AWS Key Management Service bewährte Verfahren

AWS Prescriptive Guidance

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Prescriptive Guidance: AWS Key Management Service bewährte Verfahren

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und die Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Einführung 1
Gezielte Geschäftsergebnisse 1
Über AWS KMS keys 3
Verwalten von Schlüsseln 5
Wahl eines Managementmodells 5
Auswahl der Schlüsseltypen 7
Auswahl eines Schlüsselspeichers 9
Löschen und Deaktivieren von KMS-Schlüsseln 10
Datenschutz 12
Verschlüsselung 12
Protokolldaten verschlüsseln 14
Standardmäßige Verschlüsselung 14
Datenbankverschlüsselung 16
PCI DSS-Datenverschlüsselung 17
Verwenden von KMS-Schlüsseln mit Amazon EC2 Auto Scaling 18
Schlüsselrotation 18
Symmetrische Schlüsselrotation 19
Schlüsselrotation für Amazon EBS 19
Schlüsselrotation für Amazon RDS 21
Schlüsselrotation für Amazon S3 21
Rotierende Schlüssel mit importiertem Material 22
Verwendung der AWS Encryption SDK 22
Identity and Access Management 24
Schlüsselrichtlinien und IAM-Richtlinien 24
Berechtigungen mit den geringsten Rechten 27
Rollenbasierte Zugriffskontrolle 29
Attributbasierte Zugriffskontrolle 30
Verschlüsselungskontext 31
Problembehandlung bei Berechtigungen 32
Erkennung und Überwachung 34
Überwachung von AWS KMS Vorgängen 34
Überwachung des Schlüsselzugriffs 36
Überwachung der Verschlüsselungseinstellungen 37
CloudWatch Alarme konfigurieren 38

Antworten automatisieren 38
Kosten und Abrechnung 40
Wichtige Speicherkosten 40
Amazon-S3-Bucket-Schlüssel 41
Zwischenspeichern von Datenschlüsseln 41
Alternativen 41
Verwaltung der Kosten für die Protokollierung 41
Ressourcen 43
AWS KMS Dokumentation 43
Tools 43
AWS Präskriptive Leitlinien 43
Strategien 43
Leitfäden 43
Muster 43
Mitwirkende 44
Verfassen 44
Überprüfend 44
Technisches Schreiben 44
Dokumentverlauf 45
..... xlvi

AWS Key Management Service bewährte Verfahren

Amazon Web Services (Mitwirkende)

März 2025 (Verlauf der Dokumente)

AWS Key Management Service (AWS KMS) ist ein verwalteter Dienst, mit dem Sie die kryptografischen Schlüssel, die zum Schutz Ihrer Daten verwendet werden, auf einfache Weise erstellen und kontrollieren können. Dieses Handbuch beschreibt, wie Sie es effektiv nutzen können, AWS KMS und bietet bewährte Verfahren. Es hilft Ihnen, die Konfigurationsoptionen zu vergleichen und das für Ihre Bedürfnisse am besten geeignete Set auszuwählen.

Dieser Leitfaden enthält Empfehlungen, wie Ihr Unternehmen sensible Informationen schützen und Signaturen für mehrere Anwendungsfälle implementieren kann. AWS KMS Es berücksichtigt aktuelle Empfehlungen, die die folgenden Dimensionen verwenden:

- Verwaltung von Schlüsseln — Delegierungsoptionen für die Verwaltung und Optionen zur Speicherung von Schlüsseln
- Datenschutz — Verschlüsseln Sie Daten in Ihren eigenen Anwendungen und AWS-Services nicht in Ihrem Namen
- Zugriffsmanagement — Verwendung AWS KMS wichtiger Richtlinien und AWS Identity and Access Management (IAM) -Richtlinien zur Implementierung einer rollenbasierten Zugriffskontrolle (RBAC) oder einer attributebasierten Zugriffskontrolle (ABAC).
- Architektur mit mehreren Konten und mehreren Regionen — Empfehlungen für groß angelegte Implementierungen.
- Abrechnung und Kostenmanagement — Überblick über Ihre Kosten und Nutzung sowie Empfehlungen zur Kostensenkung.
- Detective Controls — Überwachung des Status Ihrer KMS-Schlüssel, Verschlüsselungseinstellungen und verschlüsselter Daten.
- Reaktion auf Vorfälle — Korrektur von Fehlkonfigurationen, die zur Nichteinhaltung Ihrer Datenschutzrichtlinien führen.

Gezielte Geschäftsergebnisse

Ihre Daten sind ein wichtiger und sensibler Vermögenswert für Ihr Unternehmen. Mit AWS KMS verwalten Sie die kryptografischen Schlüssel, die zum Schutz und zur Überprüfung Ihrer Daten

verwendet werden. Sie kontrollieren, wie Ihre Daten verwendet werden, wer Zugriff darauf hat und wie sie verschlüsselt werden. Dieses Handbuch soll Entwicklern, Systemadministratoren und Sicherheitsexperten dabei helfen, bewährte Verschlüsselungsmethoden zu implementieren, mit denen Sie sensible Daten schützen können, die gespeichert oder übertragen werden AWS-Services. Wenn Sie die Empfehlungen in diesem Leitfaden verstehen und umsetzen, können Sie die Vertraulichkeit und Integrität von Daten in Ihrer gesamten AWS Umgebung fördern. Sie können Ihre Datenschutzanforderungen erfüllen, unabhängig davon, ob diese Anforderungen intern formuliert wurden oder ob Sie spezifische Anforderungen für ein Compliance- oder Validierungsprogramm haben. Weitere Informationen dazu, wie Sie Daten in Ihrer AWS Umgebung schützen AWS KMS können, finden Sie AWS-Services in der AWS KMS Dokumentation unter AWS KMS Verschlüsselung verwenden mit.

Über AWS KMS keys

AWS Key Management Service (AWS KMS) ermöglicht es Ihnen, kryptografische Schlüssel zu erstellen, die für Daten verwendet werden können, die Sie an den Dienst weitergeben. Der primäre Ressourcentyp ist der KMS-Schlüssel, von dem es drei Typen gibt:

- Symmetrische AES-Schlüssel (Advanced Encryption Standard) — Dies sind 256-Bit-Schlüssel, die im Galois Counter Mode (GCM) -Modus von AES verwendet werden. Diese Schlüssel ermöglichen die authentifizierte Verschlüsselung und Entschlüsselung von Daten mit einer Größe von weniger als 4 KB. Dies ist der gebräuchlichste Schlüsseltyp. Er wird verwendet, um andere Datenschlüssel zu schützen, z. B. solche, die in Ihren Anwendungen verwendet werden AWS-Services , oder um Daten in Ihrem Namen zu verschlüsseln.
- Asymmetrische RSA-Schlüssel oder Schlüssel mit elliptischer Kurve — Diese Schlüssel sind in verschiedenen Größen erhältlich und unterstützen viele Algorithmen. Je nach Algorithmus können sie zur Verschlüsselung und Entschlüsselung sowie zum Signieren und Überprüfen verwendet werden.
- Symmetrische Schlüssel für die Durchführung von HMAC-Vorgängen (Hash-Based Message Authentication Code) — Bei diesen Schlüsseln handelt es sich um 256-Bit-Schlüssel, die für Signier- und Überprüfungsvorgänge verwendet werden.

KMS-Schlüssel können nicht im Klartext aus dem Dienst exportiert werden. Sie werden von den vom Dienst verwendeten Hardware-Sicherheitsmodulen (HSMs) generiert und können nur innerhalb dieser verwendet werden. Dies ist eine grundlegende Sicherheitseigenschaft, um wichtige AWS KMS Sicherheitsbedrohungen zu verhindern. In den Regionen China (Peking) und China (Ningxia) HSMs sind diese von OSCCA zertifiziert. In allen anderen Regionen HSMs werden die verwendeten im AWS KMS Rahmen des FIPS 140-Programms innerhalb von NIST auf Sicherheitsstufe 3 validiert. Weitere Informationen zu Design und Kontrollen zum Schutz Ihrer Schlüssel finden Sie unter AWS Key Management Service Kryptografische Details. AWS KMS

Sie können Daten an senden, AWS KMS indem Sie verschiedene kryptografische APIs Daten verwenden, um Vorgänge mit KMS-Schlüsseln zu verschlüsseln, zu entschlüsseln, zu signieren oder zu verifizieren. Sie können sich auch dafür entscheiden, dass ein KMS-Schlüssel wie ein Schlüsselverschlüsselungsschlüssel funktioniert, der einen Schlüsseltyp schützt, der als Datenschlüssel bezeichnet wird. Ein Datenschlüssel kann AWS KMS für die Verwendung in Ihrer lokalen Anwendung oder in einer Anwendung AWS-Service , die Daten in Ihrem Namen schützt, exportiert werden. Die Verwendung von Datenschlüsseln ist in allen

Schlüsselverwaltungssystemen üblich und wird häufig als Envelope-Verschlüsselung bezeichnet. Durch die Umschlagverschlüsselung kann ein Datenschlüssel auf dem Remotesystem verwendet werden, das Ihre vertraulichen Daten verarbeitet, anstatt Ihre vertraulichen Daten direkt mit einem KMS-Schlüssel AWS KMS zur Verschlüsselung an dieses senden zu müssen.

Weitere Informationen finden Sie AWS KMS keysin der AWS KMS Dokumentation unter Grundlagen der AWS KMS Kryptografie.

Bewährte Methoden für die Schlüsselverwaltung für AWS KMS

Wenn Sie AWS Key Management Service (AWS KMS) verwenden, müssen Sie einige grundlegende Entwurfsentscheidungen treffen. Dazu gehören, ob ein zentrales oder dezentrales Modell für die Schlüsselverwaltung und den Zugriff verwendet werden soll, die Art der zu verwendenden Schlüssel und die Art des zu verwendenden Schlüsselspeichers. Die folgenden Abschnitte helfen Ihnen dabei, die richtigen Entscheidungen für Ihr Unternehmen und Ihre Anwendungsfälle zu treffen. Dieser Abschnitt schließt mit wichtigen Überlegungen zum Deaktivieren und Löschen von KMS-Schlüsseln, einschließlich Maßnahmen, die Sie zum Schutz Ihrer Daten und Schlüssel ergreifen sollten.

In diesem Abschnitt werden folgende Themen behandelt:

- Wählen Sie ein zentralisiertes oder dezentrales Modell
- Auswahl von kundenverwalteten Schlüsseln, AWS verwalteten Schlüsseln oder AWS eigenen Schlüsseln
- Auswahl eines AWS KMS Schlüsselgeschäfts
- Löschen und Deaktivieren von KMS-Schlüsseln

Wählen Sie ein zentralisiertes oder dezentrales Modell

AWS empfiehlt, mehrere Konten zu verwenden AWS-Konten und diese als eine einzige Organisation in zu verwalten AWS Organizations. Für die Verwaltung AWS KMS keys in Umgebungen mit mehreren Konten gibt es zwei allgemeine Ansätze.

Der erste Ansatz ist ein dezentraler Ansatz, bei dem Sie Schlüssel für jedes Konto erstellen, das diese Schlüssel verwendet. Wenn Sie die KMS-Schlüssel in denselben Konten speichern wie die Ressourcen, die sie schützen, ist es einfacher, Berechtigungen an lokale Administratoren zu delegieren, die die Zugriffsanforderungen für ihre AWS Prinzipale und Schlüssel kennen. Sie können die Schlüsselverwendung autorisieren, indem Sie nur eine Schlüsselrichtlinie verwenden, oder Sie können eine Schlüsselrichtlinie und identitätsbasierte Richtlinien in (IAM) kombinieren. AWS Identity and Access Management

Bei der zweiten Methode handelt es sich um einen zentralisierten Ansatz, bei dem Sie KMS-Schlüssel in einem oder mehreren bestimmten Kategorien verwalten. AWS-Konten Sie erlauben anderen Konten, die Schlüssel nur für kryptografische Operationen zu verwenden. Sie verwalten

Schlüssel, ihren Lebenszyklus und ihre Berechtigungen von einem zentralen Konto aus. Sie gestatten anderen AWS-Konten die Verwendung des Schlüssels, gewähren jedoch keine anderen Berechtigungen. Die externen Konten können nichts über den Lebenszyklus oder die Zugriffsberechtigungen des Schlüssels verwalten. Dieses zentralisierte Modell kann dazu beitragen, das Risiko einer unbeabsichtigten Löschung von Schlüsseln oder einer Rechteerweiterung durch delegierte Administratoren oder Benutzer zu minimieren.

Welche Option Sie wählen, hängt von mehreren Faktoren ab. Beachten Sie bei der Auswahl eines Ansatzes Folgendes:

1. Verfügen Sie über einen automatisierten oder manuellen Prozess für die Bereitstellung von Schlüssel- und Ressourcenzugriffen? Dazu gehören Ressourcen wie Bereitstellungspipelines und IaC-Vorlagen (Infrastructure as Code). Diese Tools können Ihnen helfen, Ressourcen (wie KMS-Schlüssel, wichtige Richtlinien, IAM-Rollen und IAM-Richtlinien) in vielen Bereichen bereitzustellen und zu verwalten. AWS-Konten Wenn Sie nicht über diese Bereitstellungstools verfügen, ist ein zentralisierter Ansatz für die Schlüsselverwaltung für Ihr Unternehmen möglicherweise einfacher zu handhaben.
2. Haben Sie die administrative Kontrolle über alle Ressourcen AWS-Konten , die KMS-Schlüssel verwenden? Falls ja, kann ein zentralisiertes Modell die Verwaltung vereinfachen und den Wechsel AWS-Konten zur Schlüsselverwaltung überflüssig machen. Beachten Sie jedoch, dass IAM-Rollen und Benutzerberechtigungen zur Verwendung von Schlüsseln weiterhin pro Konto verwaltet werden müssen.
3. Müssen Sie Kunden oder Partnern, die über eigene AWS-Konten Ressourcen verfügen, Zugriff auf Ihre KMS-Schlüssel gewähren? Bei diesen Schlüsseln kann ein zentralisierter Ansatz den Verwaltungsaufwand für Ihre Kunden und Partner reduzieren.
4. Haben Sie Autorisierungsanforderungen für den Zugriff auf AWS Ressourcen, die besser durch einen zentralen oder lokalen Zugriffsansatz gelöst werden können? Wenn beispielsweise verschiedene Anwendungen oder Geschäftsbereiche für die Verwaltung der Sicherheit ihrer eigenen Daten verantwortlich sind, ist ein dezentraler Ansatz für die Schlüsselverwaltung besser.
5. Überschreiten Sie die Kontingente für Serviceressourcen AWS KMS? Da diese Kontingente pro Person festgelegt sind AWS-Konto, verteilt ein dezentrales Modell die Last auf die Konten, wodurch die Servicekontingente effektiv vervielfacht werden.

> **Note**
>
> Das Verwaltungsmodell für Schlüssel ist irrelevant, wenn es um Anforderungskontingente geht, da diese Kontingente für den Hauptbenutzer gelten, der eine Anfrage für den Schlüssel stellt, und nicht für das Konto, das den Schlüssel besitzt oder verwaltet.

Im Allgemeinen empfehlen wir, mit einem dezentralen Ansatz zu beginnen, es sei denn, Sie können die Notwendigkeit eines zentralisierten KMS-Schlüsselmodells artikulieren.

Auswahl von kundenverwalteten Schlüsseln, AWS verwalteten Schlüsseln oder AWS eigenen Schlüsseln

Die KMS-Schlüssel, die Sie für die Verwendung in Ihren eigenen kryptografischen Anwendungen erstellen und verwalten, werden als vom Kunden verwaltete Schlüssel bezeichnet. AWS-Services kann vom Kunden verwaltete Schlüssel verwenden, um die Daten zu verschlüsseln, die der Dienst in Ihrem Namen speichert. Vom Kunden verwaltete Schlüssel werden empfohlen, wenn Sie die volle Kontrolle über den Lebenszyklus und die Verwendung Ihrer Schlüssel haben möchten. Es fallen monatliche Kosten an, wenn Sie einen vom Kunden verwalteten Schlüssel in Ihrem Konto haben. Darüber hinaus fallen bei Anfragen zur Verwendung oder Verwaltung des Schlüssels Nutzungskosten an. Weitere Informationen finden Sie unter AWS KMS Preise.

Wenn Sie Ihre Daten verschlüsseln AWS-Service möchten, aber nicht den Aufwand oder die Kosten für die Schlüsselverwaltung in Anspruch nehmen möchten, können Sie einen AWS verwalteten Schlüssel verwenden. Diese Art von Schlüssel ist in Ihrem Konto vorhanden, kann jedoch nur unter bestimmten Umständen verwendet werden. Er kann nur in dem Kontext verwendet werden AWS-Service , in dem Sie tätig sind, und er kann nur von Prinzipalen innerhalb des Kontos verwendet werden, das den Schlüssel enthält. Sie können nichts über den Lebenszyklus oder die Berechtigungen dieser Schlüssel verwalten. Manche AWS-Services verwenden AWS verwaltete Schlüssel. Das Format eines Alias für AWS verwaltete Schlüssel ist`aws/<service code>`. Ein `aws/ebs` Schlüssel kann beispielsweise nur zur Verschlüsselung von Amazon Elastic Block Store (Amazon EBS) -Volumes verwendet werden, die sich in demselben Konto wie der Schlüssel befinden, und kann nur von IAM-Prinzipalen in diesem Konto verwendet werden. Ein AWS verwalteter Schlüssel kann nur von Benutzern in diesem Konto und für Ressourcen in diesem Konto verwendet werden. Sie können Ressourcen, die unter einem AWS verwalteten Schlüssel verschlüsselt wurden, nicht mit anderen Konten teilen. Wenn dies eine Einschränkung für Ihren

Anwendungsfall darstellt, empfehlen wir, stattdessen einen vom Kunden verwalteten Schlüssel zu verwenden. Sie können diesen Schlüssel mit jedem anderen Konto teilen. Das Vorhandensein eines AWS verwalteten Schlüssels in Ihrem Konto wird Ihnen nicht in Rechnung gestellt, aber die Nutzung dieses Schlüsseltyps durch die Person AWS-Service , die dem Schlüssel zugewiesen ist, wird Ihnen in Rechnung gestellt.

Ein AWS verwalteter Schlüssel ist ein veralteter Schlüsseltyp, der ab 2021 nicht mehr für neue AWS-Services Schlüssel erstellt wird. Stattdessen verwenden neue (und ältere) AWS-Services standardmäßig einen AWS eigenen Schlüssel, um Ihre Daten zu verschlüsseln. AWS Eigene Schlüssel sind eine Sammlung von KMS-Schlüsseln, die ein AWS-Service Unternehmen besitzt und verwaltet, sodass sie in mehreren AWS-Konten Fällen verwendet werden können. Diese Schlüssel befinden sich zwar nicht in Ihrem AWS-Konto, aber Sie AWS-Service können einen verwenden, um die Ressourcen in Ihrem Konto zu schützen.

Wir empfehlen Ihnen, vom Kunden verwaltete Schlüssel zu verwenden, wenn eine detaillierte Kontrolle am wichtigsten ist, und AWS eigene Schlüssel zu verwenden, wenn der Komfort am wichtigsten ist.

In der folgenden Tabelle werden die wichtigsten Richtlinien-, Protokollierungs-, Verwaltungs- und Preisunterschiede zwischen den einzelnen Schlüsseltypen beschrieben. Weitere Informationen zu Schlüsseltypen finden Sie unter AWS KMS Konzepte.

Überlegungen	Kundenseitig verwaltete Schlüssel	AWS verwaltete Schlüssel	AWS eigene Schlüssel
Schlüsselrichtlinie	Ausschließlich vom Kunden kontrolliert	Wird vom Service gesteuert; vom Kunden einsehbar	Ausschließlich kontrolliert und nur sichtbar von AWS-Service demjenige n, der Ihre Daten verschlüsselt
Protokollierung	AWS CloudTrail Speicherung von Kundendaten oder Veranstaltungsdaten	CloudTrail Datenspei cher für Kundendaten oder Ereignisse	Für den Kunden nicht sichtbar

Überlegungen	Kundenseitig verwaltete Schlüssel	AWS verwaltete Schlüssel	AWS eigene Schlüssel
Lebenszyklusmanagement	Der Kunde verwaltet Rotation, Löschung und AWS-Region	AWS-Service verwaltet Rotation (jährlich), Löschung und Region	AWS-Service verwaltet Rotation (jährlich), Löschung und Region
Preise	Monatliche Gebühr für die Existenz des Schlüssels (anteilig pro Stunde); die API-Nutzung wird dem Anrufer in Rechnung gestellt	Keine Gebühr für die Existenz des Schlüssels; dem Anrufer wird die API-Nutzung in Rechnung gestellt	Keine Gebühren für den Kunden

Auswahl eines AWS KMS Schlüsselgeschäfts

Ein Schlüsselspeicher ist ein sicherer Ort für die Speicherung und Verwendung von kryptografischem Schlüsselmaterial. Die branchenweit bewährte Methode für Schlüsselspeicher besteht darin, ein als Hardware-Sicherheitsmodul (HSM) bezeichnetes Gerät zu verwenden, das gemäß dem NIST Federal Information Processing Standards (FIPS) 140 zur Validierung kryptografischer Module auf Sicherheitsstufe 3 validiert wurde. Es gibt andere Programme zur Unterstützung von Schlüsselspeichern, die zur Zahlungsabwicklung verwendet werden. AWS Payment Cryptographyist ein Dienst, mit dem Sie Daten im Zusammenhang mit Ihren Zahlungsaufgaben schützen können.

AWS KMS unterstützt mehrere Schlüsselspeichertypen, um Ihr Schlüsselmaterial bei der Erstellung und Verwaltung Ihrer Verschlüsselungsschlüssel AWS KMS zu schützen. Alle von bereitgestellten Schlüsselspeicheroptionen AWS KMS werden kontinuierlich gemäß FIPS 140 auf Sicherheitsstufe 3 validiert. Sie sind so konzipiert, dass niemand, auch keine AWS Bediener, auf Ihre Klartext-Schlüssel zugreifen oder sie ohne Ihre Zustimmung verwenden kann. Weitere Informationen zu den verfügbaren Typen von Schlüsselspeichern finden Sie in der AWS KMS Dokumentation unter Schlüsselspeicher.

Der AWS KMS Standard-Schlüsselspeicher ist für die meisten Workloads die beste Wahl. Wenn Sie sich für eine andere Art von Schlüsselspeicher entscheiden müssen, sollten Sie sorgfältig abwägen,

ob gesetzliche oder andere Anforderungen (z. B. interne) diese Wahl erfordern, und wägen Sie die Kosten und Vorteile sorgfältig ab.

Löschen und Deaktivieren von KMS-Schlüsseln

Das Löschen eines KMS-Schlüssels kann erhebliche Auswirkungen haben. Bevor Sie einen KMS-Schlüssel löschen, den Sie nicht mehr verwenden möchten, sollten Sie überlegen, ob es ausreichend ist, den Schlüsselstatus auf Deaktiviert zu setzen. Solange ein Schlüssel deaktiviert ist, kann er nicht für kryptografische Operationen verwendet werden. Es ist immer noch vorhanden und Sie können es bei Bedarf in future wieder aktivieren. AWS Für deaktivierte Schlüssel fallen weiterhin Speichergebühren an. Wir empfehlen, Schlüssel zu deaktivieren, anstatt sie zu löschen, bis Sie sicher sind, dass der Schlüssel keine Daten oder Datenschlüssel schützt.

> **Important**
>
> Das Löschen eines Schlüssels muss sorgfältig geplant werden. Daten können nicht entschlüsselt werden, wenn der entsprechende Schlüssel gelöscht wurde. AWS hat keine Möglichkeit, einen gelöschten Schlüssel wiederherzustellen, nachdem er gelöscht wurde. Wie bei anderen wichtigen Vorgängen in sollten Sie eine Richtlinie anwenden AWS, die einschränkt, wer Schlüssel für das Löschen planen kann und für das Löschen von Schlüsseln eine Multi-Faktor-Authentifizierung (MFA) vorschreibt.

Um ein versehentliches Löschen von Schlüsseln zu verhindern AWS KMS , wird eine standardmäßige Mindestwartezeit von sieben Tagen nach der Ausführung eines `DeleteKey` Anrufs eingeführt, bevor der Schlüssel gelöscht wird. Sie können die Wartezeit auf einen Höchstwert von 30 Tagen festlegen. Während der Wartezeit befindet sich der Schlüssel weiterhin AWS KMS im Status Ausstehende Löschung. Er kann nicht für Ver- oder Entschlüsselungsvorgänge verwendet werden. Jeder Versuch, einen Schlüssel, der sich im Status „Ausstehende Löschung“ befindet, für die Verschlüsselung oder Entschlüsselung zu verwenden, wird protokolliert. AWS CloudTrail Sie können in Ihren CloudTrail Protokollen einen CloudWatch Amazon-Alarm für diese Ereignisse einrichten. Wenn Sie bei diesen Ereignissen Alarme erhalten, können Sie den Löschvorgang bei Bedarf abbrechen. Bis zum Ablauf der Wartezeit können Sie den Schlüssel aus dem Status Ausstehende Löschung wiederherstellen und ihn entweder in den Status Deaktiviert oder Aktiviert zurückversetzen.

Um einen Schlüssel für mehrere Regionen zu löschen, müssen Sie die Replikate vor der ursprünglichen Kopie löschen. Weitere Informationen finden Sie unter Schlüssel für mehrere Regionen löschen.

Wenn Sie einen Schlüssel mit importiertem Schlüsselmaterial verwenden, können Sie das importierte Schlüsselmaterial sofort löschen. Dies unterscheidet sich in mehrfacher Hinsicht vom Löschen eines KMS-Schlüssels. Wenn Sie die `DeleteImportedKeyMaterial` Aktion ausführen, AWS KMS wird das Schlüsselmaterial gelöscht, und der Schlüsselstatus wird auf Ausstehender Import geändert. Nachdem Sie das Schlüsselmaterial gelöscht haben, ist der Schlüssel sofort unbrauchbar. Es gibt keine Wartezeit. Um die Verwendung des Schlüssels wieder zu ermöglichen, müssen Sie dasselbe Schlüsselmaterial erneut importieren. Die Wartezeit für das Löschen von KMS-Schlüsseln gilt auch für KMS-Schlüssel mit importiertem Schlüsselmaterial.

Wenn Datenschlüssel durch einen KMS-Schlüssel geschützt sind und von diesem aktiv verwendet werden AWS-Services, wirkt sich dies nicht unmittelbar darauf aus, wenn der zugehörige KMS-Schlüssel deaktiviert oder das importierte Schlüsselmaterial gelöscht wird. Nehmen wir beispielsweise an, dass ein Schlüssel mit importiertem Material verwendet wurde, um ein Objekt mit SSE-KMS zu verschlüsseln. Sie laden das Objekt in einen Amazon Simple Storage Service (Amazon S3) -Bucket hoch. Bevor Sie das Objekt in den Bucket hochladen, importieren Sie das Material in Ihren Schlüssel. Nachdem das Objekt hochgeladen wurde, löschen Sie das importierte Schlüsselmaterial aus diesem Schlüssel. Das Objekt verbleibt in verschlüsseltem Zustand im Bucket, aber niemand kann auf das Objekt zugreifen, bis das gelöschte Schlüsselmaterial erneut in den Schlüssel importiert wurde. Dieser Ablauf erfordert zwar eine präzise Automatisierung für den Import und das Löschen von Schlüsselmaterial aus einem Schlüssel, kann aber ein zusätzliches Maß an Kontrolle innerhalb einer Umgebung bieten.

AWS bietet ausführliche Anleitungen, die Sie dabei unterstützen, das geplante Löschen von KMS-Schlüsseln zu überwachen und (falls erforderlich) zu korrigieren. Weitere Informationen finden Sie unter Überwachen und Korrigieren des geplanten Löschens von Schlüsseln. AWS KMS

Bewährte Datenschutzpraktiken für AWS KMS

Dieser Abschnitt hilft Ihnen dabei, Entscheidungen über die Verwendung von AWS Key Management Service (AWS KMS) Schlüsseln für den Datenschutz zu treffen, z. B. welche Schlüssel für jeden Datentyp verwendet werden sollen. Es enthält auch konkrete Beispiele für die Verwendung AWS KMS mit verschiedenen AWS-Services. Diese Empfehlungen und Beispiele helfen Ihnen zu verstehen, wie viele Schlüssel Sie möglicherweise benötigen und welche Prinzipale Berechtigungen für die Verwendung dieser Schlüssel benötigen.

In diesem Abschnitt wird auch die Schlüsselrotation behandelt. Bei der Schlüsselrotation wird entweder ein vorhandener KMS-Schlüssel durch einen neuen Schlüssel ersetzt oder das mit einem vorhandenen KMS-Schlüssel verknüpfte kryptografische Material durch neues Material ersetzt. Dieses Handbuch enthält Beispiele und Anweisungen für die Rotation von KMS-Schlüsseln für häufig verwendete AWS-Services Schlüssel. Die Empfehlungen und Beispiele sollen Ihnen helfen, fundierte Entscheidungen über Ihre Strategie zur Schlüsselrotation zu treffen.

Schließlich enthält dieser Abschnitt Empfehlungen zur Verwendung von AWS Encryption SDK, einem Tool zur Implementierung der clientseitigen Verschlüsselung in Ihren Anwendungen. Dieser Abschnitt enthält Entwurfsentscheidungen, die Sie auf der Grundlage des Funktionsumfangs und der Fähigkeiten von treffen können. AWS Encryption SDK

In diesem Abschnitt werden die folgenden Verschlüsselungsthemen behandelt:

- Verschlüsselung mit AWS KMS
- Rotation der wichtigsten Faktoren AWS KMS und Umfang der Auswirkungen
- Empfehlungen für die Verwendung des AWS Encryption SDK

Verschlüsselung mit AWS KMS

Verschlüsselung ist eine allgemein bewährte Methode zum Schutz der Vertraulichkeit und Integrität vertraulicher Informationen. Sie sollten Ihre bestehenden Datenklassifizierungsebenen verwenden und mindestens einen AWS Key Management Service (AWS KMS) Schlüssel pro Ebene verwenden. Sie könnten beispielsweise einen KMS-Schlüssel für Daten definieren, die als vertraulich eingestuft sind, einen für nur intern und einen für vertrauliche Daten. Auf diese Weise können Sie sicherstellen, dass nur autorisierte Benutzer berechtigt sind, die Schlüssel zu verwenden, die jeder Klassifizierungsebene zugeordnet sind.

> **Note**
>
> Ein einziger vom Kunden verwalteter KMS-Schlüssel kann für jede Kombination von AWS-Services oder für Ihre eigenen Anwendungen verwendet werden, die Daten einer bestimmten Klassifizierung speichern. Der limitierende Faktor bei der Verwendung eines Schlüssels für mehrere Workloads AWS-Services besteht darin, wie komplex die Nutzungsberechtigungen sein müssen, um den Zugriff auf die Daten für eine Gruppe von Benutzern zu kontrollieren. Das JSON-Dokument mit den AWS KMS wichtigsten Richtlinien muss weniger als 32 KB groß sein. Wenn diese Größenbeschränkung zu einer Beschränkung wird, sollten Sie erwägen, AWS KMS Zuschüsse zu verwenden oder mehrere Schlüssel zu erstellen, um die Größe des wichtigsten Richtliniendokuments zu minimieren.

Anstatt sich bei der Partitionierung Ihres KMS-Schlüssels nur auf die Datenklassifizierung zu verlassen, können Sie auch einen KMS-Schlüssel zuweisen, der für eine Datenklassifizierung innerhalb eines einzelnen Schlüssels verwendet wird AWS-Service. Beispielsweise sollten alle `Sensitive` in Amazon Simple Storage Service (Amazon S3) markierten Daten unter einem KMS-Schlüssel verschlüsselt werden, der einen Namen wie hat`S3-Sensitive`. Sie können Ihre Daten innerhalb Ihrer definierten Datenklassifizierung AWS-Service und/oder Anwendung weiter auf mehrere KMS-Schlüssel verteilen. Beispielsweise können Sie möglicherweise einige Datensätze in einem bestimmten Zeitraum und andere Datensätze in einem anderen Zeitraum löschen. Mithilfe von Ressourcen-Tags können Sie Daten identifizieren und sortieren, die mit bestimmten KMS-Schlüsseln verschlüsselt sind.

Wenn Sie sich für ein dezentrales Verwaltungsmodell für KMS-Schlüssel entscheiden, sollten Sie Schutzmaßnahmen ergreifen, um sicherzustellen, dass neue Ressourcen mit einer bestimmten Klassifizierung erstellt werden, und die erwarteten KMS-Schlüssel mit den richtigen Berechtigungen verwenden. Weitere Informationen darüber, wie Sie die Ressourcenkonfiguration mithilfe von Automatisierung erzwingen, erkennen und verwalten können, finden Sie im Erkennung und Überwachung Abschnitt dieses Handbuchs.

In diesem Abschnitt werden die folgenden Verschlüsselungsthemen behandelt:

- Verschlüsselung von Protokolldaten mit AWS KMS
- Standardmäßige Verschlüsselung
- Datenbankverschlüsselung mit AWS KMS
- PCI-DSS-Datenverschlüsselung mit AWS KMS

- Verwenden von KMS-Schlüsseln mit Amazon EC2 Auto Scaling

Verschlüsselung von Protokolldaten mit AWS KMS

Viele AWS-Services, wie Amazon GuardDuty und AWS CloudTrail, bieten Optionen zum Verschlüsseln von Protokolldaten, die an Amazon S3 gesendet werden. Wenn Sie Ergebnisse von GuardDuty nach Amazon S3 exportieren, müssen Sie einen KMS-Schlüssel verwenden. Wir empfehlen, dass Sie alle Protokolldaten verschlüsseln und nur autorisierten Benutzern wie Sicherheitsteams, Incident-Respondern und Auditoren Zugriff auf die Entschlüsselung gewähren.

Die AWS Security Reference Architecture empfiehlt die Einrichtung einer zentralen Stelle für die Protokollierung. AWS-Konto Auf diese Weise können Sie auch den Aufwand für die Schlüsselverwaltung reduzieren. Mit können Sie CloudTrail beispielsweise einen Organisationspfad oder einen Ereignisdatenspeicher erstellen, um Ereignisse in Ihrer gesamten Organisation zu protokollieren. Wenn Sie Ihren organisatorischen Trail- oder Event-Datenspeicher konfigurieren, können Sie einen einzelnen Amazon S3 S3-Bucket und einen KMS-Schlüssel in Ihrem angegebenen Logging-Konto angeben. Diese Konfiguration gilt für alle Mitgliedskonten in der Organisation. Alle Konten senden dann ihre CloudTrail Protokolle an den Amazon S3 S3-Bucket im Protokollierungskonto, und die Protokolldaten werden mit dem angegebenen KMS-Schlüssel verschlüsselt. Sie müssen die Schlüsselrichtlinie für diesen KMS-Schlüssel aktualisieren, um CloudTrail die erforderlichen Berechtigungen für die Verwendung des Schlüssels zu gewähren. Weitere Informationen finden Sie CloudTrail in der CloudTrail Dokumentation unter AWS KMS Schlüsselrichtlinien konfigurieren für.

Zum Schutz der GuardDuty CloudTrail UND-Protokolle müssen sich der Amazon S3 S3-Bucket und der KMS-Schlüssel im selben Verzeichnis befinden AWS-Region. Die AWS Security Reference Architecture bietet auch Anleitungen zur Protokollierung und zu Architekturen mit mehreren Konten. Wenn Sie Logs über mehrere Regionen und Konten hinweg aggregieren, lesen Sie in der CloudTrail Dokumentation unter Erstellen eines Pfads für eine Organisation mehr über Opt-in-Regionen und stellen Sie sicher, dass Ihre zentralisierte Protokollierung wie vorgesehen funktioniert.

Standardmäßige Verschlüsselung

AWS-Services die Daten speichern oder verarbeiten, bieten in der Regel Verschlüsselung im Ruhezustand. Diese Sicherheitsfunktion trägt zum Schutz Ihrer Daten bei, indem sie verschlüsselt werden, wenn sie nicht verwendet werden. Autorisierte Benutzer können bei Bedarf weiterhin darauf zugreifen.

Die Implementierungs- und Verschlüsselungsoptionen variieren je nach Region AWS-Services. Viele bieten standardmäßig Verschlüsselung. Es ist wichtig zu verstehen, wie die Verschlüsselung für jeden Dienst funktioniert, den Sie verwenden. Im Folgenden sind einige Beispiele aufgeführt:

- Amazon Elastic Block Store (Amazon EBS) — Wenn Sie die Verschlüsselung standardmäßig aktivieren, werden alle neuen Amazon EBS-Volumes und Snapshot-Kopien verschlüsselt. AWS Identity and Access Management (IAM) -Rollen oder Benutzer können keine Instances mit unverschlüsselten Volumes oder Volumes starten, die keine Verschlüsselung unterstützen. Diese Funktion hilft bei Sicherheit, Compliance und Prüfung, indem sie sicherstellt, dass alle auf Amazon EBS-Volumes gespeicherten Daten verschlüsselt sind. Weitere Informationen zur Verschlüsselung in diesem Service finden Sie unter Amazon EBS-Verschlüsselung in der Amazon EBS-Dokumentation.
- Amazon Simple Storage Service (Amazon S3) — Alle neuen Objekte werden standardmäßig verschlüsselt. Amazon S3 wendet für jedes neue Objekt automatisch eine serverseitige Verschlüsselung mit verwalteten Amazon S3 S3-Schlüsseln (SSE-S3) an, sofern Sie keine andere Verschlüsselungsoption angeben. IAM-Prinzipale können weiterhin unverschlüsselte Objekte auf Amazon S3 hochladen, indem sie dies im API-Aufruf ausdrücklich angeben. Um in Amazon S3 die SSE-KMS-Verschlüsselung durchzusetzen, müssen Sie eine Bucket-Richtlinie mit Bedingungen verwenden, die eine Verschlüsselung erfordern. Eine Beispielrichtlinie finden Sie in der Amazon S3 S3-Dokumentation unter SSE-KMS für alle in einen Bucket geschriebenen Objekte erforderlich. Einige Amazon S3 S3-Buckets empfangen und bedienen eine große Anzahl von Objekten. Wenn diese Objekte mit KMS-Schlüsseln verschlüsselt sind, führt eine große Anzahl von Amazon S3 S3-Vorgängen zu einer großen Anzahl von `GenerateDataKey` `Decrypt` AND-Aufrufen AWS KMS. Dies kann die Gebühren erhöhen, die Ihnen für die AWS KMS Nutzung entstehen. Sie können Amazon S3 S3-Bucket-Keys konfigurieren, was Ihre AWS KMS Kosten erheblich senken kann. Weitere Informationen zur Verschlüsselung in diesem Service finden Sie unter Schützen von Daten durch Verschlüsselung in der Amazon S3 S3-Dokumentation.
- Amazon DynamoDB — DynamoDB ist ein vollständig verwalteter NoSQL-Datenbankservice, der standardmäßig serverseitige Verschlüsselung im Ruhezustand aktiviert, und Sie können ihn nicht deaktivieren. Wir empfehlen Ihnen, einen vom Kunden verwalteten Schlüssel für die Verschlüsselung Ihrer DynamoDB-Tabellen zu verwenden. Dieser Ansatz hilft Ihnen bei der Implementierung der geringsten Rechte mit detaillierten Berechtigungen und Aufgabentrennung, indem Sie in Ihren wichtigsten Richtlinien auf bestimmte IAM-Benutzer und Rollen abzielen. AWS KMS Sie können bei der Konfiguration der Verschlüsselungseinstellungen für Ihre DynamoDB-Tabellen auch AWS verwaltete oder AWS eigene Schlüssel wählen. Für Daten, die ein hohes Maß an Schutz erfordern (bei denen Daten nur als Klartext für den Client sichtbar sein sollten), sollten

Sie die clientseitige Verschlüsselung mit dem Database Encryption SDK in Betracht ziehen.AWS Weitere Informationen zur Verschlüsselung in diesem Dienst finden Sie unter Datenschutz in der DynamoDB-Dokumentation.

Datenbankverschlüsselung mit AWS KMS

Die Ebene, auf der Sie die Verschlüsselung implementieren, wirkt sich auf die Datenbankfunktionalität aus. Im Folgenden sind die Kompromisse aufgeführt, die Sie berücksichtigen müssen:

- Wenn Sie nur AWS KMS Verschlüsselung verwenden, ist der Speicher, der Ihre Tabellen sichert, für DynamoDB und Amazon Relational Database Service (Amazon RDS) verschlüsselt. Das bedeutet, dass das Betriebssystem, auf dem die Datenbank ausgeführt wird, den Inhalt des Speichers als Klartext betrachtet. Alle Datenbankfunktionen, einschließlich der Indexgenerierung und anderer Funktionen höherer Ordnung, die Zugriff auf die Klartextdaten erfordern, funktionieren weiterhin wie erwartet.
- Amazon RDS baut auf Amazon Elastic Block Store (Amazon EBS)-Verschlüsselung, um Datenbank-Volumes vollständig zu verschlüsseln. Wenn Sie eine verschlüsselte Datenbank-Instance mit Amazon RDS erstellen, erstellt Amazon RDS in Ihrem Namen ein verschlüsseltes Amazon EBS-Volume, um die Datenbank zu speichern. Auf dem Volume gespeicherte Daten, Datenbank-Snapshots, automatische Backups und Read Replicas werden alle unter dem KMS-Schlüssel verschlüsselt, den Sie bei der Erstellung der Datenbank-Instance angegeben haben.
- Amazon Redshift integriert sich in AWS KMS und erstellt eine vierstufige Hierarchie von Schlüsseln, die zur Verschlüsselung der Cluster-Ebene über die Datenebene verwendet werden. Wenn Sie Ihren Cluster starten, können Sie wählen, ob Sie Verschlüsselung verwenden möchten. AWS KMS Nur die Amazon Redshift Redshift-Anwendung und Benutzer mit entsprechenden Berechtigungen können Klartext sehen, wenn die Tabellen im Speicher geöffnet (und entschlüsselt) werden. Dies entspricht weitgehend den Funktionen für transparente oder tabellenbasierte Datenverschlüsselung (TDE), die in einigen kommerziellen Datenbanken verfügbar sind. Das bedeutet, dass alle Datenbankfunktionen, einschließlich der Indexgenerierung und anderer Funktionen höherer Ordnung, die Zugriff auf die Klartextdaten erfordern, weiterhin wie erwartet funktionieren.
- Die clientseitige Verschlüsselung auf Datenebene, die durch das AWS Database Encryption SDK (und ähnliche Tools) implementiert wird, bedeutet, dass sowohl das Betriebssystem als auch die Datenbank nur Chiffretext sehen. Benutzer können Klartext nur sehen, wenn sie von einem Client aus auf die Datenbank zugreifen, auf dem das AWS Database Encryption SDK

installiert ist, und wenn sie Zugriff auf den entsprechenden Schlüssel haben. Datenbankfunktionen höherer Ordnung, die Zugriff auf Klartext benötigen, um wie vorgesehen zu funktionieren, wie z. B. die Indexgenerierung, funktionieren nicht, wenn sie angewiesen werden, mit verschlüsselten Feldern zu arbeiten. Wenn Sie sich für die clientseitige Verschlüsselung entscheiden, stellen Sie sicher, dass Sie einen robusten Verschlüsselungsmechanismus verwenden, der dazu beiträgt, häufige Angriffe auf verschlüsselte Daten zu verhindern. Dazu gehören die Verwendung eines starken Verschlüsselungsalgorithmus und geeigneter Techniken, wie z. B. eines Salt-Verschlüsselungsalgorithmus, zur Abwehr von Chiffretext-Angriffen.

Wir empfehlen, die AWS KMS integrierten Verschlüsselungsfunktionen für AWS Datenbankdienste zu verwenden. Bei Workloads, die vertrauliche Daten verarbeiten, sollte eine clientseitige Verschlüsselung für die sensiblen Datenfelder in Betracht gezogen werden. Wenn Sie die clientseitige Verschlüsselung verwenden, sollten Sie die Auswirkungen auf den Datenbankzugriff berücksichtigen, z. B. Verknüpfungen innerhalb von SQL-Abfragen oder die Indexerstellung.

PCI-DSS-Datenverschlüsselung mit AWS KMS

Die Sicherheits- und Qualitätskontrollen AWS KMS wurden validiert und zertifiziert, um die Anforderungen des Payment Card Industry Data Security Standard (PCI DSS) zu erfüllen. Das bedeutet, dass Sie die Daten der primären Kontonummer (PAN) mit einem KMS-Schlüssel verschlüsseln können. Durch die Verwendung eines KMS-Schlüssels zur Verschlüsselung von Daten entfällt ein Teil des Verwaltungsaufwands für Verschlüsselungsbibliotheken. Darüber hinaus können KMS-Schlüssel nicht aus exportiert werden AWS KMS, sodass Sie sich keine Sorgen darüber machen müssen, dass die Verschlüsselungsschlüssel auf unsichere Weise gespeichert werden.

Es gibt andere Möglichkeiten, die PCI-DSS-Anforderungen AWS KMS zu erfüllen. Wenn Sie beispielsweise Amazon S3 verwenden AWS KMS , können Sie PAN-Daten in Amazon S3 speichern, da sich der Zugriffskontrollmechanismus für jeden Service von dem anderen unterscheidet.

Stellen Sie bei der Überprüfung Ihrer Compliance-Anforderungen wie immer sicher, dass Sie sich von entsprechend erfahrenen, qualifizierten und verifizierten Parteien beraten lassen. Beachten Sie die AWS KMS Anforderungsquoten, wenn Sie Anwendungen entwickeln, die den Schlüssel direkt zum Schutz von Kartentransaktionsdaten verwenden, die in den Anwendungsbereich des PCI DSS fallen.

Da alle AWS KMS Anfragen protokolliert werden AWS CloudTrail, können Sie die Schlüsselnutzung anhand der CloudTrail Protokolle überprüfen. Wenn Sie jedoch Amazon S3 S3-Bucket-Keys verwenden, gibt es keinen Eintrag, der jeder Amazon S3 S3-Aktion entspricht. Das liegt daran, dass der Bucket-Schlüssel die Datenschlüssel verschlüsselt, mit denen Sie die Objekte in Amazon S3

verschlüsseln. Die Verwendung eines Bucket-Schlüssels eliminiert zwar nicht alle API-Aufrufe AWS KMS, reduziert aber deren Anzahl. Daher gibt es keine one-to-one Übereinstimmung mehr zwischen Amazon S3 S3-Objektzugriffsversuchen und API-Aufrufen von AWS KMS.

Verwenden von KMS-Schlüsseln mit Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling ist ein empfohlener Service für die Automatisierung der Skalierung Ihrer Amazon EC2 EC2-Instances. Er hilft Ihnen sicherzustellen, dass Ihnen die richtige Anzahl von Instances zur Verfügung steht, um die Last für Ihre Anwendung zu bewältigen. Amazon EC2 Auto Scaling verwendet eine serviceverknüpfte Rolle, die dem Service entsprechende Berechtigungen gewährt und dessen Aktivitäten innerhalb Ihres Kontos autorisiert. Um KMS-Schlüssel mit Amazon EC2 Auto Scaling zu verwenden, müssen Ihre AWS KMS wichtigsten Richtlinien es der serviceverknüpften Rolle ermöglichen, Ihren KMS-Schlüssel bei einigen API-Vorgängen zu verwenden`Decrypt`, z. B. damit die Automatisierung nützlich ist. Wenn die AWS KMS Schlüsselrichtlinie den IAM-Principal, der den Vorgang ausführt, nicht autorisiert, eine Aktion durchzuführen, wird diese Aktion verweigert. Weitere Informationen zur korrekten Anwendung von Berechtigungen in der Schlüsselrichtlinie, um den Zugriff zu ermöglichen, finden Sie unter Datenschutz in Amazon EC2 Auto Scaling in der Amazon EC2 Auto Scaling Scaling-Dokumentation.

Rotation der wichtigsten Faktoren AWS KMS und Umfang der Auswirkungen

Wir empfehlen die Schlüsselrotation nicht AWS Key Management Service (AWS KMS), es sei denn, Sie müssen die Schlüssel aus regulatorischen Gründen wechseln. Beispielsweise müssen Sie Ihre KMS-Schlüssel möglicherweise aufgrund von Geschäftsrichtlinien, Vertragsregeln oder behördlichen Vorschriften rotieren. Durch das Design von werden die Arten von Risiken, die normalerweise durch Schlüsselrotation gemindert werden, AWS KMS erheblich reduziert. Wenn Sie KMS-Schlüssel rotieren müssen, empfehlen wir, die automatische Schlüsselrotation zu verwenden und die manuelle Schlüsselrotation nur dann zu verwenden, wenn die automatische Schlüsselrotation nicht unterstützt wird.

In diesem Abschnitt werden die folgenden Themen zur Schlüsselrotation behandelt:

- AWS KMS symmetrische Schlüsselrotation
- Schlüsselrotation für Amazon EBS-Volumes
- Schlüsselrotation für Amazon RDS
- Schlüsselrotation für Amazon S3 und Replikation in derselben Region

- Rotierende KMS-Schlüssel mit importiertem Material

AWS KMS symmetrische Schlüsselrotation

AWS KMS unterstützt die automatische Schlüsselrotation nur für symmetrische Verschlüsselung von KMS-Schlüsseln mit Schlüsselmaterial, das AWS KMS erstellt. Die automatische Rotation ist für vom Kunden verwaltete KMS-Schlüssel optional. Das Schlüsselmaterial für AWS verwaltete KMS-Schlüssel wird jährlich AWS KMS rotiert. AWS KMS speichert alle früheren Versionen des kryptografischen Materials auf unbestimmte Zeit, sodass Sie alle Daten entschlüsseln können, die mit diesem KMS-Schlüssel verschlüsselt wurden. AWS KMS löscht kein rotiertes Schlüsselmaterial, bis Sie den KMS-Schlüssel löschen. Wenn Sie ein Objekt mit Hilfe von entschlüsseln AWS KMS, bestimmt der Service außerdem das richtige Trägermaterial, das für den Entschlüsselungsvorgang verwendet werden soll. Es müssen keine zusätzlichen Eingabeparameter angegeben werden.

Da frühere Versionen des kryptografischen Schlüsselmaterials AWS KMS beibehalten werden und Sie dieses Material zum Entschlüsseln von Daten verwenden können, bietet die Schlüsselrotation keine zusätzlichen Sicherheitsvorteile. Der Schlüsselrotationsmechanismus dient dazu, die Rotation von Schlüsseln zu vereinfachen, wenn Sie eine Arbeitslast in einem Kontext ausführen, in dem gesetzliche oder andere Anforderungen dies erfordern.

Schlüsselrotation für Amazon EBS-Volumes

Sie können Amazon Elastic Block Store (Amazon EBS) -Datenschlüssel rotieren, indem Sie einen der folgenden Ansätze verwenden. Der Ansatz hängt von Ihren Workflows, Bereitstellungsmethoden und Ihrer Anwendungsarchitektur ab. Möglicherweise möchten Sie dies tun, wenn Sie von einem AWS verwalteten Schlüssel zu einem vom Kunden verwalteten Schlüssel wechseln.

Um die Daten mithilfe von Betriebssystem-Tools von einem Volume auf ein anderes zu kopieren

1. Erstellen Sie den neuen KMS-Schlüssel. Anweisungen finden Sie unter Erstellen eines KMS-Schlüssels.
2. Erstellen Sie ein neues Amazon EBS-Volume, das dieselbe Größe wie das Original oder größer als das Original hat. Geben Sie für die Verschlüsselung den KMS-Schlüssel an, den Sie erstellt haben. Anweisungen finden Sie unter Erstellen eines Amazon EBS-Volumes.
3. Mounten Sie das neue Volume auf derselben Instance oder demselben Container wie das ursprüngliche Volume. Anweisungen finden Sie unter Anhängen eines Amazon EBS-Volumes an eine Amazon EC2 EC2-Instance.

4. Kopieren Sie mit Ihrem bevorzugten Betriebssystem-Tool Daten vom vorhandenen Volume auf das neue Volume.
5. Wenn die Synchronisierung abgeschlossen ist, beenden Sie während eines vorab geplanten Wartungsfensters den Datenverkehr zur Instance. Anweisungen finden Sie unter Manuelles Stoppen und Starten Ihrer Instances.
6. Hängen Sie das ursprüngliche Volume aus. Anweisungen finden Sie unter Trennen eines Amazon EBS-Volumes von einer Amazon EC2 EC2-Instance.
7. Mounten Sie das neue Volume am ursprünglichen Bereitstellungspunkt.
8. Stellen Sie sicher, dass das neue Volume ordnungsgemäß funktioniert.
9. Löschen Sie das ursprüngliche Volume. Anweisungen finden Sie unter Löschen eines Amazon EBS-Volumes.

So verwenden Sie einen Amazon EBS-Snapshot, um die Daten von einem Volume auf ein anderes zu kopieren

1. Erstellen Sie den neuen KMS-Schlüssel. Anweisungen finden Sie unter Erstellen eines KMS-Schlüssels.
2. Erstellen Sie einen Amazon EBS-Snapshot des ursprünglichen Volumes. Anweisungen finden Sie unter Amazon EBS-Snapshots erstellen.
3. Erstellen Sie ein neues Volume aus dem Snapshot. Geben Sie für die Verschlüsselung den neuen KMS-Schlüssel an, den Sie erstellt haben. Anweisungen finden Sie unter Erstellen eines Amazon EBS-Volumes.

   > **Note**
   >
   > Abhängig von Ihrer Arbeitslast möchten Sie möglicherweise Amazon EBS Fast Snapshot Restore verwenden, um die anfängliche Latenz auf dem Volume zu minimieren.

4. Erstellen Sie eine neue Amazon EC2 EC2-Instance. Anweisungen finden Sie unter Starten einer Amazon EC2 EC2-Instance.
5. Hängen Sie das von Ihnen erstellte Volume an die Amazon EC2 EC2-Instance an. Anweisungen finden Sie unter Anhängen eines Amazon EBS-Volumes an eine Amazon EC2 EC2-Instance.
6. Wechseln Sie die neue Instance in die Produktionsumgebung.
7. Dreht die ursprüngliche Instanz aus der Produktion und löscht sie. Anweisungen finden Sie unter Löschen eines Amazon EBS-Volumes.

> **Note**
>
> Es ist möglich, Snapshots zu kopieren und den für die Zielkopie verwendeten Verschlüsselungsschlüssel zu ändern. Nachdem Sie den Snapshot kopiert und mit Ihren bevorzugten KMS-Schlüsseln verschlüsselt haben, können Sie auch ein Amazon Machine Image (AMI) aus Snapshots erstellen. Weitere Informationen finden Sie unter Amazon EBS-Verschlüsselung in der Amazon EC2 EC2-Dokumentation.

Schlüsselrotation für Amazon RDS

Bei einigen Diensten, wie Amazon Relational Database Service (Amazon RDS), erfolgt die Datenverschlüsselung innerhalb des Dienstes und wird von AWS KMS bereitgestellt. Verwenden Sie die folgenden Anweisungen, um einen Schlüssel für eine Amazon RDS-Datenbank-Instance zu rotieren.

So rotieren Sie einen KMS-Schlüssel für eine Amazon RDS-Datenbank

1. Erstellen Sie einen Snapshot der ursprünglichen verschlüsselten Datenbank. Anweisungen finden Sie unter Manuelle Backups verwalten in der Amazon RDS-Dokumentation.
2. Kopieren Sie den Snapshot in einen neuen Snapshot. Geben Sie für die Verschlüsselung den neuen KMS-Schlüssel an. Anweisungen finden Sie unter Kopieren eines DB-Snapshots für Amazon RDS.
3. Verwenden Sie den neuen Snapshot, um einen neuen Amazon RDS-Cluster zu erstellen. Anweisungen finden Sie unter Wiederherstellen auf eine DB-Instance in der Amazon RDS-Dokumentation. Standardmäßig verwendet der Cluster den neuen KMS-Schlüssel.
4. Überprüfen Sie den Betrieb der neuen Datenbank und der darin enthaltenen Daten.
5. Rotieren Sie die neue Datenbank in die Produktionsumgebung.
6. Rotieren Sie die alte Datenbank aus der Produktion und löschen Sie sie. Anweisungen finden Sie unter Löschen einer DB-Instance.

Schlüsselrotation für Amazon S3 und Replikation in derselben Region

Um den Verschlüsselungsschlüssel eines Objekts für Amazon Simple Storage Service (Amazon S3) zu ändern, müssen Sie das Objekt lesen und neu schreiben. Wenn Sie das Objekt neu schreiben, geben Sie den neuen Verschlüsselungsschlüssel beim Schreibvorgang explizit an. Um dies für

viele Objekte zu tun, können Sie Amazon S3 Batch Operations verwenden. Geben Sie in den Auftragseinstellungen für den Kopiervorgang die neuen Verschlüsselungseinstellungen an. Sie könnten beispielsweise SSE-KMS wählen und die KeyID eingeben.

Alternativ können Sie Amazon S3 Same-Region Replication (SRR) verwenden. SSR kann die Objekte während der Übertragung erneut verschlüsseln.

Rotierende KMS-Schlüssel mit importiertem Material

AWS KMS stellt Ihr importiertes Schlüsselmaterial nicht wieder her oder rotiert es nicht. Um einen KMS-Schlüssel mit importiertem Schlüsselmaterial zu drehen, müssen Sie den Schlüssel manuell drehen.

Empfehlungen für die Verwendung des AWS Encryption SDK

Das AWS Encryption SDKist ein leistungsstarkes Tool für die Implementierung der clientseitigen Verschlüsselung in Ihren Anwendungen. Bibliotheken sind für Java, C JavaScript, Python und andere Programmiersprachen verfügbar. Es lässt sich in AWS Key Management Service (AWS KMS) integrieren. Sie können es auch als eigenständiges SDK verwenden, ohne auf KMS-Schlüssel zu verweisen.

Zu den empfohlenen Methoden für die Verwendung dieses Tools gehört die sorgfältige Prüfung der Anforderungen Ihrer Anwendung. Wägen Sie diese Anforderungen gegen die Risiken ab, die durch bestimmte Konfigurationen entstehen können, z. B. durch die Einführung von Schlüssel-Caching in Ihrer Anwendung. Weitere Informationen zum Zwischenspeichern von Datenschlüsseln finden Sie in der Dokumentation unter Zwischenspeichern von Datenschlüsseln. AWS Encryption SDK

Beachten Sie die folgenden Fragen, wenn Sie entscheiden, ob Sie das verwenden möchten: AWS Encryption SDK

- Gibt es eine Anforderung an die clientseitige Verschlüsselung, die nicht durch serverseitige Verschlüsselung mit Diensten erfüllt werden kann, die sich in integrieren lassen? AWS KMS
- Können Sie die Schlüssel, die zur clientseitigen Verschlüsselung von Daten verwendet werden, angemessen schützen, und wie werden Sie das tun?
- Gibt es andere fit-for-purpose Verschlüsselungsbibliotheken, die besser zu Ihrem Anwendungsfall passen könnten? Erwägen Sie alternative AWS Angebote wie die clientseitige Verschlüsselung von Amazon S3 und das AWS Database Encryption SDK.

Weitere Informationen zur Auswahl des richtigen Dienstes für Ihren Anwendungsfall finden Sie in der AWS Crypto Tools-Dokumentation.

Bewährte Methoden für Identitäts- und Zugriffsmanagement für AWS KMS

Um AWS Key Management Service (AWS KMS) verwenden zu können, benötigen Sie Anmeldeinformationen, mit denen Sie Ihre Anfragen authentifizieren und autorisieren AWS können. Kein AWS Principal hat Berechtigungen für einen KMS-Schlüssel, es sei denn, diese Berechtigung wird ausdrücklich erteilt und niemals verweigert. Es gibt keine impliziten oder automatischen Berechtigungen zur Verwendung oder Verwaltung eines KMS-Schlüssels. In den Themen in diesem Abschnitt werden bewährte Sicherheitsmethoden beschrieben, anhand derer Sie bestimmen können, welche AWS KMS Zugriffsverwaltungskontrollen Sie zum Schutz Ihrer Infrastruktur verwenden sollten.

In diesem Abschnitt werden die folgenden Themen zur Identitäts- und Zugriffsverwaltung behandelt:

- AWS KMS wichtige Richtlinien und IAM-Richtlinien
- Berechtigungen mit den geringsten Rechten für AWS KMS
- Rollenbasierte Zugriffskontrolle für AWS KMS
- Attributbasierte Zugriffskontrolle für AWS KMS
- Verschlüsselungskontext für AWS KMS
- Problembehebung bei AWS KMS Berechtigungen

AWS KMS wichtige Richtlinien und IAM-Richtlinien

Der Zugriff auf Ihre AWS KMS Ressourcen lässt sich in erster Linie mithilfe von Richtlinien verwalten. Richtlinien sind Dokumente, in denen beschrieben wird, welche Prinzipale auf welche Ressourcen zugreifen können. Richtlinien, die mit einer AWS Identity and Access Management (IAM-) Identität verknüpft sind (Benutzer, Benutzergruppen oder Rollen), werden als identitätsbasierte Richtlinien bezeichnet. IAM-Richtlinien, die mit Ressourcen verknüpft sind, werden als ressourcenbasierte Richtlinien bezeichnet. AWS KMS Ressourcenrichtlinien für KMS-Schlüssel werden als Schlüsselrichtlinien bezeichnet. AWS KMS Unterstützt neben IAM-Richtlinien und AWS KMS wichtigen Richtlinien auch Zuschüsse. Zuschüsse bieten eine flexible und leistungsstarke Möglichkeit, Berechtigungen zu delegieren. Mithilfe von Zuschüssen können Sie zeitgebundenen KMS-Schlüsselzugriff auf IAM-Prinzipale in Ihrem AWS-Konto oder einem anderen System gewähren. AWS-Konten

Alle KMS-Schlüssel verfügen über eine Schlüsselrichtlinie. Wenn Sie keinen angeben, AWS KMS erstellt er einen für Sie. Welche Standardschlüsselrichtlinie AWS KMS verwendet wird, hängt davon ab, ob Sie den Schlüssel mithilfe der AWS KMS Konsole oder der AWS KMS API erstellen. Wir empfehlen Ihnen, die Standard-Schlüsselrichtlinie so zu bearbeiten, dass sie den Anforderungen Ihrer Organisation für Berechtigungen mit den geringsten Rechten entspricht. Dies sollte auch mit Ihrer Strategie für die Verwendung von IAM-Richtlinien in Verbindung mit wichtigen Richtlinien übereinstimmen. Weitere Empfehlungen zur Verwendung von IAM-Richtlinien mit finden Sie in der AWS KMS Dokumentation unter Bewährte Methoden für IAM-Richtlinien. AWS KMS

Sie können die Schlüsselrichtlinie verwenden, um die Autorisierung für einen IAM-Prinzipal an die identitätsbasierte Richtlinie zu delegieren. Sie können die Schlüsselrichtlinie auch verwenden, um die Autorisierung in Verbindung mit der identitätsbasierten Richtlinie zu verfeinern. In beiden Fällen bestimmen sowohl die Schlüsselrichtlinie als auch die identitätsbasierte Richtlinie den Zugriff, zusammen mit allen anderen anwendbaren Richtlinien, die den Zugriff einschränken, wie z. B. Dienststeuerungsrichtlinien (SCPs), Ressourcensteuerungsrichtlinien (RCPs) oder Berechtigungsgrenzen. Befindet sich der Principal in einem anderen Konto als der KMS-Schlüssel, werden im Grunde nur kryptografische Aktionen und Grant-Aktionen unterstützt. Weitere Informationen zu diesem kontenübergreifenden Szenario finden Sie in der Dokumentation unter Zulassen der Verwendung eines KMS-Schlüssels für Benutzer mit anderen Konten. AWS KMS

Sie müssen identitätsbasierte IAM-Richtlinien in Kombination mit wichtigen Richtlinien verwenden, um den Zugriff auf Ihre KMS-Schlüssel zu kontrollieren. Zuschüsse können auch in Kombination mit diesen Richtlinien verwendet werden, um den Zugriff auf einen KMS-Schlüssel zu kontrollieren. Um den Zugriff auf einen KMS-Schlüssel mithilfe einer identitätsbasierten Richtlinie zu steuern, muss die Schlüsselrichtlinie dem Konto die Verwendung identitätsbasierter Richtlinien ermöglichen. Sie können entweder eine wichtige Richtlinienanweisung angeben, die IAM-Richtlinien aktiviert, oder Sie können in der Schlüsselrichtlinie explizit zulässige Prinzipale angeben.

Achten Sie beim Schreiben von Richtlinien darauf, dass Sie über strenge Kontrollen verfügen, die einschränken, wer die folgenden Aktionen ausführen kann:

- Aktualisieren, erstellen und löschen Sie IAM-Richtlinien und KMS-Schlüsselrichtlinien
- Hängen Sie identitätsbasierte Richtlinien an Benutzer, Rollen und Gruppen an und trennen Sie sie
- Ordnen Sie AWS KMS wichtige Richtlinien den KMS-Schlüsseln zu und trennen Sie sie
- Berechtigungen für Ihre KMS-Schlüssel erstellen — Unabhängig davon, ob Sie den Zugriff auf Ihre KMS-Schlüssel ausschließlich mit wichtigen Richtlinien kontrollieren oder ob Sie wichtige Richtlinien mit IAM-Richtlinien kombinieren, sollten Sie die Möglichkeit einschränken, die Richtlinien

zu ändern. Implementieren Sie einen Genehmigungsprozess für die Änderung vorhandener Richtlinien. Ein Genehmigungsprozess kann dazu beitragen, Folgendes zu verhindern:

- Versehentlicher Verlust von IAM-Prinzipalberechtigungen — Es ist möglich, Änderungen vorzunehmen, die verhindern, dass IAM-Prinzipale den Schlüssel verwalten oder ihn für kryptografische Operationen verwenden können. In extremen Szenarien ist es möglich, allen Benutzern die Schlüsselverwaltungsberechtigungen zu entziehen. In diesem Fall müssen Sie Kontakt aufnehmen, AWS Supportum wieder Zugriff auf den Schlüssel zu erhalten.
- Nicht genehmigte Änderungen an den KMS-Schlüsselrichtlinien — Wenn ein nicht autorisierter Benutzer Zugriff auf die Schlüsselrichtlinie erhält, kann er diese ändern, um Berechtigungen an einen unbeabsichtigten AWS-Konto Benutzer oder Prinzipal zu delegieren.
- Nicht genehmigte Änderungen an IAM-Richtlinien — Wenn ein nicht autorisierter Benutzer Anmeldeinformationen mit Berechtigungen zur Verwaltung der Gruppenmitgliedschaft erhält, kann er seine eigenen Berechtigungen erweitern und Änderungen an Ihren IAM-Richtlinien, Schlüsselrichtlinien, der KMS-Schlüsselkonfiguration oder anderen Ressourcenkonfigurationen vornehmen. AWS

Prüfen Sie sorgfältig die IAM-Rollen und Benutzer, die den IAM-Prinzipalen zugeordnet sind, die als Ihre KMS-Schlüsseladministratoren benannt sind. Dies kann dazu beitragen, unbefugtes Löschen oder Ändern zu verhindern. Wenn Sie die Prinzipale ändern müssen, die Zugriff auf Ihre KMS-Schlüssel haben, stellen Sie sicher, dass die neuen Administratorprinzipale zu allen erforderlichen Schlüsselrichtlinien hinzugefügt wurden. Testen Sie ihre Berechtigungen, bevor Sie den vorherigen verwaltenden Prinzipal löschen. Es wird dringend empfohlen, alle bewährten Methoden für die IAM-Sicherheit zu befolgen und temporäre Anmeldeinformationen anstelle von langfristigen Anmeldeinformationen zu verwenden.

Wir empfehlen, zeitlich begrenzten Zugriff in Form von Zuschüssen zu gewähren, wenn Sie die Namen der Principals zum Zeitpunkt der Erstellung der Richtlinien nicht kennen oder wenn sich die Principals, für die Zugriff erforderlich ist, häufig ändern. Der Prinzipal des Empfängers kann sich in demselben Konto wie der KMS-Schlüssel oder in einem anderen Konto befinden. Wenn sich der Prinzipal und der KMS-Schlüssel in unterschiedlichen Konten befinden, müssen Sie zusätzlich zur Gewährung eine identitätsbasierte Richtlinie angeben. Zuschüsse erfordern zusätzliche Verwaltung, da Sie eine API aufrufen müssen, um den Zuschuss zu erstellen und den Zuschuss zurückzuziehen oder zu widerrufen, wenn er nicht mehr benötigt wird.

Kein AWS Hauptbenutzer, auch nicht der Root-Benutzer oder der Ersteller des Schlüssels, hat Berechtigungen für einen KMS-Schlüssel, es sei denn, sie sind in einer Schlüsselrichtlinie, IAM-

Richtlinie oder Zuweisung ausdrücklich erlaubt und nicht ausdrücklich verweigert. Im weiteren Sinne sollten Sie berücksichtigen, was passieren würde, wenn ein Benutzer unbeabsichtigt Zugriff auf die Verwendung eines KMS-Schlüssels erhält, und welche Auswirkungen dies hätte. Um ein solches Risiko zu minimieren, sollten Sie Folgendes berücksichtigen:

- Sie können unterschiedliche KMS-Schlüssel für verschiedene Datenkategorien verwalten. Auf diese Weise können Sie Schlüssel trennen und präzisere Schlüsselrichtlinien verwalten, die Richtlinienerklärungen enthalten, die speziell auf den Hauptzugriff auf diese Datenkategorie abzielen. Das bedeutet auch, dass bei einem unbeabsichtigten Zugriff auf relevante IAM-Anmeldeinformationen die mit diesem Zugriff verknüpfte Identität nur Zugriff auf die in der IAM-Richtlinie angegebenen Schlüssel hat und nur dann, wenn die Schlüsselrichtlinie den Zugriff auf diesen Prinzipal zulässt.
- Sie können beurteilen, ob ein Benutzer mit unbeabsichtigtem Zugriff auf den Schlüssel auf die Daten zugreifen kann. Bei Amazon Simple Storage Service (Amazon S3) muss der Benutzer beispielsweise auch über die entsprechenden Berechtigungen für den Zugriff auf verschlüsselte Objekte in Amazon S3 verfügen. Wenn ein Benutzer unbeabsichtigten Zugriff (mithilfe von RDP oder SSH) auf eine EC2 Amazon-Instance hat, deren Volume mit einem KMS-Schlüssel verschlüsselt ist, kann der Benutzer alternativ mithilfe von Betriebssystem-Tools auf die Daten zugreifen.

> **Note**
>
> AWS-Services Bei dieser Verwendung wird der Chiffretext den Benutzern AWS KMS nicht zugänglich gemacht (die meisten aktuellen Kryptoanalyseansätze erfordern Zugriff auf den Chiffretext). Ausserdem steht Chiffretext nicht für physische Untersuchungen außerhalb eines AWS Rechenzentrums zur Verfügung, da alle Speichermedien bei ihrer Außerbetriebnahme gemäß den Anforderungen von NIST 00-88 physisch vernichtet werden. SP8

Berechtigungen mit den geringsten Rechten für AWS KMS

Da Ihre KMS-Schlüssel vertrauliche Informationen schützen, empfehlen wir, dem Prinzip des Zugriffs mit den geringsten Rechten zu folgen. Delegieren Sie bei der Definition Ihrer wichtigsten Richtlinien die Mindestberechtigungen, die zur Ausführung einer Aufgabe erforderlich sind. Lassen Sie alle Aktionen (`kms:*`) für eine KMS-Schlüsselrichtlinie nur zu, wenn Sie beabsichtigen, die Berechtigungen mit zusätzlichen identitätsbasierten Richtlinien weiter einzuschränken. Wenn

Sie beabsichtigen, Berechtigungen mit identitätsbasierten Richtlinien zu verwalten, schränken Sie ein, wer IAM-Richtlinien erstellen und an IAM-Prinzipale anhängen darf, und achten Sie auf Richtlinienänderungen.

Wenn Sie alle Aktionen (`kms:*`) sowohl in der Schlüsselrichtlinie als auch in der identitätsbasierten Richtlinie zulassen, verfügt der Prinzipal sowohl über Administratorrechte als auch über Nutzungsberechtigungen für den KMS-Schlüssel. Aus Sicherheitsgründen empfehlen wir, diese Berechtigungen nur an bestimmte Prinzipale zu delegieren. Überlegen Sie, wie Sie Prinzipalen, die Ihre Schlüssel verwalten, und Prinzipalen, die Ihre Schlüssel verwenden, Berechtigungen zuweisen. Sie können dies tun, indem Sie den Prinzipal in der Schlüsselrichtlinie explizit benennen oder indem Sie einschränken, an welche Prinzipale die identitätsbasierte Richtlinie angehängt ist. Sie können auch Bedingungsschlüssel verwenden, um Berechtigungen einzuschränken. Sie können beispielsweise aws: verwenden, PrincipalTag um alle Aktionen zuzulassen, wenn der Principal, der den API-Aufruf durchführt, das in der Bedingungsregel angegebene Tag hat.

Weitere Informationen darüber, wie Richtlinienaussagen bewertet werden AWS, finden Sie in der IAM-Dokumentation unter Bewertungslogik für Richtlinien. Wir empfehlen, dieses Thema zu lesen, bevor Sie Richtlinien verfassen, um die Wahrscheinlichkeit zu verringern, dass Ihre Richtlinie unbeabsichtigte Auswirkungen hat, wie z. B. die Gewährung von Zugriff für Prinzipale, die keinen Zugriff haben sollten.

> **Tip**
>
> Verwenden Sie AWS Identity and Access Management Access Analyzer (IAM Access Analyzer), wenn Sie eine Anwendung in einer Umgebung außerhalb der Produktionsumgebung testen, damit Sie in Ihren IAM-Richtlinien die Berechtigungen mit den geringsten Rechten anwenden können.

Wenn Sie IAM-Benutzer anstelle von IAM-Rollen verwenden, empfehlen wir dringend, die AWS Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheitsanfälligkeit langfristiger Anmeldeinformationen zu verringern. Über MFA können Sie die folgenden Aktionen ausführen:

- Erfordern Sie, dass Benutzer ihre Anmeldeinformationen mit MFA validieren, bevor sie privilegierte Aktionen ausführen, z. B. das Löschen von Schlüsseln planen.
- Teilen Sie den Besitz eines Administratorkontokennworts und eines MFA-Geräts auf einzelne Personen auf, um die geteilte Autorisierung zu implementieren.

Beispielrichtlinien, die Ihnen bei der Konfiguration von Berechtigungen mit den geringsten Rechten helfen können, finden Sie in der Dokumentation unter Beispiele für IAM-Richtlinien. AWS KMS

Rollenbasierte Zugriffskontrolle für AWS KMS

Bei der rollenbasierten Zugriffskontrolle (RBAC) handelt es sich um eine Autorisierungsstrategie, die Benutzern nur die für die Erfüllung ihrer Aufgaben erforderlichen Berechtigungen gewährt, mehr nicht. Dieser Ansatz kann Ihnen bei der Umsetzung des Prinzips der geringsten Rechte helfen.

AWS KMS unterstützt RBAC. Es ermöglicht Ihnen, den Zugriff auf Ihre Schlüssel zu kontrollieren, indem Sie innerhalb der wichtigsten Richtlinien detaillierte Berechtigungen angeben. In den wichtigsten Richtlinien werden eine Ressource, eine Aktion, eine Wirkung, ein Hauptprinzip und optionale Bedingungen für die Gewährung des Zugriffs auf Schlüssel festgelegt. Um RBAC zu implementieren, empfehlen wir AWS KMS, die Berechtigungen für Schlüsselbenutzer und Schlüsseladministratoren voneinander zu trennen.

Weisen Sie Schlüsselbenutzern nur die Berechtigungen zu, die der Benutzer benötigt. Verwenden Sie die folgenden Fragen, um die Berechtigungen weiter zu verfeinern:

- Welche IAM-Prinzipale benötigen Zugriff auf den Schlüssel?
- Welche Aktionen muss jeder Principal mit dem Schlüssel ausführen? Benötigt der Principal beispielsweise nur `Encrypt` `Sign` Berechtigungen?
- Auf welche Ressourcen muss der Principal zugreifen?
- Ist die Entität ein Mensch oder ein AWS-Service? Wenn es sich um einen Dienst handelt, können Sie den ViaService Bedingungsschlüssel kms: verwenden, um die Schlüsselverwendung auf einen bestimmten Dienst zu beschränken.

Weisen Sie Schlüsseladministratoren nur die Berechtigungen zu, die der Administrator benötigt. Beispielsweise können die Berechtigungen eines Administrators variieren, je nachdem, ob der Schlüssel in Test- oder Produktionsumgebungen verwendet wird. Wenn Sie in bestimmten Umgebungen, die nicht zur Produktion gehören, weniger restriktive Berechtigungen verwenden, implementieren Sie einen Prozess, um die Richtlinien zu testen, bevor sie für die Produktion freigegeben werden.

Beispielrichtlinien, die Ihnen bei der Konfiguration der rollenbasierten Zugriffskontrolle für Hauptbenutzer und Administratoren helfen können, finden Sie unter RBAC für. AWS KMS

Attributbasierte Zugriffskontrolle für AWS KMS

Die attributebasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, die Berechtigungen auf der Grundlage von Attributen definiert. Wie bei RBAC handelt es sich um einen Ansatz, der Sie bei der Implementierung des Prinzips der geringsten Rechte unterstützen kann.

AWS KMS unterstützt ABAC, indem es Ihnen ermöglicht, Berechtigungen auf der Grundlage von Tags zu definieren, die der Zielressource zugeordnet sind, z. B. einem KMS-Schlüssel, und auf Tags, die dem Prinzipal zugeordnet sind, der den API-Aufruf durchführt. In können Sie Tags und Aliase verwenden AWS KMS, um den Zugriff auf Ihre vom Kunden verwalteten Schlüssel zu kontrollieren. Sie können beispielsweise IAM-Richtlinien definieren, die Tag-Bedingungsschlüssel verwenden, um Operationen zu ermöglichen, wenn das Tag des Prinzipals mit dem Tag übereinstimmt, das dem KMS-Schlüssel zugeordnet ist. Ein Tutorial finden Sie in der AWS KMS Dokumentation unter Definieren von Berechtigungen für den Zugriff auf AWS Ressourcen auf der Grundlage von Tags.

Es hat sich bewährt, ABAC-Strategien zur Vereinfachung der IAM-Richtlinienverwaltung zu verwenden. Mit ABAC können Administratoren Tags verwenden, um den Zugriff auf neue Ressourcen zu ermöglichen, anstatt bestehende Richtlinien zu aktualisieren. ABAC benötigt weniger Richtlinien, da Sie nicht unterschiedliche Richtlinien für verschiedene Aufgabenbereiche erstellen müssen. Weitere Informationen finden Sie in der IAM-Dokumentation unter Vergleich von ABAC mit dem herkömmlichen RBAC-Modell.

Wenden Sie das bewährte Verfahren für Berechtigungen mit den geringsten Rechten auf das ABAC-Modell an. Stellen Sie IAM-Prinzipalen nur die Berechtigungen zur Verfügung, die sie zur Ausführung ihrer Aufgaben benötigen. Kontrollieren Sie sorgfältig den Zugriff auf Tagging APIs , sodass Benutzer Tags für Rollen und Ressourcen ändern können. Wenn Sie zur Unterstützung von ABAC in Schlüsselalias Bedingungsschlüssel verwenden, stellen Sie sicher AWS KMS, dass Sie auch über strenge Kontrollen verfügen, die einschränken, wer Schlüssel erstellen und Aliase ändern kann.

Sie können Tags auch verwenden, um einen bestimmten Schlüssel mit einer Geschäftskategorie zu verknüpfen und zu überprüfen, ob der richtige Schlüssel für eine bestimmte Aktion verwendet wird. Sie können beispielsweise mithilfe von AWS CloudTrail Protokollen überprüfen, ob der Schlüssel, der zur Ausführung einer bestimmten AWS KMS Aktion verwendet wurde, derselben Geschäftskategorie angehört wie die Ressource, für die er verwendet wird.

> **Warning**
>
> Geben Sie keine vertraulichen oder sensiblen Informationen in den Tag-Schlüssel oder Tag-Wert ein. Tags sind nicht verschlüsselt. Sie sind für viele zugänglich AWS-Services, auch für die Abrechnung.

Bevor Sie einen ABAC-Ansatz für Ihre Zugriffskontrolle implementieren, sollten Sie prüfen, ob die anderen Dienste, die Sie verwenden, diesen Ansatz unterstützen. Hilfe bei der Bestimmung, welche Dienste ABAC unterstützen AWS-Services , finden Sie in der IAM-Dokumentation unter Diese Dienste funktionieren mit IAM.

Weitere Informationen zur Implementierung von ABAC for AWS KMS und zu den Bedingungsschlüsseln, die Ihnen bei der Konfiguration von Richtlinien helfen können, finden Sie unter ABAC for. AWS KMS

Verschlüsselungskontext für AWS KMS

Alle AWS KMS kryptografischen Operationen mit symmetrischer Verschlüsselung von KMS-Schlüsseln akzeptieren einen Verschlüsselungskontext. Der Verschlüsselungskontext ist ein optionaler Satz nicht geheimer Schlüssel-Wert-Paare, die zusätzliche kontextbezogene Informationen zu den Daten enthalten können. Als bewährte Methode können Sie Verschlüsselungskontext in `Encrypt` Operationen einfügen, um die Autorisierung und Überprüfbarkeit Ihrer API-Aufrufe AWS KMS zur Entschlüsselung zu verbessern. AWS KMS AWS KMS verwendet den Verschlüsselungskontext als zusätzliche authentifizierte Daten (AAD), um die authentifizierte Verschlüsselung zu unterstützen. Der Verschlüsselungskontext ist kryptografisch an den Chiffretext gebunden, sodass derselbe Verschlüsselungskontext zum Entschlüsseln der Daten erforderlich ist.

Der Verschlüsselungskontext ist nicht geheim und nicht verschlüsselt. Er erscheint im Klartext in AWS CloudTrail Protokollen, sodass Sie ihn zur Identifizierung und Kategorisierung Ihrer kryptografischen Operationen verwenden können. Da der Verschlüsselungskontext nicht geheim ist, sollten Sie nur autorisierten Prinzipalen Zugriff auf Ihre Protokolldaten gewähren. CloudTrail

Sie können auch die Bedingungsschlüssel kms ::context-key EncryptionContext und kms: verwenden, um den Zugriff auf einen EncryptionContextKeys KMS-Schlüssel mit symmetrischer Verschlüsselung auf der Grundlage des Verschlüsselungskontextes zu steuern. Sie können diese Bedingungsschlüssel auch verwenden, um vorzuschreiben, dass Verschlüsselungskontexte bei

kryptografischen Vorgängen verwendet werden. Lesen Sie sich für diese Bedingungsschlüssel die Hinweise zur Verwendung von Operatoren `ForAnyValue` oder `ForAllValues` Set-Operatoren durch, um sicherzustellen, dass Ihre Richtlinien Ihren beabsichtigten Berechtigungen entsprechen.

Problembehebung bei AWS KMS Berechtigungen

Wenn Sie Zugriffskontrollrichtlinien für einen KMS-Schlüssel schreiben, sollten Sie berücksichtigen, wie die IAM-Richtlinie und die Schlüsselrichtlinie zusammenarbeiten. Die effektiven Berechtigungen für einen Prinzipal sind die Berechtigungen, die von allen gültigen Richtlinien gewährt (und nicht ausdrücklich verweigert) werden. Innerhalb eines Kontos können die Berechtigungen für einen KMS-Schlüssel durch identitätsbasierte IAM-Richtlinien, Schlüsselrichtlinien, Berechtigungsgrenzen, Dienststeuerungsrichtlinien oder Sitzungsrichtlinien beeinflusst werden. Wenn Sie beispielsweise sowohl identitätsbasierte Richtlinien als auch Schlüsselrichtlinien verwenden, um den Zugriff auf den KMS-Schlüssel zu steuern, werden alle Richtlinien, die sich sowohl auf den Prinzipal als auch auf die Ressource beziehen, ausgewertet, um festzustellen, ob ein Prinzipal berechtigt ist, eine bestimmte Aktion auszuführen. Weitere Informationen finden Sie in der IAM-Dokumentation unter Bewertungslogik für Richtlinien.

Ausführliche Informationen und ein Ablaufdiagramm zur Fehlerbehebung bei Schlüsselzugriffen finden Sie in der Dokumentation unter Problembehandlung beim Schlüsselzugriff. AWS KMS

So beheben Sie die Fehlermeldung „Zugriff verweigert“

1. Vergewissern Sie sich, dass die identitätsbasierten IAM-Richtlinien und die KMS-Schlüsselrichtlinien den Zugriff zulassen.
2. Vergewissern Sie sich, dass eine Berechtigungsgrenze in IAM den Zugriff nicht einschränkt.
3. Vergewissern Sie sich, dass eine Service Control Policy (SCP) oder Resource Control Policy (RCP) den Zugriff nicht AWS Organizations einschränkt.
4. Wenn Sie VPC-Endpoints verwenden, vergewissern Sie sich, dass die Endpunktrichtlinien korrekt sind.
5. Entfernen Sie in den identitätsbasierten Richtlinien und Schlüsselrichtlinien alle Bedingungen oder Ressourcenverweise, die den Zugriff auf den Schlüssel einschränken. Stellen Sie nach dem Entfernen dieser Einschränkungen sicher, dass der Principal die API erfolgreich aufrufen kann, bei der zuvor ein Fehler aufgetreten ist. Wenn dies erfolgreich ist, wenden Sie die Bedingungen und Ressourcenverweise nacheinander erneut an und stellen Sie anschließend sicher, dass der Prinzipal weiterhin Zugriff hat. Auf diese Weise können Sie die Bedingung oder die Ressourcenreferenz identifizieren, die den Fehler verursacht hat.

Weitere Informationen finden Sie in der IAM-Dokumentation unter Problembehandlung bei Fehlermeldungen mit Zugriffsverweigerung.

Bewährte Methoden zur Erkennung und Überwachung von AWS KMS

Erkennung und Überwachung sind ein wichtiger Bestandteil des Verständnisses der Verfügbarkeit, des Zustands und der Verwendung Ihrer AWS Key Management Service (AWS KMS) -Schlüssel. Die Überwachung trägt dazu bei, die Sicherheit, Zuverlässigkeit, Verfügbarkeit und Leistung Ihrer AWS Lösungen aufrechtzuerhalten. AWS bietet mehrere Tools zur Überwachung Ihrer KMS-Schlüssel und AWS KMS -Vorgänge. In diesem Abschnitt wird beschrieben, wie Sie diese Tools konfigurieren und verwenden, um einen besseren Einblick in Ihre Umgebung zu erhalten und die Verwendung Ihrer KMS-Schlüssel zu überwachen.

In diesem Abschnitt werden die folgenden Themen zur Erkennung und Überwachung behandelt:

- Überwachung von AWS KMS Vorgängen mit AWS CloudTrail
- Überwachung des Zugriffs auf KMS-Schlüssel mit IAM Access Analyzer
- Überwachung der Verschlüsselungseinstellungen anderer AWS-Services mit AWS Config
- Überwachung von KMS-Schlüsseln mit CloudWatch Amazon-Alarmen
- Automatisieren von Antworten mit Amazon EventBridge

Überwachung von AWS KMS Vorgängen mit AWS CloudTrail

AWS KMS ist in einen Dienst integriert AWS CloudTrail, der alle Anrufe AWS KMS von Benutzern, Rollen und anderen Personen aufzeichnen kann AWS-Services. CloudTrail erfasst alle API-Aufrufe AWS KMS als Ereignisse, einschließlich Aufrufe von der AWS KMS Konsole AWS KMS APIs, AWS CloudFormation,, AWS Command Line Interface (AWS CLI) und AWS -Tools für PowerShell.

CloudTrail protokolliert alle AWS KMS Operationen, einschließlich schreibgeschützter Operationen wie `ListAliases` und. `GetKeyRotationStatus` Außerdem werden Vorgänge protokolliert, die KMS-Schlüssel verwalten, z. B. `CreateKey` und und`PutKeyPolicy, and cryptographic operations, such as GenerateDataKey`. `Decrypt` Außerdem werden interne Vorgänge protokolliert, AWS KMS die für Sie erforderlich sind`DeleteExpiredKeyMaterial`, z. B.`DeleteKey`,`SynchronizeMultiRegionKey`, und`RotateKey`.

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie ihn erstellen. Standardmäßig bietet der Ereignisverlauf eine einsehbare, durchsuchbare, herunterladbare und unveränderliche Aufzeichnung

der aufgezeichneten Verwaltungsereignis-API-Aktivitäten der letzten 90 Tage in einem. AWS-Region Um die Nutzung Ihrer KMS-Schlüssel nach Ablauf der 90 Tage zu überwachen oder zu überprüfen, empfehlen wir, einen CloudTrail Trail für Sie zu erstellen. AWS-Konto Wenn Sie eine Organisation in erstellt haben AWS Organizations, können Sie einen Organisationspfad oder einen Ereignisdatenspeicher erstellen, der Ereignisse für alle Mitglieder AWS-Konten dieser Organisation protokolliert.

Nachdem Sie einen Trail für Ihr Konto oder Ihre Organisation eingerichtet haben, können Sie andere verwenden, AWS-Services um Ereignisse zu speichern, zu analysieren und automatisch auf Ereignisse zu reagieren, die im Trail protokolliert werden. Sie können z. B. Folgendes tun:

- Sie können CloudWatch Amazon-Alarme einrichten, die Sie über bestimmte Ereignisse im Trail informieren. Weitere Informationen finden Sie unter Überwachung von KMS-Schlüsseln mit CloudWatch Amazon-Alarmen in diesem Handbuch.
- Sie können EventBridge Amazon-Regeln erstellen, die automatisch eine Aktion ausführen, wenn ein Ereignis im Trail eintritt. Weitere Informationen finden Sie unter Automatisieren von Antworten mit Amazon EventBridge in diesem Leitfaden.
- Sie können Amazon Security Lake verwenden, um Protokolle von mehreren zu sammeln und zu speichern AWS-Services, darunter CloudTrail. Weitere Informationen finden Sie unter Sammeln von Daten aus AWS-Services Security Lake in der Amazon Security Lake-Dokumentation.
- Um Ihre Analyse der betrieblichen Aktivitäten zu verbessern, können Sie CloudTrail Protokolle mit Amazon Athena abfragen. Weitere Informationen finden Sie unter AWS CloudTrail Abfrageprotokolle in der Amazon Athena Athena-Dokumentation.

Weitere Informationen zur Überwachung von AWS KMS Vorgängen mit CloudTrail finden Sie im Folgenden:

- AWS KMS API-Aufrufe protokollieren mit AWS CloudTrail
- Beispiele für AWS KMS Protokolleinträge
- Überwachen Sie KMS-Schlüssel mit Amazon EventBridge
- CloudTrail Integration mit Amazon EventBridge

Überwachung des Zugriffs auf KMS-Schlüssel mit IAM Access Analyzer

AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) hilft Ihnen dabei, die Ressourcen in Ihrer Organisation und die Konten (wie KMS-Schlüssel) zu identifizieren, die mit einer externen Entität gemeinsam genutzt werden. Dieser Service kann Ihnen helfen, unbeabsichtigte oder zu breite Zugriffe auf Ihre Ressourcen und Daten zu identifizieren, die ein Sicherheitsrisiko darstellen. IAM Access Analyzer identifiziert Ressourcen, die gemeinsam mit externen Prinzipalen genutzt werden. Dabei werden die ressourcenbasierten Richtlinien in Ihrer Umgebung anhand von logischen Argumenten analysiert. AWS

Mit IAM Access Analyzer können Sie ermitteln, welche externen Entitäten Zugriff auf Ihre KMS-Schlüssel haben. Wenn Sie IAM Access Analyzer aktivieren, erstellen Sie einen Analyzer für eine gesamte Organisation oder für ein Zielkonto. Die Organisation oder das Konto, das Sie auswählen, wird als Vertrauenszone für den Analyzer bezeichnet. Der Analyzer überwacht die unterstützten Ressourcen innerhalb der Vertrauenszone. Jeder Zugriff auf Ressourcen durch Prinzipale innerhalb der Vertrauenszone gilt als vertrauenswürdig.

Bei KMS-Schlüsseln analysiert IAM Access Analyzer die wichtigsten Richtlinien und Berechtigungen, die auf einen Schlüssel angewendet wurden. Es wird festgestellt, ob eine Schlüsselrichtlinie oder ein Zuschuss einer externen Entität den Zugriff auf den Schlüssel ermöglicht. Verwenden Sie IAM Access Analyzer, um festzustellen, ob externe Entitäten Zugriff auf Ihre KMS-Schlüssel haben, und überprüfen Sie dann, ob diese Entitäten Zugriff haben sollten.

Weitere Informationen zur Verwendung von IAM Access Analyzer zur Überwachung des KMS-Schlüsselzugriffs finden Sie im Folgenden:

- Verwenden von AWS Identity and Access Management Access Analyzer
- IAM Access Analyzer-Ressourcentypen für externen Zugriff
- IAM Access Analyzer-Ressourcentypen: AWS KMS keys
- Ergebnisse für externen und ungenutzten Zugriff

Überwachung der Verschlüsselungseinstellungen anderer AWS-Services mit AWS Config

AWS Configbietet einen detaillierten Überblick über die Konfiguration der AWS Ressourcen in Ihrem AWS-Konto. Sie können AWS Config damit überprüfen, ob AWS-Services die Verschlüsselungseinstellungen für diejenigen, die Ihre KMS-Schlüssel verwenden, ordnungsgemäß konfiguriert sind. Sie können beispielsweise die AWS Config Regel für verschlüsselte Volumes verwenden, um zu überprüfen, ob Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes verschlüsselt sind.

AWS Config umfasst verwaltete Regeln, mit denen Sie schnell Regeln auswählen können, anhand derer Sie Ihre Ressourcen bewerten können. Erkundigen Sie AWS-Regionen sich AWS Config in Ihrem, ob die verwalteten Regeln, die Sie benötigen, in dieser Region unterstützt werden. Zu den verfügbaren verwalteten Regeln gehören Prüfungen für die Konfiguration von Amazon Relational Database Service (Amazon RDS) -Snapshots, CloudTrail Trail-Verschlüsselung, Standardverschlüsselung für Amazon Simple Storage Service (Amazon S3) -Buckets, Amazon DynamoDB-Tabellenverschlüsselung und mehr.

Sie können auch benutzerdefinierte Regeln erstellen und Ihre Geschäftslogik anwenden, um festzustellen, ob Ihre Ressourcen Ihren Anforderungen entsprechen. Open-Source-Code für viele verwaltete Regeln ist im AWS Config Regel-Repository unter verfügbar GitHub. Diese können ein nützlicher Ausgangspunkt für die Entwicklung eigener benutzerdefinierter Regeln sein.

Wenn eine Ressource einer Regel nicht entspricht, können Sie entsprechende Aktionen einleiten. AWS Config umfasst Behebungsmaßnahmen, die die AWS Systems Manager Automatisierung durchführt. Wenn Sie beispielsweise die Regel angewendet haben und die cloud-trail-encryption-enabledRegel ein `NON_COMPLIANT` Ergebnis zurückgibt, AWS Config können Sie ein Automatisierungsdokument initiieren, das das Problem behebt, indem die CloudTrail Protokolle für Sie verschlüsselt werden.

AWS Config ermöglicht es Ihnen, proaktiv die Einhaltung der AWS Config Regeln zu überprüfen, bevor Sie Ressourcen bereitstellen. Durch die Anwendung von Regeln im proaktiven Modus können Sie die Konfigurationen Ihrer Cloud-Ressourcen bewerten, bevor sie erstellt oder aktualisiert werden. Wenn Sie Regeln im proaktiven Modus als Teil Ihrer Bereitstellungspipeline anwenden, können Sie Ressourcenkonfigurationen testen, bevor Sie Ihre Ressourcen bereitstellen.

Sie können AWS Config Regeln auch als Kontrollen implementieren AWS Security Hub CSPM. Security Hub CSPM bietet Sicherheitsstandards, die Sie auf Ihre anwenden können. AWS-Konten

Diese Standards helfen Ihnen dabei, Ihre Umgebung anhand empfohlener Verfahren zu bewerten. Der Standard AWS Basic Security Best Practices umfasst Kontrollen innerhalb der Kategorie Protect Control, mit denen überprüft werden kann, ob die Verschlüsselung im Ruhezustand konfiguriert ist und ob die KMS-Schlüsselrichtlinien den empfohlenen Methoden entsprechen.

Weitere Informationen AWS Config zur Überwachung der Verschlüsselungseinstellungen finden Sie unter: AWS-Services

- Erste Schritte mit AWS Config
- AWS Config verwaltete Regeln
- AWS Config benutzerdefinierte Regeln
- Behebung nicht konformer Ressourcen mit AWS Config

Überwachung von KMS-Schlüsseln mit CloudWatch Amazon-Alarmen

Amazon CloudWatch überwacht Ihre AWS Ressourcen und die Anwendungen, auf denen Sie laufen, AWS in Echtzeit. Sie können CloudWatch damit Metriken sammeln und verfolgen. Dabei handelt es sich um Variablen, die Sie messen können.

Der Ablauf von importiertem Schlüsselmaterial oder das Löschen eines Schlüssels sind potenziell katastrophale Ereignisse, wenn sie unbeabsichtigt oder nicht ordnungsgemäß geplant werden. Wir empfehlen, CloudWatch Alarme so zu konfigurieren, dass Sie vor diesen Ereignissen gewarnt werden, bevor sie eintreten. Wir empfehlen außerdem, AWS Identity and Access Management (IAM-) Richtlinien oder AWS Organizations Dienststeuerungsrichtlinien (SCPs) zu konfigurieren, um das Löschen wichtiger Schlüssel zu verhindern.

CloudWatch Mithilfe von Alarmen können Sie Korrekturmaßnahmen ergreifen, z. B. das Löschen von Schlüsseln rückgängig machen, oder Abhilfemaßnahmen ergreifen, z. B. gelöschtes oder abgelaufenes Schlüsselmaterial erneut importieren.

Automatisieren von Antworten mit Amazon EventBridge

Sie können Amazon auch verwenden EventBridge, um Sie über wichtige Ereignisse zu informieren, die sich auf Ihre KMS-Schlüssel auswirken. EventBridge ist ein Programm AWS-Service , das nahezu in Echtzeit einen Stream von Systemereignissen liefert, die Änderungen an AWS Ressourcen

beschreiben. EventBridgeempfängt automatisch Ereignisse von CloudTrail und Security Hub CSPM. In können Sie Regeln erstellen EventBridge, die auf Ereignisse reagieren, die von aufgezeichnet wurden. CloudTrail

AWS KMS Zu den Ereignissen gehören die folgenden:

- Das Schlüsselmaterial in einem KMS-Schlüssel wurde automatisch rotiert
- Das importierte Schlüsselmaterial in einem KMS-Schlüssel ist abgelaufen
- Ein KMS-Schlüssel, dessen Löschung geplant war, wurde gelöscht

Diese Ereignisse können zusätzliche Aktionen in Ihrem auslösen AWS-Konto. Diese Aktionen unterscheiden sich von den im vorherigen Abschnitt beschriebenen CloudWatch Alarmen, da auf sie erst reagiert werden kann, nachdem das Ereignis eingetreten ist. Beispielsweise möchten Sie möglicherweise Ressourcen löschen, die mit einem bestimmten Schlüssel verbunden sind, nachdem dieser Schlüssel gelöscht wurde, oder Sie möchten ein Compliance- oder Auditteam darüber informieren, dass der Schlüssel gelöscht wurde.

Sie können auch nach jedem anderen API-Ereignis filtern, das angemeldet ist, CloudTrail indem Sie EventBridge Das bedeutet, dass Sie nach wichtigen richtlinienbezogenen API-Aktionen filtern können, wenn sie von besonderer Bedeutung sind. Sie könnten beispielsweise nach der EventBridge `PutKeyPolicy` API-Aktion filtern. Allgemeiner gesagt können Sie nach jeder API-Aktion filtern, die mit automatisierten Antworten beginnt `Disable*` oder `Delete*` diese einleitet.

Mit EventBridge dieser Methode können Sie unerwartete oder ausgewählte Ereignisse überwachen (was eine detektive Kontrolle ist), untersuchen und darauf reagieren (bei denen es sich um reaktive Kontrollen handelt). Sie können beispielsweise Sicherheitsteams benachrichtigen und bestimmte Maßnahmen ergreifen, wenn ein IAM-Benutzer oder eine IAM-Rolle erstellt wird, wenn ein KMS-Schlüssel erstellt wird oder wenn eine wichtige Richtlinie geändert wird. Sie können eine EventBridge Ereignisregel erstellen, die die von Ihnen angegebenen API-Aktionen filtert, und dann Ziele mit der Regel verknüpfen. Zu den Beispielzielen gehören AWS Lambda Funktionen, Amazon Simple Notification Service (Amazon SNS) -Benachrichtigungen, Amazon Simple Queue Service (Amazon SQS) -Warteschlangen und mehr. Weitere Informationen zum Senden von Ereignissen an Ziele finden Sie unter Event-Bus-Ziele in Amazon EventBridge.

Weitere Informationen zur Überwachung AWS KMS EventBridge und Automatisierung von Antworten finden Sie EventBridge in der AWS KMS Dokumentation unter KMS-Schlüssel mit Amazon überwachen.

Bewährte Methoden für das Kosten- und Abrechnungsmanagement für AWS KMS

AWS-Services Bieten Sie durch Breite und Tiefe die Flexibilität, Ihre Kosten im Griff zu behalten und gleichzeitig die Geschäftsanforderungen zu erfüllen. In diesem Abschnitt werden die Preise für die Speicherung von AWS Key Management Service Schlüsseln in (AWS KMS) behandelt und Empfehlungen zur Kostensenkung, z. B. durch Schlüssel-Caching, gegeben. Sie können auch die Verwendung von KMS-Schlüsseln überprüfen, um festzustellen, ob es zusätzliche Möglichkeiten zur Kostensenkung gibt.

In diesem Abschnitt werden die folgenden Themen zum Kosten- und Abrechnungsmanagement behandelt:

- AWS KMS Preise für Schlüsselspeicher
- Amazon S3 S3-Bucket-Schlüssel mit Standardverschlüsselung
- Zwischenspeichern von Datenschlüsseln mithilfe von AWS Encryption SDK
- Alternativen zu Schlüssel-Caching und Amazon S3 S3-Bucket-Schlüsseln
- Verwaltung der Protokollierungskosten für die Nutzung von KMS-Schlüsseln

AWS KMS Preise für Schlüsselspeicher

Jedes AWS KMS key , in dem Sie etwas erstellen AWS KMS , ist kostenpflichtig. Die monatliche Gebühr ist für symmetrische Schlüssel, asymmetrische Schlüssel, HMAC-Schlüssel, Schlüssel mit mehreren Regionen (jeder Primärschlüssel und jeder Replikatschlüssel mit mehreren Regionen), Schlüssel mit importiertem Schlüsselmaterial und KMS-Schlüssel, deren Schlüsselquelle entweder aus einem externen Schlüsselspeicher stammt, identisch. AWS CloudHSM

Bei KMS-Schlüsseln, die Sie automatisch oder bei Bedarf rotieren, fallen bei der ersten und zweiten Rotation des Schlüssels zusätzliche monatliche Gebühren (anteilig pro Stunde) an. Nach der zweiten Rotation werden alle nachfolgenden Rotationen in diesem Monat nicht in Rechnung gestellt. Aktuelle AWS KMS Preisinformationen finden Sie unter Preise.

Sie können AWS Budgetses verwenden, um ein Nutzungsbudget zu konfigurieren. AWS Budgets kann Sie benachrichtigen, wenn die Ausgaben auf Ihrem Konto bestimmte Schwellenwerte überschreiten. Für die damit verbundenen Kosten können Sie ein Nutzungsbudget erstellen AWS KMS, um Benachrichtigungen auf der Grundlage von KMS-Schlüsseln oder Anfragen zu erhalten.

Auf diese Weise können Sie sich einen besseren Überblick über Ihre Kosten für die Speicherung und Nutzung Ihrer AWS KMS Schlüssel verschaffen.

Amazon S3 S3-Bucket-Schlüssel mit Standardverschlüsselung

In einigen Anwendungsfällen können Workloads, die auf eine große Anzahl von Objekten in Amazon Simple Storage Service (Amazon S3) zugreifen oder diese generieren, große Mengen an Anfragen generieren AWS KMS, was Ihre Kosten erhöht. Durch die Konfiguration von Amazon S3 S3-Bucket-Keys können Sie die Kosten um bis zu 99% senken. Dies ist eine empfohlene Alternative zur Deaktivierung der Verschlüsselung, um die damit AWS KMS verbundenen Kosten zu senken.

Zwischenspeichern von Datenschlüsseln mithilfe von AWS Encryption SDK

Wenn Sie das AWS Encryption SDKfür die clientseitige Verschlüsselung verwenden, kann das Zwischenspeichern von Datenschlüsseln dazu beitragen, die Leistung Ihrer Anwendung zu verbessern, das Risiko zu verringern, dass die Anfragen Ihrer Anwendung gedrosselt AWS KMS werden, und Sie können die Kosten senken. Weitere Informationen zu den ersten Schritten finden Sie unter So verwenden Sie das Zwischenspeichern von Datenschlüsseln.

Alternativen zu Schlüssel-Caching und Amazon S3 S3-Bucket-Schlüsseln

Wenn das Zwischenspeichern von Schlüsseln aufgrund Ihrer Datenverarbeitungsanforderungen für Sie keine Option ist, können Sie auch AWS KMS Kontingenterhöhungen beantragen, indem Sie die AWS-Managementkonsole oder die Service Quotas API verwenden. Berücksichtigen Sie das Volumen der API-Aufrufe, die Sie möglicherweise tätigen. Die Anzahl der API-Aufrufe, die Sie tätigen, ist ein wichtiger AWS KMS Preisfaktor. Wenn Sie die Quote für die Anforderungsrate erhöhen, um Ihre Leistung zu skalieren, verursacht die steigende Anzahl von Anfragen AWS KMS zusätzliche Kosten.

Verwaltung der Protokollierungskosten für die Nutzung von KMS-Schlüsseln

Alle AWS KMS API-Aufrufe werden protokolliert AWS CloudTrail. Anwendungen und Dienste können große Mengen an AWS KMS API-Aufrufen generieren (z. B. für kryptografische Operationen,

einschließlich Verschlüsseln und Entschlüsseln). Ohne ein Tool, das Ihnen hilft, diese Daten zu organisieren, Trends zu untersuchen und nach anomalen API-Aktivitäten zu suchen, kann es schwierig sein, CloudTrail Protokolle zu überprüfen. Amazon Athena bietet vordefinierte Datenstrukturen, mit denen Sie schnell Tabellen für CloudTrail Protokolle einrichten und mit der Analyse Ihrer Protokolldaten beginnen können. Dies ist besonders nützlich für Ad-hoc-Analysen oder weitere Untersuchungen während der Reaktion auf Vorfälle. Weitere Informationen finden Sie unter AWS CloudTrail Abfrageprotokolle in der Athena-Dokumentation.

Da Sie für Athena pro Abfrage zahlen, können Sie Ihre Tabellen kostenlos im Voraus einrichten. Für Anweisungen in der Datendefinitionssprache fallen keine Gebühren an. Wenn Sie auf einen Vorfall reagieren, können Sie so sicherstellen, dass viele Voraussetzungen bereits erfüllt sind. Um Ihnen bei der Vorbereitung zu helfen, empfiehlt es sich, Ihre Abfragen nach dem Erstellen der Tabelle zu schreiben, sie zu testen und sicherzustellen, dass sie die gewünschten Ergebnisse liefern. Sie können Ihre Abfragen in Athena für die future Verwendung speichern. Weitere Informationen zu den ersten Schritten mit Athena finden Sie unter Erste Schritte mit Amazon Athena.

Datenereignisse bieten Einblick in die Vorgänge, die an oder innerhalb einer Ressource ausgeführt werden. Sie werden auch als Vorgänge auf Datenebene bezeichnet. Beispiele hierfür sind Amazon S3 `PutObject` S3-Ereignisse oder API-Aufrufe für Lambda-Funktionsoperationen. Bei Datenereignissen handelt es sich häufig um umfangreiche Aktivitäten, für deren Protokollierung Gebühren anfallen. Um die Menge der Datenereignisse zu kontrollieren, die in Trails oder in Ereignisdatenspeichern protokolliert werden CloudTrail, können Sie Ihre Protokollierung optimieren, um die Kosten für CloudTrail, und Amazon S3 zu senken AWS KMS, indem Sie erweiterte Event-Selektoren konfigurieren, die einschränken, welche Datenereignisse angemeldet CloudTrail werden sollen. Weitere Informationen finden Sie unter So optimieren Sie die AWS CloudTrail Kosten mithilfe erweiterter Event-Selektoren (AWS Blogbeitrag).

Ressourcen

AWS Key Management Service (AWS KMS) Dokumentation

- AWS KMS Entwicklerhandbuch
- AWS KMS API Referenz
- AWS KMS in der AWS CLI Referenz

Tools

- AWS Encryption SDK

AWS Präskriptive Leitlinien

Strategien

- Erstellung einer Verschlüsselungsstrategie für ruhende Daten

Leitfäden

- Bewährte Methoden und Funktionen zur Verschlüsselung für AWS-Services
- AWS Referenzarchitektur zum Datenschutz (AWS PRA)

Muster

- Automatisches Verschlüsseln von Amazon EBS-Volumes
- Automatically remediate unencrypted Amazon RDS DB instances and clusters
- Überwachen und korrigieren Sie das geplante Löschen von AWS KMS keys

Mitwirkende

Verfassen

- Frank Phillis, Senior GTM Specialist Solutions Architect, AWS
- Ken Beer, Direktor von AWS KMS und Crypto Libraries, AWS
- Michael Miller, leitender Lösungsarchitekt, AWS
- Jeremy Stieglitz, Hauptproduktmanager, AWS
- Zach Miller, Hauptarchitekt für Lösungen, AWS
- Peter M. O'Donnell, leitender Lösungsarchitekt, AWS
- Patrick Palmer, Hauptarchitekt für Lösungen, AWS
- Dave Walker, Hauptarchitekt für Lösungen, AWS

Überprüfend

- Manigandan Shri, leitender Lieferberater, AWS

Technisches Schreiben

- Lilly AbouHarb, leitende technische Redakteurin, AWS
- Kimberly Garmoe, leitende technische Redakteurin, AWS

Dokumentverlauf

In der folgenden Tabelle werden wichtige Änderungen in diesem Leitfaden beschrieben. Um Benachrichtigungen über zukünftige Aktualisierungen zu erhalten, können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Erste Veröffentlichung	—	24. März 2025

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.