AWS 백서

# Amazon Web Services에서 HIPAA 보안 및 규정 준수를 위한 설계

# Amazon Web Services에서 HIPAA 보안 및 규정 준수를 위한 설계: AWS 백서

# Table of Contents

# Amazon Web Services에서 HIPAA 보안 및 규정 준수를 위한 설계

발행일: 2022년 9월 28일 () 문서 수정

이 백서에서는 고객이 Amazon Web Services (AWS) 를 사용하여 미국 건강 보험 이전 및 책임법 (HIPAA) 에 따라 규제되는 민감한 워크로드를 실행하는 방법을 간략하게 설명합니다. 보호 대상 건강 정보 (PHI) 보호를 위한 HIPAA 개인 정보 보호 및 보안 규칙, AWS를 사용하여 전송 중인 데이터와 저장된 데이터를 암호화하는 방법, AWS 기능을 사용하여 PHI를 포함하는 워크로드를 실행하는 방법을 중점적으로 다룹니다.

# 소개

1996년 건강보험 이전 및 책임에 관한 법률 (HIPAA) 은 “피보험 대상 단체” 및 “비즈니스 관계자”에게 적용됩니다. HIPAA는 경제 및 임상 건강을 위한 건강 정보 기술 (HITECH) 법에 의해 2009년에 확대되었습니다.

HIPAA와 HITECH는 PHI의 보안 및 개인 정보를 보호하기 위한 일련의 연방 표준을 제정합니다. HIPAA와 HITECH는 보호 대상 건강 정보 (PHI) 의 사용 및 공개, PHI 보호를 위한 적절한 보호 조치, 개인의 권리 및 행정적 책임과 관련된 요구 사항을 부과합니다. HIPAA 및 HITECH에 대한 자세한 내용은 건강 정보 프라이버시 홈을 참조하십시오.

피보험 대상 단체 및 비즈니스 관련자는 Amazon Web Services (AWS) 에서 제공하는 안전하고 확장 가능하며 저렴한 IT 구성 요소를 사용하여 HIPAA 및 HITECH 규정 준수 요구 사항에 따라 애플리케이션을 설계할 수 있습니다. AWS는 ISO 27001, FedRAMP, 서비스 조직 제어 보고서 (SOC1, SOC2, SOC3) 등 업계에서 인정하는 인증 및 감사를 갖춘 commercial-off-the-shelf 인프라 플랫폼을 제공합니다. AWS 서비스와 데이터 센터는 고객 데이터의 무결성과 안전을 보장하는 데 도움이 되는 여러 계층의 운영 및 물리적 보안을 갖추고 있습니다. 최소 요금이 없고, 기간 기반 계약이 필요하지 않으며, pay-as-you-use 요금이 부과되는 AWS는 성장하는 의료 산업 애플리케이션을 위한 안정적이고 효과적인 솔루션입니다.

AWS는 HIPAA의 적용을 받는 피보험 대상 단체 및 비즈니스 제휴사가 PHI를 안전하게 처리, 저장 및 전송할 수 있도록 지원합니다. 또한 2013년 7월부터 AWS는 이러한 고객을 위해 표준화된 비즈니스 제휴 부록 (BAA) 을 제공합니다. AWS BAA를 실행하는 고객은 HIPAA 계정으로 지정된 계정에서 모든 AWS 서비스를 사용할 수 있지만, AWS BAA에 정의된 HIPAA 적격 서비스를 사용해서만 PHI를 처리, 저장 및 전송할 수 있습니다. 이러한 서비스의 전체 목록은 HIPAA 적격 서비스 참조 페이지를 참조하십시오.

AWS는 표준 기반 위험 관리 프로그램을 유지하여 HIPAA 적격 서비스가 HIPAA 행정적, 기술적, 물리적 보호 조치를 구체적으로 지원하도록 합니다. 이러한 서비스를 사용하여 PHI를 저장, 처리 및 전송하면 고객과 AWS가 AWS 유틸리티 기반 운영 모델에 적용되는 HIPAA 요구 사항을 충족하는 데 도움이 됩니다.

AWS의 BAA에서는 고객이 HIPAA 적격 서비스에 저장되거나 전송되는 PHI를 암호화하도록 요구합니다: 보안되지 않은 보호 대상 건강 정보를 권한이 없는 개인은 사용할 수 없거나 읽을 수 없게 하거나 해독할 수 없게 만들기 위한 지침 (“지침”). 이 사이트는 업데이트될 수 있으며 HHS에서 지정한 후속 (또는 관련) 사이트에서 제공될 수 있으므로 이 사이트를 참조하십시오.

AWS는 PHI의 키 관리 및 암호화를 쉽게 관리하고 감사를 단순화할 수 있는 포괄적인 기능 및 서비스 세트를 제공합니다 AWS Key Management Service (AWS KMS). HIPAA 규정 준수 요구 사항이 있는 고객은 PHI에 대한 암호화 요구 사항을 매우 유연하게 충족할 수 있습니다.

암호화 구현 방법을 결정할 때 고객은 HIPAA 적격 서비스에 기본으로 제공되는 암호화 기능을 평가하고 활용할 수 있습니다. 또는 고객은 HHS의 지침에 따라 다른 방법을 통해 암호화 요구 사항을 충족할 수 있습니다.

# AWS에서의 PHI 암호화 및 보호

HIPAA 보안 규칙에는 전송 (“전송 중”) 및 저장 (“저장 중”) PHI 암호화에 대한 주소 지정 가능한 구현 사양이 포함되어 있습니다. 이는 HIPAA에서 적용할 수 있는 구현 사양이지만, AWS는 보건 복지부 장관 (HHS) 의 지침: 보안되지 않은 보호 대상 의료 정보를 권한이 없는 개인은 사용할 수 없거나 읽을 수 없게 만들기 위한 지침 (“지침”) 에 따라 고객이 HIPAA 적격 서비스에 저장되거나 전송되는 PHI를 암호화하도록 요구합니다. HHS가 지정한 후속 사이트 (또는 관련 사이트) 에서 업데이트될 수 있으므로 이 사이트를 참조하십시오.

AWS는 PHI의 키 관리 및 암호화를 쉽게 관리하고 감사를 단순화할 수 있는 포괄적인 기능 및 서비스 세트를 제공합니다 AWS Key Management Service (AWS KMS). HIPAA 규정 준수 요구 사항이 있는 고객은 PHI에 대한 암호화 요구 사항을 매우 유연하게 충족할 수 있습니다.

암호화 구현 방법을 결정할 때 고객은 HIPAA 적격 서비스에 기본으로 제공되는 암호화 기능을 평가하고 활용하거나 HHS의 지침에 부합하는 다른 방법을 통해 암호화 요구 사항을 충족할 수 있습니다. 다음 섹션에서는 각 HIPAA 적격 서비스에서 사용 가능한 암호화 기능을 사용하는 방법과 기타 PHI 암호화 패턴, AWS KMS를 사용하여 AWS에서 PHI 암호화에 사용되는 키를 암호화하는 방법에 대한 수준 높은 세부 정보를 제공합니다.

주제

- Amazon API Gateway
- 아마존 AppFlow
- 아마존 AppStream 2.0
- Amazon Athena
- Amazon Aurora
- Amazon Aurora PostgreSQL
- 아마존 CloudFront
- 아마존 CloudWatch
- 아마존 CloudWatch 이벤트
- 아마존 CloudWatch 로그
- Amazon Comprehend
- Amazon Comprehend Medical
- Amazon Connect
- Amazon DocumentDB(MongoDB 호환)

- Amazon DynamoDB
- Amazon Elastic Block Store
- Amazon Elastic Compute Cloud
- Amazon Elastic 컨테이너 레지스트리
- Amazon Elastic Container Service
- Amazon Elastic File System(Amazon EFS)
- Amazon Elastic Kubernetes Service(Amazon EKS)
- 아마존 포 ElastiCache 레디스용
- 아마존 OpenSearch 서비스
- Amazon EMR
- 아마존 EventBridge
- Amazon Forecast
- Amazon FSx
- 아마존 GuardDuty
- 아마존 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 네트워크 방화벽
- Amazon Pinpoint
- Amazon Polly
- Amazon Quantum Ledger Database(QLDB)
- 아마존 QuickSight

- Amazon RDS for MariaDB
- Amazon RDS for MySQL
- Amazon RDS for Oracle
- Amazon RDS for PostgreSQL
- Amazon RDS for SQL Server
- Amazon Redshift
- Amazon Rekognition
- Amazon Route 53
- Amazon S3 Glacier
- Amazon S3 전송 가속화
- 아마존 SageMaker
- Amazon Simple Notification Service(Amazon SNS)
- Amazon Simple Email Service(Amazon SES)
- Amazon Simple Queue Service(Amazon SQS)
- Amazon Simple Storage Service(S3)
- Amazon Simple Workflow Service
- Amazon Textract
- Amazon Transcribe
- Amazon Translate
- Amazon Virtual Private Cloud
- Amazon WorkDocs
- 아마존 WorkSpaces
- AWS App Mesh
- AWS 애플리케이션 마이그레이션 서비스
- AWS Auto Scaling
- AWS Backup
- AWS Batch
- AWS Certificate Manager
- AWS Cloud Map

- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- AWS CodeBuild
- AWS CodeDeploy
- AWS CodeCommit
- AWS CodePipeline
- AWS Config
- AWS Data Exchange
- AWS Database Migration Service
- AWS DataSync
- AWS Directory Service
- AWS Elastic Beanstalk
- AWS 엘라스틱 재해 복구
- AWS Fargate
- AWS Firewall Manager
- AWS Global Accelerator
- AWS Glue
- AWS Glue DataBrew
- AWS IoT 코어 및 AWS IoT Device Management
- AWS IoT Greengrass
- AWS Lambda
- AWS Managed Services
- AWS OpsWorks 셰프 오토메이트의 경우
- AWS OpsWorks 퍼펫 엔터프라이즈용
- AWS OpsWorks 스택
- AWS Organizations
- AWS RoboMaker
- AWS SDK 지표
- AWS Secrets Manager

- AWS Security Hub CSPM
- AWS Server Migration Service
- AWS Serverless Application Repository
- 서비스 카탈로그
- AWS Shield
- AWS Snowball Edge
- AWS Snowball Edge 에지
- AWS Step Functions
- AWS Storage Gateway
- AWS Systems Manager
- AWS Transfer for SFTP
- AWS WAF — 웹 애플리케이션 방화벽
- AWS X-Ray
- Elastic Load Balancing
- FreeRTOS
- AWS KMS PHI 암호화에 사용
- VM Import

## Amazon API Gateway

고객은 Amazon API Gateway를 사용하여 보호 대상 건강 정보 (PHI) 를 처리하고 전송할 수 있습니다. Amazon API Gateway는 전송 중 암호화에 자동으로 HTTPS 엔드포인트를 사용하지만, 고객은 클라이언트 측에서 페이로드를 암호화하도록 선택할 수도 있습니다. API Gateway는 캐시되지 않은 모든 데이터를 메모리를 통해 전달하며 디스크에 쓰지 않습니다. 고객은 API Gateway를 통한 권한 부여를 위해 AWS 서명 버전 4를 사용할 수 있습니다. 자세한 내용은 다음 자료를 참조하십시오.

- Amazon API Gateway FAQ: 보안 및 권한 부여
- API Gateway에서 REST API에 대한 액세스 제어 및 관리

고객은 API Gateway에 연결된 모든 서비스와 통합할 수 있습니다. 단, PHI가 포함될 경우 서비스가 지침 및 BAA와 일치하도록 구성되어 있어야 합니다. API Gateway를 백엔드 서비스와 통합하는 방법에 대한 자세한 내용은 API Gateway에서 REST API 메서드 설정을 참조하십시오.

고객은 CloudWatch Amazon을 사용하여 AWS CloudTrail 로깅 요구 사항과 일치하는 로깅을 활성화할 수 있습니다. API Gateway를 통해 전송되는 모든 PHI (예: 헤더, URL, 요청/응답) 는 지침과 일치하도록 구성된 HIPAA 적격 서비스에서만 캡처되도록 하십시오. API Gateway를 사용한 로깅에 대한 자세한 내용은 API Gateway REST API 또는 WebSocket API 문제 해결을 위해 CloudWatch 로그를 활성화하려면 어떻게 해야 합니까? 를 참조하십시오.

## 아마존 AppFlow

AppFlow Amazon은 고객이 Salesforce, Marketo, Slack과 같은 oftware-as-a S-Service (SaaS) 애플리케이션과 Amazon S3 ServiceNow 및 Amazon Redshift와 같은 AWS 서비스 간에 데이터를 안전하게 전송할 수 있도록 하는 완전 관리형 통합 서비스입니다. AppFlow 일정에 따라, 비즈니스 이벤트에 응답하거나, 필요에 따라 고객이 선택한 빈도로 데이터 흐름을 실행할 수 있습니다. 또한 고객은 필터링 및 검증과 같은 데이터 변환 기능을 구성하여 추가 단계 없이 흐름 자체의 일부로 풍부한 ready-to-use 데이터를 생성할 수 있습니다.

Amazon은 PHI를 포함하는 데이터를 처리하고 전송하는 데 사용할 AppFlow 수 있습니다. 구성된 소스/목적지 간 AppFlow 전송 중 데이터 암호화는 TLS 1.2 이상을 사용하여 기본적으로 제공됩니다. S3에 저장된 미사용 데이터는 고객이 지정한 AWS KMS 키 (이전 명칭 CMK) 를 사용하여 자동으로 암호화됩니다. S3가 아닌 대상으로 전송되는 PHI 데이터의 경우 고객은 선택한 대상의 미사용 스토리지가 보안 요구 사항을 충족하는지 확인해야 합니다. AppFlow AWS CloudTrail to log API 호출 및 Amazon과 통합하여 흐름 실행 이벤트를 내보내 애플리케이션을 EventBridge 모니터링할 수 있도록 합니다.

## 아마존 AppStream 2.0

Amazon AppStream 2.0은 완전 관리형 애플리케이션 스트리밍 서비스입니다. 고객은 데이터를 소유하며 규제 요구 사항을 충족하는 방식으로 필요한 Windows 애플리케이션을 구성해야 합니다. 고객은 홈 폴더를 통해 영구 스토리지를 구성할 수 있습니다. 파일과 폴더는 Amazon S3의 SSL 엔드포인트를 사용하여 전송 시 암호화됩니다. 파일 및 폴더는 Amazon S3에서 관리하는 암호화 키를 사용하여 저장 중에 암호화됩니다. 자세한 내용은 AppStream 2.0 사용자를 위한 영구 스토리지 활성화 및 관리를 참조하십시오. 고객이 타사 스토리지 솔루션을 사용하기로 선택한 경우 해당 솔루션의 구성이 지침과 일치하는지 확인해야 합니다. Amazon AppStream 2.0과의 모든 퍼블릭 API 통신은 TLS를 사용하여 암호화됩니다. 자세한 내용은 Amazon AppStream 2.0 설명서를 참조하십시오.

Amazon AppStream 2.0은 고객의 AWS 계정에서 Amazon 2.0에 의해 또는 Amazon AppStream 2.0을 대신하여 이루어진 API 호출을 기록하고 지정된 Amazon S3 버킷으로 AWS CloudTrail로그 파일을 전달하는 서비스와 통합되어 있습니다. CloudTrail 아마존 AppStream 2.0 콘솔 또는 아마존 2.0 API에서 이루어진 API 호출을 캡처합니다. AppStream 고객은 CloudWatch Amazon을 사용하여 리소스 사용량

지표를 기록할 수도 있습니다. 자세한 내용은 Amazon AppStream 2.0 리소스 모니터링 및 AppStream 2.0 API 호출 로깅을 참조하십시오 AWS CloudTrail.

## Amazon Athena

Amazon Athena는표준 SQL을 사용하여 Amazon Simple Storage Service(S3)에 있는 데이터를 직접 간편하게 분석할 수 있는 대화형 쿼리 서비스입니다. Athena는 고객이 Amazon S3에 저장된 비정형, 반정형 및 정형 데이터를 분석할 수 있도록 지원합니다. 예를 들면 CSV, JSON 또는 컬럼 방식 데이터 형식(예: Apache Parquet 및 Apache ORC)이 해당됩니다. 고객은 데이터를 집계하거나 Athena로 로드할 필요 없이 Athena를 사용하여 ANSI SQL을 사용하여 임시 쿼리를 실행할 수 있습니다.

이제 Amazon Athena를 사용하여 PHI를 포함하는 데이터를 처리할 수 있습니다. Amazon Athena와 S3 간에 전송되는 동안의 데이터 암호화는 기본적으로 SSL/TLS를 사용하여 제공됩니다. S3에 저장된 상태에서의 PHI 암호화는 S3 섹션에 제공된 지침에 따라 수행되어야 합니다. Amazon S3 관리 키 (SSE-S3), 관리 키 (SSE-KMS) 를 사용한 서버 측 암호화 또는 관리 키를 사용한 클라이언트 측 암호화 (CSE-KMS) 를 사용하여 Amazon Athena와 내부 쿼리 결과를 암호화할 수 있도록 설정해야 합니다. AWS KMS AWS KMS Amazon Athena는 모든 API 호출을 AWS CloudTrail 기록하는 데 사용합니다.

## Amazon Aurora

Amazon Aurora를 사용하면 고객이 관리하는 키를 사용하여 저장된 Aurora 데이터베이스 클러스터와 스냅샷을 암호화할 수 있습니다. AWS KMS Amazon Aurora 암호화를 실행하는 데이터베이스 인스턴스에서는 자동 백업, 읽기 전용 복제본, 스냅샷과 마찬가지로 기본 스토리지에 저장된 데이터가 암호화됩니다.

지침이 업데이트될 수 있으므로 고객은 Amazon Aurora 암호화가 규정 준수 및 규제 요구 사항을 충족하는지 여부를 계속 평가하고 결정해야 합니다. Amazon Aurora를 사용한 저장 중 암호화에 대한 자세한 내용은 암호화를 사용한 데이터 보호를 참조하십시오.

Aurora MySQL을 실행하는 DB 클러스터에 연결하려면 보안 소켓 계층 (SSL) 또는 전송 계층 보안 (TLS) 을 활용하는 전송 암호화를 사용해야 합니다. SSL/TLS를 구현하는 방법에 대한 자세한 내용은 Aurora MySQL DB 클러스터에서 SSL/TLS 사용을 참조하십시오.

## Amazon Aurora PostgreSQL

Amazon Aurora를 사용하면 고객이 관리하는 키를 사용하여 저장된 Aurora 데이터베이스 클러스터와 스냅샷을 암호화할 수 있습니다. AWS KMS Amazon Aurora 암호화를 실행하는 데이터베이스 인스턴

스에서는 자동 백업, 읽기 전용 복제본, 스냅샷과 마찬가지로 기본 스토리지에 저장된 데이터가 암호화됩니다.

지침이 업데이트될 수 있으므로 고객은 Amazon Aurora 암호화가 규정 준수 및 규제 요구 사항을 충족하는지 여부를 계속 평가하고 결정해야 합니다. Amazon Aurora를 사용한 저장 중 암호화에 대한 자세한 내용은 암호화를 사용한 데이터 보호를 참조하십시오.

Aurora PostgreSQL을 실행하는 DB 클러스터에 연결하려면 보안 소켓 계층 (SSL) 또는 전송 계층 보안 (TLS) 을 활용하는 전송 암호화를 사용해야 합니다. SSL/TLS를 구현하는 방법에 대한 자세한 내용은 SSL을 사용한 Aurora PostgreSQL 데이터 보안을 참조하십시오.

# 아마존 CloudFront

CloudFront Amazon은 고객 웹 사이트, API, 비디오 콘텐츠 또는 기타 웹 자산의 전송을 가속화하는 글로벌 콘텐츠 전송 네트워크 (CDN) 서비스입니다. 다른 Amazon Web Services 제품과 통합되므로 개발자와 기업은 최소 사용 약정 없이 최종 사용자에게 콘텐츠를 빠르게 제공할 수 있는 손쉬운 방법을 제공합니다. 전송 중에 PHI를 암호화하려면 고객이 오리진에서 CloudFront end-to-end 뷰어까지 HTTPS를 사용하도록 CloudFront 구성해야 합니다.

여기에는 최종 사용자 간 CloudFront 트래픽, 사용자 지정 오리진에서의 CloudFront 재배포, Amazon S3 오리진에서의 CloudFront 배포가 포함됩니다. 또한 고객은 데이터가 캐싱되는 동안 유휴 상태에서도 암호화된 상태를 유지할 수 있도록 오리진에서 데이터를 암호화해야 합니다. CloudFront Amazon S3를 오리진으로 사용하는 경우 고객은 S3 서버 측 암호화 기능을 사용할 수 있습니다. 고객이 사용자 지정 오리진에서 배포하는 경우 오리진에서 데이터가 암호화되었는지 확인해야 합니다.

## Lambda@Edge

Lambda @Edge 는 AWS 엣지 로케이션에서 Lambda 함수를 실행할 수 있게 해주는 컴퓨팅 서비스입니다. Lambda @Edge 를 사용하여 전송되는 콘텐츠를 사용자 지정할 수 있습니다. CloudFront Lambda @Edge 를 PHI와 함께 사용하는 경우 고객은 사용에 대한 지침을 따라야 합니다. CloudFront Lambda @Edge 로 들어오고 나가는 모든 연결은 HTTPS 또는 SSL/TLS를 사용하여 암호화해야 합니다.

# 아마존 CloudWatch

CloudWatch Amazon은 고객이 AWS에서 실행하는 AWS 클라우드 리소스 및 애플리케이션에 대한 모니터링 서비스입니다. 고객은 CloudWatch Amazon을 사용하여 지표를 수집 및 추적하고, 로그 파일을 수집 및 모니터링하고, 경보를 설정할 수 있습니다. Amazon CloudWatch 자체는 PHI를 생성, 저장

또는 전송하지 않습니다. 고객은 를 사용하여 CloudWatch API 호출을 모니터링할 수 있습니다. AWS CloudTrail자세한 내용은 Amazon CloudWatch API 호출 로깅을 참조하십시오 AWS CloudTrail.

구성 요구 사항에 대한 자세한 내용은 Amazon CloudWatch Logs 섹션을 참조하십시오.

## 아마존 CloudWatch 이벤트

Amazon CloudWatch Events는 AWS 리소스의 변경 사항을 설명하는 시스템 이벤트 near-real-time 스트림을 제공합니다. 고객은 PHI가 CloudWatch Events로 유입되지 않도록 해야 하며, PHI를 저장, 처리 또는 전송하는 CloudWatch 이벤트를 내보내는 모든 AWS 리소스가 지침에 따라 구성되어 있는지 확인해야 합니다.

고객은 AWS API 콜인으로 등록하도록 Amazon CloudWatch Events를 구성할 수 CloudTrail 있습니다. 자세한 내용은 를 사용하여 AWS CloudTrail AWS API 호출에서 트리거되는 CloudWatch 이벤트 규칙 생성을 참조하십시오.

## 아마존 CloudWatch 로그

고객은 Amazon CloudWatch Logs를 사용하여 Amazon Elastic Compute Cloud (Amazon EC2) 인스턴스, Amazon Route 53 및 기타 소스에서 로그 파일을 모니터링 AWS CloudTrail, 저장 및 액세스할 수 있습니다. 그러면 로그에서 CloudWatch 관련 로그 데이터를 검색할 수 있습니다. 로그 데이터는 전송 중이거나 유휴 상태일 때 암호화됩니다. 따라서 다른 서비스에서 내보낸 PHI를 Logs로 전송하여 다시 암호화할 필요가 없습니다. CloudWatch

## Amazon Comprehend

Amazon Comprehend는 자연어 처리를 사용하여 문서 내용에 대한 인사이트를 추출합니다. Amazon Comprehend는 UTF-8 형식의 모든 텍스트 파일을 처리합니다. 문서에 있는 개체, 핵심 문구, 언어, 감정 및 기타 일반적인 요소를 인식하여 인사이트를 개발합니다. Amazon Comprehend는 PHI를 포함하는 데이터와 함께 사용할 수 있습니다. Amazon Comprehend는 데이터를 보관하거나 저장하지 않으며 API에 대한 모든 호출은 SSL/TLS로 암호화됩니다. Amazon CloudTrail Comprehend는 모든 API 호출을 기록하는 데 사용합니다.

### AWS Identity and Access Management

Amazon Comprehend에 액세스하려면 인증 및 권한 부여와 같은 보안 액세스 기능이 필요하며 IAM (IAM) AWS Identity and Access Management으로 제어할 수 있으며 자격 증명을 사용하여 IAM에 액

세스할 수 있습니다. 자세한 내용은 아마존 Comprehend 사용 설명서의 Amazon Comprehend에 대한 인증 및 액세스 제어를 참조하십시오.

## 계정 관리

기본적으로 IAM 사용자에게는 Amazon Comprehend 리소스를 생성 또는 수정하거나 Amazon Comprehend API를 사용하여 작업을 수행할 권한이 없습니다. 사용자가 리소스를 생성 또는 수정하고 작업을 수행할 수 있도록 하려면 고객은 IAM 정책을 활용하여 사용자에게 사용해야 하는 특정 리소스 (예: Amazon Comprehend 및 API 작업) 에 대한 권한을 부여한 다음 특정 권한이 필요한 사용자 또는 그룹에 정책을 연결할 책임이 있습니다.

Amazon Comprehend를 AWS Identity and Access Management 사용하면 (IAM) 을 사용하여 정책을 첨부하여 Amazon Comprehend 권한을 활성화하는 사용자를 생성할 수 있습니다. 필요에 따라 사용자 지정 정책을 생성하여 역할에 연결하도록 선택할 수 있습니다. 그런 다음 조직에서 정의한 역할 기반 액세스 및 최소 권한 원칙에 따라 Amazon Comprehend 관리용 API를 호출할 수 있는 권한을 가진 관리자를 역할에 추가할 수 있습니다.

## 자격 증명 및 액세스

Amazon Comprehend를 사용하면 조직의 인증 요구 사항에 따라 사용자에게 다단계 인증을 사용하도록 AWS 인증하도록 요구할 수 있습니다.

IAM 관리자는 를 사용하여 사용자가 자신의 자격 증명과 MFA 디바이스를 관리하는 데 필요한 권한을 제외한 모든 권한을 거부하는 고객 관리형 정책을 만들 수 있습니다. AWS Management Console JSON 정책 템플릿은 IAM 콘솔의 내 보안 자격 증명 페이지에서 사용할 수 있습니다.

선택적으로 IAM 파트너와 호환되는 타사 MFA 기능을 활용할 수 있습니다. 자세한 내용은 IAM 파트너를 참조하십시오.

## 관리

Amazon Comprehend에서는 계정 관리자가 IAM 자격 증명 (사용자, 그룹 및 역할) 에 권한 정책을 첨부하여 Amazon Comprehend 리소스에서 작업을 수행할 수 있는 권한을 부여할 수 있는 자격 증명 기반 정책을 선택하는 것이 좋습니다.

Amazon Comprehend의 API 작업 목록은 API 참조 가이드에서 찾을 수 있습니다. 또한 최소 권한 및 역할 기반 조직 요구 사항에 따라 사용자 또는 역할에 대해 사전 정의된 IAM 정책, 고객 IAM 정책 및 API 작업에 대한 액세스를 승인하는 것도 고려해야 합니다. 자세한 내용은 개발자 안내서의 Amazon Comprehend API 사용을 참조하십시오.

### 외부 인증

Amazon Comprehend는 IAM 역할을 사용하는 자격 증명 페더레이션과 호환됩니다. 이를 통해 Amazon Comprehend는 관리자가 프로비저닝한 역할을 맡아 사용자가 인증을 AWS 받을 수 있습니다. 조직 또는 제3자의 자격 증명을 AWS 사용하여 액세스하는 사용자는 간접적으로 역할을 맡습니다.

AWS Kerberos 및 Active Directory에 대한 지원은 데이터베이스 사용자에 대한 싱글 사인온 및 중앙 집중식 인증의 이점을 제공합니다. AWS 사용자는 Microsoft Active AWS Directory Service Directory용 또는 고객 온-프레미스 Active Directory에서 사용자 자격 증명을 관리하고 저장하도록 선택할 수 있습니다.

### 데이터 흐름 적용

AWS 데이터 컨트롤러 또는 데이터 처리자 역할을 하는 고객 및 APN 파트너는 Amazon Comprehend에 저장하는 모든 개인 데이터에 대한 책임이 있습니다. AWS 클라우드 사용자는 IAM 정책을 사용하여 Amazon Comprehend의 데이터 입력 및 출력 흐름을 제어할 책임이 있습니다.

## 데이터 보호 및 비밀 관리

AWS 공동 책임 모델은 Amazon Comprehend의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로, AWS 는 모든 클라우드를 실행하는 글로벌 인프라를 보호하는 역할을 합니다 AWS . 이 인프라에서 호스팅되는 콘텐츠에 대한 제어를 유지하는 것은 사용자의 책임입니다. 이 콘텐츠에는 사용하는 AWS 서비스의 보안 구성 및 관리 작업이 포함됩니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요.

Amazon Comprehend 개발자 안내서의 Amazon Comprehend 데이터 보호 섹션에서는 전송을 위한 TLS 사용, 태그 또는 자유 형식 필드에 민감한 정보가 배치되지 않도록 하는 등 데이터를 보호할 때 고려해야 할 팁을 제공합니다.

### 암호화: data-at-rest

Amazon Comprehend는 AWS Key Management Service(AWS KMS)와 함께 작동하여 데이터에 대한 향상된 암호화를 제공합니다. Amazon Simple Storage Service (Amazon S3) 를 사용하면 텍스트 분석, 주제 모델링 또는 사용자 지정 Amazon Comprehend 작업을 생성할 때 이미 입력 문서를 암호화할 수 있습니다. 와 AWS KMS 통합하면 시작* 및 생성* 작업을 위해 스토리지 볼륨의 데이터를 암호화할 수 있으며, 시작* 작업의 출력 결과를 사용자 고유의 키를 사용하여 암호화합니다. AWS KMS

Amazon Comprehend 사용자는 조직 정책에 따라 사용 가능한 S3 암호화 솔루션을 사용하여 입력 문서에 사용되는 Amazon S3 버킷을 암호화하는 것이 가장 좋습니다.

는 AWS Management Console자체 키를 사용하여 Amazon Comprehend 사용자 지정 모델을 암호화합니다. AWS KMS 의 AWS CLI경우 Amazon Comprehend는 AWS KMS 자체 키 또는 제공된 고객 관리 키 (CMK) 를 사용하여 사용자 지정 모델을 암호화할 수 있습니다.

를 사용할 때 암호화를 선택하는 경우 다음 AWS Management Console선택적 방법 중 하나 또는 둘 다를 선택할 수 있습니다.

- 볼륨 암호화 - Comprehend에서 사용하는 EBS 볼륨의 데이터가 훈련/추론 중에 암호화되도록 합니다 (데이터는 훈련/추론 후에 플러시되므로 이 키는 작업이 진행 중인 동안에만 유효함).
- 출력 결과 암호화 - Comprehend가 고객의 버킷에 저장한 출력을 고객 제공 키를 사용하여 암호화합니다. AWS KMS

볼륨 암호화와 같은 암호화 유형에 대한 자세한 내용은 Amazon Comprehend에서의AWS KMS 암호화를 참조하십시오.

### 개인 식별 정보

Amazon Comprehend 콘솔 또는 API를 사용하여 영어 텍스트 문서에서 개인 식별 정보(PII)를 감지할 수 있습니다. PII 엔티티를 탐지 및 레이블링하고 다양한 PII 분석 작업을 운영하는 방법에 대한 자세한 내용은 Amazon Comprehend 개발자 안내서의 개인 식별 정보 섹션을 참조하십시오.

### 데이터 삭제

Amazon S3를 사용하고 AWS KMS 자체 키를 관리하기로 선택한 Amazon Comprehend 고객인 경우, 조직 요구 사항에 따라 키를 AWS KMS 취소하고 이를 수행할 절차적 근거를 정의하는 것을 고려해야 합니다. Amazon S3의 AWS KMS 키를 취소하면 모든 데이터를 사용할 수 없거나 읽을 수 없게 됩니다.

## 네트워크 세분화 및 강화

관리형 서비스인 Amazon Comprehend는 보안, ID 및 규정 준수에AWS 대한 모범 사례를 준수합니다.

권장되는 네트워크 보안 보호 조치는 Amazon Comprehend 개발자 안내서의 Amazon Comprehend의 인프라 보안을 참조하십시오.

### 아마존 가상 사설 클라우드 (Amazon VPC) 를 사용하여 작업을 보호합니다.

Amazon Comprehend는 Amazon Comprehend에서 데이터가 저장된 작업 컨테이너를 사용하는 동안 데이터의 안전을 보장하기 위해 다양한 보안 조치를 사용합니다. 하지만 작업 컨테이너는 인터넷을 통해 데이터 및 모델 AWS 아티팩트를 저장하는 Amazon S3 버킷과 같은 리소스에 액세스합니다.

사용자 데이터에 대한 액세스를 제어하려면 Virtual Private Cloud(VPC)를 생성하고 구성하여 데이터와 컨테이너가 인터넷을 통해 액세스 되지 않도록 구성하는 것이 좋습니다. VPC 생성 및 구성에 대한 내용은 Amazon VPC 사용 설명서의 Amazon VPC 시작하기를 참조하십시오. VPC를 사용하면 사용자 데이터가 인터넷에 연결되지 않도록 VPC를 구성할 수 있기 때문에 데이터 보호에 도움이 됩니다. 또한 VPC를 사용하면 VPC 흐름 로그를 통하여 당사 작업 컨테이너에 들어오고 나가는 모든 네트워크 트래픽을 모니터링할 수 있습니다. 자세한 내용은 Amazon VPC 사용 설명서의 VPC 흐름 로그를 참조하세요.

작업을 생성할 때 서브넷 및 보안 그룹을 지정하여 프라이빗 VPC 구성을 지정합니다. 서브넷 및 보안 그룹을 지정할 때 Amazon Comprehend가 서브넷 중 하나에 있는 보안 그룹과 연결된 탄력적 네트워크 인터페이스(ENI)를 생성합니다. ENI를 통해 작업 컨테이너는 사용자 VPC에 있는 리소스와 연결될 수 있습니다. ENI에 대한 자세한 내용은 Amazon VPC 사용 설명서의 탄력적 네트워크 인터페이스를 참조하세요.

> **Note**
>
> 작업의 경우, 사용자는 사용자 인스턴스가 실행되는 공유 하드웨어의 기본 테넌시 VPC 만을 사용하여 서브넷을 구성할 수 있습니다. VPC 테넌시에 대한 자세한 내용은 Linux 인스턴스용 Amazon EC2 사용 설명서의 전용 인스턴스를 참조하세요.

인터페이스 VPC 엔드포인트를 생성하여 VPC와 Amazon Comprehend 간에 프라이빗 연결을 설정할 수 있습니다. 자세한 내용은 Amazon Comprehend 및 인터페이스 VPC 엔드포인트 () 를 참조하십시오.AWS PrivateLink

## 호스트 및 이미지 강화

AWS 공동 책임 모델에 따라 Amazon Comprehend AWS 환경의 호스트 및 이미지 강화는 제공된 서비스로 AWS 관리됩니다.

## 멀티테넌시

권장 사항의 보안을 강화하려면 다음과 같은 멀티테넌시 보안 권장 사항을 구현하는 것이 좋습니다.

- 도메인 일치를 기반으로 테넌트에 대한 사용자 액세스 권한을 부여하는 데 확인된 이메일 주소만 사용합니다. 앱에서 확인하거나 외부 IdP가 확인 증명을 제공하는 경우에만 이메일 주소와 전화 번호를 신뢰하세요. 이러한 권한 설정에 대한 자세한 내용은 속성 권한 및 범위를 참조하세요.

- 테넌트를 식별하는 사용자 프로필 속성에 변경 불가능한 속성 또는 변경 가능한 속성을 사용합니다. 관리자는 이러한 속성을 변경할 수 있어야 합니다. 또한 앱 클라이언트에 이러한 속성에 대한 읽기 전용 권한을 부여합니다.
- 외부 IdP와 애플리케이션 클라이언트 간에 일대일 매핑을 사용하여 무단 테넌트 간 액세스를 방지합니다. 외부 IdP에서 인증되었으며 유효한 Amazon Cognito 세션 쿠키가 있는 사용자는 동일한 IdP를 신뢰하는 다른 테넌트 앱에 액세스할 수 있습니다.
- 애플리케이션에서 테넌트 일치 및 권한 부여 로직을 구현할 때 테넌트에 대한 사용자 액세스 권한을 부여하는 기준을 사용자가 직접 수정할 수 없도록 합니다. 또한 페더레이션에 외부 IdP 가 사용되는 경우 테넌트 ID 공급자 관리자가 사용자 액세스를 수정할 수 없도록 합니다.

## 교차 서비스 혼동된 대리인 방지

대리인 문제는 멀티테넌시 보안 문제로, 작업을 수행할 권한이 없는 엔티티가 더 많은 권한을 가진 엔티티에게 작업을 수행하도록 강요할 수 있는 멀티 테넌시 보안 문제입니다. 에서 크로스 서비스 AWS 사칭은 대리인 문제로 혼란스러운 결과를 초래할 수 있습니다. 교차 서비스 가장은 한 서비스(호출하는 서비스)가 다른 서비스(호출되는 서비스)를 직접적으로 호출할 때 발생할 수 있습니다. 호출하는 서비스는 다른 고객의 리소스에 대해 액세스 권한이 없는 방식으로 작동하게 권한을 사용하도록 조작될 수 있습니다. 이를 방지하기 위해 계정 내 리소스에 대한 액세스 권한이 부여된 서비스 보안 주체를 통해 모든 서비스의 데이터를 보호하는 데 도움이 되는 도구를 AWS 제공합니다. 이 보안 문제를 해결하기 위해 고려해야 하는 보호 장치를 포함한 자세한 내용은 Amazon Comprehend 개발자 안내서의 서비스 간 혼란 부정 방지를 참조하십시오.

# Amazon Comprehend Medical

지침은 이전 섹션을 참조하십시오. Amazon Comprehend

# Amazon Connect

Amazon Connect는 모든 규모에서 동적이고 개인적이며 자연스러운 고객 참여를 가능하게 하는 셀프 서비스 클라우드 기반 콜 센터 서비스입니다. 고객은 Amazon Connect 내에서 사용자, 보안 프로필 및 통화 흐름 관리와 관련된 필드에 PHI를 포함해서는 안 됩니다.

Amazon Connect의 기능인 Amazon Connect 고객 프로필은 콜 센터 상담원이 최신 정보와 함께 고객 프로필을 보다 통합적으로 볼 수 있도록 하여 보다 개인화된 고객 서비스를 제공합니다. 고객 프로필은 여러 애플리케이션의 고객 정보를 통합 고객 프로필로 자동으로 통합하여 지원 전화 또는 상담이 시작되는 즉시 에이전트에게 프로필을 직접 전달하도록 설계되었습니다. 고객은 PHI 데이터로 도메인이나

개체 키의 이름을 지정하지 않아야 합니다. 도메인 및 개체의 콘텐츠는 암호화되고 보호되지만 키 식별자는 암호화되지 않습니다.

## Amazon DocumentDB(MongoDB 호환)

Amazon DocumentDB (MongoDB 호환 가능) (Amazon DocumentDB) 는 클러스터를 생성하는 동안 고객이 AWS 또는 고객 관리 키를 사용하여 데이터베이스를 암호화할 수 있도록 하는 미사용 암호화를 제공합니다. AWS KMS암호화가 활성화된 상태로 실행되는 데이터베이스 인스턴스에서는 자동 백업, 읽기 전용 복제본 및 스냅샷과 마찬가지로 저장된 데이터가 이 백서 발행 당시 유효한 지침에 따라 암호화됩니다. 지침이 업데이트될 수 있으므로 고객은 Amazon DocumentDB 암호화가 규정 준수 및 규제 요구 사항을 충족하는지 여부를 계속 평가하고 결정해야 합니다. Amazon DocumentDB를 사용한 저장 중 암호화에 대한 자세한 내용은 저장된 Amazon DocumentDB 데이터 암호화를 참조하십시오.

PHI를 포함하는 Amazon DocumentDB에 연결하려면 암호화된 전송 (HTTPS) 을 허용하는 엔드포인트를 사용해야 합니다. 기본적으로 새로 생성된 Amazon DocumentDB 클러스터는 전송 계층 보안 (TLS) 을 사용한 보안 연결만 허용합니다. 자세한 내용은 전송 데이터 암호화를 참조하십시오. Amazon AWS CloudTrail DocumentDB는 모든 API 호출을 기록하는 데 사용합니다. 자세한 내용은 Amazon DocumentDB의 로깅 및 모니터링을 참조하십시오.

일부 관리 기능의 경우 Amazon DocumentDB는 Amazon RDS와 공유되는 운영 기술을 사용합니다. Amazon DocumentDB 콘솔, AWS CLI 및 API 호출은 Amazon RDS API에 대한 호출로 기록됩니다.

## Amazon DynamoDB

PHI를 포함하는 Amazon DynamoDB에 대한 연결은 암호화된 전송 (HTTPS) 을 허용하는 엔드포인트를 사용해야 합니다. 리전 엔드포인트 목록은 AWS 서비스 엔드포인트를 참조하십시오.

Amazon DynamoDB는 고객이 관리하는 키를 사용하여 데이터베이스를 암호화할 수 있는 DynamoDB 암호화를 제공합니다. AWS KMS Amazon DynamoDB 암호화를 실행하는 데이터베이스 인스턴스에서는 자동 백업, 읽기 전용 복제본, 스냅샷과 마찬가지로 기본 스토리지에 저장된 데이터가 이 백서 발행 당시 유효한 지침에 따라 암호화됩니다.

지침이 업데이트될 수 있으므로 고객은 Amazon DynamoDB 암호화가 규정 준수 및 규제 요구 사항을 충족하는지 계속 평가하고 결정해야 합니다. Amazon DynamoDB를 사용한 저장 중 암호화에 대한 자세한 내용은 저장 중인 DynamoDB 암호화를 참조하십시오.

# Amazon Elastic Block Store

Amazon EBS 미사용 암호화는 본 백서 발행 당시 유효한 지침과 일치합니다. 지침이 업데이트될 수 있으므로 고객은 Amazon EBS 암호화가 규정 준수 및 규제 요구 사항을 충족하는지 계속 평가하고 결정해야 합니다. Amazon EBS 암호화를 사용하면 각 EBS 볼륨에 대해 고유한 볼륨 암호화 키가 생성됩니다. 고객은 에서 각 볼륨 키를 암호화하는 데 사용할 KMS 키를 유연하게 선택할 수 있습니다. AWS Key Management Service 자세한 내용은 Amazon EBS 암호화를 참조하세요.

# Amazon Elastic Compute Cloud

Amazon EC2는 저장 데이터를 암호화하는 여러 방법을 지원하는 확장 가능하고 사용자 구성 가능한 컴퓨팅 서비스입니다. 예를 들어, 고객은 Amazon EC2 인스턴스에 호스팅된 애플리케이션 또는 데이터베이스 플랫폼 내에서 처리될 때 애플리케이션 또는 필드 수준 PHI 암호화를 수행하도록 선택할 수 있습니다. 접근 방식은 Java 또는 .NET과 같은 애플리케이션 프레임워크의 표준 라이브러리를 사용하여 데이터를 암호화하는 것, Microsoft SQL 또는 Oracle의 투명한 데이터 암호화 기능을 활용하는 것, 다른 타사 및 SaaS (Software as a Service) 기반 솔루션을 애플리케이션에 통합하는 것까지 다양합니다.

고객은 Amazon EC2에서 실행되는 애플리케이션을 AWS KMS SDK와 통합하여 키 관리 및 스토리지 프로세스를 간소화할 수 있습니다. 또한 고객은 AWS Marketplace 파트너의 타사 소프트웨어 또는 기본 파일 시스템 암호화 도구 (예: dm-crypt, LUKS 등) 를 사용하여 파일 수준 또는 전체 디스크 암호화 (FDE) 를 사용하여 저장 데이터를 암호화할 수 있습니다.

PHI를 포함하는 네트워크 트래픽은 전송 데이터를 암호화해야 합니다. 외부 소스 (예: 인터넷 또는 기존 IT 환경) 와 Amazon EC2 간 트래픽의 경우 고객은 지침에 따라 전송 계층 보안 (TLS) 또는 IPsec VPN (가상 사설망) 과 같은 개방형 표준 전송 암호화 메커니즘을 사용해야 합니다. Amazon EC2 인스턴스 간 데이터 이동을 위한 Amazon VPC (Virtual Private Cloud) 내부에서는 PHI를 포함하는 네트워크 트래픽도 암호화해야 합니다. 대부분의 애플리케이션은 지침과 일치하도록 구성할 수 있는 전송 중 암호화를 제공하는 TLS 또는 기타 프로토콜을 지원합니다. 암호화를 지원하지 않는 애플리케이션 및 프로토콜의 경우 IPsec 또는 인스턴스 간 유사한 구현을 사용하여 암호화된 터널을 통해 PHI를 전송하는 세션을 전송할 수 있습니다.

# Amazon Elastic 컨테이너 레지스트리

Amazon Elastic Container 레지스트리 (Amazon ECR) 는 Amazon Elastic Container Service (Amazon ECS) 와 통합되어 고객이 Amazon ECS에서 실행되는 애플리케이션을 위한 컨테이너 이미지를 쉽게 저장, 실행 및 관리할 수 있도록 합니다. 고객이 작업 정의에서 Amazon ECR 리포지토리를 지정한 후 Amazon ECS는 애플리케이션에 적합한 이미지를 검색합니다.

PHI가 포함된 컨테이너 이미지에 Amazon ECR을 사용하는 데는 특별한 단계가 필요하지 않습니다. 컨테이너 이미지는 Amazon S3 서버 측 암호화 (SSE-S3) 를 사용하여 전송 중에 암호화되고 저장 중에는 암호화되어 저장됩니다.

## Amazon Elastic Container Service

Amazon Elastic Container Service (Amazon ECS) 는 Docker 컨테이너를 지원하고 고객이 Amazon EC2 인스턴스의 관리형 클러스터에서 애플리케이션을 쉽게 실행할 수 있도록 하는 확장성이 뛰어난 고성능 컨테이너 관리 서비스입니다. Amazon ECS를 사용하면 고객이 자체 클러스터 관리 인프라를 설치, 운영 및 확장할 필요가 없습니다.

간단한 API 호출을 통해 고객은 Docker 지원 애플리케이션을 시작 및 중지하고, 클러스터의 전체 상태를 쿼리하고, 보안 그룹, Elastic Load Balancing, EBS 볼륨 및 IAM 역할과 같은 많은 친숙한 기능에 액세스할 수 있습니다. 고객은 Amazon ECS를 사용하여 리소스 요구 사항 및 가용성 요구 사항에 따라 클러스터 전체에 컨테이너를 배치하도록 예약할 수 있습니다.

PHI를 처리하는 워크로드와 함께 ECS를 사용하면 추가 구성이 필요하지 않습니다. ECS는 EC2에서 컨테이너 (S3에 저장된 이미지) 의 시작을 조정하는 오케스트레이션 서비스 역할을 하며, 오케스트레이션되는 워크로드 내의 데이터와 함께 또는 그 이후에 작동하지 않습니다. HIPAA 규정 및 AWS 비즈니스 제휴 부록에 따라, ECS로 출시된 컨테이너를 통해 PHI를 액세스할 경우 전송 중이거나 유휴 상태에서 PHI를 암호화해야 합니다. 저장 시 암호화를 위한 다양한 메커니즘은 각 AWS 스토리지 옵션 (예: S3, EBS, KMS) 에서 사용할 수 있습니다. 컨테이너 간에 전송되는 PHI를 완전히 암호화하면 고객이 중복 암호화 계층을 제공하기 위해 오버레이 네트워크 (예: VNS3, Weave Net 등) 를 배포해야 할 수도 있습니다. 그럼에도 불구하고 전체 로깅도 활성화 (예: 통해 CloudTrail) 해야 하며 모든 컨테이너 인스턴스 로그를 대상으로 보내야 합니다. CloudWatch

PHI를 처리하는 워크로드와 함께 Firelens와 Fluent Bit를 사용하면 로그에 PHI가 포함되어 있지 않는 한 추가 구성이 필요하지 않습니다. AWS 로그에 PHI가 포함된 경우 디스크 암호화가 활성화되어 있지 않는 한 PHI를 로그 파일로 내보내면 안 됩니다. 대신 에서 자동으로 수집되는 로그를 표준 출력/오류로 내보내도록 애플리케이션을 구성하십시오. FireLens 마찬가지로 디스크 암호화가 활성화되어 있지 않는 한 Fluent Bit에 대한 파일 버퍼링을 활성화하지 마십시오. 마지막으로 로그 대상이 지원해야 합니다 encryption-in-transit. Fluent Bit용 AWS의 모든 AWS 서비스 출력 플러그인은 항상 TLS 암호화를 사용하여 로그를 내보냅니다.

## Amazon Elastic File System(Amazon EFS)

Amazon Elastic File System (Amazon EFS) 은 AWS 클라우드 서비스 및 온프레미스 리소스와 함께 사용할 수 있는 단순하고 확장 가능하며 탄력적인 파일 스토리지를 제공합니다. 사용이 간편하며 고객이

파일 시스템을 빠르고 쉽게 생성하고 구성할 수 있는 간단한 인터페이스를 제공합니다. Amazon EFS는 애플리케이션을 중단하지 않고 필요에 따라 탄력적으로 확장할 수 있도록 구축되었으며, 고객이 파일을 추가하고 제거함에 따라 자동으로 확장 및 축소됩니다.

저장 시 PHI를 암호화해야 한다는 요구 사항을 충족하기 위해 EFS에서는 두 가지 경로를 사용할 수 있습니다. EFS는 새 파일 시스템 생성 시 저장 시 암호화를 지원합니다. 생성 시 "저장된 데이터 암호화 활성화" 옵션을 선택해야 합니다. 이 옵션을 선택하면 EFS 파일 시스템에 있는 모든 데이터가 AES-256 암호화 및 AWS KMS관리 키를 사용하여 암호화됩니다. 고객은 EFS에 데이터를 저장하기 전에 암호화할 수도 있지만, 이때 암호화 프로세스 및 키 관리를 관리할 책임은 고객에게 있습니다.

PHI를 파일 이름 또는 폴더 이름의 전체 또는 일부로 사용해서는 안 됩니다. EFS 서비스와 파일 시스템을 마운트하는 인스턴스 간의 전송 계층 보안 (TLS) 을 통해 Amazon EFS로 전송 중인 PHI를 암호화합니다. EFS는 TLS를 사용하여 파일 시스템에 쉽게 연결할 수 있는 마운트 도우미를 제공합니다. 기본적으로 TLS는 사용되지 않으며 EFS 마운트 도우미를 사용하여 파일 시스템을 마운트할 때 활성화해야 합니다. mount 명령에 TLS 암호화를 활성화하는 "-o tls" 옵션이 포함되어 있는지 확인하십시오. 또는 EFS 마운트 도우미를 사용하지 않기로 선택한 고객은 EFS 설명서의 지침에 따라 TLS 터널을 통해 연결하도록 NFS 클라이언트를 구성할 수 있습니다.

## Amazon Elastic Kubernetes Service(Amazon EKS)

Amazon Elastic Kubernetes Service (Amazon EKS) 는 고객이 자체 쿠버네티스 컨트롤 플레인을 설치하거나 유지 관리할 필요 없이 AWS에서 쉽게 쿠버네티스를 실행할 수 있게 해주는 관리형 서비스입니다. Kubernetes는 컨테이너화된 애플리케이션의 배포, 조정 및 관리 자동화를 위한 오픈 소스 시스템입니다. 추가 보안 및 규정 준수 정보는 Amazon EKS의 HIPAA 보안 및 규정 준수를 위한 아키텍처 설계 백서를 참조하십시오.

## 아마존 포 ElastiCache 레디스용

Amazon ElastiCache for Redis는 데이터 저장소 또는 캐시로 사용할 수 있는 Redis와 호환되는 인메모리 데이터 구조 서비스입니다. PHI를 저장하려면 고객은 Redis 엔진에 ElastiCache 적합한 최신 HIPAA 호환 버전과 현재 세대 노드 유형을 실행하고 있는지 확인해야 합니다. Amazon ElastiCache for Redis는 다음 노드 유형 및 Redis 엔진 버전에 대한 PHI 저장을 지원합니다.

- 노드 유형: 현재 세대 전용 (예: 본 백서 발행 시점을 기준으로 M4, M5, R4, R5, T2, T3)
- ElastiCache 레디스 엔진 버전의 경우: 3.2.6 및 4.0.10 이상

현재 세대 노드 선택에 대한 자세한 내용은 Amazon ElastiCache 요금을 참조하십시오. Redis 엔진 선택에 대한 자세한 내용은 ElastiCache ElastiCache Redis용 Amazon이란 무엇입니까? 를 참조하십시오.

또한 고객은 클러스터 및 클러스터 내 노드가 저장된 데이터를 암호화하고, 전송 암호화를 활성화하고, Redis 명령 인증을 활성화하도록 구성되었는지 확인해야 합니다. 또한 고객은 항상 '권장 적용 날짜' (업데이트 적용 권장 날짜) 또는 그 이전에 최신 '보안' 유형 서비스 업데이트로 Redis 클러스터를 업데이트해야 합니다. 자세한 내용은 아래의 섹션을 참조하십시오.

주제

- 유휴 데이터 암호화
- 전송 데이터 암호화
- 인증
- 서비스 업데이트 적용 ElastiCache

## 유휴 데이터 암호화

Amazon ElastiCache for Redis는 클러스터에 데이터 암호화를 제공하여 저장된 데이터를 보호하는 데 도움이 됩니다. 고객이 클러스터를 생성할 때 미사용 암호화를 활성화하면 Amazon ElastiCache for Redis는 디스크의 데이터와 자동화된 Redis 백업을 암호화합니다. 디스크에 있는 고객 데이터는 하드웨어 가속 고급 암호화 표준 (AES) -512 대칭 키를 사용하여 암호화됩니다. Redis 백업은 Amazon S3에서 관리하는 암호화 키 (SSE-S3) 를 통해 암호화됩니다. 서버 측 암호화가 활성화된 S3 버킷은 데이터를 버킷에 저장하기 전에 하드웨어 가속 고급 암호화 표준 (AES) -256개의 대칭 키를 사용하여 암호화합니다.

Amazon S3에서 관리하는 암호화 키 (SSE-S3) 에 대한 자세한 내용은 Amazon S3 관리형 암호화 키 (SSE-S3) 를 사용한 서버 측 암호화를 사용한 데이터 보호를 참조하십시오. 암호화를 사용하여 실행되는 ElastiCache Redis 클러스터 (단일 또는 다중 노드) 에서 저장된 데이터는 본 백서 발행 당시 유효한 지침에 따라 암호화됩니다. 여기에는 디스크에 있는 데이터와 S3 버킷의 자동 백업이 포함됩니다. 지침이 업데이트될 수 있으므로 고객은 Amazon ElastiCache for Redis 암호화가 규정 준수 및 규제 요구 사항을 충족하는지 계속 평가하고 결정해야 합니다. Redis용 Amazon을 사용한 저장 중 암호화에 대한 자세한 내용은 ElastiCache Redis용 Amazon이란 무엇입니까? ElastiCache 를 참조하십시오.

## 전송 데이터 암호화

Amazon ElastiCache for Redis는 TLS를 사용하여 전송 중인 데이터를 암호화합니다. PHI를 포함하는 ElastiCache Redis용 연결은 전송 암호화를 사용하고 지침과의 일관성을 위해 구성을 평가해야 합니

다. 자세한 내용은 을 참조하십시오. CreateReplicationGroup 전송 암호화를 활성화하는 방법에 대한 자세한 내용은 Redis 전송 중 암호화 (TLS) 를 참조하십시오ElastiCache .

## 인증

PHI를 포함하는 Amazon ElastiCache for Redis 클러스터 (단일/다중 노드) 는 Redis 명령 인증을 활성화하기 위해 Redis 인증 토큰을 제공해야 합니다. Redis 인증은 저장 중 암호화와 전송 중 암호화가 모두 활성화된 경우 사용할 수 있습니다. 고객은 Redis AUTH를 위한 강력한 토큰을 제공해야 하며 다음과 같은 제약 조건이 적용됩니다.

- 인쇄 가능한 ASCII 문자만 사용할 수 있어야 합니다.
- 16자 이상, 128자 이하여야 합니다.
- '/', "" 또는 “@” 문자는 포함할 수 없습니다.

이 토큰은 Redis 복제 그룹 (단일/다중 노드) 생성 시 요청 매개변수 내에서 설정해야 하며 나중에 새 값으로 업데이트할 수 있습니다. AWS는 AWS Key Management Service (AWS KMS) 를 사용하여 이 토큰을 암호화합니다. Redis AUTH에 대한 자세한 내용은 Redis 전송 중 암호화 (TLS) ElastiCache 를 참조하십시오.

## 서비스 업데이트 적용 ElastiCache

PHI를 포함하는 Amazon ElastiCache for Redis 클러스터 (단일/다중 노드) 는 '권장 날짜 적용' 당일 또는 그 이전에 최신 '보안' 유형 서비스 업데이트로 업데이트해야 합니다. ElastiCache 이를 고객이 필요할 때 언제든지 실시간으로 업데이트를 적용하는 데 사용할 수 있는 셀프 서비스 기능으로 제공합니다. 각 서비스 업데이트는 '심각도' 및 '날짜별 권장 적용'과 함께 제공되며 해당 Redis 복제 그룹에만 사용할 수 있습니다.

서비스 업데이트 기능의 'SLA Met' 필드에는 업데이트가 '날짜별 권장 적용' 당일 또는 이전에 적용되었는지 여부가 표시됩니다. 고객이 '날짜별 권장 적용'까지 해당 Redis 복제 그룹에 업데이트를 적용하지 않기로 선택하면 업데이트를 적용하기 위한 어떠한 조치도 취하지 않습니다. ElastiCache 고객은 서비스 업데이트 기록 대시보드를 사용하여 시간이 지남에 따라 Redis 복제 그룹에 적용된 업데이트를 검토할 수 있습니다. 이 기능을 사용하는 방법에 대한 자세한 내용은 ElastiCacheAmazon의 셀프 서비스 업데이트를 참조하십시오.

# 아마존 OpenSearch 서비스

아마존 OpenSearch 서비스를 통해 고객은 전용 아마존 가상 사설 클라우드 (Amazon VPC) 에서 관리형 OpenSearch 또는 레거시 Elasticsearch OSS 클러스터를 실행할 수 있습니다. PHI와 함께

OpenSearch 서비스를 사용할 경우 고객은 Elasticsearch 6.0 OpenSearch 이상을 사용해야 합니다. 고객은 Amazon Service 내에서 PHI가 저장 중이거나 전송 중에 암호화되도록 해야 합니다. OpenSearch 고객은 AWS KMS 키 암호화를 사용하여 OpenSearch 서비스 도메인에 저장된 데이터를 암호화할 수 있으며, 이는 Elasticsearch 5.1 이상에서만 사용할 OpenSearch 수 있습니다. 저장된 데이터를 암호화하는 방법에 대한 자세한 내용은 Amazon OpenSearch Service의 미사용 데이터 암호화를 참조하십시오.

각 OpenSearch 서비스 도메인은 자체 VPC에서 실행됩니다. 고객은 모든 OpenSearch 버전과 Elasticsearch 6.0 이상에서 사용할 수 있는 node-to-node 암호화를 활성화해야 합니다. 고객이 HTTPS를 통해 OpenSearch Service에 데이터를 보내는 경우 node-to-node 암호화를 통해 클러스터 전체에 데이터를 OpenSearch 배포 (및 재배포) 할 때 데이터가 암호화된 상태로 유지되도록 할 수 있습니다. 데이터가 HTTP를 통해 암호화되지 않은 상태로 도착하는 경우, OpenSearch 서비스는 데이터가 클러스터에 도달한 후 데이터를 암호화합니다. 따라서 Amazon OpenSearch 서비스 클러스터에 들어오는 모든 PHI는 HTTPS를 통해 전송되어야 합니다. 자세한 내용은 Amazon OpenSearch 서비스를 위한 Node-to-node 암호화를 참조하십시오.

OpenSearch 서비스 구성 API의 로그를 캡처할 수 AWS CloudTrail있습니다. 자세한 내용은 Amazon OpenSearch 서비스 API 호출 모니터링을 참조하십시오 AWS CloudTrail.

## Amazon EMR

Amazon EMR은 Amazon EC2 인스턴스 클러스터를 고객 계정에 배포하고 관리합니다. Amazon EMR을 사용한 암호화에 대한 자세한 내용은 암호화 옵션을 참조하십시오.

## 아마존 EventBridge

Amazon EventBridge (이전 명칭 Amazon CloudWatch Events) 은 확장 가능한 이벤트 기반 애플리케이션을 만들 수 있는 서버리스 이벤트 버스입니다. EventBridge Zendesk, Datadog 또는 Pagerduty 같은 이벤트 소스로부터 실시간 데이터 스트림을 전달하고 해당 데이터를 다음과 같은 대상으로 라우팅합니다. AWS Lambda

기본적으로 AWS 소유의 CMK에 따른 256비트 고급 암호화 표준 (AES-256) 을 사용하여 데이터를 EventBridge 암호화하며, 이는 무단 액세스로부터 고객 데이터를 보호하는 데 도움이 됩니다. 고객은 PHI를 저장, 처리 또는 전송하는 이벤트를 내보내는 모든 AWS 리소스가 모범 사례에 따라 구성되었는지 확인해야 합니다.

EventBridge Amazon은 AWS CloudTrail Amazon과 통합되어 있으며 고객은 CloudTrail 콘솔의 이벤트 기록에서 가장 최근 이벤트를 볼 수 있습니다. 자세한 내용은 의 EventBridge 정보를 참조하십시오 CloudTrail.

# Amazon Forecast

Amazon Forecast는 기계 학습을 사용하여 매우 정확한 예측을 제공하는 완전 관리형 서비스입니다. Amazon.com에서 사용하는 것과 동일한 기계 학습 예측 기술을 기반으로 합니다. 고객이 Amazon Forecast와 하는 모든 상호 작용은 암호화로 보호됩니다. Amazon Forecast에서 처리하는 모든 콘텐츠는 Amazon 키 관리 서비스를 통해 고객 키로 암호화되고, 고객이 서비스를 사용하는 AWS 리전에서는 저장 시 암호화됩니다.

Amazon Forecast는 Amazon Forecast에서 사용자, 역할 또는 AWS 서비스가 수행한 작업의 기록을 제공하는 서비스와 통합되어 있습니다. AWS CloudTrail CloudTrail Amazon Forecast에 대한 모든 API 호출을 이벤트로 캡처합니다. 캡처된 호출에는 Amazon Forecast 콘솔에서의 호출과 Amazon Forecast API 작업에 대한 코드 호출이 포함됩니다. 고객이 트레일을 생성하는 경우, 고객은 Amazon Forecast에 대한 CloudTrail 이벤트를 포함하여 Amazon S3 버킷으로 이벤트를 지속적으로 전송할 수 있습니다. 자세한 내용은 Forecast API 호출 로깅을 참조하십시오 AWS CloudTrail.

기본적으로 버킷으로 전송되는 로그 파일은 Amazon S3에서 관리하는 암호화 키 (SSE-S3) 를 사용한 Amazon 서버 측 암호화로 암호화됩니다. CloudTrail 고객은 직접 관리할 수 있는 보안 계층을 제공하기 위해 대신 로그 파일에 AWS KMS—Managed KMS (관리 키) 를 사용한 서버 측 암호화를 사용할 수 있습니다. CloudTrail 서버 측 암호화를 활성화하면 SSE-KMS를 사용하여 로그 파일이 암호화되지만 다이제스트 파일은 암호화되지 않습니다. 다이제스트 파일은 Amazon S3 관리형 암호화 키(SSE-S3)를 사용하여 암호화됩니다.

AWS Forecast는 S3 버킷으로 데이터를 가져오거나 S3 버킷에서 데이터를 내보냅니다. Amazon S3에서 데이터를 가져오고 내보낼 때 고객은 지침과 일치하는 방식으로 S3 버킷을 구성해야 합니다. 자세한 내용은 시작하기를 참조하십시오.

# Amazon FSx

Amazon FSx는 기능이 풍부하고 성능이 뛰어난 파일 시스템을 제공하는 완전 관리형 서비스입니다. Windows File Server용 Amazon FSx는 매우 안정적이고 확장 가능한 파일 스토리지를 제공하며 서버 메시지 블록 (SMB) 프로토콜을 통해 액세스할 수 있습니다. Amazon FSx for Lustre는 컴퓨팅 워크로드를 위한 고성능 스토리지를 제공하며, 세계에서 가장 인기 있는 고성능 파일 시스템인 Lustre를 기반으로 합니다.

Amazon FSx는 파일 시스템에 대해 두 가지 형태의 암호화, 즉 전송 데이터 암호화와 저장 데이터 암호화를 지원합니다. Windows용 Amazon FSx 파일 서버에서는 를 사용하여 모든 API 호출에 대한 로깅도 지원합니다. AWS CloudTrail

전송 중인 데이터의 암호화는 SMB 프로토콜 3.0 이상을 지원하는 컴퓨팅 인스턴스에서는 Windows File Server용 Amazon FSx에서, 전송 중 암호화를 지원하는 Amazon EC2 인스턴스에서는 Amazon FSx for Lustre에서 지원합니다. 또는 고객이 Amazon FSx에 데이터를 저장하기 전에 암호화할 수도 있지만, 이때 암호화 프로세스 및 키 관리에 대한 책임은 고객에게 있습니다.

Amazon FSx 파일 시스템을 생성할 때 AES-256 암호화 알고리즘 AWS KMS및 관리 키를 사용하여 저장 데이터 암호화가 자동으로 활성화됩니다. 데이터와 메타데이터는 파일 시스템에 기록되기 전에 자동으로 암호화되고 애플리케이션에 제공되기 전에 자동으로 해독됩니다. 파일 또는 폴더 이름에는 PHI를 사용해서는 안 됩니다.

## 아마존 GuardDuty

GuardDuty Amazon은 악의적 또는 무단 행동을 지속적으로 모니터링하여 고객이 AWS 계정과 워크로드를 보호할 수 있도록 지원하는 관리형 위협 탐지 서비스입니다. 비정상적인 API 호출 또는 계정 손상 가능성을 나타내는 잠재적 무단 배포와 같은 활동을 모니터링합니다. Amazon은 GuardDuty 또한 잠재적으로 손상된 인스턴스 또는 공격자의 정찰을 탐지합니다.

Amazon은 VPC 흐름 로그, AWS CloudTrail 이벤트 로그, DNS 로그와 같은 데이터 소스를 GuardDuty 지속적으로 모니터링하고 분석합니다. 악성 IP 및 도메인 목록과 같은 위협 인텔리전스 피드와 기계 학습을 사용하여 AWS 환경 내에서 예상치 못한 잠재적 무단 및 악의적인 활동을 식별합니다. 따라서 Amazon은 PHI를 GuardDuty 발견해서는 안 됩니다. 이 데이터는 위에 나열된 AWS 기반 데이터 소스에 저장되지 않기 때문입니다.

## 아마존 HealthLake

Amazon은 의료 및 생명과학 산업의 고객이 페타바이트 규모로 의료 데이터를 저장, 변환, 쿼리 및 분석할 수 HealthLake 있도록 지원합니다. 고객은 HealthLake Amazon을 사용하여 PHI를 전송, 처리 및 저장할 수 있습니다. Amazon은 기본적으로 고객 데이터 스토어에 저장된 데이터를 HealthLake 암호화합니다. 모든 서비스 데이터와 메타데이터는 서비스 소유의 KMS 키로 암호화됩니다. Fast Healthcare 상호 운용성 리소스 (FHIR) 사양에 따라 고객이 FHIR 리소스를 삭제하면 해당 리소스는 검색되지 않도록 숨겨지고 서비스에서 버전 관리를 위해 보관합니다. 고객이 StartFhir API를 ImportJob 사용하는 경우 HealthLake Amazon은 데이터를 암호화된 Amazon S3 버킷으로 내보내도록 요구합니다.

Amazon은 전송 중인 데이터와 저장된 데이터를 모두 HealthLake 암호화합니다. 전송 중인 데이터를 암호화하기 위해 AWS에 게시된 API 호출을 사용하여 네트워크를 HealthLake 통해 액세스할 수 있습니다. 클라이언트가 전송 계층 보안(TLS) 1.0 이상을 지원해야 합니다. TLS 1.2는 필수이며 TLS 1.3

을 권장합니다. 클라이언트는 Ephemeral Diffie-Hellman(DHE) 또는 Elliptic Curve Ephemeral Diffie-Hellman(ECDHE)과 같은 PFS(전달 완전 보안, Perfect Forward Secrecy)가 포함된 암호 제품군도 지원해야 합니다. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다. 또한 요청은 액세스 키 ID 및 IAM 주체와 관련된 비밀 액세스 키를 사용하여 서명해야 합니다. 또는 고객은 AWS Security Token Service (AWS STS) 를 사용하여 요청에 서명하기 위한 임시 보안 자격 증명을 생성할 수 있습니다. 저장된 데이터의 암호화를 위해 Amazon은 기본적으로 고객 소유의 AWS KMS 키 또는 서비스 소유의 AWS KMS 키를 사용하여 고객 데이터 스토어의 데이터를 HealthLake 암호화합니다. 모든 서비스 데이터와 메타데이터는 서비스 소유의 AWS KMS 키를 사용하여 유휴 상태에서 암호화됩니다.

HealthLake Amazon은 과 통합되어 AWS CloudTrail있습니다. CloudTrail 명령줄 인터페이스 (CLI) 및 소프트웨어 개발 키트 (SDK) 를 사용한 프로그래밍 방식으로 이루어진 호출을 포함하여 Amazon에 대한 모든 API 호출을 HealthLake 이벤트로 캡처합니다. AWS Management Console

## Amazon Inspector

Amazon Inspector는 AWS에 배포된 애플리케이션의 보안 및 규정 준수를 개선하고자 하는 고객을 위한 자동 보안 평가 서비스입니다. Amazon Inspector는 자동으로 애플리케이션의 취약점 또는 모범 사례와의 차이를 평가합니다. 평가를 수행한 후 Amazon Inspector는 심각도 수준에 따라 우선 순위가 지정된 보안 조사 결과의 세부 목록을 생성합니다. 고객은 PHI를 포함하는 EC2 인스턴스에서 Amazon Inspector를 실행할 수 있습니다. Amazon Inspector는 네트워크를 통해 전송되는 모든 데이터와 미사용 상태로 저장된 모든 텔레메트리 데이터를 암호화합니다.

## Amazon Managed Service for Apache Flink

Apache Flink용 Amazon 관리형 서비스를 사용하면 고객이 거의 실시간으로 데이터를 지속적으로 읽고, 처리하고, 저장하는 SQL 코드를 빠르게 작성할 수 있습니다. 스트리밍 데이터에 대한 표준 SQL 쿼리를 사용하여 고객은 데이터를 변환하고 이에 대한 통찰력을 제공하는 애플리케이션을 구축할 수 있습니다. Apache Flink용 관리형 서비스는 Kinesis Data Streams 및 Firehose 전송 스트림의 입력을 분석 애플리케이션의 소스로 지원합니다. 스트림이 암호화된 경우 Apache Flink용 관리형 서비스는 추가 구성 없이 암호화된 스트림의 데이터에 원활하게 액세스합니다. Apache Flink용 관리형 서비스는 Kinesis Data Streams에서 읽은 암호화되지 않은 데이터를 저장하지 않습니다. 자세한 설명은 애플리케이션 입력 구성을 참조하십시오.

Apache Flink용 관리형 서비스는 애플리케이션 모니터링을 위해 AWS CloudTrail Amazon CloudWatch Logs와 둘 다 통합됩니다. 자세한 내용은 모니터링 도구 및 Amazon CloudWatch Logs 사용을 참조하십시오.

# Amazon Data Firehose

고객이 데이터 생산자의 데이터를 Kinesis 데이터 스트림으로 보내면 Amazon Kinesis Data Streams는 데이터를 유휴 상태로 저장하기 전에 AWS KMS 키를 사용하여 데이터를 암호화합니다. Firehose 전송 스트림이 Kinesis 스트림에서 데이터를 읽으면 Kinesis 데이터 스트림은 먼저 데이터를 복호화한 다음 Firehose로 전송합니다. Firehose는 고객이 지정한 버퍼링 힌트를 기반으로 메모리의 데이터를 버퍼링합니다.

그런 다음 암호화되지 않은 데이터를 유휴 상태로 저장하지 않고 목적지로 데이터를 전송합니다. Firehose를 사용한 암호화에 대한 자세한 내용은 Amazon Data Firehose의 데이터 보호를 참조하십시오.

AWS는 Amazon CloudWatch 지표, Amazon CloudWatch Logs, Kinesis Agent, API 로깅 및 기록을 포함하여 고객이 Amazon Data Firehose를 모니터링하는 데 사용할 수 있는 다양한 도구를 제공합니다. 자세한 내용은 Amazon 데이터 Firehose 모니터링을 참조하십시오.

# Amazon Kinesis Streams

Amazon Kinesis Streams를 사용하면 고객이 특수한 요구 사항에 맞게 스트리밍 데이터를 처리하거나 분석하는 사용자 지정 애플리케이션을 구축할 수 있습니다. 서버 측 암호화 기능을 통해 고객은 저장된 데이터를 암호화할 수 있습니다. 서버 측 암호화가 활성화되면 Kinesis Streams는 데이터를 디스크에 저장하기 전에 AWS KMS 키를 사용하여 데이터를 암호화합니다. 자세한 내용은 Amazon Kinesis Data Streams의 데이터 보호를 참조하세요. PHI를 포함하는 Amazon S3에 대한 연결은 암호화된 전송(즉, HTTPS) 을 허용하는 엔드포인트를 사용해야 합니다. 리전 엔드포인트 목록은 AWS 서비스 엔드포인트를 참조하십시오.

# Amazon Kinesis Video Streams

Amazon Kinesis Video Streams는 고객이 디바이스에서 AWS 클라우드로 라이브 비디오를 스트리밍하거나 실시간 비디오 처리 또는 배치 지향 비디오 분석을 위한 애플리케이션을 구축하는 데 사용할 수 있는 완전 관리형 AWS 서비스입니다. 서버 측 암호화는 고객이 지정한 AWS KMS 키 (이전 명칭 CMK) 를 사용하여 저장된 데이터를 자동으로 암호화하는 Kinesis Video Streams의 기능입니다. 데이터는 Kinesis Video Streams 스트림 스토리지 계층에 기록되기 전에 암호화되고 스토리지에서 검색된 후에 복호화됩니다.

Amazon Kinesis Video Streams SDK는 PHI를 포함하는 스트리밍 비디오 데이터를 전송하는 데 사용할 수 있습니다. 기본적으로 SDK는 TLS를 사용하여 설치된 하드웨어 디바이스에서 생성된 프레임

과 프래그먼트를 암호화합니다. SDK는 저장된 데이터를 관리하거나 영향을 주지 않습니다. Amazon Kinesis Video Streams는 모든 API 호출을 기록하는 데 AWS CloudTrail 사용합니다.

## Amazon Lex

Amazon Lex는 음성 및 텍스트를 사용하는 애플리케이션에 대화형 인터페이스를 구축하기 위한 AWS 서비스입니다. Amazon Lex를 사용하면 Amazon Alexa를 지원하는 것과 동일한 대화형 엔진을 이제 모든 개발자가 사용할 수 있으므로 고객은 새로운 애플리케이션과 기존 애플리케이션에 정교한 자연어 챗봇을 구축할 수 있습니다. Amazon Lex는 자연어 이해 (NLU) 및 자동 음성 인식 (ASR) 의 심층적인 기능과 유연성을 제공하므로 고객은 실제와 같은 대화형 상호 작용을 통해 매우 매력적인 사용자 경험을 구축하고 새로운 범주의 제품을 만들 수 있습니다.

Lex는 HTTPS 프로토콜을 사용하여 클라이언트는 물론 다른 AWS 서비스와 통신합니다. Lex에 대한 액세스는 API 기반이며 적절한 IAM 최소 권한을 적용할 수 있습니다. 자세한 내용은 Amazon Lex의 데이터 보호를 참조하십시오.

모니터링은 고객 Amazon Lex 챗봇의 안정성, 가용성 및 성능을 유지하는 데 중요합니다. Amazon Lex 봇의 상태를 추적하려면 CloudWatch Amazon을 사용하십시오. 를 통해 CloudWatch 고객은 개별 Amazon Lex 운영 또는 계정에 대한 글로벌 Amazon Lex 운영에 대한 지표를 얻을 수 있습니다. 또한 고객은 하나 이상의 지표가 고객이 정의한 임계값을 초과할 때 알림을 받도록 CloudWatch 경보를 설정할 수 있습니다. 예를 들어 고객은 특정 기간 동안 봇에 이루어진 요청 수를 모니터링하거나, 성공적인 요청의 대기 시간을 확인하거나, 오류가 임계값을 초과할 경우 경보를 울릴 수 있습니다. Lex는 Lex API 호출을 AWS CloudTrail 기록하는 데도 통합되어 있습니다. 자세한 내용은 Amazon Lex에서의 모니터링을 참조하십시오.

## Amazon Managed Streaming for Apache Kafka(Amazon MSK)

Amazon MSK는 저장된 데이터와 전송 중인 데이터에 대한 암호화 기능을 제공합니다. 저장 데이터 암호화의 경우 Amazon MSK 클러스터는 Amazon EBS 서버 측 암호화와 AWS KMS 키를 사용하여 스토리지 볼륨을 암호화합니다. 전송 중인 데이터의 경우 Amazon MSK 클러스터에는 브로커 간 통신을 위해 TLS를 통한 암호화가 활성화되어 있습니다.

클러스터가 생성되면 암호화 구성 설정이 활성화됩니다. 또한 CLI 또는 Console에서 생성된 클러스터의 경우 기본적으로 전송 중 암호화가 TLS로 설정됩니다. AWS 클라이언트가 TLS 암호화를 사용하여 클러스터와 통신하려면 추가 구성이 필요합니다. 고객은 TLS/일반 텍스트 설정을 선택하여 기본 암호화 설정을 변경할 수 있습니다. 자세한 내용은 Amazon MSK 암호화를 참조하십시오.

고객은 Amazon MSK 콘솔 또는 Amazon 콘솔을 사용하여 고객 클러스터의 성능을 모니터링하거나, 오픈 소스 모니터링 솔루션인 Prometheus의 개방형 모니터링을 사용하여 JMX 및 호스트 지표에 액세스할 수 있습니다. CloudWatch

Prometheus 익스포터로부터 읽을 수 있도록 설계된 도구는 데이터독, 렌즈, 뉴렐릭, 수몰로직 또는 프로메테우스 서버와 같은 개방형 모니터링과 호환됩니다. 공개 모니터링에 대한 자세한 내용은 Amazon MSK 공개 모니터링 설명서를 참조하십시오.

Apache Kafka와 함께 번들로 제공되는 Apache Zookeeper의 기본 버전은 암호화를 지원하지 않는다는 점에 유의하십시오. 하지만 Apache Zookeeper와 Apache Kafka 브로커 간의 통신은 브로커, 주제 및 파티션 상태 정보로만 제한된다는 점에 유의하십시오. Amazon MSK 클러스터에서 데이터를 생성하고 사용할 수 있는 유일한 방법은 VPC에 있는 클라이언트와 Amazon MSK 클러스터 간의 프라이빗 연결을 통해서입니다. Amazon MSK는 퍼블릭 엔드포인트를 지원하지 않습니다.

## Amazon MQ

Amazon MQ는 Apache ActiveMQ용 관리형 메시지 브로커 서비스로, 클라우드에서 메시지 브로커를 쉽게 설정하고 운영할 수 있게 해줍니다. Amazon MQ는 고객이 자체 메시징 시스템을 관리, 운영 또는 유지할 필요 없이 기존 애플리케이션 및 서비스와 함께 작동합니다. 전송 중에 PHI 데이터를 암호화하려면 TLS가 활성화된 다음 프로토콜을 사용하여 브로커에 액세스해야 합니다.

- AMQP
- MQTT
- MQTT 오버 WebSocket
- OpenWire
- STOMP
- 스톰프 오버 WebSocket

Amazon MQ는 안전하게 관리하고 저장하는 암호화 키를 사용하여 미사용 및 전송 중인 메시지를 암호화합니다. Amazon MQ는 모든 API 호출을 CloudTrail 기록하는 데 사용합니다.

## Amazon Neptune

Amazon Neptune은 빠르고 안정적인 종합 관리형 그래프 데이터베이스 서비스로, 고도로 연결된 데이터 세트를 사용하는 애플리케이션을 쉽게 빌드하고 실행할 수 있습니다. Amazon Neptune의 핵심은 수십억 개의 관계를 저장하고 밀리초의 지연 시간으로 그래프를 쿼리하도록 최적화된 특수 목적

의 고성능 그래프 데이터베이스 엔진입니다. Amazon Neptune은 널리 사용되는 그래프 쿼리 언어인 TinkerPop 아파치 그렘린과 W3C의 SPARQL을 지원합니다.

이제 PHI를 포함하는 데이터를 Amazon Neptune의 암호화된 인스턴스에 보관할 수 있습니다. Amazon Neptune 콘솔에서 '암호화 활성화'를 선택하여 생성 시에만 Amazon Neptune의 암호화된 인스턴스를 지정할 수 있습니다. Amazon Neptune 암호화 인스턴스의 경우 모든 로그, 백업 및 스냅샷이 암호화됩니다. Amazon Neptune의 암호화된 인스턴스에 대한 키 관리는 를 통해 제공됩니다. AWS KMS전송 중인 데이터의 암호화는 SSL/TLS를 통해 제공됩니다. Amazon Neptune은 모든 API 호출을 기록하는 데 CloudTrail 사용합니다.

## AWS 네트워크 방화벽

AWS Network Firewall은 모든 Amazon Virtual Private Cloud (Amazon VPC) 에 필수적인 네트워크 보호 기능을 쉽게 배포할 수 있게 해주는 관리형 방화벽 서비스입니다. 이 서비스는 네트워크 트래픽 볼륨에 따라 자동으로 확장되므로 기본 인프라를 설정하거나 유지 관리할 필요 없이 고가용성 보호 기능을 제공합니다. 고객 규칙과 액세스 로그에는 모두 최종 사용자 IP 주소가 포함될 수 있으며, 이 주소는 아키텍처 내에서 저장 중이거나 전송 중일 때 모두 암호화됩니다. AWS 또한 AWS Network Firewall은 구성 요소 AWS 서비스 (Amazon S3, Amazon DynamoDB CloudWatch , Amazon Logs, Amazon EBS) 에 저장된 데이터와 구성 요소 서비스 간에 전송되는 모든 데이터를 암호화합니다. 이 서비스는 특별한 구성 없이 데이터를 자동으로 암호화합니다.

## Amazon Pinpoint

Amazon Pinpoint는 개발자에게 단일 API 계층, CLI 지원 및 클라이언트측 SDK 지원을 제공하여 사용자와의 애플리케이션 커뮤니케이션 채널을 확장합니다. 적격 채널에는 이메일, SMS 문자 메시지, 모바일 푸시 알림 및 사용자 지정 채널이 포함됩니다. Amazon Pinpoint는 또한 앱 사용자 행동 및 사용자 참여를 추적하는 분석 시스템을 제공합니다. 이 서비스를 통해 개발자는 각 사용자가 선호하는 참여 방식을 파악하고 사용자 경험을 개인화하여 사용자 만족도를 높일 수 있습니다.

또한 Amazon Pinpoint는 개발자가 직접 또는 트랜잭션 메시징, 대상 또는 캠페인 메시징, 이벤트 기반 메시징과 같은 여러 메시징 사용 사례를 해결할 수 있도록 지원합니다. Amazon Pinpoint를 통해 모든 최종 사용자 참여 채널을 통합하고 활성화함으로써 개발자는 모든 고객 접점에서 사용자 참여를 360도로 파악할 수 있습니다. Amazon Pinpoint는 사용자, 엔드포인트 및 이벤트 데이터를 저장하므로 고객이 세그먼트를 생성하고, 수신자에게 메시지를 보내고, 참여 데이터를 캡처할 수 있습니다.

Amazon Pinpoint는 미사용 데이터와 전송 중인 데이터를 모두 암호화합니다. 자세한 내용은 아마존 Pinpoint FAQ를 참조하십시오. Amazon Pinpoint는 저장된 데이터와 전송 중인 모든 데이터를 암호화

하지만 SMS 또는 이메일과 같은 최종 채널은 암호화되지 않을 수 있으므로 고객은 요구 사항에 맞는 방식으로 채널을 구성해야 합니다.

또한 SMS 채널을 통해 PHI를 전송해야 하는 고객은 PHI를 전송할 목적으로 전용 단축 코드 (5, 6자리 발신 전화번호) 를 사용해야 합니다. 단축 코드를 요청하는 방법에 대한 자세한 내용은 Amazon Pinpoint를 통한 SMS 메시징용 전용 단축 코드 요청을 참조하십시오. 고객은 최종 채널을 통해 PHI를 전송하지 않고 대신 HTTPS를 통해 PHI에 안전하게 액세스할 수 있는 메커니즘을 제공할 수도 있습니다.

를 사용하여 Amazon Pinpoint에 대한 API 호출을 캡처할 수 있습니다. AWS CloudTrail캡처된 호출에는 Amazon Pinpoint 콘솔에서의 호출과 Amazon Pinpoint API 작업에 대한 코드 호출이 포함됩니다. 고객이 트레일을 생성하는 경우, 고객은 Amazon Pinpoint에 대한 AWS CloudTrail 이벤트를 포함하여 Amazon S3 버킷으로 이벤트를 지속적으로 전송할 수 있습니다. 고객이 트레일을 구성하지 않아도 AWS CloudTrail 콘솔에서 이벤트 기록을 사용하여 가장 최근 이벤트를 볼 수 있습니다. 에서 수집한 AWS CloudTrail정보를 사용하여 고객은 Amazon Pinpoint에 요청이 이루어졌는지, 요청한 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다. 자세한 내용은 Amazon Pinpoint API 호출 로깅을 참조하십시오. AWS CloudTrail

## Amazon Polly

Amazon Polly는 텍스트를 생생한 스피치로 변환하는 클라우드 서비스입니다. Amazon Polly는 고객이 기존 애플리케이션과 쉽게 통합할 수 있는 간단한 API 작업을 제공합니다. Amazon Polly는 HTTPS 프로토콜을 사용하여 클라이언트와 통신합니다. Amazon Polly에 대한 액세스는 API 기반이며 적절한 IAM 최소 권한을 적용할 수 있습니다. 자세한 내용은 데이터 보호를 참조하십시오. PHI를 포함하는 몇 가지 사용 사례의 예:

- 간병인은 걷거나 다른 업무를 수행하는 동안 보고서를 들을 수 있도록 PHI가 포함된 텍스트 보고서를 합성 음성으로 변환합니다.
- 시각 장애 환자는 의학적 지침을 받고 음성 합성 형태의 안내서를 사용합니다.

Amazon Polly의 최종 전송 채널로 인해 공용 공간에서 PHI로 오디오가 재생될 수 있으므로 이러한 점을 고려하여 전송하도록 예방 조치를 취해야 합니다. 암호화가 활성화된 상태에서 합성된 음성 출력을 Amazon S3 버킷으로 비동기적으로 전송할 수도 있습니다.

Amazon Polly에서 지원되는 이벤트 활동이 발생하면 해당 활동이 이벤트 기록의 다른 AWS 서비스 AWS CloudTrail 이벤트와 함께 이벤트에 기록됩니다. Amazon Polly의 이벤트를 포함하여 고객 AWS 계정의 지속적인 이벤트 기록을 보려면 트레일을 생성하십시오. 트레일을 사용하면 CloudTrail

Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 에서 수집한 CloudTrail 정보를 사용하여 고객은 Amazon Polly에 요청한 내용, 요청한 IP 주소, 요청한 사람, 요청 시기, 추가 세부 정보를 확인할 수 있습니다.

## Amazon Quantum Ledger Database(QLDB)

Amazon QLDB는 완전관리형 원장 데이터베이스로, 중앙의 신뢰할 수 있는 기관이 소유하는 투명하고, 변경 불가능하며, 암호화 방식으로 검증 가능한 트랜잭션 로그를 제공합니다. Amazon QLDB는 모든 애플리케이션 데이터 변경을 추적하고 시간 경과에 따른 완전하고 검증 가능한 변경 기록을 유지합니다. 이제 PHI를 포함하는 데이터를 QLDB 인스턴스에 보관할 수 있습니다. 기본적으로 전송 중인 Amazon QLDB 데이터와 저장된 모든 Amazon QLDB 데이터는 암호화됩니다. 전송 중인 데이터는 TLS를 사용하여 암호화되고 저장된 데이터는 관리 키를 사용하여 AWS 암호화됩니다. 데이터 보호를 위해 고객은 AWS 계정 자격 증명을 보호하고 개별 사용자 계정 AWS Identity and Access Management (IAM) 을 설정하여 각 사용자에게 직무를 수행하는 데 필요한 권한만 부여하도록 하는 것이 좋습니다. 자세한 내용은 Amazon QLDB의 데이터 보호를 참조하십시오.

Amazon QLDB는 QLDB에서 사용자, 역할 또는 서비스가 수행한 작업의 기록을 제공하는 AWS 서비스와 AWS CloudTrail통합됩니다. CloudTrail QLDB에 대한 모든 컨트롤 플레인 API 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 QLDB 콘솔에서 수행한 호출과 QLDB API 작업에 대한 코드 호출이 포함됩니다. 고객이 트레일을 생성하면 고객은 QLDB에 대한 CloudTrail 이벤트를 포함하여 Amazon Simple Storage Service (Amazon S3) 버킷으로 이벤트를 지속적으로 전송할 수 있습니다. 고객이 트레일을 구성하지 않아도 고객은 CloudTrail 콘솔의 이벤트 기록에서 가장 최근의 이벤트를 계속 볼 수 있습니다.  에서 수집한 정보를 사용하여 고객은 QLDB에 요청한 내용 CloudTrail, 요청한 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다.

## 아마존 QuickSight

QuickSight Amazon은 고객이 데이터에서 시각화를 구축하고, 임시 분석을 수행하고, 비즈니스 통찰력을 신속하게 얻는 데 사용할 수 있는 비즈니스 분석 서비스입니다. Amazon은 강력한 인메모리 엔진 (SPICE) 을 사용하여 AWS 데이터 소스를 QuickSight 검색하고, 조직이 수십만 명의 사용자까지 확장할 수 있도록 지원하며, 응답성이 뛰어난 성능을 제공합니다.

SPICE에 저장된 미사용 데이터의 암호화를 지원하므로 고객은 Amazon QuickSight Enterprise 에디션에서만 PHI를 포함하는 데이터를 사용할 수 있습니다. 데이터 암호화는 AWS 관리 키를 사용하여 수행됩니다.

# Amazon RDS for MariaDB

MariaDB용 Amazon RDS를 사용하면 고객이 관리하는 키를 사용하여 MariaDB 데이터베이스를 암호화할 수 있습니다. AWS KMS Amazon RDS 암호화를 실행하는 데이터베이스 인스턴스에서는 자동 백업, 읽기 전용 복제본, 스냅샷과 마찬가지로 기본 스토리지에 저장된 데이터가 이 백서 발행 당시 유효한 지침에 따라 암호화됩니다.

지침이 업데이트될 수 있으므로 고객은 Amazon RDS for MariaDB 암호화가 규정 준수 및 규제 요구 사항을 충족하는지 여부를 계속 평가하고 결정해야 합니다. Amazon RDS를 사용한 저장 중 암호화에 대한 자세한 내용은 Amazon RDS 리소스 암호화를 참조하십시오.

PHI를 포함하는 MariaDB용 RDS에 대한 연결은 전송 암호화를 사용해야 합니다. 암호화된 연결을 활성화하는 방법에 대한 자세한 내용은 SSL/TLS를 사용하여 DB 인스턴스에 대한 연결 암호화를 참조하십시오.

# Amazon RDS for MySQL

MySQL용 Amazon RDS를 사용하면 고객이 관리하는 키를 사용하여 MySQL 데이터베이스를 암호화할 수 있습니다. AWS KMS Amazon RDS 암호화를 실행하는 데이터베이스 인스턴스에서는 자동 백업, 읽기 전용 복제본, 스냅샷과 마찬가지로 기본 스토리지에 저장된 데이터가 이 백서 발행 당시 유효한 지침에 따라 암호화됩니다.

지침이 업데이트될 수 있으므로 고객은 계속해서 Amazon RDS for MySQL 암호화가 규정 준수 및 규제 요구 사항을 충족하는지 여부를 평가하고 결정해야 합니다. Amazon RDS를 사용한 저장 중 암호화에 대한 자세한 내용은 Amazon RDS 리소스 암호화를 참조하십시오.

PHI를 포함하는 MySQL용 RDS에 대한 연결은 전송 암호화를 사용해야 합니다. 암호화된 연결을 활성화하는 방법에 대한 자세한 내용은 SSL/TLS를 사용하여 DB 인스턴스 연결 암호화를 참조하십시오.

# Amazon RDS for Oracle

고객은 Oracle용 Amazon RDS를 사용하여 저장 중인 PHI를 암호화하는 몇 가지 옵션을 사용할 수 있습니다. 고객은 자신이 관리하는 키를 사용하여 Oracle 데이터베이스를 암호화할 수 있습니다. AWS KMS Amazon RDS 암호화를 실행하는 데이터베이스 인스턴스에서는 자동 백업, 읽기 전용 복제본, 스냅샷과 마찬가지로 기본 스토리지에 저장된 데이터가 이 백서 발행 당시 유효한 지침에 따라 암호화됩니다.

지침이 업데이트될 수 있으므로 고객은 Amazon RDS for Oracle 암호화가 규정 준수 및 규제 요구 사항을 충족하는지 계속 평가하고 결정해야 합니다. Amazon RDS를 사용한 저장 중 암호화에 대한 자세한 내용은 Amazon RDS 리소스 암호화를 참조하십시오.

고객은 Oracle TDE (투명 데이터 암호화) 를 사용할 수도 있으며, 구성이 지침과 일치하는지 평가해야 합니다. Oracle TDE는 오라클 엔터프라이즈 에디션에서 사용할 수 있는 오라클 어드밴스드 시큐리티 옵션의 기능입니다. 이 기능은 스토리지에 데이터를 쓰기 전에 자동으로 데이터를 암호화한 뒤에 데이터를 스토리지에서 읽을 때 다시 자동으로 해독합니다. 또한 고객은 Amazon RDS Oracle TDE 키를 저장하는 AWS CloudHSM 데 사용할 수 있습니다. 자세한 내용은 다음 자료를 참조하십시오.

- 오라클용 Amazon RDS 투명한 데이터 암호화: 오라클의 투명한 데이터 암호화.
- Amazon RDS Oracle TDE 키를 저장하는 AWS CloudHSM 데 사용: 아마존 관계형 데이터베이스 서비스 (Amazon RDS) 란 무엇입니까?

PHI를 포함하는 Amazon RDS for Oracle에 연결하려면 전송 암호화를 사용해야 하며 지침과 일관성이 있는지 구성을 평가해야 합니다. 이는 Oracle 네이티브 네트워크 암호화를 사용하여 수행되며, Amazon RDS for Oracle용 옵션 그룹에서 활성화됩니다. 자세한 내용은 Oracle 네이티브 네트워크 암호화를 참조하십시오.

## Amazon RDS for PostgreSQL

PostgreSQL용 Amazon RDS를 사용하면 고객이 관리하는 키를 사용하여 PostgreSQL 데이터베이스를 암호화할 수 있습니다. AWS KMS Amazon RDS 암호화를 실행하는 데이터베이스 인스턴스에서는 자동 백업, 읽기 전용 복제본, 스냅샷과 마찬가지로 기본 스토리지에 저장된 데이터가 이 백서 발행 당시 유효한 지침에 따라 암호화됩니다.

지침이 업데이트될 수 있으므로 고객은 PostgreSQL용 Amazon RDS의 암호화가 규정 준수 및 규제 요구 사항을 충족하는지 여부를 계속 평가하고 결정해야 합니다. Amazon RDS를 사용한 저장 중 암호화에 대한 자세한 내용은 Amazon RDS 리소스 암호화를 참조하십시오.

PHI를 포함하는 PostgreSQL용 RDS에 대한 연결은 전송 암호화를 사용해야 합니다. 암호화된 연결을 활성화하는 방법에 대한 자세한 내용은 SSL/TLS를 사용하여 DB 인스턴스에 대한 연결 암호화를 참조하십시오.

## Amazon RDS for SQL Server

SQL Server용 RDS는 다음 버전 및 에디션 조합에 대한 PHI 저장을 지원합니다.

- 2008 R2 - 엔터프라이즈 에디션만 해당
- 2012년, 2014년, 2016년 - 웹, 스탠다드 및 엔터프라이즈 에디션

중요: SQL Server Express 에디션은 지원되지 않으므로 PHI 저장에 사용해서는 안 됩니다.

PHI를 저장하려면 고객은 아래에 설명된 대로 인스턴스가 저장된 데이터를 암호화하고 전송 암호화 및 감사를 활성화하도록 구성되어 있는지 확인해야 합니다.

### 유휴 데이터 암호화

고객은 자신이 관리하는 키를 사용하여 SQL Server 데이터베이스를 암호화할 수 있습니다. AWS KMS Amazon RDS 암호화를 실행하는 데이터베이스 인스턴스에서 기본 스토리지에 저장된 데이터는 자동 백업 및 스냅샷과 마찬가지로 이 백서 발행 당시 유효한 지침에 따라 암호화됩니다. 지침이 업데이트 될 수 있으므로 고객은 Amazon RDS for SQL Server 암호화가 규정 준수 및 규제 요구 사항을 충족하는지 계속 평가하고 결정해야 합니다. Amazon RDS를 사용한 저장 중 암호화에 대한 자세한 내용은 Amazon RDS 리소스 암호화를 참조하십시오.

고객이 SQL Server 엔터프라이즈 에디션을 사용하는 경우 서버 투명 데이터 암호화 (TDE) 를 대안으로 사용할 수 있습니다. 이 기능은 스토리지에 데이터를 쓰기 전에 자동으로 데이터를 암호화한 뒤에 데이터를 스토리지에서 읽을 때 다시 자동으로 해독합니다. SQL Server 투명한 데이터 암호화를 위한 RDS에 대한 자세한 내용은 SQL Server의 투명한 데이터 암호화 지원을 참조하십시오.

### 전송 데이터 암호화

PHI를 포함하는 SQL Server용 Amazon RDS에 연결하려면 SQL Server 강제 SSL에서 제공하는 전송 암호화를 사용해야 합니다. 강제 SSL은 Amazon RDS SQL Server의 파라미터 그룹 내에서 활성화됩니다. SQL Server용 RDS 강제 SSL에 대한 자세한 내용은 Microsoft SQL Server DB 인스턴스에서 SSL 사용을 참조하십시오.

### 감사

PHI를 포함하는 SQL Server용 RDS 인스턴스에는 감사가 활성화되어 있어야 합니다. Amazon RDS SQL Server의 파라미터 그룹 내에서 감사를 활성화할 수 있습니다. SQL Server용 RDS 감사에 대한 자세한 내용은 Microsoft SQL Server DB 인스턴스에 대한 규정 준수 프로그램 지원을 참조하십시오.

## Amazon Redshift

Amazon Redshift는 클러스터에 데이터베이스 암호화를 제공하여 저장된 데이터를 보호하는 데 도움이 됩니다. 고객이 클러스터 암호화를 활성화하면 Amazon Redshift는 하드웨어 가속 고급 암호화 표준

(AES) -256 대칭 키를 사용하여 백업을 포함한 모든 데이터를 암호화합니다. Amazon Redshift는 암호화를 위해 4개 티어, 키 기반 계층 구조를 사용합니다. 이러한 키는 데이터 암호화 키, 데이터베이스 키, 클러스터 키 및 KMS 키로 구성됩니다.

클러스터 키는 Amazon Redshift 클러스터에 대한 데이터베이스 키를 암호화합니다. 고객은 둘 중 하나 AWS KMS 또는 AWS CloudHSM (하드웨어 보안 모듈) 을 사용하여 클러스터 키를 관리할 수 있습니다. Amazon Redshift 미사용 암호화는 본 백서 발행 당시 유효한 지침과 일치합니다. 지침이 업데이트 될 수 있으므로 고객은 Amazon Redshift 암호화가 규정 준수 및 규제 요구 사항을 충족하는지 여부를 계속 평가하고 결정해야 합니다. 자세한 내용은 Amazon Redshift 데이터베이스 암호화를 참조하세요.

PHI를 포함하는 Amazon Redshift에 대한 연결은 전송 암호화를 사용해야 하며 고객은 지침과 일관성이 있는지 구성을 평가해야 합니다. 자세한 내용은 연결을 위한 보안 옵션 구성을 참조하세요. Amazon Redshift Spectrum을 사용하면 고객이 Amazon S3에 있는 엑사바이트 규모의 데이터에 대해 Amazon Redshift SQL 쿼리를 실행할 수 있습니다. Redshift 스펙트럼은 Amazon Redshift의 기능이므로 HIPAA BAA의 범위에도 포함됩니다.

## Amazon Rekognition

Amazon Rekognition을 사용하면 이미지 및 동영상 분석을 고객 애플리케이션에 쉽게 추가할 수 있습니다. 고객은 Amazon Rekognition API에 이미지 또는 동영상만 제공하면 서비스가 객체, 사람, 텍스트, 장면 및 활동을 식별하고 부적절한 콘텐츠를 감지할 수 있습니다. Amazon Rekognition은 또한 매우 정확한 안면 분석 및 안면 인식 기능을 제공합니다.

Amazon Rekognition은 PHI를 포함하는 이미지 또는 동영상을 사용할 수 있습니다. Amazon Rekognition은 관리형 서비스로 작동하며 데이터 처리를 위한 구성 가능한 옵션을 제공하지 않습니다. Amazon Rekognition은 BAA 약관에서 허용하는 대로만 PHI를 사용, 공개 및 유지 관리합니다. AWS 모든 데이터는 Amazon Rekognition을 통해 유휴 및 전송 중에 암호화됩니다. Amazon AWS CloudTrail Rekognition은 모든 API 호출을 기록하는 데 사용합니다.

## Amazon Route 53

Amazon Route 53는 고객에게 도메인 이름을 등록하고, 인터넷 트래픽, 고객 도메인 리소스를 라우팅하고, 해당 리소스의 상태를 확인할 수 있는 기능을 제공하는 관리형 DNS 서비스입니다. Amazon Route 53은 HIPAA 적격 서비스이지만, Amazon Route 53 내의 리소스 이름이나 태그에는 PHI를 저장해서는 안 됩니다. 이러한 데이터의 암호화는 지원되지 않기 때문입니다. 대신 Amazon Route 53을 사용하여 PHI를 전송하거나 저장하는 고객 도메인 리소스 (예: Amazon EC2에서 실행되는 웹 서버 또는 Amazon S3와 같은 스토리지) 에 대한 액세스를 제공할 수 있습니다.

# Amazon S3 Glacier

Amazon S3 Glacier는 AES 256비트 대칭 키를 사용하여 저장된 데이터를 자동으로 암호화하고 보안 프로토콜을 통해 고객 데이터를 안전하게 전송할 수 있도록 지원합니다. PHI를 포함하는 Amazon S3 Glacier에 연결하려면 암호화된 전송 (HTTPS) 을 허용하는 엔드포인트를 사용해야 합니다. 리전 엔드포인트 목록은 서비스 엔드포인트를 참조하십시오.AWS

보관 및 저장소 이름 또는 메타데이터에는 PHI를 사용하지 마십시오. 이 데이터는 Amazon S3 Glacier 서버 측 암호화를 사용하여 암호화되지 않으며 일반적으로 클라이언트 측 암호화 아키텍처에서 암호화되지 않기 때문입니다.

# Amazon S3 전송 가속화

Amazon S3 Transfer Acceleration (S3TA) 을 사용하면 고객의 클라이언트와 S3 버킷 간에 장거리 파일을 빠르고 쉽고 안전하게 전송할 수 있습니다. 전송 가속화는 전 세계에 분산된 CloudFront Amazon의 엣지 로케이션을 활용합니다. 엣지 로케이션에 도착한 데이터는 최적화된 네트워크 경로를 통해 Amazon S3로 라우팅됩니다. 고객은 AWS S3TA를 사용하여 전송된 PHI를 포함하는 모든 데이터가 전송 및 저장 중에 암호화되도록 해야 합니다. 사용 가능한 암호화 옵션을 이해하려면 Amazon S3 지침을 참조하십시오.

# 아마존 SageMaker

SageMaker Amazon은 완전 관리형 기계 학습 서비스입니다. SageMakerAmazon을 사용하면 데이터 과학자와 개발자가 기계 학습 모델을 쉽고 빠르게 구축 및 교육한 다음 프로덕션 준비가 완료된 호스팅 환경에 직접 배포할 수 있습니다. 탐색과 분석을 위해 데이터 소스에 쉽게 액세스할 수 있는 통합 Jupyter 저작 노트북 인스턴스를 제공합니다. SageMaker 또한 Amazon은 분산 환경에서 매우 큰 데이터를 효율적으로 실행하도록 최적화된 일반적인 기계 학습 알고리즘을 제공합니다.

SageMaker Amazon은 bring-your-own-algorithms 및 프레임워크에 대한 기본 지원을 통해 고객의 특정 워크플로에 맞게 조정되는 유연한 분산 교육 옵션을 제공합니다. SageMakerAmazon은 PHI를 포함하는 데이터를 운영할 자격이 있습니다. 전송 데이터 암호화는 SSL/TLS에서 제공하며 Amazon의 프런트 엔드 인터페이스 (노트북) 와 통신할 때와 SageMaker Amazon이 AWS 다른 서비스와 상호 작용할 때마다 (예: SageMaker Amazon S3에서 데이터 가져오기) 사용됩니다.

저장 시 PHI를 암호화해야 한다는 요구 사항을 충족하기 위해 Amazon SageMaker 모델을 실행하는 인스턴스에 저장된 데이터를 엔드포인트 (DescribeEndpointConfig: KmsKey ID) 설정 시 AWS Key Management Service (KMS) 를 사용하여 암호화할 수 있습니다. 를 사용하여 모델 교육 결과 (아티

팩트) 를 암호화할 수 AWS KMS 있으며 설명에 있는 KmsKey ID를 사용하여 키를 지정해야 합니다. OutputDataConfig KMS 키 ID가 제공되지 않는 경우 역할 계정의 기본 Amazon S3 KMS 키가 사용됩니다. SageMaker Amazon은 모든 API 호출을 AWS CloudTrail 기록하는 데 사용합니다.

## Amazon Simple Notification Service(Amazon SNS)

고객은 보호 대상 건강 정보 (PHI) 와 함께 Amazon Simple Service (SNS) 를 사용하려면 다음 키 암호화 요구 사항을 이해해야 합니다. 고객은 각 AWS 지역에서 SNS가 제공하는 HTTPS API 엔드포인트를 사용해야 합니다. HTTPS 엔드포인트는 암호화된 연결을 활용하고 전송 대상 데이터의 개인 정보 보호 및 무결성을 보호합니다. AWS모든 HTTPS API 엔드포인트 목록은 서비스 엔드포인트를 참조하십시오.AWS

또한 Amazon SNS는 고객 AWS 계정에서 Amazon SNS에서 또는 Amazon SNS를 대신하여 이루어진 API 호출을 캡처하고 고객이 지정한 Amazon S3 버킷으로 로그 파일을 전송하는 서비스를 사용합니다 CloudTrail. CloudTrail Amazon SNS 콘솔 또는 Amazon SNS API에서 이루어진 API 호출을 캡처합니다. 에서 수집한 CloudTrail 정보를 사용하여 고객은 Amazon SNS에 어떤 요청이 이루어졌는지, 어떤 소스 IP 주소에서 요청했는지, 누가 언제 요청했는지 파악할 수 있습니다. SNS 작업 로깅에 대한 자세한 내용은 다음을 사용하여 Amazon SNS API 호출 로깅을 참조하십시오 CloudTrail.

## Amazon Simple Email Service(Amazon SES)

Amazon Simple 이메일 서비스 (Amazon SES) 는 유연하고 확장성이 뛰어난 이메일 송수신 서비스입니다. 전체 end-to-end 암호화를 위해 메시지를 암호화하는 S/MIME 및 PGP 프로토콜을 모두 지원하며, Amazon SES와의 모든 통신은 SSL (TLS 1.2) 을 사용하여 보호됩니다. 고객은 Amazon S3 버킷에 메시지를 저장하기 전에 메시지를 수신하고 암호화하도록 Amazon SES를 구성하여 저장된 메시지를 암호화하여 저장할 수 있습니다. 자세한 내용은 스토리지용 메시지 암호화에 대한 자세한 내용은 Amazon Simple Email Service (Amazon SES) 가 AWS KMS사용하는 방법을 참조하십시오. 메시지는 HTTPS 엔드포인트 또는 암호화된 SMTP 연결을 통해 Amazon SES로 전송되는 동안 보호됩니다.

Amazon SES에서 수신자에게 보낸 메시지의 경우 Amazon SES는 먼저 수신 메일 서버에 보안 연결을 시도하지만 보안 연결을 설정할 수 없는 경우 메시지를 암호화되지 않은 상태로 전송합니다. 수신자에게 전송할 때 암호화를 요구하려면 고객은 Amazon SES에서 구성 세트를 생성하고 를 사용하여 TlsPolicy 속성을 AWS CLI Require로 설정해야 합니다. 자세한 내용은 Amazon SES 및 보안 프로토콜을 참조하십시오. Amazon SES는 와 통합되어 모든 API AWS CloudTrail 호출을 모니터링합니다. 에서 수집한 AWS CloudTrail정보를 사용하여 고객은 Amazon SES에 요청이 이루어졌는지, 요청의 IP 주소, 요청한 사람, 요청 시기, 추가 세부 정보를 확인할 수 있습니다. 자세한 내용은 Amazon SES API 호출 로깅을 참조하십시오 AWS CloudTrail. Amazon SES는 전송, 거부, 반송률, 전송, 열기, 클릭과 같은

전송 활동을 모니터링하는 방법도 제공합니다. 자세한 내용은 Amazon SES 전송 활동 모니터링을 참조하십시오.

## Amazon Simple Queue Service(Amazon SQS)

고객은 Amazon SQS를 PHI와 함께 사용하려면 다음 주요 암호화 요구 사항을 이해해야 합니다.

- 쿼리 요청을 통한 Amazon SQS 대기열과의 통신은 HTTPS로 암호화되어야 합니다. SQS 요청에 대한 자세한 내용은 쿼리 API 요청 만들기를 참조하십시오.
- Amazon SQS는 저장된 데이터를 보호하기 AWS KMS 위해 와 통합된 서버 측 암호화를 지원합니다. 서버 측 암호화가 추가되어 고객은 암호화된 대기열을 사용하여 보안이 강화되어 민감한 데이터를 전송 및 수신할 수 있습니다. Amazon SQS 서버 측 암호화는 256비트 고급 암호화 표준(AES-256 GCM 알고리즘) 을 사용하여 각 메시지의 본문을 암호화합니다. 와의 통합을 AWS KMS 통해 고객은 Amazon SQS 메시지를 보호하는 키와 다른 리소스를 보호하는 키를 중앙에서 관리할 수 AWS 있습니다. AWS KMS 모든 암호화 키 사용을 기록하여 규제 및 규정 준수 요구 사항을 충족하는 AWS CloudTrail 데 도움이 됩니다. 자세한 내용을 확인하고 Amazon SQS용 SSE의 가용성에 대한 지역을 확인하려면 저장 중 암호화를 참조하십시오.
- 서버 측 암호화를 사용하지 않는 경우 SQS로 전송하기 전에 메시지 페이로드 자체를 암호화해야 합니다. 메시지 페이로드를 암호화하는 한 가지 방법은 Amazon S3 암호화 클라이언트와 함께 Amazon SQS 확장 클라이언트를 사용하는 것입니다. 클라이언트 측 암호화 사용에 대한 자세한 내용은 Amazon SQS 확장 클라이언트 및 Amazon S3 암호화 클라이언트를 사용한 메시지 페이로드 암호화를 참조하십시오.

Amazon SQS는 고객 AWS 계정에서 Amazon SQS에서 또는 Amazon SQS를 대신하여 이루어진 API 호출을 기록하고 지정된 Amazon S3 버킷으로 로그 파일을 전송하는 서비스를 사용합니다 CloudTrail. CloudTrail Amazon SQS 콘솔 또는 Amazon SQS API에서 이루어진 API 호출을 캡처합니다. 고객은 에서 수집한 CloudTrail 정보를 사용하여 Amazon SQS에 어떤 요청이 이루어지는지, 어떤 소스 IP 주소에서 요청했는지, 누가 언제 요청했는지 등을 확인할 수 있습니다. SQS 작업 로깅에 대한 자세한 내용은 를 사용하여 Amazon SQS API 호출 로깅을 참조하십시오. AWS CloudTrail

## Amazon Simple Storage Service(S3)

고객은 Amazon S3를 사용할 때 서버 측 및 클라이언트 측 암호화와 여러 가지 키 관리 방법을 포함하여 저장된 데이터를 암호화하는 몇 가지 옵션을 사용할 수 있습니다. 자세한 내용은 암호화를 사용한 데이터 보호를 참조하십시오.

PHI를 포함하는 Amazon S3에 연결하려면 암호화된 전송 (HTTPS) 을 허용하는 엔드포인트를 사용해야 합니다. 리전 엔드포인트 목록은 서비스 엔드포인트를 참조하십시오.AWS

버킷 이름, 객체 이름 또는 메타데이터에는 PHI를 사용하지 마십시오. 이 데이터는 S3 서버 측 암호화를 사용하여 암호화되지 않으며 클라이언트 측 암호화 아키텍처에서 일반적으로 암호화되지 않기 때문입니다.

## Amazon Simple Workflow Service

Amazon Simple Workflow Service (Amazon SWF) 는 개발자가 병렬 또는 순차 단계가 있는 백그라운드 작업을 구축, 실행 및 확장할 수 있도록 지원합니다. Amazon SWF는 클라우드에서 완전히 관리되는 상태 추적기 및 작업 코디네이터로 생각할 수 있습니다.

Amazon Simple Workflow Service는 워크플로를 조정하는 데 사용되며 데이터를 저장하거나 전송할 수 없습니다. PHI를 Amazon SWF의 메타데이터나 작업 설명 내에 포함해서는 안 됩니다. Amazon SWF는 모든 API 호출을 AWS CloudTrail 기록하는 데 사용합니다.

## Amazon Textract

Amazon Textract는 기계 학습 기술을 사용하여 스캔한 문서에서 텍스트와 데이터를 자동으로 추출합니다. 이는 단순한 광학 문자 인식 (OCR) 을 넘어서서 양식과 테이블에서 데이터를 식별, 이해 및 추출합니다. 예를 들어, 고객은 의료 청구를 처리하기 위해 사람의 개입 없이 Amazon Textract를 사용하여 데이터를 자동으로 추출하고 보호 대상 건강 정보 (PHI) 가 포함된 양식을 처리할 수 있습니다.

Amazon Textract를 사용하여 문서 아카이브의 규정 준수를 유지할 수도 있습니다. 예를 들어, 고객은 Amazon Textract를 사용하여 보험 청구 또는 의료 처방에서 데이터를 추출하고 해당 문서에서 키-값 쌍을 자동으로 인식하여 민감한 문서를 수정할 수 있습니다.

Amazon Textract는 입력 문서에 대한 서버 측 암호화 (SSE-S3 및 SSE-KMS) 와 서비스와 에이전트 간에 전송되는 데이터에 대한 TLS 암호화를 지원합니다. 고객은 CloudWatch Amazon을 사용하여 리소스 사용량 지표를 추적하고 Amazon AWS CloudTrail Textract에 대한 API 호출을 캡처할 수 있습니다.

## Amazon Transcribe

Amazon Transcribe는 고급 기계 학습 기술을 사용하여 오디오 파일의 음성을 인식하고 이를 텍스트로 변환합니다. 예를 들어, 고객은 Amazon Transcribe를 사용하여 미국 영어 및 멕시코 스페인어 오디오를 텍스트로 변환하고 오디오 파일의 콘텐츠를 통합하는 애플리케이션을 만들 수 있습니다. Amazon

Transcribe는 PHI를 포함하는 데이터와 함께 사용할 수 있습니다. Amazon Transcribe는 데이터를 보관하거나 저장하지 않으며 API에 대한 모든 호출은 SSL/TLS로 암호화됩니다. Amazon Transcribe는 모든 API 호출을 CloudTrail 기록하는 데 사용합니다.

## Amazon Translate

Amazon Translate는 고급 기계 학습 기술을 사용하여 온디맨드 방식으로 고품질 번역을 제공합니다. 고객은 Amazon Translate를 사용하여 구조화되지 않은 텍스트 문서를 번역하거나 여러 언어로 작동하는 애플리케이션을 구축할 수 있습니다. PHI를 포함하는 문서는 Amazon Translate로 처리할 수 있습니다. PHI가 포함된 문서를 번역할 때는 추가 구성이 필요하지 않습니다. 전송 중 데이터 암호화는 SSL/TLS에서 제공하며 Amazon Translate를 사용하면 어떤 데이터도 유휴 상태로 유지되지 않습니다. Amazon Translate는 모든 API 호출을 CloudTrail 기록하는 데 사용합니다.

## Amazon Virtual Private Cloud

Amazon VPC (Virtual Private Cloud) 는 HIPAA 규제 워크로드의 아키텍처에 맞게 잘 조정된 일련의 네트워크 보안 기능을 제공합니다. 스테이트리스 네트워크 액세스 제어 목록 및 스테이트풀 보안 그룹으로의 동적 인스턴스 재할당과 같은 기능을 통해 무단 네트워크 액세스로부터 인스턴스를 보호할 수 있는 유연성을 제공합니다.

또한 Amazon VPC를 사용하면 고객이 자신의 네트워크 주소 공간을 AWS확장하고 데이터 센터를 연결하는 다양한 방법을 제공할 수 있습니다. AWS VPC 흐름 로그는 PHI를 처리, 전송 또는 저장하는 인스턴스에 대한 허용 및 거부된 연결의 감사 추적을 제공합니다.

AWS Transit Gateway 네트워크 허브 역할을 하며 Amazon VPC와 온프레미스 네트워크 간의 연결을 단순화합니다. AWS Transit Gateway 또한 백본을 사용하여 글로벌 네트워크를 구축할 수 있도록 다른 Transit Gateway에 지역 간 피어링 기능을 제공합니다. AWS Amazon VPC에 대한 자세한 내용은 Amazon Virtual Private Cloud를 참조하십시오.

## Amazon WorkDocs

Amazon WorkDocs 사용자 생산성을 향상시키는 강력한 관리 제어 및 피드백 기능을 갖춘 안전한 완전 관리형 엔터프라이즈 파일 스토리지 및 공유 서비스입니다. Amazon WorkDocs 고객이 AWS Key Management Service (AWS KMS) 를 통해 관리하는 키를 사용하여 유휴 상태의 파일을 암호화합니다. 전송 중인 모든 데이터는 SSL/TLS를 사용하여 암호화됩니다. AWS 웹 및 모바일 애플리케이션과 데스크톱 동기화 클라이언트는 SSL/TLS를 사용하여 파일을 직접 전송합니다. Amazon WorkDocs

WorkDocs 관리자는 Amazon WorkDocs Management Console을 사용하여 감사 로그를 보고 파일 및 사용자 활동을 시간별로 추적하고 사용자가 조직 외부의 다른 사람과 파일을 공유하도록 허용할지 여부를 선택할 수 있습니다. Amazon WorkDocs 또한 CloudTrail (고객 Amazon WorkDocs 계정에서 또는 고객 AWS 계정을 대신하여 이루어진 API 호출을 캡처하는 서비스) 와 통합되어 고객이 지정하는 Amazon S3 버킷으로 CloudTrail 로그 파일을 전송합니다.

RADIUS 서버를 사용하는 다단계 인증 (MFA) 을 사용할 수 있으며 인증 프로세스 중에 고객에게 추가 보안 계층을 제공할 수 있습니다. 사용자는 사용자 이름과 암호를 입력한 다음 하드웨어 또는 소프트웨어 토큰에서 제공하는 OTP (One-Time Passcode) 를 입력하여 로그인합니다.

자세한 내용은 다음을 참조하세요.

- Amazon WorkDocs feature
- 를 사용하여 API 호출을 로깅합니다 Amazon WorkDocs . AWS CloudTrail

고객은 PHI를 파일 이름이나 디렉터리 이름에 저장해서는 안 됩니다.

## 아마존 WorkSpaces

WorkSpaces Amazon은 에서 실행되는 완전 관리형의 안전한 D esktop-as-a 서비스 (DaaS) 솔루션입니다. AWS WorkSpacesAmazon을 통해 고객은 지원되는 모든 디바이스에서 언제 어디서나 필요한 문서, 애플리케이션 및 리소스에 액세스할 수 있도록 사용자에게 클라우드 기반 가상 Microsoft Windows 데스크톱을 쉽게 프로비저닝할 수 있습니다.

Amazon은 Amazon 엘라스틱 블록 스토어 볼륨에 데이터를 WorkSpaces 저장합니다. 고객은 고객이 관리하는 키를 사용하여 고객의 WorkSpaces 스토리지 볼륨을 암호화할 수 있습니다. AWS Key Management Service WorkSpacea에서 암호화를 활성화하면 기본 스토리지에 저장된 데이터와 디스크 스토리지의 자동 백업 (EBS 스냅샷) 이 지침에 따라 암호화됩니다. WorkSpace 클라이언트와의 WorkSpace 통신은 SSL/TLS를 사용하여 보호됩니다. WorkSpacesAmazon을 사용한 저장 중 암호화에 대한 자세한 내용은 WorkSpaces암호화를 참조하십시오.

## AWS App Mesh

AWS App Mesh는 Amazon ECS, Amazon EKS 또는 Amazon EC2 서비스와 같은 여러 유형의 컴퓨팅 인프라에서 서비스가 서로 쉽게 통신할 수 있도록 애플리케이션 수준의 네트워킹을 제공하는 서비스 메쉬입니다. App Mesh는 가시성을 제공하기 위해 통합 가시성 데이터를 수집하고 구성한 모니터링 세트로 전송하도록 Envoy 프록시를 구성합니다. end-to-end 애플리케이션의 고가용성을 보장하도록

구성된 라우팅 및 트래픽 정책을 기반으로 트래픽을 라우팅할 수 있습니다. 애플리케이션 간 트래픽은 TLS를 사용하도록 구성할 수 있습니다. App Mesh는 쿠버네티스용 AWS SDK 또는 App Mesh 컨트롤러를 사용하여 사용할 수 있습니다. HIPAA 적격 서비스이긴 하지만 AWS App Mesh , 해당 데이터를 보호할 수 있는 지원이 없기 AWS App Mesh 때문에 리소스 이름/속성에 PHI를 저장해서는 안 됩니다. 대신 PHI를 전송하거나 저장하는 고객 도메인 리소스를 모니터링, 제어 및 보호하는 데 사용할 AWS App Mesh 수 있습니다.

## AWS 애플리케이션 마이그레이션 서비스

AWS 애플리케이션 마이그레이션 서비스 (AWS MGN) 를 사용하면 서버와 애플리케이션을 변경 없이 다운타임을 최소화하면서 신속하게 마이그레이션할 AWS수 있습니다. AWS 리프트 앤 시프트 마이그레이션에 권장되는 기본 마이그레이션 서비스는 MGN입니다. AWS

AWS MGN은 블록 레벨 데이터 복제를 사용하여 소스 디스크를 고객 계정의 EBS 볼륨에 직접 복사합니다. 데이터는 AWS MGN으로 제어되는 클라우드 환경을 통해 전송되지 않습니다. 복제된 데이터는 기본적으로 전송 중에 암호화됩니다. 고객의 EBS 볼륨에 있는 데이터는 기본적으로 고객 고유의 키를 사용하여 암호화됩니다.

## AWS Auto Scaling

AWS Auto Scaling을 통해 고객은 몇 분 만에 고객 애플리케이션의 일부인 AWS 리소스에 대한 자동 크기 조정을 구성할 수 있습니다. 고객은 Amazon DynamoDB, Amazon ECS, Amazon RDS Aurora 복제본, AWS Auto Scaling 그룹의 Amazon EC2 인스턴스 등 PHI를 포함하는 다양한 서비스에 Auto Scaling을 사용할 수 있습니다.

AWS Auto Scaling은 고객 콘텐츠를 직접 처리, 저장 또는 전송하지 않는 오케스트레이션 서비스이므로 고객은 암호화된 콘텐츠와 함께 이 서비스를 사용할 수 있습니다. AWS 공동 책임 모델은 AWS Auto Scaling의 데이터 보호에 적용됩니다. 즉, AWS 네트워크 보안 절차를 담당하는 반면, 고객은 이 인프라에서 호스팅되는 고객 콘텐츠에 대한 제어를 유지할 책임이 있습니다. AWS 이 콘텐츠에는 고객이 사용하는 AWS 서비스의 보안 구성 및 관리 작업이 포함됩니다. 데이터 보호를 위해 고객은 AWS 계정 자격 증명을 보호하고 AWS Identity and Access Management (IAM) 을 사용하여 개별 사용자 계정을 설정하는 것이 좋습니다. 이러한 방식에서는 각 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다.

고객 계정 번호와 같은 민감한 식별 정보를 이름 필드와 같은 자유 형식 필드에 입력하지 않는 것이 좋습니다. 여기에는 고객이 AWS Management Console AWS CLI, API 또는 AWS SDK를 사용하여 AWS Auto Scaling 또는 기타 AWS 서비스를 사용하는 경우가 포함됩니다.

고객이 AWS Auto Scaling 또는 기타 서비스에 입력하는 모든 데이터는 진단 로그에 포함되도록 선별될 수 있습니다. 고객이 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위한 자격 증명 정보를 URL에 포함해서는 안 됩니다. AWS 또한 고객에게 다음과 같은 방법으로 데이터를 보호할 것을 권장합니다.

- 각 계정에 다중 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 리소스와 통신하세요. AWS TLS 1.2 이상을 사용하는 것이 좋습니다.
- 를 사용하여 API 및 사용자 활동 로깅을 AWS CloudTrail설정합니다.
- AWS 서비스 내의 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용하십시오.
- Amazon S3에 저장된 개인 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용합니다.

# AWS Backup

AWS Backup 중앙 집중식 완전 관리형 정책 기반 서비스를 제공하여 고객 데이터를 보호하고 비즈니스 연속성을 위해 AWS 서비스 전반에서 규정 준수를 보장합니다. 를 통해 고객은 Amazon EBS 볼륨 AWS Backup, Amazon 관계형 데이터베이스 서비스 (Amazon RDS) 데이터베이스 (Aurora 클러스터 포함), Amazon DynamoDB 테이블, Amazon Elastic File System (Amazon EFS), Amazon FSx 파일 시스템, Amazon EC2를 비롯한 고객 AWS 리소스 전반의 데이터 보호 (백업) 정책을 중앙에서 구성하고 백업 활동을 모니터링할 수 있습니다. 2 인스턴스 및 볼륨. AWS Storage Gateway

AWS Backup 전송 중인 고객 데이터와 저장된 고객 데이터를 암호화합니다. 기존 스냅샷 기능이 있는 서비스의 백업은 소스 서비스의 스냅샷 암호화 방법을 사용하여 암호화됩니다. 예를 들어 EBS 스냅샷은 스냅샷이 생성된 볼륨의 암호화 키를 사용하여 암호화됩니다.

Amazon EFS와 같이 백업 기능을 기반으로 AWS Backup구축된 새 AWS 서비스의 백업은 전송 중 및 저장 중에 소스 서비스와 독립적으로 암호화되므로 고객 백업에 추가 보호 계층이 제공됩니다. 암호화는 Backup Vault 수준에서 구성됩니다. 기본 저장소는 암호화됩니다. 고객이 새 저장소를 생성할 때는 암호화 키를 선택해야 합니다.

# AWS Batch

AWS Batch 개발자, 과학자, 엔지니어가 수십만 개의 배치 컴퓨팅 작업을 쉽고 효율적으로 실행할 수 있도록 AWS합니다. AWS Batch 제출된 배치 작업의 볼륨 및 특정 리소스 요구 사항을 기반으로 최적의 양과 유형의 컴퓨팅 리소스 (예: CPU 또는 메모리 최적화 인스턴스) 를 동적으로 프로비저닝합니다. AWS Batch 전체 컴퓨팅 서비스 및 기능에 걸쳐 배치 컴퓨팅 워크로드를 계획하고, 일정을 잡고, 실행합니다. AWS

Amazon ECS 지침과 마찬가지로 PHI를 작업 정의, 작업 대기열 또는 태그에 직접 삽입해서는 안 됩니다. AWS Batch대신 로 스케줄링되고 실행된 작업은 암호화된 PHI에서 작동할 AWS Batch 수 있습니다. 작업 단계별로 반환되는 모든 정보에도 PHI가 AWS Batch 포함되어서는 안 됩니다. 에서 실행 중인 작업이 PHI를 전송하거나 AWS Batch 수신해야 할 때마다 HTTPS 또는 SSL/TLS를 사용하여 해당 연결을 암호화해야 합니다.

## AWS Certificate Manager

AWS Certificate Manager 고객이 서비스 및 내부 연결 리소스에 사용할 공개 및 사설 SSL/TLS 인증서를 쉽게 프로비저닝, 관리 및 배포할 수 있는 서비스입니다. AWS AWS Certificate Manager 모든 API 호출을 CloudTrail 기록하는 데 사용합니다.

AWS 외부 사용자와 상호 작용하려는 사용자는 프로그래밍 방식의 액세스가 필요합니다. AWS Management Console프로그래밍 방식 액세스를 허용하는 방법은 액세스하는 사용자 유형에 따라 다릅니다. AWS

사용자에게 프로그래밍 방식 액세스 권한을 부여하려면 다음 옵션 중 하나를 선택합니다.

| 프로그래밍 방식 액세스가 필요한 사용자는 누구인가요? | 액세스 권한을 부여 받을 사용자 | 액세스 권한을 부여하는 사용자 |
| --- | --- | --- |
| 작업 인력 ID<br><br>(IAM 자격 증명 센터에서 관리되는 사용자) | 임시 자격 증명을 사용하여 AWS CLI, AWS SDK 또는 API에 대한 프로그래밍 요청에 서명할 수 있습니다. AWS | 사용하고자 하는 인터페이스에 대한 지침을 따릅니다.<br><br>• AWS CLI 에 대한 내용은 사용 설명서의 AWS CLI사용을 AWS IAM Identity Center위한 구성을 참조하십시오.AWS Command Line Interface<br>• AWS SDK, 도구 및 AWS API의 경우 AWS SDK 및 도구 참조 안내서의 IAM ID 센터 인증을 참조하십시오. |
| IAM | 임시 자격 증명을 사용하여 AWS CLI, AWS SDK 또는 API에 대한 프로그래밍 방식 요청에 서명할 수 있습니다. AWS | IAM 사용 설명서의 AWS 리소스와 함께 임시 자격 증명 사용의 지침을 따르십시오. |

| 프로그래밍 방식 액세스가 필요한 사용자는 누구인가요? | 액세스 권한을 부여 받을 사용자 | 액세스 권한을 부여하는 사용자 |
| --- | --- | --- |
| IAM | (권장되지 않음)<br>장기 자격 증명을 사용하여 AWS CLI, AWS SDK 또는 API에 대한 프로그래밍 요청에 서명할 수 있습니다. AWS | 사용하고자 하는 인터페이스에 대한 지침을 따릅니다.<br>• 에 대한 내용은 사용 설명서의 IAM 사용자 자격 증명을 사용한 인증을 참조하십시오. AWS CLIAWS Command Line Interface<br>• AWS SDK 및 도구의 경우 SDK 및 도구 참조 안내서의 장기 자격 증명을 사용한 인증을 참조하십시오.AWS<br>• AWS API의 경우 IAM 사용 설명서의 IAM 사용자의 액세스 키 관리를 참조하십시오. |

## AWS Cloud Map

AWS Cloud Map은 클라우드 리소스 검색 서비스입니다. AWS 클라우드 맵을 사용하면 고객은 Amazon ECS 작업, Amazon EC2 인스턴스, Amazon S3 버킷, Amazon DynamoDB 테이블, Amazon SQS 대기열 또는 기타 클라우드 리소스와 같은 애플리케이션 리소스의 사용자 지정 이름을 정의할 수 있습니다. 그런 다음 고객은 이러한 사용자 지정 이름을 사용하여 AWS SDK와 인증된 API 쿼리를 사용하여 애플리케이션에서 클라우드 리소스의 위치와 메타데이터를 검색할 수 있습니다. AWS Cloud Map은 HIPAA 적격 서비스이지만, AWS Cloud Map 내의 리소스 이름/속성에는 PHI를 저장해서는 안 됩니다. 이러한 데이터를 보호할 수 있는 지원이 없기 때문입니다. 대신 AWS Cloud Map을 사용하여 PHI를 전송하거나 저장하는 고객 도메인 리소스를 검색할 수 있습니다.

## AWS CloudFormation

AWS CloudFormation 고객이 예측 가능하고 반복적으로 AWS 인프라 배포를 생성하고 프로비저닝할 수 있도록 합니다. 이를 통해 고객은 Amazon EC2, Amazon Elastic Block Store, Amazon SNS, Elastic Load Balancing 및 Auto Scaling과 같은 AWS 제품을 활용하여 기본 AWS 인프라를 만들고 구성할 걱정 없이 클라우드에서 매우 안정적이고 확장성이 뛰어나며 비용 효율적인 애플리케이션을 구축할 수

있습니다. AWS CloudFormation 고객이 템플릿 파일을 사용하여 리소스 컬렉션을 단일 단위 (스택) 로 생성 및 삭제할 수 있도록 합니다.

AWS CloudFormation 자체적으로 PHI를 저장, 전송 또는 처리하지 않습니다. 대신 PHI를 저장, 전송 및/또는 처리할 수 있는 다른 AWS 서비스를 사용하는 아키텍처를 구축하고 배포하는 데 사용됩니다. HIPAA 적격 서비스만 PHI와 함께 사용해야 합니다. 해당 서비스에서 PHI를 사용하는 방법에 대한 지침은 본 백서의 해당 서비스 항목을 참조하십시오. AWS CloudFormation 모든 API 호출을 AWS CloudTrail 기록하는 데 사용합니다.

## AWS CloudHSM

AWS CloudHSM 고객이 AWS 클라우드에서 자체 암호화 키를 쉽게 생성하고 사용할 수 있도록 하는 클라우드 기반 하드웨어 보안 모듈 (HSM) 입니다. CloudHSM을 사용하면 고객은 FIPS 140-2 레벨 3 검증 HSM을 사용하여 자체 암호화 키를 관리할 수 있습니다. CloudHSM은 고객에게 PKCS #11, 자바 암호화 확장 (JCE) 및 Microsoft CryptoNG (CNG) 라이브러리와 같은 개방형 표준 API를 사용하여 애플리케이션과 통합할 수 있는 유연성을 제공합니다.

또한 CloudHSM은 표준을 준수하므로 고객이 모든 키를 다른 상용 HSM으로 내보낼 수 있습니다. 하드웨어 어플라이언스 키 관리 서비스와 마찬가지로 AWS CloudHSM PHI를 저장하거나 전송할 수 없습니다. 고객은 PHI를 태그 (메타데이터) 에 저장해서는 안 됩니다. 다른 특별한 지침은 필요하지 않습니다.

## AWS CloudTrail

AWS CloudTrail AWS 계정의 거버넌스, 규정 준수, 운영 감사 및 위험 감사를 지원하는 서비스입니다. 를 CloudTrail 통해 고객은 AWS 인프라 전반의 작업과 관련된 계정 활동을 기록하고, 지속적으로 모니터링하고, 유지할 수 있습니다. CloudTrail , AWS SDK, 명령줄 도구 및 기타 AWS 서비스를 통해 수행한 작업을 포함하여 AWS 계정 활동의 이벤트 기록을 제공합니다. AWS Management Console이 이벤트 기록은 보안 분석, 리소스 변경 추적 및 문제 해결을 간소화합니다.

AWS CloudTrail 모든 AWS 계정에서 사용할 수 있으며, AWS BAA에서 요구하는 대로 감사 로깅에 사용할 수 있습니다. 특정 트레일은 CloudTrail 콘솔 또는 AWS 명령줄 인터페이스를 사용하여 생성해야 합니다. CloudTrail 암호화된 트레일이 생성되면 전송 중 및 유휴 상태의 모든 트래픽을 암호화합니다. PHI를 기록할 가능성이 있는 경우 암호화된 트레일을 생성해야 합니다.

기본적으로 암호화된 트레일은 Amazon S3 (SSE-S3) 관리 키를 사용한 서버 측 암호화를 사용하여 Amazon S3에 항목을 저장합니다. 키를 통한 추가 관리가 필요한 경우 AWS KMS-관리형 키 (SSE-KMS) 를 사용하여 구성할 수도 있습니다. PHI를 처리하는 모든 아키텍처의 핵심 구성 요소인 AWS 로

그 항목의 최종 목적지이므로 CloudTrail 로그 파일 무결성 검증을 활성화하고 관련 CloudTrail 다이제스트 파일을 정기적으로 검토해야 합니다. CloudTrail 일단 활성화되면 로그 파일이 변경되거나 변경되지 않았다는 확신을 가질 수 있습니다.

## AWS CodeBuild

AWS CodeBuild 클라우드의 완전 관리형 빌드 서비스입니다. AWS CodeBuild 소스 코드를 컴파일하고, 단위 테스트를 실행하고, 배포할 준비가 된 아티팩트를 생성합니다. AWS CodeBuild AWS KMS 키를 사용하여 빌드 출력 아티팩트를 암호화합니다. 모든 API 호출을 기록하는 데 사용하는 PHI, 비밀/암호, 인증서 등이 포함된 아티팩트를 빌드하기 전에 KMS 키를 생성하고 구성해야 합니다. AWS CodeBuild AWS CloudTrail

## AWS CodeDeploy

AWS CodeDeploy Amazon EC2, AWS Fargate, AWS Lambda및 온프레미스 서버를 비롯한 다양한 컴퓨팅 서비스에 대한 소프트웨어 배포를 자동화하는 완전 관리형 배포 서비스입니다. 고객은 AWS CodeDeploy 를 사용하여 컨테이너식 워크로드의 새로운 기능을 신속하게 릴리스하고 애플리케이션 업데이트의 복잡성을 처리합니다.

AWS CodeDeploy 배포 아티팩트에 대한 서버 측 암호화 (SSE-S3) 및 서비스와 에이전트 간에 전송되는 데이터에 대한 TLS 암호화를 지원합니다. 고객은 Amazon CloudWatch Events를 사용하여 배포를 추적하고 API 호출을 AWS CloudTrail 캡처할 수 있습니다. AWS CodeDeploy

## AWS CodeCommit

AWS CodeCommit 프라이빗 Git 리포지토리를 호스팅하는 안전하고 확장성이 뛰어난 관리형 소스 컨트롤 서비스입니다. AWS CodeCommit 고객이 자체 소스 제어 시스템을 관리하거나 인프라 확장에 대해 걱정할 필요가 없습니다.

AWS CodeCommit 전송 중이거나 유휴 상태일 때 모든 트래픽과 저장된 정보를 암호화합니다. 기본적으로 리포지토리가 생성되면 AWS 관리형 키가 AWS KMS 생성되며 해당 리포지토리에서만 저장된 모든 데이터를 암호화하는 데 사용됩니다. AWS CodeCommit AWS CodeCommit 모든 API 호출을 AWS CloudTrail 기록하는 데 사용됩니다.

## AWS CodePipeline

AWS CodePipeline 고객이 빠르고 안정적인 애플리케이션 및 인프라 업데이트를 위해 고객 릴리스 파이프라인을 자동화할 수 있도록 지원하는 완전 관리형 지속적 전달 서비스입니다. 고객이 사용하는 워

크플로 파이프라인의 몇 가지 예로는 연구자가 임상 시험 데이터, 실험 결과 및 유전체 데이터를 자동으로 AWS CodePipeline 처리하도록 허용하는 경우를 들 수 있습니다.

AWS CodePipeline 코드 아티팩트에 대한 서버 측 암호화 (SSE-S3 및 SSE-KMS) 와 서비스와 에이전트 간 전송 중인 데이터에 대한 TLS 암호화를 지원합니다. 고객은 Amazon CloudWatch Events를 사용하여 파이프라인 변경 사항을 추적하고 대상 API 호출을 AWS CloudTrail 캡처할 수 AWS CodePipeline있습니다.

## AWS Config

AWS Config 구성 방식, 리소스 간의 관계, 시간 경과에 따른 구성 및 관계 변화를 비롯하여 고객의 AWS 계정과 관련된 리소스를 자세히 보여줍니다.

AWS Config 그 자체로는 PHI를 저장하거나 전송하는 데 사용할 수 없습니다.

대신 PHI를 처리하는 아키텍처를 비롯한 다른 AWS 서비스로 구축된 아키텍처를 모니터링하고 평가하는 데 활용하여 해당 아키텍처가 의도한 설계 목표를 준수하는지 여부를 판단할 수 있습니다. PHI를 처리하는 아키텍처는 HIPAA 적격 서비스로만 구축해야 합니다. AWS Config AWS CloudTrail 모든 결과를 기록하는 데 사용합니다.

## AWS Data Exchange

AWS Data Exchange를 사용하면 클라우드에서 타사 데이터를 쉽게 찾고, 구독하고, 사용할 수 있습니다. 데이터 제품을 구독한 고객은 AWS Data Exchange API를 사용하여 Amazon S3에 직접 데이터를 로드한 다음 다양한 AWS 분석 및 기계 학습 서비스를 통해 데이터를 분석할 수 있습니다. 데이터 공급자의 경우, AWS Data Exchange를 사용하면 데이터 스토리지, 전송, 청구 및 권한 부여를 위한 인프라를 구축하고 유지할 필요가 없으므로 클라우드로 마이그레이션하는 수백만 AWS 고객에게 쉽게 다가갈 수 있습니다.

AWS Data Exchange는 추가 구성 없이 서비스에 저장된 모든 데이터 제품을 항상 암호화합니다. 이 암호화는 서비스 관리형 KMS 키를 통해 자동으로 수행됩니다. AWS Data Exchange는 전송 중 암호화를 위해 전송 계층 보안 (TLS) 및 클라이언트 측 암호화를 사용합니다. AWS Data Exchange와의 통신은 항상 HTTPS를 통해 이루어지므로 고객 데이터는 전송 중에 항상 암호화됩니다. 이 암호화는 고객이 AWS Data Exchange를 사용할 때 기본적으로 구성됩니다. 자세한 내용은 AWS Data Exchange의 데이터 보호를 참조하십시오.

AWS Data Exchange는 와 통합되어 AWS CloudTrail있습니다. AWS CloudTrail AWS 데이터 교환 콘솔에서의 호출 및 AWS 데이터 교환 API 작업에 대한 코드 호출을 포함하여 AWS 데이터 교환 API에

대한 모든 호출을 이벤트로 캡처합니다. 고객이 취할 수 있는 일부 조치는 콘솔 전용 조치입니다. AWS SDK 또는 AWS CLI에는 해당 API가 없습니다. 이는 제품 게시 또는 구독과 같이 AWS Marketplace 기능에 의존하는 작업입니다. AWS Data Exchange는 이러한 콘솔 전용 작업의 하위 집합에 대한 CloudTrail 로그를 제공합니다. 자세한 내용은 AWS 데이터 교환 API 호출 로깅을 참조하십시오 AWS CloudTrail.

AWS Data Exchange를 사용하는 모든 목록은 특정 범주의 데이터를 제한하는 AWS Data Exchange의 게시 지침 및 AWS Marketplace 공급자용 AWS Data Exchange FAQ를 준수해야 한다는 점에 유의하십시오. 자세한 내용은 AWS 데이터 교환 FAQ를 참조하십시오.

## AWS Database Migration Service

AWS Database Migration Service (AWS DMS) 는 고객이 데이터베이스를 AWS로 쉽고 안전하게 마이그레이션할 수 있도록 지원합니다. 고객은 Oracle, MySQL, PostgreSQL과 같이 가장 널리 사용되는 상용 및 오픈 소스 데이터베이스로 또는 그 데이터베이스에서 데이터를 마이그레이션할 수 있습니다. 이 서비스는 Oracle에서 Oracle로의 동종 마이그레이션뿐만 아니라 Oracle에서 PostgreSQL로 또는 MySQL에서 Oracle로 등 서로 다른 데이터베이스 플랫폼 간 이종 마이그레이션도 지원합니다.

온프레미스에서 실행되고 AWS DMS를 통해 클라우드로 마이그레이션되는 데이터베이스에는 PHI 데이터가 포함될 수 있습니다. AWS DMS는 전송 중에 그리고 AWS의 대상 데이터베이스로 최종 마이그레이션하기 위해 데이터가 스테이징될 때 데이터를 암호화합니다. AWS DMS는 복제 인스턴스가 사용하는 스토리지와 엔드포인트 연결 정보를 암호화합니다. 복제 인스턴스가 사용하는 스토리지를 암호화하기 위해 AWS DMS는 AWS 계정 고유의 AWS KMS 키를 사용합니다. 마이그레이션이 완료된 후에도 데이터가 암호화된 상태로 유지되도록 하려면 해당 대상 데이터베이스의 지침을 참조하십시오. AWS DMS는 모든 API 호출을 CloudTrail 기록하는 데 사용합니다.

## AWS DataSync

DataSync AWS는 온 프레미스 스토리지와 AWS 간의 데이터 이동을 간소화, 자동화 및 가속화하는 온라인 전송 서비스입니다. 고객은 AWS를 DataSync 사용하여 데이터 소스를 Amazon S3 또는 Amazon EFS에 연결할 수 있습니다. 고객은 Amazon S3 및 Amazon EFS가 지침과 일치하는 방식으로 구성되었는지 확인해야 합니다. 기본적으로 고객 데이터는 TLS 1.2를 사용하여 전송 중에 암호화됩니다. 암호화와 DataSync AWS에 대한 자세한 내용은 AWS DataSync 기능을 참조하십시오. 고객은 를 사용하여 DataSync 활동을 모니터링할 수 AWS CloudTrail있습니다. 로깅에 대한 자세한 내용은 AWS DataSync API 호출 로깅을 참조하십시오 AWS CloudTrail. CloudTrail

# AWS Directory Service

## Microsoft AD용 AWS Directory Service

AWS Microsoft AD라고도 하는 Microsoft Active Directory용 AWS Directory 서비스 (엔터프라이즈 에디션) 를 사용하면 디렉터리 인식 워크로드와 AWS 리소스가 AWS 클라우드의 관리형 Active Directory를 사용할 수 있습니다. AWS Microsoft AD는 AWS에서 관리하는 암호화 키를 사용하여 디렉터리 콘텐츠 (PHI를 포함하는 콘텐츠 포함) 를 암호화된 Amazon Elastic 블록 스토어 볼륨에 저장합니다. 자세한 내용은 Amazon EBS 암호화를 참조하세요.

Active Directory 클라이언트와 주고 받는 데이터는 고객의 Amazon Virtual Private Cloud (Amazon Virtual Private Cloud) 네트워크를 통해 LDAP (경량 디렉터리 액세스 프로토콜) 를 통해 이동할 때 암호화됩니다. Active Directory 클라이언트가 온프레미스 네트워크에 있는 경우 트래픽은 가상 사설망 링크 또는 링크를 통해 고객의 VPC로 이동합니다. AWS Direct Connect

## Amazon Cloud Directory

Amazon Cloud Directory를 사용하면 고객이 유연한 클라우드 네이티브 디렉터리를 구축하여 다차원에 따른 데이터 계층 구조를 구성할 수 있습니다. 또한 고객은 조직도, 교육 과정 카탈로그, 디바이스 레지스트리와 같은 다양한 사용 사례에 맞는 디렉터리를 생성할 수 있습니다. 예를 들어 고객은 보고 구조, 위치 및 비용 센터에 대해 별도의 계층 구조를 통해 탐색할 수 있는 조직도를 만들 수 있습니다. Amazon Cloud Directory는 () 에서 관리하는 256비트 암호화 키를 사용하여 저장 중인 데이터와 전송 중인 데이터를 자동으로 암호화합니다. AWS Key Management Service AWS KMS

# AWS Elastic Beanstalk

를 사용하면 AWS Elastic Beanstalk고객은 애플리케이션을 실행하는 인프라에 대해 배울 필요 없이 AWS 클라우드에서 애플리케이션을 빠르게 배포하고 관리할 수 있습니다. 고객은 간단히 코드를 업로드하고 용량 프로비저닝, 로드 밸런싱, 자동 크기 조정에서 애플리케이션 상태 모니터링에 이르기까지 배포를 AWS Elastic Beanstalk 자동으로 처리할 수 있습니다. 동시에 고객은 애플리케이션을 구동하는 AWS 리소스를 완전히 제어할 수 있으며 언제든지 기본 리소스에 액세스할 수 있습니다.

AWS Elastic Beanstalk 자체적으로 PHI를 저장, 전송 또는 처리하지는 않습니다. 대신 고객은 이를 사용하여 PHI를 저장, 전송 및/또는 처리할 수 있는 다른 AWS 서비스와 함께 아키텍처를 구축하고 배포할 수 있습니다. 에서 배포한 AWS Elastic Beanstalk 서비스를 선택할 때 고객은 PHI와 함께 HIPAA 적격 서비스만 사용하도록 해야 합니다. 해당 서비스에서 PHI를 사용하는 방법에 대한 지침은 이 백서의 해당 서비스 항목을 참조하십시오.

고객은 이름 필드와 AWS Elastic Beanstalk 같은 자유 형식 필드에 PHI를 포함해서는 안 됩니다. AWS Elastic Beanstalk 모든 API AWS CloudTrail 호출을 기록하는 데 사용합니다.

## AWS 엘라스틱 재해 복구

AWS Elastic Disaster Recovery (AWS DRS) 는 저렴한 스토리지, 최소한의 컴퓨팅 및 복구를 사용하여 온프레미스 및 클라우드 기반 애플리케이션을 빠르고 안정적으로 복구함으로써 다운타임과 데이터 손실을 최소화합니다. point-in-time

고객은 소스 서버에 AWS Elastic 재해 복구를 설정하여 안전한 데이터 복제를 시작할 수 있습니다. 해당 데이터는 선택한 AWS 리전의 AWS 계정의 스테이징 영역 서브넷에 복제됩니다. 스테이징 영역 설계는 저렴한 스토리지와 최소한의 컴퓨팅 리소스를 사용하여 지속적인 복제를 유지함으로써 비용을 절감합니다. AWS Elastic Disaster Recovery에서 복제된 고객 데이터는 TLS 1.2를 사용하여 전송 중에 암호화되고 소스 서버에서 VPC로 직접 전송됩니다. 고객은 AWS Direct Connect 또는 VPN과 같은 프라이빗 연결을 활용하여 복제 경로를 구성할 수 있습니다. Amazon EBS 암호화를 사용하여 AWS에 저장된 고객 데이터를 암호화할 수도 있습니다.

고객은 무중단 테스트를 수행하여 구현이 완료되었는지 확인할 수 있습니다. 정상 운영 중에는 복제를 모니터링하고 무중단 복구 및 페일백 훈련을 정기적으로 수행하여 준비 상태를 유지하십시오. 애플리케이션을 복구해야 하는 경우 대부분의 up-to-date 서버 상태 또는 이전 시점을 사용하여 몇 분 내에 AWS에서 복구 인스턴스를 시작할 수 있습니다. 고객 애플리케이션을 AWS에서 실행한 후에는 애플리케이션을 그대로 두거나 문제가 해결되면 기본 사이트로 다시 데이터 복제를 시작할 수 있습니다. 고객은 준비가 되면 언제든지 기본 사이트로 페일백할 수 있습니다.

## AWS Fargate

AWS Fargate 고객이 서버나 클러스터를 관리할 필요 없이 컨테이너를 실행할 수 있도록 하는 기술입니다. 이를 통해 AWS Fargate고객은 더 이상 컨테이너를 실행하기 위해 가상 시스템 클러스터를 프로비저닝, 구성 및 확장할 필요가 없습니다. 따라서 서버 유형을 선택하거나, 클러스터를 확장할 시기를 결정하거나, 클러스터 패킹을 최적화할 필요가 없습니다. AWS Fargate 고객이 서버 또는 클러스터와 상호 작용하거나 이에 대해 생각할 필요가 없습니다. Fargate를 사용하는 고객은 애플리케이션을 실행하는 인프라를 관리하는 대신 애플리케이션을 설계하고 구축하는 데 집중할 수 있습니다.

Fargate는 PHI를 처리하는 워크로드를 처리하기 위해 추가 구성이 필요하지 않습니다. 고객은 Amazon ECS와 같은 컨테이너 오케스트레이션 서비스를 사용하여 Fargate에서 컨테이너 워크로드를 실행할 수 있습니다. Fargate는 기본 인프라만 관리하며 오케스트레이션되는 워크로드 내의 데이터를 사용하거나 해당 데이터를 기반으로 운영하지 않습니다. HIPAA 요구 사항에 따라 Fargate를 통해 출

시된 컨테이너가 PHI에 액세스하는 경우 전송 중이거나 유휴 상태일 때는 항상 PHI를 암호화해야 합니다. 이 백서에 설명된 각 AWS 스토리지 옵션에는 저장 중 암호화를 위한 다양한 메커니즘이 제공됩니다. 추가 HIPAA 보안 및 구성 정보는 Amazon EKS 기반 HIPAA 보안 및 규정 준수를 위한 아키텍처 설계 백서를 참조하십시오.

## AWS Firewall Manager

AWS Firewall Manager 는 고객이 고객 계정 및 애플리케이션 전반의 방화벽 규칙을 중앙에서 구성하고 관리할 수 있도록 하는 보안 관리 서비스입니다. AWS Organizations새 애플리케이션이 생성되면 Firewall Manager를 사용하면 공통 보안 규칙 세트를 적용하여 새 애플리케이션과 리소스를 손쉽게 규정을 준수할 수 있습니다. 이제 고객은 단일 서비스를 통해 중앙 관리자 계정을 통해 방화벽 규칙을 구축하고, 보안 정책을 만들고, 전체 인프라에서 일관되고 계층적인 방식으로 적용할 수 있습니다.

AWS Firewall Manager 사용자 데이터를 직접 처리, 저장 또는 전송하지 않는 오케스트레이션 서비스입니다. 서비스는 고객 콘텐츠를 암호화하지 않지만, DynamoDB와 같이 AWS Firewall Manager 사용하는 기본 서비스는 사용자 데이터를 암호화합니다.

## AWS Global Accelerator

AWS Global Accelerator 다중 지역 애플리케이션의 가용성과 지연 시간을 개선하는 글로벌 로드 밸런싱 서비스입니다. PHI를 전송 및 사용 AWS Global Accelerator중에 암호화된 상태로 유지하려면 Global Accelerator에서 부하 분산을 수행하는 아키텍처에서 HTTPS 또는 SSL/TLS와 같은 암호화된 프로토콜을 사용해야 합니다. 백엔드 리소스에 사용할 수 있는 암호화 옵션을 더 잘 이해하려면 Amazon EC2, Elastic Load Balancing 및 기타 AWS 서비스 지침을 참조하십시오. AWS Global Accelerator 모든 API 호출을 AWS CloudTrail 기록하는 데 사용합니다.

## AWS Glue

AWS Glue 는 완전관리형 ETL (추출, 변환, 로드) 서비스로, 이를 통해 고객이 간단하고 비용 효율적으로 데이터를 분류하고, 정리하고, 보강하고, 다양한 데이터 저장소 간에 안정적으로 이동할 수 있습니다. 전송 중에 PHI를 포함하는 데이터를 암호화하려면 SSL/TLS가 있는 데이터 저장소에 대한 JDBC 연결을 사용하도록 AWS Glue 구성해야 합니다. 또한 전송 중에 암호화를 유지하려면 서버 측 암호화 (SSE-S3) 설정을 ETL 작업 실행에 매개 변수로 전달해야 합니다. AWS Glue데이터 카탈로그 내에 저장된 모든 데이터는 Data Catalog AWS Glue 객체 생성 시 암호화가 AWS KMS 활성화될 때 관리되는 키를 사용하여 암호화됩니다. AWS Glue 모든 API 호출을 CloudTrail 기록하는 데 사용됩니다.

# AWS Glue DataBrew

AWS DataBrew Glue는 데이터 분석가와 데이터 과학자가 데이터를 쉽게 정리하고 정규화하여 분석 및 기계 학습에 맞게 준비할 수 있게 해주는 완전 관리형 시각적 데이터 준비 서비스입니다. 전송 중에 PHI를 포함하는 데이터를 암호화하려면 SSL/TLS가 있는 데이터 스토어에 대한 JDBC 연결을 사용하도록 DataBrew 구성해야 합니다. JDBC 데이터 소스에 연결할 때는 “SSL 연결 필요” 옵션을 비롯한 AWS Glue 연결의 설정을 DataBrew 사용합니다. 또한 S3 버킷에 저장된 상태에서 암호화를 유지하려면 서버 측 암호화 (SSE-S3 또는 SSE-KMS) 설정을 파라미터로 작업에 전달해야 합니다. DataBrew

# AWS IoT 코어 및 AWS IoT Device Management

AWS IoT 센서, 액추에이터, 임베디드 마이크로 컨트롤러 또는 스마트 어플라이언스와 같은 인터넷 연결 디바이스와 AWS 클라우드 간의 안전한 양방향 통신을 코어 및 AWS IoT Device Management 제공합니다. AWS IoT Core와 Core는 이제 AWS IoT Device Management PHI를 포함하는 데이터를 전송하는 디바이스를 수용할 수 있습니다. AWS IoT Core와의 모든 AWS IoT Device Management 통신은 TLS를 사용하여 암호화됩니다. AWS IoT 모든 API 호출을 AWS CloudTrail 기록하는 데 코어 및 AWS IoT Device Management 사용

# AWS IoT Greengrass

AWS IoT Greengrass 고객이 커넥티드 디바이스에 대해 로컬 컴퓨팅, 메시징, 데이터 캐싱, 동기화 및 ML 추론 기능을 안전한 방식으로 실행할 수 있습니다. AWS IoT Greengrass X.509 인증서, 관리형 구독, AWS IoT 정책, IAM 정책 및 역할을 사용하여 고객의 Greengrass 애플리케이션 보안을 보장합니다. AWS IoT Greengrass AWS IoT 전송 보안 모델을 사용하여 TLS를 사용하여 클라우드와의 통신을 암호화합니다. 또한 AWS IoT Greengrass 데이터는 (클라우드에) 유휴 상태일 때 암호화됩니다. Greengrass 보안에 대한 자세한 내용은 보안 AWS IoT Greengrass 개요를 참조하십시오.

고객은 를 사용하여 AWS IoT Greengrass AWS CloudTrail API 작업을 기록할 수 있습니다. 자세한 내용은 AWS IoT Greengrass API 호출 로깅을 참조하십시오 AWS CloudTrail.

# AWS Lambda

AWS Lambda 고객이 직접 서버를 프로비저닝하거나 관리하지 않고도 코드를 실행할 수 있습니다. AWS Lambda 는 지역 내 여러 가용 영역에 걸쳐 Amazon Elastic Compute Cloud (Amazon EC2) 인스턴스의 컴퓨팅 플릿을 사용하여 AWS 인프라의 고가용성, 보안, 성능 및 확장성을 제공합니다.

PHI를 사용하는 AWS Lambda동안 암호화된 상태를 유지하려면 외부 리소스에 연결할 때 HTTPS 또는 SSL/TLS와 같은 암호화된 프로토콜을 사용해야 합니다. 예를 들어, Lambda 프로시저에서 S3에 액세스하는 경우 https://bucket.s3-aws-region.amazonaws.com 으로 해결해야 합니다.

실행 중인 프로시저 내에서 PHI가 유휴 상태이거나 유휴 상태인 경우 또는 에서 가져온 키를 사용하여 클라이언트 측 또는 서버 측에서 암호화해야 합니다. AWS KMS AWS CloudHSM서비스를 통해 AWS Lambda 함수를 트리거할 때는 Amazon API Gateway에 대한 관련 지침을 따르십시오. 다른 AWS 서비스의 이벤트를 사용하여 AWS Lambda 함수를 트리거하는 경우 이벤트 데이터에 PHI를 포함해서는 안 됩니다. 예를 들어, Lambda 프로시저가 S3 이벤트에서 트리거되는 경우 (예: S3에 객체 도착), Lambda로 전달되는 객체 이름에는 PHI가 없어야 합니다. 단, 객체 자체에는 PHI가 포함될 수 있습니다.

## AWS Managed Services

AWS Managed Services AWS 인프라의 지속적인 관리를 제공합니다. 고객의 인프라를 유지 관리하는 모범 사례를 구현하면 운영 오버헤드와 위험을 줄이는 AWS Managed Services 데 도움이 됩니다. AWS Managed Services 변경 요청, 모니터링, 패치 관리, 보안, 백업 서비스와 같은 일반적인 활동을 자동화하고 인프라를 프로비저닝, 실행 및 지원하는 전체 수명 주기 서비스를 제공합니다.

고객은 PHI를 포함하는 AWS Managed Services 데이터로 운영되는 AWS 워크로드를 관리하는 데 사용할 수 있습니다. 를 사용한다고 해서 PHI와 함께 사용할 수 있는 AWS 서비스가 변경되지는 AWS Managed Services 않습니다. 에서 제공하는 도구 및 자동화는 PHI를 저장하거나 전송하는 데 사용할 AWS Managed Services 수 없습니다.

## AWS OpsWorks 셰프 오토메이트의 경우

AWS OpsWorks for Chef Automate는 인프라 및 애플리케이션 관리를 위한 Chef의 자동화 도구 세트인 Chef Automate를 호스팅하는 완전 관리형 구성 관리 서비스입니다. 서비스 자체는 PHI 또는 민감한 정보를 포함, 전송 또는 처리하지 않지만 고객은 Chef Automate에서 구성한 OpsWorks 모든 리소스가 지침에 따라 구성되었는지 확인해야 합니다. API 호출은 로 AWS CloudTrail캡처됩니다. 자세한 내용은 AWS OpsWorks 스택 API 호출 로깅을 AWS CloudTrail 참조하십시오.

## AWS OpsWorks 퍼펫 엔터프라이즈용

AWS OpsWorks for Puppet Enterprise는 인프라 및 애플리케이션 관리를 위한 Puppet의 자동화 도구 세트인 Puppet Enterprise를 호스팅하는 완전 관리형 구성 관리 서비스입니다. 서비스 자체는 PHI 또는 민감한 정보를 포함, 전송 또는 처리하지 않지만 고객은 Puppet OpsWorks Enterprise용으로 구성

된 모든 리소스가 지침에 따라 구성되어 있는지 확인해야 합니다. API 호출은 를 사용하여 캡처됩니다. AWS CloudTrail자세한 내용은 AWS OpsWorks 스택 API 호출 로깅을 AWS CloudTrail 참조하십시오.

## AWS OpsWorks 스택

AWS OpsWorks 스택은 스택과 애플리케이션을 생성하고 관리할 수 있는 간단하고 유연한 방법을 제공합니다. 고객은 스택을 사용하여 AWS OpsWorks 스택에 애플리케이션을 배포하고 모니터링할 수 있습니다.

AWS OpsWorks Stacks는 전송 중인 모든 트래픽을 암호화합니다. 하지만 암호화된 데이터 백 (Chef 데이터 스토리지 메커니즘) 은 사용할 수 없으며 PHI, 비밀/암호, 인증서 등과 같이 안전하게 저장해야 하는 모든 자산은 Amazon S3의 암호화된 버킷에 저장해야 합니다. AWS OpsWorks Stack은 모든 API 호출을 AWS CloudTrail 기록하는 데 사용합니다.

## AWS Organizations

AWS Organizations 고객이 AWS 리소스를 확장하고 확장할 때 환경을 중앙에서 관리하고 관리할 수 있도록 지원합니다. 를 사용하여 AWS Organizations프로그래밍 방식으로 새 AWS 계정을 만들고 리소스를 할당하고, 계정을 그룹화하여 워크플로를 구성하고, 거버넌스를 위해 계정 또는 그룹에 정책을 적용하고, 모든 계정에 대해 단일 결제 방법을 사용하여 청구를 간소화할 수 있습니다.

또한 다른 AWS 서비스와 AWS Organizations 통합되므로 고객은 중앙 구성, 보안 메커니즘, 감사 요구 사항 및 조직 내 계정 간 리소스 공유를 정의할 수 있습니다. AWS Organizations 모든 AWS 고객이 추가 비용 없이 이용할 수 있습니다.

AWS Organizations 사용자 데이터를 직접 처리, 저장 또는 전송하지 않는 오케스트레이션 서비스입니다. 이 서비스는 고객 콘텐츠를 암호화하지 않지만, 서비스 내에서 AWS Organizations실행되는 기본 서비스는 사용자 데이터를 암호화합니다. AWS Organizations 에서 사용자 AWS CloudTrail, 역할 또는 AWS 서비스가 수행한 작업의 기록을 제공하는 서비스와 통합되어 AWS Organizations있습니다.

## AWS RoboMaker

RoboMaker AWS는 고객이 애플리케이션 개발을 위해 클라우드에서 코드를 실행할 수 있도록 지원하고 애플리케이션 테스트를 가속화하는 로보틱스 시뮬레이션 서비스를 제공합니다. RoboMaker또한 AWS는 원격 애플리케이션 배포, 업데이트 및 관리를 위한 로보틱스 플릿 관리 서비스를 제공합니다.

PHI를 포함하는 네트워크 트래픽은 전송 데이터를 암호화해야 합니다. 시뮬레이션 서버와의 모든 관리 통신은 TLS를 통해 이루어지므로 고객은 다른 AWS 서비스에 연결하기 위해 개방형 표준 전송 암호화

메커니즘을 사용해야 합니다. RoboMaker 또한 AWS는 와 CloudTrail 통합하여 특정 Amazon S3 버킷에 대한 모든 API 호출을 기록합니다.

AWS RoboMaker 로그에는 PHI가 포함되어 있지 않으며 시뮬레이션 서버에서 사용하는 EBS 볼륨은 암호화됩니다. PHI를 포함할 수 있는 데이터를 Amazon S3와 같은 다른 서비스로 전송할 때 고객은 수신 서비스의 PHI 저장 지침을 따라야 합니다. 로봇에 배포할 경우 고객은 전송 중인 데이터와 저장 중인 데이터의 암호화가 지침의 해석과 일치하는지 확인해야 합니다.

## AWS SDK 지표

엔터프라이즈 고객은 AWS CloudWatch 에이전트를 엔터프라이즈 지원용 AWS SDK 지표 (SDK 지표)와 함께 사용하여 호스트 및 클라이언트의 AWS SDK에서 지표를 수집할 수 있습니다. 이러한 지표는 AWS Enterprise Support와 공유됩니다. SDK Metrics를 사용하면 고객이 코드에 사용자 지정 계측을 추가하지 않고도 AWS 서비스에 대한 애플리케이션 연결에 대한 관련 지표 및 진단 데이터를 수집할 수 있으며, 로그와 데이터를 공유하는 데 필요한 수동 작업을 줄일 수 있습니다. AWS Support

SDK 지표는 Enterprise Support 구독을 보유한 AWS 고객만 사용할 수 있다는 점에 유의하십시오. 고객은 AWS 서비스를 직접 호출하고 AWS Metrics 설명서에 나열된 버전 중 하나인 AWS SDK를 사용하여 구축된 모든 애플리케이션에서 SDK 메트릭을 사용할 수 있습니다.

SDK Metrics는 AWS SDK의 호출을 모니터링하고 클라이언트 애플리케이션과 동일한 환경에서 실행되는 CloudWatch 에이전트를 사용합니다.

CloudWatch 에이전트는 로컬 시스템에서 대상 로그 그룹의 전송까지 전송 중인 데이터를 암호화합니다. 로그의 로그 데이터 암호화 사용의 지침에 따라 로그 그룹을 암호화하도록 구성할 수 있습니다. CloudWatch AWS KMS

## AWS Secrets Manager

AWS Secrets Manager는 고객이 “비밀”을 보다 쉽게 관리할 수 있게 해주는 AWS 서비스입니다. 비밀은 데이터베이스 자격 증명, 암호, 타사 API 키, 심지어 임의의 텍스트일 수 있습니다. AWS 이러한 정보가 “비밀”에 포함되어 있는 경우 Secrets Manager를 사용하여 PHI를 저장할 수 있습니다. Secrets Manager에 저장된 모든 AWS 비밀은 AWS 키 관리 시스템 (KMS) 을 사용하여 유휴 상태에서 암호화됩니다. 사용자는 새 암호를 생성할 때 사용할 AWS KMS 키를 선택할 수 있습니다. 키를 선택하지 않으면 계정의 기본 키가 사용됩니다. AWS Secrets Manager는 모든 API 호출을 AWS CloudTrail 기록하는 데 사용합니다.

# AWS Security Hub CSPM

AWS Security Hub CSPM Amazon의 침입 탐지 결과, Amazon Inspector의 취약성 스캔, Amazon Macie의 Amazon S3 버킷 정책 결과 GuardDuty, IAM Access Analyzer의 공개적으로 액세스 가능한 계정 간 리소스, WAF 적용 범위가 부족한 리소스 등 고객 환경에서 사용할 수 있는 AWS 보안 서비스의 결과를 수집하고 통합합니다. AWS Firewall Manager AWS Security Hub CSPM 또한 통합된 AWS 파트너 네트워크 (APN) 보안 솔루션의 결과를 통합합니다.

AWS Security Hub CSPM Amazon CloudWatch Events와 통합되어 고객이 사용자 지정 대응 및 수정 워크플로를 생성할 수 있습니다. 고객은 결과를 SIEM, 채팅 도구, 티켓 시스템, SOAR (보안 오케스트레이션 자동화 및 대응) 도구, 통화 중 관리 플랫폼으로 쉽게 보낼 수 있습니다. 대응 및 수정 조치는 완전히 자동화하거나 콘솔에서 수동으로 트리거할 수 있습니다. 또한 고객은 AWS Systems Manager 자동화 문서 및 AWS Lambda 기능을 사용하여 시작할 수 있는 자동화된 문제 해결 워크플로를 구축할 수 있습니다. AWS Step Functions AWS Security Hub CSPM

데이터 보호를 보장하기 위해 미사용 데이터와 AWS Security Hub CSPM 구성 요소 서비스 간에 전송되는 데이터를 암호화합니다. 타사 감사자는 여러 AWS 규정 준수 프로그램의 AWS Security Hub CSPM 일환으로 보안 및 규정 준수를 평가합니다. AWS Security Hub CSPM AWS의 SOC, ISO, PCI 및 HIPAA 규정 준수 프로그램의 일부입니다.

# AWS Server Migration Service

AWS 서버 마이그레이션 서비스 (AWS SMS) 는 온프레미스 VMware vSphere 또는 Microsoft Hyper-V/SCVMM 가상 머신을 AWS 클라우드로 마이그레이션하는 작업을 자동화합니다. AWS SMS는 서버 VM을 Amazon EC2에 배포할 준비가 된 클라우드 호스팅 Amazon 머신 이미지 (AMI) 로 점진적으로 복제합니다.

온프레미스에서 실행되고 (AWS SMS) 로 클라우드로 마이그레이션되는 서버는 PHI 데이터를 포함할 수 있습니다. AWS SMS는 전송 중에 그리고 EC2에 최종 배치하기 위해 서버 VM 이미지를 스테이징할 때 데이터를 암호화합니다. PHI를 포함하는 서버 VM을 AWS SMS로 마이그레이션할 때는 EC2 및 암호화된 스토리지 볼륨 설정 지침을 참조하십시오. AWS SMS는 모든 API 호출을 CloudTrail 기록하는 데 사용합니다.

# AWS Serverless Application Repository

AWS Serverless Application Repository (SAR) 은 서버리스 애플리케이션을 위한 관리형 리포지토리입니다. 이를 통해 팀, 조직 및 개인 개발자는 재사용 가능한 애플리케이션을 저장 및 공유하고 강력하고 새로운 방식으로 서버리스 아키텍처를 쉽게 조립 및 배포할 수 있습니다. 애플리케이션은 애플리케

이션 인프라의 정의와 애플리케이션 함수 코드의 컴파일된 바이너리를 포함하는 CloudFormation 템플릿입니다. AWS Lambda

에 있는 애플리케이션이 PHI를 처리할 수는 있지만 SAR 자체의 일부가 아닌 고객 계정에 배포한 후에만 PHI를 처리할 수 있습니다. AWS Serverless Application Repository 배포 패키지 및 계층 아카이브를 포함하여 고객이 업로드하는 파일을 AWS Serverless Application Repository 암호화합니다. 전송 중인 데이터의 경우 AWS Serverless Application Repository 는 TLS를 사용하여 서비스와 에이전트 간의 데이터를 암호화합니다. AWS Serverless Application Repository 는 와 통합되어 있으며 AWS CloudTrail, 이는 사용자, 역할 또는 AWS 서비스가 수행한 작업의 기록을 제공하는 AWS Serverless Application Repository서비스입니다.

# 서비스 카탈로그

Service Catalog를 통해 IT 관리자는 승인된 제품 포트폴리오를 만들고 관리하여 최종 사용자에게 배포할 수 있으며, 최종 사용자는 개인화된 포털에서 필요한 제품에 액세스할 수 있습니다. Service Catalog는 AWS에서 셀프 서비스 솔루션을 카탈로그, 공유 및 배포하는 데 사용되며 PHI를 저장, 전송 또는 처리하는 데에는 사용할 수 없습니다. Service Catalog 항목의 메타데이터나 항목 설명 내에 PHI를 삽입해서는 안 됩니다. Service Catalog는 모든 API 호출을 AWS CloudTrail 기록하는 데 사용합니다.

# AWS Shield

AWS Shield AWS에서 실행되는 웹 애플리케이션을 보호하는 관리형 분산 서비스 거부 (DDoS) 보호 서비스입니다. AWS Shield 애플리케이션 다운타임과 지연 시간을 최소화하는 상시 탐지 및 자동 인라인 완화 기능을 제공하므로 DDoS 보호 혜택을 받기 위해 개입할 필요가 없습니다. AWS Support

AWS Shield PHI를 저장하거나 전송하는 데에는 사용할 수 없지만 대신 PHI로 작동하는 웹 애플리케이션을 보호하는 데 사용할 수 있습니다. 따라서 참여 시 특별한 구성이 필요하지 않습니다. AWS Shield

모든 AWS 고객은 추가 비용 없이 자동 보호 기능을 이용할 수 있습니다. AWS Shield Standard AWS Shield Standard 웹 사이트 또는 애플리케이션을 대상으로 하는 가장 흔하고 자주 발생하는 네트워크 및 전송 계층 DDoS 공격을 방어합니다. Elastic Load Balancing (ELB) CloudFront, Amazon 및 Amazon Route 53 리소스에서 실행되는 웹 애플리케이션을 대상으로 하는 공격으로부터 더 높은 수준의 보호를 받으려면 AWS Shield Advanced고객이 구독할 수 있습니다.

# AWS Snowball Edge

AWS Snowball Edge (Snowball) 를 사용하면 고객은 온프레미스 데이터 센터와 Amazon Simple Storage Service (Amazon S3) 간에 수백 테라바이트 또는 페타바이트의 데이터를 전송할 수 있습니다.

에 저장된 PHI는 지침에 따라 유휴 상태에서 AWS Snowball Edge 암호화해야 합니다. 가져오기 작업을 생성할 때 고객은 Snowball 내 데이터를 보호하는 데 사용할 AWS KMS 키의 ARN을 지정해야 합니다. 또한 고객은 가져오기 작업을 생성할 때 지침에서 설정한 암호화 표준을 충족하는 대상 S3 버킷을 선택해야 합니다.

Snowball은 현재 관리 키를 사용한 서버 측 암호화 (SSE-KMS) 또는 고객 제공 키를 사용한 서버 측 암호화 (SSE-C) 를 지원하지 않지만, Snowball은 Amazon S3에서 AWS KMS관리하는 암호화 키 (SSE-S3) 를 사용한 서버 측 암호화를 지원합니다. 더 자세한 내용은 Amazon S3-관리 암호화 키(SSE-S3)와 함께 서버측 암호화를 사용하여 보호하기를 참조하십시오.

또는 고객이 데이터를 저장하기 전에 원하는 암호화 방법을 사용하여 PHI를 암호화할 수도 있습니다. AWS Snowball Edge

현재 고객은 표준 AWS Snowball Edge 어플라이언스를 BAA의 일부로 사용할 수 있습니다.

## AWS Snowball Edge 에지

AWS Snowball Edge Edge는 표준 스토리지 인터페이스를 사용하여 기존 고객 애플리케이션 및 인프라에 연결하여 데이터 전송 프로세스를 간소화하고 설정 및 통합을 최소화합니다. Snowball Edge는 함께 클러스터링하여 로컬 스토리지 계층을 형성하고 고객 데이터를 현장에서 처리하므로 고객이 클라우드에 액세스할 수 없는 경우에도 애플리케이션이 계속 실행되도록 할 수 있습니다.

Snowball Edge를 사용하는 동안 PHI가 암호화된 상태를 유지할 수 있도록 고객은 Snowball Edge 외부 리소스와 PHI를 주고 AWS IoT Greengrass 받는 프로시저를 사용할 때 AWS Lambda HTTPS 또는 SSL/TLS와 같은 암호화된 연결 프로토콜을 사용해야 합니다. 또한 PHI는 로컬 액세스 또는 NFS를 통해 Snowball Edge의 로컬 볼륨에 저장되는 동안 암호화해야 합니다. 암호화는 Snowball 관리 콘솔과 S3로의 대량 전송을 위한 API를 사용하여 Snowball Edge에 배치된 데이터에 자동으로 적용됩니다. S3로의 데이터 전송에 대한 자세한 내용은 의 관련 지침을 참조하십시오. the section called “AWS Snowball Edge”

## AWS Step Functions

AWS Step Functions 시각적 워크플로를 사용하여 분산 애플리케이션 및 마이크로서비스의 구성 요소를 쉽게 조정할 수 있습니다. AWS Step Functions PHI를 저장, 전송 또는 처리할 수 없습니다. PHI를 작업 또는 상태 시스템 정의의 메타데이터 내부 AWS Step Functions 또는 내부에 배치해서는 안 됩니다. AWS Step Functions 모든 API 호출을 AWS CloudTrail 기록하는 데 사용합니다.

# AWS Storage Gateway

AWS Storage Gateway 고객의 온 프레미스 애플리케이션이 AWS 클라우드 스토리지를 원활하게 사용할 수 있도록 지원하는 하이브리드 스토리지 서비스입니다. 게이트웨이는 개방형 표준 스토리지 프로토콜을 사용하여 기존 스토리지 애플리케이션과 워크플로를 AWS 클라우드 스토리지 서비스에 연결하여 프로세스 중단을 최소화합니다.

## 파일 게이트웨이

파일 게이트웨이는 Amazon S3에 대한 AWS Storage Gateway 파일 인터페이스를 지원하고 현재 블록 기반 볼륨 및 VTL 스토리지에 추가하는 유형입니다. 파일 게이트웨이는 HTTPS를 사용하여 S3와 통신하고, 기본적으로 SSE-S3 또는 키가 저장된 클라이언트 측 암호화를 사용하여 S3에 있는 동안 암호화된 모든 객체를 저장합니다. AWS KMS파일 이름과 같은 파일 메타데이터는 암호화되지 않은 상태로 유지되며 PHI를 포함하지 않아야 합니다.

## 볼륨 게이트웨이

볼륨 게이트웨이는 고객이 온프레미스 애플리케이션 서버에서 인터넷 소형 컴퓨터 시스템 인터페이스 (iSCSI) 디바이스로 마운트할 수 있는 클라우드 기반 스토리지 볼륨을 제공합니다. 고객은 내부 규정 준수 및 규제 요구 사항에 따라 로컬 디스크를 볼륨 게이트웨이 VM에 업로드 버퍼 및 캐시로 연결해야 합니다. PHI의 경우 이러한 디스크가 저장 시 암호화를 제공할 수 있어야 하는 것이 좋습니다. 볼륨 게이트웨이 VM과 AWS 간의 통신은 TLS 1.2를 사용하여 암호화되어 전송 중인 PHI를 보호합니다.

## Tape Gateway

테이프 게이트웨이는 온프레미스에서 실행되는 타사 백업 애플리케이션에 VTL (가상 테이프 라이브러리) 인터페이스를 제공합니다. 고객은 테이프 백업 작업을 설정할 때 타사 백업 애플리케이션 내에서 PHI 암호화를 활성화해야 합니다. 테이프 게이트웨이 VM과 AWS 간의 통신은 TLS 1.2를 사용하여 암호화되어 전송 중인 PHI를 보호합니다. PHI와 함께 Storage Gateway 구성을 사용하는 고객은 전체 로깅을 활성화해야 합니다. 자세한 내용은 AWS Storage Gateway이란 무엇인가요?를 참조하세요.

# AWS Systems Manager

AWS Systems Manager 고객이 운영 데이터를 쉽게 중앙 집중화하고, AWS 리소스 전반에서 작업을 자동화하고, 인프라에서 운영 문제를 감지하고 해결하는 시간을 단축할 수 있는 통합 인터페이스입니다. Systems Manager는 고객의 인프라 성능 및 구성을 전체적으로 파악하고, 리소스 및 애플리케이션 관리를 단순화하고, 규모에 맞게 인프라를 쉽게 운영 및 관리할 수 있도록 합니다.

PHI를 포함할 수 있는 데이터를 Amazon S3와 같은 다른 서비스에 출력할 때 고객은 PHI 저장에 대한 수신 서비스의 지침을 따라야 합니다. 고객은 문서 이름 및 파라미터 이름과 같은 메타데이터나 식별자에 PHI를 포함해서는 안 됩니다.

## AWS Transfer for SFTP

SFTP용 AWS Transfer는 고객의 S3 리소스에 대한 보안 파일 전송 프로토콜 (SFTP) 액세스를 제공합니다. 고객에게는 지역 서비스 엔드포인트에서 표준 SFTP 프로토콜을 사용하여 액세스할 수 있는 가상 서버가 제공됩니다. AWS 고객과 SFTP 클라이언트의 관점에서 SFTP 게이트웨이는 고가용성 표준 SFTP 서버처럼 보입니다. 서비스 자체는 PHI를 저장, 처리 또는 전송하지 않지만 고객이 Amazon S3에서 액세스하는 리소스는 지침과 일치하는 방식으로 구성해야 합니다. 또한 고객은 SFTP용 AWS Transfer에 대한 API 호출을 기록하는 AWS CloudTrail 데 사용할 수 있습니다.

## AWS WAF — 웹 애플리케이션 방화벽

AWS WAF는 애플리케이션 가용성에 영향을 미치거나, 보안을 손상시키거나, 리소스를 과도하게 소비할 수 있는 일반적인 웹 공격으로부터 고객 웹 애플리케이션을 보호하는 데 도움이 되는 웹 애플리케이션 방화벽입니다. 고객은 PHI를 사용하거나 PHI를 교환하는 AWS에 호스팅되는 웹 애플리케이션과 최종 사용자 사이에 AWS WAF를 배치할 수 있습니다. AWS에서 PHI를 전송할 때와 마찬가지로 PHI를 포함하는 데이터는 전송 중에 암호화해야 합니다. 사용 가능한 암호화 옵션을 더 잘 이해하려면 Amazon EC2 지침을 참조하십시오.

## AWS X-Ray

AWS X-Ray 고객의 애플리케이션이 처리하는 요청에 대한 데이터를 수집하고, 고객이 해당 데이터를 보고, 필터링하고, 통찰력을 확보하여 문제와 최적화 기회를 식별하는 데 사용할 수 있는 도구를 제공하는 서비스입니다. 고객 애플리케이션에 대한 모든 추적 요청의 경우 요청 및 응답뿐만 아니라 애플리케이션이 다운스트림 AWS 리소스, 마이크로서비스, 데이터베이스 및 HTTP 웹 API에 대해 수행하는 호출에 대한 세부 정보도 볼 수 있습니다. AWS X-Ray PHI를 저장하거나 처리하는 데 사용해서는 안 됩니다. 송수신되는 정보는 기본적으로 암호화됩니다. AWS X-Ray 사용 AWS X-Ray시 세그먼트 주석이나 세그먼트 메타데이터에 PHI를 삽입하지 마십시오.

## Elastic Load Balancing

고객은 Elastic Load Balancing을 사용하여 PHI를 포함하는 세션을 종료하고 처리할 수 있습니다. 고객은 Classic Load Balancer 또는 Application Load Balancer를 선택할 수 있습니다. PHI를 포함하는 모

든 네트워크 트래픽은 전송 중에 end-to-end 암호화되어야 하므로 고객은 두 가지 아키텍처를 유연하게 구현할 수 있습니다.

고객은 연결에 암호화된 프로토콜을 사용하는 로드 밸런서를 생성하여 Elastic Load Balancing에서 HTTPS, TLS를 통한 HTTP/2 (애플리케이션용) 또는 SSL/TLS를 종료할 수 있습니다. 이 기능을 사용하면 로드 밸런서와 HTTPS, HTTP/2 over TLS 또는 SSL/TLS 세션을 시작하는 클라이언트 간의 트래픽 암호화와 로드 밸런서와 고객 백엔드 인스턴스 간의 연결을 암호화할 수 있습니다. PHI를 포함하는 세션은 전송 암호화를 위해 프런트엔드와 백엔드 리스너를 모두 암호화해야 합니다. 고객은 인증서와 세션 협상 정책을 평가하고 지침과 일관되게 유지해야 합니다. 자세한 내용은 Classic Load Balancer의 HTTPS 리스너를 참조하십시오.

또는 고객은 Amazon ELB를 기본 TCP 모드 (클래식용) 또는 오버 WebSockets (애플리케이션용) 로 구성하고 암호화된 세션을 암호화된 세션이 종료되는 백엔드 인스턴스로 전달할 수 있습니다. 이 아키텍처에서 고객은 자체 인스턴스에서 실행되는 애플리케이션의 자체 인증서 및 TLS 협상 정책을 관리합니다. 자세한 내용은 Classic Load Balancer의 리스너를 참조하십시오. 두 아키텍처 모두에서 고객은 HIPAA 및 HITECH 요구 사항에 부합한다고 판단되는 수준의 로깅을 구현해야 합니다.

## FreeRTOS

FreeRTOS는 소형 저전력 에지 장치를 쉽게 프로그래밍, 배포, 보호, 연결 및 관리할 수 있게 해주는 마이크로컨트롤러용 운영 체제입니다. FreeRTOS는 마이크로컨트롤러용으로 널리 사용되는 오픈 소스 운영 체제인 FreeRTOS 커널을 기반으로 하며, 소형 저전력 디바이스를 Core와 같은 AWS 클라우드 서비스 또는 실행 중인 더 강력한 에지 디바이스에 쉽게 안전하게 연결할 수 있는 소프트웨어 라이브러리로 이를 확장합니다. AWS IoT AWS IoT Greengrass

이제 FreeRTOS를 실행하는 적격 장치를 사용할 때 PHI를 포함하는 데이터를 전송 중 및 유휴 상태에서 암호화할 수 있습니다. FreeRTOS는 플랫폼 보안을 제공하는 두 가지 라이브러리, 즉 TLS 및 PKCS #11 라이브러리를 제공합니다. PHI를 포함하는 모든 네트워크 트래픽을 암호화하고 인증하려면 TLS API를 사용해야 합니다. PKCS #11 는 소프트웨어 암호화 작업을 위한 표준 인터페이스를 제공하며 FreeRTOS를 실행하는 적격 장치에 저장된 모든 PHI를 암호화하는 데 사용해야 합니다.

## AWS KMS PHI 암호화에 사용

KMS 키는 고객의 애플리케이션 또는 사용하는 AWS 서비스에서 PHI를 암호화하는 데 사용되는 데이터 암호화 키를 암호화/복호화하는 데 사용할 수 있습니다. AWS KMS AWS KMS HIPAA 계정과 함께 사용할 수 있지만 PHI는 HIPAA 적격 서비스에서만 처리, 저장 또는 전송할 수 있습니다. AWS KMS 일반적으로 다른 HIPAA 적격 서비스에서 실행되는 애플리케이션의 키를 생성하고 관리하는 데 사용됩니다.

예를 들어 Amazon EC2에서 PHI를 처리하는 애플리케이션은 API 호출을 사용하여 GenerateDataKey 애플리케이션에서 PHI를 암호화 및 복호화하기 위한 데이터 암호화 키를 생성할 수 있습니다. 데이터 암호화 키는 저장된 고객의 KMS 키로 보호되므로 API 호출이 로그인되므로 감사가 매우 AWS KMS용이한 키 계층 구조가 만들어집니다. AWS KMS AWS CloudTrail저장된 모든 키의 PHI를 태그 (메타데이터) 에 저장해서는 안 됩니다. AWS KMS

# VM Import

VM Import/Export를 사용하면 고객이 기존 환경에서 Amazon EC2 인스턴스로 가상 머신 이미지를 쉽게 가져와서 다시 온 프레미스 환경으로 내보낼 수 있습니다. 이 오퍼링을 통해 고객은 가상 머신을 Amazon ready-to-use EC2에 인스턴스로 가져와서 IT 보안, 구성 관리 및 규정 준수 요구 사항을 충족하도록 구축한 가상 머신에 대한 기존 투자를 활용할 수 있습니다. 또한 고객은 가져온 인스턴스를 온프레미스 가상화 인프라로 다시 내보내 IT 인프라 전체에 워크로드를 배포할 수 있습니다.

VM 가져오기/내보내기는 Amazon EC2 및 Amazon S3의 표준 사용 요금 외에 추가 비용 없이 사용할 수 있습니다.

고객 이미지를 가져오려면 고객은 AWS CLI 또는 다른 개발자 도구를 사용하여 VMware 환경에서 가상 머신 (VM) 이미지를 가져올 수 있습니다. VMware vSphere 가상화 플랫폼을 사용하는 고객은 vCenter용 AWS 관리 포털을 사용하여 가상 머신을 가져올 수도 있습니다. 가져오기 프로세스의 일부로 VM Import는 고객 VM을 Amazon EC2 AMI로 변환하여 Amazon EC2 인스턴스를 실행하는 데 사용할 수 있습니다. VM을 가져오고 나면 Auto Scaling, Elastic Load Balancing과 같은 서비스를 통해 Amazon의 탄력성, 확장성 및 CloudWatch 모니터링을 활용하고 가져온 이미지를 지원할 수 있습니다.

고객은 Amazon EC2 API 도구를 사용하여 이전에 가져온 Amazon EC2 인스턴스를 내보낼 수 있습니다. 대상 인스턴스, 가상 머신 파일 형식, 대상 Amazon S3 버킷을 지정하기만 하면 VM Import/Export가 암호화 옵션과 함께 인스턴스를 Amazon S3 버킷으로 자동으로 내보내 VM 이미지의 전송 및 저장을 보호합니다. 그러면 고객은 온프레미스 가상화 인프라 내에서 내보낸 VM을 다운로드하고 시작할 수 있습니다.

고객은 VMware ESX 또는 워크스테이션, Microsoft Hyper-V 및 Citrix Xen 가상화 형식을 사용하는 Windows 및 Linux VM을 가져올 수 있습니다. 또한 고객은 이전에 가져온 Amazon EC2 인스턴스를 VMware ESX, Microsoft Hyper-V 또는 Citrix Xen 형식으로 내보낼 수 있습니다. 지원되는 운영 체제, 버전 및 형식의 전체 목록은 VM 가져오기/내보내기 요구 사항을 참조하십시오. AWS는 향후 추가 운영 체제, 버전 및 형식에 대한 지원을 추가할 계획입니다.

# 감사, 백업 및 재해 복구

HIPAA의 보안 규칙에는 심층 감사 기능, 데이터 백업 절차 및 재해 복구 메커니즘과 관련된 세부 요구 사항이 있습니다. AWS의 서비스에는 고객이 요구 사항을 해결하는 데 도움이 되는 많은 기능이 포함되어 있습니다. 예를 들어, 고객은 보안 분석가가 자세한 활동 로그 또는 보고서를 검토하여 누가 액세스했는지, IP 주소 입력, 액세스한 데이터 등을 확인할 수 있도록 감사 기능을 구축하는 것을 고려해야 합니다.

감사에 대비하여 이 데이터를 중앙 위치에서 장기간 추적, 기록 및 저장해야 합니다. Amazon EC2를 사용하면 고객은 기존 하드웨어에서와 마찬가지로 가상 서버의 패킷 레이어까지 활동 로그 파일 및 감사를 실행할 수 있습니다. 또한 가상 서버 인스턴스에 도달하는 모든 IP 트래픽을 추적할 수 있습니다. 고객의 관리자는 로그 파일을 Amazon S3에 백업하여 장기간 안정적으로 보관할 수 있습니다.

또한 HIPAA에는 긴급 상황 발생 시 데이터를 보호하기 위한 비상 계획 유지와 관련된 세부 요구 사항이 있으며, 검색 가능한 정확한 전자 PHI 사본을 생성하고 유지해야 합니다. AWS에서 데이터 백업 계획을 구현하기 위해 Amazon EBS는 Amazon EC2 가상 서버 인스턴스를 위한 영구 스토리지를 제공합니다. 이러한 볼륨은 표준 블록 디바이스로 노출될 수 있으며, 인스턴스 수명과 무관하게 지속되는 오프 인스턴스 스토리지를 제공합니다. HIPAA 지침을 준수하기 위해 고객은 Amazon S3에 자동으로 저장되고 다른 가용 영역의 장애로부터 격리되도록 설계된 별개의 위치인 여러 가용 영역에 복제되는 Amazon EBS 볼륨의 point-in-time 스냅샷을 생성할 수 있습니다.

이러한 스냅샷은 언제든지 액세스할 수 있으며 데이터를 보호하여 장기적인 내구성을 유지할 수 있습니다. 또한 Amazon S3는 데이터 스토리지 및 자동 백업을 위한 고가용성 솔루션을 제공합니다. 파일이나 이미지를 Amazon S3에 로드하기만 하면 여러 개의 중복 사본이 자동으로 생성되어 별도의 데이터 센터에 저장됩니다. 이러한 파일은 언제 어디서나 (권한에 따라) 액세스할 수 있으며 의도적으로 삭제될 때까지 저장됩니다.

또한 AWS는 기본적으로 다양한 재해 복구 메커니즘을 제공합니다. 재해 발생 시 조직의 데이터와 IT 인프라를 보호하는 프로세스인 재해 복구에는 가용성이 높은 시스템을 유지 관리하고, 데이터와 시스템을 모두 오프사이트에 복제하고, 두 데이터에 지속적으로 액세스할 수 있도록 하는 것이 포함됩니다.

Amazon EC2를 사용하면 관리자가 서버 인스턴스를 매우 빠르게 시작할 수 있으며 엘라스틱 IP 주소 (클라우드 컴퓨팅 환경의 고정 IP 주소) 를 사용하여 한 시스템에서 다른 시스템으로의 정상적인 장애 조치를 수행할 수 있습니다. Amazon EC2는 가용 영역도 제공합니다. 관리자는 여러 가용 영역에서 Amazon EC2 인스턴스를 시작하여 지리적으로 다양하고 내결함성이 있는 시스템을 만들 수 있습니다. 이 시스템은 네트워크 장애, 자연 재해 및 대부분의 기타 가동 중지 가능성이 있는 발생 시 복원력이 뛰어납니다.

Amazon S3를 사용하면 고객 데이터가 별도의 데이터 센터에 복제되고 자동으로 저장되므로 99.99% 가용성을 제공하도록 설계된 안정적인 데이터 스토리지가 제공됩니다.

고객은 AWS Elastic Disaster Recovery (AWS DRS) 를 사용하여 애플리케이션의 up-to-date 상태가 가장 높거나 이전 시점부터 AWS에서 애플리케이션을 신속하게 복구할 수 있습니다.

# 문서 수정

이 설명서에 대한 업데이트 알림을 받으려면 RSS 피드를 구독하면 됩니다.

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| 마이너 업데이트 | 마이너 업데이트 | 2023년 5월 12일 |
| 마이너 업데이트 | 서비스에서 사용할 수 있는 콘텐츠를 확대하기 위해 백서를 업데이트했습니다. | 2022년 9월 28일 |
| 마이너 업데이트 | 포괄적이지 않은 언어를 수정하세요. | 2022년 4월 6일 |
| 백서 업데이트 | AWS 애플리케이션 마이그레이션 서비스에 대한 정보 추가 및 Amazon ECS 정보 업데이트 | 2021년 12월 6일 |
| 백서 업데이트 | Amazon Healthlake 및 Amazon VPC 섹션의 정보가 업데이트되었습니다. | 2021년 11월 9일 |
| 백서 업데이트 | AWS 네트워크 방화벽에 대한 정보가 추가되었습니다. | 2021년 9월 9일 |
| 백서 업데이트 | Amazon Connect 고객 프로필에 대한 정보가 업데이트되었습니다. | 2021년 8월 26일 |
| 백서 업데이트 | 아마존 AppFlow 및 AWS Glue 섹션 추가 DataBrew | 2021년 7월 22일 |
| 백서 업데이트 | 탐색 및 구성이 업데이트되었습니다. | 2021년 4월 26일 |
| 백서 업데이트 | ,, 아마존 오로라 AWS CodeDeploy AWS CodePipel | 2021년 3월 31일 |

| | | |
|---|---|---|
| | ine, Aurora PostgreSQL, 아마존 텍스트트랙, 아마존 폴리, 아마존 FSx, AWS Auto Scaling,,,, VM 가져오기/내보내기, 아마존, 아마존, 아마존 등의 섹션이 추가되었습니다. AWS Backup AWS Elastic Beanstalk AWS Firewall Manager AWS Organizations AWS Security Hub CSPM AWS Serverless Application Repository HealthLake EventBridge Amazon Aurora 섹션이 업데이트되었습니다. | |
| 백서 업데이트 | AWS App Mesh에 섹션을 추가하고 AWS 시스템 관리자 콘텐츠를 업데이트했습니다. | 2020년 8월 25일 |
| 백서 업데이트 | 아마존 앱스트림 2.0, AWS SDK 메트릭, AWS 데이터 익스체인지, 아마존 MSK, 아마존 핀포인트, 아마존 렉스, 아마존 SES, 아마존 예측, 아마존 퀀텀 레저 데이터베이스 (QLDB) 등의 섹션이 추가되었습니다. AWS Cloud Map | 2020년 5월 7일 |

| | | |
|---|---|---|
| 백서 업데이트 | 아마존, 아마존 CloudWatch 이벤트 CloudWatch, 아마존 데이터 파이어호스, 아파치 플링크용 아마존 매니지드 서비스, 아마존 서비스, OpenSearch 아마존 DocumentDB (MongoDB 호환), AWS Mobile Hub, AWS OpsWorks 셰프 오토메이트용, 퍼펫 엔터프라이즈용, AWS AWS IoT Greengrass Transfer for SFTP, AWS, Amazon Comprehend Medical 및 DataSync AWS에 섹션을 추가했습니다.. AWS OpsWorks AWS Global Accelerator RoboMaker | 2020년 1월 1일 |
| 백서 업데이트 | 아마존 Comprehend, Amazon Transcribe, Amazon Translate 및 AWS Certificate Manager에 섹션이 추가되었습니다. | 2019년 1월 1일 |
| 백서 업데이트 | 아마존 아테나, 아마존 EKS, AWS IoT 코어 및 아마존 AWS IoT Device Management프리어토스, 아마존, 아마존 넵튠, AWS 서버 마이그레이션 서비스, GuardDuty 아마존 MQ 등에 섹션이 추가되었습니다. AWS Database Migration Service AWS Glue | 2018년 11월 1일 |

| | | |
|---|---|---|
| 백서 업데이트 | 아마존 Elastic File System (EFS), 아마존 키네시스 비디오 스트림, 아마존 Rekognition, 아마존, 아마존 심플 워크플로, SageMaker AWS Secrets Manage, Service Catalog 등에 섹션이 추가되었습니다. AWS Step Functions | 2018년 6월 1일 |
| 백서 업데이트 | AWS CloudFormation,,,, AWS X-Ray AWS CloudTrail AWS CodeBuild AWS CodeCommit, AWS Config스택에 대한 섹션이 추가되었습니다. AWS OpsWorks | 2018년 4월 1일 |
| 백서 업데이트 | 에 섹션이 추가되었습니다 AWS Fargate. | 2018년 1월 1일 |

2018년 이전에 이루어진 업데이트:

| 날짜 | 설명 |
|---|---|
| 2017년 11월 | Amazon EC2 컨테이너 레지스트리, Amazon Macie, Amazon 등에 섹션을 추가했습니다. QuickSight AWS Managed Services |
| 2017년 11월 | Amazon에서 Redis와 ElastiCache Amazon용 섹션을 추가했습니다. CloudWatch |
| 2017년 10월 일 | 아마존 SNS, 아마존 루트 53 및 에 섹션을 추가했습니다 AWS CloudHSM. AWS Storage Gateway에 섹션이 업데이트되었습니다 AWS Key Management Service. |
| 2017년 9월 일 | 아마존 커넥트, 아마존 키네시스 스트림, 아마존 RDS (마리아) DB, 아마존 RDS SQL 서버,,, |

| 날짜 | 설명 |
| --- | --- |
| | 엣지 AWS Batch AWS Lambda AWS Snowball Edge , 아마존의 Lambda @Edge 기능에 섹션을 추가했습니다. CloudFront |
| 2017년 8월 | Amazon EC2 Systems Manager 및 Amazon Inspector에 섹션이 추가되었습니다. |
| 2017년 7월 | 아마존 WorkSpaces, 아마존, AWS 디렉터리 서비스 WorkDocs, 아마존 ECS에 섹션을 추가했습니다. |
| 2017년 6월 | 아마존 CloudFront, AWS WAF 및 아마존 S3 Transfer AWS Shield Acceleration에 대한 섹션이 추가되었습니다. |
| 2017년 5월 | EC2 및 EMR에서 PHI를 처리하기 위한 전용 인스턴스 또는 전용 호스트에 대한 요구 사항을 제거했습니다. |
| 2017년 3월 일 | 규정 준수 프로그램의 AWS 범위 내 서비스 페이지를 가리키도록 서비스 목록을 업데이트했습니다. Amazon API Gateway에 대한 설명이 추가되었습니다. |
| 2017년 1월 | 최신 템플릿으로 업데이트되었습니다. |
| 2016년 10월 일 | 첫 게시 |

# 고지 사항

고객은 본 문서의 정보를 독립적으로 평가할 책임이 있습니다. 이 문서: (a) 정보 제공만을 목적으로 하고, (b) 현행 AWS 제품 제공 및 관행을 나타내며, (c) AWS와 그 계열사, 공급업체 또는 라이선스 제공자로부터 어떠한 약정이나 보증도 하지 않습니다. AWS 제품 또는 서비스는 명시적이든 묵시적이든 어떠한 종류의 보증, 진술 또는 조건 없이 “있는 그대로” 제공됩니다. 고객에 대한 AWS의 책임 및 채무는 AWS 계약에 준거합니다. 본 문서는 AWS와 고객 간의 어떠한 계약도 구성하지 않으며 이를 변경하지도 않습니다.

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.