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

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。