AWS Key Management Service praktik terbaik

AWS Panduan Preskriptif

AWS Panduan Preskriptif: AWS Key Management Service praktik terbaik

Table of Contents

AWS Key Management Service praktik terbaik

Amazon Web Services (kontributor)

Maret 2025 (sejarah dokumen)

AWS Key Management Service (AWS KMS) adalah layanan terkelola yang memudahkan Anda membuat dan mengontrol kunci kriptografi yang digunakan untuk melindungi data Anda. Panduan ini menjelaskan cara menggunakan AWS KMS dan memberikan praktik terbaik secara efektif. Ini membantu Anda membandingkan opsi konfigurasi dan memilih set terbaik untuk kebutuhan Anda.

Panduan ini mencakup rekomendasi tentang bagaimana organisasi Anda dapat menggunakan AWS KMS untuk melindungi informasi sensitif dan menerapkan penandatanganan untuk beberapa kasus penggunaan. Ini mempertimbangkan rekomendasi saat ini yang menggunakan dimensi berikut:

- Mengelola kunci - Opsi delegasi untuk pilihan manajemen dan penyimpanan kunci
- Perlindungan data — Mengenkripsi data dalam aplikasi Anda sendiri vs Layanan AWS melakukannya atas nama Anda
- Manajemen akses — Menggunakan kebijakan AWS KMS utama dan kebijakan AWS Identity and Access Management (IAM) untuk menerapkan kontrol akses berbasis peran (RBAC) atau kontrol akses berbasis atribut (ABAC).
- Arsitektur multi-akun dan Multi-wilayah — Rekomendasi untuk penerapan skala besar.
- Manajemen penagihan dan biaya — Memahami biaya dan penggunaan Anda, dan rekomendasi untuk cara mengurangi biaya.
- Kontrol Detektif — Memantau status kunci KMS Anda, pengaturan enkripsi, dan data terenkripsi.
- Respons insiden — Memperbaiki kesalahan konfigurasi yang mengakibatkan ketidakpatuhan terhadap kebijakan perlindungan data Anda.

Hasil bisnis yang ditargetkan

Data Anda adalah aset penting dan sensitif untuk bisnis Anda. Dengan AWS KMS, Anda mengelola kunci kriptografi yang digunakan untuk melindungi dan memverifikasi data Anda. Anda mengontrol bagaimana data Anda digunakan, siapa yang memiliki akses ke sana, dan bagaimana itu dienkripsi. Panduan ini dimaksudkan untuk membantu pengembang, administrator sistem, dan profesional keamanan menerapkan praktik terbaik enkripsi yang membantu Anda mengamankan data sensitif yang disimpan atau ditransmisikan Layanan AWS. Dengan memahami dan menerapkan

rekomendasi dalam panduan ini, Anda dapat mempromosikan kerahasiaan dan integritas data di seluruh lingkungan Anda AWS . Anda dapat memenuhi persyaratan perlindungan data Anda, apakah persyaratan tersebut dirumuskan secara internal, atau Anda memiliki persyaratan khusus untuk program kepatuhan atau validasi. Untuk informasi selengkapnya tentang cara membantu AWS KMS Anda mengamankan data di AWS lingkungan Anda, lihat Menggunakan AWS KMS enkripsi dengan Layanan AWS dalam AWS KMS dokumentasi.

Tentang AWS KMS keys

AWS Key Management Service (AWS KMS) memungkinkan Anda untuk membuat kunci kriptografi yang dapat digunakan pada data yang Anda berikan ke layanan. Jenis sumber daya utama adalah kunci KMS, yang ada tiga jenis:

- Kunci simetris Advanced Encryption Standard (AES) — Ini adalah kunci 256-bit yang digunakan di bawah mode Galois Counter Mode (GCM) AES. Kunci ini menyediakan enkripsi dan dekripsi data yang diautentikasi yang berukuran kurang dari 4 KB. Ini adalah jenis kunci yang paling umum. Ini digunakan untuk melindungi kunci data lainnya, seperti yang digunakan dalam aplikasi Anda atau dengan Layanan AWS mengenkripsi data atas nama Anda.
- Kunci asimetris kurva RSA atau elips - Tombol ini tersedia dalam berbagai ukuran dan mendukung banyak algoritma. Tergantung pada algoritma, mereka dapat digunakan untuk enkripsi dan dekripsi dan untuk menandatangani dan memverifikasi operasi.
- Kunci simetris untuk melakukan operasi kode otentikasi pesan berbasis hash (HMAC) — Kunci ini adalah kunci 256-bit yang digunakan untuk menandatangani dan memverifikasi operasi.

Kunci KMS tidak dapat diekspor dari layanan dalam teks biasa. Mereka dihasilkan oleh dan hanya dapat digunakan dalam modul keamanan perangkat keras (HSMs) yang digunakan oleh layanan. Ini adalah properti keamanan dasar AWS KMS untuk mencegah kompromi kunci. Di Wilayah Tiongkok (Beijing) dan Tiongkok (Ningxia), HSMs ini disertifikasi oleh OSCCA. Di semua Wilayah lain, yang HSMs digunakan di AWS KMS divalidasi di bawah program FIPS 140 dalam NIST di Security Level 3. Untuk informasi selengkapnya tentang desain dan kontrol AWS KMS yang membantu melindungi kunci Anda, lihat Detail AWS Key Management Service Kriptografi.

Anda dapat mengirimkan data AWS KMS dengan menggunakan berbagai kriptografi APIs untuk melakukan enkripsi, mendekripsi, menandatangani, atau memverifikasi operasi dengan kunci KMS. Anda juga dapat memilih untuk memiliki kunci KMS bertindak seperti kunci enkripsi kunci, yang melindungi tipe kunci yang disebut kunci data. Kunci data dapat diekspor dari AWS KMS untuk digunakan dalam aplikasi lokal Anda atau Layanan AWS yang melindungi data atas nama Anda. Penggunaan kunci data umum di semua sistem manajemen kunci dan sering disebut sebagai enkripsi amplop. Enkripsi amplop memungkinkan kunci data untuk digunakan pada sistem jarak jauh yang menangani data sensitif Anda, daripada harus mengirim data sensitif Anda AWS KMS untuk enkripsi langsung di bawah kunci KMS.

Untuk informasi lebih lanjut, lihat AWS KMS keysdan AWS KMS kriptografi penting dalam dokumentasi. AWS KMS

Praktik terbaik manajemen kunci untuk AWS KMS

Saat menggunakan AWS Key Management Service (AWS KMS), ada beberapa keputusan desain mendasar yang harus Anda buat. Ini termasuk apakah akan menggunakan model terpusat atau terdesentralisasi untuk manajemen dan akses kunci, jenis kunci yang akan digunakan, dan jenis penyimpanan kunci yang akan digunakan. Bagian berikut membantu Anda membuat keputusan yang tepat untuk organisasi dan kasus penggunaan Anda. Bagian ini diakhiri dengan pertimbangan penting untuk menonaktifkan dan menghapus kunci KMS, termasuk tindakan yang harus Anda ambil untuk membantu melindungi data dan kunci Anda.

Bagian ini berisi topik berikut:

- Memilih model terpusat atau terdesentralisasi
- Memilih kunci yang dikelola pelanggan, kunci AWS terkelola, atau kunci AWS yang dimiliki
- Memilih toko AWS KMS kunci
- Menghapus dan menonaktifkan tombol KMS

Memilih model terpusat atau terdesentralisasi

AWS merekomendasikan agar Anda menggunakan beberapa akun Akun AWS dan mengelola akun tersebut sebagai satu organisasi AWS Organizations. Ada dua pendekatan luas untuk mengelola AWS KMS keys di lingkungan multi-akun.

Pendekatan pertama adalah pendekatan terdesentralisasi, di mana Anda membuat kunci di setiap akun yang menggunakan kunci tersebut. Saat Anda menyimpan kunci KMS di akun yang sama dengan sumber daya yang mereka lindungi, lebih mudah untuk mendelegasikan izin ke administrator lokal yang memahami persyaratan akses untuk kepala sekolah dan kunci mereka AWS . Anda dapat mengotorisasi penggunaan kunci hanya dengan menggunakan kebijakan kunci, atau Anda dapat menggabungkan kebijakan kunci dan kebijakan berbasis identitas di AWS Identity and Access Management (IAM).

Pendekatan kedua adalah pendekatan terpusat, di mana Anda mempertahankan kunci KMS dalam satu atau beberapa yang ditunjuk. Akun AWS Anda mengizinkan akun lain hanya menggunakan kunci untuk operasi kriptografi. Anda mengelola kunci, siklus hidupnya, dan izinnya dari akun terpusat. Anda mengizinkan Akun AWS orang lain untuk menggunakan kunci tetapi tidak mengizinkan izin lain. Akun eksternal tidak dapat mengelola apa pun tentang siklus hidup kunci atau

izin akses. Model terpusat ini dapat membantu meminimalkan risiko penghapusan kunci yang tidak diinginkan atau eskalasi hak istimewa oleh administrator atau pengguna yang didelegasikan.

Opsi yang Anda pilih tergantung pada beberapa faktor. Pertimbangkan hal berikut saat memilih pendekatan:

1. Apakah Anda memiliki proses otomatis atau manual untuk menyediakan kunci dan akses sumber daya? Ini termasuk sumber daya seperti pipeline penyebaran dan templat infrastruktur sebagai kode (IAc). Alat-alat ini dapat membantu Anda menyebarkan dan mengelola sumber daya (seperti kunci KMS, kebijakan utama, peran IAM, dan kebijakan IAM) di banyak hal. Akun AWS Jika Anda tidak memiliki alat penyebaran ini, pendekatan terpusat untuk manajemen kunci mungkin lebih mudah dikelola untuk bisnis Anda.
2. Apakah Anda memiliki kontrol administratif atas semua Akun AWS yang berisi sumber daya yang menggunakan kunci KMS? Jika demikian, model terpusat dapat menyederhanakan manajemen dan menghilangkan kebutuhan untuk beralih Akun AWS untuk mengelola kunci. Perhatikan, bagaimanapun, bahwa peran IAM dan izin pengguna untuk menggunakan kunci masih harus dikelola per akun.
3. Apakah Anda perlu menawarkan akses untuk menggunakan kunci KMS Anda kepada pelanggan atau mitra yang memiliki sumber daya Akun AWS dan sumber daya mereka sendiri? Untuk kunci ini, pendekatan terpusat dapat mengurangi beban administrasi pada pelanggan dan mitra Anda.
4. Apakah Anda memiliki persyaratan otorisasi untuk akses ke AWS sumber daya yang lebih baik diselesaikan dengan pendekatan akses terpusat atau lokal? Misalnya, jika aplikasi atau unit bisnis yang berbeda bertanggung jawab untuk mengelola keamanan data mereka sendiri, pendekatan terdesentralisasi untuk manajemen kunci lebih baik.
5. Apakah Anda melebihi kuota sumber daya layanan untuk? AWS KMS Karena kuota ini ditetapkan per Akun AWS, model terdesentralisasi mendistribusikan beban di seluruh akun, secara efektif mengalikan kuota layanan.

> **Note**
>
> Model manajemen untuk kunci tidak relevan ketika mempertimbangkan kuota permintaan karena kuota ini diterapkan pada prinsipal akun yang membuat permintaan terhadap kunci, bukan akun yang memiliki atau mengelola kunci.

Secara umum, kami menyarankan Anda memulai dengan pendekatan terdesentralisasi kecuali Anda dapat mengartikulasikan kebutuhan akan model kunci KMS terpusat.

Memilih kunci yang dikelola pelanggan, kunci AWS terkelola, atau kunci AWS yang dimiliki

Kunci KMS yang Anda buat dan kelola untuk digunakan dalam aplikasi kriptografi Anda sendiri dikenal sebagai kunci yang dikelola pelanggan. Layanan AWS dapat menggunakan kunci yang dikelola pelanggan untuk mengenkripsi data yang disimpan layanan atas nama Anda. Kunci yang dikelola pelanggan disarankan jika Anda ingin kontrol penuh atas siklus hidup dan penggunaan kunci Anda. Ada biaya bulanan untuk memiliki kunci yang dikelola pelanggan di akun Anda. Selain itu, permintaan untuk menggunakan atau mengelola kunci dikenakan biaya penggunaan. Untuk informasi selengkapnya, lihat harga AWS KMS.

Jika Anda Layanan AWS ingin mengenkripsi data Anda tetapi tidak ingin overhead atau biaya mengelola kunci, Anda dapat menggunakan kunci AWS terkelola. Jenis kunci ini ada di akun Anda, tetapi hanya dapat digunakan dalam keadaan tertentu. Ini hanya dapat digunakan dalam konteks tempat Layanan AWS Anda beroperasi, dan hanya dapat digunakan oleh kepala sekolah dalam akun yang berisi kunci. Anda tidak dapat mengelola apa pun tentang siklus hidup atau izin kunci ini. Beberapa Layanan AWS menggunakan kunci AWS terkelola. Format alias kunci AWS terkelola adalah`aws/<service code>`. Misalnya, `aws/ebs` kunci hanya dapat digunakan untuk mengenkripsi volume Amazon Elastic Block Store (Amazon EBS) di akun yang sama dengan kunci dan hanya dapat digunakan oleh prinsipal IAM di akun tersebut. Kunci AWS terkelola hanya dapat digunakan oleh pengguna di akun itu dan untuk sumber daya di akun itu. Anda tidak dapat membagikan sumber daya yang dienkripsi di bawah kunci AWS terkelola dengan akun lain. Jika ini adalah batasan untuk kasus penggunaan Anda, sebaiknya gunakan kunci yang dikelola pelanggan; Anda dapat membagikan penggunaan kunci itu dengan akun lain. Anda tidak dikenakan biaya untuk keberadaan kunci AWS terkelola di akun Anda, tetapi Anda dikenakan biaya untuk setiap penggunaan jenis kunci ini oleh Layanan AWS yang ditetapkan ke kunci.

Kunci AWS terkelola adalah tipe kunci lama yang tidak lagi dibuat untuk yang baru Layanan AWS pada tahun 2021. Sebagai gantinya, new (dan legacy) Layanan AWS menggunakan kunci yang AWS dimiliki untuk mengenkripsi data Anda secara default. AWS kunci yang dimiliki adalah kumpulan kunci KMS yang Layanan AWS dimiliki dan dikelola untuk digunakan dalam beberapa. Akun AWS Meskipun kunci ini tidak ada dalam Anda Akun AWS, Layanan AWS dapat menggunakannya untuk melindungi sumber daya di akun Anda.

Kami menyarankan Anda menggunakan kunci yang dikelola pelanggan saat kontrol granular paling penting dan menggunakan kunci yang AWS dimiliki saat kenyamanan paling penting.

Tabel berikut menjelaskan perbedaan kebijakan, pencatatan, manajemen, dan harga utama antara setiap jenis kunci. Untuk informasi selengkapnya tentang tipe kunci, lihat AWS KMS konsep.

Pertimbangan	Kunci yang dikelola pelanggan	AWS kunci terkelola	AWS kunci yang dimiliki
Kebijakan utama	Dikendalikan secara eksklusif oleh pelanggan	Dikendalikan oleh layanan; dapat dilihat oleh pelanggan	Dikontrol secara eksklusif dan hanya dapat dilihat oleh Layanan AWS yang mengenkripsi data Anda
Pencatatan log	AWS CloudTrail jejak pelanggan atau toko data acara	CloudTrail jejak pelanggan atau toko data acara	Tidak dapat dilihat oleh pelanggan
Manajemen siklus hidup	Pelanggan mengelola rotasi, penghapusan, dan Wilayah AWS	Layanan AWS mengelola rotasi (tahunan), penghapusan, dan Wilayah	Layanan AWS mengelola rotasi (tahunan), penghapusan, dan Wilayah
Harga	Biaya bulanan untuk keberadaan kunci (pro-rated per jam); penelepon dikenakan biaya untuk penggunaan API	Tidak ada biaya untuk keberadaan kunci; penelepon dikenakan biaya untuk penggunaan API	Tidak ada biaya untuk pelanggan

Memilih toko AWS KMS kunci

Toko kunci adalah lokasi yang aman untuk menyimpan dan menggunakan bahan kunci kriptografi. Praktik terbaik industri untuk toko utama adalah menggunakan perangkat yang dikenal sebagai modul keamanan perangkat keras (HSM) yang telah divalidasi di bawah NIST Federal Information Processing Standards (FIPS) 140 Cryptographic Module Validation Program di Security Level 3. Ada program lain untuk mendukung toko-toko utama yang digunakan untuk memproses pembayaran.

AWS Payment Cryptographyadalah layanan yang dapat Anda gunakan untuk melindungi data yang terkait dengan beban kerja pembayaran Anda.

AWS KMS mendukung beberapa jenis penyimpanan kunci untuk membantu melindungi materi kunci Anda saat menggunakan AWS KMS untuk membuat dan mengelola kunci enkripsi Anda. Semua opsi penyimpanan utama yang disediakan oleh terus AWS KMS divalidasi di bawah FIPS 140 di Security Level 3. Mereka dirancang untuk mencegah siapa pun, termasuk AWS operator, mengakses kunci teks biasa Anda atau menggunakannya tanpa izin Anda. Untuk informasi selengkapnya tentang jenis toko utama yang tersedia, lihat Toko kunci dalam AWS KMS dokumentasi.

Toko kunci AWS KMS standar adalah pilihan terbaik untuk sebagian besar beban kerja. Jika Anda perlu memilih jenis toko kunci yang berbeda, pertimbangkan dengan cermat apakah peraturan atau persyaratan lain (seperti internal) mandat membuat pilihan ini, dan pertimbangkan dengan cermat biaya dan manfaatnya.

Menghapus dan menonaktifkan tombol KMS

Penghapusan kunci KMS dapat memiliki dampak yang signifikan. Sebelum Anda menghapus kunci KMS yang tidak lagi ingin Anda gunakan, pertimbangkan apakah cukup untuk mengatur status kunci ke Dinonaktifkan. Sementara kunci dinonaktifkan, itu tidak dapat digunakan untuk operasi kriptografi. Itu masih ada di AWS, dan Anda dapat mengaktifkannya kembali di masa depan jika diperlukan. Kunci yang dinonaktifkan terus dikenakan biaya penyimpanan. Kami menyarankan Anda menonaktifkan kunci alih-alih menghapusnya sampai Anda yakin bahwa kunci tersebut tidak melindungi data atau kunci data apa pun.

> **Important**
>
> Menghapus kunci harus direncanakan dengan cermat. Data tidak dapat didekripsi jika kunci yang sesuai telah dihapus. AWS tidak memiliki sarana untuk memulihkan kunci yang dihapus setelah dihapus. Seperti operasi penting lainnya di AWS, Anda harus menerapkan kebijakan yang membatasi siapa yang dapat menjadwalkan kunci untuk dihapus dan memerlukan otentikasi multi-faktor (MFA) untuk penghapusan kunci.

Untuk membantu mencegah penghapusan kunci yang tidak disengaja, AWS KMS memberlakukan periode tunggu minimum default tujuh hari setelah eksekusi `DeleteKey` panggilan sebelum menghapus kunci. Anda dapat mengatur masa tunggu ke nilai maksimum 30 hari. Selama masa tunggu, kunci masih disimpan AWS KMS dalam status Penghapusan Tertunda. Itu tidak dapat

digunakan untuk mengenkripsi atau mendekripsi operasi. Setiap upaya untuk menggunakan kunci yang berada dalam status Penghapusan Tertunda untuk enkripsi atau dekripsi dicatat. AWS CloudTrail Anda dapat mengatur CloudWatch alarm Amazon untuk acara ini di CloudTrail log Anda. Jika Anda menerima alarm pada acara ini, Anda dapat memilih untuk membatalkan proses penghapusan jika diperlukan. Sampai masa tunggu berakhir, Anda dapat memulihkan kunci dari status Penghapusan Tertunda dan mengembalikannya ke status Dinonaktifkan atau Diaktifkan.

Penghapusan kunci Multi-region mengharuskan Anda menghapus replika sebelum salinan asli. Untuk informasi selengkapnya, lihat Menghapus kunci Multi-wilayah.

Jika Anda menggunakan kunci dengan bahan kunci impor, Anda dapat segera menghapus materi kunci yang diimpor. Ini berbeda dengan menghapus kunci KMS dalam beberapa cara. Saat Anda melakukan `DeleteImportedKeyMaterial` tindakan, AWS KMS menghapus materi kunci, dan status kunci berubah menjadi Impor tertunda. Setelah Anda menghapus materi kunci, kuncinya segera tidak dapat digunakan. Tidak ada masa tunggu. Untuk mengaktifkan penggunaan kunci lagi, Anda perlu mengimpor materi kunci yang sama lagi. Masa tunggu penghapusan kunci KMS juga berlaku untuk kunci KMS dengan bahan kunci impor.

Jika kunci data dilindungi oleh kunci KMS dan aktif digunakan oleh Layanan AWS, mereka tidak langsung terpengaruh jika kunci KMS terkait dinonaktifkan atau jika materi kunci yang diimpor dihapus. Misalnya, katakan bahwa kunci dengan bahan impor digunakan untuk mengenkripsi objek dengan SSE-KMS. Anda mengunggah objek ke bucket Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3). Sebelum Anda mengunggah objek ke bucket, Anda mengimpor materi ke kunci Anda. Setelah objek diunggah, Anda menghapus materi kunci yang diimpor dari kunci itu. Objek tetap berada di bucket dalam keadaan terenkripsi, tetapi tidak ada yang dapat mengakses objek sampai materi kunci yang dihapus diimpor kembali ke kunci. Meskipun aliran ini memerlukan otomatisasi yang tepat untuk mengimpor dan menghapus materi kunci dari kunci, ini dapat memberikan tingkat kontrol tambahan dalam suatu lingkungan.

AWS menawarkan panduan preskriptif untuk membantu Anda memantau dan memulihkan (jika perlu) penghapusan kunci KMS yang dijadwalkan. Untuk informasi selengkapnya, lihat Memantau dan memulihkan penghapusan kunci yang dijadwalkan. AWS KMS

Praktik terbaik perlindungan data untuk AWS KMS

Bagian ini membantu Anda membuat pilihan tentang AWS Key Management Service (AWS KMS) penggunaan kunci untuk perlindungan data, seperti kunci mana yang akan digunakan untuk setiap tipe data. Ini juga memberikan contoh spesifik penggunaan AWS KMS dengan berbeda Layanan AWS. Rekomendasi dan contoh ini membantu Anda memahami berapa banyak kunci yang mungkin Anda perlukan dan prinsipal mana yang memerlukan izin untuk menggunakan kunci tersebut.

Bagian ini juga membahas rotasi kunci. Rotasi kunci adalah praktik mengganti kunci KMS yang ada dengan kunci baru atau mengganti materi kriptografi yang terkait dengan kunci KMS yang ada dengan materi baru. Panduan ini memberikan contoh dan instruksi tentang cara memutar tombol KMS untuk umum digunakan Layanan AWS. Rekomendasi dan contoh dirancang untuk membantu Anda membuat pilihan berdasarkan informasi tentang strategi rotasi kunci Anda.

Akhirnya, bagian ini membuat rekomendasi tentang cara menggunakan AWS Encryption SDK, alat untuk menerapkan enkripsi sisi klien dalam aplikasi Anda. Bagian ini mencakup pilihan desain yang dapat Anda buat berdasarkan set fitur dan kemampuan AWS Encryption SDK.

Bagian ini membahas topik enkripsi berikut:

- Enkripsi dengan AWS KMS
- Rotasi kunci untuk AWS KMS dan ruang lingkup dampak
- Rekomendasi untuk menggunakan AWS Encryption SDK

Enkripsi dengan AWS KMS

Enkripsi adalah praktik terbaik umum untuk melindungi kerahasiaan dan integritas informasi sensitif. Anda harus menggunakan tingkat klasifikasi data yang ada dan memiliki setidaknya satu AWS Key Management Service (AWS KMS) kunci per level. Misalnya, Anda dapat menentukan kunci KMS untuk data yang diklasifikasikan sebagai Rahasia, satu untuk Internal-Only, dan satu untuk Sensitif. Ini membantu Anda memastikan bahwa hanya pengguna yang berwenang yang memiliki izin untuk menggunakan kunci yang terkait dengan setiap tingkat klasifikasi.

> **Note**
>
> Kunci KMS yang dikelola pelanggan tunggal dapat digunakan di kombinasi Layanan AWS atau aplikasi Anda sendiri yang menyimpan data klasifikasi tertentu. Faktor pembatas

dalam menggunakan kunci di beberapa beban kerja dan Layanan AWS seberapa kompleks izin penggunaan yang diperlukan untuk mengontrol akses ke data di seluruh kumpulan pengguna. Dokumen JSON kebijakan AWS KMS utama harus kurang dari 32 KB. Jika pembatasan ukuran ini menjadi batasan, pertimbangkan untuk menggunakan AWS KMS hibah atau membuat beberapa kunci untuk meminimalkan ukuran dokumen kebijakan utama.

Alih-alih hanya mengandalkan klasifikasi data untuk mempartisi kunci KMS Anda, Anda juga dapat memilih untuk menetapkan kunci KMS yang akan digunakan untuk klasifikasi data dalam satu. Layanan AWS Misalnya, semua data yang ditandai `Sensitive` di Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) harus dienkripsi di bawah kunci KMS yang memiliki nama seperti. `S3-Sensitive` Anda dapat mendistribusikan data Anda lebih lanjut di beberapa kunci KMS dalam klasifikasi dan Layanan AWS atau aplikasi data yang Anda tentukan. Misalnya, Anda mungkin dapat menghapus beberapa kumpulan data dalam jangka waktu tertentu dan menghapus kumpulan data lain dalam periode waktu yang berbeda. Anda dapat menggunakan tag sumber daya untuk membantu Anda mengidentifikasi dan mengurutkan data yang dienkripsi dengan kunci KMS tertentu.

Jika Anda memilih model manajemen terdesentralisasi untuk kunci KMS, Anda harus menerapkan pagar pembatas untuk memastikan bahwa sumber daya baru dengan klasifikasi tertentu dibuat dan menggunakan kunci KMS yang diharapkan dengan izin yang tepat. Untuk informasi selengkapnya tentang cara menerapkan, mendeteksi, dan mengelola konfigurasi sumber daya menggunakan otomatisasi, lihat Deteksi dan pemantauan bagian panduan ini.

Bagian ini membahas topik enkripsi berikut:

- Enkripsi data log dengan AWS KMS
- Enkripsi secara default
- Enkripsi basis data dengan AWS KMS
- Enkripsi data PCI DSS dengan AWS KMS
- Menggunakan tombol KMS dengan Amazon EC2 Auto Scaling

Enkripsi data log dengan AWS KMS

Banyak Layanan AWS, seperti Amazon GuardDuty dan AWS CloudTrail, menawarkan opsi untuk mengenkripsi data log yang dikirim ke Amazon S3. Saat mengekspor temuan dari Amazon S3 GuardDuty ke, Anda harus menggunakan kunci KMS. Kami menyarankan Anda mengenkripsi semua

data log dan memberikan akses dekripsi hanya kepada kepala sekolah yang berwenang, seperti tim keamanan, responden insiden, dan auditor.

Arsitektur Referensi AWS Keamanan merekomendasikan untuk membuat pusat Akun AWS untuk logging. Ketika Anda melakukan ini, Anda juga dapat mengurangi overhead manajemen kunci Anda. Misalnya, dengan CloudTrail, Anda dapat membuat jejak organisasi atau penyimpanan data acara untuk mencatat peristiwa di seluruh organisasi Anda. Saat mengonfigurasi jejak organisasi atau penyimpanan data peristiwa, Anda dapat menentukan satu bucket Amazon S3 dan kunci KMS di akun logging yang ditentukan. Konfigurasi ini berlaku untuk semua akun anggota di organisasi. Semua akun kemudian mengirim CloudTrail log mereka ke bucket Amazon S3 di akun logging, dan data log dienkripsi dengan kunci KMS yang ditentukan. Anda perlu memperbarui kebijakan kunci untuk kunci KMS ini untuk memberikan izin CloudTrail yang diperlukan untuk menggunakan kunci tersebut. Untuk informasi selengkapnya, lihat Mengonfigurasi kebijakan AWS KMS kunci untuk CloudTrail CloudTrail dokumentasi.

Untuk membantu melindungi GuardDuty dan CloudTrail log, bucket Amazon S3 dan kunci KMS harus sama. Wilayah AWSArsitektur Referensi AWS Keamanan juga memberikan panduan tentang pencatatan dan arsitektur multi-akun. Saat menggabungkan log di beberapa Wilayah dan akun, tinjau Membuat jejak untuk organisasi dalam CloudTrail dokumentasi untuk mempelajari lebih lanjut tentang opt-in Region dan memastikan bahwa logging terpusat Anda berfungsi seperti yang dirancang.

Enkripsi secara default

Layanan AWS yang menyimpan atau memproses data biasanya menawarkan enkripsi saat istirahat. Fitur keamanan ini membantu melindungi data Anda dengan mengenkripsi ketika tidak digunakan. Pengguna yang berwenang masih dapat mengaksesnya saat diperlukan.

Opsi implementasi dan enkripsi bervariasi antara Layanan AWS. Banyak yang menyediakan enkripsi secara default. Penting untuk memahami cara kerja enkripsi untuk setiap layanan yang Anda gunakan. Berikut ini beberapa contohnya:

- Amazon Elastic Block Store (Amazon EBS) — Saat Anda mengaktifkan enkripsi secara default, semua volume Amazon EBS baru dan salinan snapshot dienkripsi. AWS Identity and Access Management (IAM) peran atau pengguna tidak dapat meluncurkan instance dengan volume atau volume yang tidak terenkripsi yang tidak mendukung enkripsi. Fitur ini membantu keamanan, kepatuhan, dan audit dengan memastikan bahwa semua data yang disimpan di volume Amazon EBS dienkripsi. Untuk informasi selengkapnya tentang enkripsi dalam layanan ini, lihat enkripsi Amazon EBS di dokumentasi Amazon EBS.

- Amazon Simple Storage Service (Amazon S3) - Semua objek baru dienkripsi secara default. Amazon S3 secara otomatis menerapkan enkripsi sisi server dengan kunci terkelola Amazon S3 (SSE-S3) untuk setiap objek baru, kecuali jika Anda menentukan opsi enkripsi yang berbeda. Prinsipal IAM masih dapat mengunggah objek yang tidak terenkripsi ke Amazon S3 dengan menyatakannya secara eksplisit dalam panggilan API. Di Amazon S3, untuk menerapkan enkripsi SSE-KMS, Anda harus menggunakan kebijakan bucket dengan kondisi yang memerlukan enkripsi. Untuk kebijakan sampel, lihat Memerlukan SSE-KMS untuk semua objek yang ditulis ke bucket dalam dokumentasi Amazon S3. Beberapa ember Amazon S3 menerima dan melayani sejumlah besar objek. Jika objek tersebut dienkripsi dengan kunci KMS, sejumlah besar operasi Amazon S3 menghasilkan sejumlah besar dan panggilan ke. `GenerateDataKey` `Decrypt` AWS KMS Ini dapat meningkatkan biaya yang Anda keluarkan untuk AWS KMS penggunaan. Anda dapat mengonfigurasi kunci bucket Amazon S3, yang dapat mengurangi biaya secara signifikan. AWS KMS Untuk informasi selengkapnya tentang enkripsi dalam layanan ini, lihat Melindungi data dengan enkripsi di dokumentasi Amazon S3.
- Amazon DynamoDB — DynamoDB adalah layanan database NoSQL yang dikelola sepenuhnya yang memungkinkan enkripsi sisi server saat istirahat secara default, dan Anda tidak dapat menonaktifkannya. Kami menyarankan Anda menggunakan kunci yang dikelola pelanggan untuk mengenkripsi tabel DynamoDB Anda. Pendekatan ini membantu Anda menerapkan hak istimewa paling sedikit dengan izin terperinci dan pemisahan tugas dengan menargetkan pengguna dan peran IAM tertentu dalam kebijakan utama Anda. AWS KMS Anda juga dapat memilih kunci yang AWS dikelola atau AWS dimiliki saat mengonfigurasi pengaturan enkripsi untuk tabel DynamoDB Anda. Untuk data yang memerlukan perlindungan tingkat tinggi (di mana data seharusnya hanya terlihat sebagai cleartext ke klien), pertimbangkan untuk menggunakan enkripsi sisi klien dengan AWS Database Encryption SDK. Untuk informasi selengkapnya tentang enkripsi dalam layanan ini, lihat Perlindungan data dalam dokumentasi DynamoDB.

Enkripsi basis data dengan AWS KMS

Tingkat di mana Anda menerapkan enkripsi mempengaruhi fungsionalitas database. Berikut ini adalah pengorbanan yang harus Anda pertimbangkan:

- Jika Anda hanya menggunakan AWS KMS enkripsi, penyimpanan yang mendukung tabel Anda dienkripsi untuk DynamoDB dan Amazon Relational Database Service (Amazon RDS). Ini berarti bahwa sistem operasi yang menjalankan database melihat isi penyimpanan sebagai cleartext. Semua fungsi database, termasuk pembuatan indeks dan fungsi tingkat tinggi lainnya yang memerlukan akses ke data cleartext, terus berfungsi seperti yang diharapkan.

- Amazon RDS dibangun di atas Amazon Elastic Block Store (Amazon EBS) untuk menyediakan enkripsi disk penuh untuk volume database. Saat Anda membuat instance database terenkripsi dengan Amazon RDS, Amazon RDS membuat volume Amazon EBS terenkripsi atas nama Anda untuk menyimpan database. Data yang disimpan saat istirahat pada volume, snapshot database, backup otomatis, dan replika baca semuanya dienkripsi di bawah kunci KMS yang Anda tentukan saat Anda membuat instance database.
- Amazon Redshift terintegrasi dengan AWS KMS dan menciptakan hierarki kunci empat tingkat yang digunakan untuk mengenkripsi level cluster melalui tingkat data. Ketika Anda meluncurkan cluster Anda, Anda dapat memilih untuk menggunakan AWS KMS enkripsi. Hanya aplikasi Amazon Redshift dan pengguna dengan izin yang sesuai yang dapat melihat cleartext saat tabel dibuka (dan didekripsi) di memori. Ini secara luas analog dengan fitur enkripsi data transparan atau berbasis tabel (TDE) yang tersedia di beberapa database komersial. Ini berarti bahwa semua fungsi database, termasuk pembuatan indeks dan fungsi tingkat tinggi lainnya yang memerlukan akses ke data cleartext, terus berfungsi seperti yang diharapkan.
- Enkripsi tingkat data sisi klien yang diimplementasikan melalui SDK Enkripsi AWS Database (dan alat serupa) berarti bahwa sistem operasi dan database hanya melihat ciphertext. Pengguna dapat melihat cleartext hanya jika mereka mengakses database dari klien yang memiliki AWS Database Encryption SDK diinstal dan mereka memiliki akses ke kunci yang relevan. Fungsi database tingkat tinggi yang memerlukan akses ke cleartext agar berfungsi sebagaimana dimaksud — seperti pembuatan indeks — tidak akan berfungsi jika diarahkan untuk beroperasi pada bidang terenkripsi. Saat memilih untuk menggunakan enkripsi sisi klien, pastikan Anda menggunakan mekanisme enkripsi yang kuat yang membantu mencegah serangan umum terhadap data terenkripsi. Ini termasuk menggunakan algoritma enkripsi yang kuat dan teknik yang tepat, seperti garam, untuk membantu mengurangi serangan ciphertext.

Sebaiknya gunakan kemampuan enkripsi AWS KMS terintegrasi untuk layanan AWS database. Untuk beban kerja yang memproses data sensitif, enkripsi sisi klien harus dipertimbangkan untuk bidang data sensitif. Saat menggunakan enkripsi sisi klien, Anda harus mempertimbangkan dampaknya terhadap akses database, seperti bergabung dalam kueri SQL atau pembuatan indeks.

Enkripsi data PCI DSS dengan AWS KMS

Kontrol keamanan dan kualitas AWS KMS telah divalidasi dan disertifikasi untuk memenuhi persyaratan Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS). Ini berarti Anda dapat mengenkripsi data nomor akun utama (PAN) dengan kunci KMS. Penggunaan kunci KMS untuk mengenkripsi data menghilangkan beberapa beban mengelola pustaka enkripsi. Selain itu, kunci

KMS tidak dapat diekspor AWS KMS, yang mengurangi kekhawatiran tentang kunci enkripsi yang disimpan dengan cara yang tidak aman.

Ada cara lain yang dapat Anda gunakan AWS KMS untuk memenuhi persyaratan PCI DSS. Misalnya, jika Anda menggunakan AWS KMS Amazon S3, Anda dapat menyimpan data PAN di Amazon S3 karena mekanisme kontrol akses untuk setiap layanan berbeda dari yang lain.

Seperti biasa, saat meninjau persyaratan kepatuhan Anda, pastikan Anda mendapatkan saran dari pihak yang berpengalaman, berkualitas, dan terverifikasi. Waspadai kuota AWS KMS permintaan saat Anda merancang aplikasi yang menggunakan kunci secara langsung untuk melindungi data transaksi kartu yang berada dalam lingkup PCI DSS.

Karena semua AWS KMS permintaan masuk AWS CloudTrail, Anda dapat mengaudit penggunaan kunci dengan meninjau CloudTrail log. Namun, jika Anda menggunakan kunci bucket Amazon S3, tidak ada entri yang sesuai dengan setiap tindakan Amazon S3. Ini karena kunci bucket mengenkripsi kunci data yang Anda gunakan untuk mengenkripsi objek di Amazon S3. Meskipun penggunaan kunci bucket tidak menghilangkan semua panggilan API AWS KMS, ini mengurangi jumlahnya. Akibatnya, tidak ada lagi one-to-one kecocokan antara upaya akses objek Amazon S3 dan panggilan API ke. AWS KMS

Menggunakan tombol KMS dengan Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling adalah layanan yang direkomendasikan untuk mengotomatiskan penskalaan instans Amazon EC2 Anda. Ini membantu Anda memastikan bahwa Anda memiliki jumlah instance yang benar yang tersedia untuk menangani beban aplikasi Anda. Amazon EC2 Auto Scaling menggunakan peran terkait layanan yang memberikan izin yang sesuai untuk layanan dan mengotorisasi aktivitasnya dalam akun Anda. Untuk menggunakan kunci KMS dengan Amazon EC2 Auto Scaling, kebijakan utama AWS KMS Anda harus mengizinkan peran yang ditautkan layanan untuk menggunakan kunci KMS Anda dengan beberapa operasi API, `Decrypt` seperti, agar otomatisasi berguna. Jika kebijakan AWS KMS kunci tidak memberi wewenang kepada kepala IAM yang melakukan operasi untuk melakukan suatu tindakan, tindakan tersebut akan ditolak. Untuk informasi selengkapnya tentang cara menerapkan izin dengan benar dalam kebijakan utama untuk mengizinkan akses, lihat Perlindungan data di Amazon EC2 Auto Scaling dalam dokumentasi Amazon EC2 Auto Scaling.

Rotasi kunci untuk AWS KMS dan ruang lingkup dampak

Kami tidak merekomendasikan AWS Key Management Service (AWS KMS) rotasi kunci kecuali Anda diminta untuk memutar kunci untuk kepatuhan terhadap peraturan. Misalnya, Anda mungkin diminta

untuk memutar kunci KMS Anda karena kebijakan bisnis, aturan kontrak, atau peraturan pemerintah. Desain secara AWS KMS signifikan mengurangi jenis risiko yang biasanya digunakan untuk mengurangi rotasi kunci. Jika Anda harus memutar tombol KMS, kami sarankan Anda menggunakan rotasi tombol otomatis dan menggunakan rotasi tombol manual hanya jika rotasi tombol otomatis tidak didukung.

Bagian ini membahas topik rotasi utama berikut:

- AWS KMS rotasi kunci simetris
- Rotasi kunci untuk volume Amazon EBS
- Rotasi kunci untuk Amazon RDS
- Rotasi kunci untuk Amazon S3 dan Replikasi Wilayah yang Sama
- Memutar kunci KMS dengan bahan impor

AWS KMS rotasi kunci simetris

AWS KMS mendukung rotasi kunci otomatis hanya untuk kunci KMS enkripsi simetris dengan bahan kunci yang AWS KMS dibuat. Rotasi otomatis adalah opsional untuk kunci KMS yang dikelola pelanggan. Secara tahunan, AWS KMS memutar materi kunci untuk kunci KMS yang AWS dikelola. AWS KMS menyimpan semua versi sebelumnya dari materi kriptografi selama-lamanya, sehingga Anda dapat mendekripsi data apa pun yang dienkripsi dengan kunci KMS itu. AWS KMS tidak menghapus materi kunci yang diputar sampai Anda menghapus kunci KMS. Juga, ketika Anda mendekripsi objek dengan menggunakan AWS KMS, layanan menentukan bahan pendukung yang benar untuk digunakan untuk operasi dekripsi; tidak ada parameter input tambahan yang perlu disediakan.

Karena AWS KMS mempertahankan versi sebelumnya dari materi kunci kriptografi dan karena Anda dapat menggunakan materi itu untuk mendekripsi data, rotasi kunci tidak memberikan manfaat keamanan tambahan. Mekanisme rotasi kunci ada untuk memudahkan memutar kunci jika Anda mengoperasikan beban kerja dalam konteks di mana peraturan atau persyaratan lain menuntutnya.

Rotasi kunci untuk volume Amazon EBS

Anda dapat memutar kunci data Amazon Elastic Block Store (Amazon EBS) Elastic Block Store (Amazon EBS) dengan menggunakan salah satu pendekatan berikut. Pendekatannya tergantung pada alur kerja, metode penerapan, dan arsitektur aplikasi Anda. Anda mungkin ingin melakukan ini ketika mengubah dari kunci AWS terkelola ke kunci yang dikelola pelanggan.

Untuk menggunakan alat sistem operasi untuk menyalin data dari satu volume ke volume lainnya

1. Buat kunci KMS baru. Untuk petunjuk, lihat Membuat kunci KMS.
2. Buat volume Amazon EBS baru yang ukurannya sama atau lebih besar dari aslinya. Untuk enkripsi, tentukan kunci KMS yang Anda buat. Untuk petunjuk, lihat Membuat volume Amazon EBS.
3. Pasang volume baru pada instance atau wadah yang sama dengan volume aslinya. Untuk petunjuk, lihat Melampirkan volume Amazon EBS ke instans Amazon EC2.
4. Menggunakan alat sistem operasi pilihan Anda, salin data dari volume yang ada ke volume baru.
5. Saat sinkronisasi selesai, selama jendela pemeliharaan yang dijadwalkan sebelumnya, hentikan lalu lintas ke instance. Untuk petunjuk, lihat Menghentikan dan memulai instans Anda secara manual.
6. Lepaskan volume aslinya. Untuk petunjuknya, lihat Melepaskan volume Amazon EBS dari instans Amazon EC2.
7. Pasang volume baru ke titik pemasangan asli.
8. Verifikasi bahwa volume baru beroperasi dengan benar.
9. Hapus volume asli. Untuk petunjuk, lihat Menghapus volume Amazon EBS.

Untuk menggunakan snapshot Amazon EBS untuk menyalin data dari satu volume ke volume lainnya

1. Buat kunci KMS baru. Untuk petunjuk, lihat Membuat kunci KMS.
2. Buat snapshot Amazon EBS dari volume aslinya. Untuk petunjuk, lihat Membuat snapshot Amazon EBS.
3. Buat snapshot volume baru dari snapshot. Untuk enkripsi, tentukan kunci KMS baru yang Anda buat. Untuk petunjuk, lihat Membuat volume Amazon EBS.

   > **Note**
   >
   > Bergantung pada beban kerja Anda, Anda mungkin ingin menggunakan pemulihan snapshot cepat Amazon EBS untuk meminimalkan latensi awal pada volume.

4. Buat instans Amazon EC2 baru. Untuk petunjuknya, lihat Meluncurkan instans Amazon EC2.
5. Lampirkan volume yang Anda buat ke instans Amazon EC2. Untuk petunjuk, lihat Melampirkan volume Amazon EBS ke instans Amazon EC2.
6. Putar instance baru ke dalam produksi.

7. Putar instance asli dari produksi dan hapus. Untuk petunjuk, lihat Menghapus volume Amazon EBS.

> **Note**
>
> Dimungkinkan untuk menyalin snapshot dan memodifikasi kunci enkripsi yang digunakan untuk salinan target. Setelah Anda menyalin snapshot dan mengenkripsi dengan kunci KMS pilihan Anda, Anda juga dapat membuat Amazon Machine Image (AMI) dari snapshot. Untuk informasi selengkapnya, lihat enkripsi Amazon EBS di dokumentasi Amazon EC2.

Rotasi kunci untuk Amazon RDS

Untuk beberapa layanan, seperti Amazon Relational Database Service (Amazon RDS), enkripsi data terjadi dalam layanan dan disediakan oleh. AWS KMS Gunakan petunjuk berikut untuk memutar kunci untuk instance database Amazon RDS.

Untuk memutar kunci KMS untuk database Amazon RDS

1. Buat snapshot dari database terenkripsi asli. Untuk petunjuk, lihat Mengelola backup manual dalam dokumentasi Amazon RDS.
2. Salin snapshot ke snapshot baru. Untuk enkripsi, tentukan kunci KMS baru. Untuk petunjuk, lihat Menyalin snapshot DB untuk Amazon RDS.
3. Gunakan snapshot baru untuk membuat cluster Amazon RDS baru. Untuk petunjuknya, lihat Memulihkan ke instans DB dalam dokumentasi Amazon RDS. Secara default, cluster menggunakan kunci KMS baru.
4. Verifikasi pengoperasian database baru dan data di dalamnya.
5. Putar database baru ke dalam produksi.
6. Putar database lama dari produksi dan hapus. Untuk petunjuk, lihat Menghapus instans DB.

Rotasi kunci untuk Amazon S3 dan Replikasi Wilayah yang Sama

Untuk Amazon Simple Storage Service (Amazon S3), untuk mengubah kunci enkripsi objek, Anda perlu membaca dan menulis ulang objek. Saat Anda menulis ulang objek, Anda secara eksplisit menentukan kunci enkripsi baru dalam operasi tulis. Untuk melakukan ini untuk banyak objek, Anda dapat menggunakan Operasi Batch Amazon S3. Dalam pengaturan pekerjaan, untuk operasi

penyalinan, tentukan pengaturan enkripsi baru. Misalnya, Anda dapat memilih SSE-KMS dan memasukkan KeyID.

Atau, Anda dapat menggunakan Amazon S3 Same-Region Replication (SRR). SSR dapat mengenkripsi ulang objek dalam perjalanan.

Memutar kunci KMS dengan bahan impor

AWS KMS tidak memulihkan atau memutar materi kunci impor Anda. Untuk memutar kunci KMS dengan bahan kunci yang diimpor, Anda harus memutar tombol secara manual.

Rekomendasi untuk menggunakan AWS Encryption SDK

AWS Encryption SDKIni adalah alat yang ampuh untuk menerapkan enkripsi sisi klien dalam aplikasi Anda. Perpustakaan tersedia untuk Java,, C JavaScript, Python, dan bahasa pemrograman lainnya. Ini terintegrasi dengan AWS Key Management Service (AWS KMS). Anda juga dapat menggunakannya sebagai SDK yang berdiri sendiri tanpa mereferensikan kunci KMS.

Praktik yang disarankan untuk menggunakan alat ini termasuk mempertimbangkan dengan cermat persyaratan aplikasi Anda. Seimbangkan persyaratan tersebut terhadap risiko yang dapat diperkenalkan oleh konfigurasi tertentu, seperti memperkenalkan caching kunci ke dalam aplikasi Anda. Untuk informasi selengkapnya tentang caching kunci data, lihat Caching kunci data dalam dokumentasi. AWS Encryption SDK

Pertimbangkan pertanyaan-pertanyaan berikut saat menentukan apakah akan menggunakan AWS Encryption SDK:

- Apakah ada persyaratan untuk enkripsi sisi klien yang tidak dapat dipenuhi oleh enkripsi sisi server dengan layanan yang terintegrasi dengannya? AWS KMS
- Dapatkah Anda cukup melindungi kunci yang digunakan untuk mengenkripsi data sisi klien, dan bagaimana Anda akan melakukannya?
- Apakah ada pustaka fit-for-purpose enkripsi lain yang mungkin sesuai dengan kasus penggunaan Anda dengan lebih tepat? Pertimbangkan AWS penawaran alternatif, seperti enkripsi sisi klien Amazon S3 dan SDK Enkripsi Database.AWS

Temukan informasi selengkapnya tentang memilih layanan yang tepat untuk kasus penggunaan Anda, lihat Dokumentasi Alat AWS Crypto.

Praktik terbaik manajemen identitas dan akses untuk AWS KMS

Untuk menggunakan AWS Key Management Service (AWS KMS), Anda harus memiliki kredensi yang AWS dapat digunakan untuk mengautentikasi dan mengotorisasi permintaan Anda. Tidak ada AWS prinsipal yang memiliki izin untuk kunci KMS kecuali izin tersebut diberikan secara eksplisit dan tidak pernah ditolak. Tidak ada izin implisit atau otomatis untuk menggunakan atau mengelola kunci KMS. Topik di bagian ini menentukan praktik terbaik keamanan untuk membantu Anda menentukan kontrol manajemen AWS KMS akses mana yang harus Anda gunakan untuk mengamankan infrastruktur Anda.

Bagian ini membahas topik identitas dan manajemen akses berikut:

- AWS KMS kebijakan utama dan kebijakan IAM
- Izin hak istimewa paling sedikit untuk AWS KMS
- Kontrol akses berbasis peran untuk AWS KMS
- Kontrol akses berbasis atribut untuk AWS KMS
- Konteks enkripsi untuk AWS KMS
- Izin pemecahan masalah AWS KMS

AWS KMS kebijakan utama dan kebijakan IAM

Cara utama untuk mengelola akses ke AWS KMS sumber daya Anda adalah dengan kebijakan. Kebijakan adalah dokumen yang menjelaskan prinsip mana yang dapat mengakses sumber daya mana. Kebijakan yang dilampirkan pada identitas AWS Identity and Access Management (IAM) (pengguna, kelompok pengguna, atau peran) disebut kebijakan berbasis identitas. Kebijakan IAM yang melekat pada sumber daya disebut kebijakan berbasis sumber daya. AWS KMS kebijakan sumber daya untuk kunci KMS disebut kebijakan kunci. Selain kebijakan IAM dan kebijakan AWS KMS utama, AWS KMS mendukung hibah. Hibah menyediakan cara yang fleksibel dan ampuh untuk mendelegasikan izin. Anda dapat menggunakan hibah untuk mengeluarkan akses kunci KMS terikat waktu ke kepala sekolah IAM di Anda atau yang lain. Akun AWS Akun AWS

Semua kunci KMS memiliki kebijakan kunci. Jika Anda tidak menyediakannya, AWS KMS buatlah satu untuk Anda. Kebijakan kunci default yang AWS KMS digunakan berbeda-beda tergantung pada apakah Anda membuat kunci menggunakan AWS KMS konsol atau Anda menggunakan AWS KMS

API. Sebaiknya Anda mengedit kebijakan kunci default agar selaras dengan persyaratan organisasi Anda untuk izin hak istimewa paling sedikit. Ini juga harus selaras dengan strategi Anda untuk menggunakan kebijakan IAM dalam hubungannya dengan kebijakan utama. Untuk rekomendasi selengkapnya tentang penggunaan kebijakan IAM AWS KMS, lihat Praktik terbaik untuk kebijakan IAM dalam dokumentasi. AWS KMS

Anda dapat menggunakan kebijakan kunci untuk mendelegasikan otorisasi prinsipal IAM ke kebijakan berbasis identitas. Anda juga dapat menggunakan kebijakan kunci untuk menyempurnakan otorisasi bersama dengan kebijakan berbasis identitas. Dalam kedua kasus tersebut, kebijakan kunci dan kebijakan berbasis identitas menentukan akses, bersama dengan kebijakan lain yang berlaku yang mencakup akses, seperti kebijakan kontrol layanan (), kebijakan kontrol sumber daya (SCPsRCPs), atau batas izin. Jika prinsipal berada di akun yang berbeda dari kunci KMS, pada dasarnya, hanya tindakan kriptografi dan hibah yang didukung. Untuk informasi selengkapnya tentang skenario lintas akun ini, lihat Mengizinkan pengguna di akun lain menggunakan kunci KMS dalam dokumentasi. AWS KMS

Anda harus menggunakan kebijakan berbasis identitas IAM dalam kombinasi dengan kebijakan utama untuk mengontrol akses ke kunci KMS Anda. Hibah juga dapat digunakan dalam kombinasi dengan kebijakan ini untuk mengontrol akses ke kunci KMS. Untuk menggunakan kebijakan berbasis identitas untuk mengontrol akses ke kunci KMS, kebijakan kunci harus mengizinkan akun menggunakan kebijakan berbasis identitas. Anda dapat menentukan pernyataan kebijakan kunci yang mengaktifkan kebijakan IAM, atau Anda dapat secara eksplisit menentukan prinsip yang diizinkan dalam kebijakan utama.

Saat menulis kebijakan, pastikan Anda memiliki kontrol kuat yang membatasi siapa yang dapat melakukan tindakan berikut:

- Memperbarui, membuat, dan menghapus kebijakan IAM dan kebijakan kunci KMS
- Melampirkan dan melepaskan kebijakan berbasis identitas dari pengguna, peran, dan grup
- Pasang dan lepaskan kebijakan AWS KMS kunci dari kunci KMS
- Buat hibah untuk kunci KMS Anda — Apakah Anda mengontrol akses ke kunci KMS Anda secara eksklusif dengan kebijakan utama, atau Anda menggabungkan kebijakan utama dengan kebijakan IAM, Anda harus membatasi kemampuan untuk mengubah kebijakan. Menerapkan proses persetujuan untuk mengubah kebijakan yang ada. Proses persetujuan dapat membantu mencegah hal-hal berikut:
  - Kehilangan izin utama IAM secara tidak sengaja — Dimungkinkan untuk membuat perubahan yang akan mencegah prinsipal IAM untuk dapat mengelola kunci atau menggunakannya dalam

operasi kriptografi. Dalam skenario ekstrem, dimungkinkan untuk mencabut izin manajemen kunci dari semua pengguna. Jika ini terjadi, Anda perlu menghubungi AWS Dukunganuntuk mendapatkan kembali akses ke kunci.

- Perubahan yang tidak disetujui pada kebijakan kunci KMS — Jika pengguna yang tidak sah mendapatkan akses ke kebijakan kunci, mereka dapat memodifikasinya untuk mendelegasikan izin ke yang tidak diinginkan atau prinsipal. Akun AWS
- Perubahan yang tidak disetujui pada kebijakan IAM — Jika pengguna yang tidak sah memperoleh serangkaian kredensil dengan izin untuk mengelola keanggotaan grup, mereka dapat meningkatkan izin mereka sendiri dan membuat perubahan pada kebijakan IAM, kebijakan utama, konfigurasi kunci KMS, atau konfigurasi sumber daya lainnya. AWS

Tinjau dengan cermat peran IAM dan pengguna yang terkait dengan kepala sekolah IAM yang ditunjuk sebagai administrator kunci KMS Anda. Ini dapat membantu mencegah penghapusan atau perubahan yang tidak sah. Jika Anda perlu mengubah prinsipal yang memiliki akses ke kunci KMS Anda, verifikasi bahwa kepala administrator baru ditambahkan ke semua kebijakan kunci yang diperlukan. Uji izin mereka sebelum Anda menghapus prinsipal pengelola sebelumnya. Kami sangat menyarankan untuk mengikuti semua praktik terbaik keamanan IAM dan menggunakan kredensil sementara alih-alih kredensil jangka panjang.

Kami merekomendasikan untuk mengeluarkan akses terikat waktu melalui hibah jika Anda tidak mengetahui nama kepala sekolah pada saat kebijakan dibuat atau jika kepala sekolah yang memerlukan akses sering berubah. Pokok penerima hibah dapat berada di akun yang sama dengan kunci KMS atau di akun yang berbeda. Jika kunci utama dan KMS berada di akun yang berbeda, maka Anda harus menentukan kebijakan berbasis identitas selain hibah. Hibah memerlukan manajemen tambahan karena Anda harus memanggil API untuk membuat hibah dan untuk pensiun atau mencabut hibah ketika tidak lagi diperlukan.

Tidak ada AWS prinsipal, termasuk pengguna root akun atau pembuat kunci, yang memiliki izin untuk kunci KMS kecuali mereka secara eksplisit diizinkan dan tidak secara eksplisit ditolak dalam kebijakan kunci, kebijakan IAM, atau hibah. Dengan ekstensi, Anda harus mempertimbangkan apa yang akan terjadi jika pengguna mendapatkan akses yang tidak diinginkan untuk menggunakan kunci KMS dan apa dampaknya. Untuk mengurangi risiko seperti itu, pertimbangkan hal berikut:

- Anda dapat mempertahankan kunci KMS yang berbeda untuk berbagai kategori data. Ini membantu Anda memisahkan kunci dan mempertahankan kebijakan kunci yang lebih ringkas yang berisi pernyataan kebijakan yang secara khusus menargetkan akses utama ke kategori data tersebut. Ini juga berarti bahwa jika kredensil IAM yang relevan diakses secara tidak sengaja,

identitas yang terkait dengan akses tersebut hanya memiliki akses ke kunci yang ditentukan dalam kebijakan IAM dan hanya jika kebijakan kunci mengizinkan akses ke prinsipal tersebut.

- Anda dapat menilai apakah pengguna dengan akses yang tidak diinginkan ke kunci dapat mengakses data. Misalnya, dengan Amazon Simple Storage Service (Amazon S3), pengguna juga harus memiliki izin yang sesuai untuk mengakses objek terenkripsi di Amazon S3. Sebagai alternatif, jika pengguna memiliki akses yang tidak diinginkan (dengan menggunakan RDP atau SSH) ke instans EC2 Amazon yang memiliki volume yang dienkripsi dengan kunci KMS, pengguna dapat mengakses data dengan menggunakan alat sistem operasi.

> **Note**
>
> Layanan AWS penggunaan itu AWS KMS tidak mengekspos ciphertext kepada pengguna (pendekatan terkini untuk cryptoanalysis memerlukan akses ke ciphertext). Selain itu, ciphertext tidak tersedia untuk pemeriksaan fisik di luar pusat AWS data karena semua media penyimpanan hancur secara fisik ketika dinonaktifkan, sesuai dengan persyaratan NIST 00-88. SP8

Izin hak istimewa paling sedikit untuk AWS KMS

Karena kunci KMS Anda melindungi informasi sensitif, kami sarankan untuk mengikuti prinsip akses yang paling tidak memiliki hak istimewa. Delegasikan izin minimum yang diperlukan untuk melakukan tugas saat Anda menentukan kebijakan utama Anda. Izinkan semua tindakan (`kms:*`) pada kebijakan kunci KMS hanya jika Anda berencana untuk membatasi izin lebih lanjut dengan kebijakan berbasis identitas tambahan. Jika Anda berencana untuk mengelola izin dengan kebijakan berbasis identitas, batasi siapa yang memiliki kemampuan untuk membuat dan melampirkan kebijakan IAM ke prinsipal IAM dan memantau perubahan kebijakan.

Jika Anda mengizinkan semua tindakan (`kms:*`) dalam kebijakan kunci dan kebijakan berbasis identitas, prinsipal memiliki izin administratif dan penggunaan ke kunci KMS. Sebagai praktik keamanan terbaik, kami sarankan untuk mendelegasikan izin ini hanya kepada prinsipal tertentu. Pertimbangkan bagaimana Anda menetapkan izin kepada kepala sekolah yang akan mengelola kunci dan kepala sekolah Anda yang akan menggunakan kunci Anda. Anda dapat melakukan ini dengan secara eksplisit menyebutkan prinsipal dalam kebijakan kunci atau dengan membatasi prinsip mana kebijakan berbasis identitas dilampirkan. Anda juga dapat menggunakan tombol kondisi untuk membatasi izin. Misalnya, Anda dapat menggunakan aws: PrincipalTag untuk mengizinkan

semua tindakan jika prinsipal yang membuat panggilan API memiliki tag yang ditentukan dalam aturan kondisi.

Untuk bantuan memahami bagaimana pernyataan kebijakan dievaluasi AWS, lihat Logika evaluasi kebijakan dalam dokumentasi IAM. Sebaiknya tinjau topik ini sebelum menulis kebijakan untuk membantu mengurangi kemungkinan kebijakan Anda memiliki efek yang tidak diinginkan, seperti menyediakan akses ke kepala sekolah yang seharusnya tidak memiliki akses.

> **Tip**
>
> Saat menguji aplikasi di lingkungan non-produksi, gunakan AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) untuk membantu Anda menerapkan izin hak istimewa paling sedikit dalam kebijakan IAM Anda.

Jika Anda menggunakan pengguna IAM alih-alih peran IAM, kami sangat menyarankan menggunakan otentikasi AWS multi-faktor (MFA) untuk mengurangi kerentanan kredensil jangka panjang. Anda dapat menggunakan MFA untuk melakukan hal berikut:

- Mengharuskan pengguna memvalidasi kredensialnya dengan MFA sebelum melakukan tindakan istimewa, seperti menjadwalkan penghapusan kunci.
- Pisahkan kepemilikan kata sandi akun administrator dan perangkat MFA antar individu untuk menerapkan otorisasi terpisah.

Untuk contoh kebijakan yang dapat membantu Anda mengonfigurasi izin hak istimewa terkecil, lihat contoh kebijakan IAM dalam dokumentasi. AWS KMS

Kontrol akses berbasis peran untuk AWS KMS

Kontrol akses berbasis peran (RBAC) adalah strategi otorisasi yang memberi pengguna hanya izin yang diperlukan untuk melakukan tugas pekerjaan mereka, dan tidak lebih. Ini adalah pendekatan yang dapat membantu Anda menerapkan prinsip hak istimewa paling sedikit.

AWS KMS mendukung RBAC. Ini memungkinkan Anda untuk mengontrol akses ke kunci Anda dengan menentukan izin terperinci dalam kebijakan utama. Kebijakan kunci menentukan sumber daya, tindakan, efek, prinsip, dan kondisi opsional untuk memberikan akses ke kunci. Untuk mengimplementasikan RBAC di AWS KMS, sebaiknya pisahkan izin untuk pengguna kunci dan administrator kunci.

Untuk pengguna kunci, tetapkan hanya izin yang dibutuhkan pengguna. Gunakan pertanyaan berikut untuk membantu Anda menyempurnakan izin lebih lanjut:

- Prinsipal IAM mana yang membutuhkan akses ke kunci?
- Tindakan apa yang harus dilakukan setiap kepala sekolah dengan kunci? Misalnya, apakah kepala sekolah hanya perlu `Encrypt` dan `Sign` izin?
- Sumber daya apa yang perlu diakses oleh prinsipal?
- Apakah entitas itu manusia atau Layanan AWS? Jika ini adalah layanan, Anda dapat menggunakan kms: ViaService condition key untuk membatasi penggunaan kunci ke layanan tertentu.

Untuk administrator kunci, tetapkan hanya izin yang dibutuhkan administrator. Misalnya, izin administrator dapat bervariasi tergantung pada apakah kunci digunakan dalam lingkungan pengujian atau produksi. Jika Anda menggunakan izin yang tidak terlalu ketat di lingkungan non-produksi tertentu, terapkan proses untuk menguji kebijakan sebelum dirilis ke produksi.

Untuk contoh kebijakan yang dapat membantu Anda mengonfigurasi kontrol akses berbasis peran untuk pengguna dan administrator utama, lihat RBAC untuk. AWS KMS

Kontrol akses berbasis atribut untuk AWS KMS

Attribute-based access control (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut. Seperti RBAC, ini adalah pendekatan yang dapat membantu Anda menerapkan prinsip hak istimewa paling sedikit.

AWS KMS mendukung ABAC dengan memungkinkan Anda menentukan izin berdasarkan tag yang terkait dengan sumber daya target, seperti kunci KMS, dan tag yang terkait dengan prinsipal yang membuat panggilan API. Di AWS KMS, Anda dapat menggunakan tag dan alias untuk mengontrol akses ke kunci yang dikelola pelanggan Anda. Misalnya, Anda dapat menentukan kebijakan IAM yang menggunakan kunci kondisi tag untuk mengizinkan operasi saat tag prinsipal cocok dengan tag yang terkait dengan kunci KMS. Untuk tutorial, lihat Menentukan izin untuk mengakses AWS sumber daya berdasarkan tag dalam AWS KMS dokumentasi.

Sebagai praktik terbaik, gunakan strategi ABAC untuk menyederhanakan manajemen kebijakan IAM. Dengan ABAC, administrator dapat menggunakan tag untuk mengizinkan akses ke sumber daya baru alih-alih memperbarui kebijakan yang ada. ABAC memerlukan lebih sedikit kebijakan karena Anda tidak perlu membuat kebijakan yang berbeda untuk fungsi pekerjaan yang berbeda. Untuk

informasi lebih lanjut, lihat Perbandingan ABAC dengan model RBAC tradisional dalam dokumentasi IAM.

Terapkan praktik terbaik izin hak istimewa terkecil ke model ABAC. Berikan kepala sekolah IAM hanya dengan izin yang mereka butuhkan untuk melakukan pekerjaan mereka. Hati-hati mengontrol akses ke penandaan APIs yang akan memungkinkan pengguna untuk memodifikasi tag pada peran dan sumber daya. Jika Anda menggunakan kunci kondisi alias kunci untuk mendukung ABAC AWS KMS, pastikan Anda juga memiliki kontrol kuat yang membatasi siapa yang dapat membuat kunci dan memodifikasi alias.

Anda juga dapat menggunakan tag untuk menautkan kunci tertentu ke kategori bisnis dan memverifikasi bahwa kunci yang benar digunakan untuk tindakan tertentu. Misalnya, Anda dapat menggunakan AWS CloudTrail log untuk memverifikasi bahwa kunci yang digunakan untuk melakukan AWS KMS tindakan tertentu termasuk dalam kategori bisnis yang sama dengan sumber daya yang digunakan.

> **Warning**
>
> Jangan sertakan informasi rahasia atau sensitif dalam kunci tag atau nilai tag. Tag tidak dienkripsi. Mereka dapat diakses oleh banyak orang Layanan AWS, termasuk penagihan.

Sebelum menerapkan pendekatan ABAC untuk kontrol akses Anda, pertimbangkan apakah layanan lain yang Anda gunakan mendukung pendekatan ini. Untuk bantuan menentukan layanan mana yang mendukung ABAC, lihat layanan Layanan AWS yang berfungsi dengan IAM dalam dokumentasi IAM.

Untuk informasi selengkapnya tentang penerapan ABAC untuk AWS KMS dan kunci kondisi yang dapat membantu Anda mengonfigurasi kebijakan, lihat ABAC untuk. AWS KMS

Konteks enkripsi untuk AWS KMS

Semua operasi AWS KMS kriptografi dengan kunci KMS enkripsi simetris menerima konteks enkripsi. Konteks enkripsi adalah kumpulan opsional pasangan kunci-nilai non-rahasia yang dapat berisi informasi kontekstual tambahan tentang data. Sebagai praktik terbaik, Anda dapat menyisipkan konteks enkripsi dalam `Encrypt` operasi AWS KMS untuk meningkatkan otorisasi dan auditabilitas panggilan API dekripsi Anda. AWS KMS AWS KMS menggunakan konteks enkripsi sebagai data otentikasi tambahan (AAD) untuk mendukung enkripsi yang diautentikasi. Konteks enkripsi terikat secara kriptografis ke ciphertext sehingga konteks enkripsi yang sama diperlukan untuk mendekripsi data.

Konteks enkripsi tidak rahasia dan tidak dienkripsi. Itu muncul dalam plaintext di AWS CloudTrail log sehingga Anda dapat menggunakannya untuk mengidentifikasi dan mengkategorikan operasi kriptografi Anda. Karena konteks enkripsi bukan rahasia, Anda harus mengizinkan hanya kepala sekolah yang berwenang untuk mengakses data log Anda CloudTrail .

Anda juga dapat menggunakan kms ::context-key EncryptionContext dan kms: condition EncryptionContextKeys keys untuk mengontrol akses ke kunci KMS enkripsi simetris berdasarkan konteks enkripsi. Anda juga dapat menggunakan kunci kondisi ini untuk mengharuskan konteks enkripsi digunakan dalam operasi kriptografi. Untuk kunci kondisi ini, tinjau panduan tentang penggunaan `ForAnyValue` atau `ForAllValues` set operator untuk memastikan bahwa kebijakan Anda mencerminkan izin yang Anda inginkan.

Izin pemecahan masalah AWS KMS

Saat Anda menulis kebijakan kontrol akses untuk kunci KMS, pertimbangkan bagaimana kebijakan IAM dan kebijakan kunci bekerja sama. Izin efektif untuk prinsipal adalah izin yang diberikan (dan tidak secara eksplisit ditolak) oleh semua kebijakan yang efektif. Dalam akun, izin ke kunci KMS dapat dipengaruhi oleh kebijakan berbasis identitas IAM, kebijakan utama, batas izin, kebijakan kontrol layanan, atau kebijakan sesi. Misalnya, jika Anda menggunakan kebijakan berbasis identitas dan kunci untuk mengontrol akses ke kunci KMS, semua kebijakan yang berkaitan dengan prinsipal dan sumber daya dievaluasi untuk menentukan otorisasi prinsipal untuk melakukan tindakan tertentu. Untuk informasi selengkapnya, lihat Logika evaluasi kebijakan dalam dokumentasi IAM.

Untuk informasi rinci dan diagram alur untuk memecahkan masalah akses kunci, lihat Memecahkan masalah akses kunci dalam dokumentasi. AWS KMS

Untuk memecahkan masalah pesan kesalahan akses ditolak

1. Konfirmasikan bahwa kebijakan berbasis identitas IAM dan kebijakan kunci KMS mengizinkan akses.
2. Konfirmasikan bahwa batas izin di IAM tidak membatasi akses.
3. Konfirmasikan bahwa kebijakan kontrol layanan (SCP) atau kebijakan kontrol sumber daya (RCP) di AWS Organizations tidak membatasi akses.
4. Jika Anda menggunakan titik akhir VPC, konfirmasikan bahwa kebijakan endpoint sudah benar.
5. Dalam kebijakan berbasis identitas dan kebijakan utama, hapus kondisi atau referensi sumber daya apa pun yang membatasi akses ke kunci. Setelah menghapus pembatasan ini, konfirmasikan bahwa prinsipal dapat berhasil memanggil API yang sebelumnya gagal.

Jika berhasil, terapkan kembali kondisi dan referensi sumber daya satu per satu dan, setelah masing-masing, verifikasi bahwa kepala sekolah masih memiliki akses. Ini membantu Anda mengidentifikasi kondisi atau referensi sumber daya yang menyebabkan kesalahan.

Untuk informasi selengkapnya, lihat Memecahkan masalah akses ditolak pesan kesalahan dalam dokumentasi IAM.

Deteksi dan pemantauan praktik terbaik untuk AWS KMS

Deteksi dan pemantauan adalah bagian penting untuk memahami ketersediaan, status, dan penggunaan kunci AWS Key Management Service (AWS KMS) Anda. Pemantauan membantu menjaga keamanan, keandalan, ketersediaan, dan kinerja AWS solusi Anda. AWS menyediakan beberapa alat untuk memantau kunci dan AWS KMS operasi KMS Anda. Bagian ini menjelaskan cara mengonfigurasi dan menggunakan alat ini untuk mendapatkan visibilitas yang lebih besar ke lingkungan Anda dan memantau penggunaan kunci KMS Anda.

Bagian ini membahas topik deteksi dan pemantauan berikut:

- Memantau AWS KMS operasi dengan AWS CloudTrail
- Memantau akses ke kunci KMS dengan IAM Access Analyzer
- Memantau pengaturan enkripsi lainnya Layanan AWS dengan AWS Config
- Memantau kunci KMS dengan alarm Amazon CloudWatch
- Mengotomatiskan tanggapan dengan Amazon EventBridge

Memantau AWS KMS operasi dengan AWS CloudTrail

AWS KMS terintegrasi dengan AWS CloudTrail, layanan yang dapat merekam semua panggilan AWS KMS oleh pengguna, peran, dan lainnya Layanan AWS. CloudTrail menangkap semua panggilan API ke AWS KMS sebagai peristiwa, termasuk panggilan dari AWS KMS konsol,, AWS KMS APIs AWS CloudFormation, AWS Command Line Interface (AWS CLI), dan Alat AWS untuk PowerShell.

CloudTrail mencatat semua AWS KMS operasi, termasuk operasi hanya-baca, seperti `ListAliases` dan. `GetKeyRotationStatus` Ini juga mencatat operasi yang mengelola kunci KMS, seperti `CreateKey` dan `PutKeyPolicy, and cryptographic operations, such as GenerateDataKey` dan`Decrypt`. Ini juga mencatat operasi internal yang AWS KMS memanggil Anda, seperti`DeleteExpiredKeyMaterial`,`DeleteKey`,`SynchronizeMultiRegionKey`, dan`RotateKey`.

CloudTrail diaktifkan pada Anda Akun AWS saat Anda membuatnya. Secara default, riwayat Peristiwa menyediakan rekaman yang dapat dilihat, dapat dicari, dapat diunduh, dan tidak dapat diubah selama 90 hari terakhir dari aktivitas API peristiwa manajemen yang direkam dalam file. Wilayah AWS Untuk memantau atau mengaudit penggunaan kunci KMS Anda di luar 90 hari,

kami sarankan untuk membuat CloudTrail jejak untuk Anda Akun AWS. Jika Anda telah membuat organisasi di AWS Organizations, Anda dapat membuat jejak organisasi atau penyimpanan data peristiwa yang mencatat peristiwa untuk semua Akun AWS di organisasi tersebut.

Setelah Anda membuat jejak untuk akun atau organisasi Anda, Anda dapat menggunakan yang lain Layanan AWS untuk menyimpan, menganalisis, dan secara otomatis menanggapi peristiwa yang dicatat di jejak. Misalnya, Anda dapat melakukan hal berikut:

- Anda dapat mengatur CloudWatch alarm Amazon yang memberi tahu Anda tentang peristiwa tertentu di jalan setapak. Untuk informasi selengkapnya, lihat Memantau kunci KMS dengan alarm Amazon CloudWatch dalam panduan ini.
- Anda dapat membuat EventBridge aturan Amazon yang secara otomatis melakukan tindakan saat peristiwa terjadi di jejak. Untuk informasi selengkapnya, lihat Mengotomatiskan tanggapan dengan Amazon EventBridge di panduan ini.
- Anda dapat menggunakan Amazon Security Lake untuk mengumpulkan dan menyimpan log dari beberapa Layanan AWS, termasuk CloudTrail. Untuk informasi selengkapnya, lihat Mengumpulkan data dari Layanan AWS Security Lake di dokumentasi Amazon Security Lake.
- Untuk meningkatkan analisis aktivitas operasional, Anda dapat melakukan kueri CloudTrail log dengan Amazon Athena. Untuk informasi selengkapnya, lihat AWS CloudTrail Log kueri di dokumentasi Amazon Athena.

Untuk informasi selengkapnya tentang pemantauan AWS KMS operasi dengan CloudTrail, lihat berikut ini:

- Pencatatan panggilan AWS KMS API dengan AWS CloudTrail
- Contoh entri AWS KMS log
- Pantau tombol KMS dengan Amazon EventBridge
- CloudTrail Integrasi dengan Amazon EventBridge

Memantau akses ke kunci KMS dengan IAM Access Analyzer

AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) membantu Anda mengidentifikasi sumber daya di organisasi dan akun Anda (seperti kunci KMS) yang dibagikan dengan entitas eksternal. Layanan ini dapat membantu Anda mengidentifikasi akses yang tidak diinginkan atau terlalu luas ke sumber daya dan data Anda, yang merupakan risiko keamanan. IAM

Access Analyzer mengidentifikasi sumber daya yang dibagikan dengan prinsipal eksternal dengan menggunakan penalaran berbasis logika untuk menganalisis kebijakan berbasis sumber daya di lingkungan Anda. AWS

Anda dapat menggunakan IAM Access Analyzer untuk mengidentifikasi entitas eksternal mana yang memiliki akses ke kunci KMS Anda. Bila Anda mengaktifkan IAM Access Analyzer, Anda membuat analyzer untuk seluruh organisasi atau untuk akun target. Organisasi atau akun yang Anda pilih dikenal sebagai zona kepercayaan untuk penganalisis. Penganalisis memantau sumber daya yang didukung dalam zona kepercayaan. Setiap akses ke sumber daya oleh kepala sekolah dalam zona kepercayaan dianggap tepercaya.

Untuk kunci KMS, IAM Access Analyzer menganalisis kebijakan utama dan hibah yang diterapkan pada kunci. Ini menghasilkan temuan jika kebijakan kunci atau hibah memungkinkan entitas eksternal untuk mengakses kunci. Gunakan IAM Access Analyzer untuk menentukan apakah entitas eksternal memiliki akses ke kunci KMS Anda, lalu verifikasi apakah entitas tersebut harus memiliki akses.

Untuk informasi selengkapnya tentang penggunaan IAM Access Analyzer untuk memantau akses kunci KMS, lihat berikut ini:

- Menggunakan AWS Identity and Access Management Access Analyzer
- Jenis sumber daya IAM Access Analyzer untuk akses eksternal
- Jenis sumber daya IAM Access Analyzer: AWS KMS keys
- Temuan untuk akses eksternal dan tidak terpakai

Memantau pengaturan enkripsi lainnya Layanan AWS dengan AWS Config

AWS Configmemberikan tampilan rinci tentang konfigurasi AWS sumber daya di Anda Akun AWS. Anda dapat menggunakan AWS Config untuk memverifikasi bahwa yang menggunakan kunci KMS Anda memiliki pengaturan enkripsi yang dikonfigurasi dengan tepat. Layanan AWS Misalnya, Anda dapat menggunakan AWS Config aturan volume terenkripsi untuk memvalidasi volume Amazon Elastic Block Store (Amazon EBS) Anda dienkripsi.

AWS Config termasuk aturan terkelola yang membantu Anda dengan cepat memilih aturan untuk menilai sumber daya Anda. Periksa AWS Config Wilayah AWS untuk menentukan apakah aturan terkelola yang Anda butuhkan didukung di Wilayah tersebut. Aturan terkelola yang tersedia mencakup pemeriksaan konfigurasi snapshot Amazon Relational Database Service (Amazon RDS),

enkripsi jejak CloudTrail , enkripsi default untuk bucket Amazon Simple Storage Service (Amazon S3), enkripsi tabel Amazon DynamoDB, dan banyak lagi.

Anda juga dapat membuat aturan khusus dan menerapkan logika bisnis Anda untuk menentukan apakah sumber daya Anda sesuai dengan kebutuhan Anda. Kode sumber terbuka untuk banyak aturan terkelola tersedia di AWS Config Rules Repository on. GitHub Ini bisa menjadi titik awal yang berguna untuk mengembangkan aturan kustom Anda sendiri.

Ketika sumber daya tidak sesuai dengan aturan, Anda dapat memulai tindakan responsif. AWS Config termasuk tindakan remediasi yang dilakukan AWS Systems Manager Otomasi. Misalnya, jika Anda telah menerapkan cloud-trail-encryption-enabledaturan dan aturan mengembalikan `NON_COMPLIANT` hasil, AWS Config dapat memulai dokumen Otomasi yang memperbaiki masalah dengan mengenkripsi log untuk Anda. CloudTrail

AWS Config memungkinkan Anda secara proaktif memeriksa kepatuhan terhadap AWS Config aturan sebelum Anda menyediakan sumber daya. Menerapkan aturan dalam mode proaktif membantu Anda mengevaluasi konfigurasi sumber daya cloud Anda sebelum dibuat atau diperbarui. Menerapkan aturan dalam mode proaktif sebagai bagian dari pipeline penerapan memungkinkan Anda menguji konfigurasi sumber daya sebelum menerapkan sumber daya.

Anda juga dapat menerapkan AWS Config aturan sebagai kontrol melalui AWS Security Hub CSPM. Security Hub CSPM menawarkan standar keamanan yang dapat Anda terapkan untuk Anda. Akun AWS Standar ini membantu Anda menilai lingkungan Anda terhadap praktik rekomendasi. Standar Praktik Terbaik Keamanan AWS Dasar mencakup kontrol dalam kategori kontrol proteksi untuk memverifikasi bahwa enkripsi saat istirahat dikonfigurasi dan bahwa kebijakan kunci KMS mengikuti praktik yang direkomendasikan.

Untuk informasi selengkapnya tentang penggunaan AWS Config untuk memantau pengaturan enkripsi di Layanan AWS, lihat berikut ini:

- Memulai dengan AWS Config
- AWS Config aturan terkelola
- AWS Config aturan kustom
- Memulihkan sumber daya yang tidak sesuai dengan AWS Config

Memantau kunci KMS dengan alarm Amazon CloudWatch

Amazon CloudWatch memantau AWS sumber daya Anda dan aplikasi yang Anda jalankan AWS secara real time. Anda dapat menggunakan CloudWatch untuk mengumpulkan dan melacak metrik, yang merupakan variabel yang dapat Anda ukur.

Berakhirnya bahan kunci yang diimpor, atau penghapusan kunci, berpotensi menjadi peristiwa bencana jika tidak diinginkan atau tidak direncanakan dengan benar. Kami menyarankan Anda mengonfigurasi CloudWatch alarm untuk mengingatkan Anda tentang peristiwa ini sebelum terjadi. Kami juga menyarankan Anda mengonfigurasi kebijakan AWS Identity and Access Management (IAM) atau kebijakan kontrol AWS Organizations layanan (SCPs) untuk mencegah penghapusan kunci penting.

CloudWatch alarm membantu Anda mengambil tindakan korektif, seperti membatalkan penghapusan kunci, atau tindakan remediasi, seperti mengimpor ulang materi kunci yang dihapus atau kedaluwarsa.

Mengotomatiskan tanggapan dengan Amazon EventBridge

Anda juga dapat menggunakan Amazon EventBridge untuk memberi tahu Anda tentang peristiwa penting yang memengaruhi kunci KMS Anda. EventBridge adalah Layanan AWS yang memberikan aliran peristiwa sistem yang mendekati waktu nyata yang menggambarkan perubahan AWS sumber daya. EventBridgesecara otomatis menerima peristiwa dari CloudTrail dan Security Hub CSPM. Di EventBridge, Anda dapat membuat aturan yang merespons peristiwa yang direkam oleh CloudTrail.

AWS KMS acara meliputi yang berikut:

- Materi kunci dalam kunci KMS diputar secara otomatis
- Materi kunci yang diimpor dalam kunci KMS kedaluwarsa
- Kunci KMS yang telah dijadwalkan untuk dihapus telah dihapus

Peristiwa ini dapat memulai tindakan tambahan di Anda Akun AWS. Tindakan ini berbeda dari CloudWatch alarm yang dijelaskan di bagian sebelumnya karena mereka hanya dapat ditindaklanjuti setelah peristiwa terjadi. Misalnya, Anda mungkin ingin menghapus sumber daya yang terhubung ke kunci tertentu setelah kunci tersebut dihapus, atau Anda mungkin ingin memberi tahu tim kepatuhan atau audit bahwa kunci tersebut telah dihapus.

Anda juga dapat memfilter untuk setiap peristiwa API lain yang masuk CloudTrail dengan menggunakan EventBridge. Ini berarti bahwa jika tindakan API terkait kebijakan utama menjadi perhatian khusus, Anda dapat memfilternya. Misalnya, Anda dapat memfilter EventBridge untuk tindakan `PutKeyPolicy` API. Secara lebih luas, Anda dapat memfilter tindakan API apa pun yang dimulai dengan `Disable*` atau `Delete*` untuk memulai respons otomatis.

Dengan menggunakan EventBridge, Anda dapat memantau (yang merupakan kontrol detektif) dan menyelidiki dan merespons (yang merupakan kontrol responsif) terhadap peristiwa yang tidak terduga atau dipilih. Misalnya, Anda dapat memberi tahu tim keamanan dan mengambil tindakan tertentu jika pengguna atau peran IAM dibuat, saat kunci KMS dibuat, atau saat kebijakan kunci diubah. Anda dapat membuat aturan EventBridge acara yang memfilter tindakan API yang Anda tentukan dan kemudian mengaitkan target dengan aturan tersebut. Contoh target meliputi AWS Lambda fungsi, notifikasi Amazon Simple Notification Service (Amazon SNS), antrian Amazon Simple Queue Service (Amazon SQS), dan banyak lagi. Untuk informasi selengkapnya tentang pengiriman acara ke target, lihat Target bus acara di Amazon EventBridge.

Untuk informasi selengkapnya tentang pemantauan AWS KMS dengan EventBridge dan otomatisasi respons, lihat Memantau kunci KMS dengan Amazon EventBridge dalam dokumentasi. AWS KMS

Praktik terbaik manajemen biaya dan penagihan untuk AWS KMS

Melalui luas dan mendalam, Layanan AWS tawarkan fleksibilitas untuk mengelola biaya Anda sambil memenuhi persyaratan bisnis. Bagian ini mencakup harga untuk penyimpanan kunci di AWS Key Management Service (AWS KMS), dan memberikan rekomendasi untuk mengurangi biaya, seperti melalui caching kunci. Anda juga dapat meninjau penggunaan kunci KMS untuk menentukan apakah ada peluang tambahan untuk mengurangi biaya.

Bagian ini membahas topik manajemen biaya dan penagihan berikut:

- AWS KMS harga untuk penyimpanan kunci
- Kunci bucket Amazon S3 dengan enkripsi default
- Menyembunyikan kunci data dengan menggunakan AWS Encryption SDK
- Alternatif untuk caching kunci dan kunci bucket Amazon S3
- Mengelola biaya logging untuk penggunaan kunci KMS

AWS KMS harga untuk penyimpanan kunci

Setiap AWS KMS key yang Anda buat AWS KMS dikenakan biaya. Biaya bulanan sama untuk kunci simetris, kunci asimetris, kunci HMAC, kunci Multi-wilayah (masing-masing kunci utama dan setiap replika Multi-wilayah), kunci dengan bahan kunci yang diimpor, dan kunci KMS dengan asal kunci dari salah satu atau penyimpanan kunci eksternal. AWS CloudHSM

Untuk kunci KMS yang Anda putar secara otomatis atau sesuai permintaan, rotasi kunci pertama dan kedua menambahkan biaya bulanan tambahan (prorata per jam) dalam biaya. Setelah rotasi kedua, setiap rotasi berikutnya di bulan itu tidak ditagih. Silakan lihat AWS KMS harga untuk informasi harga terbaru.

Anda dapat menggunakan AWS Budgetsuntuk mengkonfigurasi anggaran penggunaan. AWS Budgets dapat mengingatkan Anda ketika pengeluaran dalam akun Anda melebihi ambang batas tertentu. Untuk biaya yang terkait AWS KMS, Anda dapat membuat anggaran penggunaan untuk memberi tahu berdasarkan kunci atau permintaan KMS. Ini dapat meningkatkan visibilitas Anda ke penyimpanan AWS KMS kunci dan biaya penggunaan Anda.

Kunci bucket Amazon S3 dengan enkripsi default

Dalam beberapa kasus penggunaan, beban kerja yang mengakses atau menghasilkan sejumlah besar objek di Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) dapat menghasilkan volume permintaan yang tinggi AWS KMS, yang meningkatkan biaya Anda. Mengonfigurasi kunci bucket Amazon S3 dapat membantu Anda mengurangi biaya hingga 99%. Ini adalah alternatif yang direkomendasikan untuk menonaktifkan enkripsi untuk membantu mengurangi biaya yang terkait dengannya. AWS KMS

Menyembunyikan kunci data dengan menggunakan AWS Encryption SDK

Saat menggunakan enkripsi sisi klien AWS Encryption SDKuntuk melakukan enkripsi sisi klien, caching kunci data dapat membantu meningkatkan kinerja aplikasi Anda, mengurangi risiko permintaan aplikasi Anda AWS KMS dibatasi, dan membantu Anda mengurangi biaya. Untuk informasi selengkapnya tentang cara memulai, lihat Cara menggunakan caching kunci data.

Alternatif untuk caching kunci dan kunci bucket Amazon S3

Jika caching kunci bukan merupakan pilihan bagi Anda karena persyaratan penanganan data Anda, Anda juga dapat meminta peningkatan AWS KMS kuota dengan menggunakan Konsol Manajemen AWS atau Service Quotas API. Pertimbangkan volume panggilan API yang mungkin Anda lakukan. Jumlah panggilan API yang Anda lakukan merupakan faktor penting dalam AWS KMS penetapan harga. Jika Anda meningkatkan kuota request-rate untuk menskalakan kinerja Anda, semakin banyak permintaan yang menimbulkan biaya tambahan. AWS KMS

Mengelola biaya logging untuk penggunaan kunci KMS

Semua panggilan AWS KMS API dicatat AWS CloudTrail. Aplikasi dan layanan dapat menghasilkan volume besar panggilan AWS KMS API (seperti untuk operasi kriptografi, termasuk enkripsi dan dekripsi). Mungkin sulit untuk meninjau CloudTrail log tanpa alat yang membantu Anda mengatur data tersebut, menyelidiki tren, dan mencari aktivitas API anomali. Amazon Athena menyediakan struktur data yang telah ditentukan sebelumnya yang dapat membantu Anda dengan cepat mengatur tabel untuk CloudTrail log dan mulai menganalisis data log Anda. Ini sangat berguna untuk analisis ad-hoc atau penyelidikan lebih lanjut selama respons insiden. Untuk informasi selengkapnya, lihat AWS CloudTrail Log kueri di dokumentasi Athena.

Karena Anda membayar berdasarkan per kueri untuk Athena, Anda dapat mengatur tabel Anda di muka tanpa biaya. Tidak ada biaya untuk pernyataan bahasa definisi data. Ketika Anda menanggapi suatu insiden, ini membantu Anda memastikan bahwa banyak prasyarat sudah terpenuhi. Untuk membantu Anda mempersiapkan, itu adalah praktik terbaik untuk menulis pertanyaan Anda setelah membuat tabel Anda, mengujinya, dan memastikan bahwa mereka menghasilkan hasil yang Anda inginkan. Anda dapat menyimpan kueri Anda di Athena untuk digunakan di masa mendatang. Untuk informasi selengkapnya tentang cara memulai dengan Athena, lihat Memulai Amazon Athena.

Peristiwa data memberikan visibilitas ke dalam operasi yang dilakukan pada atau di dalam sumber daya. Ini juga dikenal sebagai operasi pesawat data. Contohnya termasuk `PutObject` peristiwa Amazon S3 atau panggilan API operasi fungsi Lambda. Peristiwa data seringkali merupakan aktivitas bervolume tinggi, dan Anda dikenakan biaya untuk mencatatnya. Untuk membantu mengontrol volume peristiwa data yang dicatat ke jejak atau penyimpanan data peristiwa CloudTrail, Anda dapat mengoptimalkan pencatatan untuk mengurangi biaya CloudTrail AWS KMS, dan Amazon S3 dengan mengonfigurasi pemilih peristiwa lanjutan untuk membatasi peristiwa data mana yang akan masuk. CloudTrail Untuk informasi selengkapnya, lihat Cara mengoptimalkan AWS CloudTrail biaya dengan menggunakan pemilih acara lanjutan (posting AWS blog).

Sumber daya

AWS Key Management Service (AWS KMS) dokumentasi

- AWS KMS Panduan Pengembang
- Referensi AWS KMS API
- AWS KMS dalam AWS CLI Referensi

Alat

- AWS Encryption SDK

AWS Bimbingan Preskriptif

Strategi

- Membuat strategi enkripsi untuk data saat istirahat

Panduan

- Praktik dan fitur terbaik enkripsi untuk Layanan AWS
- AWS Arsitektur Referensi Privasi (AWS PRA)

Pola

- Secara otomatis mengenkripsi volume Amazon EBS
- Secara otomatis memulihkan instans dan klaster Amazon RDS DB yang tidak terenkripsi
- Memantau dan memulihkan penghapusan terjadwal AWS KMS keys

Kontributor

Mengotorisasi

- Frank Phillis, Arsitek Solusi Spesialis Senior GTM, AWS
- Ken Beer, Direktur AWS KMS dan Perpustakaan Crypto, AWS
- Michael Miller, Arsitek Solusi Senior, AWS
- Jeremy Stieglitz, Manajer Produk Utama, AWS
- Zach Miller, Arsitek Solusi Utama, AWS
- Peter M. O'Donnell, Arsitek Solusi Utama, AWS
- Patrick Palmer, Arsitek Solusi Utama, AWS
- Dave Walker, Arsitek Solusi Utama, AWS

Meninjau

- Manigandan Shri, Konsultan Pengiriman Senior, AWS

Penulisan teknis

- Lilly AbouHarb, Penulis Teknis Senior, AWS
- Kimberly Garmoe, Penulis Teknis Senior, AWS

Riwayat dokumen

Tabel berikut menjelaskan perubahan signifikan pada panduan ini. Jika Anda ingin diberi tahu tentang pembaruan masa depan, Anda dapat berlangganan umpan RSS.

Perubahan	Deskripsi	Tanggal
Publikasi awal	—	24 Maret 2025

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.