AWS Key Management Service ベストプラクティス

AWS 規範ガイダンス

AWS 規範ガイダンス: AWS Key Management Service ベストプラクティス

Table of Contents

AWS Key Management Service ベストプラクティス

アマゾン ウェブ サービス (寄稿者)

2025 年 3 月 (ドキュメント履歴)

AWS Key Management Service (AWS KMS) は、ユーザーのデータ保護に使用する暗号化キーの作成と制御を容易にするマネージドサービスです。このガイドでは、 を効果的に使用する方法について説明 AWS KMS し、ベストプラクティスを提供します。設定オプションを比較し、ニーズに最適なセットを選択するのに役立ちます。

このガイドには、組織が AWS KMS を使用して機密情報を保護し、複数のユースケースの署名を実装する方法に関する推奨事項が含まれています。以下のディメンションを使用する現在の推奨事項を考慮します。

- キーの管理 – 管理とキーストレージの選択のための委任オプション
- データ保護 – 独自のアプリケーション内でのデータの暗号化と、ユーザーに代わって AWS のサービス 行うデータの暗号化
- アクセス管理 – AWS KMS キーポリシーと AWS Identity and Access Management (IAM) ポリシーを使用して、ロールベースのアクセスコントロール (RBAC) または属性ベースのアクセスコントロール (ABAC) を実装します。
- マルチアカウントおよびマルチリージョンアーキテクチャ — 大規模なデプロイに関する推奨事項。
- 請求とコスト管理 — コストと使用状況、およびコストを削減する方法に関する推奨事項を理解します。
- 検出コントロール – KMS キー、暗号化設定、および暗号化されたデータのステータスをモニタリングします。
- インシデント対応 – データ保護ポリシーに準拠していない原因となる設定ミスを修正します。

ターゲットを絞ったビジネス成果

データはビジネスにとって重要で機密性の高いアセットです。では AWS KMS、データの保護と検証に使用される暗号化キーを管理します。データの使用方法、データにアクセスできるユーザー、暗号化の方法を制御します。このガイドは、開発者、システム管理者、およびセキュリティプロフェッショナルが、保存または送信される機密データを保護するのに役立つ暗号化のベストプラクティスを実装するのに役立つことを目的としています AWS のサービス。このガイドの推奨事項を理解して実

装することで、 AWS 環境全体でデータの機密性と整合性を高めることができます。データ保護要件は、要件が内部で策定されているか、コンプライアンスまたは検証プログラムに固有の要件があるかにかかわらず、満たすことができます。 AWS KMS が AWS 環境内のデータを保護する方法の詳細については、 AWS KMS ドキュメントの「 での AWS KMS 暗号化 AWS のサービスの使用」を参照してください。

について AWS KMS keys

AWS Key Management Service （ AWS KMS) では、サービスに渡すデータで使用できる暗号化キーを作成できます。プライマリリソースタイプは KMS キーで、そのうちの 3 つのタイプがあります。

- Advanced Encryption Standard (AES) 対称キー – AES の Galois Counter Mode (GCM) モードで使用される 256 ビットキーです。これらのキーは、サイズが 4 KB 未満のデータの認証された暗号化と復号を提供します。これは最も一般的なタイプのキーです。これは、アプリケーションで使用されるデータキーや、ユーザーに代わってデータを暗号化 AWS のサービス する によって使用されるデータキーなど、他のデータキーを保護するために使用されます。
- RSA または楕円曲線非対称キー — これらのキーはさまざまなサイズで利用可能で、多くのアルゴリズムをサポートしています。アルゴリズムに応じて、暗号化と復号、および署名と検証オペレーションに使用できます。
- ハッシュベースのメッセージ認証コード (HMAC) オペレーションを実行するための対称キー – これらのキーは、署名および検証オペレーションに使用される 256 ビットキーです。

KMS キーは、サービスからプレーンテキストでエクスポートすることはできません。これらはサービスに使用されるハードウェアセキュリティモジュール (HSM) により生成され、そのモジュール内でのみ使用できます。これは、キーの侵害 AWS KMS を防ぐための の基本的なセキュリティプロパティです。中国 (北京) および中国 (寧夏) リージョンでは、これらの HSMsは OSCCA によって認定されています。他のすべてのリージョンでは、 で使用される HSMs AWS KMS は、セキュリティレベル 3 の NIST 内の FIPS 140 プログラムで検証されます。キーの保護 AWS KMS に役立つ の設計とコントロールの詳細については、AWS Key Management Service 「暗号化の詳細」を参照してください。

KMS キーを使用して暗号化、復号、署名、または検証オペレーションを実行するために、さまざまな暗号化 APIs AWS KMS を使用してデータを に送信できます。また、KMS キーをキー暗号化キーのように動作させて、データキーと呼ばれるキータイプを保護することもできます。データキーは、ローカルアプリケーション内で使用する AWS KMS ため、またはユーザーに代わってデータを保護する AWS のサービス からエクスポートできます。データキーの使用は、すべてのキー管理システムで一般的であり、多くの場合、エンベロープ暗号化と呼ばれます。エンベロープ暗号化を使用すると、KMS キーで直接暗号化 AWS KMS するために機密データを に送信しなくても、機密データを処理するリモートシステムでデータキーを使用できます。

詳細については、 AWS KMS ドキュメントのAWS KMS keys「」およびAWS KMS 「暗号化の必須事項」を参照してください。

の主要な管理のベストプラクティス AWS KMS

AWS Key Management Service (AWS KMS) を使用する場合は、いくつかの基本的な設計上の決定を行う必要があります。これには、キーの管理とアクセスに一元化モデルを使用するか、分散モデルを使用するか、使用するキーのタイプ、使用するキーストアのタイプが含まれます。以下のセクションは、組織やユースケースに適した意思決定を行うのに役立ちます。このセクションでは、データとキーを保護するために実行する必要があるアクションを含め、KMS キーを無効化および削除するための重要な考慮事項をまとめます。

このセクションは、以下のトピックで構成されます。

- 集中型モデルまたは分散型モデルの選択
- カスタマーマネージドキー、 AWS マネージドキー、または AWS 所有キーの選択
- AWS KMS キーストアの選択
- KMS キーの削除と無効化

集中型モデルまたは分散型モデルの選択

AWS では、複数の を使用し AWS アカウント 、それらのアカウントを の 1 つの組織として管理することをお勧めしますAWS Organizations。 AWS KMS keys マルチアカウント環境で を管理するには、2 つの広範なアプローチがあります。

最初のアプローチは、分散型アプローチです。このアプローチでは、これらのキーを使用する各アカウントにキーを作成します。KMS キーを保護対象のリソースと同じアカウントに保存すると、AWS プリンシパルとキーのアクセス要件を理解しているローカル管理者にアクセス許可を委任しやすくなります。キーポリシーのみを使用してキーの使用を承認するか、 AWS Identity and Access Management (IAM) でキーポリシーとアイデンティティベースのポリシーを組み合わせることができます。

2 番目のアプローチは、1 つまたは少数の指定された KMS キーを維持する一元化されたアプローチです AWS アカウント。暗号化オペレーションにのみキーを使用することを他の アカウントに許可します。キー、そのライフサイクル、およびアクセス許可は、一元化されたアカウントから管理します。他の AWS アカウント にキーの使用を許可しますが、他のアクセス許可は許可しません。外部アカウントは、キーのライフサイクルまたはアクセス許可について何も管理できません。この一元化されたモデルは、委任された管理者またはユーザーによるキーの意図しない削除や特権のエスカレーションのリスクを最小限に抑えるのに役立ちます。

選択するオプションは、いくつかの要因によって異なります。アプローチを選択するときは、次の点を考慮してください。

1. キーとリソースへのアクセスをプロビジョニングする自動プロセスまたは手動プロセスはありますか? これには、デプロイパイプラインやInfrastructure as Code (IaC) テンプレートなどのリソースが含まれます。これらのツールは、多くの にリソース (KMS キー、キーポリシー、IAM ロール、IAM ポリシーなど) をデプロイして管理するのに役立ちます AWS アカウント。これらのデプロイツールがない場合は、キー管理への一元化されたアプローチがビジネスにとってより管理しやすい場合があります。
2. KMS キーを使用するリソース AWS アカウント を含むすべての を管理することができますか? その場合、一元化されたモデルによって管理が簡素化され、キーを管理する AWS アカウント ための切り替えが不要になります。ただし、キーを使用するための IAM ロールとユーザーアクセス許可は、引き続きアカウントごとに管理する必要があります。
3. 独自の AWS アカウント および リソースを持つ顧客またはパートナーに KMS キーを使用するためのアクセスを提供する必要がありますか? これらのキーの場合、一元化されたアプローチにより、顧客やパートナーの管理上の負担を軽減できます。
4. 一元化されたアクセスアプローチまたはローカルアクセスアプローチのいずれかでより適切に解決された AWS リソースへのアクセスに対する認可要件はありますか? 例えば、異なるアプリケーションやビジネスユニットが独自のデータのセキュリティを管理する場合は、キー管理への分散アプローチの方が適しています。
5. のサービスリソースクォータを超えていますか AWS KMS? これらのクォータは ごとに設定されるため AWS アカウント、分散モデルはアカウント間で負荷を分散し、サービスクォータを効果的に乗算します。

> **Note**
>
> リクエストクォータを考慮する場合、キーの管理モデルは関係ありません。これらのクォータは、キーを所有または管理するアカウントではなく、キーに対してリクエストを行うアカウントプリンシパルに適用されるためです。

一般に、一元化された KMS キーモデルの必要性を明確にしない限り、分散アプローチから始めることをお勧めします。

カスタマーマネージドキー、 AWS マネージドキー、または AWS 所有キーの選択

独自の暗号化アプリケーションで使用するために作成および管理する KMS キーは、カスタマーマネージドキーと呼ばれます。 AWS のサービス は、カスタマーマネージドキーを使用して、サービスがユーザーに代わって保存するデータを暗号化できます。ライフサイクルとキーの使用を完全に制御する場合は、カスタマーマネージドキーをお勧めします。アカウント内でカスタマーマネージドキーを使用する場合、月額料金が発生します。さらに、キーを使用または管理するリクエストには、使用コストが発生します。詳細については、「AWS KMS 料金表」を参照してください。

AWS のサービス でデータを暗号化したいが、キー管理のオーバーヘッドやコストは不要な場合は、AWS マネージドキーを使用できます。このタイプのキーはアカウントに存在しますが、特定の状況でのみ使用できます。これは、運用 AWS のサービス している のコンテキストでのみ使用でき、キーを含むアカウント内のプリンシパルのみが使用できます。これらのキーのライフサイクルやアクセス許可については、何も管理できません。一部の は AWS マネージドキー AWS のサービス を使用します。 AWS マネージドキーエイリアスの形式は ですaws/<service code>。たとえば、aws/ebsキーは、キーと同じアカウントの Amazon Elastic Block Store (Amazon EBS) ボリュームの暗号化にのみ使用でき、そのアカウントの IAM プリンシパルのみが使用できます。 AWS マネージドキーは、そのアカウントのユーザーとそのアカウントのリソースに対してのみ使用できます。AWS マネージドキーで暗号化されたリソースを他のアカウントと共有することはできません。これがユースケースの制限である場合は、代わりに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。そのキーの使用を他のアカウントと共有できます。アカウントに AWS マネージドキーが存在する場合は課金されませんが、このキータイプの使用は、キー AWS のサービス に割り当てられたによって課金されます。

AWS マネージドキーは、2021 年 AWS のサービス の時点で新しい 用に作成されなくなったレガシーキータイプです。代わりに、新しい (およびレガシー) AWS のサービス は AWS 所有キーを使用してデフォルトでデータを暗号化します。 AWS 所有キーは、 が複数の で使用するために AWS のサービス 所有および管理する KMS キーのコレクションです AWS アカウント。これらのキーは にはありませんが AWS アカウント、 AWS のサービス はアカウント内のリソースを保護するためにキーを使用できます。

きめ細かな制御が最も重要な場合はカスタマーマネージドキーを使用し、利便性が最も重要な場合は AWS 所有キーを使用することをお勧めします。

次の表に、各キータイプのキーポリシー、ログ記録、管理、および料金の違いを示します。キータイプの詳細については、「 のAWS KMS 概念」を参照してください。

考慮事項	カスタマーマネージドキー	AWS マネージドキー	AWS 所有キー
キーポリシー	カスタマーが排他的に制御する	サービスによって制御され、カスタマーは閲覧可能	排他的に制御され、データを暗号化 AWS のサービス する でのみ表示可能
ログ記録	AWS CloudTrail カスタマー証跡またはイベントデータストア	CloudTrail カスタマー証跡またはイベントデータストア	カスタマーは閲覧できない
ライフサイクル管理	お客様がローテーション、削除、および AWS リージョン	AWS のサービス がローテーション (年単位) 、削除、リージョンを管理する	AWS のサービス がローテーション (年単位) 、削除、リージョンを管理する
料金	キー存在に対する月額料金 (時間単位で按分) 。呼び出し元には API の使用料金が請求されます。	キーの存在には料金はかかりません。呼び出し元には API の使用料金がかかります。	カスタマーへの請求はなし

AWS KMS キーストアの選択

キーストアは、暗号化キーマテリアルを保存して使用するための安全な場所です。キーストアの業界のベストプラクティスは、セキュリティレベル 3 の NIST Federal Information Processing Standards (FIPS) 140 暗号化モジュール検証プログラムで検証されたハードウェアセキュリティモジュール (HSM) と呼ばれるデバイスを使用することです。支払いの処理に使用されるキーストアをサポートする他のプログラムもあります。 AWS Payment Cryptographyは、支払いワークロードに関連するデータを保護するために使用できるサービスです。

AWS KMS は、 AWS KMS を使用して暗号化キーを作成および管理するときにキーマテリアルを保護するのに役立つ複数のキーストアタイプをサポートしています。が提供するすべてのキーストアオプション AWS KMS は、セキュリティレベル 3 の FIPS 140 で継続的に検証されます。 AWS 演算子を含むすべてのユーザーが、プレーンテキストキーにアクセスしたり、アクセス許可なしで使用した

りできないように設計されています。使用可能なキーストアのタイプの詳細については、 AWS KMS ドキュメントの「キーストア」を参照してください。

AWS KMS 標準キーストアは、ほとんどのワークロードに最適な選択肢です。別のタイプのキーストアを選択する必要がある場合は、規制やその他の要件 (内部など) でこの選択を必須としているかどうかを慎重に検討し、コストと利点を慎重に検討してください。

KMS キーの削除と無効化

KMS キーを削除すると、大きな影響を与える可能性があります。今後使用しない KMS キーを削除する前に、キーの状態を無効に設定するのが適切かどうかを検討してください。キーが無効になっている間は、暗号化オペレーションには使用できません。まだ に存在し AWS、必要に応じて後で再有効化できます。無効になっているキーには、引き続きストレージ料金が発生します。キーがデータやデータキーを保護しないと確信できるまでは、キーを削除するのではなく、キーを無効にすることをお勧めします。

> **Important**
>
> キーの削除は慎重に計画する必要があります。対応するキーが削除された場合、データは復号できません。 AWS には、削除されたキーが削除された後に復元する手段はありません。の他の重要なオペレーションと同様に AWS、キーの削除をスケジュールし、キーの削除に多要素認証 (MFA) を必要とするユーザーを制限するポリシーを適用する必要があります。

キーの偶発的な削除を防ぐため、 は、キーを削除する前に、`DeleteKey`呼び出しの実行から 7 日間のデフォルトの最小待機期間 AWS KMS を適用します。待機期間は、最大値の 30 日に設定できます。待機期間中、キーは削除保留中の状態で AWS KMS に保存されます。暗号化または復号オペレーションには使用できません。暗号化または復号のために削除保留中状態のキーを使用しようとすると、 にログ記録されます AWS CloudTrail。これらのイベントの Amazon CloudWatch アラームは、CloudTrail ログで設定できます。 CloudTrail これらのイベントでアラームを受け取った場合は、必要に応じて削除プロセスをキャンセルすることを選択できます。待機期間が終了するまで、削除保留中の状態からキーを復元し、無効または有効状態に復元できます。

マルチリージョンキーを削除するには、元のコピーの前にレプリカを削除する必要があります。詳細については、「マルチリージョンキーの削除」を参照してください。

インポートされたキーマテリアルでキーを使用している場合は、インポートされたキーマテリアルをすぐに削除できます。これは、いくつかの方法で KMS キーを削除する場合とは異なりま

す。DeleteImportedKeyMaterial アクションを実行すると、 はキーマテリアル AWS KMS を削除し、キーの状態はインポート保留中に変わります。キーマテリアルを削除すると、そのキーはすぐに使用できなくなります。待機期間はありません。キーを再度使用できるようにするには、同じキーマテリアルを再度インポートする必要があります。KMS キーの削除の待機期間は、インポートされたキーマテリアルを持つ KMS キーにも適用されます。

データキーが KMS キーによって保護されていて、 によってアクティブに使用されている場合 AWS のサービス、関連する KMS キーが無効になっているか、インポートされたキーマテリアルが削除されても、すぐには影響を受けません。たとえば、インポートされたマテリアルを持つキーを使用して SSE-KMS でオブジェクトを暗号化したとします。オブジェクトを Amazon Simple Storage Service (Amazon S3) バケットにアップロードしています。オブジェクトをバケットにアップロードする前に、マテリアルをキーにインポートします。オブジェクトがアップロードされたら、インポートされたキーマテリアルをそのキーから削除します。オブジェクトは暗号化された状態でバケットに残りますが、削除されたキーマテリアルがキーに再インポートされるまでオブジェクトにアクセスすることはできません。このフローでは、キーからキーマテリアルをインポートおよび削除するための正確な自動化が必要ですが、環境内で追加のレベルの制御を提供することができます。

AWS は、KMS キーのスケジュールされた削除を (必要に応じて) モニタリングおよび修復するのに役立つ規範的なガイダンスを提供します。詳細については、「スケジュールされた AWS KMS キーの削除のモニタリングと修復」を参照してください。

のデータ保護のベストプラクティス AWS KMS

このセクションでは、各データ型に使用するキーなど、データ保護のための AWS Key Management Service (AWS KMS) キーの使用法を選択するのに役立ちます。また、さまざまな AWS KMS で を使用する具体的な例も示します AWS のサービス。これらの推奨事項と例は、必要なキーの数と、それらのキーを使用するためのアクセス許可を必要とするプリンシパルを理解するのに役立ちます。

このセクションでは、キーローテーションについても説明します。キーローテーションは、既存の KMS キーを新しいキーに置き換えるか、既存の KMS キーに関連付けられた暗号化マテリアルを新しいマテリアルに置き換える方法です。このガイドでは、一般的に使用される KMS キーをローテーションする方法の例と手順を示します AWS のサービス。推奨事項と例は、キーローテーション戦略について情報に基づいた選択を行うのに役立つように設計されています。

最後に、このセクションでは、アプリケーションにクライアント側の暗号化を実装するためのツール AWS Encryption SDKである の使用方法に関する推奨事項を示します。このセクションでは、 の機能セットと機能に基づいて実行できる設計上の選択について説明します AWS Encryption SDK。

このセクションでは、以下の暗号化トピックについて説明します。

- による暗号化 AWS KMS
- 影響のキーローテーション AWS KMS と範囲
- の使用に関する推奨事項 AWS Encryption SDK

による暗号化 AWS KMS

暗号化は、機密情報の機密性と完全性を保護するための一般的なベストプラクティスです。既存のデータ分類レベルを使用し、レベルごとに少なくとも 1 つの AWS Key Management Service (AWS KMS) キーが必要です。例えば、機密として分類されるデータには KMS キーを定義し、内部専用には KMS キーを定義し、機密には KMS キーを定義できます。これにより、承認されたユーザーのみが各分類レベルに関連付けられたキーを使用するアクセス許可を持つようになります。

> **Note**
>
> 単一のカスタマーマネージド KMS キーは、特定の分類のデータを保存する AWS のサービス または独自のアプリケーションの任意の組み合わせで使用できます。複数のワークロードでキーを使用する際の制限要因 AWS のサービス は、一連のユーザー間でデータへのアクセスを制御するために、使用許可をどの程度複雑にする必要があるかです。 AWS KMS キーポリシー JSON ドキュメントは 32 KB 未満である必要があります。このサイズ制限が制限に

なった場合は、AWS KMS 許可を使用するか、複数のキーを作成してキーポリシードキュメントのサイズを最小限に抑えることを検討してください。

KMS キーを分割するためにデータ分類のみに依存する代わりに、単一の 内のデータ分類に使用する KMS キーを割り当てることもできます AWS のサービス。例えば、Amazon Simple Storage Service (Amazon S3) Sensitiveでタグ付けされたすべてのデータは、 のような名前の KMS キーで暗号化する必要がありますS3-Sensitive。さらに、定義されたデータ分類 AWS のサービス やアプリケーション内の複数の KMS キーにデータを分散できます。たとえば、特定の期間の一部のデータセットを削除したり、別の期間の他のデータセットを削除したりできます。リソースタグを使用すると、特定の KMS キーで暗号化されたデータを識別してソートできます。

KMS キーの分散管理モデルを選択した場合は、ガードレールを適用して、特定の分類を持つ新しいリソースが作成され、適切なアクセス許可を持つ期待される KMS キーが使用されていることを確認する必要があります。自動化を使用してリソース設定を強制、検出、管理する方法の詳細については、このガイドの検出とモニタリング「」セクションを参照してください。

このセクションでは、以下の暗号化トピックについて説明します。

- による ログデータの暗号化 AWS KMS
- デフォルトでの暗号化
- を使用したデータベース暗号化 AWS KMS
- を使用した PCI DSS データ暗号化 AWS KMS
- Amazon EC2 Auto Scaling での KMS キーの使用

による ログデータの暗号化 AWS KMS

Amazon GuardDuty や AWS のサービスなどの多くの にはAWS CloudTrail、Amazon S3 に送信されるログデータを暗号化するオプションが用意されています。GuardDuty から Amazon S3 に結果を エクスポートする場合は、KMS キーを使用する必要があります。すべてのログデータを暗号化し、セキュリティチーム、インシデント対応者、監査者などの承認されたプリンシパルにのみ復号アクセスを許可することをお勧めします。

AWS セキュリティリファレンスアーキテクチャでは、ログ AWS アカウント 記録用の中央 を作成することをお勧めします。これを行うと、キー管理のオーバーヘッドを減らすこともできます。例えば、CloudTrail を使用すると、組織全体のイベントをログに記録する組織の証跡またはイベントデータストアを作成できます。組織の証跡またはイベントデータストアを設定するときは、指定した

ログ記録アカウントに 1 つの Amazon S3 バケットと KMS キーを指定できます。この設定は、組織内のすべてのメンバーアカウントに適用されます。その後、すべてのアカウントは CloudTrail ログをログ記録アカウントの Amazon S3 バケットに送信し、ログデータは指定された KMS キーで暗号化されます。この KMS キーのキーポリシーを更新して、CloudTrail にキーを使用するために必要なアクセス許可を付与する必要があります。詳細については、CloudTrail ドキュメントのCloudTrail の AWS KMS キーポリシーを設定する」を参照してください。

GuardDuty ログと CloudTrail ログを保護するために、Amazon S3 バケットと KMS キーが同じ にある必要がありますAWS リージョン。 AWS セキュリティリファレンスアーキテクチャは、ログ記録とマルチアカウントアーキテクチャに関するガイダンスも提供します。複数のリージョンとアカウント間でログを集約する場合は、CloudTrail ドキュメントの「組織の証跡の作成」を参照して、オプトインリージョンの詳細を確認し、一元化されたログ記録が設計どおりに機能することを確認します。

デフォルトでの暗号化

AWS のサービス データを保存または処理する は通常、保管時の暗号化を提供します。このセキュリティ機能は、使用されていないデータを暗号化して保護するのに役立ちます。承認されたユーザーは、必要に応じて引き続きアクセスできます。

実装オプションと暗号化オプションは異なりますAWS のサービス。多くはデフォルトで暗号化を提供します。使用する各サービスで暗号化がどのように機能するかを理解することが重要です。次に例をいくつか示します。

- Amazon Elastic Block Store (Amazon EBS) – デフォルトで暗号化を有効にすると、すべての新しい Amazon EBS ボリュームとスナップショットコピーが暗号化されます。 AWS Identity and Access Management (IAM) ロールまたはユーザーは、暗号化されていないボリュームまたは暗号化をサポートしていないボリュームを持つインスタンスを起動できません。この機能は、Amazon EBS ボリュームに保存されているすべてのデータが暗号化されていることを確認することで、セキュリティ、コンプライアンス、監査に役立ちます。このサービスの暗号化の詳細については、Amazon EBS ドキュメントの「Amazon EBS 暗号化」を参照してください。
- Amazon Simple Storage Service (Amazon S3) – すべての新しいオブジェクトはデフォルトで暗号化されます。Amazon S3 は、別の暗号化オプションを指定しない限り、新しいオブジェクトごとに Amazon S3 マネージドキー (SSE-S3) によるサーバー側の暗号化を自動的に適用します。IAM プリンシパルは、API コールで明示的に を指定することで、暗号化されていないオブジェクトを Amazon S3 にアップロードできます。Amazon S3 で SSE-KMS 暗号化を適用するには、暗号化が必要な条件でバケットポリシーを使用する必要があります。サンプルポリシーについては、Amazon S3 ドキュメントの「バケットに書き込まれたすべてのオブジェクトに SSE-KMS を要求する」を参照してください。 Amazon S3 一部の Amazon S3 バケットは、多数のオブジェク

トを受信して処理します。これらのオブジェクトが KMS キーで暗号化されている場合、Amazon S3 オペレーションの数が多いと、 `GenerateDataKey`および `Decrypt`呼び出しの数が多くなります AWS KMS。これにより、 AWS KMS の使用に対して発生する料金が増加する可能性があります。Amazon S3 バケットキーを設定できるため、 AWS KMS コストを大幅に削減できます。このサービスの暗号化の詳細については、Amazon S3 ドキュメントの「暗号化によるデータの保護」を参照してください。

- Amazon DynamoDB – DynamoDB は、保管中のサーバー側の暗号化をデフォルトで有効にするフルマネージド NoSQL データベースサービスであり、無効にすることはできません。DynamoDB テーブルの暗号化には、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。このアプローチは、 AWS KMS キーポリシーで特定の IAM ユーザーとロールをターゲットにすることで、きめ細かなアクセス許可と職務の分離による最小特権を実装するのに役立ちます。DynamoDB テーブルの暗号化設定を構成するときに、 AWS マネージドキーまたは AWS 所有キーを選択することもできます。高度な保護を必要とするデータ (データがクライアントにクリアテキストとしてのみ表示される) については、 AWS Database Encryption SDK でクライアント側の暗号化を使用することを検討してください。このサービスの暗号化の詳細については、DynamoDB ドキュメントの「データ保護」を参照してください。

を使用したデータベース暗号化 AWS KMS

暗号化を実装するレベルは、データベースの機能に影響します。以下は、考慮すべきトレードオフです。

- AWS KMS 暗号化のみを使用する場合、テーブルをバックアップするストレージは DynamoDB および Amazon Relational Database Service (Amazon RDS) 用に暗号化されます。 DynamoDB Amazon Relational Database Service つまり、データベースを実行するオペレーティングシステムは、ストレージの内容をクリアテキストとして認識します。インデックス生成やクリアテキストデータへのアクセスを必要とする他の高次関数を含むすべてのデータベース関数は、引き続き期待どおりに動作します。
- Amazon RDS は、 Amazon Elastic Block Store (Amazon EBS) 暗号化 に基づいて構築され、データベースボリュームの完全なディスク暗号化を提供します。Amazon RDS で暗号化されたデータベースインスタンスを作成すると、Amazon RDS はユーザーに代わって暗号化された Amazon EBS ボリュームを作成し、データベースを保存します。ボリューム、データベーススナップショット、自動バックアップ、リードレプリカに保存されているデータはすべて、データベースインスタンスの作成時に指定した KMS キーで暗号化されます。
- Amazon Redshift は と統合 AWS KMS し、データレベルを通じてクラスターレベルを暗号化するために使用される 4 階層のキー階層を作成します。クラスターを起動するときに、AWS KMS

暗号化の使用を選択できます。適切なアクセス許可を持つ Amazon Redshift アプリケーションとユーザーのみが、テーブルがメモリで開かれたとき (および復号されたとき) にクリアテキストを表示できます。これは、一部の商用データベースで利用できる透過的またはテーブルベースのデータ暗号化 (TDE) 機能と広く似ています。つまり、インデックス生成やクリアテキストデータへのアクセスを必要とする他の上位関数を含むすべてのデータベース関数は、期待どおりに動作し続けます。

- AWS Database Encryption SDK (および同様のツール) を介して実装されるクライアント側のデータレベルの暗号化は、オペレーティングシステムとデータベースの両方が暗号文のみを表示することを意味します。ユーザーは、 AWS Database Encryption SDK がインストールされたクライアントからデータベースにアクセスし、関連するキーにアクセスできる場合にのみ、クリアテキストを表示できます。インデックス生成など、意図したとおりに機能するためにクリアテキストへのアクセスを必要とする高次データベース関数は、暗号化されたフィールドで動作するように指示された場合は機能しません。クライアント側の暗号化を使用する場合は、暗号化されたデータに対する一般的な攻撃を防ぐのに役立つ堅牢な暗号化メカニズムを使用してください。これには、強力な暗号化アルゴリズムと、暗号文攻撃の軽減に役立つソルトなどの適切な手法の使用が含まれます。

AWS データベースサービスには、 AWS KMS 統合された暗号化機能を使用することをお勧めします。機密データを処理するワークロードでは、機密データフィールドに対してクライアント側の暗号化を検討する必要があります。クライアント側の暗号化を使用する場合は、SQL クエリ内の結合やインデックスの作成など、データベースアクセスへの影響を考慮する必要があります。

を使用した PCI DSS データ暗号化 AWS KMS

のセキュリティと品質管理 AWS KMS は、Payment Card Industry Data Security Standard (PCI DSS) の要件を満たすために検証され、認定されています。つまり、KMS キーを使用してプライマリアカウント番号 (PAN) データを暗号化できます。KMS キーを使用してデータを暗号化すると、暗号化ライブラリを管理する負担の一部が軽減されます。さらに、KMS キーは から エクスポートできないため AWS KMS、安全でない方法で保存される暗号化キーに関する懸念が軽減されます。

PCI DSS 要件を満たす AWS KMS ために使用できる方法は他にもあります。例えば、Amazon S3 AWS KMS で を使用している場合、各サービスのアクセスコントロールメカニズムは他のサービスと異なるため、PAN データを Amazon S3 に保存できます。

常に、コンプライアンス要件を確認するときは、適切な経験、資格、検証済みの関係者からアドバイスを受けてください。PCI DSS の範囲内にあるAWS KMS カードトランザクションデータを保護するためにキーを直接使用するアプリケーションを設計する場合は、リクエストクォータに注意してください。

すべての AWS KMS リクエストがログインするため AWS CloudTrail、CloudTrail ログを確認することでキーの使用状況を監査できます。ただし、Amazon S3 バケットキーを使用する場合、すべての Amazon S3 アクションに対応するエントリはありません。これは、バケットキーが Amazon S3 のオブジェクトの暗号化に使用するデータキーを暗号化するためです。バケットキーを使用しても、へのすべての API コールが排除されるわけではありませんが AWS KMS、バケットキーの数は減ります。その結果、Amazon S3 オブジェクトのアクセス試行と API 呼び出しの間に one-to-one の一致がなくなりました AWS KMS。

Amazon EC2 Auto Scaling での KMS キーの使用

Amazon EC2 Auto Scaling は、Amazon EC2 インスタンスのスケーリングを自動化するために推奨されるサービスです。これにより、アプリケーションの負荷を処理できるインスタンスの数が適切になります。Amazon EC2 Auto Scaling は、サービスに適切なアクセス許可を付与し、アカウント内のアクティビティを承認するサービスにリンクされたロールを使用します。Amazon EC2 Auto Scaling で KMS キーを使用するには、自動化が役立つように`Decrypt`、 AWS KMS キーポリシーでサービスにリンクされたロールが などの一部の API オペレーションで KMS キーを使用することを許可する必要があります。 AWS KMS キーポリシーが、アクションを実行するオペレーションを実行している IAM プリンシパルを許可しない場合、そのアクションは拒否されます。キーポリシーでアクセス許可を正しく適用してアクセスを許可する方法の詳細については、Amazon EC2 Auto Scaling ドキュメントの「Amazon EC2 Auto Scaling でのデータ保護」を参照してください。Amazon EC2 Auto Scaling

影響のキーローテーション AWS KMS と範囲

規制コンプライアンスのためにキーをローテーションする必要がある場合を除き、 AWS Key Management Service (AWS KMS) キーローテーションはお勧めしません。たとえば、ビジネスポリシー、契約ルール、または政府の規制により、KMS キーのローテーションが必要になる場合があります。の設計により、キーローテーションが軽減に通常使用されるリスクのタイプ AWS KMS が大幅に軽減されます。KMS キーをローテーションする必要がある場合は、自動キーローテーションを使用し、自動キーローテーションがサポートされていない場合にのみ手動キーローテーションを使用することをお勧めします。

このセクションでは、以下の主要なローテーショントピックについて説明します。

- AWS KMS 対称キーローテーション
- Amazon EBS ボリュームのキーローテーション
- Amazon RDS のキーローテーション
- Amazon S3 および同一リージョンレプリケーションのキーローテーション

- インポートされたマテリアルを使用した KMS キーの更新

AWS KMS 対称キーローテーション

AWS KMS は、 が AWS KMS 作成するキーマテリアルを持つ対称暗号化 KMS キーに対してのみ、自動キーローテーションをサポートします。カスタマー管理の KMS キーでは、自動ローテーションはオプションです。は、 AWS マネージド KMS キーのキーマテリアルを毎年 AWS KMS ローテーションします。 AWS KMS は、暗号化マテリアルのすべての以前のバージョンを永続的に保存するため、その KMS キーで暗号化されたデータを復号できます。 AWS KMS は、KMS キーを削除するまでローテーションされたキーマテリアルを削除しません。また、 を使用してオブジェクトを復号すると AWS KMS、サービスは復号オペレーションに使用する正しいバッキングマテリアルを決定します。追加の入力パラメータを指定する必要はありません。

は暗号化キーマテリアルの以前のバージョン AWS KMS を保持し、そのマテリアルを使用してデータを復号できるため、キーローテーションは追加のセキュリティ上の利点を提供しません。キーローテーションメカニズムは、規制やその他の要件が要求するコンテキストでワークロードを運用している場合に、キーのローテーションを容易にするために存在します。

Amazon EBS ボリュームのキーローテーション

Amazon Elastic Block Store (Amazon EBS) データキーは、次のいずれかの方法でローテーションできます。このアプローチは、ワークフロー、デプロイ方法、アプリケーションアーキテクチャによって異なります。これは、 AWS マネージドキーからカスタマーマネージドキーに変更するときに実行できます。

オペレーティングシステムツールを使用して、あるボリュームから別のボリュームにデータをコピーするには

1. 新しい KMS キーを作成します。手順については、「KMS キーの作成」を参照してください。
2. 元のボリュームと同じサイズ以上の新しい Amazon EBS ボリュームを作成します。暗号化には、作成した KMS キーを指定します。手順については、「Amazon EBS ボリュームの作成」を参照してください。
3. 新しいボリュームを元のボリュームと同じインスタンスまたはコンテナにマウントします。手順については、「Amazon EC2 インスタンスに Amazon EBS ボリュームをアタッチする」を参照してください。
4. 任意のオペレーティングシステムツールを使用して、既存のボリュームから新しいボリュームにデータをコピーします。

5. 同期が完了したら、事前にスケジュールされたメンテナンスウィンドウ中に、インスタンスへのトラフィックを停止します。手順については、「インスタンスの手動停止と起動」を参照してください。
6. 元のボリュームをアンマウントします。手順については、「Amazon EC2 インスタンスから Amazon EBS ボリュームをデタッチする」を参照してください。
7. 新しいボリュームを元のマウントポイントにマウントします。
8. 新しいボリュームが正しく動作していることを確認します。
9. 元のボリュームを削除します。手順については、「Amazon EBS ボリュームの削除」を参照してください。

Amazon EBS スナップショットを使用して、あるボリュームから別のボリュームにデータをコピーするには

1. 新しい KMS キーを作成します。手順については、「KMS キーの作成」を参照してください。
2. 元のボリュームの Amazon EBS スナップショットを作成します。手順については、「Amazon EBS スナップショットの作成」を参照してください。
3. スナップショットから新しいボリュームを作成します。暗号化には、作成した新しい KMS キーを指定します。手順については、「Amazon EBS ボリュームの作成」を参照してください。

> **Note**
>
> ワークロードによっては、ボリュームの初期レイテンシーを最小限に抑えるために Amazon EBS 高速スナップショット復元を使用することをお勧めします。

4. 新しい Amazon EC2 インスタンスを作成します。手順については、Amazon EC2 インスタンスを起動する」を参照してください。
5. 作成したボリュームを Amazon EC2 インスタンスにアタッチします。手順については、「Amazon EC2 インスタンスに Amazon EBS ボリュームをアタッチする」を参照してください。
6. 新しいインスタンスを本番環境にローテーションします。
7. 元のインスタンスを本番環境からローテーションして削除します。手順については、「Amazon EBS ボリュームの削除」を参照してください。

> **Note**
>
> スナップショットをコピーし、ターゲットコピーに使用される暗号化キーを変更できます。スナップショットをコピーして任意の KMS キーで暗号化したら、スナップショットから Amazon マシンイメージ (AMI) を作成することもできます。詳細については、Amazon EC2 ドキュメントの「Amazon EBS 暗号化」を参照してください。 Amazon EC2

Amazon RDS のキーローテーション

Amazon Relational Database Service (Amazon RDS) などの一部のサービスでは、データ暗号化はサービス内で行われ、 によって提供されます AWS KMS。次の手順を使用して、Amazon RDS データベースインスタンスのキーをローテーションします。

Amazon RDS データベースの KMS キーをローテーションするには

1. 元の暗号化されたデータベースのスナップショットを作成します。手順については、Amazon RDS ドキュメントの「手動バックアップの管理」を参照してください。
2. スナップショットを新しいスナップショットにコピーします。暗号化には、新しい KMS キーを指定します。手順については、「Amazon RDS の DB スナップショットのコピー」を参照してください。
3. 新しいスナップショットを使用して、新しい Amazon RDS クラスターを作成します。手順については、Amazon RDS ドキュメントの「DB インスタンスへの復元」を参照してください。デフォルトでは、クラスターは新しい KMS キーを使用します。
4. 新しいデータベースとその中のデータのオペレーションを確認します。
5. 新しいデータベースを本番環境にローテーションします。
6. 古いデータベースを本番環境からローテーションして削除します。手順については、「DB インスタンスの削除」を参照してください。

Amazon S3 および同一リージョンレプリケーションのキーローテーション

Amazon Simple Storage Service (Amazon S3) の場合、オブジェクトの暗号化キーを変更するには、オブジェクトを読み書きする必要があります。オブジェクトを書き換えるときは、書き込みオペレーションで新しい暗号化キーを明示的に指定します。多くのオブジェクトに対してこれを行うには、Amazon S3 バッチオペレーションを使用できます。ジョブ設定内で、コピーオペレーションに新しい暗号化設定を指定します。たとえば、SSE-KMS を選択し、keyId を入力できます。

または、Amazon S3 同一リージョンレプリケーション (SRR) を使用することもできます。SSR は、転送中のオブジェクトを再暗号化できます。

インポートされたマテリアルを使用した KMS キーの更新

AWS KMS は、インポートしたキーマテリアルを復元またはローテーションしません。インポートされたキーマテリアルで KMS キーをローテーションするには、キーを手動でローテーションする必要があります。

の使用に関する推奨事項 AWS Encryption SDK

AWS Encryption SDK は、アプリケーションにクライアント側の暗号化を実装するための強力なツールです。Java、JavaScript 、C、Python、およびその他のプログラミング言語のライブラリをご用意しています。これは AWS Key Management Service () と統合されますAWS KMS。KMS キーを参照せずにスタンドアロン SDK として使用することもできます。

このツールを使用するための推奨プラクティスには、アプリケーションの要件を慎重に検討することが含まれます。これらの要件と、キーキャッシュをアプリケーションに導入するなど、特定の設定によって発生する可能性のあるリスクのバランスを取ります。データキーキャッシュの詳細については、 AWS Encryption SDK ドキュメントの「データキーキャッシュ」を参照してください。

を使用するかどうかを決定するときは、次の質問を考慮してください AWS Encryption SDK。

- と統合するサービスとのサーバー側の暗号化では満たすことができないクライアント側の暗号化の要件はありますか AWS KMS?
- クライアント側のデータの暗号化に使用されるキーを適切に保護できますか。また、どのように保護しますか?
- ユースケースにより適したfit-for-purpose暗号化ライブラリは他にもありますか? Amazon S3 クライアント側の暗号化や AWS Database Encryption SDK などの代替 AWS サービスを検討してください。

ユースケースに適したサービスの選択の詳細については、AWS Crypto Tools ドキュメントを参照してください。

の Identity and Access Management のベストプラクティス AWS KMS

AWS Key Management Service （ AWS KMS) を使用するには、 がリクエストの認証と認可 AWS に使用できる認証情報が必要です。アクセス許可が明示的に提供され、拒否されていない限り、プリンシパルには AWS KMS キーに対するアクセス許可はありません。KMS キーを使用または管理する暗黙的または自動的なアクセス許可はありません。このセクションのトピックでは、インフラストラクチャの保護に使用する AWS KMS アクセス管理コントロールを決定するのに役立つセキュリティのベストプラクティスを定義します。

このセクションでは、以下の ID とアクセスの管理トピックについて説明します。

- AWS KMS キーポリシーと IAM ポリシー
- の最小特権のアクセス許可 AWS KMS
- のロールベースのアクセスコントロール AWS KMS
- の属性ベースのアクセスコントロール AWS KMS
- の暗号化コンテキスト AWS KMS
- アクセス AWS KMS 許可のトラブルシューティング

AWS KMS キーポリシーと IAM ポリシー

AWS KMS リソースへのアクセスを管理する主な方法は、 ポリシーを使用することです。ポリシーは、どのプリンシパルがどのリソースにアクセスできるかを記述するドキュメントです。 AWS Identity and Access Management (IAM) ID (ユーザー、ユーザーのグループ、またはロール) にアタッチされたポリシーは、アイデンティティベースのポリシーと呼ばれます。リソースにアタッチする IAM ポリシーはリソースベースのポリシーと呼ばれます。KMS キーの AWS KMS リソースポリシーはキーポリシーと呼ばれます。IAM ポリシーと AWS KMS キーポリシーに加えて、 AWS KMS は許可をサポートします。グラントは、アクセス許可付与のためのフレキシブルかつ強力な手法です。権限を使用して、 AWS アカウント または他の の IAM プリンシパルに期限付き KMS キーアクセスを発行できます AWS アカウント。

すべての KMS キーにはキーポリシーがあります。指定しない場合、 によって AWS KMS 自動的に作成されます。が AWS KMS 使用するデフォルトのキーポリシーは、 AWS KMS コンソールを使用してキーを作成するか AWS KMS API を使用するかによって異なります。最小特権のアクセス許可に関する組織の要件に合わせて、デフォルトのキーポリシーを編集することをお勧めします。これ

は、IAM ポリシーをキーポリシーと組み合わせて使用する戦略とも一致させる必要があります。での IAM ポリシーの使用に関するその他の推奨事項については AWS KMS、 AWS KMS ドキュメントの「IAM ポリシーのベストプラクティス」を参照してください。

キーポリシーを使用して、IAM プリンシパルの認可をアイデンティティベースのポリシーに委任できます。キーポリシーを使用して、アイデンティティベースのポリシーと組み合わせて認可を絞り込むこともできます。いずれの場合も、キーポリシーとアイデンティティベースのポリシーの両方がアクセスと、サービスコントロールポリシー (SCPs)、リソースコントロールポリシー (RCPs)、アクセス許可の境界など、アクセスをスコープするその他の適用可能なポリシーを決定します。 https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.htmlプリンシパルが KMS キーとは異なるアカウントにある場合、基本的に、暗号化アクションと許可アクションのみがサポートされます。このクロスアカウントシナリオの詳細については、 ドキュメントの「他のアカウントのユーザーに KMS キーの使用を許可する」を参照してください。 AWS KMS

KMS キーへのアクセスを制御するには、IAM アイデンティティベースのポリシーをキーポリシーと組み合わせて使用する必要があります。グラントは、KMS キーへのアクセスを制御するために、これらのポリシーと組み合わせて使用することもできます。アイデンティティベースのポリシーを使用して KMS キーへのアクセスを制御するには、キーポリシーでアカウントがアイデンティティベースのポリシーを使用することを許可する必要があります。IAM ポリシー を有効にするキーポリシーステートメントを指定するか、もしくはキーポリシー内で許可対象のプリンシパルを明示的に指定できます。

ポリシーを作成するときは、次のアクションを実行できるユーザーを制限する強力なコントロールがあることを確認してください。

- IAM ポリシーと KMS キーポリシーの更新、作成、削除
- ユーザー、ロール、グループとのアイデンティティベースのポリシーのアタッチとデタッチ
- KMS AWS KMS キーからのキーポリシーのアタッチとデタッチ
- KMS キーの許可を作成する – KMS キーへのアクセスをキーポリシーでのみ制御するか、キーポリシーを IAM ポリシーと組み合わせるかにかかわらず、ポリシーを変更する機能を制限する必要があります。既存のポリシーを変更するための承認プロセスを実装します。承認プロセスは、以下を防ぐのに役立ちます。
  - IAM プリンシパルのアクセス許可の偶発的な喪失 – IAM プリンシパルがキーを管理したり、暗号化オペレーションで使用したりできないように変更を加えることができます。極端なシナリオでは、すべてのユーザーからキー管理アクセス許可を取り消すことができます。この場合、AWS サポートに連絡してキーへのアクセスを回復する必要があります。

- KMS キーポリシーへの未承認の変更 – 権限のないユーザーがキーポリシーにアクセスした場合、意図しない AWS アカウント またはプリンシパルにアクセス許可を委任するように変更することができます。
- IAM ポリシーへの未承認の変更 – 権限のないユーザーがグループのメンバーシップを管理するアクセス許可を持つ認証情報のセットを取得した場合、独自のアクセス許可を昇格させ、IAM ポリシー、キーポリシー、KMS キー設定、またはその他の AWS リソース設定を変更することができます。

KMS キー管理者として指定されている IAM プリンシパルに関連付けられている IAM ロールとユーザーを慎重に確認します。これにより、不正な削除や変更を防ぐことができます。KMS キーにアクセスできるプリンシパルを変更する必要がある場合は、必要なすべてのキーポリシーに新しい管理者プリンシパルが追加されていることを確認します。前の管理プリンシパルを削除する前に、アクセス許可をテストします。すべての IAM セキュリティのベストプラクティスに従い、長期的な認証情報の代わりに一時的な認証情報を使用することを強くお勧めします。

ポリシーの作成時にプリンシパルの名前がわからない場合や、アクセスを必要とするプリンシパルが頻繁に変更される場合は、許可を通じて期限付きアクセスを発行することをお勧めします。被付与者プリンシパルは、KMS キーと同じアカウントまたは別のアカウントにあることができます。プリンシパルと KMS キーが異なるアカウントにある場合は、グラントに加えてアイデンティティベースのポリシーを指定する必要があります。グラントを作成するには API を呼び出し、不要になったグラントを廃止または取り消す必要があるため、グラントには追加の管理が必要です。

アカウントのルートユーザーまたはキー作成者を含む AWS プリンシパルには、キーポリシー、IAM ポリシー、または許可で明示的に許可および明示的に拒否されていない限り、KMS キーに対するアクセス許可はありません。さらに、ユーザーが KMS キーを使用するための意図しないアクセスを取得した場合の対処方法と影響を考慮する必要があります。このようなリスクを軽減するには、次の点を考慮してください。

- データのカテゴリごとに異なる KMS キーを維持できます。これにより、キーを分離し、そのデータカテゴリへのプリンシパルアクセスを特にターゲットとするポリシーステートメントを含むより簡潔なキーポリシーを維持できます。また、関連する IAM 認証情報が意図せずにアクセスされた場合、そのアクセスに関連付けられた ID は、IAM ポリシーで指定されたキーにのみアクセスでき、キーポリシーがそのプリンシパルへのアクセスを許可する場合に限ります。
- キーへの意図しないアクセスを持つユーザーがデータにアクセスできるかどうかを評価できます。例えば、Amazon Simple Storage Service (Amazon S3) では、ユーザーは Amazon S3 の暗号化されたオブジェクトにアクセスするための適切なアクセス許可も必要です。または、ユーザーが (RDP または SSH を使用して) KMS キーで暗号化されたボリュームを持つ Amazon EC2 インスタ

ンスへの意図しないアクセスを持っている場合、ユーザーはオペレーティングシステムツールを使用してデータにアクセスできます。

> **Note**
>
> AWS のサービス を使用する は、暗号文をユーザーに公開 AWS KMS しません (暗号分析に対する最新のアプローチでは、暗号文へのアクセスが必要です) 。さらに、NIST SP800-88 の要件に従って、すべてのストレージメディアが廃止されると物理的に破棄されるため、暗号文は AWS データセンターの外部で物理的に検査することはできません。

の最小特権のアクセス許可 AWS KMS

KMS キーは機密情報を保護するため、最小特権アクセスの原則に従うことをお勧めします。キーポリシーを定義する際は、タスクの実行に必要な最小限のアクセス許可のみを委任してください。追加のアイデンティティベースのポリシーでアクセス許可をさらに制限する予定がある場合にのみ、KMS キーポリシーに対するすべてのアクション (`kms:*`) を許可します。アイデンティティベースのポリシーでアクセス許可を管理する場合は、IAM ポリシーを作成して IAM プリンシパルにアタッチし、ポリシーの変更をモニタリングできるユーザーを制限します。

キーポリシーとアイデンティティベースのポリシーの両方ですべてのアクション (`kms:*`) を許可する場合、プリンシパルには KMS キーに対する管理アクセス許可と使用アクセス許可の両方があります。セキュリティのベストプラクティスとして、これらのアクセス許可を特定のプリンシパルにのみ委任することをお勧めします。キーを管理するプリンシパルと、キーを使用するプリンシパルにアクセス許可を割り当てる方法を検討してください。これを行うには、キーポリシーでプリンシパルに明示的に名前を付けるか、アイデンティティベースのポリシーがアタッチされているプリンシパルを制限します。条件キーを使用してアクセス許可を制限することもできます。たとえば、aws:PrincipalTag を使用して、API コールを行うプリンシパルに条件ルールで指定されたタグがある場合に、すべてのアクションを許可できます。

でポリシーステートメントがどのように評価されるかを理解するには AWS、IAM ドキュメントの「ポリシー評価ロジック」を参照してください。ポリシーを作成する前に、このトピックを確認して、アクセス権限を持たないプリンシパルへのアクセスを提供するなど、ポリシーが意図しない影響を及ぼす可能性を減らすことをお勧めします。

> **Tip**
>
> 非本番環境でアプリケーションをテストする場合は、 AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) を使用して、IAM ポリシーに最小特権のアクセス許可を適用するのに役立ちます。

IAM ロールの代わりに IAM ユーザーを使用する場合は、長期的な認証情報の脆弱性を軽減するためにAWS 多要素認証 (MFA) を使用することを強くお勧めします。MFA の使用により、以下が可能となります。

- キー削除のスケジューリングなどの特権アクションを実行する前に、MFA を使用して認証情報を検証するようユーザーに義務付けることができます。
- 管理者アカウントのパスワードと MFA デバイスの所有権を複数の人の間で分割する「分割認証」を実装することができます。

最小特権のアクセス許可の設定に役立つサンプルポリシーについては、 AWS KMS ドキュメントの「IAM ポリシーの例」を参照してください。

のロールベースのアクセスコントロール AWS KMS

ロールベースのアクセスコントロール (RBAC) は、ユーザーに職務の実行に必要なアクセス許可のみを提供し、それ以上のアクセス許可は付与しない認可戦略です。これは、最小特権の原則を実装するのに役立つアプローチです。

AWS KMS は RBAC をサポートしています。これにより、キーポリシー内で詳細なアクセス許可を指定することで、キーへのアクセスを制御できます。キーポリシーは、キーへのアクセスを許可するリソース、アクション、効果、プリンシパル、およびオプション条件を指定します。RBAC を実装するには AWS KMS、キーユーザーとキー管理者のアクセス許可を分離することをお勧めします。

キーユーザーには、ユーザーが必要とするアクセス許可のみを割り当てます。アクセス許可をさらに絞り込むには、次の質問を使用します。

- どの IAM プリンシパルがキーにアクセスする必要がありますか？
- 各プリンシパルがそのキーを用いて実行する必要があるアクションはどんなものがありますか? たとえば、プリンシパルには `Encrypt`と `Sign`アクセス許可のみが必要ですか？
- プリンシパルはどのリソースにアクセスする必要がありますか？

- エンティティは人間ですか、それとも AWS のサービスですか。サービスの場合は、kms:ViaService 条件キーを使用して、キーの使用を特定のサービスに制限できます。

キー管理者には、管理者に必要なアクセス許可のみを割り当てます。たとえば、管理者のアクセス許可は、キーがテスト環境と本番環境のどちらで使用されているかによって異なります。特定の非本番環境で制限の少ないアクセス許可を使用する場合は、ポリシーを本番環境にリリースする前にテストするプロセスを実装します。

キーユーザーと管理者のロールベースのアクセスコントロールを設定するのに役立つサンプルポリシーについては、「RBAC for AWS KMS」を参照してください。

の属性ベースのアクセスコントロール AWS KMS

属性ベースのアクセスコントロール (ABAC) は、属性に基づいてアクセス許可を定義する認可戦略です。RBAC と同様に、最小特権の原則を実装するのに役立つアプローチです。

AWS KMS は、KMS キーなどのターゲットリソースに関連付けられたタグと、API コールを行うプリンシパルに関連付けられたタグに基づいてアクセス許可を定義できるようにすることで、ABAC をサポートします。では AWS KMS、タグとエイリアスを使用して、カスタマーマネージドキーへのアクセスを制御できます。たとえば、プリンシパルのタグが KMS キーに関連付けられたタグと一致する場合に、タグ条件キーを使用してオペレーションを許可する IAM ポリシーを定義できます。チュートリアルについては、 ドキュメントの「タグに基づいて AWS リソースにアクセスするためのアクセス許可を定義する AWS KMS 」を参照してください。

ベストプラクティスとして、ABAC 戦略を使用して IAM ポリシー管理を簡素化します。ABAC を使用すると、管理者は既存のポリシーを更新する代わりにタグを使用して新しいリソースへのアクセスを許可できます。ABAC では、ジョブ機能ごとに異なるポリシーを作成する必要がないため、必要なポリシーが少なくなります。詳細については、IAM ドキュメントの「ABAC と従来の RBAC モデルの比較」を参照してください。

最小特権アクセス許可のベストプラクティスを ABAC モデルに適用します。ジョブの実行に必要なアクセス許可のみを IAM プリンシパルに提供します。ユーザーがロールとリソースのタグを変更できるようにするタグ付け APIs へのアクセスを慎重に制御します。キーエイリアス条件キーを使用して で ABAC をサポートする場合は AWS KMS、キーを作成してエイリアスを変更できるユーザーを制限する強力なコントロールがあることを確認してください。

タグを使用して特定のキーをビジネスカテゴリにリンクし、特定のアクションに正しいキーが使用されていることを確認することもできます。たとえば、 AWS CloudTrail ログを使用して、特定の

AWS KMS アクションを実行するために使用されるキーが、使用されているリソースと同じビジネスカテゴリに属していることを確認できます。

> **Warning**
>
> タグキーまたはタグ値には、機密情報や重要情報を含めないでください。タグは暗号化されません。請求など AWS のサービス、多くのユーザーがアクセスできます。

アクセスコントロールに ABAC アプローチを実装する前に、使用している他のサービスがこのアプローチをサポートしているかどうかを検討してください。ABAC をサポートするサービスを決定する方法については、IAM ドキュメントの「IAM AWS のサービス と連携するサービス」を参照してください。

の ABAC の実装 AWS KMS と、ポリシーの設定に役立つ条件キーの詳細については、「ABAC for AWS KMS」を参照してください。

の暗号化コンテキスト AWS KMS

対称 AWS KMS 暗号化 KMS キーを使用するすべての暗号化オペレーションは、暗号化コンテキストを受け入れます。暗号化コンテキストは、データに関する追加のコンテキスト情報を含むことができるシークレット以外のキーと値のペアのオプションセットです。ベストプラクティスとして、`Encrypt`のオペレーションに暗号化コンテキストを挿入 AWS KMS して、 への復号 API 呼び出しの認可と監査可能性を高めることができます AWS KMS。 AWS KMS は、暗号化コンテキストを追加の認証済みデータ (AAD) として使用して、認証済み暗号化をサポートします。暗号化コンテキストは、暗号化されて暗号文にバインドされます。これにより、データの復号には同じ暗号化コンテキストが必要になります。

この暗号化コンテキストは秘密ではなく、暗号化されていません。 AWS CloudTrail ログにはプレーンテキストで表示されるため、これを使用して暗号化オペレーションを識別して分類できます。暗号化コンテキストはシークレットではないため、CloudTrail ログデータへのアクセスは承認されたプリンシパルのみに許可する必要があります。

kms:EncryptionContext:context-key および kms:EncryptionContextKeys 条件キーを使用して、暗号化コンテキストに基づいて対称暗号化 KMS キーへのアクセスを制御することもできます。これらの条件キーを使用して、暗号化オペレーションで暗号化コンテキストを使用することを要求することもできます。これらの条件キーについては、 `ForAnyValue`または `ForAllValues` セット演算子の使用に関するガイダンスを確認して、ポリシーが意図したアクセス許可を反映していることを確認します。

アクセス AWS KMS 許可のトラブルシューティング

KMS キーのアクセスコントロールポリシーを作成するときは、IAM ポリシーとキーポリシーがどのように連携するかを検討してください。プリンシパルの有効なアクセス許可は、有効なすべてのポリシーによって付与される (明示的に拒否されない) アクセス許可です。アカウント内では、KMS キーへのアクセス許可は、IAM アイデンティティベースのポリシー、キーポリシー、アクセス許可の境界、サービスコントロールポリシー、またはセッションポリシーの影響を受ける可能性があります。たとえば、アイデンティティベースのポリシーとキーポリシーの両方を使用して KMS キーへのアクセスを制御する場合、プリンシパルとリソースの両方に関連するすべてのポリシーが評価され、特定のアクションを実行するプリンシパルの認可が決定されます。詳細については、IAM ドキュメントの「ポリシーの評価論理」を参照してください。

キーアクセスのトラブルシューティングの詳細とフローチャートについては、 AWS KMS ドキュメントの「キーアクセスのトラブルシューティング」を参照してください。

アクセス拒否エラーメッセージをトラブルシューティングするには

1. IAM アイデンティティベースのポリシーと KMS キーポリシーでアクセスが許可されていることを確認します。
2. IAM のアクセス許可の境界がアクセスを制限していないことを確認します。
3. のサービスコントロールポリシー (SCP) またはリソースコントロールポリシー (RCP) AWS Organizations がアクセスを制限していないことを確認します。
4. 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が正しいことを確認します。
5. アイデンティティベースのポリシーとキーポリシーで、キーへのアクセスを制限する条件またはリソース参照を削除します。これらの制限を削除した後、プリンシパルが以前に失敗した API を正常に呼び出せることを確認します。成功したら、条件とリソース参照を一度に 1 つずつ再適用し、その後、プリンシパルが引き続きアクセスできることを確認します。これにより、エラーの原因となっている条件またはリソースリファレンスを特定できます。

詳細については、IAM ドキュメントの「アクセス拒否エラーメッセージのトラブルシューティング」を参照してください。

の検出とモニタリングのベストプラクティス AWS KMS

検出とモニタリングは、 AWS Key Management Service (AWS KMS) キーの可用性、状態、使用状況を理解する上で重要な部分です。モニタリングは、 AWS ソリューションのセキュリティ、信頼性、可用性、パフォーマンスを維持するのに役立ちます。 には、KMS キーと AWS KMS オペレーションをモニタリングするためのいくつかのツール AWS が用意されています。このセクションでは、これらのツールを設定して使用して環境の可視性を高め、KMS キーの使用状況をモニタリングする方法について説明します。

このセクションでは、以下の検出とモニタリングのトピックについて説明します。

- による AWS KMS オペレーションのモニタリング AWS CloudTrail
- IAM Access Analyzer を使用した KMS キーへのアクセスのモニタリング
- AWS のサービス を使用した他の の暗号化設定のモニタリング AWS Config
- Amazon CloudWatch アラームによる KMS キーのモニタリング
- Amazon EventBridge によるレスポンスの自動化

による AWS KMS オペレーションのモニタリング AWS CloudTrail

AWS KMS は、 ユーザーAWS CloudTrail、ロール、その他 AWS KMS による へのすべての呼び出しを記録できるサービスである と統合されています AWS のサービス。CloudTrail は、 へのすべての API コールをイベント AWS KMS としてキャプチャします。これには、 AWS KMS コンソール、AWS KMS APIs、 AWS Command Line Interface (AWS CLI) AWS CloudFormation、および からの呼び出しが含まれます AWS Tools for PowerShell。

CloudTrail は、 `ListAliases`や などの読み取り専用 AWS KMS オペレーションを含むすべてのオペレーションをログに記録します`GetKeyRotationStatus`。また、 `CreateKey`や や などの KMS キーを管理するオペレーションもログに記録し`PutKeyPolicy, and cryptographic operations, such as GenerateDataKey`ます`Decrypt`。また、、、、`DeleteExpiredKeyMaterial` `DeleteKey`など`SynchronizeMultiRegionKey`、 が AWS KMS 呼び出す内部オペレーションもログに記録されます`RotateKey`。

CloudTrail は、作成 AWS アカウント 時に で有効になります。デフォルトでは、イベント履歴は、で過去 90 日間に記録された管理イベント API アクティビティの表示可能、検索可能、ダウンロード可能、およびイミュータブルなレコードを提供します AWS リージョン。90 日間を超える KMS キーの使用状況をモニタリングまたは監査するには、 の CloudTrail 証跡を作成することをお勧めします

AWS アカウント。で組織を作成した場合は AWS Organizations、その組織内のすべての のイベントをログに記録する組織の証跡またはイベントデータストアを作成できます。 AWS アカウント

アカウントまたは組織の証跡を確立したら、他の を使用して、証跡に記録されたイベント AWS のサービス を保存、分析、および自動的に応答できます。例えば、次のオペレーションを実行できます。

- 証跡内の特定のイベントを通知する Amazon CloudWatch アラームを設定できます。詳細については、このガイドの「Amazon CloudWatch アラームによる KMS キーのモニタリング」を参照してください。
- 証跡でイベントが発生したときにアクションを自動的に実行する Amazon EventBridge ルールを作成できます。詳細については、このガイドの「Amazon EventBridge によるレスポンスの自動化」を参照してください。
- Amazon Security Lake を使用して AWS のサービス、CloudTrail を含む複数の からログを収集して保存できます。詳細については、Amazon Security Lake ドキュメントの「Security Lake AWS のサービス での からのデータ収集」を参照してください。
- 運用アクティビティの分析を強化するために、Amazon Athena で CloudTrail ログをクエリできます。詳細については、Amazon Athena ドキュメントの「クエリ AWS CloudTrail ログ」を参照してください。

CloudTrail による AWS KMS オペレーションのモニタリングの詳細については、以下を参照してください。

- を使用した API コールのログ記録 AWS KMSAWS CloudTrail
- AWS KMS ログエントリの例
- Amazon EventBridge で KMS キーをモニタリングする
- CloudTrail と Amazon EventBridge の統合

IAM Access Analyzer を使用した KMS キーへのアクセスのモニタリング

AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) は、外部エンティティと共有されている組織およびアカウント (KMS キーなど) 内のリソースを識別するのに役立ちます。このサービスは、セキュリティ上のリスクであるリソースやデータへの意図しないアクセスや過度に広範なアクセスを特定するのに役立ちます。IAM Access Analyzer は、ロジックベースの推論を

使用して AWS 環境内のリソースベースのポリシーを分析することで、外部プリンシパルと共有されているリソースを識別します。

IAM Access Analyzer を使用して、KMS キーにアクセスできる外部エンティティを特定できます。IAM Access Analyzer を有効にすると、組織全体またはターゲットアカウントのアナライザーが作成されます。選択した組織またはアカウントは、アナライザーの信頼ゾーンと呼ばれます。アナライザーは、信頼ゾーン内のサポートされているリソースをモニタリングします。信頼ゾーン内のプリンシパルによるリソースへのアクセスは、信頼されたと見なされます。

KMS キーの場合、IAM Access Analyzer はキーに適用されるキーポリシーと許可を分析します。キーポリシーまたは許可が外部エンティティにキーへのアクセスを許可する場合、結果が生成されます。IAM Access Analyzer を使用して、外部エンティティが KMS キーにアクセスできるかどうかを判断し、それらのエンティティがアクセスする必要があるかどうかを確認します。

IAM Access Analyzer を使用して KMS キーアクセスをモニタリングする方法の詳細については、以下を参照してください。

- AWS Identity and Access Management Access Analyzerの使用
- 外部アクセス用の IAM Access Analyzer リソースタイプ
- IAM Access Analyzer リソースタイプ: AWS KMS keys
- 外部アクセスと未使用のアクセスの検出結果

AWS のサービス を使用した他の の暗号化設定のモニタリング AWS Config

AWS Config は、 内の AWS リソースの設定の詳細ビューを提供します AWS アカウント。を使用して AWS Config 、KMS キーを使用する AWS のサービス で暗号化設定が適切に設定されていることを確認します。例えば、暗号化されたボリューム AWS Config ルールを使用して、Amazon Elastic Block Store (Amazon EBS) ボリュームが暗号化されていることを検証できます。

AWS Config には、リソースを評価するルールをすばやく選択するためのマネージドルールが含まれています。 AWS Config AWS リージョン で、必要なマネージドルールがそのリージョンでサポートされているかどうかを確認します。利用可能なマネージドルールには、Amazon Relational Database Service (Amazon RDS) スナップショットの設定のチェック、CloudTrail 証跡の暗号化、Amazon Simple Storage Service (Amazon S3) バケットのデフォルトの暗号化、Amazon DynamoDB テーブルの暗号化などが含まれます。

カスタムルールを作成し、ビジネスロジックを適用して、リソースが要件に準拠しているかどうかを判断することもできます。多くのマネージドルールのオープンソースコードは、GitHub AWS Config のルールリポジトリで入手できます。これらは、独自のカスタムルールを開発するための出発点として役立ちます。

リソースがルールに準拠していない場合は、応答アクションを開始できます。 AWS Config には、AWS Systems Manager 自動化が実行する修復アクションが含まれます。例えば、cloud-trail-encryption-enabled ルールを適用し、ルールがNON_COMPLIANT結果を返した場合、 は CloudTrail ログを暗号化することで問題を修正する自動化ドキュメントを開始 AWS Config できます。

AWS Config では、リソースをプロビジョニングする前に AWS Config 、ルールへの準拠を事前にチェックできます。プロアクティブモードでルールを適用すると、クラウドリソースが作成または更新される前に、その設定を評価するのに役立ちます。デプロイパイプラインの一部としてプロアクティブモードでルールを適用すると、リソースをデプロイする前にリソース設定をテストできます。

を通じて AWS Config ルールをコントロールとして実装することもできますAWS Security Hub CSPM。Security Hub CSPM には、 に適用できるセキュリティ標準が用意されています AWS アカウント。これらの標準は、推奨プラクティスに照らして環境を評価するのに役立ちます。AWS Foundational Security Best Practices 標準には、保管時の暗号化が設定されていること、および KMS キーポリシーが推奨プラクティスに従っていることを確認するための保護コントロールカテゴリ内のコントロールが含まれています。

を使用して の暗号化設定をモニタリング AWS Config する方法の詳細については AWS のサービス、以下を参照してください。

- AWS Configの開始方法
- AWS Config マネージドルール
- AWS Config custom rules
- を使用した非準拠リソースの修復 AWS Config

Amazon CloudWatch アラームによる KMS キーのモニタリング

Amazon CloudWatch は、 AWS リソースと で実行されるアプリケーションを AWS リアルタイムでモニタリングします。CloudWatch を使用して、測定できる変数であるメトリクスを収集および追跡できます。

インポートされたキーマテリアルの有効期限切れ、またはキーの削除は、意図しない、または適切に計画されていない場合、致命的なイベントになる可能性があります。これらのイベントが発生する前

に警告するように CloudWatch アラームを設定することをお勧めします。また、重要なキーの削除を防ぐために、 AWS Identity and Access Management (IAM) ポリシーまたは AWS Organizations サービスコントロールポリシー (SCPs) を設定することをお勧めします。

CloudWatch アラームは、キーの削除のキャンセルなどの修正アクションや、削除または期限切れのキーマテリアルの再インポートなどの修正アクションを実行するのに役立ちます。

Amazon EventBridge によるレスポンスの自動化

Amazon EventBridge を使用して、KMS キーに影響する重要なイベントを通知することもできます。EventBridge は、 AWS リソースへの変更を記述するシステムイベントのほぼリアルタイムのストリーム AWS のサービス を配信する です。EventBridge は CloudTrail と Security Hub CSPM からイベントを自動的に受信します。EventBridge では、CloudTrail で記録されたイベントに対応するルールを作成することができます。

AWS KMS イベントには以下が含まれます。

- KMS キーのキーマテリアルが自動的にローテーションされました
- KMS キーのインポートされたキーマテリアルの有効期限が切れました
- 削除がスケジュールされていた KMS キーが削除されました

これらのイベントは、 で追加のアクションを開始できます AWS アカウント。これらのアクションは、イベントが発生した後にのみ処理できるため、前のセクションで説明した CloudWatch アラームとは異なります。たとえば、キーが削除された後に特定のキーに接続されているリソースを削除したり、キーが削除されたことをコンプライアンスチームまたは監査チームに通知したりできます。

EventBridge を使用して CloudTrail に記録された他の API イベントをフィルタリングすることもできます。つまり、キーポリシー関連の API アクションが特に懸念される場合は、それらをフィルタリングできます。たとえば、EventBridge で `PutKeyPolicy` API アクションをフィルタリングできます。より広くは、 `Disable*`または `Delete*` で始まる API アクションをフィルタリングして、自動レスポンスを開始できます。

EventBridge を使用すると、 (検出コントロールである) をモニタリングし、 (応答コントロールである) 調査して、予期しないイベントや選択したイベントに対応できます。たとえば、IAM ユーザーまたはロールが作成された場合、KMS キーが作成された場合、またはキーポリシーが変更された場合、セキュリティチームに警告し、特定のアクションを実行できます。指定した API アクションをフィルタリングし、ターゲットをルールに関連付ける EventBridge イベントルールを作成できます。ターゲットの例には、 AWS Lambda 関数、Amazon Simple Notification Service (Amazon SNS) 通

知、Amazon Simple Queue Service (Amazon SQS) キューなどがあります。ターゲットへのイベントの送信の詳細については、「Amazon EventBridge のイベントバスターゲット」を参照してください。

EventBridge AWS KMS によるモニタリングとレスポンスの自動化の詳細については、 AWS KMS ドキュメントの「Amazon EventBridge による KMS キーのモニタリング」を参照してください。

のコストと請求管理のベストプラクティス AWS KMS

の幅と深さを通じて、ビジネス要件を満たしながらコストを AWS のサービス 柔軟に管理できます。このセクションでは、 (AWS KMS) の AWS Key Management Service キーストレージの料金について説明し、キーキャッシュなどを通じてコストを削減するための推奨事項を提供します。KMS キーの使用状況を確認して、コストを削減する追加の機会があるかどうかを調べることもできます。

このセクションでは、以下のコストと請求の管理トピックについて説明します。

- AWS KMS キーストレージの料金
- デフォルトの暗号化を使用した Amazon S3 バケットキー
- を使用したデータキーのキャッシュ AWS Encryption SDK
- キーキャッシュと Amazon S3 バケットキーの代替方法
- KMS キー使用のログ記録コストの管理

AWS KMS キーストレージの料金

で AWS KMS key 作成する ごとに料金 AWS KMS が発生します。月額料金は、対称キー、非対称キー、HMAC キー、マルチリージョンキー (各プライマリキーと各レプリカマルチリージョンキー) 、インポートされたキーマテリアルを持つキー、キーオリジンが AWS CloudHSM または外部キーストアの KMS キーで同じです。

自動またはオンデマンドでローテーションする KMS キーの場合、キーの最初のローテーションと 2 番目のローテーションにより、月額料金 (時間単位の按分計算) が追加されます。2 回目のローテーションの後、その月のそれ以降のローテーションは請求されません。最新のAWS KMS 料金情報については、「 の料金」を参照してください。

AWS Budgets を使用して使用量の予算を設定できます。 AWS Budgets は、アカウント内の支出が特定のしきい値を超えたときに警告できます。に関連するコストについては AWS KMS、KMS キーまたはリクエストに基づいてアラートする使用予算を作成できます。これにより、 AWS KMS キーストレージと使用コストの可視性が向上します。

デフォルトの暗号化を使用した Amazon S3 バケットキー

ユースケースによっては、Amazon Simple Storage Service (Amazon S3) で多数のオブジェクトにアクセスまたは生成するワークロードによって AWS KMS、 への大量のリクエストが生成され、コス

トが増加する可能性があります。Amazon S3 バケットキーを設定すると、コストを最大 99% 削減できます。これは、関連するコストを削減するために暗号化を無効にするための推奨される代替手段です AWS KMS。

を使用したデータキーのキャッシュ AWS Encryption SDK

を使用してクライアント側の暗号化AWS Encryption SDKを実行する場合、データキーキャッシュはアプリケーションのパフォーマンスを向上させ、アプリケーションから へのリクエストがスロットリング AWS KMS されるリスクを軽減し、コストを削減するのに役立ちます。開始方法の詳細については、「データキーキャッシュの使用方法」を参照してください。

キーキャッシュと Amazon S3 バケットキーの代替方法

データ処理要件のためにキーキャッシュがオプションでない場合は、 AWS マネジメントコンソールまたは Service Quotas API を使用して AWS KMS クォータの引き上げをリクエストすることもできます。実行できる API コールの量を考慮してください。実行する API コールの数は、AWS KMS 料金の重要な要素です。リクエストレートクォータを増やしてパフォーマンスをスケールすると、 へのリクエスト数が増えると、追加コスト AWS KMS が発生します。

KMS キー使用のログ記録コストの管理

すべての AWS KMS API コールがログに記録されます AWS CloudTrail。アプリケーションとサービスは、大量の AWS KMS API コールを生成できます (暗号化や復号化を含む暗号化オペレーションなど) 。データの整理、傾向の調査、異常な API アクティビティの検索に役立つツールなしで CloudTrail ログを確認するのは難しい場合があります。Amazon Athena には、CloudTrail ログのテーブルをすばやくセットアップし、ログデータの分析を開始するのに役立つ事前定義されたデータ構造が用意されています。これは、インシデント対応中のアドホック分析やさらなる調査に特に役立ちます。詳細については、Athena ドキュメントの「クエリ AWS CloudTrail ログ」を参照してください。

Athena の料金はクエリごとに支払うため、テーブルは事前に無料で設定できます。データ定義言語ステートメントには料金はかかりません。インシデントに対応すると、多くの前提条件が既に満たされていることを確認するのに役立ちます。準備に役立つように、テーブルの作成後にクエリを記述し、テストして、必要な結果を生成していることを確認するのがベストプラクティスです。クエリは、今後の使用のために Athena に保存できます。Athena の開始方法の詳細については、Amazon Athena の開始方法」を参照してください。

データイベントは、リソース上またはリソース内で実行されるオペレーションを可視化します。これらのイベントは、データプレーンオペレーションとも呼ばれます。例としては、Amazon S3 `PutObject`イベントや Lambda 関数オペレーション API コールなどがあります。データイベントは多くの場合、大量のアクティビティであり、ログ記録に対して料金が発生します。CloudTrail の証跡またはイベントデータストアにログ記録されるデータイベントの量を制御するために、CloudTrail と Amazon S3 のコストを削減するために AWS KMS、CloudTrail にログインするデータイベントを制限する高度なイベントセレクタを設定することで、ログ記録を最適化できます。 Amazon S3 詳細については、「高度なイベントセレクタを使用して AWS CloudTrail コストを最適化する方法」(AWS ブログ記事) を参照してください。

リソース

AWS Key Management Service （ AWS KMS) ドキュメント

- AWS KMS デベロッパーガイド
- AWS KMS API リファレンス
- AWS KMS 「 リファレンス」の AWS CLI

ツール

- AWS Encryption SDK

AWS 規範ガイダンス

戦略

- 保管中のデータの暗号化戦略の作成

ガイド

- の暗号化のベストプラクティスと機能 AWS のサービス
- AWS プライバシーリファレンスアーキテクチャ (AWS PRA)

パターン

- Amazon EBS ボリュームを自動的に暗号化する
- Automatically remediate unencrypted Amazon RDS DB instances and clusters
- のスケジュールされた削除のモニタリングと修復 AWS KMS keys

寄稿者

オーサリング

- Frank Phillis、シニア GTM スペシャリストソリューションアーキテクト、 AWS
- AWS KMS および Crypto ライブラリのディレクター、Ken Beer AWS
- マイケル・ミラー、シニアソリューションアーキテクト、 AWS
- Jeremy Stieglitz、Principal Product Manager、 AWS
- Zach Miller、プリンシパルソリューションアーキテクト、 AWS
- Peter M. O'Donnell、プリンシパルソリューションアーキテクト、 AWS
- パトリック・パーマー、プリンシパル・ソリューション・アーキテクト、 AWS
- Dave Walker、プリンシパルソリューションアーキテクト、 AWS

レビュー

- Manigandan Shri、シニアデリバリーコンサルタント、 AWS

テクニカルライティング

- " AbouHarb、シニアテクニカルライター、 AWS
- Kimberly Garmoe、シニアテクニカルライター、 AWS

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。今後の更新に関する通知を受け取る場合は、RSS フィード をサブスクライブできます。

変更	説明	日付
初版発行	—	2025 年 3 月 24 日

AWS 規範ガイダンスの用語集

以下は、 AWS 規範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 PostgreSQL 互換エディションに移行する。
- 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の最適化レベルを導入します。例: お客様のオンプレミスの Oracle データベースを AWS クラウドの Oracle 用の Amazon Relational Database Service (Amazon RDS) に移行する。
- 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 に移行する。
- 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: お客様のオンプレミスの Oracle データベースを AWS クラウドの EC2 インスタンス上の Oracle に移行する。
- 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。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サーバーを移行します。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。
- 廃止 — 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制御」をご覧ください。

抽象化されたサービス

「マネージドユーザー」をご覧ください。

ACID

「原子性、一貫性、分離性、耐久性 (ACID)」をご覧ください。

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な方法ですが、さらに多くの作業が必要となります。

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

複数行に処理を行い、グループ全体を対象に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 MAX などがあります。

AI

「人工知能」をご覧ください。

AIOps

「AI オペレーション」をご覧ください。

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。

アプリケーション制御

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 の重要な要素であり、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?」をご覧ください。

AI 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。 AWS 移行戦略での AIOps の使用方法については、オペレーション統合ガイド を参照してください。

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。

原子性、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制御 (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「 の ABAC 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 (AZ)

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)

組織がクラウドへの移行を成功させるための効率的で効果的な計画を立て AWS るための、 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整理しています。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、クラウド導入を成功させるための組織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の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 のホワイトペーパー 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

個人や組織に混乱や損害を与えることを目的としたボット。

BCP

「ビジネス継続性計画 (BCP)」をご覧ください。

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 の動作グラフを使用すると、失敗したログオンの試行、不審な API 呼び出し、その他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「動作グラフのデータ」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。「エンディアン性」もご覧ください。

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

それぞれが独立しているが、同一の環境を 2 つ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を 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を別の環境 (グリーン) で実行します。この戦略は、最小限の影響で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やり取り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、個人や組織を混乱させたり、損害を与えたりすることを意図したものもあります。

ボットネット

マルウェアに感染しており、ボットハーダーまたはボットオペレーターと呼ばれる単一の当事者によって制御されているボットのネットワーク。ボットネットは、ボットとその影響力を拡大する仕組みとして、非常によく知られています。

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、「ブランチの概要」(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

例外的な状況では、承認されたプロセスを通じて、ユーザーが AWS アカウント 通常アクセス許可を持たない にすばやくアクセスできるようにします。詳細については、 AWS 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、AWSでのコンテナ化されたマイクロサービスの実行ホワイトペーパーの「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。

ビジネス継続性計画 (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

カナリアデプロイ

エンドユーザーへのバージョンリリースを、時間をかけて段階的に行うこと。確信が持てたら新規バージョンをデプロイして、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

「変更データキャプチャ」を参照してください。

変更データキャプチャ (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。CDC は、ターゲットシステムでの変更を監査またはレプリケートして同期を維持するなど、さまざまな目的に使用できます。

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すること。AWS Fault Injection Service (AWS FIS) を使用して、 AWS ワークロードにストレスを与え、その応答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 AWS のサービス 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の CCoE 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、 AWS クラウドへの移行時に通常実行する 4 つの段階。

- 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
- 基礎固め — お客様のクラウドの導入を拡大するための基礎的な投資 (ランディングゾーンの作成、CCoE の定義、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。移行戦略との関連性については、 AWS 「移行準備ガイド」を参照してください。

CMDB

「構成管理データベース (CMDB)」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 や Bitbucket Cloud があります。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といった、ビジュアル形式の情報を分析および抽出する AI の分野。例えば、Amazon SageMaker AI では、CV 用の画像処理アルゴリズムを利用できます。

設定ドリフト

ワークロードにおいて、設定が想定した状態から変化すること。これによって、ワークロードが非準拠になる可能性がありますが、この状態は、徐々に生じ、意図的なものではありません。

構成管理データベース (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、CMDB のデータは、移行のポートフォリオの検出と分析の段階で使用します。

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。YAML 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。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

非一元的で分散型のデータ所有権を持つとともに、一元的な管理およびガバナンスを行え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できるようにします。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、一般的に、大量の履歴データが含まれており、多くの場合、それらはクエリや分析に使用されます。

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ます。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。

深層学習

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。

多層防御

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。たとえば、多層防御アプローチでは、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。

トラブルシューティング

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、「 AWSでのセキュリティコントロールの実装」の「検出的コントロール」を参照してください。

開発バリュー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・プラクティスのために設計されたバリューストリームマッピング・プロセスを拡張したものです。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

スタースキーマにおいて、ファクトテーブルの定量データに関するデータ属性が含まれる小さいテーブル。ディメンションテーブルの属性は、通常、テキストフィールド、またはテキストのように扱える個別の数値で示されます。これらの属性は、一般的に、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)

ディザスタ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の戦略とプロセス。詳細については、 AWS Well-Architected フレームワークの「 Disaster Recovery of Workloads on AWS: Recovery in the Cloud」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の詳細については、「コンテナと Amazon API Gateway を使用して、従来の Microsoft ASP.NET (ASMX) ウェブサービスを段階的にモダナイズ」を参照してください。

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を追跡します。たとえば、 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するランディングゾーンの変更を検出したりできます。

DVSM

「開発バリュー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。

EDI

「電子データ交換」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、応答時間を改善できます。

電子データ交換 (EDI)

組織間で行う、ビジネスドキュメントの自動交換。詳細については、「電子データ交換とは」を参照してください。

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処理。

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) 内でホストして、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 VPC エンドポイントを作成することで、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 VPC) ドキュメントの「エンドポイントサービスを作成する」を参照してください。

エンタープライズリソースプランニング (ERP)

エンタープライズの主要なビジネスプロセス (会計、MES、プロジェクト管理など) を自動化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、統計の概要を計算し、データの可視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にあるテーブル。ビジネスオペレーションに関する定量的データが保存されます。一般的に、ファクトテーブルは、2 種類の列で構成されます。1 つは測定値が含まれる列、もう 1 つはディメンションテーブルへの外部キーが含まれる列です。

フェイルファスト

開発ライフサイクルを短縮するために、頻繁かつ段階的にテストを行う哲学であり、アジャイルアプローチでは、この考え方がきわめて重要です。

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 Deskonations (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で表されます。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。

数ショットプロンプト

LLM に、タスクと望ましい出力を示す例を少数提示した後に、類似のタスクを実行させること。この手法は、プロンプトに記述された例 (ショット) からモデルが学習する「インコンテキスト学

習」の一種です。数ショットプロンプトは、特定のフォーマット、推論、専門知識が必要なタスクに効果的です。「ゼロショットプロンプト」も参照してください。

FGAC

「きめ細かなアクセス制御」を参照してください。

きめ細かなアクセス制御 (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

変更データのキャプチャによる継続的なデータ複製を利用して、段階的なアプローチではなく、可能な限り短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。

FM

「基盤モデル」を参照してください。

基盤モデル (FM)

大規模な深層学習ニューラルネットワークであり、一般化およびラベル付けされていないデータからなる大規模データセットでトレーニングされています。FM により、言語理解、テキストおよび画像生成、自然言語での会話といった、一般的な各種タスクを実行できます。詳細については、「基盤モデルとは何ですか?」を参照してください。

G

生成 AI

AI モデルのサブセット。大量のデータでトレーニングされており、シンプルなテキストプロンプトを使用して、画像、動画、テキスト、オーディオなどの新しいコンテンツやアーティファクトを作成できます。詳細については、「生成 AI とは何ですか?」を参照してください。

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)

特定の国のユーザーがコンテンツ配信にアクセスできないようにするための、Amazon CloudFront のオプション。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 ワークフローは古いと見なされている方法であり、トランクベースのワークフローは推奨されている新しい方法です。

ゴールデンイメージ

システムまたはソフトウェアのスナップショットであり、システムまたはソフトウェアの新規インスタンスをデプロイするテンプレートとして使用されます。製造の例で言えば、ゴールデンイメージを使用すると、複数のデバイスにソフトウェアをプロビジョニングして、デバイス製造オペレーションの速度、スケーラビリティ、生産性を向上させることができます。

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 (OU) 全般のリソース、ポリシー、コンプライアンスを管理するのに役立つ概略的なルール。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、、 AWS Security Hub CSPM、Amazon GuardDuty、、 AWS Trusted Advisor Amazon Inspector、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。

高可用性 (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。

ホールドアウトデータ

機械学習モデルのトレーニング用データセットから保留される、ラベル付き履歴データの一部。ホールドアウトデータを使用すると、モデル予測をホールドアウトデータと比較して、モデルのパフォーマンスを評価できます。

同種データベースの移行

お客様の出典データベースを、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 (Microsoft SQL Server から Amazon RDS for SQL Server など) に移行する。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。緊急性が高いため、通常の DevOps のリリースワークフローからは外れた形で実施されます。

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 日間の平均的な CPU およびメモリ使用率が 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

「インダストリアル IoT」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

既存インフラストラクチャの更新、パッチ適用、変更などを行わずに、本番環境ワークロードに使用する新規インフラストラクチャをデプロイするモデル。本質的に、イミュータブルインフラストラクチャは、ミュータブルインフラストラクチャよりも一貫性、信頼性、予測性に優れています。詳細については、 AWS Well-Architected フレームワークにある「イミュータブルインフラストラクチャを使用してデプロイする」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 (受信) VPC

AWS マルチアカウントアーキテクチャでは、アプリケーションの外部からネットワーク接続を受け入れ、検査し、ルーティングする VPC。AWS Security Reference Architecture 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のインターフェイスを保護するために、インバウンド、アウトバウンド、インスペクションの各 VPC を使用してネットワークアカウントを設定することを推奨しています。

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 氏が提唱した用語で、接続、リアルタイムデータ、オートメーション、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意味します。

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。

インダストリアル IoT (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、「インダストリアル IoT (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。

インスペクション VPC

AWS マルチアカウントアーキテクチャでは、VPC (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を管理する一元化された VPCs。AWS Security Reference Architecture 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のインターフェイスを保護するために、インバウンド、アウトバウンド、インスペクションの各 VPC を使用してネットワークアカウントを設定することを推奨しています。

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、「 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。

IoT

「IoT」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 ITSM の基盤を提供します。

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

ラベルベースアクセス制御 (LBAC)

強制アクセス制御 (MAC) の実装で、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ます。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。

大規模言語モデル (LLM)

大量のデータで事前トレーニングされた深層学習 AI モデル。LLM では、質問への回答、ドキュメントの要約、他言語へのテキスト翻訳、文を完成させるなど、さまざまなタスクを実行できます。詳細については、「大規模言語モデル (LLM) とは何ですか?」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

「ラベルベースアクセス制御」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 Rs」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。「エンディアン性」もご覧ください。

LLM

「大規模言語モデル」を参照してください。

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やプライバシーを侵害するように設計されたソフトウェア。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、不正アクセスを招く可能性があります。マルウェアの例には、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 は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、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。マネージドサービスの例として、Amazon Simple Storage Service (Amazon S3) と Amazon DynamoDB が挙げられます。このサービスは、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、制御するソフトウェアシステムであり、工場では、これによって、原材料から製品を完成させます。

MAP

「Migration Acceleration Program」を参照してください。

メカニズム

ツールを作成してその導入を推進し、導入結果を調べて調整を行うための包括的なプロセス。メカニズムとは、運用中にそれ自体を強化し改善するサイクルを意味します。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

組織の一部である管理アカウント AWS アカウント 以外のすべて 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。

Message Queuing Telemetry Transport (MQTT)

発行/サブスクライブのパターンに基づく、軽量のマシンツーマシン (M2M) 通信プロトコルであり、リソースに限りのある IoT デバイスに使用されます。

マイクロサービス

明確に定義された API を介して通信し、通常は小規模な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です。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 API 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。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)

組織がクラウドに移行するための強力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、サービスを提供する AWS プログラム。MAP には、組織的な方法でレガシー移行を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および高速化する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、運用、ビジネスアナリストおよび所有者、移行エンジニア、デベロッパー、およびスプリントで作業する 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としては、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: AWS Application Migration Service を使用して Amazon EC2 への移行をリホストします。

Migration Portfolio Assessment (MPA)

オンラインツール。これによって、 AWS クラウドに移行するビジネスケースの検証に必要な情報を得られます。MPA は、詳細なポートフォリオ評価 (サーバーの適切なサイジング、価格設定、TCO 比較、移行コスト分析) および移行プラン (アプリケーションデータの分析とデータ収集、アプリケーションのグループ化、移行の優先順位付け、および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)

AWS CAF を使用して、組織のクラウド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。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 移行戦略の第一段階です。

移行戦略

ワークロードを AWS クラウドに移行するために使用するアプローチ。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、「AWS クラウドでのアプリケーションのモダナイズ戦略」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、「AWS クラウドで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評価する」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

「Migration Portfolio Assessment」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。

ミュータブルなインフラストラクチャ

本番ワークロードに使用する既存のインフラストラクチャを更新および変更するためのモデル。Well-Architected AWS フレームワークでは、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

「オリジンアクセス制御」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

「オペレーショナルレベルアグリーメント」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。

Open Process Communications - Unified Architecture (OPC-UA)

産業オートメーション用のマシンツーマシン (M2M) 通信プロトコル。OPC-UA により、相互運用の際に、データ暗号化、認証、認可の各スキームを標準化できます。

オペレーショナルレベルアグリーメント (OLA)

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

運用準備状況レビュー (ORR)

質問と関連するベストプラクティスのチェックリスト。インシデントや起こり得る障害を理解、評価、防止したり、その範囲を縮小したりする際に役立ちます。詳細については、 AWS Well-Architected フレームワークの「Operational Readiness Reviews (ORR)」を参照してください。

運用テクノロジー (OT)

産業オペレーション、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させるハードウェアおよびソフトウェアシステム。製造分野では、Industry 4.0 への変革を進める上で、OT と情報技術 (IT) システムの統合に焦点が当てられています。

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

組織 AWS アカウント 内のすべての のすべてのイベント AWS CloudTrail を ログに記録する 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、CloudTrail ドキュメントの「組織の証跡の作成」を参照してください。

組織変更管理 (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、移行問題に対処し、文化や組織の変化を推進することで、組織が新しいシステムと戦略の準備と移行するのを支援します。 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により、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。

オリジンアクセス制御 (OAC)

Amazon Simple Storage Service (Amazon S3) コンテンツを保護するための、CloudFront のアクセス制限の強化オプション。OAC は AWS リージョン、すべての S3 バケット、 AWS KMS (SSE-KMS) 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)

CloudFront の、Amazon S3 コンテンツを保護するためのアクセス制限オプション。OAI を使用すると、CloudFront が、Amazon S3 に認証可能なプリンシパルを作成します。認証されたプリンシパルは、S3 バケット内のコンテンツに、特定の CloudFront ディストリビューションを介してのみアクセスできます。OAC も併せて参照してください。OAC では、より詳細な、強化されたアクセス制御が可能です。

ORR

「運用準備状況レビュー」を参照してください。

OT

「運用テクノロジー」を参照してください。

アウトバウンド (送信) 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たネットワーク接続を処理する VPC。AWS Security Reference Architecture 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のインターフェイスを保護するために、インバウンド、アウトバウンド、インスペクションの各 VPC を使用してネットワークアカウントを設定することを推奨しています。

P

アクセス許可の境界

ユーザーまたはロールが使用できるアクセス許可の上限を設定する、IAM プリン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。PII の例には、氏名、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

「プログラマブル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

次の操作を可能にするオブジェクト: アクセス許可を定義する (ID ベースのポリシーを参照)。アクセス条件を指定する (リソースベースのポリシーを参照)。 AWS Organizations の組織における全アカウントにアクセス許可の上限を定義する (サービスコントロールポリシーを参照)。

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。

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、「移行の準備状況の評価」を参照してください。

述語

`true` または `false` を返すためのクエリ条件。一般的に、`WHERE` 句に記述されます。

述語プッシュダウン

データベースクエリを最適化する手法。これによって、転送前にクエリ内のデータをフィルタリングします。この手法を取ると、リレーショナルデータベースから取得し処理する必要のあるデータの量が減少するため、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、「AWSでのセキュリティコントロールの実装」の「予防的コントロール」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 AWS アカウントロール、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「ロールに関する用語と概念」にある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

開発プロセス全体を通してプライバシーが考慮されている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

1 つ以上の VPC 内のドメインとそのサブドメインへの DNS クエリに対し、Amazon Route 53 が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。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

非準拠リソースのデプロイ防止を目的としたセキュリティコントロール。このコントロールにより、プロビジョニング前にリソースをスキャンします。コントロールに準拠していないリソースは、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「 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)

製品の設計、開発、発売から、成長、成熟、衰退、廃棄に至る、製品のライフサイクル全体を通してデータとプロセスを管理すること。

本番環境

「環境」を参照してください。

プログラマブルロジックコントローラー (PLC)

製造分野で使用される、信頼性と適応性に優れたコンピュータであり、これによって、マシンをモニタリングするとともに、製造プロセスを自動化します。

プロンプトチェイニング

1 つの LLM プロンプトによる出力を次のプロンプトの入力に使用して、より良いレスポンスを生成します。この手法を使用すると、複雑なタスクをサブタスクに分割したり、事前レスポンスを繰り返し改良または拡張したりできます。これによって、モデルのレスポンスの精度と関連性が向上し、粒度の高いパーソナライズされた結果を得られます。

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。

発行/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。これにより、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 MES の場合、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可能なチャネルにイベントメッセージを発行できます。このシステムでは、発行サービスの変更なしに、新規マイクロサービスを追加できます。

Q

クエリプラン

手順などの一連のステップであり、SQL リレーショナルデータベースシステムのデータにアクセスするために使用されます。

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

「実行責任者、説明責任者、協業先、報告先 (RACI)」を参照してください。

RAG

「検索拡張生成」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

「実行責任者、説明責任者、協業先、報告先 (RACI)」を参照してください。

RCAC

「行と列のアクセス制御」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。

リアーキテクト

「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 Rs」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、「アカウントが使用できる AWS リージョン を指定する」を参照してください。

リグレッション

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 Rs」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 Rs」を参照してください。

リプラットフォーム

「7 Rs」を参照してください。

再購入

「7 Rs」を参照してください。

回復性

中断に抵抗または中断から回復するアプリケーションの機能。 AWS クラウドでの回復力を計画する際には、一般的に、高可用性とディザスタリカバリが考慮されます。詳細については、「AWS クラウド の耐障害性」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。

実行責任者、説明責任者、協業先、報告先 (RACI) に基づくマトリックス

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。サポートが含まれる場合は RASCI マトリックスと呼ばれ、含まれない場合は RACI マトリックスと呼ばれます。

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、「 AWSでのセキュリティコントロールの実装」の「レスポンシブコントロール」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。

検索拡張生成 (RAG)

生成 AI の技術。これにより、LLM では、レスポンスの生成前に、トレーニングデータソースの外部にある信頼できるデータソースが参照されます。例えば、RAG モデルによって、組織のナレッジベースまたはカスタムデータのセマンティック検索を実行できる場合があります。細については、「RAG (検索拡張生成) とは何ですか?」を参照してください。

ローテーション

定期的にシークレット情報を更新して、攻撃者が認証情報にアクセスするのをより困難にするプロセス。

行と列のアクセス制御 (RCAC)

アクセスルールが定義された、基本的で柔軟な SQL 表現の使用。RCAC は行権限と列マスクで構成されています。

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 (IdP) が使用しているオープンスタンダード。この機能を使用すると、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、ユーザーは組織内のすべてのユーザーを IAM で作成しなくても、 AWS マネジメントコンソール にログインしたり AWS 、API オペレーションを呼び出すことができます。SAML 2.0 ベースのフェデレーションの詳細については、IAM ドキュメントの「SAML 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

「監視制御とデータ取得」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

暗号化された形式で保存するパスワードやユーザー認証情報などの AWS Secrets Manager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。シークレット値には、バイナリ、1 つの文字列、複数の文字列を指定できます。詳細については、Secrets Manager ドキュメントの「Secrets Manager シークレットの概要」を参照してください。

セキュリティバイデザイン

開発プロセス全体を通してセキュリティが考慮されているシステムエンジニアリングのアプローチ。

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、主に 4 つの種類があります。4 つとは、予防、検出、レスポンシブ、プロアクティブです。

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。

Security Information and Event Management (SIEM) システム

セキュリティ情報管理 (SIM) とセキュリティイベント管理 (SEM) の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、その他ソースからデータを収集、モニタリング、分析して、脅威やセキュリティ違反を検出し、アラートを発信します。

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への自動レスポンスまたは自動修復を目的として、事前定義および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には、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、認証情報の更新などがあります。

サーバー側の暗号化

送信先にあるデータの、それ AWS のサービス を受け取る 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。SCP は、管理者がユーザーまたはロールに委任するアクションに、ガードレールを定義したり、アクションの制限を設定したりします。SCP は、許可リストまたは拒否リストとして、許可または禁止するサービスやアクションを指定する際に使用できます。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

のエントリポイントの URL 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、スループットといった、サービスパフォーマンス面の指標。

サービスレベル目標 (SLO)

サービスレベルインジケータによって測定され、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

「Security Information and Event Management システム」を参照してください。

単一障害点 (SPOF)

特定のアプリケーションを構成する単一の重要なコンポーネントで発生し、システム稼働に支障をきたす可能性のある障害。

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。

スプリットアンドシードモデル

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、「AWS クラウドで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」を参照してください。

SPOF

「単一障害点」を参照してください。

スタースキーマ

データベースの編成構造を意味し、1 つの大きいファクトテーブルにトランザクションデータまたは測定データが保存され、1 つ以上の小さいディメンションテーブルにデータ属性が保存されます。この構造は、データウェアハウスやビジネスインテリジェンスを用途と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。このパターンの適用方法の例については、「コンテナと Amazon API Gateway を使用して、従来の Microsoft ASP.NET (ASMX) ウェブサービスを段階的にモダナイズ」を参照してください。

サブネット

VPC 内の IP アドレスの範囲。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。

監視制御とデータ取得 (SCADA)

製造分野において、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本番運用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

ユーザーとのやり取りをシミュレートして、起こり得る問題を検出したり、パフォーマンスをモニタリングしたりすることで、システムをテストします。Amazon CloudWatch Synthetics を使用すると、こうしたテストを作成できます。

システムプロンプト

コンテキスト、指示、ガイドラインなどを提示して、LLM に動作を指示する手法。システムプロンプトは、コンテキストを設定して、ユーザーとやり取りするルールを確立するのに有用です。

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

VPC とオンプレミスネットワークを相互接続するために使用できる、ネットワークの中継ハブ。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したサービスに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「 を他の AWS のサービス AWS Organizations 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 枚のピザを分け合えることができるくらい小さな 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できる、2 つの VPC 間の接続。詳細については、Amazon VPC ドキュメントの「VPC ピア機能とは」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

現在のレコードに何らかの形で関連している行のグループに計算を実行する SQL 関数。ウィンドウ関数は、移動平均を計算したり、現在の行の相対位置に基づいて他の行の値にアクセスするといったタスクの処理に役立ちます。

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

「Write-Once-Read-Many」を参照してください。

WQF

「AWS ワークロード資格フレームワーク」を参照してください

Write-Once-Read-Many (WORM)

データを 1 回のみ書き込むことで、データの削除や変更を防ぐストレージモデル。承認済みユーザーは、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

ゼロデイ脆弱性を悪用した攻撃 (一般的にマルウェアによる)。

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。

ゼロショットプロンプト

LLM にタスク実行の手順は提示するが、実行のガイドとして役立つ例 (ショット) は提示しない方法。LLM は、事前トレーニング済みの知識を使用してタスクを処理する必要があります。ゼロショットプロンプトの有効性は、タスクの複雑さとプロンプトの品質によって異なります。「数ショットプロンプト」も参照してください。

ゾンビアプリケーション

平均 CPU およびメモリ使用率が 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。