の暗号化のベストプラクティスと機能 AWS のサービス

AWS 規範ガイダンス

AWS 規範ガイダンス: の暗号化のベストプラクティスと機能 AWS のサービス

Table of Contents

暗号化のベストプラクティスと AWS のサービスの機能

Kurt Kumar、Amazon Web Services

2024 年 9 月 (ドキュメント履歴)

暗号化は、デジタル時代の機密データを保護するための基本的なサイバーセキュリティツールです。生成 AI のデプロイなど、組織がデータにますます依存するにつれて、堅牢な暗号化プラクティスを通じてこの貴重な情報を保護することは、包括的なデータ保護戦略の重要な要素となっています。このガイドは、暗号化の原則と が提供する AWS 暗号化機能を理解するのに役立ちます。

最新のサイバーセキュリティの脅威には、データ侵害のリスクが含まれます。これは、情報アセットへの不正アクセスによってデータが失われた場合です。データは、各組織に固有のビジネスアセットです。これには、顧客情報、事業計画、設計文書、コードなどが含まれます。ビジネスを保護するということは、データを保護するということです。

データ暗号化は、侵害が発生した後でもビジネスデータを保護するのに役立ちます。意図しない開示に対する防御レイヤーを提供します。 AWS クラウド内の暗号化されたデータにアクセスするには、ユーザーは、キーを使用して復号化する権限と、データが保存されているサービスを使用する権限を必要とします。この両方の権限がないと、ユーザーはデータを復号化して表示することができません。

通常、暗号化できるデータは 3 種類あります。1 つは転送中のデータで、ネットワーク内 (ネットワークリソース間など) を活発に移動するデータのことです。もう 1 つは保管中のデータで、ストレージ内のデータなど、静止していて休眠中のデータのことです。例としては、ブロックストレージ、オブジェクトストレージ、データベース、アーカイブ、モノのインターネット (IoT) デバイスなどです。使用中のデータとは、アプリケーションまたはサービスがアクティブに処理または使用しているデータを指します。組織は、使用時にデータを保護することで、意図しない開示のリスクを軽減できます。

このガイドでは、転送中のデータと保管中のデータを暗号化するための考慮事項とベストプラクティスについて説明します。また、多くの で使用できる暗号化機能とコントロールについても確認します AWS のサービス。これらの暗号化レコメンデーションは、 AWS クラウド 環境のサービスレベルで実装できます。

対象者

このガイドは、公共機関と民間企業の両方の、小規模、中規模、大規模の組織で使用できます。組織がデータ保護戦略の評価と実施の初期段階にあるか、または既存のセキュリティ管理の強化を目指しているかにかかわらず、このガイドで説明する推奨事項は次の対象者に最適です。

- 最高執行責任者 ()、最高技術責任者 (CEOs) 、最高情報責任者 (CTOs) 、最高情報セキュリティ責任者 (CISOs) などCIOs、企業のポリシーを策定する執行責任者
- 技術担当副社長や取締役など、技術標準の設定を担当する技術責任者
- 以下の責任を負うビジネスステークホルダーとアプリケーションオーナー
  - リスク体制、データ分類、保護要件の評価
  - 確立された組織基準の遵守状況の監視
- 法定および任意のコンプライアンス制度を含む、コンプライアンスポリシーの遵守状況の監視を担当するコンプライアンス、内部監査、ガバナンス担当者

AWS 暗号化サービスについて

暗号化アルゴリズムとは、プレーンテキストのメッセージを暗号化された暗号文に変換する数式または手順のことです。暗号化やその用語に初めて触れる場合は、まず「About data encryption」と「Cryptography concepts」を読んでから、このガイドを読むことをお勧めします。

AWS 暗号化サービスは、安全なオープンソースの暗号化アルゴリズムに依存しています。これらのアルゴリズムは、公的標準化団体や学術研究によって精査されています。一部の AWS ツールやサービスは特定のアルゴリズムの使用を強制します。他のサービスでは、複数のアルゴリズムとキーの長さから選択したり、推奨デフォルトを使用したりできます。

このセクションでは、AWS ツールとサービスがサポートするアルゴリズムについて説明します。このアルゴリズムは、キーの機能によって、対称型と非対称型の 2 つのカテゴリに分類されます。

- 対象暗号化では、同じキーを使用してデータを暗号化および復号化します。AWS のサービスは、広く使われている対称アルゴリズムである Advanced Encryption Standard (AES) とTriple Data Encryption Standard (3DES または TDES) をサポートしています。詳細については、「AWS cryptographic services and tools guide」の「Symmetric algorithms」を参照してください。
- 非対称暗号化では、暗号化用のパブリックキーと復号化用のプライベートキーから成る 1 組のキーを使用します。パブリックキーは復号化には使用されないので共有できますが、プライベートキーへのアクセスは厳しく制限する必要があります。AWS のサービス は通常、RSA と楕円曲線暗号 (ECC) の非対称アルゴリズムをサポートしています。詳細については、「AWS cryptographic services and tools guide」の「Asymmetric algorithms」を参照してください。

AWS 暗号化サービスは幅広い暗号セキュリティ標準に準拠しているため、政府や専門家の規制に準拠できます。AWS のサービス が準拠しているデータセキュリティ基準の詳細なリストについては、「AWS コンプライアンスプログラム」を参照してください。暗号化ツールとサービスの詳細については、「AWS cryptographic services and tools」を参照してください。

暗号化のベストプラクティスの概略

このセクションでは、 でデータを暗号化する場合に適用される推奨事項を示します AWS クラウド。これらの一般的な暗号化のベストプラクティスは、 に固有ではありません AWS のサービス。このセクションでは、次のトピックについて説明します。

- データ分類
- 転送中のデータの暗号化
- 保管中のデータの暗号化

データ分類

データ分類とは、ネットワーク内のデータを重要度と機密性に基づいて識別、分類するプロセスのことです。データに適した保護および保持のコントロールを判断する際に役立つため、あらゆるサイバーセキュリティのリスク管理戦略において重要な要素です。データ分類は、 Well-Architected フレームワークのセキュリティの AWS 柱のコンポーネントです。カテゴリには、極秘データ、機密データ、非機密データ、公開データなどがありますが、分類階層とその名前は組織によって異なる場合があります。データ分類プロセス、考慮事項、モデルの詳細については、「データ分類 (AWS ホワイトペーパー) 」を参照してください。

データを分類したら、各カテゴリに必要な保護レベルに基づいて、組織の暗号化戦略を作成することができます。例えば、極秘データには非対称暗号化を使用し、公開データには暗号化は必要ないと組織で判断する場合があります。暗号化戦略の設計の詳細については、「Creating an enterprise encryption strategy for data at rest」を参照してください。このガイドに記載されている技術的な考慮事項と推奨事項は保管中のデータに限られていますが、段階的なアプローチを使用して転送中のデータの暗号化戦略を作成することもできます。

転送中のデータの暗号化

AWS グローバルネットワーク AWS リージョン 経由で 間で送信されるすべてのデータは、 AWS 安全な施設を離れる前に、物理レイヤーで自動的に暗号化されます。アベイラビリティーゾーン間のトラフィックは、すべて暗号化されます。

AWS クラウドで転送中のデータを暗号化するときの一般的なベストプラクティスを次に示します。

- データ分類、組織の要件、該当する規制やコンプライアンス基準に基づいて、転送中のデータに関する組織の暗号化ポリシーを定義します。極秘データ、または機密データに分類される転送中の

データを暗号化することを強くお勧めします。ポリシーによっては、必要に応じて、非機密データや公開データなど、他のカテゴリの暗号化を指定する場合もあります。

- 転送中のデータを暗号化する場合は、暗号化ポリシーで定義されている承認済みの暗号化アルゴリズム、ブロック暗号モード、キーの長さを使用することをお勧めします。
- 次のいずれかを使用して、企業ネットワークと AWS クラウド インフラストラクチャ内の情報アセットとシステム間のトラフィックを暗号化します。
  - AWS Site-to-Site VPN 接続
  - IPsec暗号化されたプライベートAWS Direct Connect接続を提供する AWS Site-to-Site VPN と接続の組み合わせ
  - AWS Direct Connect 企業ネットワークから AWS Direct Connect ロケーションへのデータを暗号化するためのMACセキュリティ (MACsec) をサポートする 接続
- 最小特権の原則に基づいて、暗号化キーのアクセス制御ポリシーを特定します。最小特権とは、ユーザーに職務を遂行するために必要最小限のアクセス権を付与するという、セキュリティのベストプラクティスです。最小特権のアクセス許可の適用の詳細については、「」の「セキュリティのベストプラクティスIAM」およびIAM「ポリシーのベストプラクティス」を参照してください。

保管中のデータの暗号化

Amazon Simple Storage Service (Amazon S3) や Amazon Elastic File System (Amazon EFS) などのすべての AWS データストレージサービスには、保管中のデータを暗号化するオプションが用意されています。暗号化は、256 ビット Advanced Encryption Standard (AES-256) ブロック暗号および AWS Key Management Service （ AWS KMS ） や などの AWS 暗号化サービスを使用して実行されますAWS CloudHSM。

データ分類、暗号化の必要性、 end-to-end 暗号化の使用を妨げる技術的な制限などの要因に基づいて、クライアント側の暗号化またはサーバー側の暗号化を使用してデータを end-to-end 暗号化できます。

- クライアント側の暗号化とは、対象となるアプリケーションまたはサービスがデータを受信する前に、データをローカルで暗号化する行為のことです。 AWS のサービス は暗号化されたデータを受け取るだけで、データの暗号化または復号化には関与しません。クライアント側の暗号化には、AWS KMS、AWS Encryption SDK、その他のサードパーティの暗号化ツールまたはサービスを使用する場合があります。
- サーバー側の暗号化とは、データの送信先でデータを暗号化することです。データを受信するアプリケーションまたはサービスが行います。サーバー側の暗号化では、ストレージブロック全体の暗

号化 AWS KMS に を使用できます。オペレーティングシステム (OS) レベルで Linux ファイルシステムを暗号化するなど、他のサードパーティーのLUKS暗号化ツールやサービスを使用することもできます。

以下は、 AWS クラウドに保管中のデータを暗号化するときの一般的なベストプラクティスです。

- データ分類、組織の要件、および該当する規制やコンプライアンス基準に基づいて、保管中のデータに関する組織の暗号化ポリシーを定義します。詳細については、「Creating an enterprise encryption strategy for data at rest」を参照してください。極秘データ、または機密データに分類される保管中のデータは暗号化することを強くお勧めします。ポリシーによっては、必要に応じて、非機密データや公開データなど、他のカテゴリの暗号化を指定する場合もあります。
- 保管中のデータを暗号化する場合は、承認された暗号化アルゴリズム、ブロック暗号モード、キーの長さを使用することをお勧めします。
- 最小特権の原則に基づいて、暗号化キーのアクセス制御ポリシーを特定します。

AWS のサービスの暗号化のベストプラクティス

このセクションでは、以下の のベストプラクティスと推奨事項について説明します AWS のサービス。

- AWS CloudTrail
- Amazon DynamoDB
- Amazon Elastic Compute Cloud (Amazon EC2) と Amazon Elastic Block Store (Amazon EBS)
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon Elastic Container Service (Amazon ECS)
- Amazon Elastic File System (Amazon EFS)
- Amazon Elastic Kubernetes Service (Amazon EKS)
- AWS Encryption SDK
- AWS Key Management Service (AWS KMS)
- AWS Lambda
- Amazon Relational Database Service (Amazon RDS)
- AWS Secrets Manager
- Amazon Simple Storage Service (Amazon S3)
- Amazon Virtual Private Cloud (Amazon VPC)

の暗号化のベストプラクティス AWS CloudTrail

AWS CloudTrail は、 AWS アカウントのガバナンス、コンプライアンス、および運用とリスクの監査を行えるように支援します。

このサービスでは、以下の暗号化のベストプラクティスを検討してください。

- CloudTrail ログは、カスタマー管理の を使用して暗号化する必要があります AWS KMS key。ログファイルを受信する S3 バケットと同じリージョンにあるKMSキーを選択します。詳細については、KMS「キー を使用するための証跡の更新」を参照してください。
- 追加のセキュリティレイヤーとして、証跡のログファイル検証を有効にします。これにより、ログファイルが CloudTrail 配信後に変更、削除、または変更されていないかどうかを判断できます。手順については、「 のログファイルの整合性検証の有効化 CloudTrail」を参照してください。

- インターフェイスVPCエンドポイントを使用して、 CloudTrail がパブリックインターネットを経由VPCsせずに他の のリソースと通信できるようにします。詳細については、「インターフェイスVPCエンドポイント AWS CloudTrail での の使用」を参照してください。
- KMS キーポリシーに `aws:SourceArn`条件キーを追加して、 が特定の証跡にのみKMSキー CloudTrail を使用するようにします。詳細については、「 の AWS KMS key ポリシーを設定する CloudTrail」を参照してください。
- で AWS Config、ログファイルの暗号化を検証して適用する cloud-trail-encryption-enabled AWS マネージドルールを実装します。
- CloudTrail が Amazon Simple Notification Service (Amazon SNS) トピックを介して通知を送信するように設定されている場合は、 CloudTrail ポリシーステートメントに `aws:SourceArn` (またはオプションで `aws:SourceAccount`) 条件キーを追加して、SNSトピックへの不正なアカウントアクセスを防止します。詳細については、「 の Amazon SNSトピックポリシー CloudTrail」を参照してください。
- を使用している場合は AWS Organizations、その組織の のすべてのイベントを口グ AWS アカウント に記録する組織の証跡を作成します。これには、組織内の管理アカウントおよびすべてのメンバーアカウントが含まれます。詳細については、「組織の証跡の作成」を参照してください。
- 企業データを保存するすべての に適用される AWS リージョン証跡を作成し、それらのリージョンの AWS アカウント アクティビティを記録します。が新しいリージョン AWS を起動すると、は新しいリージョン CloudTrail を自動的に含め、そのリージョンのイベントを口グに記録します。

Amazon DynamoDB の暗号化のベストプラクティス

Amazon DynamoDB は、高速で予測可能でスケーラブルなパフォーマンスを提供するフルマネージドの NoSQL データベースサービスです。DynamoDB 保管時の暗号化は、データが耐久性のあるメディアに保存されるたびに、プライマリキー、ローカルおよびグローバルセカンダリインデックス、ストリーム、グローバルテーブル、バックアップ、DynamoDB Accelerator (DAX) クラスターなど、暗号化されたテーブル内のデータを保護します。

データ分類の要件に従い、サーバー側またはクライアント側の暗号化を実装することで、データの機密性と整合性を維持できます。

サーバー側の暗号化では、新しいテーブルの作成時に AWS KMS keys を使用してテーブルを暗号化できます。 AWS 所有キー、 AWS マネージドキー、またはカスタマーマネージドキーを使用できます。キーにはカスタマーマネージドキーを使用することをお勧めします。これは、組織でキーを完全に制御できるためです。また、このキータイプを使用すると、テーブルレベルの暗号化

キー、DynamoDB テーブル、ローカルおよびグローバルのセカンダリインデックス、ストリームがすべて同じキーで暗号化されます。これらのキータイプの詳細については、「カスタマーキーと AWS キー」を参照してください。

> **Note**
>
> AWS 所有キー、 AWS マネージドキー、カスタマーマネージドキーはいつでも切り替えることができます。

クライアント側の暗号化とデータの end-to-end 保護には、保管中と転送中の両方で、Amazon DynamoDB 暗号化クライアント を使用できます。DynamoDB Encryption Client は、項目の属性値の機密性を保護する暗号化に加えて、項目に署名します。こうすることで、属性の追加や削除、暗号化された値の別の値への置換など、項目全体への不正な変更を検出し、整合性の保護を提供します。

このサービスでは、以下の暗号化のベストプラクティスを検討してください。

- キーの無効化や削除のスケジュール設定の権限を、これらのタスクを実行する必要のあるユーザーのみに制限してください。キーの状態を無効に設定するか、削除のスケジュールを設定すると、すべてのユーザーと DynamoDB サービスは、データの暗号化と復号化、およびテーブルに対する読み取り/書き込み操作を実行できなくなります。
- DynamoDB はHTTPSデフォルトで を使用して転送中のデータを暗号化しますが、追加のセキュリティコントロールが推奨されます。以下のいずれかのオプションを使用できます。
  - AWS Site-to-Site VPN 暗号化IPsecに を使用した 接続。
  - AWS Direct Connect プライベート接続を確立するための 接続。
  - AWS Direct Connect でIPsec暗号化されたプライベート AWS Site-to-Site VPN 接続の接続との接続。
  - 仮想プライベートクラウド (VPC) 内からのみ DynamoDB へのアクセスが必要な場合は、VPC ゲートウェイエンドポイントを使用し、 内のリソースのみがVPCアクセスできるようにします。これにより、トラフィックがパブリックインターネットを経由することを防ぎます。
- VPC エンドポイントを使用している場合は、エンドポイントポリシーとエンドポイントに関連付けられたIAMポリシーを、承認されたユーザー、リソース、サービスのみに制限します。詳細については、「ポリシーを使用して DynamoDB エンドポイントへのアクセスを制御する」および「エンドポイントIAMポリシーを使用して のサービスへのアクセスを制御する」を参照してください。 https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-access.html

- 暗号化ポリシーに従って、暗号化が必要なデータに対し、列レベルのデータ暗号化をアプリケーションレベルで実装できます。
- DAX クラスターの設定時に、キャッシュ内のデータ、設定データ、ログファイルなどの保管中のデータを暗号化するようにクラスターを設定します。既存のクラスターでは保存時の暗号化を有効にすることはできません。このサーバー側の暗号化は、基盤となるストレージを経由する不正アクセスからデータを保護するのに役立ちます。DAX 保管時の暗号化は、クラスターの暗号化に使用される単一サービスのデフォルトキーAWSKMSを管理するために、 と自動的に統合されます。暗号化されたDAXクラスターの作成時にサービスのデフォルトキーが存在しない場合、 は自動的に新しい AWS マネージドキー AWS KMS を作成します。詳細については、DAX「保管時の暗号化」を参照してください。

  > **Note**
  >
  > カスタマーマネージドキーはDAXクラスターでは使用できません。

- DAX クラスターの設定時に転送中のデータを暗号化するようにクラスターを設定します。既存のクラスターでは転送中の暗号化を有効にすることはできません。DAX は、 TLSを使用してアプリケーションとクラスター間のリクエストとレスポンスを暗号化し、クラスターの x509 証明書を使用してクラスターの ID を認証します。詳細については、DAX「転送中の暗号化」を参照してください。
- で AWS Config、DAXクラスターの暗号化を検証して維持する dax-encryption-enabled AWS マネージドルールを実装します。

Amazon EC2と Amazon の暗号化のベストプラクティス EBS

Amazon Elastic Compute Cloud (Amazon EC2) は、 でスケーラブルなコンピューティング容量を提供します AWS クラウド。必要な数の仮想サーバーを起動することができ、迅速にスケールアップまたはスケールダウンができます。Amazon Elastic Block Store (Amazon EBS) は、EC2インスタンスで使用するブロックレベルのストレージボリュームを提供します。

これらのサービスでは、以下の暗号化のベストプラクティスを検討してください。

- すべてのEBSボリュームに適切なデータ分類キーと値でタグ付けします。これにより、ポリシーに従って、適切なセキュリティと暗号化の要件を決定して実装できます。
- 暗号化ポリシーと技術的実現可能性に従って、EC2インスタンス間、またはEC2インスタンスとオンプレミスネットワーク間で転送中のデータの暗号化を設定します。

- EC2 インスタンスのブートボリュームとデータEBSボリュームの両方を暗号化します。暗号化されたEBSボリュームは、次のデータを保護します。
  - ボリューム内で保管中のデータ
  - ボリュームとインスタンスの間で移動されるすべてのデータ
  - ボリュームから作成されたすべてのスナップショット
  - それらのスナップショットから作成されたすべてのボリューム

  詳細については、EBS「暗号化の仕組み」を参照してください。
- 現在の のアカウントのEBSボリュームに対して、デフォルトで暗号化を有効にします AWS リージョン。これにより、新しいEBSボリュームとスナップショットコピーの暗号化が強制されます。既存のEBSボリュームやスナップショットには影響しません。詳細については、「デフォルトで暗号化を有効にする」を参照してください。
- Amazon インスタンスのインスタンスストアルートボリュームを暗号化しますEC2。こうすることで、オペレーティングシステムで保存されている設定ファイルやデータの保護に役立ちます。詳細については、「Amazon EC2インスタンスストア暗号化を使用して保管中のデータを保護する方法」(AWS ブログ記事) を参照してください。
- で AWS Config、暗号化ボリュームルールを実装して、適切な暗号化設定を検証して適用する自動チェックを行います。

Amazon の暗号化のベストプラクティス ECR

Amazon Elastic Container Registry (Amazon ECR) は、安全でスケーラブル、信頼性の高いマネージドコンテナイメージレジストリサービスです。

Amazon は、Amazon が管理する Amazon S3 バケットにイメージECRを保存します。 ECR各 Amazon ECRリポジトリには暗号化設定があり、リポジトリの作成時に設定されます。デフォルトでは、Amazon ECRは Amazon S3-managed (SSE-S3) 暗号化キーによるサーバー側の暗号化を使用します。詳細については、「保管時の暗号化」(Amazon ECRドキュメント) を参照してください。

このサービスでは、以下の暗号化のベストプラクティスを検討してください。

- Amazon S3-managedされる (-SSSE-S3) 暗号化キーでデフォルトのサーバー側の暗号化を使用する代わりに、 に保存されているカスタマーマネージドKMSキーを使用します AWS KMS。このキータイプは最もきめ細かい管理オプションを提供します。

> **Note**
>
> KMS キーはリポジトリ AWS リージョン と同じ に存在する必要があります。

- リポジトリをプロビジョニングするときに、Amazon がデフォルトでECR作成する許可は取り消さないでください。取り消した場合、データへのアクセス、リポジトリにプッシュされた新しいイメージの暗号化、イメージがプルされた時の復号化などの機能に影響する可能性があります。
- を使用して AWS CloudTrail 、Amazon が ECRに送信するリクエストを記録します AWS KMS。ログエントリには、より簡単に識別できるように暗号化コンテキストキーが含まれています。
- 特定の Amazon VPCエンドポイントまたは特定の からのアクセスを制御するように Amazon ECR ポリシーを設定しますVPCs。これにより、実質的に特定の Amazon ECRリソースへのネットワークアクセスが分離され、特定の からのアクセスのみが可能になりますVPC。Amazon VPCエンドポイントとの仮想プライベートネットワーク (VPN) 接続を確立することで、転送中のデータを暗号化できます。
- Amazon ECRは、リソースベースのポリシーをサポートしています。これらのポリシーを使用すると、送信元 IP アドレスまたは特定の に基づいてアクセスを制限できます AWS のサービス。

Amazon の暗号化のベストプラクティス ECS

Amazon Elastic Container Service (Amazon ECS) は、クラスター上のコンテナの実行、停止、管理に役立つ、高速でスケーラブルなコンテナ管理サービスです。

Amazon ではECS、次のいずれかの方法で転送中のデータを暗号化できます。

- サービスメッシュの作成 を使用して AWS App Mesh、デプロイされた Envoy プロキシと、仮想ノードや仮想ゲートウェイ などのメッシュエンドポイント間のTLS接続を設定します。 AWS Private Certificate Authority またはお客様が用意したTLS証明書を使用できます。詳細とチュートリアルについては、「 (ACM) またはお客様が用意した証明書 AWS App Mesh を使用して AWS Certificate Manager のサービス間のトラフィック暗号化を有効にする」(AWS ブログ記事) を参照してください。
- サポートされている場合は、 AWS Nitro Enclaves を使用します。 AWS Nitro Enclaves は、Amazon EC2インスタンスから enclaves と呼ばれる分離された実行環境を作成できる Amazon EC2の機能です。これは、機密性の非常に高いデータの保護に役立つように設計されています。さらに、 ACM for Nitro Enclaves では、Nitro Enclaves TLSで Amazon EC2インスタンスで実行されているウェブアプリケーションとウェブサーバーで AWS パブリックSSL証明書とプライ

ベート証明書を使用できます。詳細については、AWS 「Nitro Enclaves — 機密データを処理するための分離されたEC2環境」(AWS ブログ記事) を参照してください。

- Application Load Balancer で Server Name Indication (SNI) プロトコルを使用します。Application Load Balancer の 1 つのHTTPSリスナーの背後に複数のアプリケーションをデプロイできます。各リスナーには独自のTLS証明書があります。が提供する証明書を使用することもACM、自己署名証明書を使用することもできます。Application Load Balancer と Network Load Balancer はどちらも をサポートしていますSNI。詳細については、「Application Load Balancer が を使用したスマート選択で複数のTLS証明書をサポートするようになりました (ブログ記事) SNI」を参照してください。AWS
- セキュリティと柔軟性を向上させるには、 AWS Private Certificate Authority を使用して Amazon ECSタスクでTLS証明書をデプロイします。詳細については、「 コンテナへのTLS完全な維持パート 2: の使用 AWS Private CA」(AWS ブログ記事) を参照してください。
- シークレット検出サービス TLS (Envoy) または () でホストされている証明書を使用して、App Mesh に相互 (mTLS) を実装しますGitHub。 ACM

このサービスでは、以下の暗号化のベストプラクティスを検討してください。

- 技術的に可能であれば、セキュリティを強化するために、 で Amazon ECSインターフェイスVPC エンドポイントを設定します AWS PrivateLink。VPN 接続経由でこれらのエンドポイントにアクセスすると、転送中のデータが暗号化されます。
- API キーやデータベース認証情報などの機密資料を安全に保存します。これらを暗号化したパラメータとしてパラメータストアに保存できます。これは AWS Systems Managerの機能です。ただし、 AWS Secrets Manager このサービスではシークレットを自動的にローテーションし、ランダムシークレットを生成し、 間でシークレットを共有できるため、 を使用することをお勧めします AWS アカウント。
- 環境変数からのデータリークのリスクを軽減するために、 AWS Secrets Manager および Config Provider for Secret Store CSI Driver () を使用することをお勧めしますGitHub。このドライバーを使用すると、Secrets Manager に保存されているシークレットと、パラメータストアに保存されているパラメータを、Kubernetes ポッドにマウントされたファイルとして表示できます。

> **Note**
>
> AWS Fargate はサポートされていません。

- データセンター内のユーザーまたはアプリケーション、またはウェブ上の外部の第三者が に直接HTTPSAPIリクエストを行う場合は AWS のサービス、 AWS Security Token Service () から取得した一時的なセキュリティ認証情報を使用してリクエストに署名しますAWS STS。

Amazon の暗号化のベストプラクティス EFS

Amazon Elastic File System (Amazon EFS) は、 で共有ファイルシステムを作成および設定するのに役立ちます AWS クラウド。

このサービスでは、以下の暗号化のベストプラクティスを検討してください。

- で AWS Config、 efs-encrypted-check AWS マネージドルールを実装します。このルールは、Amazon EFSが を使用してファイルデータを暗号化するように設定されているかどうかを確認します AWS KMS。
- `CreateFileSystem` イベントの CloudTrail ログをモニタリングし、暗号化されていないEFSファイルシステムが作成された場合に CloudWatch アラームをトリガーする Amazon アラームを作成して、Amazon ファイルシステムの暗号化を強制します。詳細については、「チュートリアル: 保管中の Amazon EFS ファイルシステムで暗号化を適用する」を参照してください。
- マウントEFSヘルパー を使用してファイルシステムをマウントします。これにより、クライアントと Amazon EFSサービス間の TLS 1.2 トンネルがセットアップおよび維持され、この暗号化されたトンネルを介してすべてのネットワークファイルシステム (NFS) トラフィックがルーティングされます。次のコマンドは、転送時の暗号化TLSに の使用を実装します。

  ```
  sudo mount -t efs  -o tls file-system-id:/ /mnt/efs
  ```

  詳細については、EFS「マウントヘルパーを使用してEFSファイルシステムをマウントする」を参照してください。
- を使用して AWS PrivateLink、インターフェイスVPCエンドポイントを実装し、 VPCsと Amazon EFS の間にプライベート接続を確立しますAPI。エンドポイントとVPNの接続を介して転送中のデータは暗号化されます。詳細については、「インターフェイスVPCエンドポイント AWS のサービス を使用して にアクセスする」を参照してください。
- IAM アイデンティティベースのポリシーで `elasticfilesystem:Encrypted`条件キーを使用して、ユーザーが暗号化されていないEFSファイルシステムを作成できないようにします。詳細については、「 を使用して暗号化されたファイルシステムの作成を強制IAMする」を参照してください。

- KMS EFS暗号化に使用される キーは、リソースベースのキーポリシーを使用して最小特権アクセス用に設定する必要があります。
- EFS ファイルシステムポリシーの `aws:SecureTransport`条件キーを使用して、EFSファイルシステムに接続するときにNFSクライアントTLSに の使用を強制します。詳細については、「Amazon Elastic File System によるファイルデータの暗号化」(ホワイトペーパー) の「転送中のデータの暗号化 Amazon Elastic File System」を参照してください。AWS

Amazon の暗号化のベストプラクティス EKS

Amazon Elastic Kubernetes Service (Amazon EKS) を使用すると、独自の Kubernetes コントロールプレーンやノードをインストールまたは維持 AWS することなく、 で Kubernetes を実行できます。Kubernetes では、シークレットはユーザー証明書、パスワード、APIキーなどの機密情報の管理に役立ちます。デフォルトでは、これらのシークレットは、 etcd と呼ばれるAPIサーバーの基盤となるデータストアに暗号化されずに保存されます。へのアクセス権またはAPIアクセス権を持つユーザーは`etcd`、シークレットを取得または変更できます。さらに、名前空間にポッドを作成する権限を持つユーザーは誰でも、そのアクセス権を使ってその名前空間のシークレットを読み取ることができます。これらのシークレットは、 AWS マネージドキーまたはカスタマーマネージドキーのいずれかEKSを使用して AWS KMS keys、Amazon で保管中に暗号化できます。を使用する代替方法は、AWS シークレットと Config プロバイダー (ASCP) (リポジトリ) GitHub を使用すること`etcd`です。ASCP は、 IAM およびリソースベースのポリシーと統合して、クラスター内の特定の Kubernetes ポッド内のシークレットへのアクセスのみを制限および制限します。

Kubernetes では、次の AWS ストレージサービスを使用できます。

- Amazon Elastic Block Store (Amazon EBS) では、ツリー内ストレージドライバー または Amazon EBSCSIドライバー を使用できます。どちらにも、ボリュームの暗号化やカスタマーマネージドキーの提供のためのパラメータが含まれています。
- Amazon Elastic File System (Amazon EFS) では、動的プロビジョニングと静的プロビジョニングの両方をサポートする Amazon EFSCSIドライバーを使用できます。

このサービスでは、以下の暗号化のベストプラクティスを検討してください。

- `etcd` を使用している場合、デフォルトでシークレットオブジェクトは暗号化されずに保存されますが、シークレットを保護するために以下を実行してください。
  - 「保管中のシークレットデータを暗号化する」(Kubernetes ドキュメント)。

- シークレットの読み取りと書き込みを制限するロールベースのアクセスコントロール (RBAC) ルールを使用して、認証を有効化または設定します。新しいシークレットの作成や、既存のシークレットの置換を行う権限を制限します。詳細については、「認証の概要」(Kubernetes ドキュメント) を参照してください。
- ポッドに複数のコンテナを定義してあり、そのうちの 1 つのコンテナのみがシークレットへのアクセスを必要とする場合は、他のコンテナがそのシークレットにアクセスできないようにボリュームマウントを定義します。tmpfs ボリュームとしてマウントされたシークレットはインスタンス化され、ポッドが削除されるとノードから自動的に削除されます。環境変数を使用することもできますが、環境変数の値がログに表示される可能性があるため、この方法はお勧めしません。詳細については、「シークレット」(Kubernetes ドキュメント) を参照してください。
- watch へのアクセスと、名前空間内のシークレットに対する list リクエストの許可はできるだけ避けてください。Kubernetes ではAPI、クライアントがその名前空間内のすべてのシークレットの値を検査できるため、これらのリクエストは強力です。
- 読み取り専用アクセスを含めて、クラスター管理者のみが etcd にアクセスできるようにしてください。
- 複数のetcdインスタンスがある場合は、etcdピア間の通信TLSに etcd が を使用していることを確認します。

- を使用している場合はASCP、シークレットを保護するために次の操作を行います。
  - IAM サービスアカウントのロールを使用して、シークレットアクセスを許可されたポッドのみに制限します。
  - AWS 暗号化プロバイダー (リポジトリ) を使用して、カスタマーマネージドKMSキーによるエンベロープ暗号化を実装することで、Kubernetes GitHub シークレットの暗号化を有効にします。
- Amazon CloudWatch メトリクスフィルターとアラームを作成して、シークレットの削除や、削除する待機期間のシークレットバージョンの使用など、管理者が指定したオペレーションに関するアラートを送信します。詳細については、「異常検出に基づいてアラームを作成する」を参照してください。

の暗号化のベストプラクティス AWS Encryption SDK

AWS Encryption SDK は、オープンソースのクライアント側暗号化ライブラリです。業界標準とベストプラクティスを使用して、いくつかのプログラミング言語での実装と相互運用性をサポートします。 は、安全で認証された対称キーアルゴリズムを使用してデータを AWS Encryption SDK 暗号化し、暗号化のベストプラクティスに準拠したデフォルトの実装を提供します。詳細については、「AWS Encryption SDKでサポートされているアルゴリズムスイート」を参照してください。

の主な機能の 1 つは、使用中のデータの暗号化のサポート AWS Encryption SDK です。 encrypt-then-use アプローチを採用することで、アプリケーションロジックで処理される前に機密データを暗号化できます。これにより、アプリケーション自体がセキュリティイベントの影響を受ける場合でも、潜在的な漏洩や改ざんからデータを保護することができます。

このサービスでは、以下のベストプラクティスを検討してください。

- 「AWS Encryption SDKのベストプラクティス」に記載されているすべての推奨事項を順守してください。
- データキーの保護に役立つラップキーを 1 つ以上選択します。詳細については、「ラップキーの選択」を参照してください。
- 信頼できないKMSキーが使用されないように、 `KeyId` パラメータを ReEncryptオペレーションに渡します。詳細については、「クライアント側の暗号化の改善: 明示的 KeyIds なキーコミットメント」(AWS ブログ記事) を参照してください。
- AWS Encryption SDK で を使用する場合は AWS KMS、ローカル`KeyId`フィルタリングを使用します。詳細については、「クライアント側の暗号化の改善: 明示的 KeyIds なキーコミットメント」(AWS ブログ記事) を参照してください。
- 暗号化または復号化を必要とする大量のトラフィックがあるアプリケーション、またはアカウントが AWS KMS リクエストクォータ を超えている場合は、 のデータキーキャッシュ機能を使用できます AWS Encryption SDK。データキーキャッシュに関しては、以下のベストプラクティスに注意してください。
  - キャッシュセキュリティのしきい値を設定し、各キャッシュデータキーの使用期間および各データキーで保護されるデータ量を制限します。これらのしきい値を設定する際の推奨事項については、「キャッシュセキュリティのしきい値の設定」を参照してください。
  - ローカルキャッシュは、特定のアプリケーションユースケースのパフォーマンスを向上させるため、データキーの数を必要最小限に設定してください。ローカルキャッシュの制限を設定する手順と例については、「データキーキャッシュの使用: Step-by-step」を参照してください。

  詳細については、AWS Encryption SDK「: データキーキャッシュがアプリケーションに適しているかどうかを判断する方法」(AWS ブログ記事) を参照してください。

の暗号化のベストプラクティス AWS Key Management Service

AWS Key Management Service (AWS KMS) は、データの保護に役立つ暗号化キーの作成と制御に役立ちます。 は、データを暗号化 AWS のサービス できる他のほとんどの と AWS KMS 統合します。詳細なリストについては、「 AWS のサービス と統合 AWS KMSされている」を参照してくだ

さい。 AWS KMS また、 とも AWS CloudTrail 統合されており、監査、規制、コンプライアンスのニーズに対応するためのKMSキーの使用を口グに記録します。

KMS キーは のプライマリリソースであり AWS KMS、暗号化キーの論理表現です。KMS キーには主に 3 つのタイプがあります。

- カスタマーマネージドキーは、作成するKMSキーです。
- AWS マネージドキーは、 がユーザーに代わってアカウントで AWS のサービス 作成するKMSキーです。
- AWS 所有キーは、 が AWS のサービス 所有および管理するKMSキーで、複数の で使用します AWS アカウント。

キーの種類の詳細については、「カスタマーキーと AWS キー」を参照してください。

では AWS クラウド、 ポリシーを使用して、リソースとサービスにアクセスできるユーザーを制御します。例えば、 AWS Identity and Access Management （ IAM) では、アイデンティティベースのポリシーはユーザー、ユーザーグループ、またはロールのアクセス許可を定義し、リソースベースのポリシーは S3 バケットなどのリソースにアタッチし、アクセスを許可するプリンシパル、サポートされているアクション、および満たす必要があるその他の条件を定義します。IAM ポリシーと同様に、 はキーポリシー AWS KMS を使用してKMSキーへのアクセスを制御します。各KMSキーにはキーポリシーが必要です。各キーにはキーポリシーを 1 つだけ持つことができます。KMS キーへのアクセスを許可または拒否するポリシーを定義するときは、次の点に注意してください。

- カスタマーマネージドキーのキーポリシーは制御できますが、 AWS マネージドキーまたは AWS 所有キーのキーポリシーを直接制御することはできません。
- キーポリシーにより、 内の コールへの AWS KMS APIきめ細かなアクセスを許可できます AWS アカウント。キーポリシーで明示的に許可されていない限り、IAMポリシーを使用してKMSキーへのアクセスを許可することはできません。キーポリシーからのアクセス許可がない場合、アクセス許可を許可するIAMポリシーは効果がありません。詳細については、IAM「ポリシーにKMSキー へのアクセスを許可する」を参照してください。
- IAM ポリシーを使用して、キーポリシーからの対応するアクセス許可なしで、カスタマーマネージドキーへのアクセスを拒否できます。
- マルチリージョンキーのキーポリシーとIAMポリシーを設計する場合は、次の点を考慮してください。
  - キーポリシーはマルチリージョンキーの共有プロパティではありません。また、関連するマルチリージョンキー間のキーポリシーをコピーまたは同期しません。

- `CreateKey` と `ReplicateKey` のアクションを使用してマルチリージョンキーを作成した場合、リクエストでキーポリシーが指定されていない限り、デフォルトキーポリシーが適用されます。
- aws:RequestedRegion などの条件キーを実装して、アクセス許可を特定の に制限できます AWS リージョン。
- 権限を使用して、マルチリージョンのプライマリキーまたはレプリカキーへのアクセス許可を付与できます。ただし、1 つの許可を使用して、複数のKMSキーが関連するマルチリージョンキーであっても、複数のキーへのアクセス許可を許可することはできません。

AWS KMS を使用してキーポリシーを作成するときは、次の暗号化のベストプラクティスとその他のセキュリティのベストプラクティスを考慮してください。

- AWS KMS ベストプラクティスについては、以下のリソースの推奨事項に従ってください。
  - AWS KMS グラントのベストプラクティス (AWS KMS ドキュメント)
  - IAM ポリシーのベストプラクティス (AWS KMS ドキュメント)
- 職務分掌のベストプラクティスに従い、キーを管理する人物と使用する人物の ID は個別に管理してください。
  - キーの作成および削除を行う管理者ロールは、そのキーを使用できないようにする必要があります。
  - 一部のサービスでは、データの暗号化のみを必要とするため、キーを使用して復号する権限を付与するべきではない場合があります。
- キーポリシーは、常に最小特権モデルに従う必要があります。IAM または キーポリシーのアクション`kms:*`に を使用しないでください。これにより、プリンシパルにキーの管理と使用の両方のアクセス許可が付与されます。
- キーポリシー内の kms:ViaService 条件キー AWS のサービス を使用して、カスタマーマネージドキーの使用を特定の に制限します。
- キータイプの中から選択できる場合は、カスタマーマネージドキーをお勧めします。これは、次のようなきめ細かな制御オプションが提供されるためです。
  - 認証とアクセスコントロールの管理
  - キーの有効化と無効化
  - AWS KMS keysのローテーション
  - キーのタグ付け
  - エイリアスの作成

  - AWS KMS keysの削除
- AWS KMS 管理アクセス許可と変更アクセス許可は、未承認のプリンシパルに対して明示的に拒否する必要があり、 AWS KMS 変更アクセス許可は、未承認のプリンシパルの許可ステートメントに存在してはいけません。詳細については、「AWS Key Management Serviceのアクション、リソース、および条件キー」を参照してください。
- KMS キーの不正使用を検出するには、 で AWS Configiam-customer-policy-blocked-kms-actions および iam-inline-policy-blocked-kms-actions ルールを実装します。これにより、プリンシパルはすべてのリソースで復 AWS KMS 号アクションを使用できなくなります。
- のサービスコントロールポリシー (SCPs) を に実装 AWS Organizations して、権限のないユーザーまたはロールがコマンドとして直接、またはコンソールを介してKMSキーを削除しないようにします。詳細については、「予防的コントロールSCPsとして を使用する」(AWS ブログ記事) を参照してください。
- コールをログ AWS KMS APIに記録します CloudTrail 。こうすることで、実行されたリクエストの内容、リクエストの送信元 IP アドレス、リクエストを実行したユーザーなど、関連するイベント属性が記録されます。詳細については、「 を使用したAPI呼び出しの口グ記録 AWS KMSAWS CloudTrail」を参照してください。
- 暗号化コンテキスト を使用する場合、機密情報を含めないでください。 は暗号化コンテキストをプレーンテキストJSONファイルに CloudTrail 保存します。プレーンテキストファイルは、情報を含む S3 バケットにアクセスできるすべてのユーザーが表示できます。
- カスタマーマネージドキーの使用状況をモニタリングする場合、キーの作成、カスタマーマネージドキーポリシーの更新、キーマテリアルのインポートなど、特定のアクションが検出された際に通知するようイベントを設定します。また、キーを無効化する AWS Lambda 関数や組織のポリシーで指定されているインシデント対応アクションを実行する関数などの自動応答を実装することもお勧めします。
- マルチリージョンキーは、コンプライアンス準拠、ディザスタリカバリ、バックアップなど、特定のシナリオにお勧めします。マルチリージョンキーのセキュリティプロパティは、単一リージョンキーとは大きく異なります。マルチリージョンキーの作成、管理、使用を許可する際には、以下の推奨事項が適用されます。
  - プリンシパルが、必要とする AWS リージョン のみにマルチリージョンキーをコピーできるようにします。
  - マルチリージョンキーのアクセス許可を、それらを必要とするプリンシパルおよびタスクに対してのみ付与します。

の暗号化のベストプラクティス AWS Lambda

AWS Lambda は、サーバーのプロビジョニングや管理を行うことなくコードを実行できるコンピューティングサービスです。環境変数の保護する場合、サーバー側の暗号化を使用して保管中のデータを保護し、クライアント側の暗号化を使用して転送中のデータを保護することができます。

このサービスでは、以下の暗号化のベストプラクティスを検討してください。

- Lambda は、 AWS KMS keyで常にサーバー側の暗号化を提供します。デフォルトでは、Lambda は AWS マネージドキーを使用します。管理、ローテーション、監査などの面でキーを完全に制御できるため、カスタマーマネージドキーを使用することをお勧めします。
- 暗号化が必要な転送中のデータの場合は、ヘルパーを有効にします。これにより、環境変数がクライアント側で暗号化され、優先KMSキーを使用して転送中の保護されます。詳細については、「環境変数の保護」の「転送中のセキュリティ」を参照してください。
- 機密データや重要なデータを保持する Lambda 関数の環境変数は、転送中に暗号化する必要があります。これにより、関数に動的に渡されるデータ (通常はアクセス情報) を不正アクセスから保護できます。
- ユーザーが環境変数を表示できないようにするには、IAMポリシー内のユーザーのアクセス許可、またはデフォルトキー、カスタマーマネージドキー、またはすべてのキーへのアクセスを拒否するキーポリシーにステートメントを追加します。詳細については、AWS Lambda 環境変数の使用を参照してください。

Amazon の暗号化のベストプラクティス RDS

Amazon Relational Database Service (Amazon RDS) は、 でリレーショナルデータベース (DB) をセットアップ、運用、スケーリングするのに役立ちます AWS クラウド。保管中に暗号化されるデータには、DB インスタンス、自動バックアップ、リードレプリカ、スナップショットの基本的なストレージが含まれます。

RDS DB インスタンスの保管中のデータを暗号化するために使用できるアプローチは次のとおりです。

- Amazon RDS DB インスタンスは AWS KMS keys AWS 、 マネージドキーまたはカスタマーマネージドキーのいずれかを使用して暗号化できます。詳細については、このガイドの「AWS Key Management Service」を参照してください。
- Amazon RDS for Oracle と Amazon RDS for SQL Server は、透過的なデータ暗号化 () による DB インスタンスの暗号化をサポートしていますTDE。詳細については、「Oracle Transparent Data

Encryption」または「Support for Transparent Data Encryption in SQL Server」を参照してください。

DB インスタンスを暗号化するには、 キーTDEと KMSキーの両方を使用できます。ただし、これはデータベースのパフォーマンスに若干影響する可能性があるため、これらのキーは個別に管理する必要があります。

RDS DB インスタンスとの間で転送中のデータを暗号化するために使用できるアプローチは次のとおりです。

- MariaDB 、Microsoft Server、My 、SQLOracle、または Postgre を実行している Amazon RDS DB インスタンスの場合SQL、 SSLを使用して接続を暗号化できます。 SQL詳細については、SSL「/TLS を使用して DB インスタンス への接続を暗号化する」を参照してください。
- Amazon RDS for Oracle は、Oracle ネイティブネットワーク暗号化 (NNE) もサポートしています。これは、DB インスタンスとの間でデータを移動するときにデータを暗号化します。NNE 暗号化と SSL 暗号化を同時に使用することはできません。詳細については、「Oracle native network encryption」を参照してください。

このサービスでは、以下の暗号化のベストプラクティスを検討してください。

- 暗号化が必要なデータを処理、保存、または送信するために Amazon RDS for SQL Server または Amazon RDS for PostgreSQL DB インスタンスに接続する場合は、RDSTransport Encryption 機能を使用して接続を暗号化します。これを実装するには、パラメータグループの `rds.force_ssl` パラメータを 1 に設定します。詳細については、「パラメータグループの操作」を参照してください。Amazon RDS for Oracle は、Oracle データベースのネイティブネットワーク暗号化を使用します。
- RDS DB インスタンス暗号化用のカスタマーマネージドキーは、その目的にのみ使用し、他の では使用しないでください AWS のサービス。
- RDS DB インスタンスを暗号化する前に、KMSキー要件を確立します。インスタンスが使用するキーは後で変更できません。例えば、暗号化ポリシーでは、ビジネス要件に基づいて、 AWS マネージドキーまたはカスタマーマネージドキーの使用および管理標準を定義します。
- カスタマーマネージドKMSキーへのアクセスを許可するときは、IAMポリシーで条件キーを使用して最小特権の原則に従います。例えば、Amazon を起点とするリクエストにのみカスタマーマネージドキーを使用できるようにするにはRDS、 `rds.<region>.amazonaws.com`値で kms:ViaService condition キーを使用します。さらに、Amazon RDS暗号化コンテキストのキーまたは値を、カスタマーマネージドキーを使用する条件として使用できます。

- 暗号化された RDS DB インスタンスのバックアップを有効にすることを強くお勧めします。Amazon は、KMSキーが有効になっていない場合やKMSキーへのアクセスが取り消された場合など、DB インスタンスのKMSキーRDSにアクセスできなくなるRDS可能性があります。この場合、暗号化された DB インスタンスは 7 日間回復可能な状態になります。DB インスタンスが 7 日経ってもキーへのアクセスを回復しない場合、最終的にデータベースにはアクセスできなくなるため、バックアップから復元する必要があります。詳細については、「DB インスタンスの暗号化」を参照してください。
- リードレプリカとその暗号化された DB インスタンスが同じ にある場合は AWS リージョン、同じKMSキーを使用して両方を暗号化する必要があります。
- で AWS Config、RDSDB インスタンスの暗号化を検証して適用する rds-storage-encrypted AWS マネージドルールと、RDSデータベーススナップショットの暗号化を検証して適用する rds-snapshots-encrypted ルールを実装します。
- を使用して AWS Security Hub 、Amazon RDSリソースがセキュリティのベストプラクティスに従っているかどうかを評価します。詳細については、「Amazon の Security Hub コントロール RDS」を参照してください。

の暗号化のベストプラクティス AWS Secrets Manager

AWS Secrets Manager は、パスワードを含むコード内のハードコードされた認証情報を Secrets Manager へのAPI呼び出しに置き換えて、プログラムでシークレットを取得するのに役立ちます。Secrets Manager は と統合 AWS KMS され、すべてのシークレット値のすべてのバージョンを、 で保護されている一意のデータキーで暗号化します AWS KMS key。この統合により、暗号化キーを使用して保存されたシークレットが保護され、 が暗号化 AWS KMS されないままになることはありません。また、 KMSキーにカスタムアクセス許可を定義して、保存されたシークレットを保護するデータキーを生成、暗号化、復号するオペレーションを監査することもできます。詳細については、「AWS Secrets Managerのシークレットの暗号化と復号」を参照してください。

このサービスでは、以下の暗号化のベストプラクティスを検討してください。

- キーポリシーでは、kms:ViaService 条件キーを使用して、値 を割り当てることによって Secrets Manager からのリクエストのみにキーの の使用を制限しますsecretsmanager.<region>.amazonaws.com。
- セキュリティを強化するには、ビジネス要件に基づいて、Secrets Manager 暗号化コンテキストのキーまたは値を、以下を作成してKMSキーを使用する条件として使用します。
  - IAM または キーポリシーの文字列条件演算子
  - 許可における権限の制約

- で AWS Config、 secretsmanager-using-cmk AWS マネージドルールを実装して、Secrets Manager のすべてのシークレットが AWS マネージドKMSキーまたはカスタマーマネージドKMSキーで暗号化されていることを確認します。
- シークレットが定義されたローテーションポリシーに準拠していることを確認するには、次の AWS Config ルールを実装します。
  - secretsmanager-rotation-enabled-check – Secrets Manager に保存されているシークレットに対してローテーションが設定されているかどうかを確認します。
  - secretsmanager-scheduled-rotation-success-check – シークレットが正常にローテーションされたかどうかを確認します。 AWS Config また、最後にローテーションされた日付が設定されたローテーション頻度の範囲内にあるかどうかも確認します。
  - secretsmanager-secret-periodic-rotation – シークレットが指定された日数内にローテーションされたかどうかを確認します。
  - secretsmanager-secret-unused – シークレットが指定された日数内にアクセスされたかどうかを確認します。
- を使用して AWS CloudTrail 、ローテーションの開始、ローテーションの成功、ローテーションの失敗、シークレットのスケジュールされた削除など、Secrets Manager と API以外のイベントに対するすべてのAPI呼び出しを記録します。詳細については、「 を使用した AWS Secrets Manager イベントのログ記録 AWS CloudTrail」を参照してください。
- Amazon EventBridge を使用して、シークレットの削除、シークレットのローテーション、削除が予定されているシークレットの使用の試行など、一部の Secrets Manager オペレーションのアラートを設定します。アラートをトリガーする操作を選択できます。アラートは、サブスクライバーに E メールまたはテキストメッセージを送信する Amazon Simple Notification Service (Amazon SNS) トピックでも、後で確認できるようにオペレーションの詳細をログに記録する 関数でもかまいません AWS Lambda 。

Amazon S3 の暗号化のベストプラクティス

Amazon Simple Storage Service (Amazon S3) は、量にかかわらず、データを保存、保護、取得するのに役立つクラウドベースのオブジェクトストレージサービスです。

Amazon S3 でのサーバー側の暗号化には 3 つのオプションがあります。

- Amazon S3-managed暗号化キーによるサーバー側の暗号化 (SSE-S3)
- AWS Key Management Service (-SSEKMS) によるサーバー側の暗号化
- お客様が用意した暗号化キーによるサーバー側の暗号化 (SSE-C)

Amazon S3 は、Amazon S3 のすべてのバケットの暗号化の基本レベルとして、Amazon SSES3 マネージドキー (-S3) によるサーバー側の暗号化を適用します。 Amazon S3 2023 年 1 月 5 日以降、Amazon S3 にアップロードされるすべての新しいオブジェクトは、追加費用なしで、パフォーマンスに影響を与えずに自動的に暗号化されます。S3 バケットのデフォルトの暗号化設定と新しいオブジェクトのアップロードの自動暗号化ステータスは、 AWS CloudTrail ログ、S3 インベントリ、S3 Storage Lens、Amazon S3 コンソール、および AWS Command Line Interface （ AWS CLI) と の追加の Amazon S3 APIレスポンスヘッダーとして使用できます AWS SDKs。詳細については、「デフォルトの暗号化FAQ」を参照してください。

アップロード時にサーバー側の暗号化を使用してオブジェクトを暗号化する場合は、 `x-amz-server-side-encryption`ヘッダーをリクエストに追加して、Amazon S3 に SSE-S3、SSE-KMS、または SSE-C を使用してオブジェクトを暗号化するように指示します。ヘッダーに使用できる値`x-amz-server-side-encryption`は次のとおりです。

- `AES256`。Amazon S3 が管理するキーを使用するよう、Amazon S3 に指示します。
- `aws:kms`。Amazon S3 に AWS KMS マネージドキーを使用するように指示します。
- -SSEC `False`の値を `True`または に設定する

詳細については、「D efense-in-depth 要件 1: バケットポリシーの使用方法」および「D 要件 1: Amazon S3 データの保護に役立つ多層防御の適用」 (ブログ記事) の「保管中および転送中にデータを暗号化する必要があります」を参照してください。 Amazon S3 AWS

Amazon S3 でのクライアント側の暗号化には 2 つのオプションがあります。

- に保存されているキー AWS KMS
- アプリケーション内に保存されたキー

このサービスでは、以下の暗号化のベストプラクティスを検討してください。

- で AWS Config、S3 bucket-server-side-encryption対応 AWS マネージドルールを実装して、S3 バケット暗号化を検証して適用します。
- アップロードされるすべてのオブジェクトが、`s3:x-amz-server-side-encryption` の条件を使用して暗号化されていることを検証する Amazon S3 バケットポリシーをデプロイします。詳細については、SSE-S3 を使用したデータの保護」のバケットポリシーの例と、「バケットポリシーの追加」の手順を参照してください。

- S3 バケットポリシーの `aws:SecureTransport`条件を使用して、 HTTPS (TLS) 経由の暗号化された接続のみを許可します。詳細については、AWS Config 「ルール S3- に準拠するためにどの S3 バケットポリシーを使用すればよいですか？」を参照してくださいbucket-ssl-requests-only。
- で AWS Config、s3bucket-ssl-requests-only AWS マネージドルールを実装して、 を使用するリクエストを要求しますSSL。
- Amazon S3 オブジェクトにクロスアカウントアクセスを許可する必要がある場合は、カスタマーマネージドキーを使用します。他の AWS アカウントからのアクセスを許可するようにキーポリシーを設定します。

Amazon の暗号化のベストプラクティス VPC

Amazon Virtual Private Cloud (Amazon VPC) は、定義した仮想ネットワークに AWS リソースを起動するのに役立ちます。この仮想ネットワークは、お客様自身のデータセンターで運用されていた従来のネットワークに似ていますが、 AWSのスケーラブルなインフラストラクチャを使用できるというメリットがあります。

このサービスでは、以下の暗号化のベストプラクティスを検討してください。

- 企業ネットワーク内の情報アセットとシステム間のトラフィックを、次のいずれかVPCsを使用して暗号化します。
  - AWS Site-to-Site VPN 接続
  - IPsec暗号化されたプライベート AWS Direct Connect 接続を提供する AWS Site-to-Site VPN と接続の組み合わせ
  - AWS Direct Connect 企業ネットワークから ロケーションへのデータを暗号化するためのMAC AWS Direct Connect セキュリティ (MACsec) をサポートする 接続
- のVPCエンドポイントを使用して AWS PrivateLink 、インターネットゲートウェイを使用 AWS のサービス せずに、サポートされている VPCsにプライベートに接続します。 AWS Direct Connect または AWS VPN のサービスを使用して、この接続を確立できます。VPC と他のサービス間のトラフィックは、 AWS ネットワークを離れません。詳細については、「 AWS のサービス 経由でのアクセス AWS PrivateLink」を参照してください。
- TCP/443 HTTPS経由など、安全なプロトコルに関連付けられたポートからのトラフィックのみを許可するセキュリティグループルールを設定します。セキュリティグループとそのルールを定期的に監査します。

リソース

- 「保管中のデータのエンタープライズ暗号化戦略の作成」(AWS 規範ガイダンス)
- のセキュリティのベストプラクティス AWS Key Management Service (AWS KMS ドキュメント)
- AWS のサービス の使用方法 AWS KMS (AWS KMS ドキュメント)
- セキュリティの柱: データ保護 (AWS Well-Architected Framework)

ドキュメント履歴

以下の表は、本ガイドの重要な変更点について説明したものです。今後の更新について通知を受ける場合は、RSSフィード をサブスクライブできます。

変更	説明	日付
AWS のサービス 更新	Amazon Elastic Kubernetes Service (Amazon EKS ）、Amazon Relational Database Service (Amazon) AWS Encryption SDK、Amazon Simple Storage Service (Amazon S3RDS) の情報と推奨事項を更新しました。Amazon S3	2024 年 9 月 4 日
初版発行	—	2022 年 12 月 2 日

AWS 規範的ガイダンスの用語集

以下は、 AWS 規範的ガイダンスが提供する戦略、ガイド、パターンで一般的に使用される用語です。エントリを提案するには、用語集の最後のフィードバックの提供リンクを使用します。

数字

7 Rs

アプリケーションをクラウドに移行するための 7 つの一般的な移行戦略。これらの戦略は、ガートナーが 2011 年に特定した 5 Rs に基づいて構築され、以下で構成されています。

- リファクタリング/アーキテクチャの再設計 — クラウドネイティブ特徴を最大限に活用して、俊敏性、パフォーマンス、スケーラビリティを向上させ、アプリケーションを移動させ、アーキテクチャを変更します。これには、通常、オペレーティングシステムとデータベースの移植が含まれます。例: オンプレミスの Oracle データベースを Amazon Aurora Postgre SQL互換エディションに移行します。
- リプラットフォーム (リフトアンドリシェイプ) – アプリケーションをクラウドに移行し、クラウド機能を活用するためにある程度の最適化を導入します。例: オンプレミスの Oracle データベースを の Oracle 用 Amazon Relational Database Service (Amazon RDS) に移行します AWS クラウド。
- 再購入 (ドロップアンドショップ) — 通常、従来のライセンスから SaaS モデルに移行して、別の製品に切り替えます。例: 顧客関係管理 (CRM) システムを Salesforce.com に移行します。
- リホスト (リフトアンドシフト) — クラウド機能を活用するための変更を加えずに、アプリケーションをクラウドに移行します。例: オンプレミスの Oracle データベースを のEC2インスタンス上の Oracle に移行します AWS クラウド。
- 再配置 (ハイパーバイザーレベルのリフトアンドシフト) – 新しいハードウェアを購入したり、アプリケーションを書き換えたり、既存の運用を変更したりすることなく、インフラストラクチャをクラウドに移行できます。サーバーをオンプレミスプラットフォームから同じプラットフォームのクラウドサービスに移行します。例: Microsoft Hyper-Vアプリケーションを に移行します AWS。
- 保持 (再アクセス) — アプリケーションをお客様のソース環境で保持します。これには、主要なリファクタリングを必要とするアプリケーションや、お客様がその作業を後日まで延期したいアプリケーション、およびそれらを移行するためのビジネス上の正当性がないため、お客様が保持するレガシーアプリケーションなどがあります。
- 使用停止 — お客様のソース環境で不要になったアプリケーションを停止または削除します。

A

ABAC

「属性ベースのアクセスコントロール」を参照してください。

抽象化されたサービス

「マネージドサービス」を参照してください。

ACID

「アトミック性、一貫性、分離性、耐久性」を参照してください。

アクティブ - アクティブ移行

(双方向レプリケーションツールまたは二重書き込み操作を使用して) ソースデータベースとターゲットデータベースを同期させ、移行中に両方のデータベースが接続アプリケーションからのトランザクションを処理するデータベース移行方法。この方法では、1 回限りのカットオーバーの必要がなく、管理された小規模なバッチで移行できます。アクティブ/パッシブ移行よりも柔軟ですが、より多くの作業が必要です。

アクティブ - パッシブ移行

ソースデータベースとターゲットデータベースを同期させながら、データがターゲットデータベースにレプリケートされている間、接続しているアプリケーションからのトランザクションをソースデータベースのみで処理するデータベース移行の方法。移行中、ターゲットデータベースはトランザクションを受け付けません。

集計関数

行のグループを操作し、グループの単一の戻り値を計算するSQL関数。集計関数の例としては、SUMや などがありますMAX。

AI

「人工知能」を参照してください。

AIOps

「人工知能オペレーション」を参照してください。

匿名化

データセット内の個人情報を完全に削除するプロセス。匿名化は個人のプライバシー保護に役立ちます。匿名化されたデータは、もはや個人データとは見なされません。

アンチパターン

繰り返し起こる問題に対して頻繁に用いられる解決策で、その解決策が逆効果であったり、効果がなかったり、代替案よりも効果が低かったりするもの。

アプリケーションコントロール

マルウェアからシステムを保護するために、承認されたアプリケーションのみを使用できるようにするセキュリティアプローチ。

アプリケーションポートフォリオ

アプリケーションの構築と維持にかかるコスト、およびそのビジネス価値を含む、組織が使用する各アプリケーションに関する詳細情報の集まり。この情報は、ポートフォリオの検出と分析プロセス の需要要素であり、移行、モダナイズ、最適化するアプリケーションを特定し、優先順位を付けるのに役立ちます。

人工知能 (AI)

コンピューティングテクノロジーを使用し、学習、問題の解決、パターンの認識など、通常は人間に関連づけられる認知機能の実行に特化したコンピュータサイエンスの分野。詳細については、「人工知能 (AI) とは何ですか?」を参照してください。

人工知能オペレーション (AIOps)

機械学習技術を使用して運用上の問題を解決し、運用上のインシデントと人の介入を減らし、サービス品質を向上させるプロセス。移行戦略での AIOpsの使用方法の詳細については、 AWS 「 オペレーション統合ガイド」を参照してください。

非対称暗号化

暗号化用のパブリックキーと復号用のプライベートキーから成る 1 組のキーを使用した、暗号化のアルゴリズム。パブリックキーは復号には使用されないため共有しても問題ありませんが、プライベートキーの利用は厳しく制限する必要があります。

アトミック性、一貫性、分離性、耐久性 (ACID)

エラー、停電、その他の問題が発生した場合でも、データベースのデータ有効性と運用上の信頼性を保証する一連のソフトウェアプロパティ。

属性ベースのアクセスコントロール (ABAC)

部署、役職、チーム名など、ユーザーの属性に基づいてアクセス許可をきめ細かく設定する方法。詳細については、 AWS Identity and Access Management （ IAM) ドキュメントの「 forABAC AWS」を参照してください。

信頼できるデータソース

最も信頼性のある情報源とされるデータのプライマリーバージョンを保存する場所。匿名化、編集、仮名化など、データを処理または変更する目的で、信頼できるデータソースから他の場所にデータをコピーすることができます。

アベイラビリティーゾーン

他のアベイラビリティーゾーンの障害から AWS リージョン 隔離され、同じリージョン内の他のアベイラビリティーゾーンへの低コストで低レイテンシーのネットワーク接続を提供する 内の別の場所。

AWS クラウド導入フレームワーク (AWS CAF)

組織がクラウドに正常に移行 AWS するための効率的で効果的な計画を立てるのに役立つ、 からのガイドラインとベストプラクティスのフレームワークです。 AWS CAF は、ビジネス、人材、ガバナンス、プラットフォーム、セキュリティ、運用という 6 つの重点分野にガイダンスを編成します。ビジネス、人材、ガバナンスの観点では、ビジネススキルとプロセスに重点を置き、プラットフォーム、セキュリティ、オペレーションの視点は技術的なスキルとプロセスに焦点を当てています。例えば、人材の観点では、人事 (HR)、人材派遣機能、および人材管理を扱うステークホルダーを対象としています。この観点から、 AWS CAF は、組織がクラウド導入を成功させるための準備に役立つ、人材開発、トレーニング、コミュニケーションに関するガイダンスを提供します。詳細については、 AWS CAFウェブサイトとAWS CAFホワイトペーパーを参照してください。

AWS ワークロード認定フレームワーク (AWS WQF)

データベース移行ワークロードを評価し、移行戦略を推奨し、作業見積もりを提供するツール。AWS WQF は AWS Schema Conversion Tool （ AWS SCT) に含まれています。データベーススキーマとコードオブジェクト、アプリケーションコード、依存関係、およびパフォーマンス特性を分析し、評価レポートを提供します。

B

不正なボット

個人または組織に混乱や損害を与えることを目的としたボット。

BCP

事業継続計画を参照してください。

動作グラフ

リソースの動作とインタラクションを経時的に示した、一元的なインタラクティブビュー。Amazon Detective で動作グラフを使用して、失敗したログオン試行、疑わしいAPI呼び出し、および同様のアクションを調べることができます。詳細については、Detective ドキュメントのData in a behavior graphを参照してください。

ビッグエンディアンシステム

最上位バイトを最初に格納するシステム。エンディアンネス も参照してください。

二項分類

バイナリ結果 (2 つの可能なクラスのうちの 1 つ) を予測するプロセス。例えば、お客様の機械学習モデルで「この E メールはスパムですか、それともスパムではありませんか」などの問題を予測する必要があるかもしれません。または「この製品は書籍ですか、車ですか」などの問題を予測する必要があるかもしれません。

ブルームフィルター

要素がセットのメンバーであるかどうかをテストするために使用される、確率的でメモリ効率の高いデータ構造。

ブルー/グリーンデプロイ

2 つの異なる同一の環境を作成するデプロイ戦略。現在のアプリケーションバージョンは 1 つの環境 (ブルー) で実行し、新しいアプリケーションバージョンは他の環境 (グリーン) で実行します。この戦略は、影響を最小限に抑えながら迅速にロールバックするのに役立ちます。

ボット

インターネット経由で自動タスクを実行し、人間のアクティビティやインタラクションをシミュレートするソフトウェアアプリケーション。インターネット上の情報のインデックスを作成するウェブクローラーなど、一部のボットは有用または有益です。悪質なボット と呼ばれる他のボットの中には、個人や組織に混乱を与えたり、損害を与えたりすることを意図しているものがあります。

ボットネット

マルウェアに感染し、ボットのヘルダーまたはボットオペレーター と呼ばれる、単一関係者の管理下にあるボットのネットワーク。ボットは、ボットとその影響をスケールするための最もよく知られているメカニズムです。

ブランチ

コードリポジトリに含まれる領域。リポジトリに最初に作成するブランチは、メインブランチといいます。既存のブランチから新しいブランチを作成し、その新しいブランチで機能を開発したり、バグを修正したりできます。機能を構築するために作成するブランチは、通常、機能ブランチと呼ばれます。機能をリリースする準備ができたら、機能ブランチをメインブランチに統合します。詳細については、「ブランチについて (GitHub ドキュメント) 」を参照してください。

ブレークグラスアクセス

例外的な状況や承認されたプロセスを通じて、ユーザーが通常アクセス許可を持たない AWS アカウント にすばやくアクセスできるようになります。詳細については、 Well-Architected ガイダンスの「ブレークグラス手順の実装」インジケータ AWS を参照してください。

ブラウンフィールド戦略

環境の既存インフラストラクチャ。システムアーキテクチャにブラウンフィールド戦略を導入する場合、現在のシステムとインフラストラクチャの制約に基づいてアーキテクチャを設計します。既存のインフラストラクチャを拡張している場合は、ブラウンフィールド戦略とグリーンフィールド戦略を融合させることもできます。

バッファキャッシュ

アクセス頻度が最も高いデータが保存されるメモリ領域。

ビジネス能力

価値を生み出すためにビジネスが行うこと (営業、カスタマーサービス、マーケティングなど)。マイクロサービスのアーキテクチャと開発の決定は、ビジネス能力によって推進できます。詳細については、ホワイトペーパー AWSでのコンテナ化されたマイクロサービスの実行 の ビジネス機能を中心に組織化 セクションを参照してください。

事業継続計画 (BCP)

大規模移行など、中断を伴うイベントが運用に与える潜在的な影響に対処し、ビジネスを迅速に再開できるようにする計画。

C

CAF

AWS 「クラウド導入フレームワーク」を参照してください。

Canary デプロイ

エンドユーザーへのバージョンの低速かつ増分的なリリース。確信できたら、新しいバージョンをデプロイし、現在のバージョン全体を置き換えます。

CCoE

「Cloud Center of Excellence」を参照してください。

CDC

「データキャプチャの変更」を参照してください。

データキャプチャの変更 (CDC)

データソース (データベーステーブルなど) の変更を追跡し、その変更に関するメタデータを記録するプロセス。は、同期を維持するために、ターゲットシステムの変更を監査またはレプリケートするなど、CDCさまざまな目的で使用できます。

カオスエンジニアリング

障害や破壊的なイベントを意図的に導入して、システムの耐障害性をテストします。AWS Fault Injection Service （ AWS FIS ） を使用して、 AWS ワークロードに負荷をかけてレスポンスを評価する実験を実行できます。

CI/CD

「継続的インテグレーションと継続的デリバリー」を参照してください。

分類

予測を生成するのに役立つ分類プロセス。分類問題の機械学習モデルは、離散値を予測します。離散値は、常に互いに区別されます。例えば、モデルがイメージ内に車があるかどうかを評価する必要がある場合があります。

クライアント側の暗号化

ターゲットがデータ AWS のサービス を受信する前に、ローカルでデータを暗号化します。

Cloud Center of Excellence (CCoE)

クラウドのベストプラクティスの作成、リソースの移動、移行のタイムラインの確立、大規模変革を通じて組織をリードするなど、組織全体のクラウド導入の取り組みを推進する学際的なチーム。詳細については、 AWS クラウド エンタープライズ戦略ブログCCoEの投稿を参照してください。

クラウドコンピューティング

リモートデータストレージと IoT デバイス管理に通常使用されるクラウドテクノロジー。クラウドコンピューティングは、一般的にエッジコンピューティングテクノロジーに接続されています。

クラウド運用モデル

IT 組織において、1 つ以上のクラウド環境を構築、成熟、最適化するために使用される運用モデル。詳細については、「クラウド運用モデルの構築」を参照してください。

導入のクラウドステージ

組織が に移行するときに通常実行する 4 つのフェーズ AWS クラウド：

- プロジェクト — 概念実証と学習を目的として、クラウド関連のプロジェクトをいくつか実行する
- 基盤 — クラウド導入を拡大するための基本的な投資 (ランディングゾーンの作成、 の定義 CCoE、運用モデルの確立など)
- 移行 — 個々のアプリケーションの移行
- 再発明 — 製品とサービスの最適化、クラウドでのイノベーション

これらのステージは、 AWS クラウド エンタープライズ戦略ブログのブログ記事「クラウドファーストへのジャーニー」と「導入のステージ」で Stephen Orban によって定義されました。移行戦略とどのように関連しているかについては、 AWS「移行準備ガイド」を参照してください。

CMDB

「設定管理データベース」を参照してください。

コードリポジトリ

ソースコードやその他の資産 (ドキュメント、サンプル、スクリプトなど) が保存され、バージョン管理プロセスを通じて更新される場所。一般的なクラウドリポジトリには、 GitHub または が含まれます AWS CodeCommit。コードの各バージョンはブランチと呼ばれます。マイクロサービスの構造では、各リポジトリは 1 つの機能専用です。1 つの CI/CD パイプラインで複数のリポジトリを使用できます。

コールドキャッシュ

空である、または、かなり空きがある、もしくは、古いデータや無関係なデータが含まれているバッファキャッシュ。データベースインスタンスはメインメモリまたはディスクから読み取る必

要があり、バッファキャッシュから読み取るよりも時間がかかるため、パフォーマンスに影響します。

コールドデータ

めったにアクセスされず、通常は過去のデータです。この種類のデータをクエリする場合、通常は低速なクエリでも問題ありません。このデータを低パフォーマンスで安価なストレージ階層またはクラスに移動すると、コストを削減することができます。

コンピュータビジョン (CV)

機械学習を使用してデジタルイメージやビデオなどのビジュアル形式から情報を分析および抽出する AI の分野。例えば、 AWS Panorama はオンプレミスのカメラネットワークに CV を追加するデバイスを提供し、Amazon SageMaker は CV の画像処理アルゴリズムを提供します。

設定ドリフト

ワークロードの場合、設定は想定した状態から変化します。これにより、ワークロードが非準拠になる可能性があり、通常は段階的かつ意図的ではありません。

設定管理データベース (CMDB)

データベースとその IT 環境 (ハードウェアとソフトウェアの両方のコンポーネントとその設定を含む) に関する情報を保存、管理するリポジトリ。通常、移行のポートフォリオ検出および分析段階で CMDB のデータを使用します。

コンフォーマンスパック

コンプライアンスチェックとセキュリティチェックをカスタマイズするためにアセンブルできる AWS Config ルールと修復アクションのコレクション。テンプレートを使用して、コンフォーマンスパックを AWS アカウント およびリージョンの単一のエンティティとしてデプロイすることも、組織全体にデプロイすることもできますYAML。詳細については、 AWS Config ドキュメントの「コンフォーマンスパック」を参照してください。

継続的インテグレーションと継続的デリバリー (CI/CD)

ソフトウェアリリースプロセスのソース、ビルド、テスト、ステージング、本番の各ステージを自動化するプロセス。CI/CD は一般的にパイプラインと呼ばれます。プロセスの自動化、生産性の向上、コード品質の向上、配信の加速化を可能にします。詳細については、「継続的デリバリーの利点」を参照してください。CD は継続的デプロイ (Continuous Deployment) の略語でもあります。詳細については「継続的デリバリーと継続的なデプロイ」を参照してください。

CV

「コンピュータビジョン」を参照してください。

D

保管中のデータ

ストレージ内にあるデータなど、常に自社のネットワーク内にあるデータ。

データ分類

ネットワーク内のデータを重要度と機密性に基づいて識別、分類するプロセス。データに適した保護および保持のコントロールを判断する際に役立つため、あらゆるサイバーセキュリティのリスク管理戦略において重要な要素です。データ分類は、 AWS Well-Architected フレームワークのセキュリティの柱のコンポーネントです。詳細については、データ分類を参照してください。

データドリフト

実稼働データと ML モデルのトレーニングに使用されたデータとの間に有意な差異が生じたり、入力データが時間の経過と共に有意に変化したりすることです。データドリフトは、ML モデル予測の全体的な品質、精度、公平性を低下させる可能性があります。

転送中のデータ

ネットワーク内 (ネットワークリソース間など) を活発に移動するデータ。

データメッシュ

一元化された管理とガバナンスにより、分散型の分散型データ所有権を提供するアーキテクチャフレームワーク。

データ最小化

厳密に必要なデータのみを収集し、処理するという原則。でデータ最小化を実践 AWS クラウドすることで、プライバシーリスク、コスト、分析のカーボンフットプリントを削減できます。

データ境界

AWS 環境内の一連の予防ガードレール。信頼できる ID のみが、期待されるネットワークから信頼できるリソースにアクセスしていることを確実にします。詳細については、「 でのデータ境界の構築 AWS」を参照してください。

データの前処理

raw データをお客様の機械学習モデルで簡単に解析できる形式に変換すること。データの前処理とは、特定の列または行を削除して、欠落している、矛盾している、または重複する値に対処することを意味します。

データ出所

データの生成、送信、保存の方法など、データのライフサイクル全体を通じてデータの出所と履歴を追跡するプロセス。

データ件名

データを収集、処理している個人。

データウェアハウス

分析などのビジネスインテリジェンスをサポートするデータ管理システム。データウェアハウスには通常、大量の履歴データが含まれており、クエリや分析によく使用されます。

データベース定義言語 (DDL)

データベース内のテーブルやオブジェクトの構造を作成または変更するためのステートメントまたはコマンド。

データベース操作言語 (DML)

データベース内の情報を変更 (挿入、更新、削除) するためのステートメントまたはコマンド。

DDL

「データベース定義言語」を参照してください。

ディープアンサンブル

予測のために複数の深層学習モデルを組み合わせる。ディープアンサンブルを使用して、より正確な予測を取得したり、予測の不確実性を推定したりできます。

ディープラーニング

人工ニューラルネットワークの複数層を使用して、入力データと対象のターゲット変数の間のマッピングを識別する機械学習サブフィールド。

defense-in-depth

一連のセキュリティメカニズムとコントロールをコンピュータネットワーク全体に層状に重ねて、ネットワークとその内部にあるデータの機密性、整合性、可用性を保護する情報セキュリティの手法。この戦略を に採用するときは AWS、 AWS Organizations 構造の異なるレイヤーに複数のコントロールを追加して、リソースの安全性を確保します。例えば、 defense-in-depth アプローチでは、多要素認証、ネットワークセグメンテーション、暗号化を組み合わせることができます。

委任管理者

では AWS Organizations、互換性のあるサービスが AWS メンバーアカウントを登録して組織のアカウントを管理し、そのサービスのアクセス許可を管理できます。このアカウントを、そのサービスの委任管理者と呼びます。詳細、および互換性のあるサービスの一覧は、 AWS Organizations ドキュメントのAWS Organizationsで使用できるサービスを参照してください。

デプロイメント

アプリケーション、新機能、コードの修正をターゲットの環境で利用できるようにするプロセス。デプロイでは、コードベースに変更を施した後、アプリケーションの環境でそのコードベースを構築して実行します。

開発環境

「環境」を参照してください。

検出管理

イベントが発生したときに、検出、ログ記録、警告を行うように設計されたセキュリティコントロール。これらのコントロールは副次的な防衛手段であり、実行中の予防的コントロールをすり抜けたセキュリティイベントをユーザーに警告します。詳細については、Implementing security controls on AWSのDetective controlsを参照してください。

開発値ストリームマッピング (DVSM)

ソフトウェア開発ライフサイクルのスピードと品質に悪影響を及ぼす制約を特定し、優先順位を付けるために使用されるプロセス。DVSM は、もともとリーンマニュファクチャリングプラクティス用に設計されたバリューストリームマッピングプロセスを拡張します。ソフトウェア開発プロセスを通じて価値を創造し、動かすために必要なステップとチームに焦点を当てています。

デジタルツイン

建物、工場、産業機器、生産ラインなど、現実世界のシステムを仮想的に表現したものです。デジタルツインは、予知保全、リモートモニタリング、生産最適化をサポートします。

ディメンションテーブル

スタースキーマ では、ファクトテーブル内の量的データに関するデータ属性を含む小さなテーブル。ディメンションテーブル属性は通常、テキストフィールドまたはテキストのように動作する離散数値です。これらの属性は、クエリの制約、フィルタリング、結果セットのラベル付けに一般的に使用されます。

ディザスタ

ワークロードまたはシステムが、導入されている主要な場所でのビジネス目標の達成を妨げるイベント。これらのイベントは、自然災害、技術的障害、または意図しない設定ミスやマルウェア攻撃などの人間の行動の結果である場合があります。

ディザスタリカバリ (DR)

災害によるダウンタイムとデータ損失を最小限に抑えるために使用する戦略とプロセス。詳細については、 AWS Well-Architected フレームワークの「 でのワークロードのディザスタリカバリ AWS: クラウドでのリカバリ」を参照してください。

DML

「データベース操作言語」を参照してください。

ドメイン駆動型設計

各コンポーネントが提供している変化を続けるドメイン、またはコアビジネス目標にコンポーネントを接続して、複雑なソフトウェアシステムを開発するアプローチ。この概念は、エリック・エヴァンスの著書、Domain-Driven Design: Tackling Complexity in the Heart of Software (ドメイン駆動設計:ソフトウェアの中心における複雑さへの取り組み) で紹介されています (ボストン: Addison-Wesley Professional、2003)。strangler fig パターンでドメイン駆動型設計を使用する方法については、「従来の Microsoft のモダナイズ」を参照してくださいASP。NET (ASMX) コンテナと Amazon API Gateway を使用してウェブサービスを段階的に行う。

DR

「ディザスタリカバリ」を参照してください。

ドリフト検出

ベースライン設定からの偏差の追跡。例えば、 AWS CloudFormation を使用してシステムリソース のドリフトを検出したり、 を使用して AWS Control Tower ガバナンス要件への準拠に影響を与える可能性のあるランディングゾーンの変更を検出したりできます。

DVSM

「開発値ストリームマッピング」を参照してください。

E

EDA

「探索的データ分析」を参照してください。

エッジコンピューティング

IoT ネットワークのエッジにあるスマートデバイスの計算能力を高めるテクノロジー。クラウドコンピューティング と比較すると、エッジコンピューティングは通信レイテンシーを短縮し、応答時間を短縮できます。

暗号化

人間が読み取り可能なプレーンテキストデータを暗号文に変換するコンピューティングプロセス。

暗号化キー

暗号化アルゴリズムが生成した、ランダム化されたビットからなる暗号文字列。キーの長さは決まっておらず、各キーは予測できないように、一意になるように設計されています。

エンディアン

コンピュータメモリにバイトが格納される順序。ビッグエンディアンシステムでは、最上位バイトが最初に格納されます。リトルエンディアンシステムでは、最下位バイトが最初に格納されます。

エンドポイント

「サービスエンドポイント」を参照してください。

エンドポイントサービス

仮想プライベートクラウド (VPC) でホストして他のユーザーと共有できるサービス。を使用してエンドポイントサービスを作成し AWS PrivateLink 、他の AWS アカウント または AWS Identity and Access Management （ IAM) プリンシパルにアクセス許可を付与できます。これらのアカウントまたはプリンシパルは、インターフェイスエンドポイントを作成することで、VPCエンドポイントサービスにプライベートに接続できます。詳細については、Amazon Virtual Private Cloud (Amazon) ドキュメントの「エンドポイントサービスの作成」を参照してください。 VPC

エンタープライズリソース計画 (ERP)

エンタープライズの主要なビジネスプロセス (アカウンティング、、プロジェクト管理など) を自動化MESおよび管理するシステム。

エンベロープ暗号化

暗号化キーを、別の暗号化キーを使用して暗号化するプロセス。詳細については、 AWS Key Management Service （ AWS KMS) ドキュメントの「エンベロープ暗号化」を参照してください。

環境

実行中のアプリケーションのインスタンス。クラウドコンピューティングにおける一般的な環境の種類は以下のとおりです。

- 開発環境 — アプリケーションのメンテナンスを担当するコアチームのみが使用できる、実行中のアプリケーションのインスタンス。開発環境は、上位の環境に昇格させる変更をテストするときに使用します。このタイプの環境は、テスト環境と呼ばれることもあります。
- 下位環境 — 初期ビルドやテストに使用される環境など、アプリケーションのすべての開発環境。
- 本番環境 — エンドユーザーがアクセスできる、実行中のアプリケーションのインスタンス。CI/CD パイプラインでは、本番環境が最後のデプロイ環境になります。
- 上位環境 — コア開発チーム以外のユーザーがアクセスできるすべての環境。これには、本番環境、本番前環境、ユーザー承認テスト環境などが含まれます。

エピック

アジャイル方法論で、お客様の作業の整理と優先順位付けに役立つ機能カテゴリ。エピックでは、要件と実装タスクの概要についてハイレベルな説明を提供します。例えば、 AWS CAFセキュリティエピックには、ID とアクセスの管理、検出コントロール、インフラストラクチャセキュリティ、データ保護、インシデント対応が含まれます。 AWS 移行戦略のエピックの詳細については、プログラム実装ガイド を参照してください。

ERP

「エンタープライズリソース計画」を参照してください。

探索的データ分析 (EDA)

データセットを分析してその主な特性を理解するプロセス。お客様は、データを収集または集計してから、パターンの検出、異常の検出、および前提条件のチェックのための初期調査を実行します。EDA は、サマリー統計を計算し、データの視覚化を作成することによって実行されます。

F

ファクトテーブル

スタースキーマ の中央テーブル。事業運営に関する定量的データを保存します。通常、ファクトテーブルには、メジャーを含む列とディメンションテーブルへの外部キーを含む列の 2 種類の列が含まれます。

フェイルファスト

頻繁で段階的なテストを使用して開発ライフサイクルを短縮する哲学。これはアジャイルアプローチの重要な部分です。

障害分離境界

では AWS クラウド、アベイラビリティーゾーン AWS リージョン、コントロールプレーン、データプレーンなどの境界で、障害の影響を制限し、ワークロードの耐障害性を向上させるのに役立ちます。詳細については、AWS 「障害分離境界」を参照してください。

機能ブランチ

「ブランチ」を参照してください。

特徴量

お客様が予測に使用する入力データ。例えば、製造コンテキストでは、特徴量は製造ラインから定期的にキャプチャされるイメージの可能性もあります。

特徴量重要度

モデルの予測に対する特徴量の重要性。これは通常、Shapley Additive Explanations (SHAP) や積分勾配など、さまざまな手法で計算できる数値スコアとして表されます。詳細については、「 を使用した機械学習モデルの解釈可能性：AWS」を参照してください。

機能変換

追加のソースによるデータのエンリッチ化、値のスケーリング、単一のデータフィールドからの複数の情報セットの抽出など、機械学習プロセスのデータを最適化すること。これにより、機械学習モデルはデータの恩恵を受けることができます。例えば、「2021-05-27 00:15:37」の日付を「2021 年」、「5 月」、「木」、「15」に分解すると、学習アルゴリズムがさまざまなデータコンポーネントに関連する微妙に異なるパターンを学習するのに役立ちます。

FGAC

「きめ細かなアクセスコントロール」を参照してください。

きめ細かなアクセスコントロール (FGAC)

複数の条件を使用してアクセス要求を許可または拒否すること。

フラッシュカット移行

段階的なアプローチを使用するのではなく、変更データキャプチャによる継続的なデータレプリケーションを使用して、可能な限り短い時間でデータを移行するデータベース移行方法。目的はダウンタイムを最小限に抑えることです。

G

ジオブロッキング

「地理的制限」を参照してください。

地理的制限 (ジオブロッキング)

Amazon では CloudFront、特定の国のユーザーがコンテンツディストリビューションにアクセスできないようにするオプションです。アクセスを許可する国と禁止する国は、許可リストまたは禁止リストを使って指定します。詳細については、 CloudFront ドキュメントの「コンテンツの地理的ディストリビューションの制限」を参照してください。

Gitflow ワークフロー

下位環境と上位環境が、ソースコードリポジトリでそれぞれ異なるブランチを使用する方法。Gitflow ワークフローはレガシーと見なされ、トランクベースのワークフローはモダンで推奨されるアプローチです。

グリーンフィールド戦略

新しい環境に既存のインフラストラクチャが存在しないこと。システムアーキテクチャにグリーンフィールド戦略を導入する場合、既存のインフラストラクチャ (別名ブラウンフィールド) との互換性の制約を受けることなく、あらゆる新しいテクノロジーを選択できます。既存のインフラストラクチャを拡張している場合は、ブラウンフィールド戦略とグリーンフィールド戦略を融合させることもできます。

ガードレール

組織単位 () 全体のリソース、ポリシー、コンプライアンスの管理に役立つ大まかなルールOUs。予防ガードレールは、コンプライアンス基準に一致するようにポリシーを実施します。これらは、サービスコントロールポリシーとIAMアクセス許可の境界を使用して実装されます。検出ガードレールは、ポリシー違反やコンプライアンス上の問題を検出し、修復のためのアラートを発信します。これらは、 AWS Config、、Amazon AWS Security Hub、 GuardDuty、Amazon Inspector AWS Trusted Advisor、およびカスタム AWS Lambda チェックを使用して実装されます。

H

HA

「高可用性」を参照してください。

異種混在データベースの移行

別のデータベースエンジンを使用するターゲットデータベースへお客様の出典データベースの移行 (例えば、Oracle から Amazon Aurora)。異種間移行は通常、アーキテクチャの再設計作業の一部であり、スキーマの変換は複雑なタスクになる可能性があります。AWS は、スキーマの変換に役立つ AWS SCTを提供します。

ハイアベイラビリティ (HA)

課題や災害が発生した場合に、介入なしにワークロードを継続的に運用できること。HA システムは、自動的にフェイルオーバーし、一貫して高品質のパフォーマンスを提供し、パフォーマンスへの影響を最小限に抑えながらさまざまな負荷や障害を処理するように設計されています。

ヒストリアンのモダナイゼーション

製造業のニーズによりよく応えるために、オペレーションテクノロジー (OT) システムをモダナイズし、アップグレードするためのアプローチ。ヒストリアンは、工場内のさまざまなソースからデータを収集して保存するために使用されるデータベースの一種です。

同種データベースの移行

ソースデータベースを、同じデータベースエンジンを共有するターゲットデータベースに移行する (Microsoft SQL Server から Amazon RDS for SQL Server など) 。同種間移行は、通常、リホストまたはリプラットフォーム化の作業の一部です。ネイティブデータベースユーティリティを使用して、スキーマを移行できます。

ホットデータ

リアルタイムデータや最近の翻訳データなど、頻繁にアクセスされるデータ。通常、このデータには高速なクエリ応答を提供する高性能なストレージ階層またはクラスが必要です。

ホットフィックス

本番環境の重大な問題を修正するために緊急で配布されるプログラム。緊急性のため、通常、修正は一般的な DevOps リリースワークフローの外で行われます。

ハイパーケア期間

カットオーバー直後、移行したアプリケーションを移行チームがクラウドで管理、監視して問題に対処する期間。通常、この期間は 1~4 日です。ハイパーケア期間が終了すると、アプリケーションに対する責任は一般的に移行チームからクラウドオペレーションチームに移ります。

I

IaC

「Infrastructure as Code」を参照してください。

ID ベースのポリシー

AWS クラウド 環境内のアクセス許可を定義する 1 つ以上のIAMプリンシパルにアタッチされたポリシー。

アイドル状態のアプリケーション

90 日間の平均使用量CPUとメモリ使用量が 5～20% のアプリケーション。移行プロジェクトでは、これらのアプリケーションを廃止するか、オンプレミスに保持するのが一般的です。

IIoT

「産業モノのインターネット」を参照してください。

イミュータブルインフラストラクチャ

既存のインフラストラクチャを更新、パッチ適用、または変更するのではなく、本番ワークロード用の新しいインフラストラクチャをデプロイするモデル。イミュータブルなインフラストラクチャは、本質的にミュータブルなインフラストラクチャ よりも一貫性、信頼性、予測性が高くなります。詳細については、 AWS Well-Architected フレームワークの「変更不可能なインフラストラクチャを使用したデプロイ」のベストプラクティスを参照してください。

インバウンド (イングレス) VPC

AWS マルチアカウントアーキテクチャでは、アプリケーション外からのネットワーク接続を受け入れ、検査し、ルーティングVPCする 。AWS セキュリティリファレンスアーキテクチャでは、アプリケーションとより広範なインターネット間の双方向インターフェイスVPCsを保護するために、インバウンド、アウトバウンド、検査でネットワークアカウントを設定することをお勧めします。

増分移行

アプリケーションを 1 回ですべてカットオーバーするのではなく、小さい要素に分けて移行するカットオーバー戦略。例えば、最初は少数のマイクロサービスまたはユーザーのみを新しいシステムに移行する場合があります。すべてが正常に機能することを確認できたら、残りのマイクロサービスやユーザーを段階的に移行し、レガシーシステムを廃止できるようにします。この戦略により、大規模な移行に伴うリスクが軽減されます。

インダストリー 4.0

2016 年に Klaus Schwab によって導入された用語で、接続、リアルタイムデータ、自動化、分析、AI/ML の進歩によるビジネスプロセスのモダナイズを指します。

インフラストラクチャ

アプリケーションの環境に含まれるすべてのリソースとアセット。

Infrastructure as Code (IaC)

アプリケーションのインフラストラクチャを一連の設定ファイルを使用してプロビジョニングし、管理するプロセス。IaC は、新しい環境を再現可能で信頼性が高く、一貫性のあるものにするため、インフラストラクチャを一元的に管理し、リソースを標準化し、スケールを迅速に行えるように設計されています。

産業モノのインターネット (IIoT)

製造、エネルギー、自動車、ヘルスケア、ライフサイエンス、農業などの産業部門におけるインターネットに接続されたセンサーやデバイスの使用。詳細については、「産業モノのインターネット (IIoT) デジタルトランスフォーメーション戦略の構築」を参照してください。

検査 VPC

AWS マルチアカウントアーキテクチャでは、 VPCs (同一または異なる 内 AWS リージョン)、インターネット、オンプレミスネットワーク間のネットワークトラフィックの検査VPCを管理する一元化された です。AWS セキュリティリファレンスアーキテクチャでは、アプリケーションとより広範なインターネット間の双方向インターフェイスVPCsを保護するために、インバウンド、アウトバウンド、検査でネットワークアカウントを設定することをお勧めします。

IoT

インターネットまたはローカル通信ネットワークを介して他のデバイスやシステムと通信する、センサーまたはプロセッサが組み込まれた接続済み物理オブジェクトのネットワーク。詳細については、「IoT とは」を参照してください。

解釈可能性

機械学習モデルの特性で、モデルの予測がその入力にどのように依存するかを人間が理解できる度合いを表します。詳細については、「 による機械学習モデルの解釈可能性AWS」を参照してください。

IoT

「モノのインターネット」を参照してください。

IT 情報ライブラリ (ITIL)

IT サービスを提供し、これらのサービスをビジネス要件に合わせるための一連のベストプラクティス。ITIL は、 の基盤を提供しますITSM。

IT サービス管理 (ITSM)

組織の IT サービスの設計、実装、管理、およびサポートに関連する活動。クラウドオペレーションとITSMツールの統合については、「 オペレーション統合ガイド」を参照してください。

ITIL

「IT 情報ライブラリ」を参照してください。

ITSM

「IT サービス管理」を参照してください。

L

ラベルベースのアクセスコントロール (LBAC)

ユーザーとデータ自体にそれぞれセキュリティラベル値が明示的に割り当てられている必須アクセスコントロール (MAC) の実装。ユーザーセキュリティラベルとデータセキュリティラベルが交差する部分によって、ユーザーに表示される行と列が決まります。

ランディングゾーン

ランディングゾーンは、スケーラブルで安全な、適切に設計されたマルチアカウント AWS 環境です。これは、組織がセキュリティおよびインフラストラクチャ環境に自信を持ってワークロードとアプリケーションを迅速に起動してデプロイできる出発点です。ランディングゾーンの詳細については、安全でスケーラブルなマルチアカウント AWS 環境のセットアップ を参照してください。

大規模な移行

300 台以上のサーバの移行。

LBAC

「ラベルベースのアクセスコントロール」を参照してください。

最小特権

タスクの実行には必要最低限の権限を付与するという、セキュリティのベストプラクティス。詳細については、 IAMドキュメントの「最小特権のアクセス許可を適用する」を参照してください。

リフトアンドシフト

「7 R」を参照してください。

リトルエンディアンシステム

最下位バイトを最初に格納するシステム。エンディアンネス も参照してください。

下位環境

「環境」を参照してください。

M

機械学習 (ML)

パターン認識と学習にアルゴリズムと手法を使用する人工知能の一種。ML は、モノのインターネット (IoT) データなどの記録されたデータを分析して学習し、パターンに基づく統計モデルを生成します。詳細については、「機械学習」を参照してください。

メインブランチ

「ブランチ」を参照してください。

マルウェア

コンピュータのセキュリティまたはプライバシーを侵害するように設計されているソフトウェア。マルウェアは、コンピュータシステムの中断、機密情報の漏洩、不正アクセスにつながる可能性があります。マルウェアの例としては、ウイルス、ワーム、ランサムウェア、トロイの木馬、スパイウェア、キーロガーなどがあります。

マネージドサービス

AWS のサービス がインフラストラクチャレイヤー、オペレーティングシステム、プラットフォーム AWS を運用し、ユーザーがエンドポイントにアクセスしてデータを保存および取得します。Amazon Simple Storage Service (Amazon S3) と Amazon DynamoDB は、 マネージドサービスの例です。これらは抽象化されたサービス とも呼ばれます。

製造実行システム (MES)

生産プロセスを追跡、モニタリング、文書化、制御するためのソフトウェアシステム。これにより、加工品を現場の完成製品に変換します。

MAP

「移行促進プログラム」を参照してください。

メカニズム

ツールを作成し、ツールの導入を推進し、調整のために結果を検査する完全なプロセス。メカニズムは、動作中にそれ自体を強化して改善するサイクルです。詳細については、 AWS Well-Architected フレームワークの「メカニズムの構築」を参照してください。

メンバーアカウント

の組織の一部である管理アカウント AWS アカウント を除くすべての AWS Organizations。アカウントが組織のメンバーになることができるのは、一度に 1 つのみです。

MES

「製造実行システム」を参照してください。

メッセージキューイングテレメトリトランスポート (MQTT)

リソースに制約のある IoT デバイス用の、パブリッシュ/サブスクライブパターンに基づく軽量の machine-to-machine (M2M) 通信プロトコル。

マイクロサービス

明確に定義された上で通信APIsし、通常は小規模で自己完結型のチームが所有する小規模で独立したサービス。例えば、保険システムには、販売やマーケティングなどのビジネス機能、または購買、請求、分析などのサブドメインにマッピングするマイクロサービスが含まれる場合があります。マイクロサービスの利点には、俊敏性、柔軟なスケーリング、容易なデプロイ、再利用可能なコード、回復力などがあります。詳細については、AWS 「サーバーレスサービスを使用したマイクロサービスの統合」を参照してください。

マイクロサービスアーキテクチャ

各アプリケーションプロセスをマイクロサービスとして実行する独立したコンポーネントを使用してアプリケーションを構築するアプローチ。これらのマイクロサービスは、軽量な を使用して明確に定義されたインターフェイスを介して通信しますAPIs。このアーキテクチャの各マイクロサービスは、アプリケーションの特定の機能に対する需要を満たすように更新、デプロイ、およびスケーリングできます。詳細については、「 でのマイクロサービスの実装 AWS」を参照してください。

Migration Acceleration Program (MAP)

コンサルティングサポート、トレーニング、サービスを提供し、組織がクラウドへの移行のための強固な運用基盤を構築し、移行の初期コストを相殺するのに役立つ AWS プログラム。MAP には、従来の移行を系統的に実行するための移行方法論と、一般的な移行シナリオを自動化して高速化するための一連のツールが含まれています。

大規模な移行

アプリケーションポートフォリオの大部分を次々にクラウドに移行し、各ウェーブでより多くのアプリケーションを高速に移動させるプロセス。この段階では、以前の段階から学んだベストプラクティスと教訓を使用して、移行ファクトリー チーム、ツール、プロセスのうち、オートメーションとアジャイルデリバリーによってワークロードの移行を合理化します。これは、AWS 移行戦略 の第 3 段階です。

移行ファクトリー

自動化された俊敏性のあるアプローチにより、ワークロードの移行を合理化する部門横断的なチーム。移行ファクトリーチームには、通常、オペレーション、ビジネスアナリストと所有者、移行エンジニア、デベロッパー、スプリントに取り組む DevOps プロフェッショナルが含まれます。エンタープライズアプリケーションポートフォリオの 20～50% は、ファクトリーのアプローチによって最適化できる反復パターンで構成されています。詳細については、このコンテンツセットの移行ファクトリーに関する解説とCloud Migration Factory ガイドを参照してください。

移行メタデータ

移行を完了するために必要なアプリケーションおよびサーバーに関する情報。移行パターンごとに、異なる一連の移行メタデータが必要です。移行メタデータの例には、ターゲットサブネット、セキュリティグループ、 AWS アカウントなどがあります。

移行パターン

移行戦略、移行先、および使用する移行アプリケーションまたはサービスを詳述する、反復可能な移行タスク。例: Application Migration Service EC2を使用して Amazon AWS への移行をリホストします。

移行ポートフォリオ評価 (MPA)

に移行するためのビジネスケースを検証するための情報を提供するオンラインツール AWS クラウド。MPA は、詳細なポートフォリオ評価 (サーバーの適切なサイズ設定、料金設定、TCO比較、移行コスト分析) と移行計画 (アプリケーションデータ分析とデータ収集、アプリケーショングループ化、移行の優先順位付け、ウェーブプランニング) を提供します。MPA ツール (ログイ

ンが必要) は、すべての AWS コンサルタントとAPNパートナーコンサルタントが無料で利用できます。

移行準備状況評価 (MRA)

を使用して、組織のクラウドの準備状況に関するインサイトを取得し、長所と短所を特定し、特定されたギャップを埋めるためのアクションプランを構築するプロセス AWS CAF。詳細については、移行準備状況ガイド を参照してください。MRA はAWS 移行戦略 の最初のフェーズです。

移行戦略

ワークロードを に移行するために使用されるアプローチ AWS クラウド。詳細については、この用語集の「7 Rs エントリ」と「組織を動員して大規模な移行を加速する」を参照してください。

ML

「機械学習」を参照してください。

モダナイゼーション

古い (レガシーまたはモノリシック) アプリケーションとそのインフラストラクチャをクラウド内の俊敏で弾力性のある高可用性システムに変換して、コストを削減し、効率を高め、イノベーションを活用します。詳細については、「」の「アプリケーションをモダナイズするための戦略 AWS クラウド」を参照してください。

モダナイゼーション準備状況評価

組織のアプリケーションのモダナイゼーションの準備状況を判断し、利点、リスク、依存関係を特定し、組織がこれらのアプリケーションの将来の状態をどの程度適切にサポートできるかを決定するのに役立つ評価。評価の結果として、ターゲットアーキテクチャのブループリント、モダナイゼーションプロセスの開発段階とマイルストーンを詳述したロードマップ、特定されたギャップに対処するためのアクションプランが得られます。詳細については、「」の「アプリケーションのモダナイゼーション準備状況の評価 AWS クラウド」を参照してください。

モノリシックアプリケーション (モノリス)

緊密に結合されたプロセスを持つ単一のサービスとして実行されるアプリケーション。モノリシックアプリケーションにはいくつかの欠点があります。1 つのアプリケーション機能エクスペリエンスの需要が急増する場合は、アーキテクチャ全体をスケーリングする必要があります。モノリシックアプリケーションの特徴を追加または改善することは、コードベースが大きくなると複雑になります。これらの問題に対処するには、マイクロサービスアーキテクチャを使用できます。詳細については、モノリスをマイクロサービスに分解する を参照してください。

MPA

「移行ポートフォリオ評価」を参照してください。

MQTT

「Message Queuing Telemetry Transport」を参照してください。

多クラス分類

複数のクラスの予測を生成するプロセス (2 つ以上の結果の 1 つを予測します)。例えば、機械学習モデルが、「この製品は書籍、自動車、電話のいずれですか?」 または、「このお客様にとって最も関心のある商品のカテゴリはどれですか?」と聞くかもしれません。

変更可能なインフラストラクチャ

本番ワークロードの既存のインフラストラクチャを更新および変更するモデル。Well-Architected AWS Framework では、一貫性、信頼性、予測可能性を向上させるために、イミュータブルインフラストラクチャの使用をベストプラクティスとして推奨しています。

O

OAC

「オリジンアクセスコントロール」を参照してください。

OAI

「オリジンアクセスアイデンティティ」を参照してください。

OCM

「組織変更管理」を参照してください。

オフライン移行

移行プロセス中にソースワークロードを停止させる移行方法。この方法はダウンタイムが長くなるため、通常は重要ではない小規模なワークロードに使用されます。

OI

「 オペレーション統合」を参照してください。

OLA

「運用レベルの契約」を参照してください。

オンライン移行

ソースワークロードをオフラインにせずにターゲットシステムにコピーする移行方法。ワークロードに接続されているアプリケーションは、移行中も動作し続けることができます。この方法はダウンタイムがゼロから最小限で済むため、通常は重要な本番稼働環境のワークロードに使用されます。

OPC-UA

「Open Process Communications - Unified Architecture」を参照してください。

オープンプロセス通信 - 統合アーキテクチャ (OPC-UA)

産業用オートメーション用の machine-to-machine (M2M) 通信プロトコル。OPC-UA は、データの暗号化、認証、認可スキームを備えた相互運用性標準を提供します。

運用レベルの契約 (OLA)

サービスレベルアグリーメント () をサポートするために、どの機能 IT グループが相互に提供することを約束するかを明確にする契約SLA。

運用準備状況レビュー (ORR)

インシデントや潜在的な障害の理解、評価、防止、または範囲の縮小に役立つ質問とそれに関連するベストプラクティスのチェックリスト。詳細については、 AWS Well-Architected フレームワークの「運用準備状況レビュー (ORR)」を参照してください。

運用テクノロジー (OT)

産業運用、機器、インフラストラクチャを制御するために物理環境と連携するハードウェアおよびソフトウェアシステム。製造では、OT と情報技術 (IT) システムの統合が、Industry 4.0 トランスフォーメーションの主要な焦点です。

オペレーション統合 (OI)

クラウドでオペレーションをモダナイズするプロセスには、準備計画、オートメーション、統合が含まれます。詳細については、オペレーション統合ガイド を参照してください。

組織の証跡

の組織 AWS アカウント 内のすべての のすべてのイベントをログ AWS CloudTrail に記録する によって作成された証跡 AWS Organizations。証跡は、組織に含まれている各 AWS アカウント に作成され、各アカウントのアクティビティを追跡します。詳細については、 ドキュメントの「組織の証跡の作成」を参照してください。 CloudTrail

組織の変更管理 (OCM)

人材、文化、リーダーシップの観点から、主要な破壊的なビジネス変革を管理するためのフレームワーク。OCM は、変化の導入を加速し、移行に伴う問題に対処し、文化的および組織的な変化を推進することで、組織が新しいシステムや戦略の準備と移行を支援します。 AWS 移行戦略では、クラウド導入プロジェクトに必要な変化のスピードから、このフレームワークは人材アクセラレーション と呼ばれます。詳細については、OCM「」ガイドを参照してください。

オリジンアクセスコントロール (OAC)

では CloudFront、Amazon Simple Storage Service (Amazon S3) コンテンツを保護するためのアクセスを制限するための拡張オプションです。OAC は、すべての のすべての S3 バケット AWS リージョン、 AWS KMS (-SSEKMS) によるサーバー側の暗号化、S3 バケットへの動的 PUTおよび DELETEリクエストをサポートします。

オリジンアクセスアイデンティティ (OAI)

では CloudFront、Amazon S3 コンテンツを保護するためのアクセスを制限するオプションです。を使用するとOAI、 は Amazon S3 が認証できるプリンシパル CloudFront を作成します。認証されたプリンシパルは、特定の CloudFront ディストリビューションを介してのみ S3 バケット内のコンテンツにアクセスできます。「」も参照してください。これによりOAC、より詳細で拡張されたアクセスコントロールが提供されます。

ORR

「運用準備状況レビュー」を参照してください。

OT

「運用技術」を参照してください。

アウトバウンド (出力) VPC

AWS マルチアカウントアーキテクチャでは、アプリケーション内から開始されるネットワーク接続VPCを処理する 。AWS セキュリティリファレンスアーキテクチャでは、アプリケーションとより広範なインターネット間の双方向インターフェイスVPCsを保護するために、インバウンド、アウトバウンド、検査でネットワークアカウントを設定することをお勧めします。

P

アクセス許可の境界

ユーザーまたはロールが持つことができるアクセス許可の上限を設定するためにプリンIAMシパルにアタッチされるIAM管理ポリシー。詳細については、 IAMドキュメントの「アクセス許可の境界」を参照してください。

個人を特定できる情報 (PII)

直接閲覧した場合、または他の関連データと組み合わせた場合に、個人の身元を合理的に推測するために使用できる情報。例としてPIIは、名前、住所、連絡先情報などがあります。

PII

個人を特定できる情報を参照してください。

プレイブック

クラウドでのコアオペレーション機能の提供など、移行に関連する作業を取り込む、事前定義された一連のステップ。プレイブックは、スクリプト、自動ランブック、またはお客様のモダナイズされた環境を運用するために必要なプロセスや手順の要約などの形式をとることができます。

PLC

「プログラム可能なロジックコントローラー」を参照してください。

PLM

「製品ライフサイクル管理」を参照してください。

ポリシー

アクセス許可の定義 (アイデンティティベースのポリシー を参照) 、アクセス条件の指定 (リソースベースのポリシー を参照) 、または の組織内のすべてのアカウントに対する最大アクセス許可の定義 AWS Organizations （ サービスコントロールポリシー を参照) が可能なオブジェクト。

多言語の永続性

データアクセスパターンやその他の要件に基づいて、マイクロサービスのデータストレージテクノロジーを個別に選択します。マイクロサービスが同じデータストレージテクノロジーを使用している場合、実装上の問題が発生したり、パフォーマンスが低下する可能性があります。マイクロサービスは、要件に最も適合したデータストアを使用すると、より簡単に実装でき、パフォーマンスとスケーラビリティが向上します。詳細については、マイクロサービスでのデータ永続性の有効化 を参照してください。

ポートフォリオ評価

移行を計画するために、アプリケーションポートフォリオの検出、分析、優先順位付けを行うプロセス。詳細については、「移行準備状況ガイド」を参照してください。

述語

`true` または を返すクエリ条件。`false`通常は `WHERE`句にあります。

述語プッシュダウン

転送前にクエリ内のデータをフィルタリングするデータベースクエリ最適化手法。これにより、リレーショナルデータベースから取得して処理する必要があるデータの量が減少し、クエリのパフォーマンスが向上します。

予防的コントロール

イベントの発生を防ぐように設計されたセキュリティコントロール。このコントロールは、ネットワークへの不正アクセスや好ましくない変更を防ぐ最前線の防御です。詳細については、Implementing security controls on AWSのPreventative controlsを参照してください。

プリンシパル

アクションを実行し AWS 、リソースにアクセスできる のエンティティ。このエンティティは通常、、 IAMロール AWS アカウント、または ユーザーのルートユーザーです。詳細については、IAMドキュメントの「ロールの用語と概念」の「プリンシパル」を参照してください。

プライバシーバイデザイン

エンジニアリングプロセス全体を通してプライバシーを考慮に入れたシステムエンジニアリングのアプローチ。

プライベートホストゾーン

Amazon Route 53 が 1 つ以上の 内のドメインとそのサブドメインのDNSクエリにどのように応答するかに関する情報を保持するコンテナVPCs。詳細については、Route 53 ドキュメントの「プライベートホストゾーンの使用」を参照してください。

プロアクティブコントロール

非準拠のリソースのデプロイを防止するように設計されたセキュリティコントロール。これらのコントロールは、プロビジョニング前にリソースをスキャンします。リソースがコントロールに準拠していない場合、プロビジョニングされません。詳細については、 AWS Control Tower ドキュメントの「 コントロールリファレンスガイド」および「 でのセキュリティコントロールの実装」の「プロアクティブコントロール」を参照してください。 AWS

製品ライフサイクル管理 (PLM)

設計、開発、発売から成長と成熟まで、製品のデータとプロセスのライフサイクル全体にわたる管理、および辞退と削除。

本番環境

「環境」を参照してください。

プログラム可能なロジックコントローラー (PLC)

製造では、マシンをモニタリングし、承認プロセスを自動化する、信頼性が高く、適応性の高いコンピュータです。

仮名化

データセット内の個人識別子をプレースホルダー値に置き換えるプロセス。仮名化は個人のプライバシー保護に役立ちます。仮名化されたデータは、依然として個人データとみなされます。

パブリッシュ/サブスクライブ (pub/sub)

マイクロサービス間の非同期通信を可能にするパターン。スケーラビリティと応答性を向上させます。例えば、マイクロサービスベースの ではMES、マイクロサービスは他のマイクロサービスがサブスクライブできるチャネルにイベントメッセージを発行できます。システムは、公開サービスを変更せずに新しいマイクロサービスを追加できます。

Q

クエリプラン

SQL リレーショナルデータベースシステム内のデータにアクセスするために使用される手順などの一連のステップ。

クエリプランのリグレッション

データベースサービスのオプティマイザーが、データベース環境に特定の変更が加えられる前に選択されたプランよりも最適性の低いプランを選択すること。これは、統計、制限事項、環境設定、クエリパラメータのバインディングの変更、およびデータベースエンジンの更新などが原因である可能性があります。

R

RACI マトリックス

責任、説明責任、相談、通知 (RACI) を参照してください。

ランサムウェア

決済が完了するまでコンピュータシステムまたはデータへのアクセスをブロックするように設計された、悪意のあるソフトウェア。

RASCI マトリックス

責任、説明責任、相談、通知 (RACI) を参照してください。

RCAC

「行と列のアクセスコントロール」を参照してください。

リードレプリカ

読み取り専用に使用されるデータベースのコピー。クエリをリードレプリカにルーティングして、プライマリデータベースへの負荷を軽減できます。

再構築

「7 Rs」を参照してください。

目標復旧時点 (RPO)

最後のデータリカバリポイントからの最大許容時間です。これにより、最後の回復時点からサービスが中断されるまでの間に許容できるデータ損失の程度が決まります。

目標復旧時間 (RTO)

サービスの中断から復旧までの最大許容遅延時間。

リファクタリング

「7 R」を参照してください。

リージョン

地理的エリア内の AWS リソースのコレクション。各 AWS リージョン は、耐障害性、安定性、耐障害性を提供するために、他の から分離され、独立しています。詳細については、AWS リージョン 「 を使用できるアカウントを指定する」を参照してください。

回帰

数値を予測する機械学習手法。例えば、「この家はどれくらいの値段で売れるでしょうか?」という問題を解決するために、機械学習モデルは、線形回帰モデルを使用して、この家に関する既知の事実 (平方フィートなど) に基づいて家の販売価格を予測できます。

リホスト

「7 R」を参照してください。

リリース

デプロイプロセスで、変更を本番環境に昇格させること。

再配置

「7 R」を参照してください。

プラットフォーム変更

「7 R」を参照してください。

再購入

「7 R」を参照してください。

回復性

中断に耐えたり、中断から回復したりするアプリケーションの機能。で障害耐性を計画する場合、高可用性とディザスタリカバリが一般的な考慮事項です AWS クラウド。詳細については、AWS クラウド 「レジリエンス」を参照してください。

リソースベースのポリシー

Amazon S3 バケット、エンドポイント、暗号化キーなどのリソースにアタッチされたポリシー。このタイプのポリシーは、アクセスが許可されているプリンシパル、サポートされているアクション、その他の満たすべき条件を指定します。

責任、説明責任、相談、情報 (RACI) マトリックス

移行活動とクラウド運用に関わるすべての関係者の役割と責任を定義したマトリックス。マトリックスの名前は、マトリックスで定義されている責任の種類、すなわち責任 (R) 、説明責任 (A) 、協議 (C) 、情報提供 (I) に由来します。サポート (S) タイプはオプションです。サポートを含めると、行列はRASCI行列 と呼ばれ、除外すると行RACI列 と呼ばれます。

レスポンシブコントロール

有害事象やセキュリティベースラインからの逸脱について、修復を促すように設計されたセキュリティコントロール。詳細については、Implementing security controls on AWSのResponsive controlsを参照してください。

保持

「7 Rs」を参照してください。

廃止

「7 Rs」を参照してください。

ローテーション

攻撃者が認証情報にアクセスすることをより困難にするために、シークレットを定期的に更新するプロセス。

行と列のアクセスコントロール (RCAC)

アクセスルールが定義されている基本的で柔軟なSQL式の使用。RCAC は、行のアクセス許可と列マスクで構成されます。

RPO

「目標復旧時点」を参照してください。

RTO

「目標復旧時間」を参照してください。

ランブック

特定のタスクを実行するために必要な手動または自動化された一連の手順。これらは通常、エラー率の高い反復操作や手順を合理化するために構築されています。

S

SAML 2.0

多くの ID プロバイダー (IdPs) が使用するオープンスタンダード。この機能により、フェデレーティッドシングルサインオン (SSO) が有効になるため、ユーザーは AWS Management Console にログインしたり、 AWS API組織内のすべてのユーザーIAMに対して でユーザーを作成したりすることなく、 オペレーションを呼び出すことができます。2SAML.0 ベースのフェデレーション

の詳細については、 IAMドキュメントSAMLの「2.0 ベースのフェデレーションについて」を参照してください。

SCADA

「監視コントロールとデータ収集」を参照してください。

SCP

「サービスコントロールポリシー」を参照してください。

シークレット

では AWS Secrets Manager、暗号化された形式で保存されるパスワードやユーザー認証情報などの機密情報または制限付き情報。シークレット値とそのメタデータで構成されます。シークレット値は、バイナリ、単一の文字列、または複数の文字列にすることができます。詳細については、Secrets Manager ドキュメントの「Secrets Manager シークレットの内容」を参照してください。

セキュリティコントロール

脅威アクターによるセキュリティ脆弱性の悪用を防止、検出、軽減するための、技術上または管理上のガードレール。セキュリティコントロールには、予防的 、検出的 、???応答的 、プロアクティブ の 4 つの主なタイプがあります。

セキュリティ強化

アタックサーフェスを狭めて攻撃への耐性を高めるプロセス。このプロセスには、不要になったリソースの削除、最小特権を付与するセキュリティのベストプラクティスの実装、設定ファイル内の不要な機能の無効化、といったアクションが含まれています。

セキュリティ情報とイベント管理 (SIEM) システム

セキュリティ情報管理 (SIM) システムとセキュリティイベント管理 (SEM) システムを組み合わせたツールとサービス。SIEM システムは、サーバー、ネットワーク、デバイス、その他のソースからデータを収集、監視、分析して、脅威やセキュリティ違反を検出し、アラートを生成します。

セキュリティレスポンスの自動化

セキュリティイベントに自動的に応答または修正するように設計された、事前定義されたプログラムされたアクション。これらの自動化は、セキュリティのベストプラクティスを実装するのに役立つ検出的または応答的な AWS セキュリティコントロールとして機能します。自動レスポンスアクションの例としては、VPCセキュリティグループの変更、Amazon EC2インスタンスへのパッチ適用、認証情報のローテーションなどがあります。

サーバー側の暗号化

送信先にあるデータの、それを受け取る AWS のサービス による暗号化。

サービスコントロールポリシー (SCP)

AWS Organizationsの組織内の、すべてのアカウントのアクセス許可を一元的に管理するポリシー。SCPs ガードレールを定義するか、管理者がユーザーまたはロールに委任できるアクションの制限を設定します。を許可リストまたは拒否リストSCPsとして使用して、許可または禁止されるサービスまたはアクションを指定できます。詳細については、 AWS Organizations ドキュメントの「サービスコントロールポリシー」を参照してください。

サービスエンドポイント

URL のエントリポイントの AWS のサービス。ターゲットサービスにプログラムで接続するには、エンドポイントを使用します。詳細については、AWS 全般のリファレンスの「AWS のサービス エンドポイント」を参照してください。

サービスレベルアグリーメント (SLA)

サービスのアップタイムやパフォーマンスなど、IT チームがお客様に提供すると約束したものを明示した合意書。

サービスレベルインジケータ (SLI)

エラー率、可用性、スループットなど、サービスのパフォーマンス側面の測定。

サービスレベルの目標 (SLO)

サービスレベルのインジケータ によって測定される、サービスの状態を表すターゲットメトリクス。

責任共有モデル

クラウドのセキュリティとコンプライアンス AWS について と共有する責任を説明するモデル。AWS はクラウドのセキュリティを担当しますが、お客様はクラウドのセキュリティを担当します。詳細については、責任共有モデルを参照してください。

SIEM

「セキュリティ情報とイベント管理システム」を参照してください。

単一障害点 (SPOF)

システムを中断させる可能性のあるアプリケーションの単一の重要なコンポーネントの障害。

SLA

「サービスレベルアグリーメント」を参照してください。

SLI

「サービスレベルインジケータ」を参照してください。

SLO

「サービスレベルの目標」を参照してください。

split-and-seed モデル

モダナイゼーションプロジェクトのスケーリングと加速のためのパターン。新機能と製品リリースが定義されると、コアチームは解放されて新しい製品チームを作成します。これにより、お客様の組織の能力とサービスの拡張、デベロッパーの生産性の向上、迅速なイノベーションのサポートに役立ちます。詳細については、「」の「アプリケーションをモダナイズするための段階的アプローチ AWS クラウド」を参照してください。

SPOF

単一障害点 を参照してください。

star スキーマ

トランザクションデータまたは測定データを保存するために 1 つの大きなファクトテーブルを使用し、データ属性を保存するために 1 つ以上の小さなディメンションテーブルを使用するデータベースの組織構造。この構造は、データウェアハウスまたはビジネスインテリジェンスの目的で使用するように設計されています。

strangler fig パターン

レガシーシステムが廃止されるまで、システム機能を段階的に書き換えて置き換えることにより、モノリシックシステムをモダナイズするアプローチ。このパターンは、宿主の樹木から根を成長させ、最終的にその宿主を包み込み、宿主に取って代わるイチジクのつるを例えています。そのパターンは、モノリシックシステムを書き換えるときのリスクを管理する方法として Martin Fowler により提唱されました。このパターンを適用する方法の例については、「従来の Microsoft のモダナイズ」を参照してくださいASP。NET (ASMX) ウェブサービスは、コンテナと Amazon API Gateway を使用して段階的に行います。

サブネット

内の IP アドレスの範囲VPC。サブネットは、1 つのアベイラビリティーゾーンに存在する必要があります。

監視コントロールとデータ収集 (SCADA)

製造では、ハードウェアとソフトウェアを使用して物理アセットと生産オペレーションをモニタリングするシステム。

対称暗号化

データの暗号化と復号に同じキーを使用する暗号化のアルゴリズム。

合成テスト

ユーザーインタラクションをシミュレートして潜在的な問題を検出したり、パフォーマンスをモニタリングしたりする方法でシステムをテストします。Amazon CloudWatch Synthetics を使用してこれらのテストを作成できます。

T

タグ

AWS リソースを整理するためのメタデータとして機能するキーと値のペア。タグは、リソースの管理、識別、整理、検索、フィルタリングに役立ちます。詳細については、「AWS リソースのタグ付け」を参照してください。

ターゲット変数

監督された機械学習でお客様が予測しようとしている値。これは、結果変数 のことも指します。例えば、製造設定では、ターゲット変数が製品の欠陥である可能性があります。

タスクリスト

ランブックの進行状況を追跡するために使用されるツール。タスクリストには、ランブックの概要と完了する必要のある一般的なタスクのリストが含まれています。各一般的なタスクには、推定所要時間、所有者、進捗状況が含まれています。

テスト環境

「環境」を参照してください。

トレーニング

お客様の機械学習モデルに学習するデータを提供すること。トレーニングデータには正しい答えが含まれている必要があります。学習アルゴリズムは入力データ属性をターゲット (お客様が予測したい答え) にマッピングするトレーニングデータのパターンを検出します。これらのパター

ンをキャプチャする機械学習モデルを出力します。そして、お客様が機械学習モデルを使用して、ターゲットがわからない新しいデータでターゲットを予測できます。

トランジットゲートウェイ

VPCs とオンプレミスのネットワークを相互接続するために使用できるネットワークトランジットハブ。詳細については、 AWS Transit Gateway ドキュメントの「トランジットゲートウェイとは」を参照してください。

トランクベースのワークフロー

デベロッパーが機能ブランチで機能をローカルにビルドしてテストし、その変更をメインブランチにマージするアプローチ。メインブランチはその後、開発環境、本番前環境、本番環境に合わせて順次構築されます。

信頼されたアクセス

ユーザーに代わって AWS Organizations およびそのアカウントで組織内でタスクを実行するために指定するサービスへのアクセス許可を付与します。信頼されたサービスは、サービスにリンクされたロールを必要なときに各アカウントに作成し、ユーザーに代わって管理タスクを実行します。詳細については、 ドキュメントの「 AWS Organizations を他の AWS のサービスで使用する AWS Organizations 」を参照してください。

チューニング

機械学習モデルの精度を向上させるために、お客様のトレーニングプロセスの側面を変更する。例えば、お客様が機械学習モデルをトレーニングするには、ラベル付けセットを生成し、ラベルを追加します。これらのステップを、異なる設定で複数回繰り返して、モデルを最適化します。

ツーピザチーム

2 つのピザを食べることができる小さな DevOps チーム。ツーピザチームの規模では、ソフトウェア開発におけるコラボレーションに最適な機会が確保されます。

U

不確実性

予測機械学習モデルの信頼性を損なう可能性がある、不正確、不完全、または未知の情報を指す概念。不確実性には、次の 2 つのタイプがあります。認識論的不確実性は、限られた、不完全なデータによって引き起こされ、弁論的不確実性 は、データに固有のノイズとランダム性によって引き起こされます。詳細については、深層学習システムにおける不確実性の定量化 ガイドを参照してください。

未分化なタスク

ヘビーリフティングとも呼ばれ、アプリケーションの作成と運用には必要だが、エンドユーザーに直接的な価値をもたらさなかったり、競争上の優位性をもたらしたりしない作業です。未分化なタスクの例としては、調達、メンテナンス、キャパシティプランニングなどがあります。

上位環境

「環境」を参照してください。

V

バキューミング

ストレージを再利用してパフォーマンスを向上させるために、増分更新後にクリーンアップを行うデータベースのメンテナンス操作。

バージョンコントロール

リポジトリ内のソースコードへの変更など、変更を追跡するプロセスとツール。

VPC ピアリング

プライベート IP アドレスを使用してトラフィックをルーティングVPCsできる 2 つの間の接続。詳細については、Amazon VPCドキュメントのVPC「ピアリングとは」を参照してください。

脆弱性

システムのセキュリティを脅かすソフトウェアまたはハードウェアの欠陥。

W

ウォームキャッシュ

頻繁にアクセスされる最新の関連データを含むバッファキャッシュ。データベースインスタンスはバッファキャッシュから、メインメモリまたはディスクからよりも短い時間で読み取りを行うことができます。

ウォームデータ

アクセス頻度の低いデータ。この種類のデータをクエリする場合、通常は適度に遅いクエリでも問題ありません。

ウィンドウ関数

現在のレコードに関連する行のグループに対して計算を実行するSQL関数。ウィンドウ関数は、移動平均の計算や、現在の行の相対位置に基づく行の値へのアクセスなどのタスクを処理するのに役立ちます。

ワークロード

ビジネス価値をもたらすリソースとコード (顧客向けアプリケーションやバックエンドプロセスなど) の総称。

ワークストリーム

特定のタスクセットを担当する移行プロジェクト内の機能グループ。各ワークストリームは独立していますが、プロジェクト内の他のワークストリームをサポートしています。たとえば、ポートフォリオワークストリームは、アプリケーションの優先順位付け、ウェーブ計画、および移行メタデータの収集を担当します。ポートフォリオワークストリームは、これらの設備を移行ワークストリームで実現し、サーバーとアプリケーションを移行します。

WORM

「書き込み 1 回」を参照し、多くの を読み取ります。

WQF

AWS 「ワークロード認定フレームワーク」を参照してください。

書き込み 1 回、読み取り数 (WORM)

データを 1 回書き込み、データの削除や変更を防ぐストレージモデル。承認されたユーザーは、必要な回数だけデータを読み取ることができますが、変更することはできません。このデータストレージインフラストラクチャはイミュータブルな と見なされます。

Z

ゼロデイエクスプロイト

ゼロデイ脆弱性 を利用する攻撃、通常はマルウェア。

ゼロデイ脆弱性

実稼働システムにおける未解決の欠陥または脆弱性。脅威アクターは、このような脆弱性を利用してシステムを攻撃する可能性があります。開発者は、よく攻撃の結果で脆弱性に気付きます。

ゾンビアプリケーション

平均使用量CPUとメモリ使用量が 5% 未満のアプリケーション。移行プロジェクトでは、これらのアプリケーションを廃止するのが一般的です。

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。