AWS Key Management Service migliori pratiche

AWS Linee guida prescrittive

AWS Linee guida prescrittive: AWS Key Management Service migliori pratiche

Table of Contents

AWS Key Management Service migliori pratiche

Amazon Web Services (collaboratori)

Marzo 2025 (cronologia dei documenti)

AWS Key Management Service (AWS KMS) è un servizio gestito che semplifica la creazione e il controllo delle chiavi crittografiche utilizzate per proteggere i dati. Questa guida descrive come utilizzarla in modo efficace AWS KMS e fornisce le migliori pratiche. Ti aiuta a confrontare le opzioni di configurazione e a scegliere il set migliore per le tue esigenze.

Questa guida include consigli su come l'organizzazione può utilizzare per AWS KMS proteggere le informazioni sensibili e implementare la firma per diversi casi d'uso. Considera le raccomandazioni attuali che utilizzano le seguenti dimensioni:

- Gestione delle chiavi: opzioni di delega per la gestione e le scelte di archiviazione delle chiavi
- Protezione dei dati: crittografia dei dati all'interno delle applicazioni aziendali anziché Servizi AWS operazioni eseguite per conto dell'utente
- Gestione degli accessi: utilizzo di policy AWS KMS chiave e policy AWS Identity and Access Management (IAM) per implementare il controllo degli accessi basato sui ruoli (RBAC) o il controllo degli accessi basato sugli attributi (ABAC).
- Architettura multiaccount e multiregione: consigli per implementazioni su larga scala.
- Fatturazione e gestione dei costi: comprensione dei costi e dell'utilizzo e consigli su come ridurre i costi.
- Controlli investigativi: monitoraggio dello stato delle chiavi KMS, delle impostazioni di crittografia e dei dati crittografati.
- Risposta agli incidenti: correzione delle configurazioni errate che comportano la non conformità alle politiche di protezione dei dati.

Obiettivi aziendali specifici

I tuoi dati sono una risorsa fondamentale e sensibile per la tua azienda. Con AWS KMS, gestisci le chiavi crittografiche utilizzate per proteggere e verificare i tuoi dati. Sei tu a controllare come vengono utilizzati i tuoi dati, chi può accedervi e come vengono crittografati. Questa guida ha lo scopo di aiutare gli sviluppatori, gli amministratori di sistema e i professionisti della sicurezza a implementare le migliori pratiche di crittografia che aiutano a proteggere i dati sensibili archiviati

o Servizi AWS trasmessi. Comprendendo e implementando i consigli contenuti in questa guida, è possibile promuovere la riservatezza e l'integrità dei dati in tutto l' AWS ambiente. Puoi soddisfare i tuoi requisiti di protezione dei dati, indipendentemente dal fatto che tali requisiti siano formulati internamente o che tu abbia requisiti specifici per un programma di conformità o convalida. Per ulteriori informazioni su come AWS KMS contribuire a proteggere i dati nel proprio AWS ambiente, vedere Utilizzo della AWS KMS crittografia con Servizi AWS nella documentazione. AWS KMS

Informazioni su AWS KMS keys

AWS Key Management Service (AWS KMS) consente di creare chiavi crittografiche che possono essere utilizzate sui dati trasmessi al servizio. Il tipo di risorsa principale è la chiave KMS, di cui esistono tre tipi:

- Chiavi simmetriche Advanced Encryption Standard (AES): si tratta di chiavi a 256 bit utilizzate nella modalità Galois Counter Mode (GCM) di AES. Queste chiavi forniscono la crittografia e la decrittografia autenticate di dati di dimensioni inferiori a 4 KB. Questo è il tipo di chiave più comune. Viene utilizzato per proteggere altre chiavi di dati, come quelle utilizzate nelle applicazioni o Servizi AWS che crittografano i dati per conto dell'utente.
- Chiavi asimmetriche a curva ellittica o RSA: queste chiavi sono disponibili in varie dimensioni e supportano molti algoritmi. A seconda dell'algoritmo, possono essere utilizzate per la crittografia e la decrittografia e per le operazioni di firma e verifica.
- Chiavi simmetriche per eseguire operazioni HMAC (Message Authentication Code) basate su hash: si tratta di chiavi a 256 bit utilizzate per le operazioni di firma e verifica.

Le chiavi KMS non possono essere esportate dal servizio in testo normale. Sono generate e possono essere utilizzate solo all'interno dei moduli di sicurezza hardware (HSMs) utilizzati dal servizio. Si tratta di una proprietà di sicurezza fondamentale AWS KMS per prevenire compromissioni chiave. Nelle regioni di Cina (Pechino) e Cina (Ningxia), questi HSMs sono certificati dall'OSCCA. In tutte le altre regioni, le informazioni HSMs utilizzate AWS KMS sono convalidate nell'ambito del programma FIPS 140 all'interno del NIST al livello di sicurezza 3. Per ulteriori informazioni sulla progettazione e sui controlli AWS KMS che aiutano a proteggere le chiavi, consulta AWS Key Management Service Dettagli crittografici.

Puoi inviare dati AWS KMS utilizzando diverse opzioni crittografiche per eseguire operazioni di crittografia APIs , decrittografia, firma o verifica con le chiavi KMS. Puoi anche scegliere di fare in modo che una chiave KMS agisca come una chiave di crittografia a chiave, che protegge un tipo di chiave chiamato chiave dati. È possibile esportare una chiave dati AWS KMS per utilizzarla all'interno dell'applicazione locale o una chiave Servizio AWS che protegge i dati per conto dell'utente. L'uso delle chiavi dati è comune in tutti i sistemi di gestione delle chiavi e viene spesso definito crittografia a busta. La crittografia a busta consente di utilizzare una chiave dati sul sistema remoto che gestisce i dati sensibili, anziché dover inviare i dati sensibili AWS KMS per la crittografia direttamente tramite una chiave KMS.

Per ulteriori informazioni, consulta AWS KMS keysgli elementi essenziali AWS KMS della crittografia nella documentazione. AWS KMS

Best practice di gestione delle chiavi per AWS KMS

Quando si utilizza AWS Key Management Service (AWS KMS), è necessario prendere alcune decisioni di progettazione fondamentali. Queste includono se utilizzare un modello centralizzato o decentralizzato per la gestione e l'accesso alle chiavi, il tipo di chiavi da utilizzare e il tipo di archivio chiavi da utilizzare. Le sezioni seguenti consentono di prendere le decisioni giuste per l'organizzazione e i casi d'uso. Questa sezione si conclude con importanti considerazioni sulla disabilitazione e l'eliminazione delle chiavi KMS, comprese le azioni da intraprendere per proteggere dati e chiavi.

Questa sezione contiene i seguenti argomenti:

Scelta di un modello centralizzato o decentralizzato

AWS consiglia di utilizzare più account Account AWS e gestirli come un'unica organizzazione in AWS Organizations. Esistono due approcci generali alla gestione AWS KMS keys in ambienti con più account.

Il primo approccio è un approccio decentralizzato, in cui si creano chiavi in ogni account che utilizza tali chiavi. Quando si archiviano le chiavi KMS negli stessi account delle risorse che proteggono, è più facile delegare le autorizzazioni agli amministratori locali che comprendono i requisiti di accesso per i propri principali e chiavi. AWS Puoi autorizzare l'utilizzo delle chiavi utilizzando solo una policy chiave oppure puoi combinare una policy chiave e politiche basate sull'identità in (IAM). AWS Identity and Access Management

Il secondo approccio è un approccio centralizzato, in cui le chiavi KMS vengono mantenute in una o più aree designate. Account AWS Consenti ad altri account di utilizzare le chiavi solo per operazioni crittografiche. Puoi gestire le chiavi, il loro ciclo di vita e le relative autorizzazioni dall'account centralizzato. Consenti Account AWS ad altri di utilizzare la chiave ma non consenti altre autorizzazioni. Gli account esterni non possono gestire nulla sul ciclo di vita della chiave o sull'autorizzazione di accesso. Questo modello centralizzato può aiutare a ridurre al minimo il rischio

di eliminazione involontaria delle chiavi o di aumento dei privilegi da parte di amministratori o utenti delegati.

L'opzione scelta dipende da diversi fattori. Quando scegli un approccio, considera quanto segue:

1. Disponete di un processo automatico o manuale per il provisioning dell'accesso a chiavi e risorse? Ciò include risorse come pipeline di distribuzione e modelli di infrastruttura come codice (IaC). Questi strumenti possono aiutarti a distribuire e gestire risorse (come chiavi KMS, politiche chiave, ruoli IAM e politiche IAM) su molte piattaforme. Account AWS Se non disponi di questi strumenti di implementazione, un approccio centralizzato alla gestione delle chiavi potrebbe essere più gestibile per la tua azienda.
2. Hai il controllo amministrativo su tutti i file Account AWS che contengono risorse che utilizzano le chiavi KMS? In tal caso, un modello centralizzato può semplificare la gestione ed eliminare la necessità di passare Account AWS alla gestione delle chiavi. Tieni presente, tuttavia, che i ruoli IAM e le autorizzazioni degli utenti per l'utilizzo delle chiavi devono comunque essere gestiti per account.
3. Devi offrire l'accesso per utilizzare le tue chiavi KMS a clienti o partner che dispongono delle proprie risorse Account AWS ? Per queste chiavi, un approccio centralizzato può ridurre l'onere amministrativo per clienti e partner.
4. Avete requisiti di autorizzazione per l'accesso alle AWS risorse che possono essere risolti meglio con un approccio di accesso centralizzato o locale? Ad esempio, se diverse applicazioni o unità aziendali sono responsabili della gestione della sicurezza dei propri dati, è preferibile un approccio decentralizzato alla gestione delle chiavi.
5. Stai superando le quote di risorse di servizio per? AWS KMS Poiché queste quote sono stabilite per volta Account AWS, un modello decentralizzato distribuisce il carico tra gli account, moltiplicando in modo efficace le quote di servizio.

> **Note**
>
> Il modello di gestione delle chiavi è irrilevante quando si considerano le quote di richiesta, poiché tali quote vengono applicate all'intestatario del conto che effettua una richiesta relativa alla chiave, non all'account che possiede o gestisce la chiave.

In generale, consigliamo di iniziare con un approccio decentralizzato, a meno che non sia possibile esprimere la necessità di un modello di chiave KMS centralizzato.

Scelta di chiavi gestite dal cliente, chiavi AWS gestite o chiavi di proprietà AWS

Le chiavi KMS create e gestite per essere utilizzate nelle vostre applicazioni crittografiche sono note come chiavi gestite dal cliente. Servizi AWS può utilizzare chiavi gestite dal cliente per crittografare i dati archiviati dal servizio per conto dell'utente. Le chiavi gestite dal cliente sono consigliate se desideri il pieno controllo sul ciclo di vita e sull'utilizzo delle chiavi. È previsto un costo mensile per avere una chiave gestita dal cliente nel proprio account. Inoltre, le richieste di utilizzo o gestione della chiave comportano un costo di utilizzo. Per ulteriori informazioni, consultare Prezzi di AWS KMS.

Se desideri Servizio AWS crittografare i tuoi dati ma non vuoi sostenere i costi o i costi di gestione delle chiavi, puoi utilizzare una chiave gestita.AWS Questo tipo di chiave esiste nel tuo account, ma può essere utilizzato solo in determinate circostanze. Può essere utilizzata solo nel contesto in Servizio AWS cui operi e può essere utilizzata solo dai responsabili all'interno dell'account che contiene la chiave. Non puoi gestire nulla sul ciclo di vita o sulle autorizzazioni di queste chiavi. Alcuni Servizi AWS utilizzano chiavi AWS gestite. Il formato di un alias di chiave AWS gestita è`aws/<service code>`. Ad esempio, una `aws/ebs` chiave può essere utilizzata solo per crittografare i volumi Amazon Elastic Block Store (Amazon EBS) nello stesso account della chiave e può essere utilizzata solo dai responsabili IAM di quell'account. Una chiave AWS gestita può essere utilizzata solo dagli utenti di quell'account e per le risorse in quell'account. Non è possibile condividere risorse crittografate con una chiave AWS gestita con altri account. Se questa è una limitazione per il tuo caso d'uso, ti consigliamo di utilizzare invece una chiave gestita dal cliente; puoi condividere l'uso di quella chiave con qualsiasi altro account. Non ti viene addebitato alcun costo per l'esistenza di una chiave AWS gestita nel tuo account, ma qualsiasi utilizzo di questo tipo di chiave ti viene addebitato dalla Servizio AWS chiave assegnata alla chiave.

Una chiave AWS gestita è un tipo di chiave legacy che non viene più creata per essere utilizzata Servizi AWS come nuova a partire dal 2021. Invece, le nuove (e le versioni precedenti) Servizi AWS utilizzano una chiave AWS proprietaria per crittografare i dati per impostazione predefinita. AWS le chiavi di proprietà sono una raccolta di chiavi KMS Servizio AWS possedute e gestite per essere utilizzate in più lingue. Account AWS Sebbene queste chiavi non siano presenti nel tuo account Account AWS, Servizio AWS puoi utilizzarne una per proteggere le risorse del tuo account.

Ti consigliamo di utilizzare chiavi gestite dal cliente quando il controllo granulare è più importante e di utilizzare chiavi AWS di proprietà quando la praticità è più importante.

La tabella seguente descrive le principali differenze in termini di politica, registrazione, gestione e prezzo tra ciascun tipo di chiave. Per ulteriori informazioni sui tipi di chiave, consulta AWS KMS i concetti.

Considerazione	Chiavi gestite dal cliente	AWS chiavi gestite	AWS chiavi possedute
Policy della chiave	Controllato esclusiva mente dal cliente	Controllato dal servizio; visualizzabile dal cliente	Controllato esclusiva mente e visualizzabile solo da chi crittogra fa Servizio AWS i tuoi dati
Registrazione di log	AWS CloudTrail percorso dei clienti o archivio dati sugli eventi	CloudTrail percorso dei clienti o archivio dati sugli eventi	Non visualizzabile dal cliente
Gestione del ciclo di vita	Il cliente gestisce la rotazione, l'elimina zione e Regione AWS	Servizio AWS gestisce la rotazione (annuale), l'elimina zione e la regione	Servizio AWS gestisce la rotazione (annuale), l'elimina zione e la regione
Prezzi	Tariffa mensile per l'esistenza della chiave (tariffa oraria proporzionale); al chiamante viene addebitato un costo per l'utilizzo dell'API	Nessun costo per l'esistenza della chiave; al chiamante viene addebitato l'utilizzo dell'API	Nessun addebito per il cliente

Scelta di un negozio di AWS KMS chiavi

Un archivio di chiavi è un luogo sicuro per l'archiviazione e l'utilizzo di materiale contenente chiavi crittografiche. La migliore pratica del settore per gli archivi di chiavi consiste nell'utilizzare un dispositivo noto come modulo di sicurezza hardware (HSM) che è stato convalidato ai sensi del programma di convalida dei moduli crittografici FIPS 140 del NIST al livello di sicurezza 3. Esistono

altri programmi per supportare gli archivi di chiavi utilizzati per elaborare i pagamenti. AWS Payment Cryptographyè un servizio che puoi utilizzare per proteggere i dati relativi ai tuoi carichi di lavoro di pagamento.

AWS KMS supporta diversi tipi di archivio delle chiavi per proteggere il materiale chiave utilizzato AWS KMS per creare e gestire le chiavi di crittografia. Tutte le opzioni di archiviazione delle chiavi fornite da AWS KMS vengono continuamente convalidate secondo lo standard FIPS 140 al livello di sicurezza 3. Sono progettate per impedire a chiunque, compresi AWS gli operatori, di accedere alle chiavi in chiaro o di utilizzarle senza la vostra autorizzazione. Per ulteriori informazioni sui tipi di archivi di chiavi disponibili, consulta Key store nella AWS KMS documentazione.

L'archivio chiavi AWS KMS standard è la scelta migliore per la maggior parte dei carichi di lavoro. Se devi scegliere un tipo diverso di key store, valuta attentamente se i requisiti normativi o di altro tipo (ad esempio interni) impongano questa scelta e valuta attentamente i costi e i benefici.

Eliminazione e disabilitazione delle chiavi KMS

L'eliminazione di una chiave KMS può avere un impatto significativo. Prima di eliminare una chiave KMS che non intendi più utilizzare, valuta se è adeguato impostare lo stato della chiave su Disabilitato. Sebbene una chiave sia disabilitata, non può essere utilizzata per operazioni crittografiche. Esiste ancora in e AWS, se necessario, è possibile riattivarlo in futuro. Le chiavi disattivate continuano a comportare costi di archiviazione. Si consiglia di disabilitare le chiavi anziché eliminarle finché non si è certi che la chiave non protegga alcun dato o chiave di dati.

> **Important**
>
> L'eliminazione di una chiave deve essere pianificata con attenzione. I dati non possono essere decrittografati se la chiave corrispondente è stata eliminata. AWS non ha mezzi per recuperare una chiave eliminata dopo che è stata eliminata. Come per altre operazioni critiche AWS, è necessario applicare una politica che limiti chi può pianificare l'eliminazione delle chiavi e richiedere l'autenticazione a più fattori (MFA) per l'eliminazione delle chiavi.

Per evitare l'eliminazione accidentale delle chiavi, AWS KMS impone un periodo di attesa minimo predefinito di sette giorni dopo l'esecuzione di una `DeleteKey` chiamata prima che questa elimini la chiave. È possibile impostare il periodo di attesa su un valore massimo di 30 giorni. Durante il periodo di attesa, la chiave è ancora memorizzata AWS KMS in uno stato di cancellazione in sospeso. Non può essere utilizzata per operazioni di crittografia o decrittografia. Qualsiasi tentativo di utilizzare

una chiave che si trova nello stato In attesa di eliminazione per la crittografia o la decrittografia viene registrato in. AWS CloudTrail Puoi impostare un CloudWatch allarme Amazon per questi eventi nei tuoi CloudTrail log. Se ricevi allarmi relativi a questi eventi, puoi scegliere di annullare il processo di eliminazione, se necessario. Fino alla scadenza del periodo di attesa, è possibile ripristinare la chiave dallo stato In sospeso di eliminazione e ripristinarla allo stato Disabilitato o Abilitato.

L'eliminazione di una chiave multiregionale richiede l'eliminazione delle repliche prima della copia originale. Per ulteriori informazioni, vedere Eliminazione delle chiavi multiregionali.

Se si utilizza una chiave con materiale chiave importato, è possibile eliminare immediatamente il materiale chiave importato. Ciò è diverso dall'eliminazione di una chiave KMS in diversi modi. Quando si esegue l'**`DeleteImportedKeyMaterial`**azione, AWS KMS elimina il materiale chiave e lo stato della chiave passa a Importazione in sospeso. Dopo aver eliminato il materiale chiave, quest'ultimo diventa immediatamente inutilizzabile. Non è previsto alcun periodo di attesa. Per abilitare nuovamente l'uso della chiave, è necessario importare nuovamente lo stesso materiale chiave. Il periodo di attesa per l'eliminazione delle chiavi KMS si applica anche alle chiavi KMS con materiale chiave importato.

Se le chiavi dati sono protette da una chiave KMS e vengono utilizzate attivamente da Servizi AWS, non ne risentono immediatamente se la chiave KMS associata viene disabilitata o se il materiale chiave importato viene eliminato. Ad esempio, supponiamo che una chiave con materiale importato sia stata utilizzata per crittografare un oggetto con SSE-KMS. Stai caricando l'oggetto in un bucket Amazon Simple Storage Service (Amazon S3). Prima di caricare l'oggetto nel bucket, importi il materiale nella tua chiave. Dopo aver caricato l'oggetto, elimini il materiale chiave importato da quella chiave. L'oggetto rimane nel bucket in uno stato crittografato, ma nessuno può accedervi finché il materiale chiave eliminato non viene reimportato nella chiave. Sebbene questo flusso richieda un'automazione precisa per l'importazione e l'eliminazione del materiale chiave da una chiave, può fornire un ulteriore livello di controllo all'interno di un ambiente.

AWS offre una guida prescrittiva per aiutarvi a monitorare e correggere (se necessario) l'eliminazione programmata delle chiavi KMS. Per ulteriori informazioni, consulta Monitorare e correggere l'eliminazione pianificata delle chiavi. AWS KMS

Le migliori pratiche di protezione dei dati per AWS KMS

Questa sezione ti aiuta a fare delle scelte sull'utilizzo delle chiavi AWS Key Management Service (AWS KMS) per la protezione dei dati, ad esempio quali chiavi utilizzare per ogni tipo di dati. Fornisce inoltre esempi specifici di utilizzo AWS KMS con diversi Servizi AWS. Questi consigli ed esempi aiutano a capire quante chiavi potrebbero essere necessarie e quali principi richiedono le autorizzazioni per utilizzarle.

La sezione illustra anche la rotazione dei tasti. La rotazione delle chiavi è la pratica di sostituire una chiave KMS esistente con una nuova chiave o di sostituire il materiale crittografico associato a una chiave KMS esistente con nuovo materiale. Questa guida fornisce esempi e istruzioni su come ruotare le chiavi KMS per usi più comuni. Servizi AWS I consigli e gli esempi sono progettati per aiutarti a fare scelte informate sulla tua strategia di rotazione chiave.

Infine, questa sezione fornisce consigli su come utilizzare AWS Encryption SDK, uno strumento per implementare la crittografia lato client nelle applicazioni. Questa sezione include le scelte di progettazione che è possibile effettuare in base al set di funzionalità e alle funzionalità di. AWS Encryption SDK

In questa sezione vengono descritti i seguenti argomenti relativi alla crittografia:

- Crittografia con AWS KMS
- Rotazione dei tasti e ambito di impatto AWS KMS
- Consigli per l'utilizzo di AWS Encryption SDK

Crittografia con AWS KMS

La crittografia è una best practice generale per proteggere la riservatezza e l'integrità delle informazioni sensibili. È necessario utilizzare i livelli di classificazione dei dati esistenti e disporre di almeno una AWS Key Management Service (AWS KMS) chiave per livello. Ad esempio, è possibile definire una chiave KMS per i dati classificati come riservati, una per uso solo interno e una per dati sensibili. Ciò consente di assicurarsi che solo gli utenti autorizzati dispongano delle autorizzazioni per utilizzare le chiavi associate a ciascun livello di classificazione.

> **Note**
>
> Una singola chiave KMS gestita dal cliente può essere utilizzata su qualsiasi combinazione di applicazioni Servizi AWS o sulle proprie applicazioni che archiviano i dati di una particolare

classificazione. Il fattore limitante nell'utilizzo di una chiave su più carichi di lavoro Servizi AWS è la complessità delle autorizzazioni di utilizzo per controllare l'accesso ai dati tra un insieme di utenti. Il documento JSON della politica AWS KMS chiave deve pesare meno di 32 KB. Se questa restrizione di dimensione diventa una limitazione, prendi in considerazione l'utilizzo di AWS KMS sovvenzioni o la creazione di più chiavi per ridurre al minimo le dimensioni del documento di policy chiave.

Invece di affidarti solo alla classificazione dei dati per partizionare la tua chiave KMS, puoi anche scegliere di assegnare una chiave KMS da utilizzare per la classificazione dei dati all'interno di una singola chiave. Servizio AWS Ad esempio, tutti i dati etichettati `Sensitive` in Amazon Simple Storage Service (Amazon S3) devono essere crittografati con una chiave KMS con un nome simile a. `S3-Sensitive` Puoi distribuire ulteriormente i dati su più chiavi KMS all'interno della tua applicazione e/o classificazione dei dati definita. Servizio AWS Ad esempio, potresti essere in grado di eliminare alcuni set di dati in un periodo di tempo specifico ed eliminare altri set di dati in un periodo di tempo diverso. Puoi utilizzare i tag di risorsa per identificare e ordinare i dati crittografati con chiavi KMS specifiche.

Se scegli un modello di gestione decentralizzato per le chiavi KMS, dovresti applicare dei guardrail per assicurarti che vengano create nuove risorse con una determinata classificazione e utilizzare le chiavi KMS previste con le autorizzazioni corrette. Per ulteriori informazioni su come applicare, rilevare e gestire la configurazione delle risorse utilizzando l'automazione, consulta la sezione di questa guida. Rilevamento e monitoraggio

Questa sezione tratta i seguenti argomenti sulla crittografia:

- Registra la crittografia dei dati con AWS KMS
- Crittografia per impostazione predefinita
- Crittografia del database con AWS KMS
- Crittografia dei dati PCI DSS con AWS KMS
- Utilizzo delle chiavi KMS con Amazon EC2 Auto Scaling

Registra la crittografia dei dati con AWS KMS

Molti Servizi AWS, come Amazon GuardDuty and AWS CloudTrail, offrono opzioni per crittografare i dati di log inviati ad Amazon S3. Quando si esportano i risultati GuardDuty da Amazon S3, è necessario utilizzare una chiave KMS. Ti consigliamo di crittografare tutti i dati di registro e di

concedere l'accesso alla decrittografia solo ai responsabili autorizzati, come i team di sicurezza, i soccorritori e gli auditor.

La AWS Security Reference Architecture consiglia di creare una centrale per la registrazione. Account AWS In questo modo, è anche possibile ridurre il sovraccarico di gestione delle chiavi. Ad esempio, con CloudTrail, puoi creare un percorso organizzativo o un data store di eventi per registrare gli eventi all'interno dell'organizzazione. Quando configuri il percorso organizzativo o il data store di eventi, puoi specificare un singolo bucket Amazon S3 e una chiave KMS nell'account di registrazione designato. Questa configurazione si applica a tutti gli account dei membri dell'organizzazione. Tutti gli account inviano quindi i propri CloudTrail log al bucket Amazon S3 nell'account di registrazione e i dati di registro vengono crittografati con la chiave KMS specificata. È necessario aggiornare la politica delle chiavi per questa chiave KMS per concedere le autorizzazioni necessarie per CloudTrail utilizzarla. Per ulteriori informazioni, consulta Configurare le politiche AWS KMS chiave CloudTrail nella CloudTrail documentazione.

Per proteggere CloudTrail i log GuardDuty and, il bucket Amazon S3 e la chiave KMS devono trovarsi nello stesso posto. Regione AWS La AWS Security Reference Architecture fornisce anche indicazioni sulla registrazione e sulle architetture multi-account. Quando aggregate i log tra più regioni e account, consultate la sezione Creazione di un percorso per un'organizzazione nella CloudTrail documentazione per saperne di più sulle regioni che accettano l'iscrizione e assicuratevi che la registrazione centralizzata funzioni come previsto.

Crittografia per impostazione predefinita

Servizi AWS che archiviano o elaborano i dati in genere offrono la crittografia a riposo. Questa funzionalità di sicurezza aiuta a proteggere i dati crittografandoli quando non sono in uso. Gli utenti autorizzati possono comunque accedervi quando necessario.

Le opzioni di implementazione e crittografia variano tra Servizi AWS. Molte forniscono la crittografia per impostazione predefinita. È importante capire come funziona la crittografia per ogni servizio utilizzato. Di seguito vengono mostrati alcuni esempi:

- Amazon Elastic Block Store (Amazon EBS) — Quando abiliti la crittografia per impostazione predefinita, tutti i nuovi volumi Amazon EBS e le copie degli snapshot vengono crittografati. AWS Identity and Access Management I ruoli o gli utenti (IAM) non possono avviare istanze con volumi non crittografati o volumi che non supportano la crittografia. Questa funzionalità aiuta a garantire la sicurezza, la conformità e il controllo assicurando che tutti i dati archiviati nei volumi Amazon EBS siano crittografati. Per ulteriori informazioni sulla crittografia in questo servizio, consulta la crittografia di Amazon EBS nella documentazione di Amazon EBS.

- Amazon Simple Storage Service (Amazon S3) — Tutti i nuovi oggetti sono crittografati per impostazione predefinita. Amazon S3 applica automaticamente la crittografia lato server con chiavi gestite di Amazon S3 (SSE-S3) per ogni nuovo oggetto, a meno che non si specifichi un'opzione di crittografia diversa. I responsabili IAM possono comunque caricare oggetti non crittografati su Amazon S3 indicandolo esplicitamente nella chiamata API. In Amazon S3, per applicare la crittografia SSE-KMS, è necessario utilizzare una bucket policy con condizioni che richiedono la crittografia. Per un esempio di policy, consulta Require SSE-KMS per tutti gli oggetti scritti in un bucket nella documentazione di Amazon S3. Alcuni bucket Amazon S3 ricevono e servono un gran numero di oggetti. Se tali oggetti sono crittografati con chiavi KMS, un gran numero di operazioni Amazon S3 genera un gran numero `GenerateDataKey` di chiamate `Decrypt` e a. AWS KMS Ciò può aumentare i costi di utilizzo. AWS KMS Puoi configurare le bucket key di Amazon S3, in modo da ridurre significativamente i costi. AWS KMS Per ulteriori informazioni sulla crittografia in questo servizio, consulta Protezione dei dati con crittografia nella documentazione di Amazon S3.
- Amazon DynamoDB — DynamoDB è un servizio di database NoSQL completamente gestito che abilita la crittografia lato server a riposo per impostazione predefinita e non è possibile disabilitarla. Ti consigliamo di utilizzare una chiave gestita dal cliente per crittografare le tabelle DynamoDB. Questo approccio ti aiuta a implementare il privilegio minimo con autorizzazioni granulari e separazione dei compiti, rivolgendoti a utenti e ruoli IAM specifici nelle tue policy chiave. AWS KMS Puoi anche scegliere chiavi AWS gestite o AWS di proprietà quando configuri le impostazioni di crittografia per le tue tabelle DynamoDB. Per i dati che richiedono un elevato grado di protezione (in cui i dati devono essere visibili al client solo come testo non crittografato), prendi in considerazione l'utilizzo della crittografia lato client con Database Encryption SDK.AWS Per ulteriori informazioni sulla crittografia in questo servizio, consulta Protezione dei dati nella documentazione di DynamoDB.

Crittografia del database con AWS KMS

Il livello di implementazione della crittografia influisce sulla funzionalità del database. Di seguito sono riportati i compromessi da considerare:

- Se utilizzi solo la AWS KMS crittografia, lo storage che supporta le tabelle viene crittografato per DynamoDB e Amazon Relational Database Service (Amazon RDS). Ciò significa che il sistema operativo che esegue il database vede il contenuto dello storage come testo non crittografato. Tutte le funzioni del database, inclusa la generazione di indici e altre funzioni di ordine superiore che richiedono l'accesso ai dati in chiaro, continuano a funzionare come previsto.

- Amazon RDS è integrato nella crittografia Amazon Elastic Block Store (Amazon EBS) per fornire la crittografia completa del disco per volumi di database. Quando crei un'istanza di database crittografata con Amazon RDS, Amazon RDS crea un volume Amazon EBS crittografato per tuo conto per archiviare il database. I dati archiviati inattivi sul volume, gli snapshot del database, i backup automatici e le repliche di lettura sono tutti crittografati con la chiave KMS specificata al momento della creazione dell'istanza di database.
- Amazon Redshift si integra AWS KMS e crea una gerarchia di chiavi a quattro livelli che vengono utilizzate per crittografare il livello del cluster attraverso il livello dei dati. Quando avvii il cluster, puoi scegliere di utilizzare la crittografia. AWS KMS Solo l'applicazione Amazon Redshift e gli utenti con le autorizzazioni appropriate possono vedere il testo in chiaro quando le tabelle vengono aperte (e decrittografate) in memoria. Ciò è sostanzialmente analogo alle funzionalità di crittografia dei dati trasparente o basata su tabelle (TDE) disponibili in alcuni database commerciali. Ciò significa che tutte le funzioni del database, inclusa la generazione di indici e altre funzioni di ordine superiore che richiedono l'accesso ai dati in chiaro, continuano a funzionare come previsto.
- La crittografia a livello di dati lato client implementata tramite Database Encryption SDK (e strumenti simili) significa che sia il sistema operativo che il AWS database visualizzano solo testo cifrato. Gli utenti possono visualizzare il testo in chiaro solo se accedono al database da un client su cui è installato AWS Database Encryption SDK e hanno accesso alla chiave pertinente. Le funzioni di database di ordine superiore che richiedono l'accesso al testo in chiaro per funzionare come previsto, come la generazione di indici, non funzioneranno se indirizzate a operare su campi crittografati. Quando scegli di utilizzare la crittografia lato client, assicurati di utilizzare un meccanismo di crittografia robusto che aiuti a prevenire attacchi comuni contro i dati crittografati. Ciò include l'utilizzo di un potente algoritmo di crittografia e di tecniche appropriate, come un salt, per contribuire a mitigare gli attacchi di testo cifrato.

Si consiglia di utilizzare le funzionalità di crittografia AWS KMS integrate per AWS i servizi di database. Per i carichi di lavoro che elaborano dati sensibili, è necessario prendere in considerazione la crittografia lato client per i campi di dati sensibili. Quando si utilizza la crittografia lato client, è necessario considerare l'impatto sull'accesso al database, ad esempio i join all'interno di query SQL o la creazione di indici.

Crittografia dei dati PCI DSS con AWS KMS

I controlli di sicurezza e qualità sono AWS KMS stati convalidati e certificati per soddisfare i requisiti del Payment Card Industry Data Security Standard (PCI DSS). Ciò significa che puoi crittografare i dati del numero di conto primario (PAN) con una chiave KMS. L'uso di una chiave KMS per

crittografare i dati elimina parte dell'onere della gestione delle librerie di crittografia. Inoltre, le chiavi KMS non possono essere esportate da AWS KMS, il che riduce la preoccupazione che le chiavi di crittografia vengano archiviate in modo non sicuro.

Esistono altri modi per soddisfare i requisiti PCI DSS. AWS KMS Ad esempio, se utilizzi AWS KMS Amazon S3, puoi archiviare i dati PAN in Amazon S3 perché il meccanismo di controllo degli accessi per ogni servizio è distinto dall'altro.

Come sempre, quando esamini i requisiti di conformità, assicurati di ottenere consigli da parti adeguatamente esperte, qualificate e verificate. Siate consapevoli delle quote di AWS KMS richiesta quando progettate applicazioni che utilizzano direttamente la chiave per proteggere i dati delle transazioni con carta che rientrano nell'ambito del PCI DSS.

Poiché tutte le AWS KMS richieste sono registrate AWS CloudTrail, è possibile verificare l'utilizzo delle chiavi esaminando i registri. CloudTrail Tuttavia, se utilizzi le chiavi bucket di Amazon S3, non esiste alcuna voce che corrisponda a ogni azione di Amazon S3. Questo perché la chiave bucket crittografa le chiavi dati utilizzate per crittografare gli oggetti in Amazon S3. Sebbene l'uso di una chiave bucket non elimini tutte le chiamate API a AWS KMS, ne riduce il numero. Di conseguenza, non esiste più una one-to-one corrispondenza tra i tentativi di accesso agli oggetti di Amazon S3 e le chiamate API a. AWS KMS

Utilizzo delle chiavi KMS con Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling è un servizio consigliato per automatizzare il ridimensionamento delle istanze Amazon EC2. Ti aiuta ad assicurarti di avere a disposizione il numero corretto di istanze per gestire il carico dell'applicazione. Amazon EC2 Auto Scaling utilizza un ruolo collegato al servizio che fornisce le autorizzazioni appropriate per il servizio e ne autorizza le attività all'interno dell'account. Per utilizzare le chiavi KMS con Amazon EC2 Auto Scaling, AWS KMS le policy chiave devono consentire al ruolo collegato al servizio di utilizzare la chiave KMS con alcune operazioni API, ad esempio affinché l'automazione `Decrypt` sia utile. Se la policy AWS KMS chiave non autorizza il responsabile IAM che sta eseguendo l'operazione a condurre un'azione, tale azione verrà negata. Per ulteriori informazioni su come applicare correttamente le autorizzazioni nella policy chiave per consentire l'accesso, consulta la sezione Protezione dei dati in Amazon EC2 Auto Scaling nella documentazione di Amazon EC2 Auto Scaling.

Rotazione dei tasti e ambito di impatto AWS KMS

Non consigliamo la rotazione delle chiavi AWS Key Management Service (AWS KMS) a meno che non sia necessario ruotare le chiavi per la conformità alle normative. Ad esempio, potrebbe esserti

richiesto di ruotare le chiavi KMS a causa di politiche aziendali, regole contrattuali o normative governative. La progettazione di riduce AWS KMS in modo significativo i tipi di rischio che la rotazione delle chiavi viene generalmente utilizzata per mitigare. Se è necessario ruotare i tasti KMS, si consiglia di utilizzare la rotazione automatica dei tasti e di utilizzare la rotazione manuale dei tasti solo se la rotazione automatica dei tasti non è supportata.

Questa sezione tratta i seguenti argomenti sulla rotazione dei tasti:

- AWS KMS rotazione simmetrica dei tasti
- Rotazione delle chiavi per i volumi Amazon EBS
- Rotazione delle chiavi per Amazon RDS
- Rotazione delle chiavi per Amazon S3 e replica nella stessa regione
- Chiavi KMS rotanti con materiale importato

AWS KMS rotazione simmetrica dei tasti

AWS KMS supporta la rotazione automatica delle chiavi solo per le chiavi KMS di crittografia simmetrica con materiale chiave che crea. AWS KMS La rotazione automatica è opzionale per le chiavi KMS gestite dal cliente. Su base annuale, AWS KMS ruota il materiale chiave per le chiavi KMS AWS gestite. AWS KMS salva tutte le versioni precedenti del materiale crittografico per sempre, in modo da poter decrittografare tutti i dati crittografati con quella chiave KMS. AWS KMS non elimina alcun materiale con chiave ruotata finché non elimini la chiave KMS. Inoltre, quando si decrittografa un oggetto utilizzando AWS KMS, il servizio determina il materiale di supporto corretto da utilizzare per l'operazione di decrittografia; non è necessario fornire parametri di input aggiuntivi.

Poiché AWS KMS conserva le versioni precedenti del materiale chiave crittografico e poiché è possibile utilizzare tale materiale per decrittografare i dati, la rotazione delle chiavi non offre ulteriori vantaggi in termini di sicurezza. Il meccanismo di rotazione delle chiavi esiste per semplificare la rotazione delle chiavi se si utilizza un carico di lavoro in un contesto in cui lo richiedono requisiti normativi o di altro tipo.

Rotazione delle chiavi per i volumi Amazon EBS

Puoi ruotare le chiavi dati di Amazon Elastic Block Store (Amazon EBS) utilizzando uno dei seguenti approcci. L'approccio dipende dai flussi di lavoro, dai metodi di distribuzione e dall'architettura dell'applicazione. Potresti volerlo fare quando passi da una chiave AWS gestita a una chiave gestita dal cliente.

Utilizzare gli strumenti del sistema operativo per copiare i dati da un volume all'altro

1. Crea la nuova chiave KMS. Per istruzioni, consulta Creare una chiave KMS.
2. Crea un nuovo volume Amazon EBS con le stesse dimensioni o più grandi dell'originale. Per la crittografia, specifica la chiave KMS che hai creato. Per istruzioni, consulta Creare un volume Amazon EBS.
3. Monta il nuovo volume sulla stessa istanza o contenitore del volume originale. Per istruzioni, consulta Collegare un volume Amazon EBS a un'istanza Amazon EC2.
4. Utilizzando lo strumento del sistema operativo preferito, copia i dati dal volume esistente al nuovo volume.
5. Una volta completata la sincronizzazione, durante una finestra di manutenzione prestabilita, interrompi il traffico verso l'istanza. Per istruzioni, consulta Arrestare e avviare manualmente le istanze.
6. Smonta il volume originale. Per istruzioni, consulta Scollegare un volume Amazon EBS da un'istanza Amazon EC2.
7. Monta il nuovo volume sul punto di montaggio originale.
8. Verificate che il nuovo volume funzioni correttamente.
9. Eliminare il volume originale. Per istruzioni, consulta Eliminare un volume Amazon EBS.

Utilizzare uno snapshot di Amazon EBS per copiare i dati da un volume all'altro

1. Crea la nuova chiave KMS. Per istruzioni, consulta Creare una chiave KMS.
2. Crea uno snapshot Amazon EBS del volume originale. Per istruzioni, consulta Creare snapshot Amazon EBS.
3. Crea un nuovo volume dallo snapshot. Per la crittografia, specifica la nuova chiave KMS che hai creato. Per istruzioni, consulta Creare un volume Amazon EBS.

   > **Note**
   >
   > A seconda del carico di lavoro, potresti voler utilizzare il ripristino rapido degli snapshot di Amazon EBS per ridurre al minimo la latenza iniziale sul volume.

4. Crea una nuova istanza Amazon EC2. Per istruzioni, consulta Avvio di un'istanza Amazon EC2.
5. Collega il volume che hai creato all'istanza Amazon EC2. Per istruzioni, consulta Collegare un volume Amazon EBS a un'istanza Amazon EC2.

6. Trasforma la nuova istanza in produzione.
7. Ruota l'istanza originale dalla produzione ed eliminala. Per istruzioni, consulta Eliminare un volume Amazon EBS.

> **Note**
>
> È possibile copiare istantanee e modificare la chiave di crittografia utilizzata per la copia di destinazione. Dopo aver copiato lo snapshot e averlo crittografato con le tue chiavi KMS preferite, puoi anche creare un'Amazon Machine Image (AMI) dalle istantanee. Per ulteriori informazioni, consulta la crittografia Amazon EBS nella documentazione di Amazon EC2.

Rotazione delle chiavi per Amazon RDS

Per alcuni servizi, come Amazon Relational Database Service (Amazon RDS), la crittografia dei dati avviene all'interno del servizio ed è fornita da. AWS KMS Utilizza le seguenti istruzioni per ruotare una chiave per un'istanza di database Amazon RDS.

Per ruotare una chiave KMS per un database Amazon RDS

1. Crea un'istantanea del database crittografato originale. Per istruzioni, consulta Gestione dei backup manuali nella documentazione di Amazon RDS.
2. Copia l'istantanea in una nuova istantanea. Per la crittografia, specifica la nuova chiave KMS. Per istruzioni, consulta Copiare uno snapshot DB per Amazon RDS.
3. Usa la nuova istantanea per creare un nuovo cluster Amazon RDS. Per istruzioni, consulta Ripristino su un'istanza DB nella documentazione di Amazon RDS. Per impostazione predefinita, il cluster utilizza la nuova chiave KMS.
4. Verifica il funzionamento del nuovo database e dei dati in esso contenuti.
5. Trasforma il nuovo database in produzione.
6. Ruota il vecchio database dalla produzione ed eliminalo. Per istruzioni, consulta Eliminazione di un'istanza DB.

Rotazione delle chiavi per Amazon S3 e replica nella stessa regione

Per Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3), per modificare la chiave di crittografia di un oggetto, devi leggere e riscrivere l'oggetto. Quando riscrivi

l'oggetto, specifichi esplicitamente la nuova chiave di crittografia nell'operazione di scrittura. Per eseguire questa operazione per molti oggetti, puoi utilizzare Amazon S3 Batch Operations. Nelle impostazioni del lavoro, per l'operazione di copia, specifica le nuove impostazioni di crittografia. Ad esempio, puoi scegliere SSE-KMS e inserire il KeyID.

In alternativa, puoi utilizzare Amazon S3 Same-Region Replication (SRR). SSR può crittografare nuovamente gli oggetti in transito.

Chiavi KMS rotanti con materiale importato

AWS KMS non recupera o ruota il materiale chiave importato. Per ruotare una chiave KMS con materiale chiave importato, è necessario ruotare la chiave manualmente.

Consigli per l'utilizzo di AWS Encryption SDK

AWS Encryption SDKÈ uno strumento potente per implementare la crittografia lato client nelle applicazioni. Le librerie sono disponibili per Java JavaScript, C, Python e altri linguaggi di programmazione. Si integra con AWS Key Management Service ()AWS KMS. Puoi anche usarlo come SDK autonomo senza fare riferimento alle chiavi KMS.

Le pratiche consigliate per l'utilizzo di questo strumento includono un'attenta valutazione dei requisiti dell'applicazione. Bilancia questi requisiti con i rischi che possono essere introdotti da determinate configurazioni, come l'introduzione della memorizzazione nella cache delle chiavi nell'applicazione. Per ulteriori informazioni sulla memorizzazione nella cache delle chiavi di dati, consulta Data key caching nella documentazione. AWS Encryption SDK

Considerate le seguenti domande per determinare se utilizzare: AWS Encryption SDK

- Esiste un requisito per la crittografia lato client che non può essere soddisfatto dalla crittografia lato server con servizi che si integrano con? AWS KMS
- Siete in grado di proteggere adeguatamente le chiavi utilizzate per crittografare i dati lato client e come intendete farlo?
- Esistono altre librerie di fit-for-purpose crittografia che potrebbero adattarsi in modo più appropriato al tuo caso d'uso? Prendi in considerazione AWS offerte alternative, come la crittografia lato client Amazon S3 e AWS il Database Encryption SDK.

Per maggiori informazioni sulla scelta del servizio giusto per il tuo caso d'uso, consulta la documentazione di Crypto Tools.AWS

Best practice per la gestione delle identità e degli accessi per AWS KMS

Per utilizzare AWS Key Management Service (AWS KMS), devi disporre di credenziali che AWS possano essere utilizzate per autenticare e autorizzare le tue richieste. Nessun AWS principale dispone di alcuna autorizzazione per una chiave KMS a meno che tale autorizzazione non venga fornita esplicitamente e mai negata. Non esistono autorizzazioni implicite o automatiche per utilizzare o gestire una chiave KMS. Gli argomenti di questa sezione definiscono le migliori pratiche di sicurezza per aiutarti a determinare quali controlli di gestione degli AWS KMS accessi utilizzare per proteggere l'infrastruttura.

In questa sezione vengono descritti i seguenti argomenti sulla gestione delle identità e degli accessi:

- AWS KMS politiche chiave e politiche IAM
- Autorizzazioni con privilegi minimi per AWS KMS
- Controllo degli accessi basato sui ruoli per AWS KMS
- Controllo degli accessi basato sugli attributi per AWS KMS
- Contesto di crittografia per AWS KMS
- Risoluzione dei problemi relativi AWS KMS alle autorizzazioni

AWS KMS politiche chiave e politiche IAM

Il modo principale per gestire l'accesso alle AWS KMS risorse è tramite policy. Le policy sono documenti che descrivono quali principali possono accedere a quali risorse. Le politiche associate a un'identità AWS Identity and Access Management (IAM) (utenti, gruppi di utenti o ruoli) sono chiamate politiche basate sull'identità. Le politiche IAM che si collegano alle risorse sono chiamate politiche basate sulle risorse. AWS KMS le politiche relative alle risorse per le chiavi KMS sono chiamate politiche chiave. Oltre alle politiche IAM e alle politiche AWS KMS chiave, AWS KMS supporta le sovvenzioni. Le sovvenzioni forniscono un modo flessibile e potente per delegare le autorizzazioni. Puoi utilizzare le sovvenzioni per concedere l'accesso con chiave KMS a tempo determinato ai presidi IAM del tuo o di altri. Account AWS Account AWS

Tutte le chiavi KMS dispongono di una policy delle chiavi. Se non ne fornisci uno, ne AWS KMS crea uno per te. La politica di chiave predefinita AWS KMS utilizzata varia a seconda che si crei la chiave utilizzando la AWS KMS console o si utilizzi l' AWS KMS API. Ti consigliamo di modificare la politica

delle chiavi predefinita per allinearla ai requisiti della tua organizzazione per le autorizzazioni con privilegi minimi. Ciò dovrebbe inoltre essere in linea con la tua strategia di utilizzo delle policy IAM insieme alle policy chiave. Per ulteriori consigli sull'utilizzo delle policy IAM con AWS KMS, consulta le Best practice per le policy IAM nella AWS KMS documentazione.

Puoi utilizzare la policy chiave per delegare l'autorizzazione per un principal IAM alla policy basata sull'identità. Puoi anche utilizzare la politica chiave per perfezionare l'autorizzazione insieme alla politica basata sull'identità. In entrambi i casi, sia la politica chiave che la politica basata sull'identità determinano l'accesso, insieme a qualsiasi altra politica applicabile che disciplina l'accesso, come le politiche di controllo dei servizi (), le politiche di controllo delle risorse (SCPs) o i limiti delle autorizzazioni. RCPs Se il principale si trova in un account diverso da quello della chiave KMS, in sostanza, sono supportate solo le azioni crittografiche e di concessione. Per ulteriori informazioni su questo scenario tra più account, consulta Consentire agli utenti di altri account di utilizzare una chiave KMS nella documentazione. AWS KMS

È necessario utilizzare le policy basate sull'identità IAM in combinazione con le policy chiave per controllare l'accesso alle chiavi KMS. Le sovvenzioni possono essere utilizzate anche in combinazione con queste politiche per controllare l'accesso a una chiave KMS. Per utilizzare una politica basata sull'identità per controllare l'accesso a una chiave KMS, la politica chiave deve consentire all'account di utilizzare politiche basate sull'identità. È possibile specificare una dichiarazione politica chiave che abiliti le politiche IAM oppure specificare in modo esplicito i principi consentiti nella politica chiave.

Quando scrivi le policy, assicurati di disporre di controlli rigorosi che limitino chi può eseguire le seguenti azioni:

- Aggiorna, crea ed elimina le politiche IAM e le politiche chiave KMS
- Allega e scollega le politiche basate sull'identità da utenti, ruoli e gruppi
- Allega e scollega le politiche chiave dalle chiavi KMS AWS KMS
- Crea concessioni per le tue chiavi KMS: indipendentemente dal fatto che tu controlli l'accesso alle tue chiavi KMS esclusivamente con le politiche chiave o che combini le politiche chiave con le politiche IAM, dovresti limitare la possibilità di modificare le politiche. Implementa un processo di approvazione per modificare le politiche esistenti. Un processo di approvazione può aiutare a prevenire quanto segue:
  - Perdita accidentale delle autorizzazioni principali IAM: è possibile apportare modifiche che impediscano ai responsabili IAM di gestire la chiave o utilizzarla nelle operazioni crittografiche. In

scenari estremi, è possibile revocare le autorizzazioni di gestione delle chiavi a tutti gli utenti. In tal caso, è necessario contattare per riottenere l'accesso Supporto AWSalla chiave.

- Modifiche non approvate alle politiche chiave del KMS: se un utente non autorizzato ottiene l'accesso alla politica chiave, può modificarla per delegare le autorizzazioni a un destinatario o a un destinatario involontario. Account AWS
- Modifiche non approvate alle policy IAM: se un utente non autorizzato ottiene un set di credenziali con autorizzazioni per gestire l'appartenenza a un gruppo, potrebbe elevare le proprie autorizzazioni e apportare modifiche alle policy IAM, alle policy chiave, alla configurazione delle chiavi KMS o ad altre configurazioni AWS delle risorse.

Esamina attentamente i ruoli e gli utenti IAM associati ai dirigenti IAM designati come amministratori chiave del KMS. Questo può aiutare a prevenire cancellazioni o modifiche non autorizzate. Se devi modificare i principali che hanno accesso alle tue chiavi KMS, verifica che i nuovi indirizzi amministrativi vengano aggiunti a tutte le politiche chiave richieste. Verifica le loro autorizzazioni prima di eliminare il precedente amministratore delegato. Consigliamo vivamente di seguire tutte le best practice di sicurezza IAM e di utilizzare credenziali temporanee anziché credenziali a lungo termine.

Ti consigliamo di concedere un accesso limitato nel tempo tramite concessioni se non conosci i nomi dei responsabili al momento della creazione delle politiche o se i principali che richiedono l'accesso cambiano frequentemente. Il beneficiario principale può trovarsi nello stesso account della chiave KMS o in un altro account. Se il principale e la chiave KMS si trovano in account diversi, è necessario specificare una politica basata sull'identità oltre alla concessione. Le sovvenzioni richiedono una gestione aggiuntiva perché è necessario chiamare un'API per creare la sovvenzione e ritirarla o revocarla quando non è più necessaria.

Nessun AWS responsabile, incluso l'utente root dell'account o il creatore della chiave, dispone delle autorizzazioni relative a una chiave KMS a meno che non siano esplicitamente consentite e non esplicitamente negate in una policy chiave, una policy IAM o una concessione. Per estensione, dovresti considerare cosa accadrebbe se un utente ottenesse l'accesso involontario all'utilizzo di una chiave KMS e quale sarebbe l'impatto. Per mitigare tale rischio, considera quanto segue:

- Puoi mantenere diverse chiavi KMS per diverse categorie di dati. Ciò consente di separare le chiavi e mantenere politiche chiave più concise che contengano dichiarazioni di policy che mirano specificamente all'accesso principale a quella categoria di dati. Significa anche che se si accede involontariamente alle credenziali IAM pertinenti, l'identità legata a tale accesso ha accesso

solo alle chiavi specificate nella policy IAM e solo se la policy chiave consente l'accesso a tale principale.

- Puoi valutare se un utente con accesso involontario alla chiave può accedere ai dati. Ad esempio, con Amazon Simple Storage Service (Amazon S3), l'utente deve inoltre disporre delle autorizzazioni appropriate per accedere agli oggetti crittografati in Amazon S3. In alternativa, se un utente ha accesso involontario (tramite RDP o SSH) a un' EC2 istanza Amazon con un volume crittografato con una chiave KMS, l'utente può accedere ai dati utilizzando gli strumenti del sistema operativo.

> **Note**
>
> Servizi AWS tale uso AWS KMS non espone il testo cifrato agli utenti (la maggior parte degli approcci attuali alla criptoanalisi richiede l'accesso al testo cifrato). Inoltre, il testo cifrato non è disponibile per l'esame fisico al di fuori di un AWS data center perché tutti i supporti di archiviazione vengono distrutti fisicamente quando vengono disattivati, in conformità ai requisiti NIST 00-88. SP8

Autorizzazioni con privilegi minimi per AWS KMS

Poiché le tue chiavi KMS proteggono le informazioni sensibili, ti consigliamo di seguire il principio dell'accesso con privilegi minimi. Delega le autorizzazioni minime richieste per eseguire un'attività quando definisci le tue politiche chiave. Consenti tutte le azioni (`kms:*`) su una politica chiave KMS solo se prevedi di limitare ulteriormente le autorizzazioni con politiche aggiuntive basate sull'identità. Se prevedi di gestire le autorizzazioni con policy basate sull'identità, limita chi ha la capacità di creare e collegare le policy IAM ai principi IAM e monitora le modifiche alle policy.

Se consenti tutte le azioni (`kms:*`) sia nella politica chiave che nella politica basata sull'identità, il principale dispone sia delle autorizzazioni amministrative che di utilizzo per la chiave KMS. Come best practice in materia di sicurezza, consigliamo di delegare queste autorizzazioni solo a responsabili specifici. Considerate come assegnate le autorizzazioni ai responsabili che gestiranno le vostre chiavi e ai responsabili che useranno le vostre chiavi. Puoi farlo nominando esplicitamente il principale nella politica chiave o limitando i principi a cui è associata la politica basata sull'identità. Puoi anche usare le chiavi condizionali per limitare le autorizzazioni. Ad esempio, puoi utilizzare aws: PrincipalTag per consentire tutte le azioni se il principale che effettua la chiamata API ha il tag specificato nella regola di condizione.

Per informazioni su come vengono valutate le dichiarazioni politiche AWS, consulta Logica di valutazione delle politiche nella documentazione IAM. Ti consigliamo di esaminare questo argomento prima di scrivere le politiche per ridurre la possibilità che la politica abbia effetti indesiderati, ad esempio fornendo accesso a soggetti che non dovrebbero avere accesso.

> **Tip**
>
> Quando testate un'applicazione in un ambiente non di produzione, utilizzate AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) per applicare le autorizzazioni con privilegi minimi nelle vostre policy IAM.

Se utilizzi utenti IAM anziché ruoli IAM, ti consigliamo vivamente di utilizzare l'AWS autenticazione a più fattori (MFA) per mitigare la vulnerabilità delle credenziali a lungo termine. È possibile usare l'MFA per le seguenti operazioni:

- Richiedi agli utenti di convalidare le proprie credenziali con MFA prima di eseguire azioni privilegiate, come la pianificazione dell'eliminazione delle chiavi.
- Dividi la proprietà di una password dell'account amministratore e del dispositivo MFA tra individui per implementare l'autorizzazione suddivisa.

Per esempi di policy che possono aiutarti a configurare le autorizzazioni con privilegi minimi, consulta gli esempi di policy IAM nella documentazione. AWS KMS

Controllo degli accessi basato sui ruoli per AWS KMS

Il controllo degli accessi basato sul ruolo (RBAC) è una strategia di autorizzazione che fornisce agli utenti solo le autorizzazioni necessarie per svolgere le proprie mansioni lavorative e nient'altro. È un approccio che può aiutarti a implementare il principio del privilegio minimo.

AWS KMS supporta RBAC. Consente di controllare l'accesso alle chiavi specificando autorizzazioni granulari all'interno delle politiche chiave. Le politiche chiave specificano una risorsa, un'azione, un effetto, una condizione principale e facoltativa per concedere l'accesso alle chiavi. Per implementare RBAC in AWS KMS, consigliamo di separare le autorizzazioni per gli utenti chiave e gli amministratori chiave.

Agli utenti chiave, assegna solo le autorizzazioni di cui l'utente ha bisogno. Utilizza le seguenti domande per perfezionare ulteriormente le autorizzazioni:

- Quali presidi IAM devono accedere alla chiave?
- Quali azioni deve eseguire ogni principale con la chiave? Ad esempio, il preside ha bisogno solo `Encrypt` `Sign` delle autorizzazioni?
- A quali risorse deve accedere il preside?
- L'entità è un essere umano o un Servizio AWS? Se si tratta di un servizio, puoi utilizzare la chiave kms: ViaService condition per limitare l'utilizzo della chiave a un servizio specifico.

Agli amministratori chiave, assegna solo le autorizzazioni di cui l'amministratore ha bisogno. Ad esempio, le autorizzazioni di un amministratore possono variare a seconda che la chiave venga utilizzata in ambienti di test o di produzione. Se utilizzi autorizzazioni meno restrittive in determinati ambienti non di produzione, implementa un processo per testare le politiche prima che vengano rilasciate in produzione.

Per esempi di policy che possono aiutarti a configurare il controllo degli accessi basato sui ruoli per utenti e amministratori chiave, consulta RBAC per. AWS KMS

Controllo degli accessi basato sugli attributi per AWS KMS

Il controllo degli accessi basato sugli attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. Come RBAC, è un approccio che può aiutarti a implementare il principio del privilegio minimo.

AWS KMS supporta ABAC consentendo di definire le autorizzazioni in base ai tag associati alla risorsa di destinazione, ad esempio una chiave KMS, e ai tag associati al principale che effettua la chiamata API. In AWS KMS, puoi utilizzare tag e alias per controllare l'accesso alle chiavi gestite dai clienti. Ad esempio, puoi definire politiche IAM che utilizzano le chiavi delle condizioni dei tag per consentire le operazioni quando il tag del principale corrisponde al tag associato alla chiave KMS. Per un tutorial, vedi Definire le autorizzazioni per accedere alle AWS risorse in base ai tag nella AWS KMS documentazione.

Come best practice, utilizza le strategie ABAC per semplificare la gestione delle policy IAM. Con ABAC, gli amministratori possono utilizzare i tag per consentire l'accesso a nuove risorse anziché aggiornare le politiche esistenti. ABAC richiede meno politiche perché non è necessario creare politiche diverse per diverse funzioni lavorative. Per ulteriori informazioni, consulta la sezione Confronto tra ABAC e il modello RBAC tradizionale nella documentazione IAM.

Applica la best practice delle autorizzazioni con privilegi minimi al modello ABAC. Fornisci ai dirigenti IAM solo le autorizzazioni di cui hanno bisogno per svolgere il loro lavoro. Controlla attentamente

l'accesso ai tag APIs che consentirebbero agli utenti di modificare i tag su ruoli e risorse. Se utilizzi le chiavi di condizione degli alias chiave per supportare ABAC in AWS KMS, assicurati di disporre anche di controlli rigorosi che limitino chi può creare chiavi e modificare gli alias.

Puoi anche utilizzare i tag per collegare una chiave specifica a una categoria aziendale e verificare che venga utilizzata la chiave corretta per una determinata azione. Ad esempio, puoi utilizzare AWS CloudTrail i log per verificare che la chiave utilizzata per eseguire un' AWS KMS azione specifica appartenga alla stessa categoria di business della risorsa su cui viene utilizzata.

> **Warning**
>
> Non includere informazioni riservate o sensibili nella chiave o nel valore del tag. I tag non sono crittografati. Sono accessibili a molti Servizi AWS, inclusa la fatturazione.

Prima di implementare un approccio ABAC per il controllo degli accessi, valuta se gli altri servizi che utilizzi supportano questo approccio. Per informazioni su come determinare quali servizi supportano ABAC, consulta Servizi AWS That work with IAM nella documentazione IAM.

Per ulteriori informazioni sull'implementazione di ABAC for AWS KMS e sulle chiavi delle condizioni che possono aiutarti a configurare le politiche, consulta ABAC for. AWS KMS

Contesto di crittografia per AWS KMS

Tutte le operazioni AWS KMS crittografiche con chiavi KMS di crittografia simmetrica accettano un contesto di crittografia. Il contesto di crittografia è un insieme opzionale di coppie chiave-valore non segrete che possono contenere informazioni contestuali aggiuntive sui dati. Come best practice, è possibile inserire un contesto di crittografia nelle `Encrypt` operazioni AWS KMS per migliorare l'autorizzazione e la verificabilità delle chiamate API di decrittografia a. AWS KMS AWS KMS utilizza il contesto di crittografia come dati autenticati aggiuntivi (AAD) per supportare la crittografia autenticata. Il contesto di crittografia è associato crittograficamente al testo cifrato in modo che lo stesso contesto di crittografia sia necessario per decrittografare i dati.

Il contesto di crittografia non è segreto e non è crittografato. Viene visualizzato in testo semplice nei AWS CloudTrail log in modo da poterlo utilizzare per identificare e classificare le operazioni crittografiche. Poiché il contesto di crittografia non è segreto, è necessario consentire solo ai responsabili autorizzati di accedere ai dati di registro. CloudTrail

Puoi anche usare le EncryptionContextKeys chiavi kms ::context-key EncryptionContext e kms: condition per controllare l'accesso a una chiave KMS di crittografia simmetrica basata sul contesto di crittografia. È inoltre possibile utilizzare queste chiavi di condizione per richiedere che i contesti di crittografia vengano utilizzati nelle operazioni crittografiche. Per queste chiavi di condizione, consulta le linee guida sull'uso `ForAnyValue` o sull'`ForAllValues`impostazione degli operatori per assicurarti che le tue politiche riflettano le autorizzazioni previste.

Risoluzione dei problemi relativi AWS KMS alle autorizzazioni

Quando scrivi le policy di controllo degli accessi per una chiave KMS, considera come la policy IAM e la policy chiave interagiscono. Le autorizzazioni effettive per un principale sono le autorizzazioni concesse (e non negate esplicitamente) da tutte le politiche efficaci. All'interno di un account, le autorizzazioni relative a una chiave KMS possono essere influenzate dalle politiche basate sull'identità di IAM, dalle politiche chiave, dai limiti delle autorizzazioni, dalle politiche di controllo del servizio o dalle politiche di sessione. Ad esempio, se si utilizzano politiche basate sull'identità e politiche chiave per controllare l'accesso alla chiave KMS, tutte le politiche relative sia al principale che alla risorsa vengono valutate per determinare l'autorizzazione del committente a eseguire una determinata azione. Per ulteriori informazioni, consulta Logica di valutazione delle politiche nella documentazione IAM.

Per informazioni dettagliate e un diagramma di flusso per la risoluzione dei problemi di accesso alle chiavi, consulta Risoluzione dei problemi di accesso tramite chiave nella AWS KMS documentazione.

Per risolvere un messaggio di errore di accesso negato

1. Verifica che le politiche basate sull'identità IAM e le politiche chiave KMS consentano l'accesso.
2. Verifica che un limite di autorizzazioni in IAM non limiti l'accesso.
3. Verifica che una policy di controllo del servizio (SCP) o una politica di controllo delle risorse (RCP) inserita non stia limitando l'accesso. AWS Organizations
4. Se utilizzi endpoint VPC, verifica che le policy degli endpoint siano corrette.
5. Nelle politiche basate sull'identità e nelle politiche chiave, rimuovi tutte le condizioni o i riferimenti alle risorse che limitano l'accesso alla chiave. Dopo aver rimosso queste restrizioni, verifica che il principale sia in grado di chiamare con successo l'API che in precedenza non funzionava. In caso di successo, riapplica le condizioni e i riferimenti alle risorse uno alla volta e, dopo ciascuno, verifica che il principale abbia ancora accesso. Ciò consente di identificare la condizione o il riferimento alla risorsa che causa l'errore.

Per ulteriori informazioni, consulta Risoluzione dei messaggi di errore di accesso negato nella documentazione IAM.

Best practice di rilevamento e monitoraggio per AWS KMS

Il rilevamento e il monitoraggio sono una parte importante della comprensione della disponibilità, dello stato e dell'utilizzo delle tue AWS Key Management Service (AWS KMS) chiavi. Il monitoraggio aiuta a mantenere la sicurezza, l'affidabilità, la disponibilità e le prestazioni delle AWS soluzioni. AWS fornisce diversi strumenti per monitorare le chiavi e le AWS KMS operazioni del KMS. Questa sezione descrive come configurare e utilizzare questi strumenti per ottenere una maggiore visibilità sull'ambiente e monitorare l'utilizzo delle chiavi KMS.

Questa sezione tratta i seguenti argomenti di rilevamento e monitoraggio:

- Monitoraggio delle AWS KMS operazioni con AWS CloudTrail
- Monitoraggio dell'accesso alle chiavi KMS con IAM Access Analyzer
- Monitoraggio delle impostazioni di crittografia di altri utenti con Servizi AWS AWS Config
- Monitoraggio delle chiavi KMS con allarmi Amazon CloudWatch
- Automatizzare le risposte con Amazon EventBridge

Monitoraggio delle AWS KMS operazioni con AWS CloudTrail

AWS KMS è integrato con AWS CloudTrail, un servizio in grado di registrare tutte le chiamate effettuate AWS KMS da utenti, ruoli e altro Servizi AWS. CloudTrail acquisisce tutte le chiamate API a AWS KMS come eventi, incluse le chiamate dalla AWS KMS console, AWS KMS APIs, AWS CloudFormation, the AWS Command Line Interface (AWS CLI) e AWS Tools for PowerShell.

CloudTrail registra tutte le AWS KMS operazioni, incluse le operazioni di sola lettura, come e. `ListAliases` `GetKeyRotationStatus` Registra inoltre le operazioni che gestiscono le chiavi KMS, come e e. `CreateKey` `PutKeyPolicy, and cryptographic operations, such as GenerateDataKey` `Decrypt` Registra anche le operazioni interne che AWS KMS richiedono l'utente, ad esempio, `DeleteExpiredKeyMaterialDeleteKey`, `SynchronizeMultiRegionKey` e. `RotateKey`

CloudTrail è abilitato sul tuo Account AWS quando lo crei. Per impostazione predefinita, la cronologia degli eventi fornisce un record visualizzabile, ricercabile, scaricabile e immutabile degli ultimi 90 giorni di attività API di gestione degli eventi registrati in un. Regione AWSPer monitorare o verificare l'utilizzo delle chiavi KMS oltre i 90 giorni, ti consigliamo di creare un percorso per il tuo. CloudTrail Account AWS Se hai creato un'organizzazione in AWS Organizations, puoi creare un

percorso organizzativo o un data store di eventi che registri gli eventi per tutti Account AWS i membri dell'organizzazione.

Dopo aver stabilito un percorso per il tuo account o la tua organizzazione, puoi Servizi AWS utilizzarne altro per archiviare, analizzare e rispondere automaticamente agli eventi registrati nel percorso. Ad esempio, puoi eseguire le operazioni seguenti:

- Puoi impostare CloudWatch allarmi Amazon che ti avvisano di determinati eventi durante il percorso. Per ulteriori informazioni sul tagging, consulta Monitoraggio delle chiavi KMS con allarmi Amazon CloudWatchin questa guida.
- Puoi creare EventBridge regole Amazon che eseguono automaticamente un'azione quando si verifica un evento nel percorso. Per ulteriori informazioni, consulta Automatizzare le risposte con Amazon EventBridge in questa guida.
- Puoi utilizzare Amazon Security Lake per raccogliere e archiviare log da più registri Servizi AWS, tra cui CloudTrail. Per ulteriori informazioni, consulta Raccolta di dati da Servizi AWS Security Lake nella documentazione di Amazon Security Lake.
- Per migliorare l'analisi dell'attività operativa, puoi eseguire query CloudTrail sui log con Amazon Athena. Per ulteriori informazioni, consulta Query AWS CloudTrail logs nella documentazione di Amazon Athena.

Per ulteriori informazioni sul monitoraggio delle AWS KMS operazioni con CloudTrail, consulta quanto segue:

- Registrazione delle chiamate AWS KMS API con AWS CloudTrail
- Esempi di voci di AWS KMS registro
- Monitora le chiavi KMS con Amazon EventBridge
- CloudTrail integrazione con Amazon EventBridge

Monitoraggio dell'accesso alle chiavi KMS con IAM Access Analyzer

AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) ti aiuta a identificare le risorse della tua organizzazione e gli account (come le chiavi KMS) condivisi con un'entità esterna. Questo servizio può aiutarti a identificare un accesso indesiderato o eccessivamente ampio alle tue risorse e ai tuoi dati, il che rappresenta un rischio per la sicurezza. IAM Access Analyzer identifica

le risorse condivise con responsabili esterni utilizzando un ragionamento basato sulla logica per analizzare le politiche basate sulle risorse nell'ambiente. AWS

Puoi utilizzare IAM Access Analyzer per identificare quali entità esterne hanno accesso alle tue chiavi KMS. Quando abiliti IAM Access Analyzer, crei un analizzatore per un'intera organizzazione o per un account di destinazione. L'organizzazione o l'account che scegli è nota come zona di fiducia per l'analizzatore. L'analizzatore monitora le risorse supportate all'interno della zona di fiducia. Qualsiasi accesso alle risorse da parte dei committenti all'interno della zona di fiducia è considerato affidabile.

Per quanto riguarda le chiavi KMS, IAM Access Analyzer analizza le politiche e le concessioni chiave applicate a una chiave. Genera una scoperta se una policy o una concessione chiave consente a un'entità esterna di accedere alla chiave. Utilizza IAM Access Analyzer per determinare se le entità esterne hanno accesso alle tue chiavi KMS, quindi verifica se tali entità devono avere accesso.

Per ulteriori informazioni sull'utilizzo di IAM Access Analyzer per monitorare l'accesso alle chiavi KMS, consulta quanto segue:

- Uso di AWS Identity and Access Management Access Analyzer
- Tipi di risorse IAM Access Analyzer per l'accesso esterno
- Tipi di risorse IAM Access Analyzer: AWS KMS keys
- Risultati relativi all'accesso esterno e non utilizzato

Monitoraggio delle impostazioni di crittografia di altri utenti con Servizi AWS AWS Config

AWS Configfornisce una visualizzazione dettagliata della configurazione delle AWS risorse del tuo Account AWS. Puoi utilizzarlo AWS Config per verificare che le tue chiavi KMS Servizi AWS che utilizzano abbiano le impostazioni di crittografia configurate in modo appropriato. Ad esempio, puoi utilizzare la AWS Config regola dei volumi crittografati per verificare che i tuoi volumi Amazon Elastic Block Store (Amazon EBS) siano crittografati.

AWS Config include regole gestite che ti aiutano a scegliere rapidamente le regole in base alle quali valutare le tue risorse. AWS Config Effettua il check-in Regioni AWS per determinare se le regole gestite necessarie sono supportate in quella regione. Le regole gestite disponibili includono i controlli per la configurazione degli snapshot di Amazon Relational Database Service (Amazon RDS), la crittografia dei trail CloudTrail , la crittografia predefinita per i bucket Amazon Simple Storage Service (Amazon S3), la crittografia delle tabelle Amazon DynamoDB e altro ancora.

Puoi anche creare regole personalizzate e applicare la tua logica di business per determinare se le tue risorse sono conformi ai tuoi requisiti. Il codice open source per molte regole gestite è disponibile nel AWS Config Rules Repository su. GitHub Questi possono essere un utile punto di partenza per sviluppare regole personalizzate.

Quando una risorsa non è conforme a una regola, puoi avviare azioni reattive. AWS Config include le azioni di riparazione eseguite da Automation.AWS Systems Manager Ad esempio, se hai applicato la cloud-trail-encryption-enabledregola e la regola restituisce un `NON_COMPLIANT` risultato, AWS Config puoi avviare un documento di automazione che risolva il problema crittografando i log per te. CloudTrail

AWS Config consente di verificare in modo proattivo la conformità alle AWS Config regole prima di effettuare il provisioning delle risorse. L'applicazione delle regole in modalità proattiva consente di valutare le configurazioni delle risorse cloud prima che vengano create o aggiornate. L'applicazione delle regole in modalità proattiva come parte della pipeline di distribuzione consente di testare le configurazioni delle risorse prima di distribuirle.

Puoi anche implementare AWS Config le regole come controlli. AWS Security Hub CSPM Security Hub CSPM offre standard di sicurezza che puoi applicare al tuo. Account AWS Questi standard consentono di valutare l'ambiente in base alle pratiche consigliate. Lo standard AWS Foundational Security Best Practices include controlli all'interno della categoria Protect Control per verificare che la crittografia a riposo sia configurata e che le politiche chiave del KMS seguano le pratiche consigliate.

Per ulteriori informazioni sull'utilizzo per AWS Config monitorare le impostazioni di crittografia in Servizi AWS, consulta quanto segue:

- Nozioni di base su AWS Config
- AWS Config regole gestite
- AWS Config regole personalizzate
- Correzione delle risorse non conformi con AWS Config

Monitoraggio delle chiavi KMS con allarmi Amazon CloudWatch

Amazon CloudWatch monitora AWS le tue risorse e le applicazioni su cui esegui AWS in tempo reale. Puoi utilizzarlo CloudWatch per raccogliere e tenere traccia delle metriche, che sono variabili che puoi misurare.

La scadenza del materiale chiave importato o l'eliminazione di una chiave sono eventi potenzialmente catastrofici se non intenzionali o non pianificati correttamente. Ti consigliamo di configurare gli CloudWatch allarmi per avvisarti di questi eventi prima che si verifichino. Ti consigliamo inoltre di configurare le policy AWS Identity and Access Management (IAM) o le policy di controllo del AWS Organizations servizio (SCPs) per impedire l'eliminazione di chiavi importanti.

CloudWatch gli allarmi ti aiutano a intraprendere azioni correttive, come annullare l'eliminazione delle chiavi, o azioni correttive, come la reimportazione di materiale chiave eliminato o scaduto.

Automatizzare le risposte con Amazon EventBridge

Puoi anche utilizzare Amazon EventBridge per avvisarti di eventi importanti che influiscono sulle tue chiavi KMS. EventBridge è un servizio Servizio AWS che fornisce un flusso quasi in tempo reale di eventi di sistema che descrivono le modifiche alle AWS risorse. EventBridgericeve automaticamente gli eventi dal CloudTrail CSPM di Security Hub. In EventBridge, è possibile creare regole che rispondono agli eventi registrati da. CloudTrail

AWS KMS gli eventi includono quanto segue:

- Il materiale chiave in una chiave KMS è stato ruotato automaticamente
- Il materiale chiave importato in una chiave KMS è scaduto
- Una chiave KMS di cui era stata pianificata l'eliminazione è stata eliminata

Questi eventi possono avviare azioni aggiuntive nel tuo. Account AWS Queste azioni sono diverse dagli CloudWatch allarmi descritti nella sezione precedente perché possono essere eseguite solo dopo che si è verificato l'evento. Ad esempio, potresti voler eliminare le risorse collegate a una chiave specifica dopo che quella chiave è stata eliminata oppure potresti voler informare un team di conformità o di controllo che la chiave è stata eliminata.

Puoi anche filtrare qualsiasi altro evento API registrato CloudTrail utilizzando. EventBridge Ciò significa che se le azioni API chiave relative alle politiche sono di particolare interesse, puoi filtrarle. Ad esempio, puoi filtrare EventBridge per l'azione dell'`PutKeyPolicy`API. Più in generale, puoi filtrare in base a qualsiasi azione dell'API che inizia con `Disable*` o `Delete*` per avviare risposte automatiche.

Utilizzando EventBridge, è possibile monitorare (che è un controllo investigativo) e indagare e rispondere (che sono controlli reattivi) a eventi imprevisti o selezionati. Ad esempio, puoi avvisare i team di sicurezza e intraprendere azioni specifiche se viene creato un utente o un ruolo IAM, quando

viene creata una chiave KMS o quando viene modificata una policy chiave. Puoi creare una regola di EventBridge evento che filtra le azioni API specificate e quindi associare gli obiettivi alla regola. Gli obiettivi di esempio includono AWS Lambda funzioni, notifiche Amazon Simple Notification Service (Amazon SNS), code Amazon Simple Queue Service (Amazon SQS) e altro ancora. Per ulteriori informazioni sull'invio di eventi alle destinazioni, consulta Event bus targets in Amazon EventBridge.

Per ulteriori informazioni sul monitoraggio EventBridge e AWS KMS l'automazione delle risposte, consulta Monitorare le chiavi KMS con Amazon EventBridge nella AWS KMS documentazione.

Best practice per la gestione dei costi e della fatturazione per AWS KMS

Grazie all'ampiezza e alla profondità, Servizi AWS offri la flessibilità necessaria per gestire i costi soddisfacendo al contempo i requisiti aziendali. Questa sezione descrive i prezzi per l'archiviazione delle chiavi in AWS Key Management Service (AWS KMS) e fornisce consigli per ridurre i costi, ad esempio tramite la memorizzazione nella cache delle chiavi. Puoi anche esaminare l'utilizzo delle chiavi KMS per determinare se esistono ulteriori opportunità per ridurre i costi.

Questa sezione tratta i seguenti argomenti sulla gestione dei costi e della fatturazione:

- AWS KMS prezzi per l'archiviazione delle chiavi
- Chiavi bucket Amazon S3 con crittografia predefinita
- Memorizzazione nella cache delle chiavi di dati utilizzando il AWS Encryption SDK
- Alternative alla memorizzazione nella cache delle chiavi e alle chiavi bucket Amazon S3
- Gestione dei costi di registrazione per l'utilizzo delle chiavi KMS

AWS KMS prezzi per l'archiviazione delle chiavi

Ciascuno AWS KMS key di essi creato AWS KMS comporta un costo. L'addebito mensile è lo stesso per le chiavi simmetriche, le chiavi asimmetriche, le chiavi HMAC, le chiavi multiregione (ogni chiave multiregione principale e ogni replica), le chiavi con materiale chiave importato e le chiavi KMS con un'origine chiave in uno o in un archivio chiavi esterno. AWS CloudHSM

Per le chiavi KMS che ruotate automaticamente o su richiesta, la prima e la seconda rotazione della chiave aggiungono un costo mensile aggiuntivo (ripartito proporzionalmente su base oraria). Dopo la seconda rotazione, le eventuali rotazioni successive in quel mese non vengono fatturate. Consulta AWS KMS i prezzi per le informazioni più recenti sui prezzi.

Puoi utilizzarlo AWS Budgetsper configurare un budget di utilizzo. AWS Budgets può avvisarti quando la spesa all'interno del tuo account supera determinate soglie. Per quanto riguarda i costi relativi a AWS KMS, puoi creare un budget di utilizzo per avvisare in base alle chiavi o alle richieste KMS. Ciò può migliorare la visibilità dei costi di archiviazione e utilizzo delle AWS KMS chiavi.

Chiavi bucket Amazon S3 con crittografia predefinita

In alcuni casi d'uso, i carichi di lavoro che accedono o generano un gran numero di oggetti in Amazon Simple Storage Service (Amazon S3) possono generare elevati volumi di richieste a AWS KMS, con un conseguente aumento dei costi. La configurazione delle bucket key di Amazon S3 può aiutarti a ridurre i costi fino al 99%. Si tratta di un'alternativa consigliata alla disabilitazione della crittografia per contribuire a ridurre i costi associati a. AWS KMS

Memorizzazione nella cache delle chiavi di dati utilizzando il AWS Encryption SDK

Quando si utilizza AWS Encryption SDKper eseguire la crittografia lato client, la memorizzazione nella cache delle chiavi di dati può contribuire a migliorare le prestazioni dell'applicazione, ridurre il rischio che le richieste dell'applicazione AWS KMS vengano limitate e contribuire a ridurre i costi. Per ulteriori informazioni su come iniziare, consulta Come utilizzare la memorizzazione nella cache delle chiavi di dati.

Alternative alla memorizzazione nella cache delle chiavi e alle chiavi bucket Amazon S3

Se la memorizzazione nella cache delle chiavi non è un'opzione per te a causa dei tuoi requisiti di gestione dei dati, puoi anche richiedere aumenti delle AWS KMS quote utilizzando l' AWS Management Console API Service Quotas. Considerate il volume di chiamate API che potreste effettuare. Il numero di chiamate API che effettui è un fattore importante per la AWS KMS determinazione dei prezzi. Se si aumenta la quota relativa al tasso di richiesta per aumentare le prestazioni, l'aumento del numero di richieste AWS KMS comporta costi aggiuntivi.

Gestione dei costi di registrazione per l'utilizzo delle chiavi KMS

Tutte le chiamate AWS KMS API vengono registrate. AWS CloudTrail Le applicazioni e i servizi possono generare grandi volumi di chiamate AWS KMS API (ad esempio per operazioni crittografiche, tra cui crittografia e decrittografia). Può essere difficile esaminare CloudTrail i log senza uno strumento che consenta di organizzare i dati, analizzare le tendenze e cercare attività anomale delle API. Amazon Athena fornisce strutture di dati predefinite che possono aiutarti a configurare rapidamente tabelle per CloudTrail i log e iniziare ad analizzare i dati di log. È particolarmente utile

per analisi ad hoc o ulteriori indagini durante la risposta agli incidenti. Per ulteriori informazioni, consulta Query AWS CloudTrail logs nella documentazione di Athena.

Poiché paghi per Athena in base alla richiesta, puoi impostare i tavoli in anticipo senza alcun costo. Non sono previsti costi per le dichiarazioni in linguaggio di definizione dei dati. Quando si risponde a un incidente, ciò consente di assicurarsi che molti prerequisiti siano già soddisfatti. Per facilitare la preparazione, è consigliabile scrivere le interrogazioni dopo aver creato la tabella, testarle e assicurarsi che producano i risultati desiderati. Puoi salvare le tue interrogazioni in Athena per utilizzi futuri. Per ulteriori informazioni su come iniziare a usare Athena, consulta Guida introduttiva ad Amazon Athena.

Gli eventi relativi ai dati forniscono visibilità sulle operazioni eseguite su o all'interno di una risorsa. Queste operazioni sono definite anche operazioni del piano dei dati. Gli esempi includono gli `PutObject` eventi Amazon S3 o le chiamate API per il funzionamento della funzione Lambda. Gli eventi relativi ai dati sono spesso attività ad alto volume e la loro registrazione comporta costi aggiuntivi. Per aiutare a controllare il volume di eventi relativi ai dati che vengono registrati nei trail o negli event data store CloudTrail, puoi ottimizzare la registrazione per CloudTrail ridurre i costi di Amazon S3 e Amazon S3 configurando selettori di eventi avanzati per limitare gli eventi di dati a cui accedere. AWS KMS CloudTrail Per ulteriori informazioni, consulta Come ottimizzare AWS CloudTrail i costi utilizzando selettori di eventi avanzati (post del blog).AWS

Risorse

AWS Key Management Service (AWS KMS) documentazione

- AWS KMS Guida per gli sviluppatori
- Riferimento API AWS KMS
- AWS KMS nel AWS CLI Reference

Strumenti

- AWS Encryption SDK

AWS Guida prescrittiva

Strategie

- Creazione di una strategia di crittografia per i dati archiviati

Guide

- Le migliori pratiche e funzionalità di crittografia per Servizi AWS
- AWS Architettura di riferimento per la privacy (AWS PRA)

Modelli

- Crittografa automaticamente i volumi Amazon EBS
- Automatically remediate unencrypted Amazon RDS DB instances and clusters
- Monitora e correggi l'eliminazione pianificata di AWS KMS keys

Collaboratori

Creazione di testi

- Frank Phillis, architetto senior specializzato in soluzioni GTM, AWS
- Ken Beer, direttore AWS KMS e direttore delle Crypto Libraries, AWS
- Michael Miller, architetto senior delle soluzioni, AWS
- Jeremy Stieglitz, responsabile principale del prodotto, AWS
- Zach Miller, architetto principale delle soluzioni, AWS
- Peter M. O'Donnell, architetto principale delle soluzioni, AWS
- Patrick Palmer, architetto principale delle soluzioni, AWS
- Dave Walker, architetto principale delle soluzioni, AWS

Revisione

- Manigandan Shri, consulente senior per le consegne, AWS

Scrittura tecnica

- Lilly AbouHarb, scrittrice tecnica senior, AWS
- Kimberly Garmoe, scrittrice tecnica senior, AWS

Cronologia dei documenti

La tabella seguente descrive le modifiche significative apportate a questa guida. Per ricevere notifiche sugli aggiornamenti futuri, puoi abbonarti a un feed RSS.

Modifica	Descrizione	Data
Pubblicazione iniziale	—	24 marzo 2025

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.