Whitepaper atualizado	Seção adicionada em AWS Fargate.	1º de janeiro de 2018

Atualizações feitas antes de 2018:

Data	Descrição
30 de novembro de 2017	Seções adicionadas sobre Amazon EC2 Container Registry, Amazon Macie, QuickSight Amazon e. AWS Managed Services
30 de novembro de 2017	Seções adicionadas na Amazon ElastiCache para Redis e Amazon CloudWatch.
Outubro de 2017	Seções adicionadas no Amazon SNS AWS Storage Gateway, Amazon Route 53 e. AWS CloudHSM Seção atualizada em AWS Key Management Service.

Data	Descrição
Setembro de 2017	Seções adicionadas sobre Amazon Connect, Amazon Kinesis Streams, Amazon RDS (Maria) DB, Amazon RDS SQL AWS Batch Server,, AWS Lambda AWS Snowball , Edge e o recurso Lambda @Edge da Amazon. CloudFront
Agosto de 2017	Seções adicionadas no Amazon EC2 Systems Manager e no Amazon Inspector.
Julho de 2017	Seções adicionadas na Amazon WorkSpaces, Amazon WorkDocs, AWS Directory Service e Amazon ECS.
Junho de 2017	Seções adicionadas na Amazon CloudFront, AWS WAF e Amazon AWS Shield S3 Transfer Acceleration.
de maio de 2017	Foi removido o requisito de instâncias dedicadas ou hosts dedicados para processam ento de PHI no EC2 e no EMR.
Março de 2017	Lista atualizada de serviços para direciona r para a página AWS Services in Scope by Compliance Program. Descrição adicionada para o Amazon API Gateway.
Janeiro de 2017	Atualizado para o modelo mais recente.
Outubro de 2016	Primeira publicação

Avisos

Os clientes são responsáveis por fazer uma avaliação independente das informações contidas neste documento. Este documento: (a) serve apenas para fins informativos, (b) representa as práticas e ofertas atuais de produtos da AWS, que estão sujeitas a alterações sem aviso prévio, e (c) não cria nenhum compromisso ou garantia por parte da AWS e de seus afiliados, fornecedores ou licenciadores. Os produtos ou serviços da AWS são fornecidos “no estado em que se encontram”, sem garantias, representações ou condições de qualquer tipo, expressas ou implícitas. As responsabilidades e as obrigações da AWS para com os clientes são controladas por contratos da AWS, e este documento não faz parte nem modifica nenhum contrato entre a AWS e seus clientes.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.