aws

Guida per gli sviluppatori

AWS Key Management Service

AWS Key Management Service: Guida per gli sviluppatori

Table of Contents

AWS Key Management Service

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. AWS KMS usa i moduli di sicurezza hardware (HSM) per proteggere e convalidare le AWS KMS keys ai sensi del programma di convalida FIPS 140-2 Cryptographic Module Validation Program. Le regioni Cina (Pechino) e Cina (Ningxia) non supportano il Programma di convalida dei moduli crittografici FIPS 140-2. AWS KMS utilizza HSM con certificazione OSCCA per proteggere le chiavi KMS nelle regioni cinesi.

AWS KMS è integrato con la maggior parte degli altri servizi AWS che crittografano i dati. AWS KMS è integrato con AWS CloudTrail per registrare l'utilizzo delle chiavi KMS con finalità di verifica, regolamentazione e conformità.

È possibile utilizzare l'API AWS KMS per creare e gestire chiavi KMS e caratteristiche speciali, come archivi delle chiavi personalizzate, e usare le chiavi KMS in operazioni di crittografia. Per informazioni dettagliate, consultare Documentazione di riferimento dell'API AWS Key Management Service.

Puoi creare e gestire le tue AWS KMS keys:

- crea, modifica e visualizza le chiavi KMS simmetriche e asimmetriche, incluse le chiavi HMAC.
- È possibile controllare l'accesso alle chiavi KMS con le policy chiave, Policy IAM e concessioni. AWS KMS supporta il controllo degli accessi basato su attributi (ABAC). È inoltre possibile perfezionare le policy utilizzando chiavi di condizione.
- Crea, elimina, elenca e aggiorna gli alias che sono nomi descrittivi per le chiavi KMS. Puoi inoltre utilizzare gli alias per controllare l'accesso alle chiavi KMS.
- Tagga le chiavi KMS per l'identificazione, l'automazione e la tracciabilità dei costi. Puoi inoltre utilizzare i tag per controllare l'accesso alle chiavi KMS.
- Abilitare e disabilitare le chiavi KMS.
- Abilita e disabilita la rotazione automatica del materiale di crittografia in una chiave KMS.
- Elimina le chiavi KMS per completare il ciclo di vita della chiave

Puoi utilizzare le chiavi KMS nelle operazioni di crittografia. Per alcuni esempi, consulta Programmazione dell'API AWS KMS.

- Crittografare, decrittare e ricrittografare i dati con le chiavi KMS simmetriche o asimmetriche.

- Firma e verifica i messaggi con le chiavi KMS asimmetriche.
- Genera coppie di chiavi di dati asimmetriche e chiavi di dati simmetriche esportabili.
- Genera e verifica codici HMAC.
- Generare di numeri casuali adatti ad applicazioni di crittografia.

Puoi utilizzare le funzionalità avanzate di AWS KMS

- Creare Chiavi multi-regione, che agiscono come copie della stessa chiave KMS in diversi Regioni AWS.
- Importare il materiale crittografico in una chiave KMS.
- Crea le chiavi KMS in un archivio delle chiavi di AWS CloudHSM supportato da un cluster AWS CloudHSM.
- Crea le chiavi KMS in un archivio delle chiavi esterne supportato dalle chiavi crittografiche al di fuori di AWS.
- Connessione diretta a AWS KMS tramite un endpoint privato nel tuo VPC.
- Utilizzare il TLS post-quantistico ibrido per fornire una crittografia lungimirante in transito per i dati inviati a AWS KMS.

Utilizzando AWS KMS, puoi ottenere un controllo maggiore sull'accesso ai dati crittografati. Puoi utilizzare la funzionalità di crittografia e gestione delle chiavi nelle applicazioni direttamente o attraverso i servizi AWS integrati con AWS KMS. Che tu scriva applicazioni per AWS o utilizzi i servizi di AWS, AWS KMS consente di mantenere il controllo sugli utenti che possono utilizzare le AWS KMS keys e ottenere l'accesso ai dati crittografati.

AWS KMS si integra con AWS CloudTrail, un servizio che fornisce i file di log per il bucket Amazon S3. Utilizzando CloudTrail puoi monitorare e indagare su come e quando le tue chiavi KMS sono state utilizzate e chi le ha utilizzate.

AWS KMS in Regioni AWS

Le Regioni AWS in cui AWS KMS è supportato sono elencate in Endpoint e quote di AWS Key Management Service. Se una funzione AWS KMS non è supportata in una Regione AWS che AWS KMS supporta, la differenza regionale viene descritta nell'argomento relativo alla funzione.

Prezzi di AWS KMS

Come per gli altri prodotti AWS, l'uso di AWS KMS non richiede contratti o quantità minime di acquisto. Per ulteriori informazioni sui prezzi di AWS KMS, consulta Prezzi di AWS Key Management Service.

Contratto sul livello di servizio

AWS Key Management Service è supportato da un contratto a livello di servizio che definisce la nostra policy di disponibilità dei servizi.

Ulteriori informazioni

- Per informazioni sui termini e sui concetti utilizzati in AWS KMS, consulta Concetti AWS KMS.
- Per ulteriori informazioni sull'API AWS KMS, consulta la Documentazione di riferimento dell'API AWS Key Management Service. Per esempi in diversi linguaggi di programmazione, consulta Programmazione dell'API AWS KMS.
- Per informazioni sull'utilizzo dei modelli AWS CloudFormation per creare e gestire chiavi e alias, consulta Creazione di risorse AWS KMScon AWS CloudFormation e il AWS Key Management Service riferimento al tipo di risorsa nella Guida per l'utente di AWS CloudFormation.
- Per ulteriori informazioni tecniche su come AWS KMS utilizza la crittografia e protegge le chiavi KMS, consulta Dettagli sulla crittografia di AWS Key Management Service. La documentazione sui dettagli sulla crittografia non descrive come funziona AWS KMS nelle regioni Cina (Pechino) e Cina (Ningxia).
- Per un elenco di endpoint AWS KMS, inclusi gli endpoint FIPS, in ogni Regione AWS, consulta Endpoint del servizio nell'argomento AWS Key Management Service della Riferimenti generali di AWS.
- Per informazioni su questioni relative a AWS KMS, consulta il forum di discussione AWS Key Management Service.

AWS KMS negli SDK AWS

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript

- AWS SDK for PHP
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby

Concetti AWS KMS

Ulteriori informazioni sui termini e i concetti di base di AWS Key Management Service (AWS KMS) e il modo in cui collaborano per proteggere i dati.

Argomenti

- AWS KMS keys
- Chiavi del cliente e chiavi AWS
- Chiavi KMS di crittografia simmetrica
- Chiavi KMS asimmetriche
- Chiavi KMS HMAC
- Chiavi di dati
- Coppia di chiavi di dati
- Alias
- store delle chiavi personalizzate
- Operazioni di crittografia
- Identificatori chiave () KeyId
- Materiale chiave
- Origine del materiale della chiave
- Specifica della chiave
- Utilizzo delle chiavi
- Crittografia envelope
- Contesto di crittografia
- Policy delle chiavi
- Grant
- Verifica dell'utilizzo della chiave KMS
- Infrastruttura di gestione delle chiavi

AWS KMS keys

AWS KMS keys (chiavi KMS) sono la risorsa principale in AWS KMS. È possibile utilizzare una chiave KMS per crittografare, decrittare e ricrittografare i dati. Può anche generare chiavi dati che è possibile utilizzare al di fuori di AWS KMS. Generalmente, utilizzerai chiavi KMS di crittografia simmetrica, ma puoi creare e utilizzare chiavi KMS asimmetriche per la crittografia o la firma, e creare e utilizzare chiavi KMS HMAC per generare e verificare tag HMAC.

> **Note**
>
> AWS KMS sta sostituendo il termine chiave master del cliente (CMK) con AWS KMS key e chiave KMS. Il concetto non è cambiato. Per evitare cambiamenti sostanziali, AWS KMS sta mantenendo alcune varianti di questo termine.

Una AWS KMS key è la rappresentazione logica di una chiave crittografica. Una chiave KMS contiene metadati, ad esempio: ID della chiave, specifica della chiave, utilizzo della chiave, data di creazione, descrizione e stato della chiave. In particolare, contiene un riferimento al materiale della chiave che viene utilizzato quando esegui operazioni di crittografia con la chiave KMS.

Puoi creare una chiave KMS con materiale della chiave crittografico generato in moduli di sicurezza hardware AWS KMS convalidati con FIPS. Il materiale delle chiave per le chiavi KMS simmetriche e le chiavi private della chiave KMS asimmetrica mantengono AWS KMS sempre crittografato. Per utilizzare o gestire le chiavi KMS, devi utilizzare AWS KMS. Per ulteriori informazioni sulla creazione e la gestione di chiavi KMS, consulta Gestione delle chiavi . Per informazioni sull'utilizzo delle chiavi KMS, consulta la documentazione di riferimento dell'API AWS Key Management Service.

Per impostazione predefinita, AWS KMS crea il materiale chiave per una chiave KMS. Non è possibile estrarre, esportare, visualizzare o gestire questo materiale della chiave. L'unica eccezione è la chiave pubblica di una coppia di chiavi asimmetriche, che è possibile esportare per l'uso al di fuori di AWS. Inoltre, non puoi eliminare questo materiale della chiave è necessario eliminare la chiave KMS. Puoi tuttavia importare il materiale della chiave personale in una chiave KMS o utilizzare un archivio delle chiavi personalizzate per creare chiavi KMS che utilizzano il materiale della chiave nel cluster AWS CloudHSM o il materiale della chiave in un gestore delle chiavi esterne che possiedi e gestisci al di fuori di AWS.

AWS KMS supporta anche le chiavi per più Regioni, che consentono di crittografare i dati in una Regione AWS e decrittarlo in un'altra Regione AWS.

Per ulteriori informazioni sulla creazione e la gestione di chiavi KMS, consulta Gestione delle chiavi . Per informazioni sull'utilizzo delle chiavi KMS, consulta la documentazione di riferimento dell'API AWS Key Management Service.

Chiavi del cliente e chiavi AWS

Le chiavi KMS create dall'utente sono chiavi gestite dal cliente. I Servizi AWS che utilizzano le chiavi KMS per crittografare le risorse di servizio spesso creano le chiavi per conto dell'utente. Le chiavi KMS che i Servizi AWS creano nell'account AWS dell'utente sono Chiavi gestite da AWS. Le chiavi KMS che i Servizi AWS creano in un account di servizio sono Chiavi di proprietà di AWS.

Tipo di chiave KMS	Può visualizzare i metadati della chiave KMS	Può gestire la chiave KMS	Utilizzata solo per il mio Account AWS	Rotazione automatica	Prezzi
Chiave gestita dal cliente	Sì	Sì	Sì	Facoltativo. Ogni anno (circa 365 giorni)	Canone mensile (proporzionale a ora) Tariffa per uso
Chiave gestita da AWS	Sì	No	Sì	Campo obbligatorio. Ogni anno (circa 365 giorni)	Nessuna tariffa mensile Tariffa per uso (alcuni Servizi AWS pagano questa tariffa per tuo conto)
Chiave di proprietà di AWS	No	No	No	Può variare	Nessuna tariffa

I servizi AWS che si integrano con AWS KMS differiscono per il supporto per le chiavi KMS. Alcuni servizi AWS eseguono la crittografia dei dati per impostazione predefinita con una Chiave di proprietà di AWS o una Chiave gestita da AWS. Alcuni servizi AWS supportano le chiavi gestite dal cliente. Altri servizi AWS invece supportano tutti i tipi di chiavi KMS per offrire la praticità di una Chiave di proprietà di AWS, la visibilità di una Chiave gestita da AWS o il controllo di una chiave gestita dal cliente. Per informazioni dettagliate sulle opzioni di crittografia offerte da un servizio AWS, consulta l'argomento relativo alla crittografia dei dati inattivi nella guida per l'utente o nella guida per gli sviluppatori del servizio.

Chiavi gestite dal cliente

Le chiavi KMS create dall'utente sono chiavi gestite dal cliente. Le chiavi gestite dal cliente sono chiavi KMS nell'Account AWS create, possedute e gestite dall'utente. L'utente ha il controllo completo su queste chiavi KMS, tra cui la definizione e il mantenimento delle policy chiave, delle policy IAM e delle concessioni, la loro attivazione e disattivazione, la rotazione del materiale crittografico, l'aggiunta di tag, la creazione di alias relativi alle chiavi KMS e la programmazione di chiavi KMS per l'eliminazione.

Le chiavi gestite dal cliente vengono visualizzate nella pagina chiavi gestite dal cliente della AWS Management Console per AWS KMS. Per identificare in modo definitivo una chiave gestita dal cliente, utilizza l'DescribeKeyoperazione. Per le chiavi gestite dal cliente, il valore del campo `KeyManager` della risposta di `DescribeKey` è `CUSTOMER`.

Si possono utilizzare chiavi gestite dal cliente in operazioni di crittografia e verificarne l'uso nei registri AWS CloudTrail. Inoltre, molti servizi AWS che si integrano con AWS KMS consentono di specificare una chiave gestita dal cliente per proteggere i dati archiviati e gestiti per l'utente.

Le chiavi gestite dal cliente sono soggette a una tariffa mensile e a una tariffa qualora l'utilizzo superi i termini del piano gratuito. Sono conteggiati in rapporto alle quote AWS KMS per l'account. Per i dettagli, vedere le sezioni Prezzi AWS Key Management Service e Quote.

Chiavi gestite da AWS

Le Chiavi gestite da AWS sono chiavi KMS nel tuo account create, gestite e utilizzate a tuo nome da un servizio AWS che si integra con AWS KMS.

Alcuni servizi AWS consentono di scegliere una Chiave gestita da AWS o una chiave gestita dal cliente per proteggere le risorse in quel determinato servizio. In generale, a meno che non sia richiesto di controllare la chiave crittografica che protegge le risorse, una Chiave gestita da AWS è

una buona scelta. Non è necessario creare o mantenere la chiave o la relativa policy delle chiavi e non è mai previsto un canone mensile per una Chiave gestita da AWS.

Hai l'autorizzazione per visualizzare le Chiavi gestite da AWS nell'account, visualizzare le loro policy delle chiavi e verificarne l'utilizzo nei registri AWS CloudTrail. Tuttavia, non puoi modificare le proprietà delle Chiavi gestite da AWS, ruotarle, modificarne policy delle chiavi o pianificarne l'eliminazione. Inoltre, non puoi utilizzare le Chiavi gestite da AWS direttamente nelle operazioni di crittografia; il servizio che le crea le utilizza per tuo conto.

Chiavi gestite da AWS appare nella pagina Chiavi gestite da AWS della AWS Management Console per AWS KMS. La maggior parte delle Chiavi gestite da AWS è identificabile tramite i relativi alias che hanno il formato `aws/service-name`, ad esempio `aws/redshift`. Per identificare definitivamente unChiavi gestite da AWS, utilizzare l'DescribeKeyoperazione. Per le Chiavi gestite da AWS, il valore del campo `KeyManager` della risposta `DescribeKey` è `AWS`.

Tutte le Chiavi gestite da AWS vengono ruotate automaticamente ogni anno. Non è possibile modificare questo programma di rotazione.

> **Note**
>
> A maggio 2022, AWS KMS ha modificato il programma di rotazione delle Chiavi gestite da AWS passando da ogni tre anni (circa 1.095 giorni) a ogni anno (circa 365 giorni).
> Le nuove Chiavi gestite da AWS vengono ruotate automaticamente un anno dopo la loro creazione e successivamente all'incirca ogni anno.
> Le Chiavi gestite da AWS esistenti vengono ruotate automaticamente un anno dopo l'ultima rotazione e successivamente ogni anno.

Non è previsto alcun canone mensile per Chiavi gestite da AWS. Possono essere soggette a tariffe se l'utilizzo supera i termini del piano gratuito, ma alcuni servizi AWS coprono questi costi per l'utente. Per informazioni dettagliate, consulta l'argomento Crittografia dei dati inattivi nella guida per l'utente o nella guida per gli sviluppatori del servizio. Per informazioni dettagliate, consulta Prezzi di AWS Key Management Service.

Le Chiavi gestite da AWS non vengono conteggiate nelle quote delle risorse per quanto riguarda il numero di chiavi KMS in ciascuna Regione dell'account. Tuttavia, quando vengono utilizzate per conto di un principale nel tuo account, le chiavi KMS vengono conteggiate ai fini delle quote di richiesta. Per informazioni dettagliate, vedi Quote.

Chiavi di proprietà di AWS

Le Chiavi di proprietà di AWS sono una raccolta di chiavi KMS che un servizio AWS possiede e gestisce per l'utilizzo in più account Account AWS. Sebbene le Chiavi di proprietà di AWS non siano presenti nel tuo Account AWS, un servizio AWS può utilizzare una Chiave di proprietà di AWS per proteggere le risorse presenti nell'account.

Alcuni servizi AWS consentono di selezionare una Chiave di proprietà di AWS o una chiave gestita dal cliente. In generale, a meno che non sia richiesto di eseguire un audit o controllare la chiave crittografica che protegge le risorse, una Chiave di proprietà di AWS è una buona scelta. Chiavi di proprietà di AWS sono completamente gratuite (senza canoni mensili o costi di utilizzo), non contano ai fini delle quote AWS KMS per il tuo account e sono facili da usare. Non è necessario creare o mantenere la chiave o la relativa policy delle chiavi.

La rotazione delle Chiavi di proprietà di AWS varia a seconda dei servizi. Per informazioni sulla rotazione di una Chiave di proprietà di AWS specifica, consultare Crittografia dei dati a riposo nella guida per l'utente o nella guida per gli sviluppatori del servizio.

Chiavi KMS di crittografia simmetrica

Quando crei una AWS KMS key, per impostazione predefinita ottieni una chiave KMS di crittografia simmetrica. Questo è il tipo di chiave KMS di base e comunemente più usato.

In AWS KMS, una chiave KMS di crittografia simmetrica rappresenta una chiave crittografica AES-GCM a 256 bit, tranne nelle regioni della Cina, dove rappresenta una chiave crittografica SM4 a 128 bit. Il materiale della chiave simmetrica mantiene sempre AWS KMS crittografato. Per utilizzare una chiave KMS di crittografia simmetrica devi richiamare AWS KMS. Le chiavi crittografiche simmetrica vengono utilizzate nella crittografia simmetrica, laddove la stessa chiave viene usata per la crittografia e la decrittografia. A meno che la tua attività non richieda esplicitamente la crittografia asimmetrica, le chiavi KMS di crittografia simmetrica, grazie alle quali AWS KMS è sempre crittografato, sono una scelta valida.

I servizi AWS integrati con AWS KMS usano soltanto chiavi KMS di crittografia simmetrica per crittografare i dati. Questi servizi non supportano la crittografia con chiavi KMS asimmetriche. Per informazioni su come determinare se una è simmetrica o asimmetrica, consulta Individuazione di chiavi KMS asimmetriche.

Tecnicamente, la specifica chiave per una chiave simmetrica è SYMMETRIC_DEFAULT, l'utilizzo della chiave è ENCRYPT_DECRYPT e l'algoritmo di crittografia è SYMMETRIC_DEFAULT. Per informazioni dettagliate, vedi Specifica della chiave SYMMETRIC_DEFAULT.

Puoi utilizzare una chiave KMS di crittografia simmetrica in AWS KMS per crittografare, decrittografare e crittografare nuovamente i dati, così come per generare chiavi di dati e coppie di chiavi di dati. Puoi creare chiavi KMS di crittografia simmetrica multi-regione, importare il materiale della chiave in una chiave KMS di crittografia simmetrica e creare chiavi KMS di crittografia simmetrica negli archivi delle chiavi personalizzate. Per una tabella di confronto delle operazioni eseguibili sulle diverse tipologie di chiavi KMS, consultare Documentazione di riferimento dei tipi di chiave.

Chiavi KMS asimmetriche

È possibile creare una chiave KMS asimmetrica in AWS KMS. Una chiave KMS asimmetrica rappresenta una coppia di chiavi, una pubblica e una privata, correlate matematicamente. Grazie alla chiave privata il servizio AWS KMS non è mai in chiaro. Per utilizzare la chiave privata, è necessario chiamare AWS KMS. È possibile utilizzare la chiave pubblica all'interno di AWS KMS chiamando le operazioni API AWS KMS o scaricare la chiave pubblica e usarla al di fuori di AWS KMS. È possibile anche creare chiavi KMS asimmetriche multi-Regione.

È possibile creare chiavi KMS asimmetriche che rappresentano coppie di chiavi RSA o coppie di chiavi SM2 (solo regioni della Cina) per la crittografia o la firma e la verifica delle chiavi pubbliche o coppie di chiavi curve ellittiche per la firma e la verifica.

Per ulteriori informazioni sulla creazione e sull'utilizzo delle chiavi KMS asimmetriche, consultare Chiavi asimmetriche in AWS KMS.

Chiavi KMS HMAC

Una chiave KMS HMAC rappresenta una chiave simmetrica di lunghezza variabile utilizzata per generare e verificare i codici di autenticazione dei messaggi basati su hash. Il materiale della chiave di una chiave HMAC mantiene sempre AWS KMS crittografato. Per utilizzare una chiave HMAC, richiama l'operazione API `GenerateMac` o `VerifyMac`.

Puoi anche creare chiavi KMS HMAC multi-regione.

Per ulteriori informazioni sulla creazione e sull'utilizzo delle chiavi KMS HMAC, consulta la sezione Chiavi HMAC in AWS KMS.

Chiavi di dati

Le chiavi di dati sono chiavi simmetriche che possono essere usate per crittografare i dati, incluse grandi quantità di dati e altre chiavi crittografiche dati. A differenza delle chiavi KMS, che non

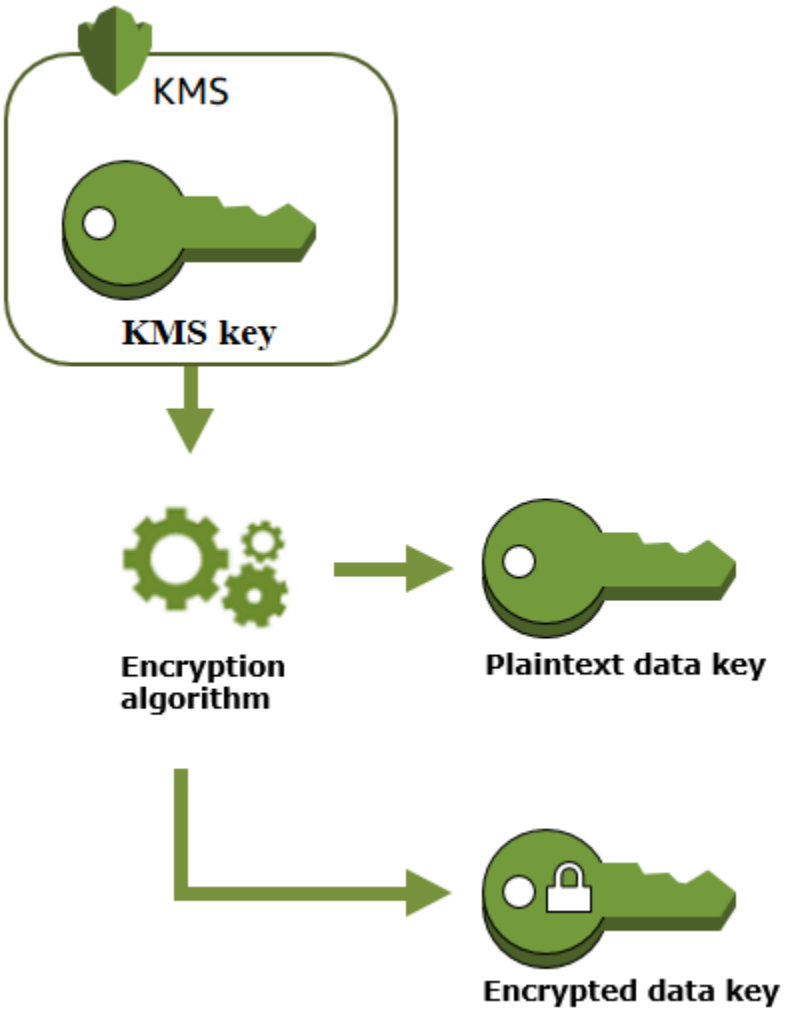
possono essere scaricate, le chiavi di dati vengono restituite all'utente per l'utilizzo al di fuori di AWS KMS.

Quando AWS KMS genera chiavi dati, in genere restituisce una chiave dati in testo normale per l'uso immediato (opzionale) e una copia crittografata della chiave dati che è possibile archiviare in modo sicuro con i dati. Quando vuoi decrittografare i dati, devi prima chiedere AWS KMS per decrittare la chiave di dati crittografati.

AWS KMS genera, crittografa e decritta le chiavi di dati. Tuttavia, AWS KMS non consente di memorizzare, gestire o monitorare le tue chiavi di dati o eseguire operazioni di crittografia con le chiavi di dati. È necessario utilizzare e gestire le chiavi dei dati al di fuori di AWS KMS. Per informazioni sull'utilizzo sicuro delle chiavi dati, consulta AWS Encryption SDK.

Crea una chiave di chiavi

Per creare una chiave dati, richiama l'GenerateDataKeyoperazione. AWS KMSgenera la chiave dati. Quindi crittografa una copia della chiave di dati con una chiave KMS di crittografia simmetrica da te specificata. L'operazione restituisce una copia in testo normale e un'altra copia della chiave dati crittografata con la chiave KMS. L'immagine seguente mostra questa operazione.

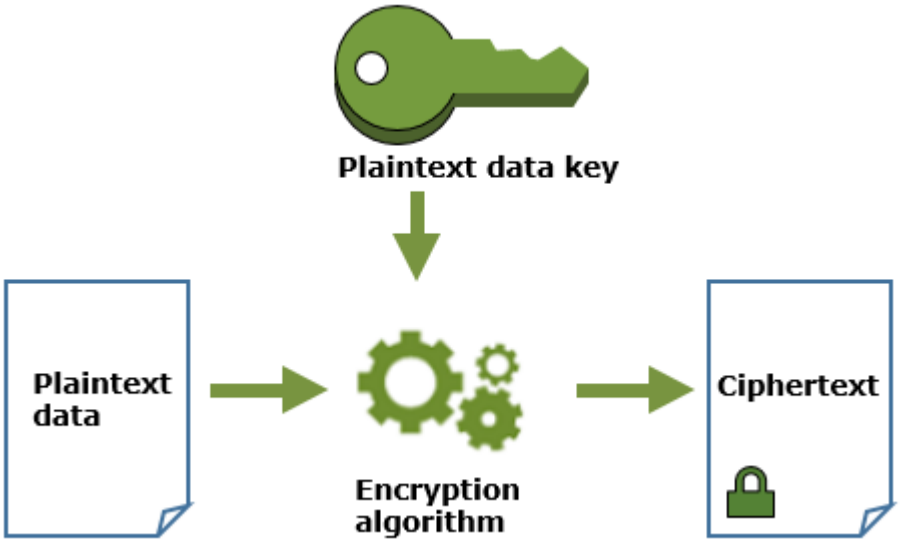


AWS KMSsupporta anche l'GenerateDataKeyWithoutPlaintextoperazione, che restituisce solo una chiave dati crittografata. Quando è necessario utilizzare la chiave di dati, chiedere a AWS KMS di decrittografarla.

Crittografia dei dati con una chiave di dati

AWS KMS non è in grado di utilizzare una chiave di dati per crittografare i dati. Tuttavia, puoi utilizzare la chiave di dati al di fuori di AWS KMS, ad esempio utilizzando OpenSSL o una libreria di crittografia come AWS Encryption SDK.

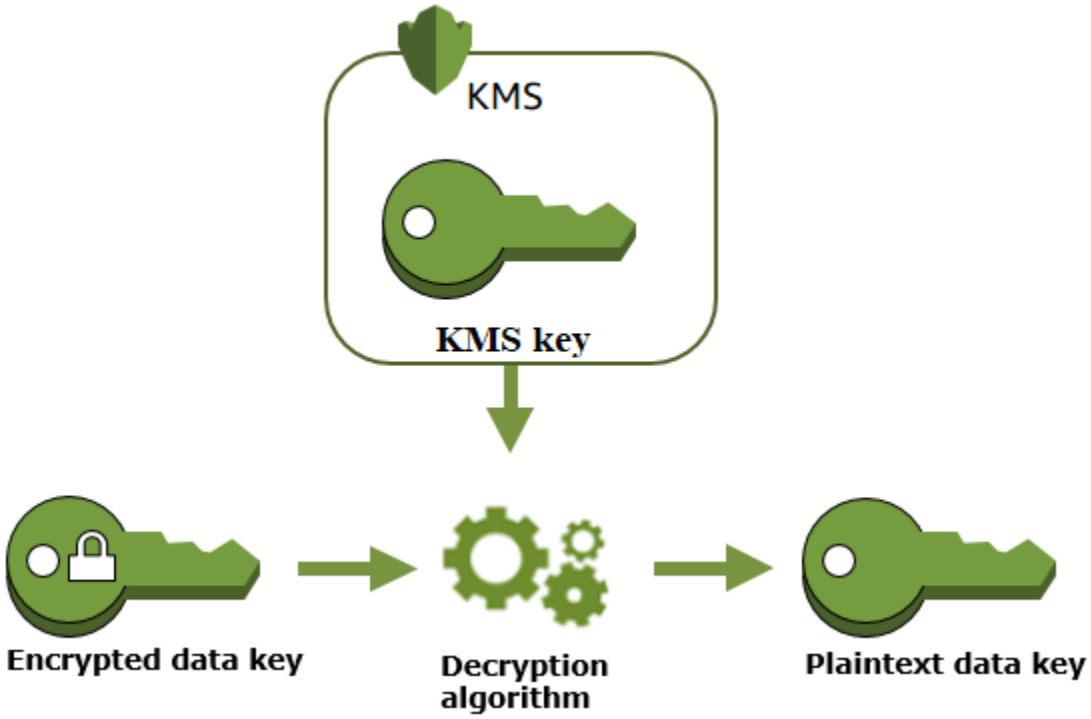
Dopo aver utilizzato la chiave di dati in testo normale per crittografare i dati, eliminarla dalla memoria il prima possibile. È possibile archiviare la chiave di dati crittografati con i dati crittografati in totale sicurezza, in modo che sia disponibile per decrittografare i dati.



Decrittografare i dati con una chiave di dati

Per decrittare i dati, trasferisci la chiave di dati crittografati all'operazione Decrittare. AWS KMS usa la chiave KMS per decrittare la chiave di dati, quindi restituisce la chiave di dati in testo normale. Utilizza la chiave di dati in testo normale per decrittografare i dati, quindi rimuovi la chiave di dati in testo normale dalla memoria al più presto.

Il seguente diagramma illustra come utilizzare l'operazione `Decrypt` per decrittografare una chiave di dati crittografati.



In che modo le chiavi KMS inutilizzabili influiscono sulle chiavi dati

Quando una chiave KMS diventa inutilizzabile, l'effetto è quasi immediato (in base alla coerenza finale). Lo stato della chiave KMS si modifica per riflettere la nuova condizione e tutte le richieste di utilizzo della chiave KMS nelle operazioni di crittografia hanno esito negativo.

Tuttavia, l'effetto sulle chiavi di dati crittografate dalla chiave KMS e sui dati crittografati dalla chiave dati viene ritardato fino a quando la chiave KMS non viene nuovamente utilizzata, ad esempio per decrittografare la chiave dati.

Le chiavi KMS possono diventare inutilizzabili per diversi motivi, incluse le azioni seguenti che è possibile eseguire.

- Disattivazione della chiave KMS
- Pianificazione dell'eliminazione della chiave KMS
- Eliminazione del materiale della chiave da una chiave KMS con materiale della chiave importato o scadenza del materiale della chiave importato.
- Disconnessione dell'archivio delle chiavi di AWS CloudHSM che ospita la chiave KMS o eliminazione della chiave dal cluster AWS CloudHSM che funge da materiale della chiave per la chiave KMS.

- Disconnessione dell'archivio delle chiavi esterne che ospita la chiave KMS o qualsiasi altra azione che interferisca con le richieste di crittografia e decrittografia al proxy, inclusa l'eliminazione della chiave esterna dal relativo gestore delle chiavi esterne.

Questo effetto è particolarmente importante per i numerosi Servizi AWS che utilizzano le chiavi dati per proteggere le risorse gestite dal servizio. L'esempio seguente utilizza Amazon Elastic Block Store (Amazon EBS) e Amazon Elastic Compute Cloud (Amazon EC2). Diversi Servizi AWS utilizzano le chiavi dati in modi diversi. Per maggiori dettagli, consulta la sezione Protezione dei dati del capitolo Sicurezza per il Servizio AWS.

Considera ad esempio questo scenario:

1. Puoi creare un volume EBS crittografato e specificare una chiave KMS per proteggerlo. Amazon EBS chiede a AWS KMS di utilizzare la chiave KMS per generare una chiave dati crittografata per il volume. Amazon EBS archivia la chiave dati crittografata con i metadati del volume.
2. Quando colleghi il volume EBS a un'istanza EC2, Amazon EC2 utilizza la chiave KMS per decodificare la chiave di dati crittografati del volume EBS. Amazon EC2 utilizza la chiave dati nell'hardware Nitro, che è responsabile della crittografia di tutti gli I/O del disco nel volume EBS. La chiave dati persiste nell'hardware Nitro fintantoché il volume EBS è collegato all'istanza EC2.
3. Esegui un'operazione in grado di rendere la chiave KMS inutilizzabile. Questa operazione non ha un effetto immediato sull'istanza EC2 o il volume EBS. Amazon EC2 utilizza la chiave dati, non la chiave KMS, per crittografare tutti gli I/O del disco fintantoché il volume è collegato all'istanza.
4. Tuttavia, quando il volume EBS crittografato è scollegato dall'istanza EC2, Amazon EBS rimuove la chiave dati dall'hardware Nitro. La prossima volta che il volume EBS crittografato viene collegato a un'istanza EC2, il collegamento ha esito negativo, poiché Amazon EBS non è in grado di utilizzare la chiave KMS per decrittare la chiave di dati crittografati del volume. Per utilizzare di nuovo il volume EBS, devi rendere utilizzabile la chiave KMS.

Coppia di chiavi di dati

Le coppie di chiavi di dati sono chiavi di dati asimmetriche costituite da una chiave pubblica e una chiave privata correlate matematicamente. Sono progettate per essere utilizzate per crittografia e decrittografia lato client o firma e verifica al di fuori di AWS KMS.

A differenza delle coppie di chiavi di dati generate da strumenti come OpenSSL, AWS KMS protegge la chiave privata in ogni coppia di chiavi di dati con una chiave KMS di crittografia simmetrica in AWS

KMS da te specificata. Tuttavia, AWS KMS non consente di memorizzare, gestire o monitorare le tue coppie di chiavi di dati o eseguire operazioni di crittografia con le coppie di chiavi di dati. È necessario utilizzare e gestire le coppie di chiavi di dati al di fuori di AWS KMS.

AWS KMS supporta i seguenti tipi di coppie di chiavi di dati:

- Coppia di chiavi RSA: RSA_2048, RSA_3072 e RSA_4096
- Coppie di chiavi basate su curve ellittiche, ECC_NIST_P256, ECC_NIST_P384, ECC_NIST_P521 e ECC_SECG_P256K1
- Coppie di chiavi SM (solo regioni della Cina): SM2

Il tipo di coppia di chiavi dati selezionata in genere dipende dal caso d'uso o dai requisiti normativi. La maggior parte dei certificati richiede chiavi RSA. Le chiavi basate su curve ellittiche sono spesso utilizzate per le firme digitali. Le chiavi ECC_SECG_P256K1 sono comunemente utilizzate per le criptovalute. AWS KMS consiglia di utilizzare coppie di chiavi ECC per la firma e di utilizzare coppie di chiavi RSA per la crittografia o la firma, ma non per entrambe le operazioni. Tuttavia, AWS KMS non può applicare alcuna restrizione all'uso di coppie di chiavi di dati al di fuori di AWS KMS.

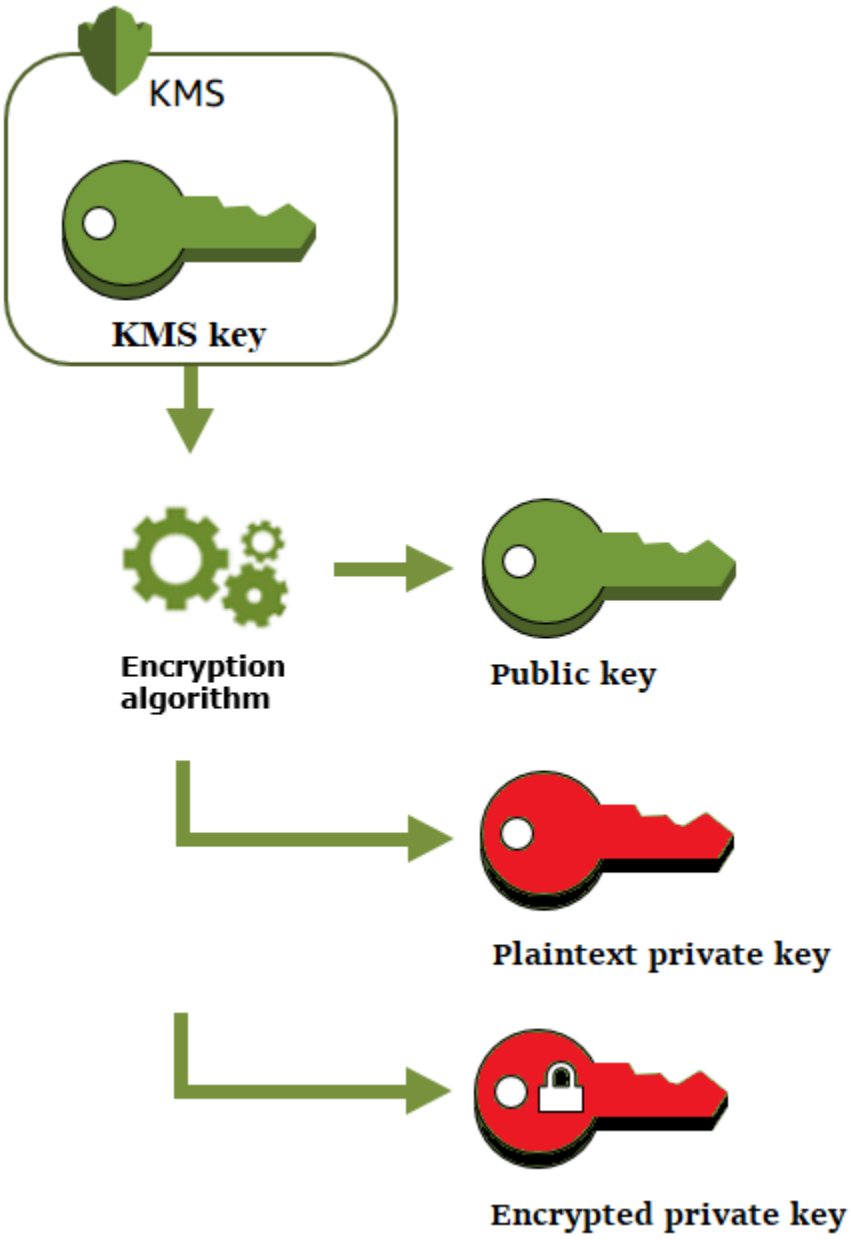
Creare una coppia di chiave di dati

Per creare una coppia di chiavi di dati, chiama le GenerateDataKeyPairWithoutPlaintextoperazioni GenerateDataKeyPairo. Specifica la chiave KMS di crittografia simmetrica che desideri utilizzare per crittografare la chiave privata.

`GenerateDataKeyPair` restituisce una chiave pubblica di testo normale, una chiave privata di testo normale e una chiave privata crittografata. Utilizza questa operazione quando è necessaria una chiave privata di testo normale immediatamente, ad esempio per generare una firma digitale.

`GenerateDataKeyPairWithoutPlaintext` restituisce una chiave pubblica di testo normale e una chiave privata crittografata, ma non una chiave privata di testo normale. Utilizza questa operazione quando non è necessaria una chiave privata di testo normale, ad esempio quando si esegue la crittografia con una chiave pubblica. Successivamente, quando è necessaria una chiave privata di testo normale per decriptare i dati, è possibile chiamare l'operazione Decrittografa.

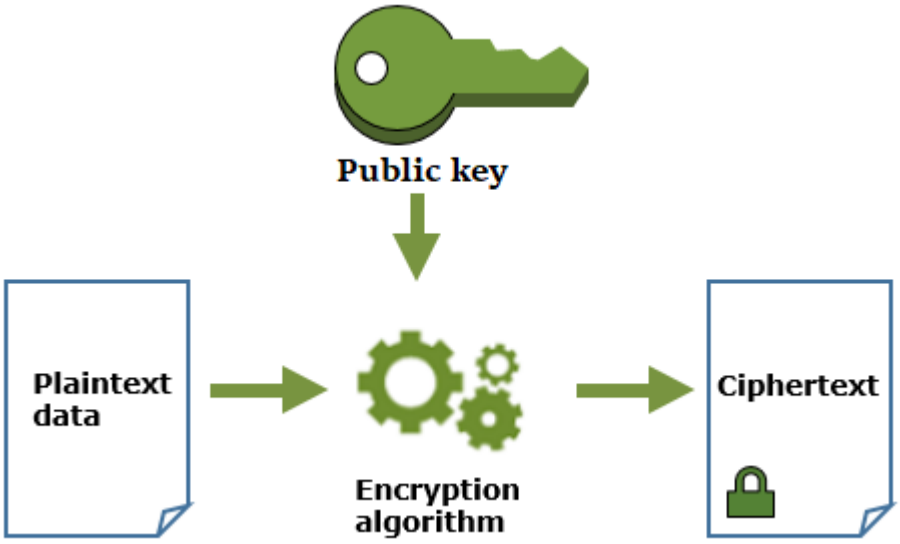
L'immagine seguente mostra l'operazione `GenerateDataKeyPair`. L'operazione `GenerateDataKeyPairWithoutPlaintext` omette la chiave privata di testo normale.



Crittografia dei dati con una coppia di chiavi di dati

Quando si esegue la crittografia con una coppia di chiavi di dati, si utilizza la chiave pubblica della coppia per crittografare i dati e la chiave privata della stessa coppia per decriptare i dati. In genere, usi le coppie di chiavi di dati quando molte parti devono crittografare i dati che solo la parte con la chiave privata può decriptare.

Le parti con la chiave pubblica utilizzano tale chiave per crittografare i dati, come mostrato nel diagramma seguente.

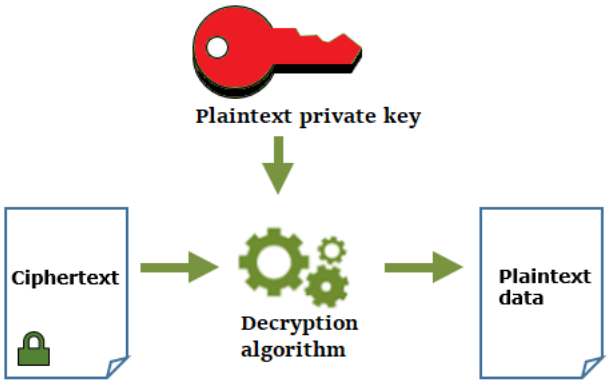


Decrittografia dei dati con una coppia di chiave di dati

Per decriptare i dati, utilizzare la chiave privata nella coppia di chiavi di dati. Affinché l'operazione abbia esito positivo, le chiavi pubbliche e private devono essere della stessa coppia di chiavi di dati ed è necessario utilizzare lo stesso algoritmo di crittografia.

Per decriptare la chiave privata crittografata, passarla all'operazione Decrittografa. Utilizza la chiave privata di testo normale per decriptare i dati. Quindi rimuovi la chiave privata di testo normale dalla memoria il prima possibile.

Il diagramma seguente mostra come utilizzare la chiave privata in una coppia di chiavi di dati per decriptare il testo cifrato.



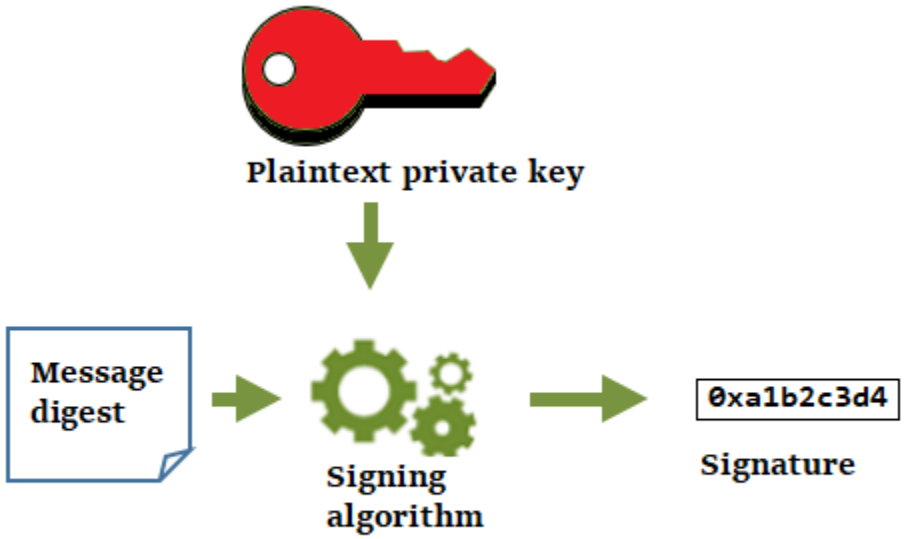
Firmare messaggi con una coppia di chiavi di dati

Per generare una firma crittografica per un messaggio, utilizzare la chiave privata nella coppia di chiavi di dati. Chiunque abbia la chiave pubblica può utilizzarla per verificare che il messaggio sia stato firmato con la chiave privata e che non sia cambiato da quando è stato firmato.

Se crittografi la chiave privata, trasmetti la chiave privata crittografata all'operazione Decrypt. AWS KMS utilizza la chiave KMS per decrittare la chiave di dati e quindi restituisce la chiave privata in testo in chiaro. Utilizza la chiave privata di testo normale per generare la firma. Quindi rimuovi la chiave privata di testo normale dalla memoria il prima possibile.

Per firmare un messaggio, creare un messaggio digest utilizzando una funzione hash di crittografia, ad esempio il comando `dgst` in OpenSSL. Quindi, passa la tua chiave privata di testo normale all'algoritmo di firma. Il risultato è una firma che rappresenta i contenuti del messaggio. (Potrebbe essere possibile firmare messaggi più brevi senza prima creare un digest. La dimensione massima del messaggio varia in base allo strumento di firma utilizzato.)

Il diagramma seguente mostra come utilizzare la chiave privata in una coppia di chiavi di dati per firmare un messaggio.



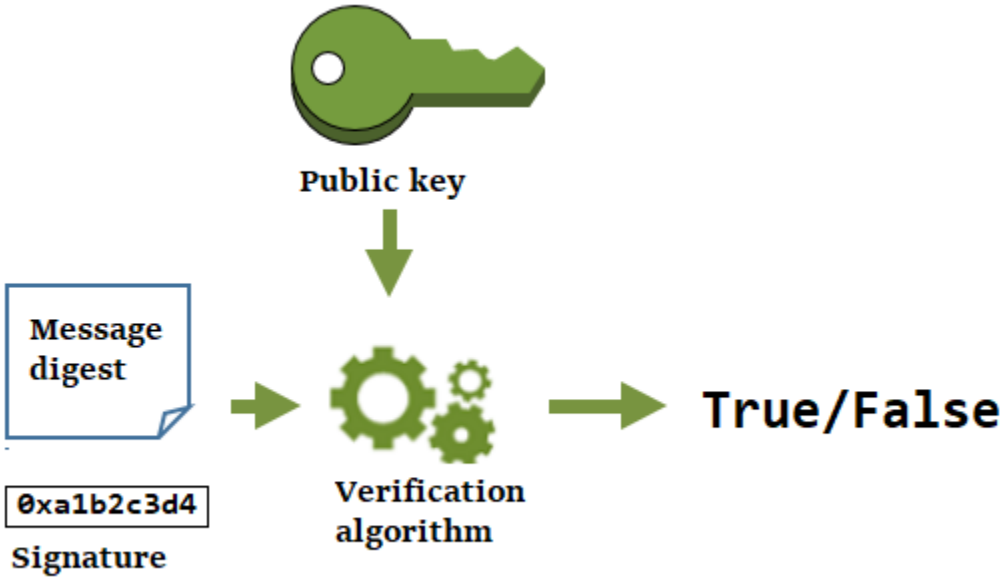
Verificare una firma con una coppia di chiavi di dati

Chiunque abbia la chiave pubblica nella coppia di chiavi di dati può utilizzarla per verificare la firma generata con la chiave privata. La verifica conferma che un utente autorizzato ha firmato il messaggio

con la chiave privata e l'algoritmo di firma specificati e che il messaggio non è cambiato da quando è stato firmato.

Per avere successo, la parte che verifica la firma deve generare lo stesso tipo di digest, utilizzare lo stesso algoritmo e utilizzare la chiave pubblica corrispondente alla chiave privata utilizzata per firmare il messaggio.

Nel diagramma seguente viene illustrato come utilizzare la chiave pubblica in una coppia di chiavi di dati per verificare una firma del messaggio.



Alias

Usa un alias come nome descrittivo per una chiave KMS. Ad esempio, puoi fare riferimento a una chiave KMS come test-key invece di 1234abcd-12ab-34cd-56ef-1234567890ab.

Gli alias semplificano l'identificazione di una chiave KMS nella AWS Management Console. Puoi utilizzare un alias per identificare una chiave KMS in alcune operazioni AWS KMS, incluse le operazioni di crittografia. Nelle applicazioni, puoi utilizzare un singolo alias per fare riferimento alle chiavi KMS diverse in ogni Regione Regione AWS.

Puoi inoltre consentire e negare l'accesso alle chiavi KMS in base ai relativi alias senza modificare le policy o gestire le concessioni. Questa funzione fa parte del supporto AWS KMS per il controllo degli accessi basati su attributi (ABAC). Per informazioni dettagliate, vedi ABAC per AWS KMS.

In AWS KMS, gli alias sono risorse indipendenti, non proprietà di una chiave KMS. Pertanto, puoi aggiungere, modificare ed eliminare un alias senza influire sulla chiave KMS.

> **Important**
>
> Non includere informazioni riservate o sensibili nel nome dell'alias. Gli alias possono apparire in testo semplice nei CloudTrail log e in altri output.

Ulteriori informazioni:

- Per informazioni dettagliate sugli alias, consulta Utilizzo di alias.
- Per informazioni sui formati degli identificatori di chiave, inclusi gli alias, consulta Identificatori chiave () KeyId.
- Per informazioni sulla ricerca degli alias associati a una chiave KMS, consulta Individuazione del nome e dell'ARN dell'alias
- Per esempi di creazione e gestione di alias in più linguaggi di programmazione, consulta Utilizzo degli alias.

store delle chiavi personalizzate

Un archivio delle chiavi personalizzate è una risorsa AWS KMS supportata da un gestore delle chiavi al di fuori di AWS KMS di tua proprietà e gestione. Quando utilizzi una chiave KMS in un archivio delle chiavi personalizzate per un'operazione di crittografia, quest'ultima viene in realtà eseguita nel gestore delle chiavi tramite le relative chiavi crittografiche.

AWS KMS supporta gli archivi delle chiavi di AWS CloudHSM chiavi basati su un cluster AWS CloudHSM e gli archivi delle chiavi esterne supportati da un gestore delle chiavi esterne al di fuori di AWS.

Per ulteriori informazioni, consulta store delle chiavi personalizzate.

Operazioni di crittografia

In AWS KMS, le operazioni di crittografia sono operazioni API che utilizzano le chiavi KMS per proteggere i dati. Poiché le chiavi KMS rimangono all'interno di AWS KMS, è necessario chiamare AWS KMS per utilizzare una chiave KMS in un'operazione di crittografia.

Per eseguire operazioni di crittografia con le chiavi KMS, usa gli SDK AWS, AWS Command Line Interface (AWS CLI), o AWS Tools for PowerShell. Non è possibile eseguire operazioni di crittografia nella console AWS KMS. Per esempi di chiamata delle operazioni crittografiche in diversi linguaggi di programmazione, consulta Programmazione dell'API AWS KMS.

Nella tabella seguente sono elencate le operazioni di crittografia di AWS KMS. Viene illustrato anche il tipo di chiave e i requisiti di utilizzo della chiave per le chiavi KMS usate nell'operazione.

Operazione	Tipo di chiavi	Utilizzo delle chiavi
Decrypt	Simmetrico o asimmetrico	`ENCRYPT_DECRYPT`
Encrypt	Simmetrico o asimmetrico	`ENCRYPT_DECRYPT`
GenerateDataKey	Simmetria	`ENCRYPT_DECRYPT`
GenerateDataKeyPair	Simmetrica [1] Non è supportato sulle chiavi KMS negli archivi delle chiavi personalizzate.	`ENCRYPT_DECRYPT`
GenerateDataKeyPairWithoutPlaintext	Simmetrica [1] Non è supportato sulle chiavi KMS negli archivi delle chiavi personalizzate.	`ENCRYPT_DECRYPT`
GenerateDataKeyWithoutPlaintext	Simmetria	`ENCRYPT_DECRYPT`
GenerateMac	HMAC	`GENERATE_VERIFY_MAC`
GenerateRandom	N/D. Questa operazione non	N/D

Operazione	Tipo di chiavi	Utilizzo delle chiavi
	utilizza una chiave KMS.	
ReEncrypt	Simmetrico o asimmetrico	`ENCRYPT_DECRYPT`
Sign	Asimmetrica	`SIGN_VERIFY`
Verify	Asimmetrica	`SIGN_VERIFY`
VerifyMac	HMAC	`GENERATE_VERIFY_MAC`

[1] Genera coppie di chiavi di dati asimmetriche protette da una chiave KMS di crittografia simmetrica.

Per informazioni sulle autorizzazioni per le operazioni di crittografia, consulta the section called “Riferimento per le autorizzazioni”.

Affinché AWS KMS sia sempre reattivo e performante per tutti gli utenti, sono state stabilite delle quote AWS KMS sul numero di operazioni di crittografia chiamate in ogni secondo. Per informazioni dettagliate, vedi the section called “Quote condivise per le operazioni di crittografia”.

Identificatori chiave () KeyId

Gli identificatori delle chiavi fungono da nomi per le tue chiavi KMS. Consentono di riconoscere le chiavi KMS nella console. Puoi utilizzarli per indicare quali chiavi KMS vuoi utilizzare nelle operazioni API AWS KMS, nelle policy chiave, nelle policy IAM e nelle concessioni. Gli identificatori delle chiavi non sono in alcun modo correlati al materiale chiave associato alla chiave KMS.

AWS KMS definisce vari identificatori di chiave. Quando crei una chiave KMS, AWS KMS genera un ARN di chiave e un ID chiave, che sono proprietà della chiave KMS. Quando crei un alias, AWS KMS genera un ARN dell'alias in base al nome alias definito da te. È possibile visualizzare la chiave e gli identificatori dell'alias nella AWS Management Console e nell'API AWS KMS.

Nella console AWS KMS puoi visualizzare e filtrare le chiavi KMS in base all'ARN di chiave, all'ID chiave o al nome alias ed eseguire l'ordinamento per ID chiave e nome alias. Per informazioni su come individuare gli identificatori della chiave nella console, consulta the section called “Individuazione dell'ID e dell'ARN della chiave”.

Nell'API AWS KMS, i parametri utilizzati per identificare una chiave KMS sono denominati `KeyId` o una variante, ad esempio `TargetKeyId` o `DestinationKeyId`. Tuttavia, i valori di tali parametri non sono limitati agli ID chiave. Alcuni possono prendere qualsiasi identificatore di chiave valido. Per informazioni sui valori di ciascun parametro, consulta la descrizione dei parametri nella documentazione di riferimento dell'API AWS Key Management Service.

> **Note**
>
> Quando utilizzi l'API AWS KMS, presta attenzione all'identificatore della chiave utilizzato. API diverse richiedono identificatori di chiave diversi. In generale, utilizza l'identificatore di chiave più completo e pratico per il processo.

AWS KMS supporta i seguenti identificatori di chiave.

ARN della chiave

L'ARN di chiave è il nome della risorsa Amazon (ARN) di una chiave KMS. Si tratta di un identificatore univoco e completo per la chiave KMS. Un ARN della chiave include l'Account AWS, la Regione e l'ID chiave. Per informazioni su come individuare l'ARN di una chiave KMS, consulta the section called “Individuazione dell'ID e dell'ARN della chiave”.

Il formato di un ARN della chiave è il seguente:

```
arn:<partition>:kms:<region>:<account-id>:key/<key-id>
```

Di seguito è riportato un esempio di ARN della chiave per una chiave KMS per una singola Regione.

```
arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

L'elemento *`key-id`* degli ARN chiave delle chiavi in più Regioni inizia con il prefisso `mrk-`. Di seguito è riportato un esempio di ARN della chiave per una chiave KMS in più Regioni.

```
arn:aws:kms:us-west-2:111122223333:key/mrk-1234abcd12ab34cd56ef1234567890ab
```

ID chiave

L'ID chiave identifica in modo univoco una chiave KMS all'interno di un account e di una Regione. Per informazioni su come individuare l'ID chiave di una chiave KMS, consulta the section called “Individuazione dell'ID e dell'ARN della chiave”.

Di seguito è riportato un esempio di ID chiave per una chiave KMS per una singola Regione.

```
1234abcd-12ab-34cd-56ef-1234567890ab
```

Gli ID chiave di chiavi per più regioni iniziano con il prefisso `mrk-`. Di seguito è riportato un esempio di ARN della chiave per una chiave KMS in più Regioni.

```
mrk-1234abcd12ab34cd56ef1234567890ab
```

ARN dell'alias

L'ARN dell'alias è l'Amazon Resource Name (ARN) di un alias AWS KMS. Si tratta di un identificatore univoco e completo per l'alias e per la chiave KMS che rappresenta. Un ARN dell'alias include l'account Account AWS, la Regione e il nome alias.

In qualsiasi momento, un ARN di alias identifica una particolare chiave KMS. Tuttavia, poiché puoi modificare la chiave KMS associata all'alias, l'ARN di alias può identificare chiavi KMS diverse in momenti diversi. Per informazioni su come individuare l'ARN di alias di una chiave KMS, consulta Individuazione del nome e dell'ARN dell'alias.

Il formato di un ARN dell'alias è il seguente:

```
arn:<partition>:kms:<region>:<account-id>:alias/<alias-name>
```

Di seguito è riportato l'ARN dell'alias per un `ExampleAlias` fittizio.

```
arn:aws:kms:us-west-2:111122223333:alias/ExampleAlias
```

Nome alias

Il nome alias è una stringa di massimo 256 caratteri. Il nome alias identifica in modo univoco una chiave KMS associata all'interno di un account e di una regione. Nell'API AWS KMS, i nomi degli

alias iniziano sempre con `alias/`. Per informazioni sulla ricerca del nome dell'alias di una chiave KMS, consulta Individuazione del nome e dell'ARN dell'alias.

Il formato di un nome alias è il seguente:

```
alias/<alias-name>
```

Ad esempio:

```
alias/ExampleAlias
```

Il prefisso `aws/` di un nome alias è riservato alle Chiavi gestite da AWS. Non è possibile creare un alias con questo prefisso. Ad esempio, il nome alias della Chiave gestita da AWS per Amazon Simple Storage Service (Amazon S3) è il seguente.

```
alias/aws/s3
```

Materiale chiave

Il materiale della chiave è la stringa di bit utilizzata in un algoritmo crittografico. Il materiale della chiave privata deve essere tenuto privato per proteggere le operazioni di crittografia che lo utilizzano. Il materiale della chiave pubblica è progettato per essere condiviso.

Ogni chiave KMS include un riferimento al relativo materiale della chiave nei suoi metadati. L'origine del materiale della chiave delle chiavi KMS di crittografia simmetrica può variare. È possibile utilizzare materiale chiave generato da AWS KMS, materiale chiave generato nel cluster AWS CloudHSM di un archivio delle chiavi personalizzate oppure importare materiale chiave. Se utilizzi materiale della chiave AWS KMS per la chiave KMS di crittografia simmetrica, puoi abilitare la rotazione automatica del materiale della chiave.

Per impostazione predefinita, ogni chiave KMS dispone di materiale chiave univoco. Tuttavia, è possibile creare un set di chiavi per più regioni con lo stesso materiale chiave.

Origine del materiale della chiave

L'origine del materiale chiave è una proprietà chiave KMS che identifica l'origine del materiale chiave nella chiave KMS. L'origine del materiale della chiave viene scelta in fase di creazione della chiave

KMS e non può essere modificata in seguito. L'origine del materiale della chiave influisce sulle caratteristiche di sicurezza, durata, disponibilità, latenza e velocità di trasmissione effettiva della chiave KMS.

Per trovare l'origine del materiale chiave di una chiave KMS, utilizza l'DescribeKeyoperazione o visualizza il valore Origin nella scheda Configurazione crittografica della pagina di dettaglio relativa a una chiave KMS nella console. AWS KMS Per informazioni, consulta Chiavi di visualizzazione.

Le chiavi KMS possono avere uno dei seguenti valori di origine del materiale della chiave.

`AWS_KMS`

AWS KMS crea e gestisce il materiale chiave per la chiave KMS nel proprio archivio delle chiavi. Questo è il valore predefinito e consigliato per la maggior parte delle chiavi KMS.

Per informazioni sulla creazione di chiavi con il materiale della chiave da AWS KMS, consulta Creazione di chiavi.

`EXTERNAL (Import key material)`

La chiave KMS dispone di materiale chiave importato. Quando crei una chiave KMS con un'origine del materiale chiave `External`, la chiave KMS non dispone di materiale chiave. Successivamente, puoi importare il materiale chiave nella chiave KMS. Quando si utilizza materiale della chiave importato, è necessario proteggere e gestire tale materiale all'esterno del AWS KMS, inclusa la sostituzione del materiale della chiave se scade. Per informazioni dettagliate, vedi Informazioni sul materiale della chiave importato.

Per informazioni sulla creazione di una chiave KMS per il materiale della chiave importato, consulta Fase 1: creare una chiave KMS senza materiale chiave.

`AWS_CLOUDHSM`

AWS KMS crea il materiale della chiave nel cluster AWS CloudHSM per l'archivio delle chiavi di AWS CloudHSM.

Per informazioni sulla creazione di una chiave KMS in un archivio delle chiavi di AWS CloudHSM, consulta la sezione Creazione di chiavi KMS in un archivio delle chiavi di AWS CloudHSM.

`EXTERNAL_KEY_STORE`

Il materiale della chiave è una chiave crittografica in un gestore delle chiavi esterne al di fuori di AWS. Questa origine è supportata solo per le chiavi KMS in un archivio delle chiavi esterne.

Per informazioni sulla creazione di una chiave KMS in un archivio delle chiavi esterne, consulta la sezione Creazione di chiavi KMS in un archivio delle chiavi esterne.

Specifica della chiave

Key spec è una proprietà che rappresenta la configurazione crittografica della chiave. Il significato delle specifiche della chiave differisce dal tipo di chiave.

- AWS KMSChiavi — Specifica della chiave specifica se la chiave KMS è simmetrica o asimmetrica. Determina anche il tipo di materiale della chiave e gli algoritmi supportati. La specifica della chiave viene scelta in fase di creazione della chiave KMS e non può essere modificata in seguito. La specifica della chiave predefinita, SYMMETRIC_DEFAULT, rappresenta una chiave crittografica simmetrica a 256 bit.

  > **Note**
  >
  > La `KeySpec` per una chiave KMS era nota come `CustomerMasterKeySpec`. Il `CustomerMasterKeySpec` parametro dell'CreateKeyoperazione è obsoleto. Utilizza invece il parametro `KeySpec`, che funziona allo stesso modo. Per evitare modifiche irreversibili, la risposta delle DescribeKeyoperazioni `CreateKey` and ora include sia `KeySpec` `CustomerMasterKeySpec` i membri che hanno gli stessi valori.

  Per un elenco di specifiche della chiave e aiuto nella scelta di specifiche della chiave, consulta Selezione delle specifiche della chiave. Per trovare le specifiche chiave di una chiave KMS, utilizza l'DescribeKeyoperazione o consulta la scheda Configurazione crittografica nella pagina dei dettagli relativa a una chiave KMS nella console. AWS KMS Per informazioni, consulta Chiavi di visualizzazione.

  Per limitare le specifiche chiave che i mandanti possono utilizzare durante la creazione delle chiavi KMS, usa la chiave kms: condition. KeySpec Puoi inoltre utilizzare la chiave di condizione `kms:KeySpec` per consentire ai principali di richiamare le operazioni AWS KMS solo su una chiave KMS con una determinata specifica della chiave. Ad esempio, puoi negare l'autorizzazione per pianificare l'eliminazione di tutte le chiavi KMS con una specifica delle chiave `RSA_4096`.
- Chiavi dati (GenerateDataKey): la specifica chiave determina la lunghezza di una chiave dati AES.
- Coppie di chiavi dati (GenerateDataKeyPair): la specifica della coppia di chiavi determina il tipo di materiale chiave nella coppia di chiavi dati.

Utilizzo delle chiavi

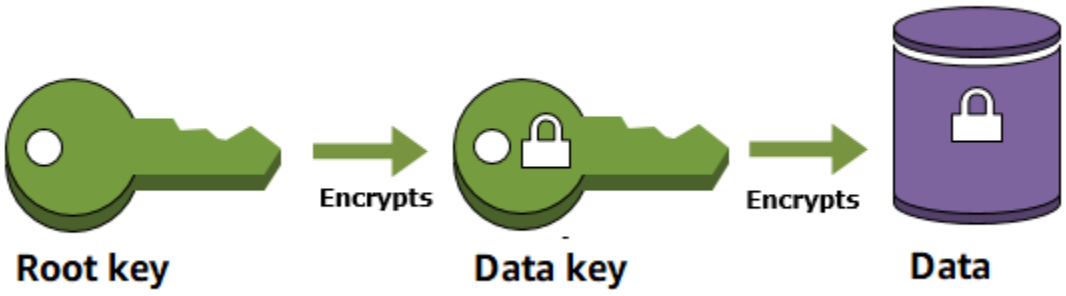
L'utilizzo della chiave è una proprietà che determina le operazioni di crittografia supportate dalla chiave. L'utilizzo della chiave per le chiavi KMS può essere `ENCRYPT_DECRYPT`, `SIGN_VERIFY` o `GENERATE_VERIFY_MAC`. Ogni chiave KMS può avere solo un utilizzo. L'utilizzo di una chiave KMS per più di un tipo di operazione rende il prodotto di entrambe le operazioni più vulnerabile agli attacchi.

Per informazioni sulla scelta dell'utilizzo della chiave per la chiave KMS, consulta la sezione Selezione dell'utilizzo della chiave. Per scoprire l'utilizzo delle chiavi di una chiave KMS, utilizza l'DescribeKeyoperazione o scegli la scheda Configurazione crittografica nella pagina dei dettagli relativa a una chiave KMS nella console. AWS KMS Per informazioni, consulta Chiavi di visualizzazione.

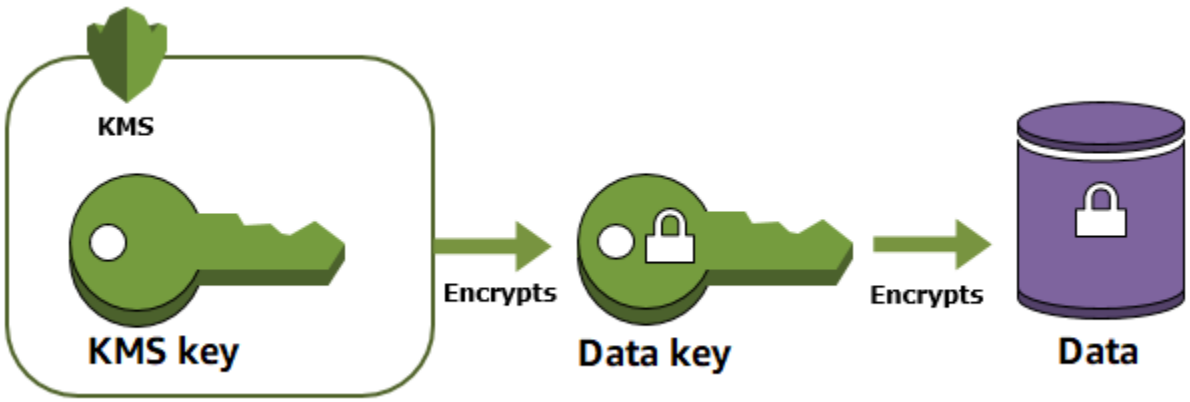
Crittografia envelope

Quando esegui la crittografia dei dati, i dati sono protetti, ma è necessario proteggere la chiave crittografica. Una strategia consiste nel crittografarla. La Crittografia envelope consiste nel crittografare i dati di testo normale con una chiave di dati, quindi crittografare la chiave di dati in un'altra chiave.

È anche possibile crittografare la chiave crittografica dei dati in un'altra chiave crittografica e crittografare tale chiave crittografica con un'altra chiave crittografica. Alla fine, però, una chiave deve rimanere in testo normale in modo da poter decrittografare le chiavi e i dati. Questa chiave crittografica di primo livello della chiave in testo normale è nota come chiave radice.



AWS KMS consente di proteggere le chiavi crittografiche per archiviarle e gestirle in modo sicuro. Le chiavi radice archiviate in AWS KMS, note come AWS KMS keys, mantengono i moduli di sicurezza hardware convalidati da FIPSAWS KMS sempre crittografati. Per utilizzare una chiave KMS, è necessario chiamare AWS KMS.



La crittografia envelope offre diversi vantaggi:

- Protezione delle chiavi dei dati

  Quando crittografi una chiave di dati, non è necessario preoccuparsi di dove archiviarla, poiché la chiave di dati è intrinsecamente protetta dalla crittografia. Puoi archiviare la chiave di dati crittografata in modo sicuro con i dati crittografati.

- Crittografia degli stessi dati con più chiavi

  Le operazioni di crittografia possono essere dispendiose in termini di tempo, soprattutto quando i dati crittografati sono oggetti di grandi dimensioni. Invece di ricrittografare dati grezzi più volte con chiavi diverse, è possibile ricrittografare solo le chiavi di dati che proteggono i dati grezzi.

- Abbinare i punti di forza di più algoritmi

  In generale, gli algoritmi di chiavi simmetriche sono più veloci e producono testi cifrati più piccoli rispetto agli algoritmi di chiave pubblica. Tuttavia, gli algoritmi di chiave pubblica forniscono una separazione intrinseca dei ruoli e facilitano la gestione delle chiavi. La crittografia envelope ti consente di abbinare i punti di forza di ciascuna strategia.

Contesto di crittografia

Tutte le operazioni crittografiche AWS KMS con chiavi KMS di crittografia simmetrica accettano un contesto di crittografia, una serie facoltativa di coppie chiave-valore non segrete che possono contenere ulteriori informazioni contestuali sui dati. AWS KMS utilizza il contesto di crittografia come dati autenticati aggiuntivi (AAD) per il supporto della crittografia autenticata.

Quando un contesto di crittografia viene fornito in una richiesta di crittografia, è vincolato a livello crittografico al testo cifrato allo stesso modo del contesto di crittografia che è necessario per decrittografare (o per decrittografare e ricrittografare) i dati. Se il contesto di crittografia fornito nella richiesta di decrittografia non costituisce una corrispondenza esatta a livello di maiuscole e minuscole, la richiesta ha esito negativo. Solo l'ordine delle coppie chiave-valore nel contesto di crittografia può variare.

> **Note**
>
> Non è possibile specificare un contesto di crittografia in un'operazione di crittografia con una chiave KMS asimmetrica o una chiave KMS HMAC. Gli algoritmi asimmetrici e gli algoritmi MAC non supportano un contesto di crittografia.

Il contesto di crittografia non è segreto e non è crittografato. Appare in testo normale nei log AWS CloudTrail in modo da poterlo utilizzare per individuare e categorizzare le operazioni di crittografia. Il contesto di crittografia non dovrebbe includere informazioni sensibili. È consigliabile che il contesto di crittografia descriva i dati crittografati o decrittografati. Ad esempio, quando si esegue la crittografia di un file, è possibile utilizzare parte del percorso di file come contesto di crittografia.

```
"encryptionContext": {
    "department": "10103.0"
}
```

Ad esempio, quando crittografa volumi e snapshot creati con l'operazione Amazon Elastic Block Store (Amazon EBS) CreateSnapshot, Amazon EBS utilizza l'ID del volume come valore del contesto di crittografia.

```
"encryptionContext": {
  "aws:ebs:id": "vol-abcde12345abc1234"
}
```

Puoi inoltre utilizzare il contesto di crittografia per perfezionare o limitare l'accesso alle AWS KMS keys nel proprio account. È possibile utilizzare il contesto di crittografia come vincolo nelle concessioni e come una condizione nelle istruzioni di policy.

Per informazioni su come utilizzare il contesto di crittografia per proteggere l'integrità dei dati crittografati, consulta il post Come proteggere l'integrità dei dati crittografati utilizzando AWS Key Management Service e EncryptionContext sul blog sulla sicurezza. AWS

Ulteriori informazioni sul contesto di crittografia.

Regole sul contesto di crittografia

AWS KMS applica le seguenti regole per le chiavi e i valori del contesto di crittografia.

- La chiave e il valore in una coppia del contesto di crittografia devono essere stringhe letterali semplici. Se utilizzi un tipo diverso, ad esempio integer o float, AWS KMS lo interpreta come una stringa.
- Le chiavi e i valori in un contesto di crittografia possono includere caratteri Unicode. Se un contesto di crittografia include caratteri non consentiti nelle policy della chiave o nelle policy IAM, non sarà possibile specificare il contesto di crittografia nelle chiavi di condizioni della policy, ad esempio `kms:EncryptionContext:context-key` e `kms:EncryptionContextKeys`. Per maggiori informazioni sulle regole delineate nel documento delle policy delle chiavi, consulta la sezione Formato della policy della chiave. Per informazioni dettagliate sulle regole delineate nel documento delle policy IAM, consulta la sezione Requisiti del nome IAM nella Guida per l'utente di IAM.

Contesto di crittografia nelle policy

Il contesto di crittografia viene utilizzato principalmente per verificare l'integrità e l'autenticità. Tuttavia, puoi anche utilizzare il contesto di crittografia per controllare l'accesso alle AWS KMS keys di crittografia simmetrica nelle policy delle chiavi e nelle policy IAM.

Le chiavi kms:EncryptionContext: e kms: EncryptionContextKeys condition consentono (o negano) un'autorizzazione solo quando la richiesta include particolari chiavi di contesto di crittografia o coppie chiave-valore.

Ad esempio, la seguente istruzione della policy delle chiavi consente al ruolo `RoleForExampleApp` di utilizzare la chiave KMS nelle operazioni `Decrypt`. Utilizza la chiave di condizione `kms:EncryptionContext:context-key` per concedere questa autorizzazione solo quando il contesto di crittografia nella richiesta include una coppia di contesto di crittografia `AppName:ExampleApp`.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:Decrypt",
  "Resource": "*",
```

```
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:AppName": "ExampleApp"
    }
  }
}
```

Per ulteriori informazioni su queste chiavi di condizione del contesto di crittografia, consulta Chiavi di condizione per AWS KMS.

Contesto di crittografia nelle concessioni

Quando si crea una concessione, è possibile includere vincoli di concessione che stabiliscono le condizioni per le autorizzazioni di concessione. AWS KMS supporta due vincoli di concessione, `EncryptionContextEquals` e `EncryptionContextSubset`, entrambi i quali coinvolgono il contesto di crittografia in una richiesta di un'operazione di crittografia. Quando utilizzi questi vincoli di concessione, le autorizzazioni nella concessione sono valide solo quando il contesto di crittografia nella richiesta per l'operazione di crittografia soddisfa i requisiti dei vincoli di concessione.

Ad esempio, puoi aggiungere un vincolo di concessione a una `EncryptionContextEquals` concessione che consente l'operazione. GenerateDataKey Con questo vincolo, la concessione consente l'operazione solo quando il contesto di crittografia nella richiesta corrisponde a livello di maiuscole e minuscole al contesto di crittografia nel vincolo di concessione.

```
$ aws kms create-grant \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:user/exampleUser \
    --retiring-principal arn:aws:iam::111122223333:role/adminRole \
    --operations GenerateDataKey \
    --constraints EncryptionContextEquals={Purpose=Test}
```

Una richiesta come la seguente dal principale beneficiario soddisferebbe il `EncryptionContextEquals` vincolo.

```
$ aws kms generate-data-key \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --key-spec AES_256 \
    --encryption-context Purpose=Test
```

Per ulteriori informazioni sui vincoli della concessione, consulta Utilizzo dei vincoli di concessione. Per informazioni dettagliate sugli alias, consulta the section called “Concessioni”.

Registrazione del contesto di crittografia

AWS KMS utilizza AWS CloudTrail per registrare il contesto di crittografia, in modo che sia possibile determinare a quali chiavi KMS e dati è stato effettuato l'accesso. La voce di log mostra esattamente la chiave KMS utilizzata per crittografare o decrittare dati specifici a cui fa riferimento il contesto di crittografia nella voce di log.

> **Important**
>
> Poiché il contesto di crittografia viene registrato, non deve contenere informazioni sensibili.

Archiviazione del contesto di crittografia

Per semplificare l'utilizzo di qualsiasi contesto di crittografia quando chiami le operazioni `Decrypt` o `ReEncrypt`, puoi archiviare il contesto di crittografia insieme ai dati crittografati. Ti consigliamo di archiviare solo il contesto di crittografia sufficiente per aiutarti a creare il contesto di crittografia completo quando ne hai bisogno per la crittografia o la decrittografia.

Ad esempio, se il contesto di crittografia è il percorso completo di un file, archivia solo la parte del percorso con i contenuti crittografati del file. Quando ti occorre il contesto di crittografia completo, puoi ricostruirlo dal frammento archiviato. Se qualcuno altera il file, ad esempio lo rinomina o lo sposta in un percorso diverso, il valore del contesto di crittografia cambia e la richiesta di decrittografia ha esito negativo.

Policy delle chiavi

Quando crei una chiave KMS, puoi stabilire chi la può utilizzare e gestire. Queste autorizzazioni sono contenute in un documento chiamato policy delle chiavi. Puoi utilizzare la policy delle chiavi per aggiungere, rimuovere o modificare le autorizzazioni in qualsiasi momento per una chiave gestita dal cliente. Tuttavia, non puoi modificare la policy delle chiavi per una Chiavi gestite da AWS. Per ulteriori informazioni, consultare Policy delle chiavi in AWS KMS.

Grant

La concessione è uno strumento policy che consente ai principali AWS da utilizzare AWS KMS keys in operazioni di crittografia. Può anche consentire loro di visualizzare una chiave KMS (DescribeKey) e creare e gestire concessioni. Quando autorizzi l'accesso a una chiave KMS, le concessioni vengono prese in considerazione insieme alle policy chiave e alle policy IAM. I privilegi vengono

spesso utilizzati per le autorizzazioni temporanee perché è possibile crearne una, utilizzarne le autorizzazioni ed eliminarla senza modificare le policy chiave o le policy IAM. Poiché le concessioni possono essere molto specifiche e sono facili da creare e revocare, vengono spesso utilizzate per fornire autorizzazioni temporanee o autorizzazioni più granulari.

Per informazioni dettagliate sulle concessioni, inclusa la terminologia delle concessioni, consulta Concessioni in AWS KMS.

Verifica dell'utilizzo della chiave KMS

È possibile utilizzare AWS CloudTrail per controllare l'utilizzo delle chiavi. CloudTrail crea file di registro che contengono una cronologia delle chiamate AWS API e degli eventi correlati per il tuo account. Questi file di log includono tutte le richieste API AWS KMS effettuate con la console di gestione AWS, gli SDK AWS e gli strumenti a riga di comando. I file di log includono anche le richieste per AWS KMS effettuate dai servizi AWS per tuo conto. Puoi utilizzare questi file di log per trovare informazioni importanti, tra cui quando sono state usate le chiavi KMS, l'operazione richiesta, l'identità del richiedente e l'indirizzo IP di origine. Per ulteriori informazioni, consulta Registrazione con AWS CloudTrail e la Guida per l'utente di AWS CloudTrail.

Infrastruttura di gestione delle chiavi

Una pratica comune nella crittografia consiste nel crittografare e decrittografare utilizzando un algoritmo pubblico e sottoposto a revisione, come, ad esempio, AES (Advanced Encryption Standard) e una chiave segreta. Riuscire a mantenere una chiave segreta costituisce uno dei problemi principali della crittografia. Questo è in genere il compito di un'infrastruttura di gestione delle chiavi (KMI). AWS KMS gestisce la KMI per te. AWS KMS crea e archivia in modo sicuro le chiavi radice, denominate AWS KMS keys. Per ulteriori informazioni su come funziona AWS KMS, consulta AWS Key Management Service Dettagli crittografici di.

Gestione delle chiavi

Per iniziare a utilizzare AWS KMS, creare una AWS KMS key.

Negli argomenti di questa sezione viene illustrato come gestire la chiave KMS di base, una chiave KMS di crittografia simmetrica, dalla sua creazione fino all'eliminazione. Include argomenti sulla modifica e la visualizzazione delle chiavi, l'assegnazione di tag alle chiavi, l'abilitazione e la disabilitazione delle chiavi, la rotazione del materiale chiave e l'utilizzo di strumenti e servizi AWS per monitorare l'uso delle chiavi KMS. Include anche informazioni sull'utilizzo di AWS CloudFormation per creare e gestire le chiavi KMS e una documentazione di riferimento sullo stato delle chaivi che mostra lo stato chiave richiesto per ciascuna operazione AWS KMS.

Per ulteriori informazioni sulla creazione, l'utilizzo e la gestione di altri tipi di chiavi KMS, consulta la sezione Chiavi per uso speciale.

Argomenti

Creazione di chiavi

È possibile creare AWS KMS keys in o utilizzando l'CreateKeyoperazione o un AWS CloudFormationmodello. AWS Management Console Durante questo processo, scegli il tipo di chiave KMS, la sua regionalità (a regione singola o multi-regione) e l'origine del materiale della chiave (per impostazione predefinita, il materiale della chiave viene creato da AWS KMS). Una volta creata la

chiave KMS, non è più possibile modificare queste proprietà. Inoltre puoi impostare la policy delle chiavi per la chiave KMS, che è possibile modificare in qualsiasi momento.

In questo argomento viene descritto come creare la chiave KMS di base, una chiave KMS di crittografia simmetrica per una singola regione con materiale della chiave generato da AWS KMS. Puoi utilizzare questa chiave KMS per proteggere le tue risorse in un Servizio AWS. Per informazioni dettagliate sulle chiavi KMS di crittografia simmetrica, consulta la sezione Specifica della chiave SYMMETRIC_DEFAULT. Per assistenza nella creazione di altri tipi di chiavi, consulta la sezione Chiavi per uso speciale.

Se stai creando una chiave KMS per crittografare i dati archiviati o gestiti in un servizio AWS, crea una chiave KMS di crittografia simmetrica. I servizi AWS integrati con AWS KMS usano soltanto chiavi KMS di crittografia simmetrica per crittografare i dati. Questi servizi non supportano la crittografia con chiavi KMS asimmetriche. Per informazioni su quale tipo di chiave KMS creare, consulta Scelta di un tipo di chiave KMS.

> **Note**
>
> Le chiavi KMS simmetriche ora vengono definite chiavi KMS di crittografia simmetrica. AWS KMS supporta due tipi di chiavi KMS simmetriche, le chiavi KMS di crittografia simmetrica (il tipo predefinito) e le chiavi KMS HMAC, anch'esse simmetriche.

Quando crei una chiave KMS nella console AWS KMS, è necessario assegnarle un alias (nome descrittivo). L'operazione `CreateKey` non crea un alias per la nuova chiave KMS. Per creare un alias per una chiave KMS nuova o esistente, usa l'CreateAliasoperazione. Per informazioni dettagliate sugli alias in AWS KMS, consulta Utilizzo di alias.

In questo argomento viene descritto come creare una chiave KMS di crittografia simmetrica. Usa la tabella seguente per trovare istruzioni per la creazione di chiavi KMS di tipo diverso.

Istruzioni per la creazione di una chiave KMS

Tipo di chiave KMS	Istruzioni
Chiave di crittografia simmetrica (SYMMETRIC_DEFAULT)	the section called “Creazione di chiavi KMS di crittografia simmetrica”
Chiave asimmetrica	the section called “Creazione di chiavi KMS asimmetriche”

Tipo di chiave KMS	Istruzioni
Chiave HMAC	the section called “Creazione di chiavi HMAC”
Chiave multi-regione (di qualunque tipo)	the section called “Creazione di una chiave primaria con materiale chiave importato” the section called “Creazione di una chiave di replica con materiale chiave importato”
Materiale della chiave importato ("Bring your own key — BYOK")	the section called “Fase 1: creare una chiave KMS senza materiale chiave”
Archivio delle chiavi di AWS CloudHSM	the section called “Creazione di chiavi KMS in un archivio delle chiavi di AWS CloudHSM”
Archivio chiavi esterno ("Hold your own key — HYOK")	the section called “Creazione di chiavi KMS in un archivio delle chiavi esterne”

Ulteriori informazioni:

- Per creare chiavi di dati per la crittografia lato client, usa l'operazione. GenerateDataKey
- Per creare una chiave KMS asimmetrica per la crittografia o la firma, consultare Creazione di chiavi KMS asimmetriche.
- Per creare una chiave KMS HMAC, consulta la sezione Creazione di chiavi KMS HMAC.
- Per creare una chiave KMS con materiale della chiave importato ("bring your own key"), consulta la sezione Importazione del materiale della chiave - Fase 1: creare una AWS KMS key senza materiale chiave.
- Per creare una chiave primaria o una chiave di replica multi-Regione, consultare Creazione di chiavi multiregione.
- Per creare una chiave KMS in un archivio delle chiavi personalizzate (dove l'origine del materiale della chiave è un archivio delle chiavi personalizzate (CloudHSM)), consulta la sezione Creazione di chiavi KMS in un archivio delle chiavi di AWS CloudHSM.
- Per utilizzare un AWS CloudFormation modello per creare una chiave KMS, consulta AWS::KMS::Keyla Guida per l'AWS CloudFormationutente.

- Per determinare se una chiave KMS esistente è simmetrica o asimmetrica, consultare Individuazione di chiavi KMS asimmetriche.
- Per utilizzare la nuova chiave KMS a livello di programmazione e nelle operazioni dell'interfaccia a riga di comando è necessario disporre di un ID chiave o ARN di chiave. Per istruzioni dettagliate, vedi Individuazione dell'ID e dell'ARN della chiave.
- Per informazioni sulle quote applicabili alle chiavi KMS, consulta Quote.

Argomenti

Autorizzazioni per la creazione di chiavi KMS

Per creare una chiave KMS nella console o utilizzando le API, è necessario disporre delle autorizzazioni seguenti in una policy IAM. Quando possibile, utilizzare le chiavi di condizione per limitare le autorizzazioni. Ad esempio, puoi utilizzare la chiave kms: KeySpec condition in una policy IAM per consentire ai principali di creare solo chiavi di crittografia simmetriche.

Per un esempio di policy IAM per le entità principali che creano chiavi, vedere Consentire a un utente di creare chiavi KMS.

> **Note**
>
> Presta attenzione quando concedi ai principali l'autorizzazione per gestire tag e alias. Modificando un tag o un alias puoi consentire o negare l'autorizzazione alla chiave gestita dal cliente. Per informazioni dettagliate, vedi ABAC per AWS KMS.

- kms: è obbligatorio. CreateKey
- kms: CreateAlias è necessario per creare una chiave KMS nella console in cui è richiesto un alias per ogni nuova chiave KMS.
- kms: TagResource è necessario per aggiungere tag durante la creazione della chiave KMS.
- iam: CreateServiceLinkedRole è necessario per creare chiavi primarie multiregionali. Per informazioni dettagliate, vedi Controllo dell'accesso alle chiavi multi-regione.

Il kms: non è richiesta PutKeyPolicy l'autorizzazione per creare la chiave KMS. L'autorizzazione `kms:CreateKey` include l'autorizzazione per impostare la policy chiave iniziale. Tuttavia, è necessario aggiungere questa autorizzazione alla policy chiave durante la creazione della chiave KMS per assicurarsi di poter controllare l'accesso alla chiave KMS. L'alternativa è utilizzare il BypassLockoutSafetyCheckparametro, che non è consigliato.

Le chiavi KMS appartengono all'account AWS in cui sono state create. L'utente IAM che crea una chiave KMS non è considerato il proprietario della chiave e non dispone automaticamente dell'autorizzazione a utilizzare o gestire la chiave KMS creata. Come qualsiasi altro principale, il creatore di chiavi deve ottenere l'autorizzazione tramite una policy chiave, una policy IAM o una concessione. Tuttavia, i principali che hanno l'autorizzazione `kms:CreateKey` possono impostare la policy chiave iniziale e concedersi l'autorizzazione all'utilizzo o alla gestione della chiave.

Creazione di chiavi KMS di crittografia simmetrica

Puoi creare chiavi KMS nella AWS Management Console o utilizzando l'API AWS KMS.

In questo argomento viene descritto come creare la chiave KMS di base, una chiave KMS di crittografia simmetrica per una singola regione con materiale della chiave generato da AWS KMS. Puoi utilizzare questa chiave KMS per proteggere le tue risorse in un Servizio AWS. Per assistenza nella creazione di altri tipi di chiavi, consulta la sezione Chiavi per uso speciale.

Creazione di chiavi KMS di crittografia simmetrica (console)

Puoi utilizzare la AWS Management Console per creareAWS KMS keys (chiavi KMS).

> **Important**
>
> Non includere informazioni riservate o sensibili nell'alias, nella descrizione o nei tag. Questi campi possono apparire in testo semplice nei CloudTrail log e in altri output.

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.
4. Scegliere Create key (Crea chiave).

5. Per creare una chiave KMS di crittografia simmetrica, in Key type (Tipo di chiave) scegli Symmetric (Simmetrica).

   Per informazioni su come creare una chiave KMS asimmetrica nella console AWS KMS, consulta Creazione di chiavi KMS asimmetriche (console).

6. In Utilizzo della chiave, l'opzione Crittografa e decrittografa è selezionata per impostazione predefinita.

   Per informazioni su come creare le chiavi KMS che generano e verificano i codici MAC, consulta la sezione Creazione di chiavi KMS HMAC.

7. Seleziona Next (Successivo).

   Per informazioni sulle opzioni avanzate, consulta Chiavi per uso speciale.

8. Digita un alias per la chiave KMS. Un nome di alias non può iniziare con **`aws/`**. Il prefisso **`aws/`** è riservato da Amazon Web Services per rappresentare le Chiavi gestite da AWS nel tuo account.

   > **Note**
   >
   > L'aggiunta, l'eliminazione o l'aggiornamento di un alias può consentire o negare l'autorizzazione alla chiave KMS. Per informazioni dettagliate, consulta ABAC per AWS KMS e Utilizzo degli alias per controllare l'accesso alle chiavi KMS.

   Un alias è un nome visualizzato che può essere utilizzato per identificare la chiave KMS. È consigliabile scegliere un alias che indica il tipo di dati che desideri proteggere o l'applicazione che desideri utilizzare con la chiave KMS.

   Gli alias sono obbligatori quando si crea una chiave KMS nella AWS Management Console. Sono opzionali quando si utilizza l'CreateKeyoperazione.

9. (Facoltativo) Digita una descrizione per la chiave KMS.

   Puoi aggiungere una descrizione ora o aggiornarla in qualsiasi momento, a meno che lo stato della chiave non sia `Pending Deletion` o `Pending Replica Deletion`. Per aggiungere, modificare o eliminare la descrizione di una chiave gestita dal cliente esistente, modifica la descrizione in AWS Management Console o utilizza l'UpdateKeyDescriptionoperazione.

10. (Facoltativo) Digitare una chiave di tag e un valore di tag facoltativo. Per aggiungere più di un tag alla chiave KMS scegli Add tag (Aggiungi tag).

> **Note**
>
> L'applicazione o l'eliminazione di un tag chiave KMS può consentire o negare l'autorizzazione alla chiave KMS. Per informazioni dettagliate, consulta ABAC per AWS KMS e Utilizzo dei tag per controllare l'accesso alle chiavi KMS.

Quando aggiungi i tag alle risorse AWS, AWS genera un report di allocazione dei costi in cui l'utilizzo e i costi sono aggregati in base ai tag. I tag possono essere utilizzati anche per controllare l'accesso a una chiave KMS. Per informazioni sull'assegnazione di tag delle chiavi KMS, consulta Chiavi di tagging e ABAC per AWS KMS.

11. Seleziona Next (Successivo).
12. Seleziona i ruoli e gli utenti IAM che possono gestire la chiave KMS.

> **Note**
>
> Questa policy delle chiavi fornisce all'Account AWS il controllo completo di questa chiave KMS. Consente agli amministratori dell'account di utilizzare policy IAM per concedere ad altri principali l'autorizzazione per la gestione della chiave KMS. Per informazioni dettagliate, vedi the section called “Policy delle chiavi predefinita”.
>
> Le best practice di IAM disincentivano l'uso di utenti IAM con credenziali a lungo termine. Quando possibile, utilizza i ruoli IAM che forniscono credenziali temporanee. Per i dettagli, consulta la sezione Best practice di sicurezza in IAM nella Guida per l'utente IAM.

13. (Facoltativo) Per impedire ai ruoli e agli utenti IAM selezionati di eliminare questa chiave KMS, nella sezione Eliminazione chiave nella parte inferiore della pagina, deseleziona la casella di controllo Consenti agli amministratori delle chiavi di eliminare questa chiave.
14. Seleziona Next (Successivo).
15. Selezionare i ruoli e gli utenti IAM che possono utilizzare la chiave nelle operazioni di crittografia.

> **Note**
>
> Questa policy delle chiavi fornisce all'Account AWS il controllo completo di questa chiave KMS. Consente agli amministratori dell'account di utilizzare le policy IAM per fornire ad

altri principali l'autorizzazione per utilizzare la chiave KMS nelle operazioni di crittografia. Per informazioni dettagliate, vedi the section called “Policy delle chiavi predefinita”.

Le best practice di IAM disincentivano l'uso di utenti IAM con credenziali a lungo termine. Quando possibile, utilizza i ruoli IAM che forniscono credenziali temporanee. Per i dettagli, consulta la sezione Best practice di sicurezza in IAM nella Guida per l'utente IAM.

16. (Facoltativo) È possibile consentire ad altri Account AWS di utilizzare questa chiave KMS per operazioni di crittografia. A questo proposito, nella sezione Altri Account AWS, nella parte inferiore della pagina, scegli Aggiungi un altro Account AWS e inserisci il numero di identificazione Account AWS di un account esterno. Per aggiungere più account esterni, ripetere questo passaggio.

> **Note**
>
> Per consentire ai principali negli account esterni di utilizzare la chiave KMS, gli amministratori dell'account esterno devono creare policy IAM che forniscono tali autorizzazioni. Per ulteriori informazioni, consultare Autorizzazione per gli utenti in altri account di utilizzare una chiave KMS.

17. Seleziona Next (Successivo).
18. Esaminare le principali impostazioni scelte. È comunque possibile tornare indietro e modificare tutte le impostazioni.
19. Scegli Termina per creare la chiave KMS.

Creazione di chiavi KMS di crittografia simmetrica (API AWS KMS)

È possibile utilizzare l'CreateKeyoperazione per creare AWS KMS keys di tutti i tipi. Questi esempi utilizzano la AWS Command Line Interface (AWS CLI), ma puoi usare anche qualsiasi linguaggio di programmazione supportato.

> **Important**
>
> Non includere informazioni riservate o sensibili nei campi `Description` o `Tags`. Questi campi possono apparire in testo semplice nei CloudTrail log e in altri output.

La seguente operazione crea la chiave KMS più comunemente utilizzata, una chiave di crittografia simmetrica in un'unica regione supportata dal materiale chiave generato da AWS KMS. Questa operazione non include parametri obbligatori. È possibile anche utilizzare il parametro `Policy` per specificare una policy delle chiavi. È possibile modificare la policy chiave (PutKeyPolicy) e aggiungere elementi opzionali, come una descrizione e tag, in qualsiasi momento. È inoltre possibile anche creare chiavi asimmetriche, chiavi multi-regione, chiavi con materiale chiave importato e chiavi in archivi delle chiavi personalizzate.

L'`CreateKey`operazione non consente di specificare un alias, ma è possibile utilizzare l'CreateAliasoperazione per creare un alias per la nuova chiave KMS.

Di seguito è riportato un esempio di una chiamata all'operazione `CreateKey` senza parametri. Questo comando utilizza tutti i valori predefiniti. Crea una chiave KMS di crittografia simmetrica per crittografare e decrittografare con materiale della chiave generato da AWS KMS.

```
$ aws kms create-key
{
    "KeyMetadata": {
        "Origin": "AWS_KMS",
        "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "Description": "",
        "KeyManager": "CUSTOMER",
        "Enabled": true,
        "KeySpec": "SYMMETRIC_DEFAULT",
        "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "KeyState": "Enabled",
        "CreationDate": 1502910355.475,
        "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "AWSAccountId": "111122223333",
        "MultiRegion": false
        "EncryptionAlgorithms": [
            "SYMMETRIC_DEFAULT"
        ],
    }
}
```

Se non specifichi una policy delle chiavi per la nuova chiave KMS, la policy delle chiavi predefinita che `CreateKey` applica è diversa dalla policy delle chiavi predefinita che la console applica quando la utilizzi per creare una nuova chiave KMS.

Ad esempio, questa chiamata all'GetKeyPolicyoperazione restituisce la politica chiave applicabile. `CreateKey` Dà all'Account AWS l'accesso alla chiave KMS e consente di creare policy AWS Identity and Access Management (IAM) per la chiave KMS. Per informazioni dettagliate sulle policy IAM e sulle policy delle chiavi KMS, consulta Autenticazione e controllo degli accessi per AWS KMS.

```
$ aws kms get-key-policy --key-id 1234abcd-12ab-34cd-56ef-1234567890ab --policy-name
 default --output text
{
  "Version" : "2012-10-17",
  "Id" : "key-default-1",
  "Statement" : [ {
    "Sid" : "Enable IAM User Permissions",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "arn:aws:iam::111122223333:root"
    },
    "Action" : "kms:*",
    "Resource" : "*"
  } ]
}
```

Utilizzo di alias

Un alias è un nome descrittivo per una AWS KMS key. Ad esempio, un alias ti consente di fare riferimento a una chiave KMS come `test-key` invece di `1234abcd-12ab-34cd-56ef-1234567890ab`.

È possibile utilizzare un alias per identificare una chiave KMS nella AWS KMS console, nell'DescribeKeyoperazione e nelle operazioni crittografiche, come Encrypt e. GenerateDataKey Gli alias semplificano anche il riconoscimento delle Chiave gestita da AWS. Gli alias per queste chiavi KMS hanno sempre il formato `aws/<service-name>`. Ad esempio, l'alias per la Chiave gestita da AWS per Amazon DynamoDB è `aws/dynamodb`. Puoi stabilire gli standard per alias simili dei progetti, ad esempio anteporre agli alias il nome di un progetto o di una categoria.

Puoi inoltre consentire e negare l'accesso alle chiavi KMS in base ai relativi alias senza modificare le policy o gestire le concessioni. Questa funzione fa parte del supporto AWS KMS per il controllo degli accessi basati su attributi (ABAC). Per informazioni dettagliate, vedi Utilizzo degli alias per controllare l'accesso alle chiavi KMS.

Gran parte del potere degli alias deriva dalla tua capacità di modificare la chiave KMS associata a un alias in qualsiasi momento. Gli alias possono rendere il tuo codice più facile da scrivere e gestire. Supponi, ad esempio, di utilizzare un alias per fare riferimento a una chiave KMS particolare e di voler modificare la chiave KMS. In tal caso, basta associare l'alias a un'altra chiave KMS. Non è necessario cambiare il codice.

Gli alias semplificano anche il riutilizzo dello stesso codice in diverse Regioni AWS. Crea alias con lo stesso nome in più regioni e associa ogni alias a una chiave KMS nella sua regione. Quando il codice viene eseguito in ogni regione, l'alias fa riferimento alla relativa chiave KMS associata in quella regione. Per vedere un esempio, consulta Utilizzo di alias nelle applicazioni.

È possibile creare un alias per una chiave KMS nella AWS KMS console, utilizzando l'CreateAliasAPI o utilizzando un modello. AWS CloudFormation

L'API AWS KMS fornisce il controllo completo degli alias in ogni account e regione. L'API include operazioni per creare un alias (CreateAlias), visualizzare nomi di alias e alias ARN (ListAliases), modificare la chiave KMS associata a un alias () ed eliminare un alias (UpdateAlias). DeleteAlias Per esempi di gestione degli alias più linguaggi di programmazione, consulta the section called “Utilizzo degli alias”.

Le seguenti risorse possono rivelarsi utili:

- Per informazioni sugli identificatori di chiave KMS, inclusi gli alias, consulta Identificatori chiave () KeyId.
- Per informazioni sull'utilizzo di un AWS CloudFormation modello per creare un alias per una chiave KMS, consulta la Guida per l'utente. AWS::KMS::AliasAWS CloudFormation
- Per informazioni sulla ricerca degli alias associati a una chiave KMS, consulta Individuazione del nome e dell'ARN dell'alias
- Per informazioni sulle quote di risorse per gli alias e sulle quote tariffarie per le operazioni API correlate agli alias, consulta Quote.
- Per esempi di creazione e gestione di alias in più linguaggi di programmazione, consulta Utilizzo degli alias.

Argomenti

- Informazioni sugli alias
- Gestione degli alias
- Utilizzo di alias nelle applicazioni

- Controllo dell'accesso agli alias
- Utilizzo degli alias per controllare l'accesso alle chiavi KMS
- Ricerca di alias nei log AWS CloudTrail

Informazioni sugli alias

Scopri come gli alias funzionano in AWS KMS.

Un alias è una risorsa AWS indipendente

Un alias non è una proprietà di una chiave KMS. Le operazioni eseguite sull'alias non influiscono sulla relativa chiave KMS associata. Puoi creare un alias per una chiave KMS e quindi aggiornare l'alias in modo che venga associato a un'altra chiave KMS. È anche possibile eliminare l'alias senza alcun effetto sulla chiave KMS associata. Tuttavia, se si elimina una chiave KMS, vengono eliminati tutti gli alias associati a tale chiave KMS.

Se si specifica un alias come risorsa in una policy IAM, la policy fa riferimento all'alias e non alla chiave KMS associata.

Ogni alias ha due formati

Quando crei un alias, specifichi il nome alias. AWS KMS crea l'alias ARN per te.

- Un ARN di alias è un Amazon Resource Name (ARN) che identifica in modo univoco l'alias.

```
# Alias ARN
arn:aws:kms:us-west-2:111122223333:alias/<alias-name>
```

- Il nome alias è unico solo per un account e per una regione. Nell'API AWS KMS, il nome alias è sempre preceduto da `alias/`. Questo prefisso viene omesso nella console AWS KMS.

```
# Alias name
alias/<alias-name>
```

Gli alias non sono segreti

Gli alias possono essere visualizzati in testo semplice nei log e in CloudTrail altri output. Non includere informazioni riservate o sensibili nel nome dell'alias.

Ogni alias è associato a una chiave KMS alla volta

L'alias e la relativa chiave KMS devono trovarsi nello stesso account e nella stessa regione.

Puoi associare un alias a qualsiasi chiave gestita dal cliente nello stesso Account AWS e regione . Tuttavia, non hai l'autorizzazione per associare un alias a una Chiave gestita da AWS.

Ad esempio, questo ListAliasesoutput mostra che l'`test-key`alias è associato esattamente a una chiave KMS di destinazione, rappresentata dalla proprietà. `TargetKeyId`

```
{
     "AliasName": "alias/test-key",
     "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/test-key",
     "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
     "CreationDate": 1593622000.191,
     "LastUpdatedDate": 1593622000.191
}
```

Puoi associare più alias alla stessa chiave KMS

Ad esempio, puoi associare gli alias `test-key` e `project-key` alla stessa chiave KMS.

```
{
     "AliasName": "alias/test-key",
     "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/test-key",
     "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
     "CreationDate": 1593622000.191,
     "LastUpdatedDate": 1593622000.191
},
{
     "AliasName": "alias/project-key",
     "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/project-key",
     "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
     "CreationDate": 1516435200.399,
     "LastUpdatedDate": 1516435200.399
}
```

L'alias deve essere univoco nell'account e nella regione

Ad esempio, è possibile avere un solo alias `test-key` in ogni account e regione. Gli alias rispettano la distinzione tra maiuscole e minuscole, ma gli alias che differiscono solo nella la distinzione tra maiuscole e minuscole sono molto inclini all'errore. Non è possibile modificare un nome alias. Tuttavia, puoi eliminare l'alias e creare un nuovo alias con il nome desiderato.

Puoi creare un alias con lo stesso nome in diverse regioni

Ad esempio, puoi avere un alias `finance-key` negli Stati Uniti orientali (Virginia settentrionale) e un alias `finance-key` in Europa (Francoforte). Ogni alias verrebbe associato a una chiave KMS nella rispettiva regione. Se il tuo codice fa riferimento a un nome alias come `alias/finance-key`, puoi eseguirlo in più regioni. In ogni regione utilizza una diversa chiave KMS. Per informazioni dettagliate, vedi Utilizzo di alias nelle applicazioni.

Puoi modificare la chiave KMS associata a un alias

È possibile utilizzare l'UpdateAliasoperazione per associare un alias a una chiave KMS diversa. Ad esempio, se l'alias `finance-key` è associato alla chiave KMS `1234abcd-12ab-34cd-56ef-1234567890ab` puoi aggiornarlo in modo che sia associato alla chiave KMS `0987dcba-09fe-87dc-65ba-ab0987654321`.

Tuttavia, le chiavi KMS correnti e nuove devono essere dello stesso tipo (entrambe simmetriche, asimmetriche o HMAC) e devono avere lo stesso utilizzo della chiave (ENCRYPT_DECRYPT, SIGN_VERIFY o GENERATE_VERIFY_MAC). Questa restrizione impedisce errori nel codice che utilizza alias. Se è necessario associare un alias a un tipo di chiave diverso e sono stati attenuati i rischi, puoi eliminare e ricreare l'alias.

Alcune chiavi KMS non hanno alias

Quando crei una chiave KMS nella console AWS KMS devi assegnarle un nuovo alias. Ma un alias non è necessario quando si utilizza l'CreateKeyoperazione per creare una chiave KMS. Inoltre, è possibile utilizzare l'UpdateAliasoperazione per modificare la chiave KMS associata a un alias e l'DeleteAliasoperazione per eliminare un alias. Di conseguenza, alcune chiavi KMS potrebbero avere diversi alias e altre potrebbero non averne alcuno.

AWS crea gli alias nell'account

AWS crea gli alias nell'account per Chiavi gestite da AWS. Questi alias hanno i nomi del modulo `alias/aws/<service-name>`, ad esempio `alias/aws/s3`.

Alcuni alias AWS non hanno una chiave KMS. Questi alias predefiniti sono generalmente associati a una Chiave gestita da AWS quando inizi a utilizzare il servizio.

Utilizzare gli alias per identificare le chiavi KMS

È possibile utilizzare un nome alias o un alias ARN per identificare una chiave KMS nelle operazioni crittografiche e. DescribeKeyGetPublicKey (Se l'opzione La chiave KMS è in un Account AWS diverso, è necessario utilizzare il suo ARN della chiave o ARN dell'alias.) Gli alias

non sono identificatori validi per le chiavi KMS in altre operazioni AWS KMS. Per informazioni sugli identificatori di chiave validi per ogni operazione API AWS KMS, consulta le descrizioni dei parametri `KeyId` nella Documentazione di riferimento di API AWS Key Management Service.

Non puoi utilizzare un nome alias o un ARN di alias per identificare una chiave KMS in una policy IAM. Per controllare l'accesso a una chiave KMS in base ai relativi alias, usa le chiavi di condizione kms: o kms:. RequestAlias ResourceAliases Per informazioni dettagliate, vedi ABAC per AWS KMS.

Gestione degli alias

Gli utenti autorizzati possono creare, visualizzare ed eliminare alias. È anche possibile aggiornare un alias, che associa un alias esistente a una chiave KMS diversa.

Argomenti

- Creazione di un alias
- Visualizzazione degli alias
- Aggiornamento degli alias
- Eliminazione di un alias

Creazione di un alias

Puoi creare alias nella console AWS KMS o utilizzando operazioni API AWS KMS.

L'alias deve essere una stringa da 1 a 256 caratteri. Può contenere solo caratteri alfanumerici, barre (/), trattini bassi (_) e trattini (-). Il nome alias per una chiave gestita dal cliente non può iniziare con `alias/aws/`. Il prefisso `alias/aws/` è riservato per Chiave gestita da AWS.

È possibile creare un alias per una nuova chiave KMS o per una chiave KMS esistente. Puoi aggiungere un alias in modo che la chiave KMS venga utilizzata un particolare progetto o applicazione.

Creare un alias (console)

Quando crei una chiave KMS nella console AWS KMS, è necessario creare un alias per la nuova chiave KMS. Per creare un alias per una chiave KMS esistente, utilizzare la scheda Alias nella pagina dei dettagli della chiave KMS.

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente. Non è possibile gestire gli alias per Chiavi gestite da AWS o Chiavi di proprietà di AWS.
4. Nella tabella scegli l'alias o l'ID chiave della chiave KMS. Quindi, nella pagina dei dettagli della chiave KMS, scegliere la scheda Alias.

   Se una chiave KMS dispone di più alias, la colonna Alias nella tabella mostra un alias e un riepilogo degli alias, ad esempio (+n più). Scegliendo il riepilogo alias puoi accedere direttamente alla scheda Alias nella pagina dei dettagli della chiave KMS.
5. Nella scheda Alias, scegli Crea alias. Immetti un nome alias e scegli Crea alias.

> **Important**
>
> Non includere informazioni riservate o sensibili in questo campo. Questo campo può essere visualizzato in testo semplice nei log e in altri output. CloudTrail

> **Note**
>
> Non aggiungere il prefisso `alias/`. La console lo aggiunge automaticamente. Se inserisci `alias/ExampleAlias`, il nome alias effettivo sarà `alias/alias/ExampleAlias`.

Creare un alias (API AWS KMS)

Per creare un alias, usa l'operazione. CreateAlias A differenza del processo di creazione delle chiavi KMS nella console, l'CreateKeyoperazione non crea un alias per una nuova chiave KMS.

> **Important**
>
> Non includere informazioni riservate o sensibili in questo campo. Questo campo può essere visualizzato in testo semplice nei log e in CloudTrail altri output.

Puoi utilizzare l'operazione `CreateAlias` per creare un alias per una nuova chiave KMS senza alias. Puoi inoltre utilizzare l'operazione `CreateAlias` per aggiungere un alias a qualsiasi chiave KMS esistente o per ricreare un alias eliminato accidentalmente.

Nelle operazioni API AWS KMS, il nome alias deve iniziare con `alias/` seguito da un nome, ad esempio `alias/ExampleAlias`. L'alias deve essere univoco nell'account e nella regione. Per trovare gli alias già in uso, usa l'operazione. ListAliases Il nome alias fa distinzione tra maiuscole e minuscole.

Il `TargetKeyId` può essere qualsiasi chiave gestita dal cliente nella stessa Regione AWS. Per identificare la chiave KMS utilizza l'ID chiave o l'ARN di chiave. Non puoi utilizzare un altro alias.

Nell'esempio seguente viene creato l'alias `example-key` e viene associato alla chiave KMS specificata. Questi esempi utilizzano l'AWS Command Line Interface (AWS CLI). Per esempi in più linguaggi di programmazione, consulta Utilizzo degli alias.

```
$ aws kms create-alias \
    --alias-name alias/example-key \
    --target-key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

`CreateAlias` non restituisce alcun output. Per visualizzare il nuovo alias utilizza l'operazione `ListAliases`. Per informazioni dettagliate, vedi Visualizzazione degli alias (API AWS KMS).

Visualizzazione degli alias

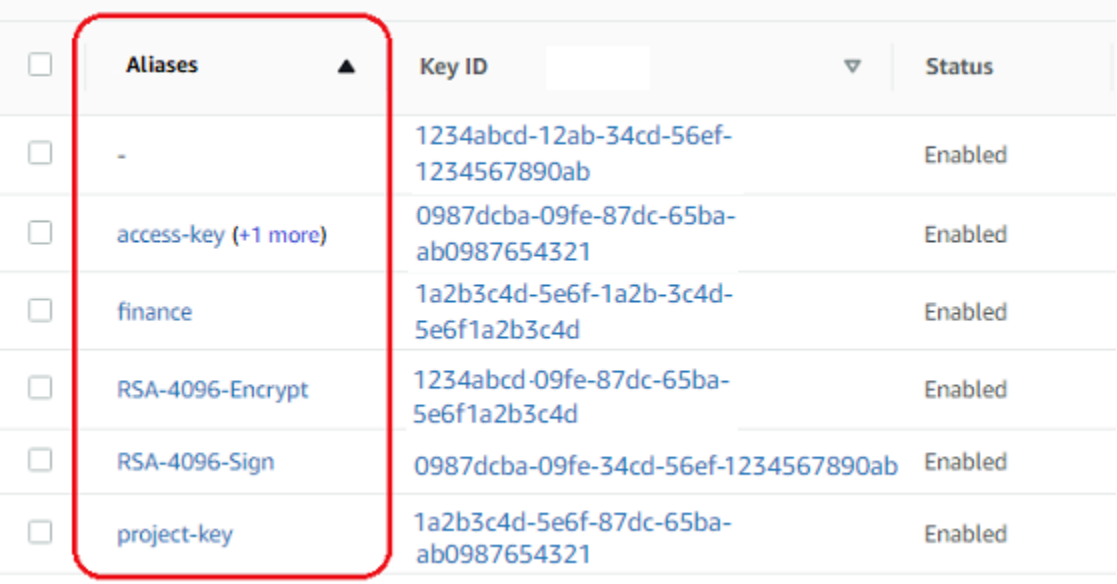
Gli alias semplificano il riconoscimento delle chiavi KMS nella console AWS KMS. È possibile visualizzare gli alias per una chiave KMS nella AWS KMS console o utilizzando l'operazione. ListAliases L'DescribeKeyoperazione, che restituisce le proprietà di una chiave KMS, non include gli alias.

Visualizzazione degli alias (console)

Le pagine delle chiavi gestite dal cliente e delle chiavi gestite da Chiavi gestite da AWS nella console AWS KMS visualizzano l'alias associato a ciascuna chiave KMS. Puoi inoltre cercare, ordinare e filtrare le chiavi KMS in base al relativo alias.

L'immagine seguente della console AWS KMS mostra gli alias nella pagina Customer managed keys (Chiavi gestite dal cliente) di un account di esempio. Come mostrato nell'immagine, alcune chiavi KMS non hanno un alias.

Quando una chiave KMS dispone di più alias, la colonna Alias mostra un alias e un riepilogo degli alias (+n più). Il riepilogo degli alias mostra il numero di alias aggiuntivi associati alla chiave KMS e i collegamenti alla visualizzazione di tutti gli alias per la chiave KMS nella scheda Alias.



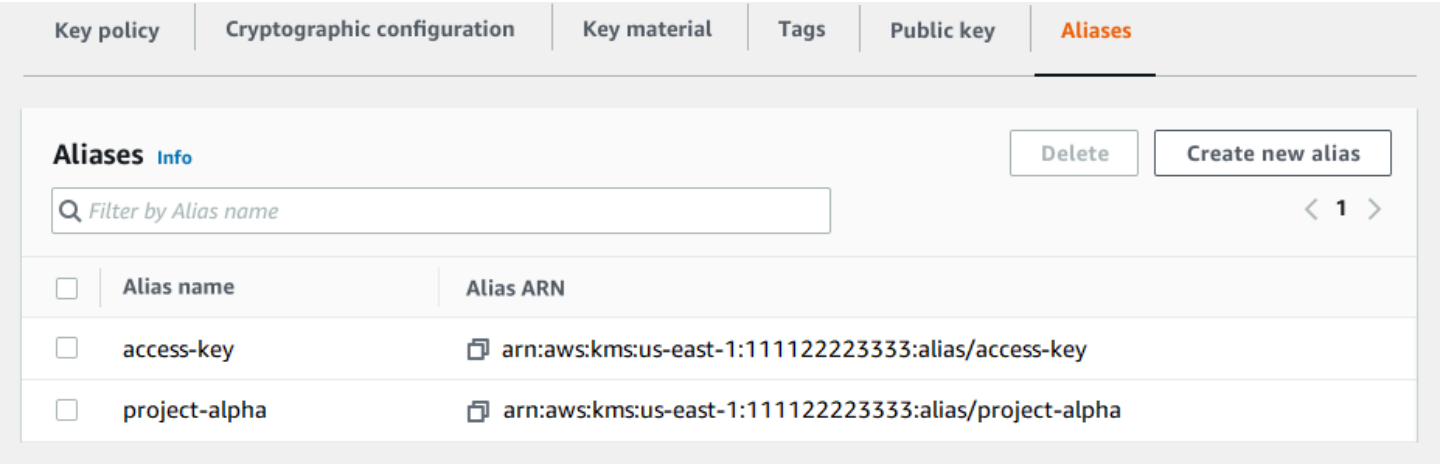
Aliases	Key ID	Status
-	1234abcd-12ab-34cd-56ef-1234567890ab	Enabled
access-key (+1 more)	0987dcba-09fe-87dc-65ba-ab0987654321	Enabled
finance	1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d	Enabled
RSA-4096-Encrypt	1234abcd-09fe-87dc-65ba-5e6f1a2b3c4d	Enabled
RSA-4096-Sign	0987dcba-09fe-34cd-56ef-1234567890ab	Enabled
project-key	1a2b3c4d-5e6f-87dc-65ba-ab0987654321	Enabled

La scheda Alias nella pagina dei dettagli per ogni chiave KMS visualizza il nome alias e l'alias ARN di tutti gli alias per la chiave KMS nel Account AWS e Regione. Puoi anche utilizzare l'opzione Alias per Creare alias e Eliminare alias.

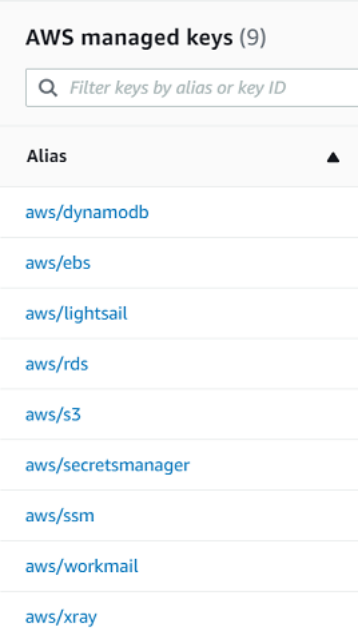
Per individuare il nome e l"ARN dell'alias di tutti gli alias della chiave KMS, utilizzare la scheda Alias.

- Per andare direttamente alla scheda Alias, nella colonna Alias, scegli il riepilogo degli alias (+n più). Un riepilogo degli alias viene mostrato solo se la chiave KMS contiene più di un alias.
- In alternativa, scegliere l'ID chiave o alias della chiave KMS (che apre la pagina dei dettagli della chiave KMS) e scegli la scheda Alias. Le schede si trovano sotto la sezione Configurazione generale.

L'immagine che segue mostra la scheda Alias per una chiave KMS di esempio.



Puoi utilizzare l'alias per riconoscere una Chiave gestita da AWS, come illustrato nella pagina Chiavi gestite da AWS di esempio. Gli alias per le Chiavi gestite da AWS hanno sempre il formato: `aws/<service-name>`. Ad esempio, l'alias per la Chiave gestita da AWS per Amazon DynamoDB è `aws/dynamodb`.



Visualizzazione degli alias (API AWS KMS)

L'ListAliasesoperazione restituisce il nome dell'alias e l'alias ARN degli alias nell'account e nella regione. L'output include gli alias per Chiavi gestite da AWS e per le chiavi gestite dal cliente. Gli alias per Chiavi gestite da AWS hanno il formato `aws/<service-name>`, ad esempio `aws/dynamodb`.

La risposta potrebbe anche includere alias che non hanno alcun campo `TargetKeyId`. Questi sono alias predefiniti che AWS ha creato, ma che non ha ancora associato a una chiave KMS.

```
$ aws kms list-aliases
{
    "Aliases": [
        {
            "AliasName": "alias/access-key",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/access-key",
            "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
            "CreationDate": 1516435200.399,
            "LastUpdatedDate": 1516435200.399
        },
        {
            "AliasName": "alias/ECC-P521-Sign",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/ECC-P521-Sign",
            "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
            "CreationDate": 1693622000.704,
            "LastUpdatedDate": 1693622000.704
        },
        {
            "AliasName": "alias/ImportedKey",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/ImportedKey",
            "TargetKeyId": "1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d",
            "CreationDate": 1493622000.704,
            "LastUpdatedDate": 1521097200.235
        },
        {
            "AliasName": "alias/finance-project",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/finance-project",
            "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
            "CreationDate": 1604958290.014,
            "LastUpdatedDate": 1604958290.014
        },
        {
            "AliasName": "alias/aws/dynamodb",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/aws/dynamodb",
            "TargetKeyId": "0987ab65-43cd-21ef-09ab-87654321cdef",
            "CreationDate": 1521097200.454,
            "LastUpdatedDate": 1521097200.454
        },
        {
            "AliasName": "alias/aws/ebs",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/aws/ebs",
            "TargetKeyId": "abcd1234-09fe-ef90-09fe-ab0987654321",
            "CreationDate": 1466518990.200,
```

```
            "LastUpdatedDate": 1466518990.200
        }
    ]
}
```

Per ottenere tutti gli alias associati a una particolare chiave KMS utilizza il parametro `KeyId` facoltativo dell'operazione `ListAliases`. Il parametro `KeyId` accetta l'ID chiave o l'ARN della chiave della chiave KMS.

In questo esempio vengono restituiti tutti gli alias associati alla chiave KMS `0987dcba-09fe-87dc-65ba-ab0987654321`.

```
$ aws kms list-aliases --key-id 0987dcba-09fe-87dc-65ba-ab0987654321
{
    "Aliases": [
        {
            "AliasName": "alias/access-key",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/access-key",
            "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
            "CreationDate": "2018-01-20T15:23:10.194000-07:00",
            "LastUpdatedDate": "2018-01-20T15:23:10.194000-07:00"
        },
        {
            "AliasName": "alias/finance-project",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/finance-project",
            "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
            "CreationDate": 1604958290.014,
            "LastUpdatedDate": 1604958290.014
        }
    ]
}
```

Il parametro `KeyId` non accetta caratteri jolly, ma puoi utilizzare le caratteristiche del linguaggio di programmazione per filtrare la risposta.

Ad esempio, il comando seguente del comando AWS CLI restituisce solo gli alias per Chiavi gestite da AWS.

```
$ aws kms list-aliases --query 'Aliases[?starts_with(AliasName, `alias/aws/`)]'
```

Il comando seguente ottiene solo l'alias `access-key`. Il nome alias fa distinzione tra maiuscole e minuscole.

```
$ aws kms list-aliases --query 'Aliases[?AliasName==`alias/access-key`]'
[
    {
        "AliasName": "alias/access-key",
        "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/access-key",
        "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
        "CreationDate": "2018-01-20T15:23:10.194000-07:00",
        "LastUpdatedDate": "2018-01-20T15:23:10.194000-07:00"
    }
]
```

Aggiornamento degli alias

Poiché un alias è una risorsa indipendente, puoi modificare la chiave KMS associata a un alias. Ad esempio, se l'`test-key`alias è associato a una chiave KMS, è possibile utilizzare l'UpdateAliasoperazione per associarlo a una chiave KMS diversa. Questo è uno dei diversi modi per ruotare manualmente una chiave KMS senza modificare il materiale della chiave. È inoltre possibile aggiornare una chiave KMS in modo che un'applicazione che utilizzava una chiave KMS per nuove risorse utilizzi ora una diversa.

Non puoi aggiornare un alias nella console AWS KMS. Inoltre, non puoi utilizzare `UpdateAlias` (o qualsiasi altra operazione) per modificare un nome di alias. Per modificare un nome di alias, elimina l'attuale alias e quindi crea un nuovo alias per la chiave KMS.

Quando aggiorni un alias, la chiave KMS corrente e la nuova chiave KMS devono essere dello stesso tipo (entrambe simmetriche, asimmetriche o HMAC). Devono anche avere lo stesso utilizzo della chiave (`ENCRYPT_DECRYPT` o `SIGN_VERIFY` o GENERATE_VERIFY_MAC). Questa restrizione impedisce errori di crittografia nel codice che utilizza alias.

L'esempio seguente inizia utilizzando l'ListAliasesoperazione per mostrare che l'`test-key`alias è attualmente associato alla chiave KMS. `1234abcd-12ab-34cd-56ef-1234567890ab`

```
$ aws kms list-aliases --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
{
    "Aliases": [
        {
            "AliasName": "alias/test-key",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/test-key",
            "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
            "CreationDate": 1593622000.191,
            "LastUpdatedDate": 1593622000.191
```

```
        }
    ]
}
```

Successivamente, utilizza l'operazione `UpdateAlias` per modificare la chiave KMS associata con l'alias `test-key` alla chiave KMS `0987dcba-09fe-87dc-65ba-ab0987654321`. Non è necessario specificare la chiave KMS attualmente associata, ma solo la nuova chiave KMS ("di destinazione"). Il nome alias fa distinzione tra maiuscole e minuscole.

```
$ aws kms update-alias --alias-name 'alias/test-key' --target-key-id
 0987dcba-09fe-87dc-65ba-ab0987654321
```

Per verificare che l'alias sia ora associato alla chiave KMS di destinazione, utilizza nuovamente l'operazione `ListAliases`. Questo comando AWS CLI utilizza il parametro `--query` per ottenere solo l'alias `test-key`. I campi `TargetKeyId` e `LastUpdatedDate` vengono aggiornati.

```
$ aws kms list-aliases --query 'Aliases[?AliasName==`alias/test-key`]'
[
    {
        "AliasName": "alias/test-key",
        "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/test-key",
        "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
        "CreationDate": 1593622000.191,
        "LastUpdatedDate": 1604958290.154
    }
]
```

Eliminazione di un alias

È possibile eliminare un alias nella AWS KMS console o utilizzando l'operazione. DeleteAlias Prima di eliminare un alias, assicurati che non sia in uso. Sebbene l'eliminazione di un alias non influisca sulla chiave KMS associata, potrebbe creare problemi per qualsiasi applicazione che lo utilizza. Se elimini un alias per errore, puoi creare un nuovo alias con lo stesso nome e associarlo alla stessa o a un'altra chiave KMS.

Se si elimina una chiave KMS, vengono eliminati tutti gli alias associati a tale chiave KMS.

Eliminazione degli alias (console)

Per eliminare un alias nella console AWS KMS utilizza la scheda Alias nella pagina dei dettagli della chiave KMS. È possibile eliminare più alias per una chiave KMS contemporaneamente.

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente. Non è possibile gestire gli alias per Chiavi gestite da AWS o Chiavi di proprietà di AWS.
4. Nella tabella scegli l'alias o l'ID chiave della chiave KMS. Quindi, nella pagina dei dettagli della chiave KMS, scegliere la scheda Alias.

   Se una chiave KMS dispone di più alias, la colonna Alias nella tabella mostra un alias e un riepilogo degli alias, ad esempio (+n più). Scegliendo il riepilogo alias puoi accedere direttamente alla scheda Alias nella pagina dei dettagli della chiave KMS.
5. Sulla scheda Alias seleziona la casella di controllo accanto agli alias che si desidera eliminare. Scegli Elimina.

Elimina un alias (API AWS KMS)

Per eliminare un alias, utilizzare l'DeleteAliasoperazione. Questa operazione elimina un alias alla volta. Il nome alias fa distinzione tra maiuscole e minuscole e deve essere preceduto dal prefisso `alias/`.

Ad esempio, il comando seguente elimina l'alias `test-key`. Questo comando non restituisce alcun output.

```
$ aws kms delete-alias --alias-name alias/test-key
```

Per verificare che l'alias venga eliminato, utilizzare l'ListAliasesoperazione. Il comando seguente utilizza il parametro `--query` nel AWS CLI per ottenere solo l'alias `test-key`. Le parentesi vuote nella risposta indicano che la risposta di `ListAliases` non include un alias `test-key`. Per eliminare le parentesi, utilizza il parametro `--output text` e il valore.

```
$ aws kms list-aliases --query 'Aliases[?AliasName==`alias/test-key`]'
[]
```

Utilizzo di alias nelle applicazioni

Puoi utilizzare un alias per rappresentare una chiave KMS nel codice dell'applicazione. Il `KeyId` parametro nelle operazioni AWS KMS crittografiche e GetPublicKeyaccetta un nome alias o un alias ARN. DescribeKey

Ad esempio, il comando `GenerateDataKey` seguente utilizza un nome alias (`alias/finance`) per identificare una chiave KMS. Il nome alias è il valore del parametro `KeyId`.

```
$ aws kms generate-data-key --key-id alias/finance --key-spec AES_256
```

Se la chiave KMS è in un altro Account AWS, è necessario utilizzare una ARN di chiave o ARN di alias in queste operazioni. Quando si utilizza un alias ARN, tenere presente che l'alias per una chiave KMS è definito nell'account proprietario della chiave KMS e potrebbe differire in ogni regione. Per informazioni sulla ricerca dell'ARN alias, consulta Individuazione del nome e dell'ARN dell'alias.

Ad esempio, il seguente comando `GenerateDataKey` utilizza una chiave KMS che non è presente nell'account del chiamante. L'alias `ExampleAlias` è associato alla chiave KMS nell'account e nella regione specificati.

```
$ aws kms generate-data-key --key-id arn:aws:kms:us-west-2:444455556666:alias/
ExampleAlias --key-spec AES_256
```

Uno degli usi più efficaci degli alias è nelle applicazioni eseguite in più Regioni AWS. Ad esempio, puoi avere un'applicazione globale che utilizza una chiave KMS asimmetrica RSA per la firma e la verifica.

- Nella regione Stati Uniti occidentali (Oregon) (us-west-2) vuoi utilizzare `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.
- In Europa (Francoforte) (eu-central-1), vuoi utilizzare `arn:aws:kms:eu-central-1:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321`
- Nella regione Asia Pacifico (Singapore) (ap-southeast-1), vuoi utilizzare `arn:aws:kms:ap-southeast-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d`.

Puoi creare una versione diversa dell'applicazione in ogni regione o utilizzare un dizionario o un'istruzione switch per selezionare la chiave KMS corretta per ogni regione. Tuttavia è molto più semplice creare un alias con lo stesso nome alias in ogni regione. Tieni presente che il nome alias rispetta la distinzione tra maiuscole e minuscole.

```
aws --region us-west-2 kms create-alias \
    --alias-name alias/new-app \
    --key-id arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

aws --region eu-central-1 kms create-alias \
    --alias-name alias/new-app \
    --key-id arn:aws:kms:eu-central-1:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321

aws --region ap-southeast-1 kms create-alias \
    --alias-name alias/new-app \
    --key-id arn:aws:kms:ap-
southeast-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d
```

Quindi, utilizza l'alias nel codice. Quando il codice viene eseguito in ogni regione, l'alias farà riferimento alla relativa chiave KMS associata in quella regione. Ad esempio, questo codice chiama l'operazione Sign con un nome alias.

```
aws kms sign --key-id alias/new-app \
    --message $message \
    --message-type RAW \
    --signing-algorithm RSASSA_PSS_SHA_384
```

Tuttavia, esiste il rischio che l'alias possa essere eliminato o aggiornato per essere associato a un'altra chiave KMS. In tal caso, i tentativi dell'applicazione di verificare le firme utilizzando il nome alias avranno esito negativo e potrebbe essere necessario ricreare o aggiornare l'alias.

Per ridurre questo rischio, presta attenzione a concedere ai principali l'autorizzazione a gestire gli alias utilizzati nell'applicazione. Per informazioni dettagliate, vedi Controllo dell'accesso agli alias.

Esistono diverse altre soluzioni per le applicazioni che crittografano i dati in più regioni Regioni AWS, tra cui AWS Encryption SDK.

Controllo dell'accesso agli alias

Quando crei o modifichi un alias, l'operazione interessa l'alias e la relativa chiave KMS associata. Di conseguenza, i principali che gestiscono gli alias devono disporre dell'autorizzazione per chiamare l'operazione alias sull'alias e su tutte le chiavi KMS interessate. Puoi fornire queste autorizzazioni utilizzando le policy delle chiavi, le policy IAM e le concessioni.

> **Note**
>
> Presta attenzione quando concedi ai principali l'autorizzazione per gestire tag e alias. Modificando un tag o un alias puoi consentire o negare l'autorizzazione alla chiave gestita dal cliente. Per informazioni dettagliate, consulta ABAC per AWS KMS e Utilizzo degli alias per controllare l'accesso alle chiavi KMS.

Per informazioni sul controllo dell'accesso a tutte le operazioni AWS KMS, consulta Riferimento per le autorizzazioni.

Le autorizzazioni per la creazione e la gestione degli alias funzionano come descritto di seguito.

km: CreateAlias

Per creare un alias, il principale richiede le seguenti autorizzazioni sia per l'alias che per la chiave KMS associata.

- `kms:CreateAlias` per l'alias. Fornisci questa autorizzazione in una policy IAM collegata al principale autorizzato a creare l'alias.

  L'esempio di istruzione di policy seguente specifica un alias particolare in un elemento `Resource`. Ma è possibile elencare più ARN alias o specificare un modello di alias, ad esempio "test*". Puoi specificare il valore `Resource` di `"*"` in modo da consentire al principale di creare qualsiasi alias nell'account e nella regione. L'autorizzazione per creare un alias può anche essere inclusa in un'autorizzazione `kms:Create*` per tutte le risorse di un account e di una regione.

  ```
  {
    "Sid": "IAMPolicyForAnAlias",
    "Effect": "Allow",
    "Action": [
      "kms:CreateAlias",
      "kms:UpdateAlias",
      "kms:DeleteAlias"
    ],
    "Resource": "arn:aws:kms:us-west-2:111122223333:alias/test-key"
  }
  ```

- `kms:CreateAlias` per la chiave KMS. Questa autorizzazione deve essere fornita in una policy delle chiavi o in una policy IAM delegata dalla policy delle chiavi.

```
{
  "Sid": "Key policy for 1234abcd-12ab-34cd-56ef-1234567890ab",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:user/KMSAdminUser"},
  "Action": [
    "kms:CreateAlias",
    "kms:DescribeKey"
  ],
  "Resource": "*"
}
```

È possibile utilizzare le chiavi di condizione per limitare le chiavi KMS che è possibile associare a un alias. Ad esempio, puoi usare la chiave kms: KeySpec condition per consentire al principale di creare alias solo su chiavi KMS asimmetriche. Per un elenco completo delle chiavi delle condizioni utilizzabili per limitare l'autorizzazione `kms:CreateAlias` sulle risorse delle chiavi KMS, vedi AWS KMS autorizzazioni.

km: ListAliases

Per elencare gli alias nell'account e nella regione, il principale deve disporre dell'autorizzazione `kms:ListAliases` in una policy IAM. Poiché questa policy non è correlata a una determinata chiave KMS o a una risorsa alias, il valore dell'elemento risorsa nella policy deve essere `"*"`.

Ad esempio, l'istruzione della policy IAM riportata di seguito consente al principale di elencare tutte le chiavi KMS e gli alias nell'account e nella regione.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:ListKeys",
      "kms:ListAliases"
    ],
    "Resource": "*"
  }
}
```

km: UpdateAlias

Per modificare la chiave KMS associata a un alias, il principale richiede tre elementi di autorizzazione: uno per l'alias, uno per la chiave KMS attuale e uno per la nuova chiave KMS.

Ad esempio, supponi di voler modificare l'alias `test-key` dalla chiave KMS con ID chiave 1234abcd-12ab-34cd-56ef-1234567890ab alla chiave KMS con ID chiave 0987dcba-09fe-87dc-65ba-ab0987654321. Per questo caso, includi le istruzioni di policy simile agli esempi riportati in questa sezione.

- `kms:UpdateAlias` per l'alias. Questa autorizzazione viene fornita in una policy IAM collegata al principale. La policy IAM seguente specifica un alias particolare. Ma è possibile elencare più ARN alias o specificare un modello di alias, ad esempio `"test*"`. Puoi specificare il valore `Resource` di `"*"` in modo da consentire al principale di creare qualsiasi alias nell'account e nella regione.

```
{
  "Sid": "IAMPolicyForAnAlias",
  "Effect": "Allow",
  "Action": [
    "kms:UpdateAlias",
    "kms:ListAliases",
    "kms:ListKeys"
  ],
  "Resource": "arn:aws:kms:us-west-2:111122223333:alias/test-key"
}
```

- `kms:UpdateAlias` per la chiave KMS che è attualmente associata all'alias. Questa autorizzazione deve essere fornita in una policy delle chiavi o in una policy IAM delegata dalla policy delle chiavi.

```
{
  "Sid": "Key policy for 1234abcd-12ab-34cd-56ef-1234567890ab",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:user/KMSAdminUser"},
  "Action": [
    "kms:UpdateAlias",
    "kms:DescribeKey"
  ],
  "Resource": "*"
}
```

- `kms:UpdateAlias` per la chiave KMS che l'operazione associa all'alias. Questa autorizzazione deve essere fornita in una policy delle chiavi o in una policy IAM delegata dalla policy delle chiavi.

```
{
  "Sid": "Key policy for 0987dcba-09fe-87dc-65ba-ab0987654321",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:user/KMSAdminUser"},
  "Action": [
    "kms:UpdateAlias",
    "kms:DescribeKey"
  ],
  "Resource": "*"
}
```

È possibile utilizzare chiavi di condizione per limitare una o entrambe le chiavi KMS in una operazione `UpdateAlias`. Ad esempio, puoi utilizzare una chiave kms: ResourceAliases condition per consentire al principale di aggiornare gli alias solo quando la chiave KMS di destinazione ha già un alias particolare. Per un elenco completo delle chiavi delle condizioni utilizzabili per limitare l'autorizzazione `kms:UpdateAlias` su una risorsa della chiave KMS, vedi AWS KMS autorizzazioni.

km: DeleteAlias

Per eliminare un alias, il principale richiede l'autorizzazione per l'alias e per la chiave KMS associata.

Come sempre, è necessario prestare attenzione quando si concedono le autorizzazioni per eliminare una risorsa. L'eliminazione di un alias non ha alcun effetto sulla chiave KMS associata. Anche se potrebbe causare errori nelle applicazioni che utilizzano l'alias, se si elimina erroneamente un alias, puoi ricrearlo.

- `kms:DeleteAlias` per l'alias. Fornisci questa autorizzazione in una policy IAM collegata al principale autorizzato a eliminare l'alias.

  L'esempio di istruzione di policy seguente specifica l'alias in un elemento `Resource`. Ma è possibile elencare più ARN alias o specificare un modello di alias, ad esempio `"test*"`, Puoi anche specificare un valore `Resource` di `"*"` per consentire al principale di eliminare qualsiasi alias nell'account e nella regione.

```
{
  "Sid": "IAMPolicyForAnAlias",
  "Effect": "Allow",
```

```
  "Action": [
    "kms:CreateAlias",
    "kms:UpdateAlias",
    "kms:DeleteAlias"
  ],
  "Resource": "arn:aws:kms:us-west-2:111122223333:alias/test-key"
}
```

- `kms:DeleteAlias` per la chiave KMS associata. Questa autorizzazione deve essere fornita in una policy delle chiavi o in una policy IAM delegata dalla policy delle chiavi.

```
{
  "Sid": "Key policy for 1234abcd-12ab-34cd-56ef-1234567890ab",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/KMSAdminUser"
  },
  "Action": [
    "kms:CreateAlias",
    "kms:UpdateAlias",
    "kms:DeleteAlias",
    "kms:DescribeKey"
  ],
  "Resource": "*"
}
```

Limitazione delle autorizzazioni alias

È possibile utilizzare le chiavi di condizione per limitare le autorizzazioni alias quando la risorsa è una chiave KMS. Ad esempio, la seguente policy IAM consente le operazioni alias sulle chiavi KMS in un determinato account e nella regione. Tuttavia, utilizza la chiave kms: KeyOrigin condition per limitare ulteriormente le autorizzazioni alle chiavi KMS con materiale chiave proveniente da. AWS KMS

Per un elenco completo delle chiavi di condizioni che è possibile utilizzare per limitare l'autorizzazione alias per una risorsa della chiave KMS, vedi AWS KMS autorizzazioni.

```
{
  "Sid": "IAMPolicyKeyPermissions",
  "Effect": "Allow",
  "Resource": "arn:aws:kms:us-west-2:111122223333:key/*",
  "Action": [
```

```
    "kms:CreateAlias",
    "kms:UpdateAlias",
    "kms:DeleteAlias"
  ],
  "Condition": {
    "StringEquals": {
      "kms:KeyOrigin": "AWS_KMS"
    }
  }
}
```

Non è possibile utilizzare le chiavi di condizione in un'istruzione della policy delle chiavi in cui la risorsa è un alias. Per limitare gli alias che un principale può gestire, utilizzare il valore dell'elemento `Resource` dell'istruzione della policy IAM che controlla l'accesso all'alias. Ad esempio, le istruzioni di policy seguenti consentono al principale di creare, aggiornare o eliminare qualsiasi alias nel Account AWS e Regione a meno che l'alias non inizi con `Restricted`.

```
{
  "Sid": "IAMPolicyForAnAliasAllow",
  "Effect": "Allow",
  "Action": [
    "kms:CreateAlias",
    "kms:UpdateAlias",
    "kms:DeleteAlias"
  ],
  "Resource": "arn:aws:kms:us-west-2:111122223333:alias/*"
},
{
  "Sid": "IAMPolicyForAnAliasDeny",
  "Effect": "Deny",
  "Action": [
    "kms:CreateAlias",
    "kms:UpdateAlias",
    "kms:DeleteAlias"
  ],
  "Resource": "arn:aws:kms:us-west-2:111122223333:alias/Restricted*"
}
```

Utilizzo degli alias per controllare l'accesso alle chiavi KMS

È possibile controllare l'accesso alle chiavi KMS in base agli alias associati alla chiave KMS. Per farlo, usa i tasti kms: RequestAlias e kms: condition. ResourceAliases Questa funzione fa parte del supporto AWS KMS per il controllo degli accessi basati su attributi (ABAC).

La chiave di condizione `kms:RequestAlias` consente o nega l'accesso a una chiave KMS in base all'alias in una richiesta. La chiave di condizione `kms:ResourceAliases` consente o nega l'accesso a una chiave KMS in base agli alias associati alla chiave KMS.

Queste funzionalità non consentono di identificare una chiave KMS utilizzando un alias nell'elemento `resource` di un'istruzione di policy. Quando un alias è il valore di un elemento `resource`, la policy si applica alla risorsa alias e non a qualsiasi chiave KMS che potrebbe essere associata.

> **Note**
>
> È possibile che occorrano fino a cinque minuti affinché le modifiche a tag e alias diventano effettive per l'autorizzazione delle chiavi KMS. Le modifiche recenti potrebbero essere visibili nelle operazioni API prima che influiscano sull'autorizzazione.

Quando si utilizzano alias per controllare l'accesso alle chiavi KMS, considerare quanto segue:

- Utilizzare gli alias per rafforzare la best practice dell'accesso con privilegio minimo. Assegna ai principali IAM solo le autorizzazioni necessarie solo per quelle chiavi KMS che devono utilizzare o gestire. Ad esempio, utilizzare gli alias per identificare le chiavi KMS utilizzate per un progetto. Quindi concedere al team di progetto l'autorizzazione a utilizzare solo le chiavi KMS con gli alias del progetto.
- Fai attenzione a concedere ai principali le autorizzazioni `kms:CreateAlias`, `kms:UpdateAlias`, oppure`kms:DeleteAlias` che consentono di aggiungere, modificare ed eliminare alias. Quando si utilizzano gli alias per controllare l'accesso alle chiavi KMS, la modifica di un alias può concedere alle entità l'autorizzazione di utilizzare chiavi KMS che altrimenti non disponevano dell'autorizzazione per utilizzare. Può inoltre negare l'accesso alle chiavi KMS richieste da altre entità principali per svolgere il proprio lavoro.
- Esamina i principali nel tuo Account AWS che attualmente dispongono dell'autorizzazione per gestire gli alias e modificare le autorizzazioni, se necessario. Gli amministratori delle chiavi che non dispongono dell'autorizzazione per modificare le policy delle chiavi o creare concessioni possono controllare l'accesso alle chiavi KMS se dispongono dell'autorizzazione per gestire gli alias.

Ad esempio, la console policy delle chiavi predefinita per amministratori delle chiavi include le autorizzazioni `kms:CreateAlias`, `kms:DeleteAlias`, e `kms:UpdateAlias`. Le policy IAM potrebbero concedere autorizzazioni alias per tutte le chiavi KMS nel Account AWS. Ad esempio, la policy AWSKeyManagementServicePowerUsergestita consente ai responsabili di creare, eliminare ed elencare alias per tutte le chiavi KMS ma non di aggiornarle.

- Prima di impostare una policy che dipende da un alias, esaminare gli alias nelle chiavi KMS nel Account AWS. Assicurati che la policy sia valida solo per gli alias che intendi includere. Usa CloudTrail i registri e gli CloudWatch allarmi per avvisarti delle modifiche agli alias che potrebbero influire sull'accesso alle tue chiavi KMS. Inoltre, la ListAliasesrisposta include la data di creazione e la data dell'ultimo aggiornamento per ogni alias.
- Le condizioni della policy degli alias utilizzano la corrispondenza dei pattern; non sono legate a una particolare istanza di un alias. Una policy che utilizza chiavi di condizione basate su alias influisce su tutti gli alias nuovi ed esistenti che corrispondono al modello. Se si elimina e si ricrea un alias che corrisponde a una condizione di policy, la condizione si applica al nuovo alias, esattamente come quello precedente.

La chiave di condizione `kms:RequestAlias` si basa sull'alias specificato esplicitamente in una richiesta di operazione. La chiave di condizione `kms:ResourceAliases` dipende dagli alias associati a una chiave KMS, anche se non vengono visualizzati nella richiesta.

km: RequestAlias

Consentire o negare l'accesso a una chiave KMS in base all'alias che identifichi la chiave KMS in una richiesta. Puoi utilizzare la chiave kms: RequestAlias condition in una policy chiave o in una policy IAM. Si applica alle operazioni che utilizzano un alias per identificare una chiave KMS in una richiesta, vale a dire le operazioni crittografiche, e. DescribeKeyGetPublicKey Non è valido per le operazioni di alias, come o. CreateAliasDeleteAlias

Nella chiave condizione, specificare un Nome alias o modello di nome alias. Non puoi specificare un ARN di alias.

Ad esempio, la seguente istruzione della policy delle chiavi consente al principale di utilizzare nella chiave KMS le operazioni specificate. L'autorizzazione diventa effettiva solo quando la richiesta utilizza un alias che include `alpha` per identificare la chiave KMS.

```
{
```

```
  "Sid": "Key policy using a request alias condition",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/alpha-developer"
  },
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:RequestAlias": "alias/*alpha*"
    }
  }
}
```

La seguente richiesta di esempio da un principale autorizzato soddisferebbe la condizione. Tuttavia, una richiesta che ha utilizzato un ID chiave, un ARN della chiave o un alias diverso non soddisferebbe la condizione, anche se questi valori identificavano la stessa chiave KMS.

```
$ aws kms describe-key --key-id "arn:aws:kms:us-west-2:111122223333:alias/project-
alpha"
```

km: ResourceAliases

Consentire o negare l'accesso a una chiave KMS in base agli alias associati alla chiave KMS, anche se l'alias non viene utilizzato in una richiesta. La chiave kms: ResourceAliases condition ti consente di specificare un alias o un pattern di alias, ad esempio, in modo da poterlo utilizzare in una policy IAM per controllare l'accesso a diverse chiavi KMS nella stessa `alias/test*` regione. È valido per qualsiasi operazione AWS KMS che utilizza una chiave KMS.

Ad esempio, la seguente policy IAM consente ai principali di gestire la rotazione automatica delle chiavi sulle chiavi KMS in due Account AWS. Tuttavia, l'autorizzazione si applica solo alle chiavi KMS associate agli alias che iniziano con `restricted`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Sid": "AliasBasedIAMPolicy",
      "Effect": "Allow",
      "Action": [
        "kms:EnableKeyRotation",
        "kms:DisableKeyRotation",
        "kms:GetKeyRotationStatus"
      ],
      "Resource": [
        "arn:aws:kms:*:111122223333:key/*",
        "arn:aws:kms:*:444455556666:key/*"
      ],
      "Condition": {
        "ForAnyValue:StringLike": {
          "kms:ResourceAliases": "alias/restricted*"
        }
      }
    }
  ]
}
```

La condizione `kms:ResourceAliases` è una condizione della risorsa, non la richiesta. Pertanto, una richiesta che non specifica l'alias può ancora soddisfare la condizione.

La seguente richiesta di esempio, che specifica un alias corrispondente, soddisfa la condizione.

```
$ aws kms enable-key-rotation --key-id "alias/restricted-project"
```

Tuttavia, la seguente richiesta di esempio soddisfa anche la condizione, a condizione che la chiave KMS specificata abbia un alias che inizia con `restricted`, anche se quell'alias non viene utilizzato nella richiesta.

```
$ aws kms enable-key-rotation --key-id "1234abcd-12ab-34cd-56ef-1234567890ab"
```

Ricerca di alias nei log AWS CloudTrail

È possibile utilizzare un alias per rappresentare una AWS KMS key in un'operazione API AWS KMS. Quando lo fai, l'alias e l'ARN di chiave della chiave KMS vengono registrati nella voce di log AWS CloudTrail per l'evento. L'alias viene visualizzato nel campo `requestParameters`. L'ARN di chiave viene visualizzato nel campo `resources`. Questo vale anche quando un servizio AWS utilizza una Chiave gestita da AWS nel tuo account.

Ad esempio, la GenerateDataKeyrichiesta seguente utilizza l'`project-key`alias per rappresentare una chiave KMS.

```
$ aws kms generate-data-key --key-id alias/project-key --key-spec AES_256
```

Quando questa richiesta viene registrata nel CloudTrail registro, la voce di registro include sia l'alias che la chiave ARN della chiave KMS effettiva utilizzata.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "ABCDE",
        "arn": "arn:aws:iam::111122223333:role/ProjectDev",
        "accountId": "111122223333",
        "accessKeyId": "FFHIJ",
        "userName": "example-dev"
    },
    "eventTime": "2020-06-29T23:36:41Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.205.123.000",
    "userAgent": "aws-cli/1.18.89 Python/3.6.10
 Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 botocore/1.17.12",
    "requestParameters": {
        "keyId": "alias/project-key",
        "keySpec": "AES_256"
    },
    "responseElements": null,
    "requestID": "d93f57f5-d4c5-4bab-8139-5a1f7824a363",
    "eventID": "d63001e2-dbc6-4aae-90cb-e5370aca7125",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
```

```
}
```

Per informazioni dettagliate sulle AWS KMS operazioni di registrazione nei CloudTrail log, vedere. Registrazione delle chiamate API AWS KMS con AWS CloudTrail

Visualizzazione di chiavi

Puoi utilizzare l'API AWS Management Console o AWS Key Management Service (AWS KMS) per visualizzare le AWS KMS keys in ogni account e regione, incluse le chiavi KMS gestite da te e quelle gestite da AWS.

Argomenti

- Visualizzazione della chiave KMS nella console
- Visualizzazione di chiavi KMS con l'API
- Visualizzazione della configurazione crittografica delle chiavi KMS
- Individuazione dell'ID e dell'ARN della chiave
- Individuazione del nome e dell'ARN dell'alias

Visualizzazione della chiave KMS nella console

In AWS Management Console, puoi visualizzare gli elenchi delle chiavi KMS nell'account e nella regione e i dettagli su ogni chiave KMS.

> **Note**
>
> La console AWS KMS visualizza le chiavi KMS di cui disponi dell'autorizzazione alla visualizzazione nel tuo account e nella tua regione. Le chiavi KMS in altre Account AWS non appaiono nella console, anche se disponi dell'autorizzazione alla visualizzazione, alla gestione e all'uso di tali chiavi. Per visualizzare le chiavi KMS in altri account, usa l'DescribeKeyoperazione.

Argomenti

- Passaggio alle tabelle chiave
- Navigazione ai dettagli delle chiavi
- Ordinamento e filtraggio delle tue chiavi KMS

- Visualizzazione dei dettagli delle chiavi KMS
- Personalizzazione delle tabelle delle chiavi KMS

Passaggio alle tabelle chiave

Le AWS KMS keys in ogni account e regione sono visibili nelle tabelle. Esistono tabelle separate per le chiavi KMS create da te e le chiavi KMS che i servizi AWS creano per te.

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il selettore della regione nell'angolo superiore destro della pagina.
3. Per visualizzare le chiavi nell'account creato e gestito dall'utente, nel riquadro di navigazione, seleziona Chiavi gestite dal cliente. Per visualizzare le chiavi nell'account creato e gestito per te da AWS, nel riquadro di navigazione, seleziona AWS managed keys (chiavi gestite). Per informazioni sui diversi tipi di chiavi KMS, consulta AWS KMS keys.

> **Tip**
>
> Per visualizzare le Chiavi gestite da AWS in cui manca un alias, utilizza la pagina Customer managed keys (Chiavi gestite dal cliente).
> La console AWS KMS visualizza anche gli store delle chiavi personalizzate nell'account e nella regione. Le chiavi KMS create negli store delle chiavi personalizzate appaiono nella pagina Chiavi gestite dal cliente. Per informazioni sugli store delle chiavi personalizzate, consulta store delle chiavi personalizzate.

Navigazione ai dettagli delle chiavi

C'è una pagina di dettagli per ogni AWS KMS key nell'account e nella regione. Nella pagina dei dettagli viene visualizzata la sezione Configurazione generale per la chiave KMS e include schede che consentono agli utenti autorizzati di visualizzare e gestire Configurazione crittografica e Policy delle chiavi per la chiave. A seconda del tipo di chiave, la pagina dei dettagli potrebbe includere anche le schede Alias, Key material (materiale delle chiavi), Key rotation (rotazione delle chiavi), Public key (chiave pubblica), Regionality (regionalità) e Tags (tag).

Per passare alla pagina dei dettagli delle chiavi per una chiave KMS.

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il selettore della regione nell'angolo superiore destro della pagina.
3. Per visualizzare le chiavi nell'account creato e gestito dall'utente, nel riquadro di navigazione, seleziona Chiavi gestite dal cliente. Per visualizzare le chiavi nell'account creato e gestito per te da AWS, nel riquadro di navigazione, seleziona AWS managed keys (chiavi gestite). Per informazioni sui diversi tipi di chiavi KMS, consulta AWS KMS key.
4. Per aprire la pagina dei dettagli delle chiavi, nella tabella delle chiavi, scegli l'ID chiave o l'alias della chiave KMS.

   Se la chiave KMS dispone di più alias, viene visualizzato un riepilogo degli alias (+n più) viene visualizzato accanto al nome di uno degli alias. La scelta del riepilogo alias consente di accedere direttamente alla sezione Alias nella pagina dei dettagli delle chiavi.

Ordinamento e filtraggio delle tue chiavi KMS

Per semplificare la ricerca delle chiavi KMS nella console, puoi ordinare e filtrare le tabelle delle chiavi.

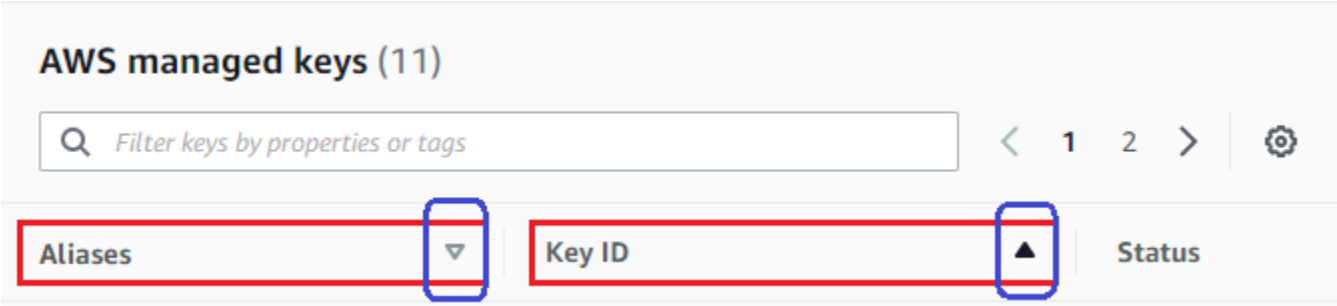
Ordina

Puoi ordinare le chiavi KMS in ordine crescente o decrescente in base ai valori di colonna. Questa caratteristica ordina tutte le chiavi KMS nella tabella, anche se non vengono visualizzate nella pagina della tabella corrente.

Le colonne ordinabili sono indicate da una freccia accanto al nome della colonna. Sulla pagina Chiavi gestite da AWS è possibile ordinare in base a Alias o ID chiave. Nella pagina Customer managed keys (Chiavi gestite dal cliente), è possibile ordinare per Alias, ID chiave o Key type (Tipo di chiave).

Per ordinare in ordine crescente, scegliere l'intestazione della colonna fino a quando la freccia non punta verso l'alto. Per ordinare in ordine decrescente, scegliere l'intestazione della colonna fino a quando la freccia non punta verso il basso. Puoi eseguire l'ordinamento in base a una colonna alla volta.

Ad esempio, puoi ordinare le chiavi KMS in ordine crescente per ID chiave, anziché alias, che è l'impostazione predefinita.



Quando si ordinano le chiavi KMS nella pagina Chiavi gestite dal cliente in ordine crescente per Tipo di chiave, tutte le chiavi asimmetriche vengono visualizzate prima di tutte quelle simmetriche.

Filtro

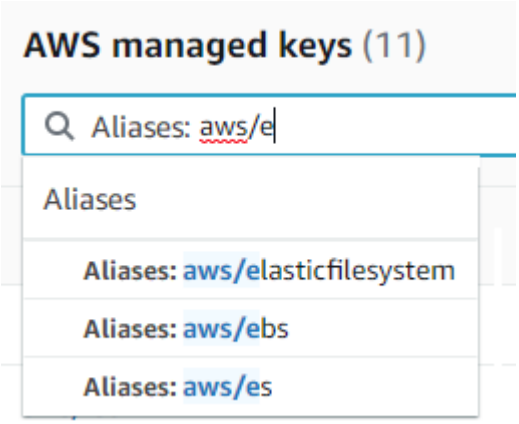
È possibile filtrare le chiavi KMS in base ai valori delle proprietà o ai tag Il filtro si applica a tutte le chiavi KMS nella tabella, anche se non vengono visualizzate nella pagina della tabella corrente. Il filtro non fa distinzione tra maiuscole e minuscole.

Le proprietà filtrabili sono elencate nella casella filtro. Sulla pagina Chiavi gestite da AWS, è possibile filtrare in base all'alias e all'ID chiave. Nella pagina Chiavi gestite dal cliente, puoi filtrare per Alias, ID Chiave, Tipo di chiave e tag.

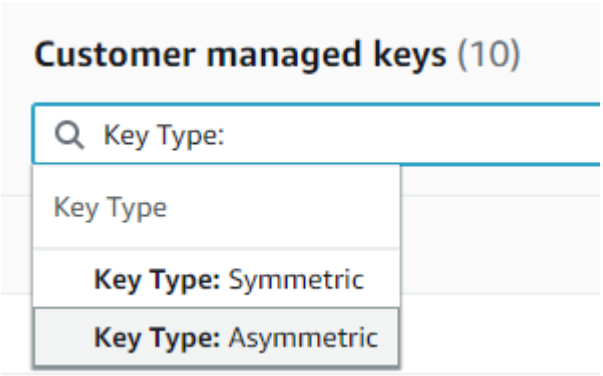
- Sulla pagina Chiavi gestite da AWS, è possibile filtrare in base all'alias e all'ID chiave.
- Sulla pagina Chiavi gestite dal cliente, è possibile filtrare in base ai tag o in base all'alias, all'ID chiave, al tipo di chiave o alle proprietà di regionalità.

Per filtrare in base al valore di una caratteristica, scegli il filtro, il nome della proprietà e scegli dall'elenco dei valori effettivi delle proprietà. Per filtrare in base a un tag, scegli il codice tag, quindi scegli dall'elenco dei valori effettivi dei tag. Dopo aver scelto una chiave di proprietà o di tag, puoi anche digitare tutto il valore della proprietà o solo parte di esso. Vedrai un'anteprima dei risultati prima di effettuare la tua scelta.

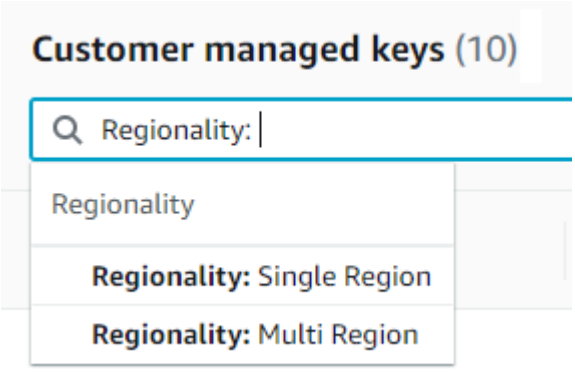
Ad esempio, per visualizzare le chiavi KMS con un nome alias contenente `aws/e`, scegli la casella del filtro, scegli Alias, digita `aws/e`, e premi `Enter` o `Return` per aggiungere il filtro.



Per visualizzare solo le chiavi KMS asimmetriche nella pagina Chiavi gestite dal cliente) fare clic sulla casella del filtro, scegliere Tipo di chiave, quindi scegliere Tipo di chiave: Asimmetrica. L'opzione Asimmetrica viene visualizzata solo quando nella tabella sono presenti chiavi KMS asimmetriche. Per ulteriori informazioni sull'identificazione delle chiavi KMS asimmetriche, vedi Individuazione di chiavi KMS asimmetriche.



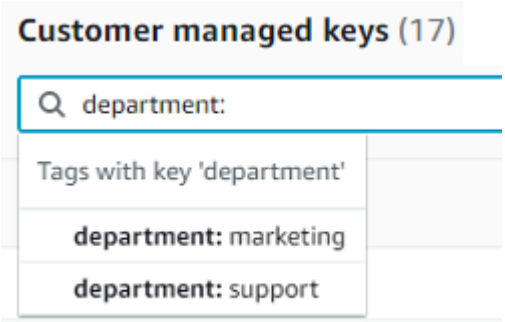
Per visualizzare solo le chiavi multi-regione, nella scheda Chiavi gestite dal cliente scegli la casella di filtro, scegli Regionalità e quindi Regionalità: Multiregione. L'opzione Multiregione viene visualizzata solo quando nella tabella sono presenti chiavi multi-regione. Per ulteriori informazioni sull'identificazione delle chiavi multi-regione, vedi Visualizzazione di chiavi multiregione.



Il filtro dei tag è un po' diverso. Per visualizzare solo le chiavi KMS con un determinato tag, scegli la casella filtro, scegli la chiave di tag, quindi scegli tra i valori effettivi dei tag. È anche possibile digitare o tutto il valore del tag o solo parte di esso.

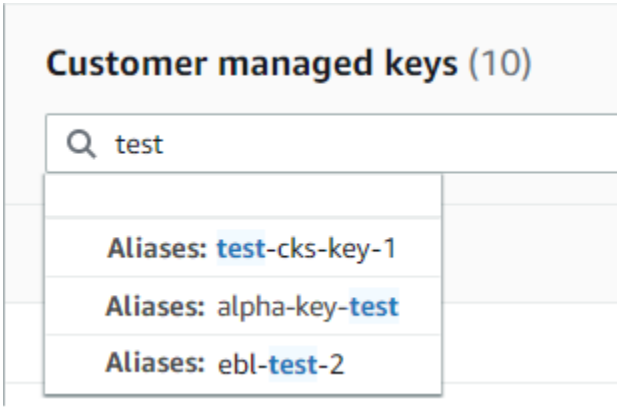
Nella tabella risultante vengono visualizzate tutte le chiavi KMS con il tag scelto. Tuttavia, il tag non viene visualizzato. Per visualizzare il tag, scegli l'alias o l'ID chiave della chiave KMS e nella pagina dei dettagli scegli la scheda Tag. Le schede appaiono nella sezione Configurazione generale.

Per questo filtro sono necessari sia la chiave di tag che il valore del tag. Non troverà le chiavi KMS digitando solo la chiave di tag o solo il suo valore. Per filtrare i tag in base alla chiave o al valore del tag, usa l'ListResourceTagsoperazione per ottenere le chiavi KMS con tag, quindi usa le funzionalità di filtro del tuo linguaggio di programmazione. Per un esempio, consultare ListResourceTags: Ottieni i tag sulle chiavi KMS.

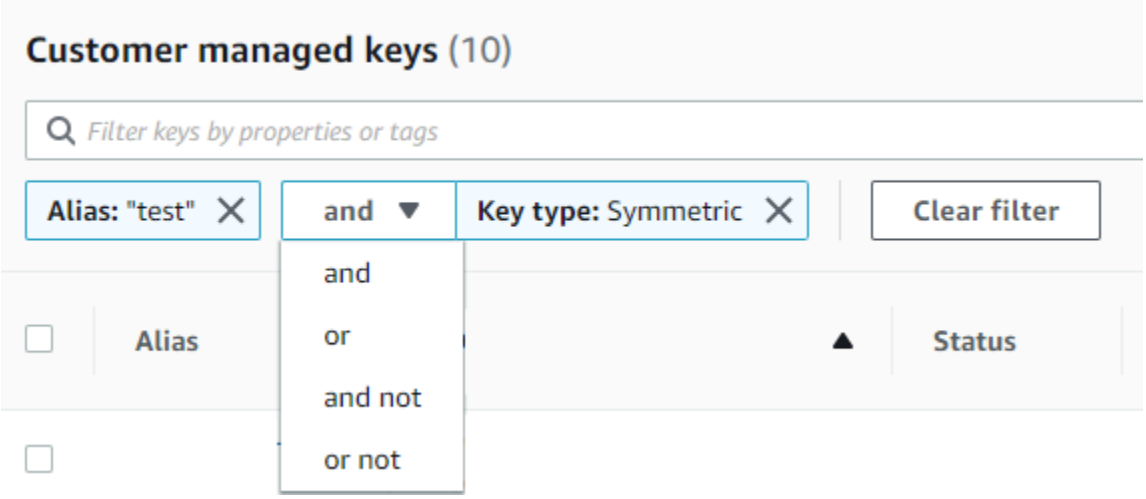


Per cercare del testo, nella casella filtro digita tutto o solo parte di un alias, di un ID chiave, di un tipo di chiave o di una chiave di tag. (Dopo aver selezionato la chiave di tag, puoi cercare un valore di tag). Vedrai un'anteprima dei risultati prima di effettuare la tua scelta.

Ad esempio, per visualizzare le chiavi KMS con `test` nelle chiavi di tag o nelle proprietà filtrabili, digitare `test` nella casella filtro. L'anteprima mostra le chiavi KMS che il filtro selezionerà. In questo caso, `test` appare solo nella proprietà Alias.



È possibile utilizzare più filtri contemporaneamente. Quando si aggiungono filtri aggiuntivi, puoi anche selezionare un operatore logico.

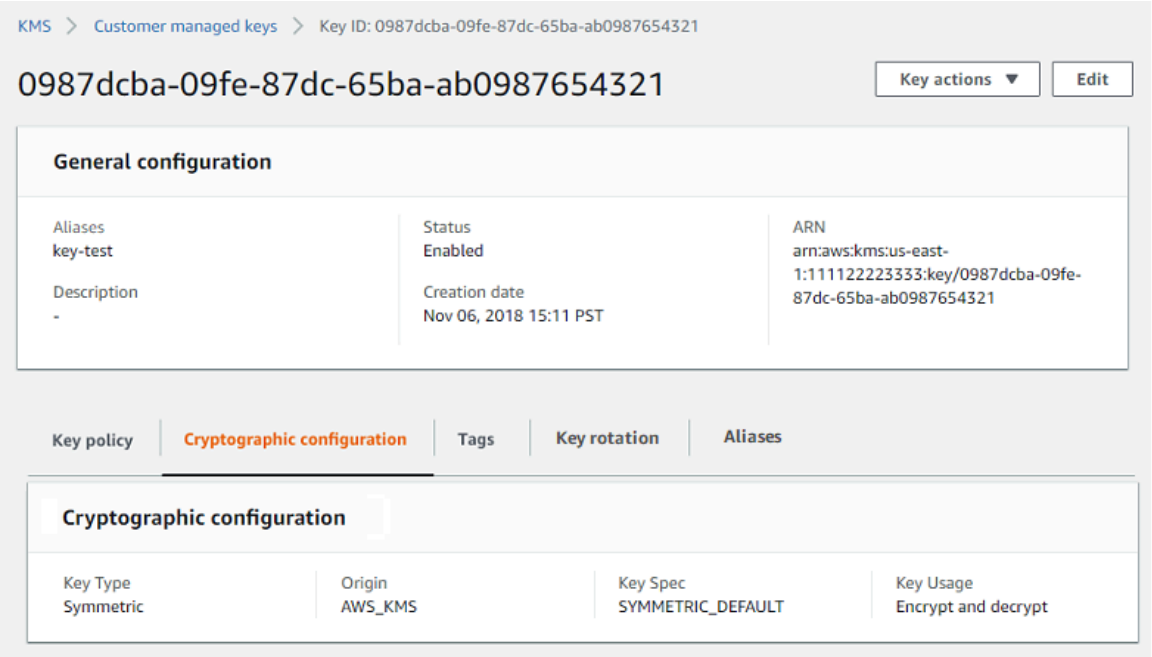


Visualizzazione dei dettagli delle chiavi KMS

La pagina dei dettagli di ogni chiave KMS visualizza le proprietà della chiave KMS. Differisce leggermente per i diversi tipi di chiavi KMS.

Per visualizzare la pagina dei dettagli di una chiave KMS, nella pagina Chiavi gestite da AWS o nella pagina Chiavi gestite dal cliente scegli l'ID chiave o l'alias della chiave KMS.

La pagina dei dettagli per una chiave KMS include una Configurazione generale in cui vengono visualizzate le proprietà di base della chiave KMS. Include inoltre delle schede in cui puoi visualizzare e modificare le proprietà della chiave KMS, ad esempio Key policy (Policy della chiave), Cryptographic configuration (Configurazione di crittografia), Tags (Tag), Key material (Materiale della chiave) (per le chiavi KMS con materiale importato), Key rotation (Rotazione della chiave) (per le chiavi KMS di crittografia simmetrica), Regionality (Regionalità) (per le chiavi multi-regione) e Public key (Chiave pubblica) (per le chiavi KMS asimmetriche).



Nell'elenco seguente vengono descritti i campi nella visualizzazione dettagliata, incluso il campo nelle schede. Alcuni di questi campi sono disponibili anche come colonne nella visualizzazione della tabella.

Alias

Dove: scheda degli Alias

Specifica un nome intuitivo per la chiave KMS. È possibile utilizzare un alias per identificare la chiave KMS nella console e in alcuni API AWS KMS. Per informazioni dettagliate, vedi Utilizzo di alias.

Nelle schede Alias vengono visualizzati tutti gli alias associati alla chiave KMS nel Account AWS e nella Regione.

ARN

Dove: sezione Configurazione generale

Il nome della risorsa Amazon (ARN) della chiave KMS. Questo valore identifica singolarmente la chiave KMS. Puoi utilizzarlo per identificare la chiave KMS nelle operazioni API AWS KMS.

Stato connessione

Indica se un archivio delle chiavi personalizzate è collegato al relativo archivio del materiale della chiave. Questo campo viene visualizzato solo quando la chiave KMS viene creata in un archivio delle chiavi personalizzate.

Per informazioni sui valori in questo campo, consulta l'AWS KMSAPI ConnectionStateReference.

Data di creazione

Dove: sezione Configurazione generale

La data e l'ora di creazione della chiave KMS. Questo valore viene visualizzato nell'ora locale per il dispositivo. Il fuso orario non dipende dalla regione.

A differenza della Expiration (Scadenza), la creazione si riferisce solo alla chiave KMS, non al materiale della chiave.

ID cluster CloudHSM

Dove: scheda Configurazione crittografica

L'ID del cluster del cluster AWS CloudHSM che contiene il materiale della chiave per la chiave KMS. Questo campo viene visualizzato solo quando la chiave KMS viene creata in un archivio delle chiavi personalizzate.

Se fai clic sull'ID del cluster CloudHSM, viene visualizzata la pagina Clusters nella console AWS CloudHSM.

ID dello store delle chiavi personalizzate

Dove: scheda Configurazione crittografica

L'ID dell'archivio delle chiavi personalizzate che contiene la chiave KMS. Questo campo viene visualizzato solo quando la chiave KMS viene creata in un archivio delle chiavi personalizzate.

Se fai clic sull'ID dell'archivio delle chiavi personalizzata, viene visualizzata la pagina Archivi delle chiavi personalizzate nella console AWS KMS.

Il nome dello store delle chiavi personalizzate

Dove: scheda Configurazione crittografica

Il nome dell'archivio delle chiavi personalizzate che contiene la chiave KMS. Questo campo viene visualizzato solo quando la chiave KMS viene creata in un archivio delle chiavi personalizzate.

Tipo di archivio delle chiavi personalizzate

Dove: scheda Configurazione crittografica

Indica se l'archivio delle chiavi personalizzate è un archivio delle chiavi di AWS CloudHSM o un archivio delle chiavi esterne. Questo campo viene visualizzato solo quando la chiave KMS viene creata in un archivio delle chiavi personalizzate.

Descrizione

Dove: sezione Configurazione generale

Una breve descrizione facoltativa della chiave KMS che puoi scrivere e modificare. Per aggiungere o aggiornare la descrizione di una chiave gestita dal cliente, sopra Configurazione generale seleziona Modifica.

Algoritmi di crittografia

Dove: scheda Configurazione crittografica

Elenca gli algoritmi di crittografia che possono essere utilizzati con la chiave KMS in AWS KMS. Questo campo viene visualizzato solo quando Key type (Tipo di chiave) è Asymmetric (Asimmetrico) e Key usage (Utilizzo della chiave) è Encrypt and decrypt (Crittografa e decripta). Per informazioni sugli algoritmi di crittografia supportati da AWS KMS, consulta Specifica della chiave SYMMETRIC_DEFAULT e Specifiche della chiave RSA per la crittografia e la decrittografia.

Data di scadenza

Dove: scheda Materiale della chiave

Data e ora in cui scade il materiale della chiave per la chiave KMS. Questo campo viene visualizzato solo per le chiavi KMS con materiale della chiave importato, ovvero quando Origin (Origine) è External (Esterna) e la chiave KMS ha materiale della chiave in scadenza.

ID chiave esterna

Dove: scheda Configurazione crittografica

L'ID della chiave esterna associata a una chiave KMS in un archivio delle chiavi esterne. Questo campo viene visualizzato solo per le chiavi KMS in un archivio delle chiavi esterne.

Stato della chiave esterna

Dove: scheda Configurazione crittografica

Lo stato più recente riportato dal proxy dell'archivio delle chiavi esterne per la chiave esterna associata alla chiave KMS. Questo campo viene visualizzato solo per le chiavi KMS in un archivio delle chiavi esterne.

Utilizzo della chiave esterna

Dove: scheda Configurazione crittografica

Le operazioni di crittografia abilitate sulla chiave esterna associata alla chiave KMS. Questo campo viene visualizzato solo per le chiavi KMS in un archivio delle chiavi esterne.

Policy delle chiavi

Dove: scheda Policy delle chiavi

Controlla l'accesso alla chiave KMS e alle policy IAM e alle concessioni. Ogni chiave KMS ha una policy delle chiavi. È l'unico elemento di autorizzazione obbligatorio. Per modificare la policy delle chiavi di una chiave gestita dal cliente, nella scheda Policy delle chiavi, scegli Modifica. Per informazioni dettagliate, vedi the section called “Policy delle chiavi”.

Rotazione delle chiavi

Dove: Scheda Rotazione della chiave

Abilita e disabilita la rotazione automatica del materiale chiave in una chiave CMK gestita dal cliente. Per modificare lo stato di rotazione della chiave di una chiave gestita dal cliente, utilizzare la casella di controllo nella scheda Key rotation (Rotazione della chiave).

Non è possibile abilitare o disabilitare la rotazione del materiale della chiave in una Chiave gestita da AWS. Le Chiavi gestite da AWS vengono ruotate automaticamente ogni anno.

Specifica della chiave

Dove: scheda Configurazione crittografica

Il tipo di materiale della chiave nella chiave KMS. AWS KMS supporta chiavi KMS di crittografia simmetrica (SYMMETRIC_DEFAULT), chiavi KMS HMAC di diversa lunghezza, chiavi KMS per chiavi RSA di diversa lunghezza e chiavi basate su curva ellittica con curve diverse. Per informazioni dettagliate, vedi Specifica della chiave.

Tipo di chiavi

Dove: scheda Configurazione crittografica

Indica se la chiave KMS è Simmetrica o Asimmetrica.

Utilizzo delle chiavi

Dove: scheda Configurazione crittografica

Indica se una chiave KMS può essere utilizzata per le operazioni Encrypt and decrypt (Crittografa e decrittografa), Sign and verify (Firma e verifica) o Generate and verify MAC (Genera e verifica MAC). Per informazioni dettagliate, vedi Utilizzo delle chiavi.

Origin

Dove: scheda Configurazione crittografica

L'origine del materiale della chiave per la chiave KMS. I valori validi sono:

- AWS KMS per il materiale della chiave generato da AWS KMS
- AWS CloudHSM per le chiavi KMS in un archivio delle chiavi di AWS CloudHSM
- Esterno per il materiale della chiave importato (BYOK)
- Archivio delle chiavi esterne per le chiavi KMS in un archivio delle chiavi esterne

Algoritmi MAC

Dove: scheda Configurazione crittografica

Elenca gli algoritmi MAC che possono essere utilizzati con la chiave KMS HMAC in AWS KMS. Questo campo viene visualizzato solo quando il valore Key spec (Specifica della chiave) è una specifica di chiave HMAC (HMAC_*). Per informazioni sugli algoritmi MAC supportati da AWS KMS, consulta la sezione Specifiche della chiave per le chiavi KMS HMAC.

Chiave primaria

Dove: scheda Regionalità

Indica che questa chiave KMS è una chiave primaria multi-regione. Gli utenti autorizzati possono utilizzare questa sezione per cambiare la chiave primaria con una diversa chiave multi-regione correlata. Questo campo viene visualizzato solo quando la chiave KMS è una chiave primaria multi-regione.

Chiavi pubbliche

Dove: scheda Chiave pubblica

Visualizza la chiave pubblica di una chiave KMS asimmetrica. Gli utenti autorizzati possono utilizzare questa scheda per copiare e scaricare la chiave pubblica.

Regionalità

Dove: sezione Configurazione generale e schede Regionalità

Indica se una chiave KMS è una chiave di singola regione, una chiave primaria multi-regione, o una chiave di replica in multi-regione. Questo campo viene visualizzato solo quando la chiave KMS è una chiave multi-regione.

Chiavi multi-regione correlate

Dove: scheda Regionalità

Visualizza tutte le relative chiavi primarie e di replica multi-regione, ad eccezione della chiave KMS corrente. Questo campo viene visualizzato solo quando la chiave KMS è una chiave multi-regione.

Nella sezione chiavi multi-regione correlate di una chiave primaria, gli utenti autorizzati possono creare nuove chiavi di replica.

Chiave di replica

Dove: scheda Regionalità

Indica che questa chiave KMS è una chiave di replica multi-regione. Questo campo viene visualizzato solo quando la chiave KMS è una chiave di replica multi-regione.

Algoritmi di firma

Dove: scheda Configurazione crittografica

Elenca gli algoritmi di firma che possono essere utilizzati con la chiave KMS in AWS KMS. Questo campo viene visualizzato solo quando Key type (Tipo di chiave) è Asymmetric (Asimmetrico) e Key usage (Utilizzo della chiave) è Sign and verify (Firma e verifica). Per informazioni sugli algoritmi di firma supportati da AWS KMS, consulta Specifiche della chiave RSA per la firma e la verifica e Specifiche della chiave basata su curva ellittica.

Stato

Dove: sezione Configurazione generale

Lo stato della chiave KMS. È possibile utilizzare la chiave KMS nelle operazioni di crittografia solo quando lo stato è Enabled (Abilitato). Per una descrizione dettagliata di ogni stato di chiave

KMS e il relativo effetto sulle operazioni che è possibile eseguire sulla chiave KMS, consulta Stati chiave delle chiavi AWS KMS.

Tag

Dove: scheda Tag

Coppie chiave-valore opzionali che descrivono la chiave KMS. Per aggiungere o modificare i tag per una chiave KMS, nella scheda Tag scegli Modifica.

Quando aggiungi i tag alle risorse AWS, AWS genera un report di allocazione dei costi in cui l'utilizzo e i costi sono aggregati in base ai tag. I tag possono essere utilizzati anche per controllare l'accesso a una chiave KMS. Per informazioni sul tagging delle chiavi KMS, consulta Chiavi di tagging e ABAC per AWS KMS.

Personalizzazione delle tabelle delle chiavi KMS

È possibile personalizzare le tabelle visualizzate nella scheda Chiavi gestite da AWS e in Chiavi gestite dal cliente nella AWS Management Console per soddisfare le tue esigenze. Puoi scegliere le colonne della tabella, il numero di AWS KMS keys in ogni pagina (Dimensioni pagina), e il testo a capo. La configurazione scelta viene salvata quando viene confermata e riapplicata ogni volta che si aprono le pagine.

Per personalizzare le tabelle delle chiavi KMS

1. Nella pagina Chiavi gestite da AWS o in Chiavi gestite dal cliente, scegli l'icona delle impostazioni

   ()

   nell'angolo in alto a destra della pagina.
2. Nella pagina Preferences (Preferenze), scegliere le impostazioni preferite e quindi Confirm (Conferma).

Ti consigliamo di utilizzare l'impostazione Page size (Dimensione pagina) per aumentare il numero di chiavi KMS visualizzate su ogni pagina, soprattutto se usi un dispositivo facile da scorrere.

Le colonne di dati visualizzate possono variare a seconda della tabella, del ruolo lavorativo, e dei tipi di chiavi KMS nell'account e nella regione. Nella tabella seguente sono riportate alcune configurazioni suggerite. Per le descrizioni delle colonne, consulta Visualizzazione dei dettagli delle chiavi KMS.

Configurazioni consigliate per le tabelle delle chiavi KMS

Puoi personalizzare le colonne visualizzate nella tabella delle chiave KMS per visualizzare le informazioni necessarie sulle chiavi KMS.

Chiavi gestite da AWS

Per impostazione predefinita, la tabella Chiave gestita da AWS mostra le colonne Alias, ID chiave e Stato. Queste colonne sono ideali per la maggior parte dei casi d'uso.

Chiavi KMS di crittografia simmetrica

Se utilizzi soltanto chiavi KMS di crittografia simmetrica con materiale della chiave generato da AWS KMS, è probabile che le colonne Aliases (Alias), Key ID (ID chiave), Status (Stato) e Creation date (Data di creazione) siano quelle più utili.

Chiavi KMS asimmetriche

Se utilizzi chiavi KMS asimmetriche, oltre alle colonne Alias, ID chiave e Stato, si consiglia di aggiungere le colonne Tipo di chiave, Key spec (Specifiche della chiave) e Key usage (Utilizzo della chiave). Queste colonne mostrano se una chiave KMS è simmetrica o asimmetrica, il tipo di materiale della chiave e se la chiave KMS può essere utilizzata per la crittografia o la firma.

Chiavi KMS HMAC

Se utilizzi chiavi KMS HMAC, oltre alle colonne Aliases (Alias), Key ID (ID chiave) e Status (Stato), ti consigliamo di aggiungere le colonne Key spec (Specifica della chiave) e Key usage (Utilizzo della chiave). Queste colonne mostrano se una chiave KMS è una chiave HMAC. Poiché non è possibile ordinare le chiavi KMS in base alla specifica o all'utilizzo della chiave, puoi utilizzare alias e tag per identificare le chiavi HMAC e quindi usare l'opzione Filter features (Filtra per caratteristiche) della console AWS KMS per filtrare per alias o tag.

Materiale della chiave importato

Se si dispone di chiavi KMS con materiale della chiave importato, prendi in considerazione l'aggiunta delle colonne Origine e Data di scadenza. Queste colonne mostreranno se il materiale della chiave in una chiave KMS viene importato o generato da AWS KMS e quando, e se, il materiale della chiave scade. Il campo Data di creazione mostra la data di creazione della chiave KMS (senza il materiale della chiave). Non riflette alcuna caratteristica del materiale della chiave.

Chiavi nello store delle chiavi personalizzate

Se disponi di chiavi KMS negli archivi delle chiavi personalizzate, prendi in considerazione l'aggiunta delle colonne Origin (Origine) e Custom key store ID (ID dell'archivio chiavi

personalizzate). Queste colonne mostrano che la chiave KMS si trova in un archivio delle chiavi personalizzate e identificano tale archivio.

Chiavi multi-regione

Se hai chiavi multi-regione, prendi in considerazione l'aggiunta della colonna Regionalità. In questo modo viene mostrato se una chiave KMS è una chiave di singola regione, una chiave primaria multi-regione o una chiave di replica multi-regione.

Visualizzazione di chiavi KMS con l'API

Puoi utilizzare l'APIAWS Key Management Service (AWS KMS) per visualizzare le tue chiavi KMS. Questa sezione illustra diverse operazioni che restituiscono dettagli sulle esistenti chiavi KMS. Gli esempi utilizzano la AWS Command Line Interface (AWS CLI), ma puoi usare anche qualsiasi linguaggio di programmazione supportato.

Argomenti

- ListKeys: Ottieni l'ID e l'ARN di tutte le chiavi KMS
- DescribeKey: Ottieni informazioni dettagliate su una chiave KMS
- GetKeyPolicy: ottieni la politica chiave allegata a una chiave KMS
- ListAliases: Ottieni nomi alias e ARN per le chiavi KMS
- ListResourceTags: Ottieni i tag sulle chiavi KMS

ListKeys: Ottieni l'ID e l'ARN di tutte le chiavi KMS

L'ListKeysoperazione restituisce l'ID e l'Amazon Resource Name (ARN) di tutte le chiavi KMS nell'account e nella regione.

Ad esempio, questa chiamata all'operazione `ListKeys` restituisce l'ID e l'ARN di ciascuna chiave KMS presente in questo account fittizio. Per esempi in più linguaggi di programmazione, consulta Ottenimento degli ID e degli ARN delle chiavi KMS.

```
$ aws kms list-keys

{
  "Keys": [
    {
```

```
      "KeyArn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    {
      "KeyArn": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321",
      "KeyId": "0987dcba-09fe-87dc-65ba-ab0987654321"
    },
    {
      "KeyArn": "arn:aws:kms:us-
east-2:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d",
      "KeyId": "1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d"
    }
}
```

DescribeKey: Ottieni informazioni dettagliate su una chiave KMS

L'DescribeKeyoperazione restituisce dettagli sulla chiave KMS specificata. Per identificare la chiave KMS, utilizza ID chiave, ARN di chiave, nome alias o alias ARN.

A differenza dell'ListKeysoperazione, che visualizza solo le chiavi KMS nell'account e nella regione del chiamante, gli utenti autorizzati possono utilizzare l'`DescribeKey`operazione per ottenere dettagli sulle chiavi KMS in altri account.

> **Note**
>
> La risposta `DescribeKey` include sia membri `KeySpec` e `CustomerMasterKeySpec` con gli stessi valori. Il membro `CustomerMasterKeySpec` è obsoleto.

Ad esempio, questa chiamata a `DescribeKey` restituisce informazioni su una chiave KMS di crittografia simmetrica. I campi nella risposta variano in base alle specifiche della AWS KMS key, allo stato della chiave e all'origine del materiale della chiave. Per esempi in più linguaggi di programmazione, consulta Visualizzazione di un AWS KMS key.

```
$ aws kms describe-key --key-id 1234abcd-12ab-34cd-56ef-1234567890ab

{
    "KeyMetadata": {
        "Origin": "AWS_KMS",
```

```
        "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "Description": "",
        "KeyManager": "CUSTOMER",
        "Enabled": true,
        "KeySpec": "SYMMETRIC_DEFAULT",
        "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "KeyState": "Enabled",
        "CreationDate": 1499988169.234,
        "MultiRegion": false,
        "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "AWSAccountId": "111122223333",
        "EncryptionAlgorithms": [
            "SYMMETRIC_DEFAULT"
        ]
    }
}
```

Questo esempio chiama l'operazione `DescribeKey` su una chiave KMS asimmetrica utilizzata per la firma e la verifica. La risposta include gli algoritmi di firma supportati da AWS KMS per questa chiave KMS.

```
$ aws kms describe-key --key-id 0987dcba-09fe-87dc-65ba-ab0987654321

{
    "KeyMetadata": {
        "KeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
        "Origin": "AWS_KMS",
        "Arn": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321",
        "KeyState": "Enabled",
        "KeyUsage": "SIGN_VERIFY",
        "CreationDate": 1569973196.214,
        "Description": "",
        "KeySpec": "ECC_NIST_P521",
        "CustomerMasterKeySpec": "ECC_NIST_P521",
        "AWSAccountId": "111122223333",
        "Enabled": true,
        "MultiRegion": false,
        "KeyManager": "CUSTOMER",
        "SigningAlgorithms": [
            "ECDSA_SHA_512"
```

```
        ]
    }
}
```

GetKeyPolicy: ottieni la politica chiave allegata a una chiave KMS

L'GetKeyPolicyoperazione ottiene la politica chiave allegata alla chiave KMS. Per identificare la chiave KMS utilizza l'ID chiave o l'ARN di chiave. Inoltre, devi specificare il nome della policy, che è sempre `default`. (Se l'output è difficile da leggere, aggiungi l'opzione `--output text` al comando.) `GetKeyPolicy`funziona solo sulle chiavi KMS nell'account e nella regione dell'intermediario.

Per esempi in più linguaggi di programmazione, consulta Recupero di una policy delle chiavi.

```
$ aws kms get-key-policy --key-id 1234abcd-12ab-34cd-56ef-1234567890ab --policy-name
 default

{
  "Version" : "2012-10-17",
  "Id" : "key-default-1",
  "Statement" : [ {
    "Sid" : "Enable IAM User Permissions",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "arn:aws:iam::111122223333:root"
    },
    "Action" : "kms:*",
    "Resource" : "*"
  } ]
}
```

ListAliases: Ottieni nomi alias e ARN per le chiavi KMS

L'ListAliasesoperazione restituisce gli alias nell'account e nella regione. Il `TargetKeyId` nella risposta mostra l'ID chiave della chiave KMS a cui l'alias fa riferimento, se del caso.

Per impostazione predefinita, il comando ListAliases restituisce tutti gli alias nell'account e nella regione. Sono inclusi gli alias creati dall'utente e associati alle chiavi gestite dal cliente, così come gli alias creati da AWS e associati alla Chiave gestita da AWS nell'account dell'utente. Gli alias AWS sono riconoscibili per il formato del nome `aws/<service-name>`, ad esempio `aws/dynamodb`.

La risposta potrebbe includere anche alias che non includono il campo `TargetKeyId`, come nel caso dell'alias `aws/redshift` in questo esempio. Questi sono alias predefiniti che AWS ha creato, ma che non ha ancora associato a una chiave KMS.

Per esempi in più linguaggi di programmazione, consulta Elenco degli alias.

```
$ aws kms list-aliases

{
    "Aliases": [
        {
            "AliasName": "alias/access-key",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/access-key",
            "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
            "CreationDate": 1516435200.399,
            "LastUpdatedDate": 1516435200.399
        },
        {
            "AliasName": "alias/financeKey",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/financeKey",
            "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
            "CreationDate": 1604958290.014,
            "LastUpdatedDate": 1604958290.014
        },
        {
            "AliasName": "alias/ECC-P521-Sign",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/ECC-P521-Sign",
            "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
            "CreationDate": 1693622000.704,
            "LastUpdatedDate": 1693622000.704
        },
        {
            "AliasName": "alias/ImportedKey",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/ImportedKey",
            "TargetKeyId": "1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d",
            "CreationDate": 1493622000.704,
            "LastUpdatedDate": 1521097200.235
        },
        {
            "AliasName": "alias/aws/dynamodb",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/aws/dynamodb",
            "TargetKeyId": "0987ab65-43cd-21ef-09ab-87654321cdef",
            "CreationDate": 1521097200.454,
```

```
            "LastUpdatedDate": 1521097200.454
        },
        {
            "AliasName": "alias/aws/ebs",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/aws/ebs",
            "TargetKeyId": "abcd1234-09fe-ef90-09fe-ab0987654321",
            "CreationDate": 1466518990.200,
            "LastUpdatedDate": 1466518990.200
        },
        {
            "AliasName": "alias/aws/redshift",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/aws/redshift"
        },
    ]
}
```

Per ottenere gli alias che fanno riferimento a una determinata chiave KMS, utilizza il parametro `KeyId`. Il valore del parametro può essere l'ID chiave o l'ARN della chiave. Non è possibile specificare un nome dell'alias o un ARN dell'alias.

Il comando nell'esempio seguente ottiene gli alias che fanno riferimento a una chiave gestita dal cliente. Tuttavia, puoi utilizzare un comando come questo anche per trovare anche gli alias che fanno riferimento alle Chiavi gestite da AWS.

```
$ aws kms list-aliases --key-id arn:aws:kms:us-
west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321
{
    "Aliases": [
        {
            "AliasName": "alias/access-key",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/access-key",
            "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
            "CreationDate": 1516435200.399,
            "LastUpdatedDate": 1516435200.399
        },
        {
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/financeKey",
            "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
            "AliasName": "alias/financeKey",
            "CreationDate": 1604958290.014,
            "LastUpdatedDate": 1604958290.014
        },
    ]
```

```
}
```

Per ottenere solo gli alias per Chiavi gestite da AWS, utilizza le caratteristiche del linguaggio di programmazione per filtrare la risposta.

```
$ aws kms list-aliases --query 'Aliases[?starts_with(AliasName, `alias/aws/`)]'
```

ListResourceTags: Ottieni i tag sulle chiavi KMS

L'ListResourceTagsoperazione restituisce i tag sulla chiave KMS specificata. L'API restituisce i tag per una chiave KMS, ma è possibile eseguire il comando in un ciclo per ottenere i tag per tutte le chiavi KMS nell'account e nella regione, o per un set di chiavi KMS selezionate. Questa API restituisce una pagina alla volta, quindi se si dispone di numerosi tag su numerose chiavi KMS, potrebbe essere necessario utilizzare l'impaginatore nel linguaggio di programmazione per ottenere tutti i tag desiderati.

L'operazione `ListResourceTags` restituisce i tag per tutte le chiavi KMS, ma le Chiave gestita da AWS non sono taggate. Funziona solo con le chiavi KMS nell'account e nella regione dell'intermediario.

Per trovare i tag per una chiave KMS, utilizza l'operazione `ListResourceTags`. Il parametro `KeyId` è obbligatorio. Accetta un ID chiave o un ARN della chiave. Prima di eseguire questo esempio, sostituisci l'ARN della chiave di esempio con uno valido.

```
$  aws kms list-resource-tags --key-id arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
      {
    "Tags": [
        {
            "TagKey": "Department",
            "TagValue": "IT"
        },
        {
            "TagKey": "Purpose",
            "TagValue": "Test"
        }
    ],
    "Truncated": false
}
```

È possibile utilizzare l'operazione `ListResourceTags` per ottenere tutte le chiavi KMS nell'account e nella Regione con un tag, una chiave di tag o un valore di tag specifico. Per fare ciò, utilizzare le funzionalità di filtraggio del linguaggio di programmazione.

Ad esempio, il seguente script Bash utilizza le `ListResourceTags` operazioni ListKeysand per ottenere tutte le chiavi KMS nell'account e nella regione con una `Project` chiave tag. Entrambe queste operazioni ottengono solo la prima pagina dei risultati. Se si dispone di numerose chiavi KMS o di numerosi tag, utilizzare le funzionalità di impaginazione della lingua per ottenere l'intero risultato da ogni operazione. Prima di eseguire questo esempio, sostituisci gli ID della chiave di esempio con quelli validi.

```
TARGET_TAG_KEY='Project'

for key in $(aws kms list-keys --query 'Keys[*].KeyId' --output text); do
  key_tags=$(aws kms list-resource-tags --key-id "$key" --query "Tags[?TagKey==\`
$TARGET_TAG_KEY\`]")
  if [ "$key_tags" != "[]" ]; then
    echo "Key: $key"
    echo "$key_tags"
  fi
done
```

L'output è formattato come l'output di esempio seguente.

```
Key: 0987dcba-09fe-87dc-65ba-ab0987654321
[
    {
        "TagKey": "Project",
        "TagValue": "Gamma"
    }
]
Key: 1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d
[
    {
        "TagKey": "Project",
        "TagValue": "Alpha"
    }
]
Key: 0987ab65-43cd-21ef-09ab-87654321cdef
[
    {
        "TagKey": "Project",
```

```
        "TagValue": "Alpha"
    }
]
```

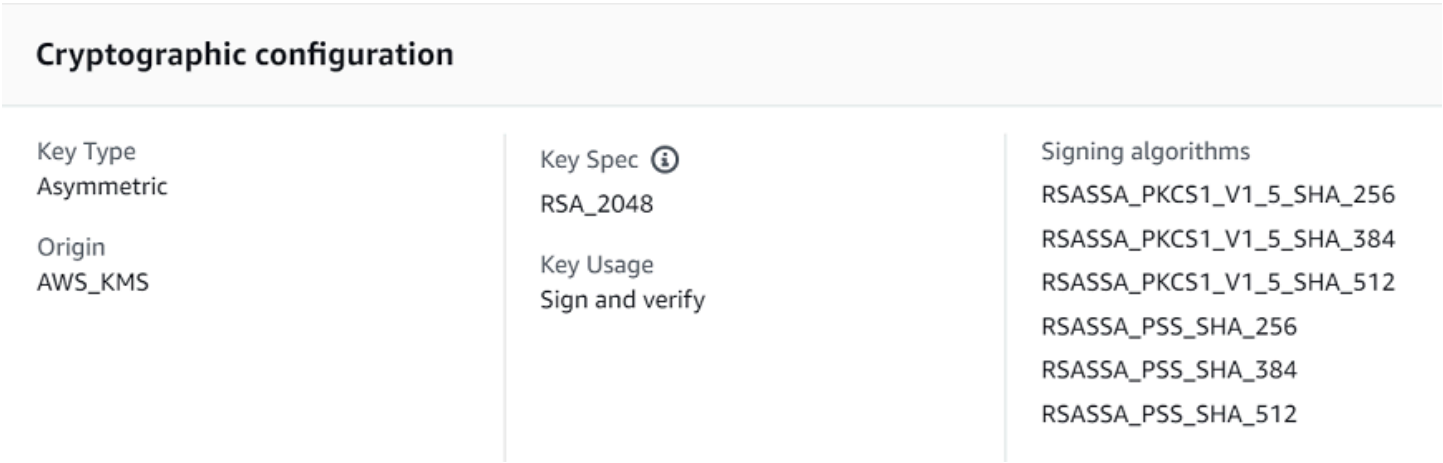
Visualizzazione della configurazione crittografica delle chiavi KMS

Dopo aver creato la chiave KMS, puoi visualizzarne la configurazione crittografica. Non puoi modificare la configurazione di una chiave KMS una volta creata. Se preferisci una configurazione diversa, elimina la chiave KMS e creane una nuova.

Puoi trovare la configurazione crittografica delle chiavi KMS, includere la specifica della chiave, l'utilizzo della chiave e gli algoritmi di crittografia o firma supportati nella console AWS KMS o utilizzando l'API AWS KMS. Per informazioni dettagliate, vedi Individuazione di chiavi KMS asimmetriche.

Nella console AWS KMS la pagina dei dettagli di ogni chiave KMS include una tab Configurazione crittografica in cui sono visualizzati i dettagli crittografici relativi alle chiavi KMS. Ad esempio, l'immagine che segue mostra la tab Configurazione crittografica di una chiave KMS RSA utilizzata per la firma e la verifica.

La scheda Cryptographic configuration (Configurazione crittografica) per determinate chiavi KMS per scopi speciali contiene sezioni specializzate aggiuntive. Ad esempio, la scheda Cryptographic configuration (Configurazione crittografica) per una chiave KMS in un archivio delle chiavi personalizzate contiene una sezione Custom key stores (Archivi delle chiavi personalizzate). La scheda Cryptographic configuration (Configurazione crittografica) per una chiave KMS in un archivio delle chiavi esterne contiene una sezione External key (Chiave esterna).



Nell'AWS KMSAPI, usa l'DescribeKeyoperazione. La struttura `KeyMetadata` nella risposta include la configurazione crittografica della chiave KMS. `DescribeKey`, ad esempio, restituisce la seguente risposta per una chiave KMS RSA utilizzata per la firma e la verifica.

```
{
  "KeyMetadata": {

    "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "AWSAccountId": "111122223333",
    "CreationDate": 1571767572.317,
    "CustomerMasterKeySpec": "RSA_2048",
    "Description": "",
    "Enabled": true,
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "KeyManager": "CUSTOMER",
    "KeyState": "Enabled",
    "MultiRegion": false,
    "Origin": "AWS_KMS",
    "KeySpec": "RSA_2048",
    "KeyUsage": "SIGN_VERIFY",
    "SigningAlgorithms": [
        "RSASSA_PKCS1_V1_5_SHA_256",
        "RSASSA_PKCS1_V1_5_SHA_384",
        "RSASSA_PKCS1_V1_5_SHA_512",
        "RSASSA_PSS_SHA_256",
        "RSASSA_PSS_SHA_384",
        "RSASSA_PSS_SHA_512"
    ]
  }
}
```

Individuazione dell'ID e dell'ARN della chiave

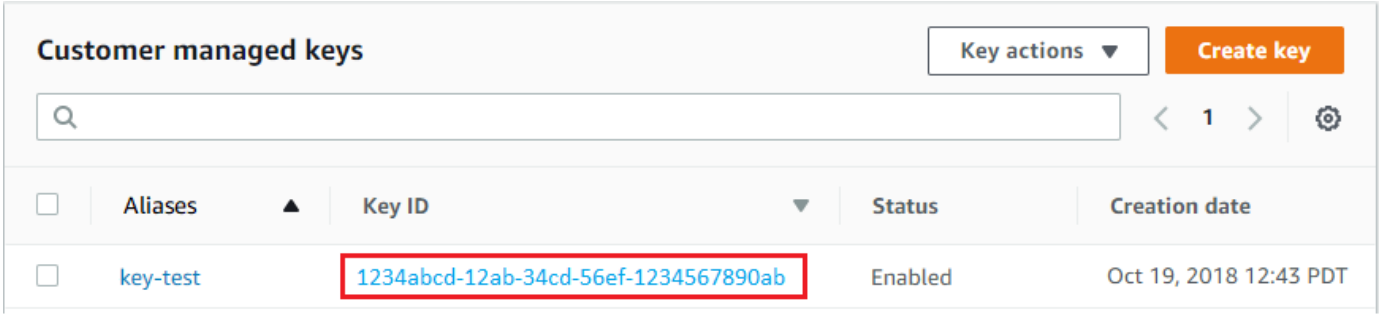
Per identificare una AWS KMS key, puoi utilizzare l'ID chiave o l'Amazon Resource Name (ARN della chiave). Nelle operazioni di crittografia, puoi anche utilizzare il nome alias o l'ARN dell'alias.

Per informazioni dettagliate sugli identificatori della chiave KMS supportati da AWS KMS, consulta Identificatori chiave () KeyId. Per informazioni sulla ricerca di un nome alias e di un alias ARN, consulta Individuazione del nome e dell'ARN dell'alias.

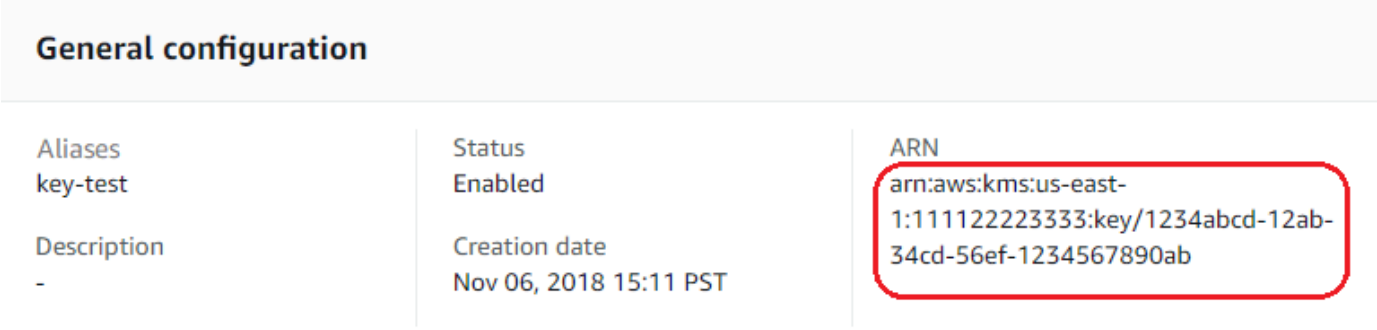
Per trovare l'ID e l'ARN della chiave (console)

1. Aprire la console AWS KMS all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il selettore della regione nell'angolo superiore destro della pagina.
3. Per visualizzare le chiavi nell'account creato e gestito dall'utente, nel riquadro di navigazione, seleziona Chiavi gestite dal cliente. Per visualizzare le chiavi nell'account creato e gestito per te da AWS, nel riquadro di navigazione, seleziona AWS chiavi gestite dal cliente.
4. Per trovare l'ID chiave per una chiave KMS, esamina la riga che inizia con l'alias della chiave KMS.

   La colonna Key ID (ID chiave) viene visualizzata nelle tabelle per impostazione predefinita. Se la colonna ID chiave non viene visualizzata nella tabella, utilizzare la procedura descritta in the section called “Personalizzazione delle tabelle delle chiavi KMS” per ripristinarla. È inoltre possibile visualizzare l'ID chiave di una chiave KMS nella relativa pagina dei dettagli.



5. Per trovare l'Amazon Resource Name (ARN) della chiave KMS, scegli l'alias o l'ID chiave. L'ARN della chiave viene visualizzato nella sezione General Configuration (Configurazione generale).



Individuazione dell'ID e dell'ARN della chiave (API AWS KMS)

Per trovare l'ID della chiave e l'ARN della chiave di anAWS KMS key, utilizzare l'ListKeysoperazione. Per esempi in più linguaggi di programmazione, consulta Ottenimento degli ID e degli ARN delle chiavi e Ottenimento degli ID e degli ARN delle chiavi.

La risposta di `ListKeys` include l'ID e l'ARN della chiave per ogni chiave KMS nell'account e nella regione.

```
$ aws kms list-keys
{
    "Keys": [
        {
            "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
            "KeyArn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        },
        {
            "KeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
            "KeyArn": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321"
        }
    ]
}
```

Individuazione del nome e dell'ARN dell'alias

Un alias è un nome intuitivo per una AWS KMS AWS KMS keys (chiave KMS). Puoi trovare il nome alias e alias ARN nella console AWS KMS nell'API AWS KMS.

Per informazioni dettagliate sugli identificatori della chiave KMS supportati da AWS KMS, consulta Identificatori chiave () KeyId. Per informazioni su come individuare l'ID e l'ARN della chiave, consulta Individuazione dell'ID e dell'ARN della chiave.

Argomenti

- Individuazione del nome e dell'ARN dell'alias (console)
- Individuazione del nome e dell'ARN dell'alias (API AWS KMS)

Individuazione del nome e dell'ARN dell'alias (console)

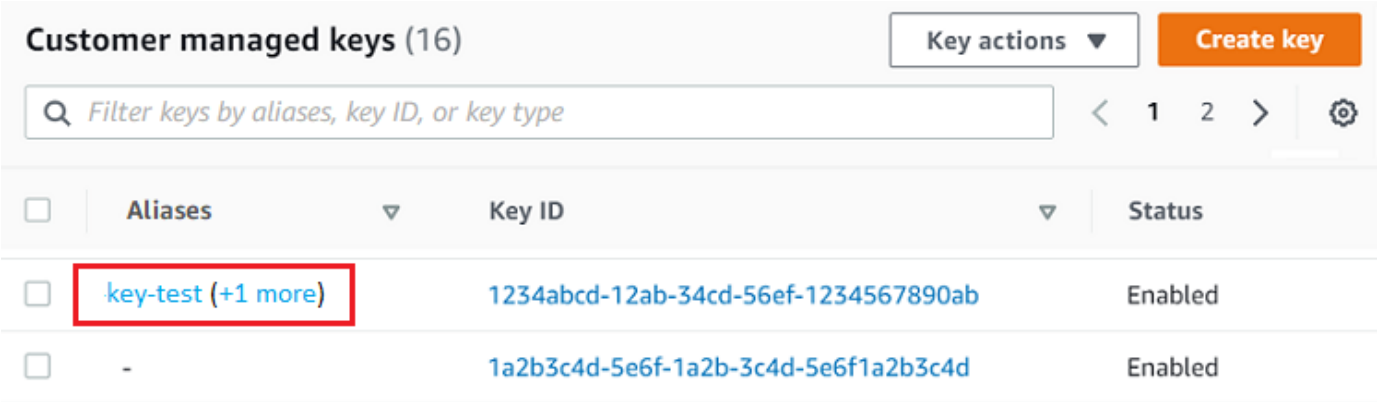
Nella console AWS KMS vengono mostrati i nomi alias associati alla chiave KMS.

1. Aprire la console AWS KMS all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il selettore della regione nell'angolo superiore destro della pagina.
3. Per visualizzare le chiavi nell'account creato e gestito dall'utente, nel riquadro di navigazione, seleziona Chiavi gestite dal cliente. Per visualizzare le chiavi nell'account creato e gestito per te da AWS, nel riquadro di navigazione, seleziona AWS chiavi gestite dal cliente.
4. La colonna Alias mostra l'alias per ogni chiave KMS. Se una chiave KMS non dispone di un alias, nella colonna Alias compare un trattino (-).

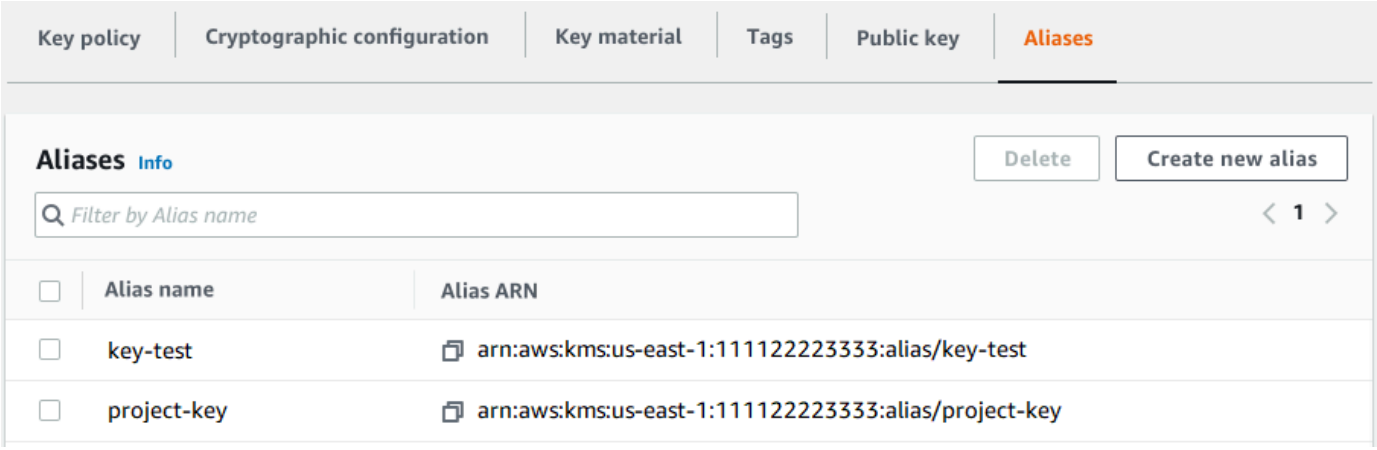
   Se una chiave KMS dispone di più alias, la colonna Alias ha anche un riepilogo degli alias, ad esempio (+n più). Ad esempio, la seguente chiave KMS ha due alias, uno dei quali è `key-test`.

   Per trovare il nome e l'ARN alias di tutti gli alias della chiave KMS, utilizza la scheda Alias.

   - Per andare direttamente alla scheda Alias, nella colonna Alias, scegli il riepilogo degli alias (+n più). Un riepilogo degli alias viene mostrato solo se la chiave KMS contiene più di un alias.
   - In alternativa, scegliere l'ID chiave o alias della chiave KMS (che apre la pagina dei dettagli della chiave KMS) e scegli la scheda Alias. Le schede si trovano sotto la sezione Configurazione generale.



5. La scheda Alias mostra il nome alias e l'ARN dell'alias di tutti gli alias per una chiave KMS. In questa scheda puoi anche creare ed eliminare alias per la chiave KMS.



Individuazione del nome e dell'ARN dell'alias (API AWS KMS)

Per trovare il nome dell'alias e l'alias ARN di anAWS KMS key, utilizzare l'operazione. ListAliases Per esempi in più linguaggi di programmazione, consulta Elenco degli alias e Ottenimento di nomi e ARN degli alias.

Per impostazione predefinita, la risposta include il nome e l'ARN di ogni alias nell'account e nella regione. Per ottenere solo gli alias per una determinata chiave KMS utilizza il parametro `KeyId`.

Ad esempio, il comando seguente ottiene solo gli alias per una chiave KMS di esempio con ID chiave `1234abcd-12ab-34cd-56ef-1234567890ab`.

```
$ aws kms list-aliases --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
{
    "Aliases": [
        {
            "AliasName": "alias/key-test",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/key-test",
            "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
            "CreationDate": 1593622000.191,
            "LastUpdatedDate": 1593622000.191
        },
        {
            "AliasName": "alias/project-key",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/project-key",
            "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
            "CreationDate": 1516435200.399,
            "LastUpdatedDate": 1516435200.399
        }
```

```
    ]
}
```

Modifica delle chiavi

È possibile modificare le seguenti proprietà delle chiavi gestite dal cliente nella console AWS KMS e utilizzando l'API AWS KMS.

Non è possibile modificare alcuna proprietà di Chiavi gestite da AWS o Chiavi di proprietà di AWS. Queste chiavi sono gestite dai servizi AWS che li hanno creati.

Descrizione

È possibile modificare la descrizione della chiave gestita dal cliente nella pagina dei dettagli della chiave KMS o utilizzando l'UpdateKeyDescriptionoperazione.

Per modificare la descrizione della chiave nella console, nell'angolo in alto a destra della pagina dei dettagli della chiave delle chiavi, seleziona Modifica.

Policy delle chiavi

È possibile modificare la politica chiave nella scheda Politica chiave della pagina dei dettagli della chiave gestita dal cliente o utilizzando l'PutKeyPolicyoperazione.

Per informazioni dettagliate, vedi Modifica di una policy delle chiavi.

Tag

Puoi creare ed eliminare i tag nella pagina Customer managed keys (chiavi gestite dal cliente) della console AWS KMS o nella scheda Tags (tag) della pagina dei dettagli della chiave gestita dal cliente. Oppure puoi utilizzare le UntagResourceoperazioni TagResourceand.

Per informazioni dettagliate, vedi Chiavi di tagging.

Abilitare e disabilitare

Puoi creare ed eliminare i tag nella pagina Customer managed keys (chiavi gestite dal cliente) della console AWS KMS o nella scheda Tags (tag) della pagina dei dettagli della chiave gestita dal cliente. Oppure puoi usare le DisableKeyoperazioni EnableKeyand.

Per informazioni dettagliate, vedi Abilitazione e disabilitazione delle chiavi.

Rotazione automatica delle chiavi

È possibile abilitare e disabilitare la rotazione automatica dei tasti nella scheda Rotazione dei tasti della pagina dei dettagli della chiave gestita dal cliente o utilizzando le DisableKeyRotationoperazioni EnableKeyRotationand.

Per informazioni dettagliate, vedi Rotazione delle AWS KMS keys.

Consulta anche

Aggiornamento degli alias

Chiavi di tagging

In AWS KMS puoi aggiungere tag a una chiave gestita dal cliente quando crei la chiave KMS e aggiungi o modifichi tag nelle chiavi KMS esistenti, a meno che non siano in attesa di eliminazione. Non puoi applicare tag agli alias, agli archivi delle chiavi personalizzate, a Chiavi gestite da AWS,a Chiavi di proprietà di AWS o a chiavi KMS in altriAccount AWS. I tag sono opzionali, ma possono essere molto utili.

Per ulteriori informazioni, consultare Creazione di chiavi e Modifica delle chiavi. Per informazioni generali sui tag, incluse le procedure consigliate, le strategie di tagging e il formato e la sintassi dei tag, consulta Tagging di risorse AWS nella Riferimenti generali di Amazon Web Services.

Argomenti

- Informazioni sui tag in AWS KMS
- Gestione dei tag delle chiavi KMS nella console
- Gestione dei tag delle chiavi KMS con operazioni API
- Controllo dell’accesso ai tag
- Utilizzo dei tag per controllare l'accesso alle chiavi KMS

Informazioni sui tag in AWS KMS

Un tag è un'etichetta di metadati che puoi assegnare (o AWS può assegnare) a una risorsa AWS. Ogni tag è costituito da una chiave di tag e da un valore di tag, entrambe le stringhe fanno distinzione tra maiuscole e minuscole. Il valore di tag può essere una stringa vuota (null). Ogni tag di una risorsa

deve avere una chiave di tag diversa, ma puoi aggiungere lo stesso tag a più risorse AWS. Ogni risorsa può avere fino a 50 tag creati dall'utente.

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

In AWS KMS puoi aggiungere tag a una chiave gestita dal cliente quando crei la chiave KMS e aggiungi o modifichi tag nelle chiavi KMS esistenti, a meno che non siano in attesa di eliminazione. Non puoi applicare tag agli alias, agli archivi delle chiavi personalizzate, a Chiavi gestite da AWS, a Chiavi di proprietà di AWS o a chiavi KMS in altriAccount AWS. I tag sono opzionali, ma possono essere molto utili.

Ad esempio, puoi aggiungere un tag `"Project"="Alpha"` a tutte le chiavi KMS e ai bucket di Amazon S3 utilizzati per il progetto Alpha.

```
TagKey   = "Project"
TagValue = "Alpha"
```

Per informazioni generali sui tag, inclusi il formato e la sintassi, consulta Tagging di risorse AWS nella Riferimenti generali di Amazon Web Services.

I tag consentono di eseguire le seguenti operazioni:

- Identificare e organizzare le risorse AWS. Molti servizi AWS supportano l'assegnazione di tag, perciò è possibile assegnare lo stesso tag a risorse di diversi servizi per indicare che queste sono correlate. Ad esempio, puoi assegnare lo stesso tag a una chiave KMS e un volume Amazon Elastic Block Store (Amazon EBS) o un AWS Secrets Manager segreto. Puoi inoltre utilizzare i tag per identificare le chiavi KMS per l'automazione.
- Tenere traccia dei costi AWS. Quando aggiungi i tag alle risorse AWS, AWS genera un report di allocazione dei costi in cui l'utilizzo e i costi sono aggregati in base ai tag. Puoi utilizzare questa funzione per monitorare i costi di AWS KMS relativi a un progetto, a un'applicazione o a un centro di costo.

  Per ulteriori informazioni sull'utilizzo dei tag per l'allocazione dei costi, consulta Uso dei tag per l'allocazione dei costi nella Guida per l'utente di AWS Billing. Per informazioni sulle regole che si applicano alle chiavi dei tag e ai valori dei tag, consulta Limitazioni per i tag definiti dall'utente nella Guida per l'utente di AWS Billing.
- Controllare l'accesso alle risorse di AWS. Consentire e negare l'accesso alle chiavi KMS in base ai relativi tag fa parte di supporto AWS KMS per Controllo degli accessi basato sugli attributi

(ABAC). Per ulteriori informazioni sul controllo dell'accessoa AWS KMS keys basato su tag, consulta Utilizzo dei tag per controllare l'accesso alle chiavi KMS. Per ulteriori informazioni generali sull'utilizzo dei tag per controllare l'accesso alle risorse AWS, consulta Controllo dell'accesso alle risorse AWS utilizzando i tag di risorsa nella Guida per l'utente di IAM.

AWS KMSscrive una voce nel AWS CloudTrail registro quando si utilizzano le ListResourceTagsoperazioni TagResourceUntagResource, o.

Gestione dei tag delle chiavi KMS nella console

Puoi aggiungere tag a una chiave KMS quando crei la chiave KMS nella console AWS KMS. È possibile utilizzare anche la scheda Tag nella console per aggiungere, modificare ed eliminare tag nelle chiavi gestite dal cliente Per aggiungere, modificare, visualizzare ed eliminare tag per una chiave KMS, è necessario disporre delle autorizzazioni necessarie. Per informazioni dettagliate, vedi Controllo dell'accesso ai tag.

Aggiungere tag durante la creazione di una chiave KMS

Per aggiungere tag durante la creazione di una chiave KMS nella console, è necessario disporre dell'autorizzazione `kms:TagResource` in una policy IAM, oltre alle autorizzazioni necessarie per creare chiavi KMS e visualizzare le chiavi KMS nella console. Come minimo, l'autorizzazione deve coprire tutte le chiavi KMS nell'account e nella regione.

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente. (Non è possibile gestire i tag di una Chiave gestita da AWS)
4. Scegli il tipo di chiave, quindi scegli Next (Successivo).
5. Immetti un alias e una descrizione opzionale.
6. Inserisci una chiave di tag e un valore di tag opzionale. Per aggiungere altri tag, scegli Aggiungi nuovo tag. Per rimuovere un tag, scegli Remove (Rimuovi). Al termine dell'applicazione dei tag alla nuova chiave KMS, scegli Successivo.
7. Completa la creazione della chiave KMS.

Visualizzare e gestire i tag nelle chiavi KMS esistenti

Per aggiungere, visualizzare, modificare ed eliminare tag nella console, è necessaria l'autorizzazione a taggare nella chiave di KMS. È possibile ottenere questa autorizzazione dalla policy delle chiavi per la chiave KMS o, se la policy delle chiavi lo consente, da una policy IAM che include la chiave KMS. Queste autorizzazioni sono necessarie oltre alle autorizzazioni per visualizzare le chiavi KMS nella console.

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente. (Non è possibile gestire i tag di una Chiave gestita da AWS)
4. È possibile utilizzare il filtro tabella per visualizzare solo le chiavi KMS con tag specifici. Per informazioni dettagliate, vedi Ordinamento e filtraggio delle tue chiavi KMS.
5. Seleziona la casella di controllo accanto all'alias di una chiave KMS.
6. Scegliere Key actions (Operazioni sulle chiavi), Add or edit tags (Aggiungi o modifica tag).
7. Nella pagina dei dettagli della chiave KMS scegli la scheda Tag.

   - Per creare il primo tag, scegli Crea tag, digita una chiave di tag (obbligatorio) e il valore di tag (opzionale), quindi scegli Salva.

     Se lasci vuoto il valore del tag, il valore effettivo del tag è una stringa nulla o vuota.
   - Per aggiungere un tag, scegli Modifica, scegli Aggiungi tag, digita una chiave di tag e il valore di tag, quindi scegli Salva.
   - Per modificare il nome o il valore di un tag, scegliere Edit (Modifica), apportare le modifiche, quindi scegliere Save (Salva).
   - Per eliminare un tag, scegliere Edit (Modifica). Nell riga del tag, scegliere Remove (Rimuovi), quindi Save (Salva).
8. Per salvare le modifiche, scegliere Save changes (Salva modifiche).

Gestione dei tag delle chiavi KMS con operazioni API

Puoi utilizzare l'API AWS Key Management Service (AWS KMS) per aggiungere, eliminare ed elencare i tag per le chiavi KMS che gestisci. Questi esempi utilizzano la AWS Command Line

Interface (AWS CLI), ma puoi usare anche qualsiasi linguaggio di programmazione supportato. Non puoi applicare tag a Chiavi gestite da AWS.

Per aggiungere, modificare, visualizzare ed eliminare i tag per una chiave KMS, è necessario disporre delle autorizzazioni necessarie. Per informazioni dettagliate, vedi Controllo dell'accesso ai tag.

Argomenti

- CreateKey: aggiungi tag a una nuova chiave KMS
- TagResource: aggiungi o modifica i tag per una chiave KMS
- ListResourceTags: Ottieni i tag per una chiave KMS
- UntagResource: elimina i tag da una chiave KMS

CreateKey: aggiungi tag a una nuova chiave KMS

Puoi aggiungere tag quando crei una chiave gestita dal cliente. Per specificare i tag, utilizza il `Tags` parametro dell'CreateKeyoperazione.

Per aggiungere tag durante la creazione di una chiave KMS, il chiamante deve disporre di autorizzazione `kms:TagResource` in una policy IAM. Come minimo, l'autorizzazione deve coprire tutte le chiavi KMS nell'account e nella regione. Per informazioni dettagliate, vedi Controllo dell'accesso ai tag.

Il valore del parametro `Tags` di `CreateKey` è una raccolta di coppie di chiave di tag e valore di tag per cui si applica la distinzione tra maiuscole e minuscole. Ogni tag in una chiave KMS deve avere un nome di tag diverso. Il valore di tag può essere una stringa nulla o vuota.

Ad esempio, il seguente comando AWS CLI crea una chiave KMS di crittografia simmetrica con un tag `Project:Alpha`. Quando si specificano più coppie chiave-valore, utilizzare uno spazio per separare ciascuna coppia.

```
$ aws kms create-key --tags TagKey=Project,TagValue=Alpha
```

Quando questo comando ha esito positivo, restituisce un oggetto `KeyMetadata` con informazioni relative alla nuova chiave KMS. Tuttavia, `KeyMetadata` non include tag. Per ottenere i tag, usa l'ListResourceTagsoperazione.

TagResource: aggiungi o modifica i tag per una chiave KMS

L'TagResourceoperazione aggiunge uno o più tag a una chiave KMS. Non puoi utilizzare questa operazione per aggiungere o modificare tag in un Account AWS diverso.

Per aggiungere un tag, specifica una nuova chiave di tag e un valore di tag. Per modificare un tag, specifica una chiave di tag esistente e un nuovo valore di tag. Ogni tag in una chiave KMS deve avere un nome di tag diverso. Il valore di tag può essere una stringa nulla o vuota.

Ad esempio, il comando seguente aggiunge i tag **`Purpose`** e **`Department`** a una chiave KMS di esempio.

```
$ aws kms tag-resource \
        --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
        --tags TagKey=Purpose,TagValue=Pretest TagKey=Department,TagValue=Finance
```

Quando questo comando ha esito positivo, non restituisce alcun output. Per visualizzare i tag su una chiave KMS, usa l'ListResourceTagsoperazione.

Puoi inoltre usare TagResource per modificare il valore di un tag esistente. Per sostituire un valore di tag, specifica la stessa chiave di tag con un valore diverso.

Ad esempio, questo comando modifica il valore del tag `Purpose` da `Pretest` a `Test`.

```
$ aws kms tag-resource \
        --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
        --tags TagKey=Purpose,TagValue=Test
```

ListResourceTags: Ottieni i tag per una chiave KMS

L'ListResourceTagsoperazione ottiene i tag per una chiave KMS. Il parametro `KeyId` è obbligatorio. Non puoi utilizzare questa operazione per visualizzare i tag nelle chiavi KMS in un Account AWS diverso.

Ad esempio, il comando seguente restituisce i tag per una chiave KMS di esempio.

```
$ aws kms list-resource-tags --key-id 1234abcd-12ab-34cd-56ef-1234567890ab

  "Truncated": false,
  "Tags": [
      {
```

```
        "TagKey": "Project",
        "TagValue": "Alpha"
    },
    {
      "TagKey": "Purpose",
      "TagValue": "Test"
    },
    {
      "TagKey": "Department",
      "TagValue": "Finance"
    }
  ]
}
```

UntagResource: elimina i tag da una chiave KMS

L'UntagResourceoperazione elimina i tag da una chiave KMS. Per identificare i tag da eliminare, specifica le chiavi dei tag. Non puoi utilizzare questa operazione per eliminare tag dalle chiavi KMS in un Account AWS diverso.

Quando l'operazione `UntagResource` ha esito positivo non restituisce alcun output. Inoltre, se la chiave di tag specificata non viene trovata nella chiave KMS, non viene generata un'eccezione né restituita una risposta. Per confermare che l'operazione ha funzionato, usa l'ListResourceTagsoperazione.

Ad esempio, questo comando elimina il tag **`Purpose`** e il relativo valore dalla chiave KMS specificata.

```
$ aws kms untag-resource --key-id 1234abcd-12ab-34cd-56ef-1234567890ab --tag-keys
 Purpose
```

Controllo dell’accesso ai tag

Per aggiungere, visualizzare ed eliminare tag, nella console AWS KMS o utilizzando l'API, i principali necessitano di autorizzazioni di tagging. Puoi fornire queste autorizzazioni nelle policy delle chiavi. Puoi anche fornirli nelle policy IAM (incluse le Policy di endpoint VPC), ma solo se la policy delle chiavi lo consente. La policy AWSKeyManagementServicePowerUsergestita consente ai responsabili di etichettare, rimuovere i tag ed elencare i tag su tutte le chiavi KMS a cui l'account può accedere.

È inoltre possibile limitare queste autorizzazioni utilizzando le chiavi di condizione globali AWS per i tag. InAWS KMS, queste condizioni possono controllare l'accesso alle operazioni di etichettatura, come e. TagResourceUntagResource

> **Note**
>
> Presta attenzione quando concedi ai principali l'autorizzazione per gestire tag e alias. Modificando un tag o un alias puoi consentire o negare l'autorizzazione alla chiave gestita dal cliente. Per informazioni dettagliate, consulta ABAC per AWS KMS e Utilizzo dei tag per controllare l'accesso alle chiavi KMS.

Per esempi di policy e ulteriori informazioni, consulta Controllo dell'accesso in base alle chiavi di tag nella Guida per l'utente di IAM.

Le autorizzazioni per creare e gestire i tag funzionano come descritto di seguito.

km: TagResource

Consente ai principali di aggiungere o modificare tag. Per aggiungere tag durante la creazione di una chiave KMS, il principale deve disporre dell'autorizzazione in una policy IAM che non sia limitato a particolari chiavi KMS.

km: ListResourceTags

Consente ai principali di visualizzare i tag sulle chiavi KMS.

km: UntagResource

Consente ai principali di eliminare i tag dalle chiavi KMS.

Autorizzazioni ad assegnare tag nelle policy

Puoi fornire l'autorizzazione ad assegnare tag in una policy delle chiavi o in una policy IAM. Ad esempio, la policy delle chiavi di esempio riportata di seguito fornisce agli utenti selezionati l'autorizzazione di tag nella chiave KMS. Fornisce a tutti gli utenti che possono assumere l'esempio dei ruoli di Amministratore o Sviluppatore il permesso di visualizzare i tag.

```
{
  "Version": "2012-10-17",
  "Id": "example-key-policy",
  "Statement": [
    {
      "Sid": "Enable IAM User Permissions",
```

```
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Sid": "Allow all tagging permissions",
      "Effect": "Allow",
      "Principal": {"AWS": [
        "arn:aws:iam::111122223333:user/LeadAdmin",
        "arn:aws:iam::111122223333:user/SupportLead"
      ]},
      "Action": [
          "kms:TagResource",
          "kms:ListResourceTags",
          "kms:UntagResource"
      ],
      "Resource": "*"
    },
    {
      "Sid": "Allow roles to view tags",
      "Effect": "Allow",
      "Principal": {"AWS": [
        "arn:aws:iam::111122223333:role/Administrator",
        "arn:aws:iam::111122223333:role/Developer"
      ]},
      "Action": "kms:ListResourceTags",
      "Resource": "*"
    }
  ]
}
```

Per concedere ai principali l'autorizzazione ad assegnare tag su più chiavi KMS, è possibile utilizzare una policy IAM. Affinché questa policy sia efficace, la policy delle chiavi per ogni chiave KMS deve consentire all'account di utilizzare le policy IAM per controllare l'accesso alla chiave KMS.

Ad esempio, la policy IAM seguente consente ai principali di creare chiavi KMS. Consente inoltre di creare e gestire i tag su tutte le chiavi KMS nell'account specificato. Questa combinazione consente ai responsabili di utilizzare il parametro Tags dell'CreateKeyoperazione per aggiungere tag a una chiave KMS durante la creazione.

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Sid": "IAMPolicyCreateKeys",
      "Effect": "Allow",
      "Action": "kms:CreateKey",
      "Resource": "*"
    },
    {
      "Sid": "IAMPolicyTags",
      "Effect": "Allow",
      "Action": [
        "kms:TagResource",
        "kms:UntagResource",
        "kms:ListResourceTags"
      ],
      "Resource": "arn:aws:kms:*:111122223333:key/*"
    }
  ]
}
```

Limitazione delle autorizzazioni ad assegnare tag

È possibile limitare le autorizzazioni di assegnazione dei tag utilizzando Condizioni della policy. Le seguenti condizioni della policy possono essere applicate alle autorizzazioni `kms:TagResource` e `kms:UntagResource`. Ad esempio, è possibile utilizzare la condizione `aws:RequestTag/`*`tag-key`* per consentire a un principale di aggiungere solo tag specifici o impedire a un principale di aggiungere tag con chiavi tag particolari. In alternativa, è possibile utilizzare la condizione `kms:KeyOrigin` per impedire ai principali di assegnare o rimuovere tag dalle chiavi KMS con materiale della chiave importato.

- Leggi: RequestTag
- aws:ResourceTag/tag-key (solo politiche IAM)
- aws: TagKeys
- km: CallerAccount
- km: KeySpec
- km: KeyUsage
- km: KeyOrigin
- km: ViaService

Come best practice nell'utilizzo dei tag per controllare l'accesso alle chiavi KMS, è consigliabile utilizzare la chiave di condizione `aws:RequestTag/`*`tag-key`* o `aws:TagKeys` per determinare quali tag (o chiavi tag) sono consentiti.

Ad esempio, la seguente istruzione della policy IAM è simile a quella precedente. Tuttavia, questa policy consente ai principali di creare tag (`TagResource`) ed eliminare i tag `UntagResource` solo per i tag con chiave di tag `Project`.

Poiché `TagResource` le `UntagResource` richieste possono includere più tag, è necessario specificare un operatore `ForAllValues` or `ForAnyValue` set con la TagKeys condizione aws:. L'operatore `ForAnyValue` richiede che almeno una delle chiavi di tag nella richiesta corrisponda a una delle chiavi di tag nella policy. L'operatore `ForAllValues` richiede che tutte le chiavi di tag nella richiesta corrispondano a una delle chiavi di tag nella policy. L'`ForAllValues`operatore restituisce anche `true` se non ci sono tag nella richiesta, ma TagResource UntagResource fallisce quando non viene specificato alcun tag. Per dettagli sugli operatori del set, consulta Utilizzare più chiavi e valori nella Guida per l'utente di IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IAMPolicyCreateKey",
      "Effect": "Allow",
      "Action": "kms:CreateKey",
      "Resource": "*"
    },
    {
      "Sid": "IAMPolicyViewAllTags",
      "Effect": "Allow",
      "Action": "kms:ListResourceTags",
      "Resource": "arn:aws:kms:*:111122223333:key/*"
    },
    {
      "Sid": "IAMPolicyManageTags",
      "Effect": "Allow",
      "Action": [
        "kms:TagResource",
        "kms:UntagResource"
      ],
      "Resource": "arn:aws:kms:*:111122223333:key/*",
      "Condition": {
          "ForAllValues:StringEquals": {"aws:TagKeys": "Project"}
```

```
      }
    }
  ]
}
```

Utilizzo dei tag per controllare l'accesso alle chiavi KMS

È possibile controllare l'accesso a AWS KMS keys in base ai tag sulla chiave KMS. Ad esempio, è possibile scrivere una policy IAM che consenta ai principali di abilitare e disabilitare solo le chiavi KMS con un tag specifico. In alternativa, è possibile utilizzare una policy IAM per impedire ai principali di utilizzare le chiavi KMS nelle operazioni di crittografia a meno che la chiave KMS non disponga di un tag specifico.

Questa caratteristica fa parte di supporto AWS KMS per Controllo degli accessi basato sugli attributi (ABAC). Per informazioni sull'uso dei tag per controllare l'accesso a AWS, consulta Che cos'è ABAC per AWS? e Controllo dell'accesso alle risorse AWSmediante i tag delle risorse nella Guida per l'utente di IAM. Per informazioni sulla risoluzione dei problemi di accesso relativi a ABAC, vedi Risoluzione dei problemi ABAC per AWS KMS.

> **Note**
>
> Potrebbero essere necessari fino a cinque minuti per le modifiche di tag e alias per influenzare l'autorizzazione delle chiavi KMS. Le modifiche recenti potrebbero essere visibili nelle operazioni API prima che influiscano sull'autorizzazione.

AWS KMSsupporta la chiave di contesto della condizione globale aws:ResourceTag/tag-key, che consente di controllare l'accesso alle chiavi KMS in base ai tag sulla chiave KMS. Poiché più chiavi KMS possono avere lo stesso tag, questa caratteristica consente di applicare l'autorizzazione a un set selezionato di chiavi KMS. È inoltre possibile modificare facilmente le chiavi KMS nel set modificandone i tag.

Nello stato AWS KMS, la chiave di condizione `aws:ResourceTag/`*`tag-key`* è supportata solo nelle policy IAM. Non è supportato nelle politiche chiave, che si applicano solo a una chiave KMS, o nelle operazioni che non utilizzano una particolare chiave KMS, come le operazioni or. ListKeysListAliases

Il controllo dell'accesso con i tag offre un modo semplice, scalabile e flessibile per gestire le autorizzazioni. Tuttavia, se non è stata progettata e gestita correttamente, può consentire o negare

l'accesso alle chiavi KMS inavvertitamente. Se utilizzi tag per controllare l'accesso, prendi in considerazione le seguenti procedure.

- Utilizza i tag per rafforzare le best practice di Accesso meno privilegiato. Assegna ai principali IAM solo le autorizzazioni necessarie solo per quelle chiavi KMS che devono utilizzare o gestire. Ad esempio, utilizzare i tag per etichettare le chiavi KMS utilizzate per un progetto. Quindi concedere al team del progetto l'autorizzazione a utilizzare solo le chiavi KMS con il tag progetto.
- Fai attenzione a dare ai principali le autorizzazioni `kms:TagResource` e `kms:UntagResource` che consentono di aggiungere, modificare ed eliminare tag. Quando si utilizzano i tag per controllare l'accesso alle chiavi KMS, la modifica di un tag può concedere ai principali l'autorizzazione di utilizzare chiavi KMS che altrimenti non disponevano dell'autorizzazione. Può inoltre negare l'accesso alle chiavi KMS richieste da altre entità per svolgere il proprio lavoro. Gli amministratori delle chiavi che non dispongono dell'autorizzazione per modificare le policy delle chiavi o creare concessioni possono controllare l'accesso alle chiavi KMS se dispongono dell'autorizzazione per gestire i tag.

  Quando possibile, utilizzare una condizione della policy, ad esempio `aws:RequestTag/`*`tag-key`* o `aws:TagKeys` per limitare le autorizzazioni di un principale ad assegnare tag a particolari tag o modelli di tag su specifiche chiavi KMS.
- Esaminare i principali nel tuo Account AWS che attualmente dispongono di autorizzazioni per assegnare e rimuovere tag e modificarli, se necessario. Ad esempio, la console policy delle chiavi predefinita include autorizzazioni `kms:TagResource` e `kms:UntagResource` su quella chiave KMS. Le policy IAM possono consentire autorizzazioni ad assegnare e rimuovere tag per tutte le chiavi KMS. Ad esempio, la policy AWSKeyManagementServicePowerUsergestita consente ai responsabili di etichettare, rimuovere i tag ed elencare i tag su tutte le chiavi KMS.
- Prima di impostare una policy che dipende da un tag, esaminare i tag nelle chiavi KMS nel Account AWS. Assicurati che la tua policy si applichi solo ai tag che intendi includere. Usa CloudTrail i registri e gli CloudWatch allarmi per avvisarti delle modifiche ai tag che potrebbero influire sull'accesso alle tue chiavi KMS.
- Le condizioni delle policy basate su tag utilizzano la corrispondenza dei modelli; non sono legate a una particolare istanza di un tag. Una policy che utilizza chiavi di condizione basate su tag influisce su tutti i tag nuovi ed esistenti che corrispondono al modello. Se si elimina e si ricrea un tag che corrisponde a una condizione della policy, la condizione si applica al nuovo tag, proprio come quello precedente.

Ad esempio, considerare il seguente esempio di policy IAM. Consente ai responsabili di richiamare GenerateDataKeyWithoutPlaintexte decriptare le operazioni solo sulle chiavi KMS del tuo account che si trovano nella regione Asia Pacifico (Singapore) e dispongono di un tag. `"Project"="Alpha"` È possibile collegare questa policy ai ruoli nel progetto Alpha di esempio.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IAMPolicyWithResourceTag",
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:ap-southeast-1:111122223333:key/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Project": "Alpha"
        }
      }
    }
  ]
}
```

La seguente policy IAM di esempio consente al principale di utilizzare qualsiasi chiave KMS nell'account per le operazioni di crittografia. Ma vieta ai principali di utilizzare queste operazioni crittografiche sulle chiavi KMS con un tag `"Type"="Reserved"` o senza tag `"Type"`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IAMAllowCryptographicOperations",
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:GenerateDataKey*",
        "kms:Decrypt",
        "kms:ReEncrypt*"
      ],
      "Resource": "arn:aws:kms:*:111122223333:key/*"
```

```
    },
    {
      "Sid": "IAMDenyOnTag",
      "Effect": "Deny",
      "Action": [
        "kms:Encrypt",
        "kms:GenerateDataKey*",
        "kms:Decrypt",
        "kms:ReEncrypt*"
      ],
      "Resource": "arn:aws:kms:*:111122223333:key/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Type": "Reserved"
        }
      }
    },
    {
      "Sid": "IAMDenyNoTag",
      "Effect": "Deny",
      "Action": [
        "kms:Encrypt",
        "kms:GenerateDataKey*",
        "kms:Decrypt",
        "kms:ReEncrypt*"
      ],
      "Resource": "arn:aws:kms:*:111122223333:key/*",
      "Condition": {
        "Null": {
          "aws:ResourceTag/Type": "true"
        }
      }
    }
  ]
}
```

Abilitazione e disabilitazione delle chiavi

È possibile disabilitare e riabilitare le chiavi gestite del cliente. Quando crei una chiave KMS è abilitata per impostazione predefinita. Se disabiliti una chiave KMS, non può essere utilizzata in nessuna operazione di crittografia fino a quando non lo riabiliti.

Poiché è temporaneo e facilmente annullato, la disabilitazione di una chiave KMS è un'alternativa sicura all'eliminazione di una chiave KMS, un'operazione distruttiva e irreversibile. Se stai pensando di eliminare una chiave KMS, disattivala prima e imposta un CloudWatch allarme o un meccanismo simile per essere certo che non avrai mai bisogno di usare la chiave per decrittografare i dati crittografati.

Quando disabiliti una chiave KMS, diventa immediatamente inutilizzabile (in base alla coerenza finale). Tuttavia, le risorse crittografate con chiavi di dati protette dalla chiave KMS non sono interessate fino a quando la chiave KMS non viene nuovamente utilizzata, ad esempio per decrittografare la chiave dati. Questo problema riguarda i Servizi AWS, molti dei quali proteggono le risorse tramite le chiavi dati. Per informazioni dettagliate, vedi In che modo le chiavi KMS inutilizzabili influiscono sulle chiavi dati.

Non puoi abilitare o disabilitare Chiavi gestite da AWS o Chiavi di proprietà di AWS. Chiavi gestite da AWS sono abilitati in modo permanente per l'uso da servizi che utilizzano AWS KMS. Chiavi di proprietà di AWS sono gestiti esclusivamente dal servizio che li possiede.

> **Note**
>
> AWS KMS non ruota il materiale chiave delle chiavi gestite dal cliente quando sono disabilitate. Per ulteriori informazioni, consulta Come funziona la rotazione automatica delle chiavi.

Argomenti

- Abilitazione e disabilitazione delle chiavi KMS (console)
- Abilitazione e disabilitazione delle chiavi KMS (API AWS KMS)

Abilitazione e disabilitazione delle chiavi KMS (console)

Puoi utilizzare la console AWS KMS per abilitare e disabilitare le chiavi gestite dal cliente.

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.

4. Scegli la casella di controllo delle chiavi KMS che vuoi abilitare o disabilitare.
5. Per abilitare una chiave KMS, scegli Azioni chiave, Abilita. Per disabilitare una chiave KMS, scegli Azioni chiave, Disabilita.

Abilitazione e disabilitazione delle chiavi KMS (API AWS KMS)

L'EnableKeyoperazione abilita un dispositivo disabilitato. AWS KMS key Questi esempi utilizzano la AWS Command Line Interface (AWS CLI), ma puoi usare anche qualsiasi linguaggio di programmazione supportato. Il parametro `key-id` è obbligatorio.

Questa operazione non restituisce alcun output. Per visualizzare lo stato della chiave, utilizzare l'DescribeKeyoperazione.

```
$ aws kms enable-key --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

L'DisableKeyoperazione disabilita una chiave KMS abilitata. Il parametro `key-id` è obbligatorio.

```
$ aws kms disable-key --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

Questa operazione non restituisce alcun output. Per vedere lo stato della chiave, usa l'DescribeKeyoperazione e guarda il `Enabled` campo.

```
$ aws kms describe-key --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
{
    "KeyMetadata": {
        "Origin": "AWS_KMS",
        "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "Description": "",
        "KeyManager": "CUSTOMER",
        "MultiRegion": false,
        "Enabled": false,
        "KeyState": "Disabled",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "CreationDate": 1502910355.475,
        "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "AWSAccountId": "111122223333"
        "KeySpec": "SYMMETRIC_DEFAULT",
        "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "EncryptionAlgorithms": [
```

```
            "SYMMETRIC_DEFAULT"
        ]
    }
}
```

Rotazione delle AWS KMS keys

Per creare nuovo materiale crittografico per le chiavi gestite dal cliente, puoi creare nuove chiavi KMS e modificare le applicazioni o gli alias per utilizzarle. Oppure, puoi abilitare la rotazione della chiave automatica per una chiave KMS esistente.

Quando si abilita la rotazione automatica delle chiavi per una chiave KMS gestita dal cliente, AWS KMS genera nuovo materiale crittografico per la chiave KMS ogni anno. AWS KMS salva inoltre tutte le versioni precedenti del materiale crittografico in modo perpetuo cosicché tale materiale sia utilizzato per decrittare i dati crittografati con quella chiave KMS. AWS KMS non elimina alcun materiale chiave ruotato finché non si elimina la chiave KMS. Puoi monitorare la rotazione del materiale chiave per le tue chiavi KMS in Amazon CloudWatch eAWS CloudTrail.

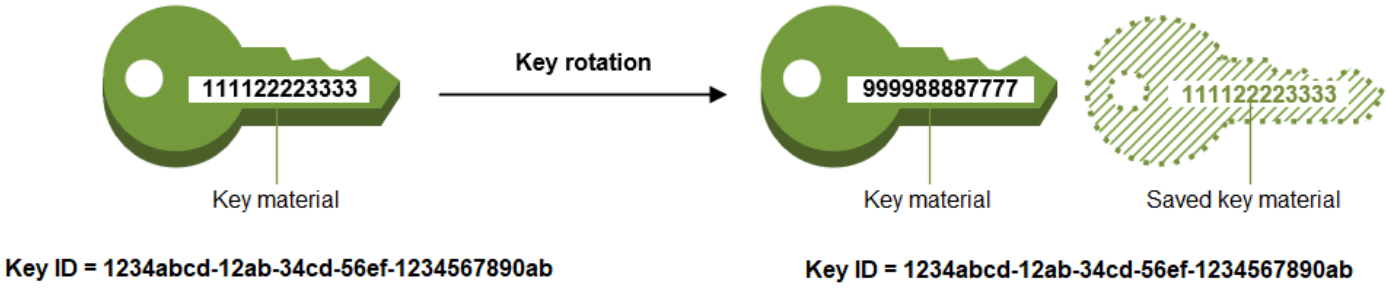
Quando si utilizza una chiave KMS ruotata per la crittografia dei dati, AWS KMS usa il materiale chiave corrente. Quando utilizzi la chiave KMS ruotata per decrittografare il testo cifrato, AWS KMS usa la stessa versione del materiale della chiave utilizzata per la crittografia. Non è possibile richiedere una versione particolare del materiale chiave. Poiché AWS KMS esegue la decrittografia in modo trasparente con il materiale della chiave appropriato, puoi utilizzare in tutta sicurezza una chiave KMS ruotata nelle applicazioni e nei Servizi AWS senza modifiche al codice.

Tuttavia, la rotazione automatica delle chiavi non ha effetto sui dati che la chiave KMS protegge. Non ruota le chiavi di dati che la chiave KMS ha generato né crittografa nuovamente i dati protetti dalla chiave KMS e non mitiga l'effetto di una chiave di dati compromessa.

AWS KMS supporta la rotazione automatica delle chiavi solo per le chiavi KMS di crittografia simmetrica con materiale della chiave creato da AWS KMS. La rotazione automatica è facoltativa per le chiavi KMS gestite dal cliente. AWS KMS ruota sempre il materiale della chiave per le chiavi KMS gestite da AWS ogni anno. La rotazione delle chiavi KMS di proprietà di AWSvaria.

> **Note**
>
> L'intervallo di rotazione per le Chiavi gestite da AWS è cambiato a maggio 2022. Per informazioni dettagliate, vedi Chiavi gestite da AWS.

La rotazione della chiave modifica solo il materiale della chiave, cioè il segreto crittografico utilizzato nelle operazioni di crittografia. La chiave KMS è la stessa risorsa logica, indipendentemente dal fatto o dal numero di volte che supporta le modifiche del materiale chiave. Le proprietà della chiave KMS non vengono modificate, come illustrato nella seguente immagine.



La rotazione automatica delle chiavi ha i seguenti vantaggi:

- Le proprietà della , tra cui l'ID chiave, l'ARN chiave, la Regione, le policy e le autorizzazioni, non cambiano quando la chiave viene ruotata.
- Non è necessario modificare le applicazioni o gli alias che fanno riferimento all'ID o all'ARN della chiave KMS.
- La rotazione del materiale della chiave non influisce sull'uso della chiave KMS in nessun Servizio AWS.
- Quando abiliti la rotazione delle chiavi, AWS KMS ruota la chiave KMS automaticamente ogni anno. Non devi ricordare o pianificare l'aggiornamento.

Potresti decidere di creare una nuova chiave KMS e di utilizzarla al posto della chiave KMS originale. Lo stesso risultato si ottiene ruotando il materiale della chiave in una chiave KMS esistente, quindi questa operazione viene spesso considerata come una rotazione manuale della chiave. La rotazione manuale è una buona scelta per controllare il programma di rotazione delle chiavi. Inoltre, fornisce un modo per ruotare le chiavi KMS che non sono idonee per la rotazione automatica delle chiavi, incluse le chiavi KMS asimmetriche, le chiavi KMS HMAC, le chiavi KMS negli archivi delle chiavi personalizzate e le chiavi KMS con materiale della chiave importato.

Rotazione delle chiave e prezzi

AWS KMS addebita una tariffa mensile per ogni versione del materiale della chiave mantenuto per la chiave KMS. Per informazioni dettagliate, consulta Prezzi di AWS Key Management Service.

> **Note**
>
> Puoi utilizzare il AWS Cost Explorer Service per visualizzare un dettaglio dei costi di archiviazione delle chiavi. Ad esempio, puoi filtrare la vista per visualizzare i costi totali per le chiavi fatturate come chiavi KMS correnti e ruotate specificando `$REGION-KMS-Keys` per Tipo di utilizzo e raggruppando i dati in base a Operazione API.
> Potresti ancora visualizzare le istanze dell'operazione dell'API con legacy `Unknown` per le date nella cronologia.

Rotazione delle chiavi e quote

Quando si calcolano le quote di risorse chiave, ogni chiave KMS conta come una chiave indipendentemente dal numero di versioni del materiale chiave ruotato.

Per informazioni più dettagliate sul materiale chiave e sulla rotazione, consultare Dettagli di crittografia di AWS Key Management Service.

Argomenti

Perché ruotare le chiavi KMS?

Le procedure crittografiche consigliate scoraggiano il riutilizzo estensivo delle chiavi che eseguono la crittografia dei dati direttamente, ad esempio le chiavi di dati generate da AWS KMS. Quando eseguono la crittografia di milioni di messaggi, le chiavi dati a 256 bit possono esaurirsi e iniziare a produrre testo criptato con trame sottili che possono essere sfruttate da abili malintenzionati per individuare i bit delle chiavi. Per evitare questo esaurimento delle chiavi, è preferibile utilizzare le chiavi di dati solo una volta o poche volte, in modo da ruotare efficacemente il materiale delle chiavi.

Tuttavia, le chiavi KMS vengono spesso utilizzate per lo più come chiavi di wrapping, note anche come chiavi di crittografia delle chiavi. Invece di crittografare i dati, le chiavi di wrapping eseguono la crittografia delle chiavi di dati che eseguono a loro volta la crittografia dei tuoi dati. Per tale motivo,

vengono utilizzate molto meno spesso delle chiavi di dati e non vengono quasi mai riutilizzate abbastanza da rischiare l'esaurimento delle chiavi.

Anche se questo rischio di esaurimento è bassissimo, potrebbe essere necessario ruotare le chiavi KMS a causa di regole aziendali/contrattuali o norme governative. Quando bisogna ruotare le chiavi KMS, è consigliabile utilizzare la rotazione automatica dei tasti, laddove è supportata, e la rotazione manuale delle chiavi, qualora la rotazione automatica delle chiavi non fosse supportata.

Come funziona la rotazione automatica delle chiavi

La rotazione delle chiavi in AWS KMS è progettata in modo da essere trasparente e facile da utilizzare. AWS KMS supporta la rotazione automatica delle chiavi opzionale solo per le chiavi gestite dal cliente.

Gestione del materiale chiave

AWS KMS conserva tutto il materiale chiave di una chiave KMS, anche se la rotazione della chiave è disattivata. AWS KMS elimina il materiale chiave solo quando si elimina la chiave KMS.

Utilizzo del materiale chiave

Quando si utilizza una chiave KMS ruotata per la crittografia dei dati, AWS KMS usa il materiale chiave corrente. Quando si utilizza la chiave KMS ruotata per decrittare il testo cifrato, AWS KMS usa la stessa versione del materiale chiave utilizzata per la crittografia. Non è possibile richiedere una versione particolare del materiale chiave.

Data di rotazione

AWS KMS ruota il materiale della chiave un anno (circa 365 giorni) dopo l'abilitazione della rotazione e, successivamente, ogni anno a seguire (circa 365 giorni).

Chiavi gestite dal cliente

Siccome la rotazione automatica delle chiavi è facoltativa nelle chiavi gestite dal cliente e può essere abilitata e disabilitata in qualunque momento, la data di rotazione dipende dalla data dell'ultima abilitazione. Tale data può cambiare molte volte nel corso della vita della chiave.

Ad esempio, se crei una chiave gestita dal cliente il 1° gennaio 2022 e abiliti la rotazione automatica delle chiavi il 15 marzo 2022, AWS KMS ruota il materiale della chiave il 15 marzo 2023, il 15 marzo 2024 e, successivamente, ogni 365 giorni.

Di seguito sono riportati alcuni casi particolari:

- Disabilitazione della rotazione delle chiavi: se disabiliti la rotazione automatica delle chiavi in un determinato momento, la chiave KMS continua a utilizzare la versione del materiale della chiave che utilizzava quando la rotazione era disabilitata. Quando abiliti (o riabiliti) la rotazione automatica delle chiavi, AWS KMS ruota il materiale della chiave un anno dopo la data di abilitazione della rotazione e, successivamente, ogni anno (circa 365 giorni).
- Chiavi KMS disabilitate: quando una chiave KMS è disabilitata, non viene ruotata da AWS KMS. Tuttavia, lo stato della rotazione della chiave non cambia e non è possibile modificarlo quando la chiave KMS è disattivata. Quando la chiave KMS viene nuovamente abilitata, se il materiale della chiave ha più di un anno, AWS KMS la ruota immediatamente e successivamente ogni anno. Se il materiale della chiave ha meno di un anno, AWS KMS riprende il programma di rotazione originale della chiave.
- Chiavi KMS in attesa di eliminazione: quando una chiave KMS è in attesa di eliminazione, non viene ruotata da AWS KMS. Lo stato di rotazione della chiave è impostato su `false` e non è possibile modificarlo quando l'eliminazione è in sospeso. Se l'eliminazione è stata annullata, viene ripristinato il precedente stato di rotazione della chiave. Se il materiale della chiave ha più di un anno, AWS KMS la ruota immediatamente e successivamente ogni anno (circa 365 giorni dall'ultima rotazione). Se il materiale della chiave ha meno di un anno, AWS KMS riprende il programma di rotazione originale della chiave.

Chiavi gestite da AWS

AWS KMS ruota automaticamente le Chiavi gestite da AWS ogni anno (circa 365 giorni). Non è possibile abilitare o disabilitare la rotazione delle chiavi per le Chiavi gestite da AWS.

Il materiale della chiave per una Chiave gestita da AWS viene ruotato per la prima volta un anno dopo la data di creazione e successivamente ogni anno (circa 365 giorni dall'ultima rotazione).

> **Note**
>
> A maggio 2022, AWS KMS ha modificato il programma di rotazione delle Chiavi gestite da AWS passando da ogni tre anni (circa 1.095 giorni) a ogni anno (circa 365 giorni).
> Le nuove Chiavi gestite da AWS vengono ruotate automaticamente un anno dopo la loro creazione e successivamente all'incirca ogni anno.
> Le Chiavi gestite da AWS esistenti vengono ruotate automaticamente un anno dopo l'ultima rotazione e successivamente ogni anno.

Chiavi di proprietà di AWS

Non è possibile abilitare o disabilitare la rotazione delle chiavi per le Chiavi di proprietà di AWS. La strategia di rotazione delle chiavi per una Chiave di proprietà di AWS è determinata dal servizio AWS che crea e gestisce la chiave. Per informazioni dettagliate, consulta l'argomento Crittografia dei dati inattivi nella guida per l'utente o nella guida per gli sviluppatori del servizio.

Tipi di chiavi KMS supportati

La rotazione automatica delle chiavi è supportata solo per le chiavi KMS di crittografia simmetrica con materiale della chiave generato da AWS KMS (origine = AWS_KMS).

La rotazione automatica delle chiavi non è supportata nei seguenti tipi di chiavi KMS, che tuttavia possono essere ruotate manualmente.

- Chiavi KMS asimmetriche
- Chiavi KMS HMAC
- Chiavi KMS nell'archivio delle chiavi personalizzate
- Chiavi KMS con materiale chiave importato

Chiavi multi-regione

Puoi abilitare e disabilitare la rotazione automatica delle chiavi per le chiavi multiregione. È possibile impostare la proprietà solo sulla chiave primaria. Quando AWS KMS sincronizza le chiavi, copia l'impostazione della proprietà dalla chiave primaria alle chiavi di replica. Quando il materiale chiave della chiave primaria viene ruotato, AWS KMS copia automaticamente il materiale chiave in tutte le relative chiavi di replica. Per informazioni dettagliate, vedi Rotazione di chiavi multiregione.

Servizi AWS

Puoi abilitare la rotazione automatica delle chiavi per le chiavi gestite dal cliente utilizzate per la crittografia lato server nei servizi AWS. La rotazione annuale è trasparente e compatibile con i servizi AWS.

Monitoraggio della rotazione delle chiavi

Quando ruota AWS KMS automaticamente il materiale chiave per una chiave Chiave gestita da AWSo una chiave gestita dal cliente, scrive un `KMS CMK Rotation` evento su Amazon EventBridge e un RotateKey evento nel tuo AWS CloudTrail registro. Puoi utilizzare questi record per verificare che la chiave KMS sia stata ruotata.

Consistenza finale

La rotazione automatica delle chiavi è soggetta agli stessi effetti di consistenza finale delle altre operazioni di gestione AWS KMS. Potrebbe esserci un leggero ritardo prima che il nuovo materiale chiave sia disponibile in AWS KMS. Tuttavia, la rotazione del materiale chiave non causa alcuna interruzione o ritardo nelle operazioni di crittografia. Il materiale chiave corrente viene utilizzato nelle operazioni di crittografia fino a quando il nuovo materiale chiave non è disponibile in AWS KMS. Quando il materiale chiave per una chiave multiregione viene ruotato automaticamente, AWS KMS utilizza il materiale chiave corrente fino a quando il nuovo materiale chiave non è disponibile in tutte le Regioni con una chiave multiregione correlata.

Come abilitare e disabilitare la rotazione automatica delle chiavi

Gli utenti autorizzati possono utilizzare la console AWS KMS o l'API AWS KMS per abilitare e disabilitare la rotazione automatica delle chiavi e visualizzare lo stato della rotazione delle chiavi.

Quando abiliti la rotazione automatica delle chiavi, AWS KMS ruota automaticamente il materiale della chiave KMS un anno dopo la data di abilitazione e successivamente ogni anno.

Argomenti

Abilitazione e disabilitazione della rotazione delle chiavi (console)

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente. Non è possibile abilitare o disabilitare la rotazione delle Chiavi gestite da AWS. Queste vengono ruotate automaticamente ogni anno.
4. Scegli l'alias o l'ID chiave di una chiave KMS.
5. Scegliere la scheda Key rotation (Rotazione chiave).

   La scheda Key rotation (Rotazione della chiave) viene visualizzata solo nella pagina dei dettagli delle chiavi KMS di crittografia simmetrica con materiale della chiave generato da AWS KMS (il

valore di Origin (Origine) è AWS_KMS), incluse le chiavi KMS di crittografia simmetrica multi-regione.

Non è possibile ruotare automaticamente le chiavi KMS asimmetriche, le chiavi KMS HMAC, le chiavi KMS con materiale della chiave importato o le chiavi KMS negli archivi delle chiavi personalizzate. Tuttavia è possibile ruotare queste chiavi manualmente.

6. Seleziona o deseleziona la casella di controllo Ruota automaticamente questa chiave KMS ogni anno.

> **Note**
>
> Se una chiave KMS è disattivata o in attesa di eliminazione, la casella di controllo Ruota automaticamente questa chiave KMS ogni anno è deselezionata e non è possibile modificarla. Lo stato della rotazione della chiave viene ripristinato quando abiliti la chiave KMS o annulli l'eliminazione. Per informazioni dettagliate, consulta Come funziona la rotazione automatica delle chiavi e Stati chiave delle chiavi AWS KMS.

7. Selezionare Salva.

Abilitazione e disabilitazione della rotazione delle chiavi (API AWS KMS)

È possibile utilizzare l'API AWS Key Management Service (AWS KMS) per abilitare e disabilitare la rotazione automatica delle chiavi e visualizzare lo stato attuale della rotazione di qualsiasi chiave gestita dal cliente. Questi esempi utilizzano AWS Command Line Interface (AWS CLI), ma è possibile usare anche qualsiasi linguaggio di programmazione supportato.

L'EnableKeyRotationoperazione consente la rotazione automatica delle chiavi per la chiave KMS specificata. L'DisableKeyRotationoperazione la disabilita. Per identificare la chiave KMS in queste operazioni, utilizza l'ID chiave o l'ARN di chiave. Per impostazione predefinita, la rotazione automatica è disabilitata per le chiavi gestite dal cliente.

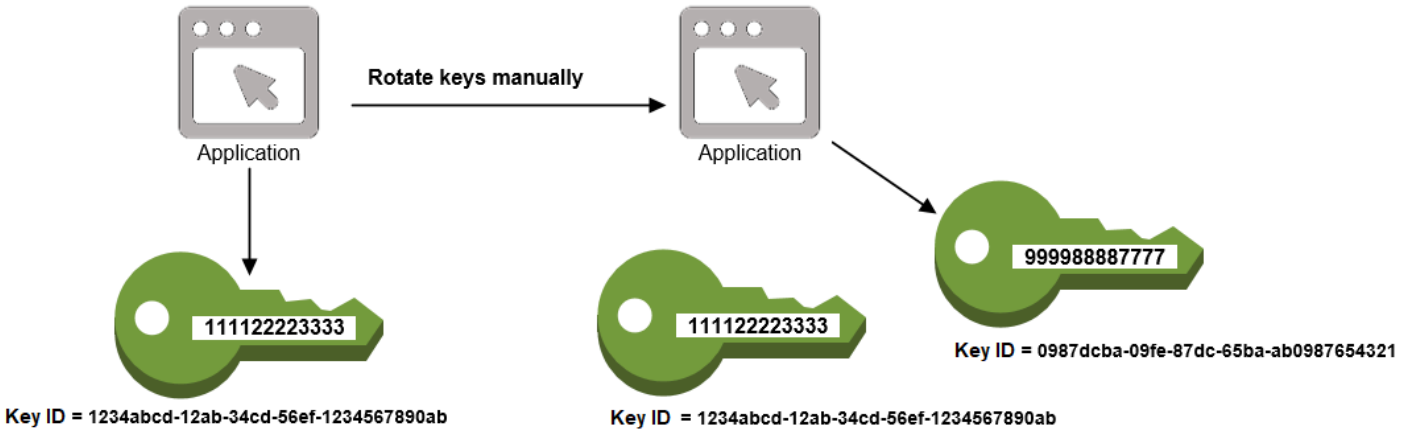
L'esempio seguente abilita la rotazione delle chiavi sulla chiave KMS di crittografia simmetrica specificata e utilizza l'GetKeyRotationStatusoperazione per visualizzare il risultato. Quindi, disabilita la rotazione della chiave e, di nuovo, utilizza GetKeyRotationStatus per visualizzare le modifiche.

```
$ aws kms enable-key-rotation --key-id 1234abcd-12ab-34cd-56ef-1234567890ab

$ aws kms get-key-rotation-status --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

```
{
    "KeyRotationEnabled": true
}

$ aws kms disable-key-rotation --key-id 1234abcd-12ab-34cd-56ef-1234567890ab

$ aws kms get-key-rotation-status --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
{
    "KeyRotationEnabled": false
}
```

Rotazione manuale delle chiavi

Puoi creare una nuova chiave KMS e utilizzarla al posto della chiave KMS attuale, anziché abilitare la rotazione automatica delle chiavi. Quando la nuova chiave KMS ha materiale crittografico diverso rispetto a quello dell'attuale chiave KMS, l'utilizzo della nuova chiave KMS ha lo stesso effetto che si ottiene modificando la chiave di supporto in una chiave KMS esistente. Il processo di sostituzione di una chiave KMS con un'altra è noto come rotazione manuale delle chiavi.



È possibile ruotare le chiavi manualmente in modo da controllare la frequenza di rotazione. Rappresenta inoltre una buona soluzione per le chiavi KMS non idonee per la rotazione automatica, ad esempio le chiavi KMS asimmetriche, le chiavi KMS HMAC, le chiavi KMS negli archivi delle chiavi personalizzate e le chiavi KMS con materiale della chiave importato.

> **Note**
>
> Quando inizi a usare la nuova chiave KMS, assicurati di mantenere la chiave KMS originale abilitata, in modo che AWS KMS possa decrittare i dati crittografati dalla chiave KMS originale.

Quando ruoti manualmente le chiavi KMS, devi aggiornare anche i riferimenti all'ID o all'ARN della chiave KMS nelle applicazioni. Gli alias, che consentono di associare un nome descrittivo a una chiave KMS, agevolano questo processo. Usa un alias per fare riferimento a una chiave KMS nelle tue applicazioni. Quindi, se desideri modificare la chiave KMS utilizzata dall'applicazione, invece di modificare il codice dell'applicazione, modifica la chiave KMS di destinazione dell'alias. Per informazioni dettagliate, vedi Utilizzo di alias nelle applicazioni.

> **Note**
>
> Gli alias che rimandano alla versione più recente di una chiave KMS ruotata manualmente sono una buona soluzione per le operazioni DescribeKey, Encrypt,, e Sign. GenerateDataKeyGenerateDataKeyPairGenerateMac Gli alias non sono consentiti nelle operazioni che gestiscono le chiavi KMS, come o. DisableKeyScheduleKeyDeletion
> Quando si chiama l'operazione Decryptsulle chiavi KMS di crittografia simmetrica ruotate manualmente, non specificare il parametro `KeyId` con il comando. AWS KMS utilizza automaticamente la chiave KMS che ha crittografato il testo criptato.
> Il `KeyId` parametro è obbligatorio quando si chiama `Decrypt` o verifica con una chiave KMS asimmetrica o si chiama VerifyMaccon una chiave KMS HMAC. Queste richieste avranno esito negativo se il valore del parametro `KeyId` è un alias che non punta più alla chiave KMS che ha eseguito l'operazione di crittografia, ad esempio quando una chiave viene ruotata manualmente. Per evitare questo errore, è necessario tenere traccia e specificare la chiave KMS corretta per ciascuna operazione.

Per modificare la chiave KMS di destinazione di un alias, utilizza l'operazione nell'API. UpdateAliasAWS KMS Ad esempio, questo comando aggiorna l'alias `alias/TestKey` per puntare a una nuova chiave KMS. Poiché l'operazione non restituisce alcun output, l'esempio utilizza l'ListAliasesoperazione per mostrare che l'alias è ora associato a una chiave KMS diversa e il `LastUpdatedDate` campo è aggiornato. I ListAliases comandi utilizzano il `query`parametro in AWS CLI per ottenere solo l'`alias/TestKey`alias.

```
$ aws kms list-aliases --query 'Aliases[?AliasName==`alias/TestKey`]'
{
    "Aliases": [
        {
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/TestKey",
            "AliasName": "alias/TestKey",
            "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
            "CreationDate": 1521097200.123,
            "LastUpdatedDate": 1521097200.123
        },
    ]
}


$ aws kms update-alias --alias-name alias/TestKey --target-key-id
 0987dcba-09fe-87dc-65ba-ab0987654321

$ aws kms list-aliases --query 'Aliases[?AliasName==`alias/TestKey`]'
{
    "Aliases": [
        {
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/TestKey",
            "AliasName": "alias/TestKey",
            "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
            "CreationDate": 1521097200.123,
            "LastUpdatedDate": 1604958290.722
        },
    ]
}
```

Monitoraggio di AWS KMS keys

Il monitoraggio è un aspetto importante per comprendere la disponibilità, lo stato e l'utilizzo delle AWS KMS keys in AWS KMS e per mantenere l'affidabilità, la disponibilità e le prestazioni delle tue soluzioni AWS. Raccogliere i dati sul monitoraggio da tutte le parti della soluzione AWS consente un debug più facile di eventuali guasti in più punti. Prima di iniziare il monitoraggio delle chiavi KMS è tuttavia opportuno creare un piano di monitoraggio che includa le risposte alle seguenti domande:

- Quali sono gli obiettivi del monitoraggio?
- Di quali risorse si intende eseguire il monitoraggio?

- Con quale frequenza sarà eseguito il monitoraggio di queste risorse?
- Quali strumenti di monitoraggio utilizzerai?
- Chi eseguirà i processi di monitoraggio?
- Chi deve ricevere una notifica quando si verifica un problema?

Il passaggio successivo è quello di monitorare le tue chiavi KMS nel corso del tempo per stabilire una linea di base per l'uso normale di AWS KMS e le aspettative nel proprio ambiente. Quando monitori le chiavi KMS, archivia i dati di monitoraggio storici per poterli confrontare con i dati correnti, identificare i normali modelli di prestazioni e le anomalie e ideare metodi per risolvere i problemi.

Ad esempio, puoi monitorare le attività delle API AWS KMS e degli eventi che interessano le chiavi KMS. Quando i dati sono sopra o sotto il livello stabilito, potrebbe essere necessario indagare o intraprendere azioni correttive.

Per stabilire una baseline per modelli normali, devi monitorare gli elementi seguenti:

- Le attività delle API AWS KMS per le operazioni del piano dati. Si tratta di operazioni crittografiche che utilizzano una chiave KMS, come Decrypt, Encrypt e. ReEncryptGenerateDataKey
- Attività dell'API di AWS KMS per le operazioni del piano di controllo importanti per te. Queste operazioni gestiscono una chiave KMS e potresti voler monitorare quelle che modificano la disponibilità di una chiave KMS (come ScheduleKeyDeletion,, CancelKeyDeletionDisableKeyEnableKeyImportKeyMaterial, e DeleteImportedKeyMaterial) o modificano il controllo di accesso di una chiave KMS (come and). PutKeyPolicyRevokeGrant
- Altri parametri AWS KMS (ad esempio la quantità di tempo rimanente fino alla scadenza del materiale chiave importato) e gli eventi (ad esempio la scadenza del materiale chiave importato o l'eliminazione o la rotazione di una chiave KMS).

Strumenti di monitoraggio

AWS offre vari strumenti che puoi utilizzare per monitorare le chiavi KMS. Alcuni di questi strumenti possono essere configurati in modo che eseguano automaticamente il monitoraggio, mentre altri richiedono l'intervento manuale. Si consiglia di automatizzare il più possibile i processi di monitoraggio.

Strumenti di monitoraggio automatici

Per controllare le chiavi KMS e segnalare l'eventuale presenza di problemi, puoi usare gli strumenti di monitoraggio automatici seguenti.

- AWS CloudTrailMonitoraggio dei registri: condividi i file di registro tra account, monitora i file di CloudTrail registro in tempo reale inviandoli a CloudWatch Logs, scrivi applicazioni di elaborazione dei log con la CloudTrail Processing Library e verifica che i file di registro non siano stati modificati dopo la consegna da parte di. CloudTrail Per ulteriori informazioni, consulta Lavorare con i file di CloudTrail registro nella Guida per l'AWS CloudTrailutente.
- Amazon CloudWatch Alarms: monitora una singola metrica in un periodo di tempo specificato ed esegui una o più azioni in base al valore della metrica rispetto a una determinata soglia in diversi periodi di tempo. L'azione è una notifica inviata a un argomento di Amazon Simple Notification Service (Amazon SNS) o a una policy di Amazon EC2 Auto Scaling. CloudWatch gli allarmi non richiamano azioni semplicemente perché si trovano in uno stato particolare; lo stato deve essere cambiato e mantenuto per un determinato numero di periodi. Per ulteriori informazioni, consulta Monitoraggio con Amazon CloudWatch.
- Amazon EventBridge: abbina gli eventi e li indirizza a una o più funzioni o flussi di destinazione per acquisire informazioni sullo stato e, se necessario, apportare modifiche o intraprendere azioni correttive. Per ulteriori informazioni, consulta Monitoraggio con Amazon EventBridge la Amazon EventBridge User Guide.
- Amazon CloudWatch Logs: monitora, archivia e accedi ai tuoi file di registro da AWS CloudTrail o altre fonti. Per ulteriori informazioni, consulta la Amazon CloudWatch Logs User Guide.

Strumenti di monitoraggio manuali

Un'altra parte importante del monitoraggio delle chiavi KMS consiste nel monitorare manualmente gli elementi che gli CloudWatch allarmi e gli eventi non coprono. I AWS dashboard AWS KMS CloudWatch,AWS Trusted Advisor, e altri forniscono una at-a-glance panoramica dello stato dell'ambiente. AWS

È possibile personalizzare le pagine Chiavi gestite da AWS e Chiavi gestite dal cliente della console AWS KMS per visualizzare le seguenti informazioni su ciascuna chiave KMS:

- ID chiave
- Stato
- Data di creazione

- Data di scadenza (per le chiavi KMS con materiale chiave importato)
- Origin
- ID dell'archivio delle chiavi personalizzate (per le chiavi KMS negli archivi delle chiavi personalizzate)

Il pannello di controllo della console CloudWatch mostra quanto segue:

- Stato e allarmi attuali
- Grafici degli allarmi e delle risorse
- Stato di integrità dei servizi

Inoltre, è possibile utilizzare CloudWatch per effettuare le seguenti operazioni:

- Crea pannelli di controllo personalizzati per monitorare i servizi di interesse.
- Creare grafici dei dati dei parametri per la risoluzione di problemi e il rilevamento di tendenze.
- Ricercare e analizzare tutti i parametri delle risorse AWS
- Creare e modificare gli allarmi per ricevere le notifiche dei problemi.

AWS Trusted Advisor facilita il monitoraggio delle risorse AWS per migliorare prestazioni, affidabilità, sicurezza e convenienza. Per tutti gli utenti sono disponibili quattro controlli di Trusted Advisor; per gli utenti con un piano di assistenza Business o Enterprise sono disponibili più di 50 controlli. Per ulteriori informazioni, consulta AWS Trusted Advisor.

Registrazione delle chiamate API AWS KMS con AWS CloudTrail

AWS KMSè integrato con AWS CloudTrail, un servizio che registra tutte le chiamate verso AWS KMS utenti, ruoli e altri AWS servizi. CloudTrail acquisisce tutte le chiamate API a AWS KMS come eventi, incluse le chiamate dalla AWS KMS console, dalle AWS KMS API, dai AWS CloudFormation modelli, da 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 ListAliasesand, le operazioni che gestiscono le chiavi KMS GetKeyRotationStatus, come and, e le operazioni crittografiche PutKeyPolicy, come CreateKeye Decrypt. GenerateDataKey Registra anche le operazioni interne che AWS KMS richiedono l'utente, ad esempio, e. DeleteExpiredKeyMaterialDeleteKeySynchronizeMultiRegionKeyRotateKey

CloudTrail registra le operazioni riuscite e i tentativi di chiamata non riusciti, ad esempio quando al chiamante viene negato l'accesso a una risorsa. Le operazioni tra account sulle chiavi KMS vengono registrate sia nell'account del chiamante che nell'account del proprietario della chiave KMS. Tuttavia, le richieste AWS KMS tra account che sono rifiutate perché l'accesso è negato vengono registrate solo nell'account del chiamante.

Per motivi di sicurezza, alcuni campi vengono omessi dalle voci di AWS KMS registro, ad esempio il `Plaintext` parametro di una richiesta Encrypt e la risposta o qualsiasi operazione di GetKeyPolicycrittografia. Per semplificare la ricerca delle voci di CloudTrail registro per particolari chiavi KMS, AWS KMS aggiunge l'ARN della chiave KMS interessata al campo nelle voci di registro per AWS KMS alcune operazioni di gestione delle chiavi, anche quando l'operazione API non restituisce l'ARN della chiave. `responseElements`

Sebbene per impostazione predefinita, tutte le AWS KMS azioni vengano registrate come CloudTrail eventi, è possibile escludere AWS KMS le azioni da una traccia. CloudTrail Per informazioni dettagliate, vedi Esclusione di eventi AWS KMS da un trail.

Ulteriori informazioni:

- Per esempi di CloudTrail log di AWS KMS operazioni per un'enclave AWS Nitro, vedi. Richieste di monitoraggio per enclavi Nitro

Argomenti

Registrazione degli eventi in CloudTrail

CloudTrail è abilitato sul tuo Account AWS quando crei l'account. Quando si verifica un'attività inAWS KMS, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti in Account AWS. Per ulteriori informazioni, vedere Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi nell'Account AWS che includa gli eventi per AWS KMS, crea un trail. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per

impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il percorso registra gli eventi di tutte le Regioni nella partizione AWSe distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, puoi configurarne altri Servizi AWS per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei CloudTrail log. Per ulteriori informazioni, consultare:

- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Per ulteriori informazioni CloudTrail, consulta la Guida AWS CloudTrail per l'utente. Per ulteriori informazioni su altri modi per monitorare l'utilizzo delle chiavi KMS, consulta Monitoraggio di AWS KMS keys.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali root o credenziali di un utente IAM.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro Servizio AWS.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Ricerca di eventi in CloudTrail

Per cercare le voci del CloudTrail registro, usa la CloudTrail console o l'CloudTrail LookupEventsoperazione. CloudTrail supporta numerosi valori di attributo per filtrare la ricerca, tra cui il nome dell'evento, il nome utente e l'origine dell'evento.

Per facilitare la ricerca delle voci di AWS KMS registro CloudTrail, AWS KMS compila i seguenti campi di immissione del CloudTrail registro.

> **Note**
>
> A partire da dicembre 2022, AWS KMS popola gli attributi Resource type (Tipo di risorsa) e Resource name (Nome risorsa) in tutte le operazioni di gestione che modificano una particolare chiave KMS. Questi valori degli attributi potrebbero essere nulli nelle CloudTrail voci precedenti per le seguenti operazioni: CreateAlias, CreateGrant, DeleteAlias,, DeleteImportedKeyMaterial, ImportKeyMaterial, ReplicateKey, RetireGrantRevokeGrantUpdateAlias, e. UpdatePrimaryRegion

Attributo	Valore	Voci di log
Origine evento (`EventSource`)	`kms.amazonaws.com`	Tutte le operazioni.
Tipo di risorsa (`ResourceType`)	`AWS::KMS::Key`	Operazioni di gestione che modificano una determinata chiave KMS, ad esempio `CreateKey` e `EnableKey`, ma non `ListKeys`.
Nome risorsa (`ResourceName`)	ARN chiave (o ID chiave e ARN chiave)	Operazioni di gestione che modificano una determinata chiave KMS, ad esempio `CreateKey` e `EnableKey`, ma non `ListKeys`.

Per aiutarti a trovare le voci di log per le operazioni di gestione su determinate chiavi KMS, AWS KMS registra l'ARN chiave della chiave KMS interessata nell'elemento `responseElements.keyId` della voce di log, anche quando l'operazione API AWS KMS non restituisce l'ARN chiave.

Ad esempio, una chiamata riuscita all'DisableKeyoperazione non restituisce alcun valore nella risposta, ma invece di un valore nullo, il `responseElements.keyId` valore nella voce di DisableKey registro include la chiave ARN della chiave KMS disattivata.

Questa funzionalità è stata aggiunta a dicembre 2022 e influisce sulle seguenti voci di CloudTrail registro: CreateAliasCreateGrant, DeleteAlias, DeleteKey,

DisableKey,, EnableKey, EnableKeyRotation, ImportKeyMaterial, RotateKey, SynchronizeMultiRegionKeyTagResourceUntagResource, UpdateAliase. UpdatePrimaryRegion

Esclusione di eventi AWS KMS da un trail

Per registrare l'uso e la gestione delle proprie AWS KMS risorse, la maggior parte AWS KMS degli utenti si affida agli eventi di un CloudTrail percorso. Il trail può essere una fonte preziosa di dati per l'audit di eventi critici, ad esempio la creazione, la disattivazione e l'eliminazione delle AWS KMS keys, la modifica delle policy delle chiavi e l'utilizzo delle da parte dei servizi AWS per tuo conto. In alcuni casi, i metadati contenuti in una voce di CloudTrail registro, ad esempio il contesto di crittografia in un'operazione di crittografia, possono aiutare a evitare o risolvere errori.

Tuttavia, poiché AWS KMS può generare un numero elevato di eventi, AWS CloudTrail permette di escludere gli eventi AWS KMS da un trail. Questa impostazione basata su trail esclude tutti gli eventi AWS KMS; non è possibile escludere eventi AWS KMS specifici.

> **Warning**
>
> L'esclusione di AWS KMS eventi da un CloudTrail registro può oscurare le azioni che utilizzano le chiavi KMS. Presta attenzione quando concedi alle entità principali l'autorizzazione `cloudtrail:PutEventSelectors` necessaria per eseguire questa operazione.

Per escludere gli eventi AWS KMS da un trail:

- Nella CloudTrail console, utilizza l'impostazione degli eventi del servizio di gestione delle chiavi di registro quando crei un percorso o lo aggiorni. Per istruzioni, consulta Registrazione di eventi di gestione con la AWS Management Console nella Guida per l'utente di AWS CloudTrail.
- Nell' CloudTrail API, usa l'PutEventSelectorsoperazione. Aggiungere l'attributo `ExcludeManagementEventSources` ai selettori di eventi con un valore `kms.amazonaws.com`. Per un esempio, consulta Esempio: percorso che non registra eventi AWS Key Management Service nella Guida per l'utente di AWS CloudTrail.

È possibile disattivare questa esclusione in qualsiasi momento modificando l'impostazione della console o i selettori di eventi per un trail. Il trail inizierà quindi a registrare gli eventi AWS KMS. Tuttavia, non è possibile ripristinare gli eventi AWS KMS che si sono verificati mentre era in atto l'esclusione.

Quando escludi AWS KMS eventi utilizzando la console o l'API, anche l'operazione CloudTrail `PutEventSelectors` API risultante viene registrata nei tuoi CloudTrail log. Se AWS KMS gli eventi non compaiono nei tuoi CloudTrail log, cerca un `PutEventSelectors` evento con l'`ExcludeManagementEventSources`attributo impostato su. `kms.amazonaws.com`

Esempi di voci di log AWS KMS

AWS KMSscrive voci nel CloudTrail registro quando richiami un'AWS KMSoperazione e quando un AWS servizio richiama un'operazione per tuo conto. AWS KMSscrive anche una voce quando richiama un'operazione per voi. Ad esempio, scrive una voce quando elimina una chiave KMS che hai pianificato per l'eliminazione.

I seguenti argomenti mostrano esempi di voci di CloudTrail registro relative AWS KMS alle operazioni.

Per esempi di voci di CloudTrail registro delle richieste AWS KMS provenienti da AWS Nitro Enclaves, vedi. Richieste di monitoraggio per enclavi Nitro

Argomenti

- CancelKeyDeletion
- ConnectCustomKeyStore
- CreateAlias
- CreateCustomKeyStore
- CreateGrant
- CreateKey
- Decrypt
- DeleteAlias
- DeleteCustomKeyStore
- DeleteExpiredKeyMaterial
- DeleteImportedKeyMaterial
- DeleteKey
- DescribeCustomKeyStores
- DescribeKey
- DisableKey
- DisableKeyRotation

- DisconnectCustomKeyStore
- EnableKey
- EnableKeyRotation
- Crittografa
- GenerateDataKey
- GenerateDataKeyPair
- GenerateDataKeyPairWithoutPlaintext
- GenerateDataKeyWithoutPlaintext
- GenerateMac
- GenerateRandom
- GetKeyPolicy
- GetKeyRotationStatus
- GetParametersForImport
- ImportKeyMaterial
- ListAliases
- ListGrants
- PutKeyPolicy
- ReEncrypt
- ReplicateKey
- RetireGrant
- RevokeGrant
- RotateKey
- ScheduleKeyDeletion
- Sign
- SynchronizeMultiRegionKey
- TagResource
- UntagResource
- UpdateAlias
- UpdateCustomKeyStore
- UpdateKeyDescription

- UpdatePrimaryRegion
- VerifyMac
- Verifica
- Esempio uno di Amazon EC2
- Esempio due di Amazon EC2

CancelKeyDeletion

Nell'esempio seguente viene illustrata una voce di log AWS CloudTrail generata chiamando l'operazione CancelKeyDeletion. Per informazioni sull'eliminazione delle AWS KMS keys, consulta Eliminazione di AWS KMS keys.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2020-07-27T21:53:17Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CancelKeyDeletion",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": {
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "e3452e68-d4b0-4ec7-a768-7ae96c23764f",
    "eventID": "d818bf03-6655-48e9-8b26-f279a07075fd",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
```

```
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

ConnectCustomKeyStore

Nell'esempio seguente viene illustrata una voce di log AWS CloudTrail generata chiamando l'operazione `ConnectCustomKeyStore`. Per informazioni sulla connessione a un archivio delle chiavi personalizzate, consultare Connessione e disconnessione di un archivio delle chiavi di AWS CloudHSM.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2021-10-21T20:17:32Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "ConnectCustomKeyStore",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "customKeyStoreId": "cks-1234567890abcdef0"
    },
    "responseElements": null,
    "additionalEventData": {
        "customKeyStoreName": "ExampleKeyStore",
        "clusterId": "cluster-1a23b4cdefg"
    },
    "requestID": "abcde9e1-f1a3-4460-a423-577fb6e695c9",
    "eventID": "114b61b9-0ea6-47f5-a9d2-4f2bdd0017d5",
    "readOnly": false,
```

```
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333"
}
```

CreateAlias

L'esempio seguente mostra una voce di AWS CloudTrail registro relativa all'CreateAliasoperazione. L'elemento `resources` include i campi per l'alias e le risorse della chiave KMS. Per informazioni sulla creazione di alias in AWS KMS, consulta Creazione di un alias.

CloudTrail le voci di registro per questa operazione registrate a partire da dicembre 2022 includono l'ARN della chiave KMS interessata nel `responseElements.keyId` valore, anche se questa operazione non restituisce l'ARN della chiave.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2022-08-14T23:08:31Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateAlias",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "aliasName": "alias/ExampleAlias",
        "targetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": {
        "keyId":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "caec1e0c-ce03-419e-bdab-6ab1f7c57c01",
    "eventID": "2dd6e784-8286-46a6-befd-d64e5a02fb28",
    "readOnly": false,
    "resources": [
```

```
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        },
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-west-2:111122223333:alias/ExampleAlias"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

CreateCustomKeyStore

L'esempio seguente mostra una voce di log AWS CloudTrail generata chiamando l'operazione `CreateCustomKeyStore` in un archivio delle chiavi di AWS CloudHSM. Per informazioni sulla creazione di archivi delle chiavi personalizzate, consultare Creazione di un archivio delle chiavi di AWS CloudHSM.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2021-10-21T20:17:32Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateCustomKeyStore",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "customKeyStoreName": "ExampleKeyStore",
```

```
        "clusterId": "cluster-1a23b4cdefg"
    },
    "responseElements": {
        "customKeyStoreId": "cks-1234567890abcdef0"
    },
    "requestID": "abcde9e1-f1a3-4460-a423-577fb6e695c9",
    "eventID": "114b61b9-0ea6-47f5-a9d2-4f2bdd0017d5",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333"
}
```

CreateGrant

L'esempio seguente mostra una voce di AWS CloudTrail registro relativa all'CreateGrantoperazione. Per informazioni sulla creazione delle concessioni in AWS KMS, consulta Concessioni in AWS KMS.

CloudTrail le voci di registro per questa operazione registrate a partire da dicembre 2022 includono l'ARN della chiave KMS interessata nel `responseElements.keyId` valore, anche se questa operazione non restituisce l'ARN della chiave.

```
{
  "eventVersion": "1.02",
  "userIdentity": {
      "type": "IAMUser",
      "principalId": "EX_PRINCIPAL_ID",
      "arn": "arn:aws:iam::111122223333:user/Alice",
      "accountId": "111122223333",
      "accessKeyId": "EXAMPLE_KEY_ID",
      "userName": "Alice"
  },
  "eventTime": "2014-11-04T00:53:12Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "CreateGrant",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "AWS Internal",
  "requestParameters": {
      "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "constraints": {
          "encryptionContextSubset": {
```

```
                "ContextKey1": "Value1"
            }
        },
        "operations": ["Encrypt",
        "RetireGrant"],
        "granteePrincipal": "EX_PRINCIPAL_ID"
    },
    "responseElements": {
        "grantId": "f020fe75197b93991dc8491d6f19dd3cebb24ee62277a05914386724f3d48758",
        "keyId":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "f3c08808-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "5d529779-2d27-42b5-92da-91aaea1fc4b5",
    "readOnly": false,
    "resources": [{
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "accountId": "111122223333"
    }],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

CreateKey

Questi esempi mostrano le voci di AWS CloudTrail registro relative all'CreateKeyoperazione.

Una voce di `CreateKey` registro può derivare da una `CreateKey` richiesta o dall'`CreateKey`operazione relativa a una ReplicateKeyrichiesta.

L'esempio seguente mostra una voce di CloudTrail registro per un'CreateKeyoperazione che crea una chiave KMS di crittografia simmetrica. Per informazioni sulla creazione di chiavi KMS, consulta Creazione di chiavi.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
```

```
        "userName": "Alice"
    },
    "eventTime": "2022-08-10T22:38:27Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "description": "",
        "origin": "EXTERNAL",
        "bypassPolicyLockoutSafetyCheck": false,
        "customerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "keySpec": "SYMMETRIC_DEFAULT",
        "keyUsage": "ENCRYPT_DECRYPT"
    },
    "responseElements": {
        "keyMetadata": {
            "AWSAccountId": "111122223333",
            "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
            "arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "creationDate": "Aug 10, 2022, 10:38:27 PM",
            "enabled": false,
            "description": "",
            "keyUsage": "ENCRYPT_DECRYPT",
            "keyState": "PendingImport",
            "origin": "EXTERNAL",
            "keyManager": "CUSTOMER",
            "customerMasterKeySpec": "SYMMETRIC_DEFAULT",
            "keySpec": "SYMMETRIC_DEFAULT",
            "encryptionAlgorithms": [
                "SYMMETRIC_DEFAULT"
            ],
            "multiRegion": false
        }
    },
    "requestID": "1aef6713-0223-4ff7-9a6d-781360521930",
    "eventID": "36327b37-f4f6-40a9-92ab-48064ec905a2",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
```

```
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

L'esempio seguente mostra il CloudTrail registro di un'`CreateKey`operazione che crea una chiave KMS di crittografia simmetrica in un archivio di chiavi. AWS CloudHSM

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::111122223333:user/Alice",
            "accountId": "111122223333",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice"
    },
    "eventTime": "2021-10-14T17:39:50Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyUsage": "ENCRYPT_DECRYPT",
        "bypassPolicyLockoutSafetyCheck": false,
        "origin": "AWS_CLOUDHSM",
        "keySpec": "SYMMETRIC_DEFAULT",
        "customerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "customKeyStoreId": "cks-1234567890abcdef0",
        "description": ""
    },
    "responseElements": {
        "keyMetadata": {
            "aWSAccountId": "111122223333",
            "keyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
```

```
            "arn": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321",
            "creationDate": "Oct 14, 2021, 5:39:50 PM",
            "enabled": true,
            "description": "",
            "keyUsage": "ENCRYPT_DECRYPT",
            "keyState": "Enabled",
            "origin": "AWS_CLOUDHSM",
            "customKeyStoreId": "cks-1234567890abcdef0",
            "cloudHsmClusterId": "cluster-1a23b4cdefg",
            "keyManager": "CUSTOMER",
            "customerMasterKeySpec": "SYMMETRIC_DEFAULT",
            "keySpec": "SYMMETRIC_DEFAULT",
            "encryptionAlgorithms": [
                "SYMMETRIC_DEFAULT"
            ],
            "multiRegion": false
        }
    },
    "additionalEventData": {
        "backingKey": "{\"keyHandle\":\"19\",\"backingKeyId\":\"backing-key-id\"}"
    },
    "requestID": "4f0b185c-588c-4767-9e90-c618f7e13cad",
    "eventID": "c73964b8-703d-49e4-bd9e-f773d0ee1e65",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


L'esempio seguente mostra il CloudTrail registro di un'`CreateKey`operazione che crea una chiave KMS di crittografia simmetrica in un archivio di chiavi esterno.


```
{
```

```
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::111122223333:user/Alice",
            "accountId": "111122223333",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice"
    },
    "eventTime": "2022-09-07T22:37:45Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "tags": [],
        "keyUsage": "ENCRYPT_DECRYPT",
        "description": "",
        "origin": "EXTERNAL_KEY_STORE",
        "multiRegion": false,
        "keySpec": "SYMMETRIC_DEFAULT",
        "customerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "bypassPolicyLockoutSafetyCheck": false,
        "customKeyStoreId": "cks-1234567890abcdef0",
        "xksKeyId": "bb8562717f809024"
    },
    "responseElements": {
        "keyMetadata": {
            "aWSAccountId": "111122223333",
            "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
            "arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "creationDate": "Dec 7, 2022, 10:37:45 PM",
            "enabled": true,
            "description": "",
            "keyUsage": "ENCRYPT_DECRYPT",
            "keyState": "Enabled",
            "origin": "EXTERNAL_KEY_STORE",
            "customKeyStoreId": "cks-1234567890abcdef0",
            "keyManager": "CUSTOMER",
            "customerMasterKeySpec": "SYMMETRIC_DEFAULT",
            "keySpec": "SYMMETRIC_DEFAULT",
            "encryptionAlgorithms": [
```

```
                "SYMMETRIC_DEFAULT"
            ],
            "multiRegion": false,
            "xksKeyConfiguration": {
                "id": "bb8562717f809024"
            }
        }
    },
    "requestID": "ba197c82-3ac7-487a-8ff4-7736bbeb1316",
    "eventID": "838ad5f4-5fdd-4044-afd7-4dbd88c6af56",
    "readOnly": false,
    "resources": [
        {
            "accountId": "227179770375",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-east-1:227179770375:key/39c5eb22-
f37c-4956-92ca-89e8f8b57ab2"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Decrypt

Questi esempi mostrano le voci di log AWS CloudTrail per l'operazione Decrypt.

La voce di CloudTrail registro per un'`Decrypt`operazione include sempre il `encryptionAlgorithm` in `requestParameters` anche se l'algoritmo di crittografia non è stato specificato nella richiesta. Il testo cifrato nella richiesta e il testo normale nella risposta sono omessi.

Argomenti

- Decrittografia con una chiave crittografica simmetrica standard
- Errore di decrittografia con una chiave crittografica simmetrica standard
- Decrittografia con una chiave KMS in un archivio delle chiavi di AWS CloudHSM
- Decrittografia con una chiave KMS in un archivio delle chiavi esterne
- Errore di decrittografia con una chiave KMS in un archivio delle chiavi esterne

Decrittografia con una chiave crittografica simmetrica standard

Di seguito è riportato un esempio di voce di CloudTrail registro per un'`Decrypt`operazione con una chiave di crittografia simmetrica standard.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2020-07-27T22:58:24Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "encryptionContext": {
            "Department": "Engineering",
            "Project": "Alpha"
        }
    },
    "responseElements": null,
    "requestID": "12345126-30d5-4b28-98b9-9153da559963",
    "eventID": "abcde202-ba1a-467c-b4ba-f729d45ae521",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
```

```
}
```

Errore di decrittografia con una chiave crittografica simmetrica standard

L'esempio seguente di voce di CloudTrail registro registra un'`Decrypt`operazione non riuscita con una chiave KMS di crittografia simmetrica standard. L'eccezione (`errorCode`) e il messaggio di errore (`errorMessage`) sono inclusi per aiutarti a risolvere l'errore.

In questo caso, la chiave KMS di crittografia simmetrica specificata nella richiesta `Decrypt` non corrispondeva alla chiave KMS utilizzata per crittografare i dati.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2022-11-24T18:57:43Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "errorCode": "IncorrectKeyException"
    "errorMessage": "The key ID in the request does not identify a CMK that can perform
 this operation.",
    "requestParameters": {
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "encryptionContext": {
            "Department": "Engineering",
            "Project": "Alpha"
        }
    },
    "responseElements": null,
    "requestID": "22345126-30d5-4b28-98b9-9153da559963",
    "eventID": "abcde202-ba1a-467c-b4ba-f729d45ae521",
    "readOnly": true,
```

```
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

Decrittografia con una chiave KMS in un archivio delle chiavi di AWS CloudHSM

L'esempio seguente di voce di CloudTrail registro registra un'`Decrypt`operazione con una chiave KMS in un archivio di chiavi. AWS CloudHSM Tutte le voci di log per le operazioni di crittografia con una chiave KMS in un archivio delle chiavi personalizzate includono un campo `additionalEventData` con l'`customKeyStoreId`. `additionalEventData` non è specificato nella richiesta.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2021-10-26T23:41:27Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "requestParameters": {
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "encryptionContext": {
            "Department": "Development",
            "Purpose": "Test"
        }
```

```
    },
    "responseElements": null,
    "additionalEventData": {
        "customKeyStoreId": "cks-1234567890abcdef0"
    },
    "requestID": "e1b881f8-2048-41f8-b6cc-382b7857ec61",
    "eventID": "a79603d5-4cde-46fc-819c-a7cf547b9df4",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Decrittografia con una chiave KMS in un archivio delle chiavi esterne

L'esempio seguente di voce di CloudTrail registro registra un'`Decrypt`operazione con una chiave KMS in un archivio di chiavi esterno. Oltre a `customKeyStoreId`, il campo `additionalEventData` include l'ID della chiave esterna (`XksKeyId`). `additionalEventData` non è specificato nella richiesta.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2022-11-24T00:26:58Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-west-2",
```

```
    "sourceIPAddress": "AWS Internal",
    "requestParameters": {
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321",
        "encryptionContext": {
            "Department": "Engineering",
            "Purpose": "Test"
        }
    },
    "responseElements": null,
    "additionalEventData": {
        "customKeyStoreId": "cks-9876543210fedcba9",
        "xksKeyId": "abc01234567890fe"
    },
    "requestID": "f1b881f8-2048-41f8-b6cc-382b7857ec61",
    "eventID": "b79603d5-4cde-46fc-819c-a7cf547b9df4",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Errore di decrittografia con una chiave KMS in un archivio delle chiavi esterne

L'esempio seguente di voce di CloudTrail registro registra una richiesta non riuscita per un'`Decrypt`operazione con una chiave KMS in un archivio di chiavi esterno. CloudWatch registra le richieste che hanno esito negativo, oltre a quelle riuscite. Quando si registra un errore, la voce di CloudTrail registro include l'eccezione (ErrorCode) e il relativo messaggio di errore (ErrorMessage).

Se la richiesta non riuscita ha raggiunto il proxy dell'archivio delle chiavi esterne, come in questo esempio, puoi utilizzare il valore `requestId` per associare la richiesta non riuscita a una richiesta corrispondente registrata dal proxy, se l'operazione è consentita.

Per informazioni sulle richieste `Decrypt` negli archivi delle chiavi esterne, consulta Errori di decrittografia.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2022-11-24T00:26:58Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "errorCode": "KMSInvalidStateException",
    "errorMessage": "The external key store proxy rejected the request because the
 specified ciphertext or additional authenticated data is corrupted, missing, or
 otherwise invalid.",
    "requestParameters": {
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321",
        "encryptionContext": {
            "Department": "Engineering",
            "Purpose": "Test"
        }
    },
    "responseElements": null,
    "additionalEventData": {
        "customKeyStoreId": "cks-9876543210fedcba9",
        "xksKeyId": "abc01234567890fe"
    },
    "requestID": "f1b881f8-2048-41f8-b6cc-382b7857ec61",
    "eventID": "b79603d5-4cde-46fc-819c-a7cf547b9df4",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
```

```
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

DeleteAlias

L'esempio seguente mostra una voce di AWS CloudTrail registro relativa all'DeleteAliasoperazione. Per informazioni sull'eliminazione di archivi, consulta Eliminazione di un alias.

CloudTrail le voci di registro per questa operazione registrate a partire da dicembre 2022 includono l'ARN della chiave KMS interessata nel `responseElements.keyId` valore, anche se questa operazione non restituisce l'ARN della chiave.

```
{
    "eventVersion": "1.02",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2014-11-04T00:52:27Z"
            }
        }
    },
    "eventTime": "2014-11-04T00:52:27Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DeleteAlias",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
```

```
        "aliasName": "alias/my_alias"
    },
    "responseElements": {
        "keyId":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "d9542792-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "12f48554-bb04-4991-9cfc-e7e85f68eda0",
    "readOnly": false,
    "resources": [{
        "ARN": "arn:aws:kms:us-east-1:111122223333:alias/my_alias",
        "accountId": "111122223333"
    },
    {
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "accountId": "111122223333"
    }],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

DeleteCustomKeyStore

Nell'esempio seguente viene illustrata una voce di log AWS CloudTrail generata chiamando l'operazione `DeleteCustomKeyStore`. Per informazioni sulla creazione di archivi delle chiavi personalizzate, consultare Eliminazione di un archivio delle chiavi di AWS CloudHSM.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2021-10-21T20:17:32Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DeleteCustomKeyStore",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
```

```
    "userAgent": "AWS Internal",
    "requestParameters": {
        "customKeyStoreId": "cks-1234567890abcdef0"
    },
    "responseElements": null,
    "additionalEventData": {
        "customKeyStoreName": "ExampleKeyStore",
        "clusterId": "cluster-1a23b4cdefg"
    },
    "requestID": "abcde9e1-f1a3-4460-a423-577fb6e695c9",
    "eventID": "114b61b9-0ea6-47f5-a9d2-4f2bdd0017d5",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333"
}
```

DeleteExpiredKeyMaterial

Quando importi materiale chiave in una AWS KMS key (chiave KMS), puoi impostare una data e un'ora di scadenza per quel materiale chiave. AWS KMSregistra una voce nel CloudTrail registro quando importi il materiale chiave (con le impostazioni di scadenza) e quando AWS KMS elimini il materiale chiave scaduto. Per ulteriori informazioni sulla creazione di chiavi KMS con materiale chiave importato, consulta Importazione di materiale chiave per le AWS KMS chiavi.

L'esempio seguente mostra una voce di log AWS CloudTrail generata quando AWS KMS elimina il materiale della chiave scaduto.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "111122223333",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2021-01-01T16:00:00Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DeleteExpiredKeyMaterial",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
```

```
    "eventID": "cfa932fd-0d3a-4a76-a8b8-616863a2b547",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "111122223333",
    "serviceEventDetails": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    }
}
```

DeleteImportedKeyMaterial

Se importi materiale chiave in una chiave KMS, puoi eliminare il materiale chiave importato in qualsiasi momento utilizzando l'DeleteImportedKeyMaterialoperazione. Quando elimini il materiale della chiave importato, lo stato della chiave KMS cambia in `PendingImport` e la chiave KMS non potrà essere utilizzata in alcuna operazione di crittografia. Per informazioni dettagliate, vedi Eliminazione del materiale della chiave importato.

L'esempio seguente illustra una voce di log AWS CloudTrail generata per l'operazione `DeleteImportedKeyMaterial`.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2022-10-04T21:43:33Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DeleteImportedKeyMaterial",
    "awsRegion": "us-west-2",
```

```
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": {
        "keyId":"&example-key-arn-1;"
    },
    "requestID": "dcf0e82f-dad0-4622-a378-a5b964ad42c1",
    "eventID": "2afbb991-c668-4641-8a00-67d62e1fecbd",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

DeleteKey

Gli esempi seguenti illustrano la voce di log AWS CloudTrail generata quando viene eliminata una chiave KMS. Per eliminare una chiave KMS, si utilizza l'ScheduleKeyDeletionoperazione. Dopo la scadenza del periodo di attesa specificato, AWS KMS elimina la chiave KMS e registra una voce come la seguente nel CloudTrail registro per registrare l'evento.

CloudTrail le voci di registro per questa operazione registrate a partire da dicembre 2022 includono l'ARN della chiave KMS interessata nel `responseElements.keyId` valore, anche se questa operazione non restituisce l'ARN della chiave.

Per un esempio della voce di CloudTrail registro relativa all'`ScheduleKeyDeletion`operazione, vedere. ScheduleKeyDeletion Per informazioni sull'eliminazione delle chiavi KMS, consulta Eliminazione di AWS KMS keys.

L'esempio seguente di voce di CloudTrail registro registra `DeleteKey` l'operazione di una chiave KMS contenente materiale chiave. AWS KMS

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "111122223333",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2020-07-31T00:07:00Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DeleteKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "b25f9cda-74e1-4458-847b-4972a0bf9668",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "111122223333",
     "managementEvent": true,
    "eventCategory": "Management"
}
```


La seguente voce di CloudTrail registro registra `DeleteKey` l'operazione di una chiave KMS in un archivio di chiavi AWS CloudHSM personalizzato.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "111122223333",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2021-10-26T23:41:27Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DeleteKey",
    "awsRegion": "us-east-1",
```

```
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": {
        "keyId":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "additionalEventData": {
        "customKeyStoreId": "cks-1234567890abcdef0",
        "clusterId": "cluster-1a23b4cdefg",
        "backingKeys": "[{\"keyHandle\":\"01\",\"backingKeyId\":\"backing-key-id\"}]",
        "backingKeysDeletionStatus": "[{\"keyHandle\":\"01\",\"backingKeyId\":
\"backing-key-id\",\"deletionStatus\":\"SUCCESS\"}]"
    },
    "eventID": "1234585c-4b0c-4340-ab11-662414b79239",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "111122223333",
    "managementEvent": true,
    "eventCategory": "Management"
}
```

DescribeCustomKeyStores

Nell'esempio seguente viene illustrata una voce di log AWS CloudTrail generata chiamando l'operazione `DescribeCustomKeyStores`. Per informazioni sulla visualizzazione degli archivi delle chiavi personalizzate, consultare Visualizzazione di un archivio delle chiavi di AWS CloudHSM.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
```

```
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2021-10-21T20:17:32Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeCustomKeyStores",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "customKeyStoreId": "cks-1234567890abcdef0"
    },
    "responseElements": null,
    "requestID": "abcde9e1-f1a3-4460-a423-577fb6e695c9",
    "eventID": "2ea1735f-628d-43e3-b2ee-486d02913a78",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333"
}
```

DescribeKey

L'esempio seguente mostra una voce di AWS CloudTrail registro relativa all'DescribeKeyoperazione. AWS KMSregistra una voce come la seguente quando si richiama l'`DescribeKey`operazione o si visualizzano le chiavi KMS nella AWS KMS console. Questa chiamata è il risultato della visualizzazione di una chiave nella console di gestione AWS KMS.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2022-09-26T18:01:36Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
```

```
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": null,
    "requestID": "12345126-30d5-4b28-98b9-9153da559963",
    "eventID": "abcde202-ba1a-467c-b4ba-f729d45ae521",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

DisableKey

L'esempio seguente mostra una voce di AWS CloudTrail registro relativa all'DisableKeyoperazione. Per informazioni sull'attivazione e la disattivazione di AWS KMS keys in AWS KMS, consulta Abilitazione e disabilitazione delle chiavi.

CloudTrail le voci di registro per questa operazione registrate a partire da dicembre 2022 includono l'ARN della chiave KMS interessata nel `responseElements.keyId` valore, anche se questa operazione non restituisce l'ARN della chiave.

```
{
    "eventVersion": "1.02",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2014-11-04T00:52:43Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DisableKey",
```

```
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": {
        "keyId":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "12345126-30d5-4b28-98b9-9153da559963",
    "eventID": "abcde202-ba1a-467c-b4ba-f729d45ae521",
    "readOnly": false,
    "resources": [{
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "accountId": "111122223333"
    }],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

DisableKeyRotation

Nell'esempio seguente viene illustrata una voce di log AWS CloudTrail generata chiamando l'operazione DisableKeyRotation. Per ulteriori informazioni sulla rotazione automatica delle chiavi, consulta Rotazione delle AWS KMS keys.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2022-09-01T19:31:39Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DisableKeyRotation",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
```

```
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": null,
    "requestID": "d6a9351a-ed6e-4581-88d1-2a9a8a538497",
    "eventID": "6313164c-83aa-4cc3-9e1a-b7c426f7a5b1",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

DisconnectCustomKeyStore

Nell'esempio seguente viene illustrata una voce di log AWS CloudTrail generata chiamando l'operazione `DisconnectCustomKeyStore`. Per informazioni sulla disconnessione di un archivio delle chiavi personalizzate, consultare Connessione e disconnessione di un archivio delle chiavi di AWS CloudHSM.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2021-10-21T20:17:32Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DisconnectCustomKeyStore",
```

```
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "customKeyStoreId": "cks-1234567890abcdef0"
    },
    "responseElements": null,
    "additionalEventData": {
        "customKeyStoreName": "ExampleKeyStore",
        "clusterId": "cluster-1a23b4cdefg"
    },
    "requestID": "abcde9e1-f1a3-4460-a423-577fb6e695c9",
    "eventID": "114b61b9-0ea6-47f5-a9d2-4f2bdd0017d5",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333"
}
```

EnableKey

L'esempio seguente mostra una voce di AWS CloudTrail registro relativa all'EnableKeyoperazione. Per informazioni sull'attivazione e la disattivazione di AWS KMS keys in AWS KMS, consulta Abilitazione e disabilitazione delle chiavi.

CloudTrail le voci di registro per questa operazione registrate a partire da dicembre 2022 includono l'ARN della chiave KMS interessata nel `responseElements.keyId` valore, anche se questa operazione non restituisce l'ARN della chiave.

```
{
    "eventVersion": "1.02",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2014-11-04T00:52:20Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "EnableKey",
    "awsRegion": "us-east-1",
```

```
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": {
        "keyId":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "d528a6fb-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "be393928-3629-4370-9634-567f9274d52e",
    "readOnly": false,
    "resources": [{
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "accountId": "111122223333"
    }],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

EnableKeyRotation

L'esempio seguente mostra una voce di AWS CloudTrail registro di una chiamata all'EnableKeyRotationoperazione. Per un esempio della voce di CloudTrail registro che viene scritta quando la chiave viene ruotata, vedeteRotateKey. Per informazioni sulla rotazione di AWS KMS keys, consulta Rotazione delle AWS KMS keys.

CloudTrail le voci di registro per questa operazione registrate a partire da dicembre 2022 includono l'ARN della chiave KMS interessata nel `responseElements.keyId` valore, anche se questa operazione non restituisce l'ARN della chiave.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2020-07-25T23:41:56Z",
```

```
    "eventSource": "kms.amazonaws.com",
    "eventName": "EnableKeyRotation",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": {
        "keyId":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "81f5b794-452b-4d6a-932b-68c188165273",
    "eventID": "fefc43a7-8e06-419f-bcab-b3bf18d6a401",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

Crittografa

Nell'esempio seguente viene illustrata una voce di log AWS CloudTrail per l'operazione Encrypt.

```
{
    "eventVersion": "1.02",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2022-07-14T20:17:42Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Encrypt",
```

```
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "encryptionContext": {
            "Department": "Engineering"
        },
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
    },
    "responseElements": null,
    "requestID": "f3423043-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "91235988-eb87-476a-ac2c-0cdc244e6dca",
    "readOnly": true,
    "resources": [{
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "accountId": "111122223333"
    }],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

GenerateDataKey

L'esempio seguente mostra una voce di AWS CloudTrail registro relativa all'GenerateDataKeyoperazione.

```
{
    "eventVersion": "1.02",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2014-11-04T00:52:40Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-east-1",
```

```
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "keySpec": "AES_256",
        "encryptionContext": {
            "Department": "Engineering",
            "Project": "Alpha"
        }
    },
    "responseElements": null,
    "requestID": "e0eb83e3-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "a9dea4f9-8395-46c0-942c-f509c02c2b71",
    "readOnly": true,
    "resources": [{
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "accountId": "111122223333"
    }],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

GenerateDataKeyPair

L'esempio seguente mostra una voce di AWS CloudTrail registro relativa all'GenerateDataKeyPairoperazione. In questo esempio viene registrata un'operazione che genera una coppia di chiavi RSA crittografate con una AWS KMS key di crittografia simmetrica.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::111122223333:user/Alice",
            "accountId": "111122223333",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice"
    },
    "eventTime": "2020-07-27T18:57:57Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKeyPair",
    "awsRegion": "us-west-2",
```

```
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyPairSpec": "RSA_3072",
        "encryptionContext": {
            "Project": "Alpha"
        },
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": null,
    "requestID": "52fb127b-0fe5-42bb-8e5e-f560febde6b0",
    "eventID": "9b6bd6d2-529d-4890-a949-593b13800ad7",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```


GenerateDataKeyPairWithoutPlaintext

L'esempio seguente mostra una voce di AWS CloudTrail registro relativa all'GenerateDataKeyPairWithoutPlaintextoperazione. In questo esempio viene registrata un'operazione che genera una coppia di chiavi RSA crittografata con una AWS KMS key di crittografia simmetrica.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::111122223333:user/Alice",
            "accountId": "111122223333",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice"
    },
    "eventTime": "2020-07-27T18:57:57Z",
```

```
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKeyPairWithoutPlaintext",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyPairSpec": "RSA_4096",
        "encryptionContext": {
            "Index": "5"
        },
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": null,
    "requestID": "52fb127b-0fe5-42bb-8e5e-f560febde6b0",
    "eventID": "9b6bd6d2-529d-4890-a949-593b13800ad7",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```


GenerateDataKeyWithoutPlaintext

L'esempio seguente mostra una voce di AWS CloudTrail registro relativa all'GenerateDataKeyWithoutPlaintextoperazione.


```
{
    "eventVersion": "1.02",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
```

```
    "eventTime": "2014-11-04T00:52:23Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKeyWithoutPlaintext",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "errorCode": "InvalidKeyUsageException",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "keySpec": "AES_256",
        "encryptionContext": {
            "Project": "Alpha"
        }
    },
    "responseElements": null,
    "requestID": "d6b8e411-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "f7734272-9ec5-4c80-9f36-528ebbe35e4a",
    "readOnly": true,
    "resources": [{
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "accountId": "111122223333"
    }],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

GenerateMac

L'esempio seguente mostra una voce di AWS CloudTrail registro relativa all'GenerateMacoperazione.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
     },
    "eventTime": "2022-12-23T19:26:54Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateMac",
```

```
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "macAlgorithm": "HMAC_SHA_512",
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": null,
    "requestID": "e0eb83e3-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "a9dea4f9-8395-46c0-942c-f509c02c2b71",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

GenerateRandom

L'esempio seguente mostra una voce di AWS CloudTrail registro relativa all'GenerateRandomoperazione. Poiché questa operazione non utilizza una AWS KMS key, il campo `resources` è vuoto.

```
{
    "eventVersion": "1.02",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2014-11-04T00:52:37Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateRandom",
    "awsRegion": "us-east-1",
```

```
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "df1e3de6-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "239cb9f7-ae05-4c94-9221-6ea30eef0442",
    "readOnly": true,
    "resources": [],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

GetKeyPolicy

L'esempio seguente mostra una voce di AWS CloudTrail registro relativa all'GetKeyPolicyoperazione. Per informazioni sulla visualizzazione della policy delle chiavi per una chiave KMS, consulta Visualizzazione di una policy di chiave.

```
{
    "eventVersion": "1.02",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2014-11-04T00:50:30Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GetKeyPolicy",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "policyName": "default"
    },
    "responseElements": null,
    "requestID": "93746dd6-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "4aa7e4d5-d047-452a-a5a6-2cce282a7e82",
    "readOnly": true,
    "resources": [{
```

```
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "accountId": "111122223333"
    }],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

GetKeyRotationStatus

L'esempio seguente mostra una voce di AWS CloudTrail registro per l'GetKeyRotationStatusoperazione. Per ulteriori informazioni sulla rotazione automatica del materiale della chiave per una chiave KMS, consulta Rotazione delle AWS KMS keys.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2022-09-01T19:32:11Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GetKeyRotationStatus",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": null,
    "requestID": "12f9b7e8-49b9-4c1c-a7e3-34ac0cdf0467",
    "eventID": "3d082126-9e7d-4167-8372-a6cfcbed4be6",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
```

```
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

GetParametersForImport

L'esempio seguente mostra una voce di AWS CloudTrail registro generata quando si utilizza l'GetParametersForImportoperazione. Questa operazione restituisce la chiave pubblica e il token di importazione utilizzati durante l'importazione del materiale della chiave in una chiave KMS. La stessa CloudTrail voce viene registrata quando si utilizza l'`GetParametersForImport`operazione o si utilizza la AWS KMS console per scaricare la chiave pubblica e importare il token.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::111122223333:user/Alice",
            "accountId": "111122223333",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice"
    },
    "eventTime": "2020-07-25T23:58:23Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GetParametersForImport",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "wrappingAlgorithm": "RSAES_OAEP_SHA_256",
        "wrappingKeySpec": "RSA_2048"
    },
    "responseElements": null,
    "requestID": "b5786406-e3c7-43d6-8d3c-6d5ef96e2278",
    "eventID": "4023e622-0c3e-4324-bdef-7f58193bba87",
    "readOnly": true,
    "resources": [
        {
```

```
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

ImportKeyMaterial

L'esempio seguente mostra una voce di AWS CloudTrail registro generata quando si utilizza l'ImportKeyMaterialoperazione. La stessa CloudTrail voce viene registrata quando si utilizza l'`ImportKeyMaterial`operazione o si utilizza la AWS KMS console per importare materiale chiave in unAWS KMS key.

CloudTrail le voci di registro per questa operazione registrate a partire da dicembre 2022 includono l'ARN della chiave KMS interessata nel `responseElements.keyId` valore, anche se questa operazione non restituisce l'ARN della chiave.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::111122223333:user/Alice",
            "accountId": "111122223333",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice"
    },
    "eventTime": "2020-07-26T00:08:00Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "ImportKeyMaterial",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "validTo": "Jan 1, 2021 8:00:00 PM",
        "expirationModel": "KEY_MATERIAL_EXPIRES"
    },
    "responseElements": {
```

```
        "keyId":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "89e10ee7-a612-414d-95a2-a128346969fd",
    "eventID": "c7abd205-a5a2-4430-bbfa-fc10f3e2d79f",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

ListAliases

L'esempio seguente mostra una voce di AWS CloudTrail registro relativa all'ListAliasesoperazione. Poiché questa operazione non utilizza alcun alias particolare o AWS KMS key, il campo `resources` è vuoto. Per informazioni sulla visualizzazione degli alias in AWS KMS, consulta Visualizzazione degli alias.

```
{
    "eventVersion": "1.02",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2014-11-04T00:51:45Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "ListAliases",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "limit": 5,
```

```
        "marker":
 "eyJiIjoiYWxpYXMvZTU0Y2MxOTMtYTMwNC00YzEwLTliZWItYTJjZjA3NjA2OTJhIiwiYSI6ImFsaWFzL2U1NGNjMTkzL
    },
    "responseElements": null,
    "requestID": "bfe6c190-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "a27dda7b-76f1-4ac3-8b40-42dfba77bcd6",
    "readOnly": true,
    "resources": [],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

ListGrants

L'esempio seguente mostra una voce di AWS CloudTrail registro relativa all'ListGrantoperazione. Per informazioni sulle concessioni in AWS KMS, consulta Concessioni in AWS KMS.

```
{
    "eventVersion": "1.02",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2014-11-04T00:52:49Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "ListGrants",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "marker":
 "eyJncmFudElkIjoiMWY4M2U2ZmM0YTY2NDgxYjQ2Yzc4MTdhM2Y4YmQwMDFkZDNiYmQ1MGVlYTMyY2RmOWFiNWY1Nzc1N
\u003d\u003d",
        "limit": 10
    },
    "responseElements": null,
    "requestID": "e5c23960-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "d24380f5-1b20-4253-8e92-dd0492b3bd3d",
```

```
    "readOnly": true,
    "resources": [{
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "accountId": "111122223333"
    }],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

PutKeyPolicy

Nell'esempio seguente viene illustrata una voce di log AWS CloudTrail generata chiamando l'operazione PutKeyPolicy. Per informazioni sull'aggiornamento di una policy delle chiavi, consulta Modifica di una policy delle chiavi.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2022-09-01T20:06:16Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "PutKeyPolicy",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "policyName": "default",
        "policy": "{\n  \"Version\" : \"2012-10-17\",\n  \"Id\" : \"key-default-1\",\n
 \"Statement\" : [ {\n    \"Sid\" : \"Enable IAM User Permissions\",\n    \"Effect\" :
 \"Allow\",\n    \"Principal\" : {\n      \"AWS\" : \"arn:aws:iam::111122223333:root
\"\n    },\n    \"Action\" : \"kms:*\",\n    \"Resource\" : \"*\"\n  } ]\n}",
        "bypassPolicyLockoutSafetyCheck": false
    },
    "responseElements": null,
    "requestID": "7bb906fa-dc21-4350-b65c-808ff0f72f55",
```

```
    "eventID": "c217db1f-903f-4a2f-8f88-9580182d6313",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

ReEncrypt

L'esempio seguente mostra una voce di AWS CloudTrail registro relativa all'ReEncryptoperazione. Il campo `resources` in questa voce di log specifica due AWS KMS keys, la chiave KMS di origine e la chiave KMS di destinazione, in questo ordine.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2020-07-27T23:09:13Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "ReEncrypt",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "sourceEncryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "sourceEncryptionContext": {
            "Project": "Alpha",
            "Department": "Engineering"
```

```
        },
        "destinationKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
        "destinationEncryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "destinationEncryptionContext": {
            "Level": "3A"
        }
    },
    "responseElements": null,
    "requestID": "03769fd4-acf9-4b33-adf3-2ab8ca73aadf",
    "eventID": "542d9e04-0e8d-4e05-bf4b-4bdeb032e6ec",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        },
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

ReplicateKey

Nell'esempio seguente viene illustrata una voce di log AWS CloudTrail generata chiamando l'operazione ReplicateKey. Una `ReplicateKey` richiesta genera un'`ReplicateKey`operazione e un'CreateKeyoperazione.

Per informazioni sulla replica di chiavi in più Regioni, consulta Creazione di chiavi di replica multiregione.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
```

```
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2020-11-18T01:29:18Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "ReplicateKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "replicaRegion": "us-west-2",
        "bypassPolicyLockoutSafetyCheck": false,
        "description": ""
    },
    "responseElements": {
        "replicaKeyMetadata": {
            "aWSAccountId": "111122223333",
            "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
            "arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "creationDate": "Nov 18, 2020, 1:29:18 AM",
            "enabled": false,
            "description": "",
            "keyUsage": "ENCRYPT_DECRYPT",
            "keyState": "Creating",
            "origin": "AWS_KMS",
            "keyManager": "CUSTOMER",
            "keySpec": "SYMMETRIC_DEFAULT",
            "customerMasterKeySpec": "SYMMETRIC_DEFAULT",
            "encryptionAlgorithms": [
                "SYMMETRIC_DEFAULT"
            ],
            "multiRegion": true,
            "multiRegionConfiguration": {
                "multiRegionKeyType": "REPLICA",
                "primaryKey": {
                    "arn": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
                    "region": "us-east-1"
                },
                "replicaKeys": [
```

```
                    {
                        "arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
                        "region": "us-west-2"
                    }
                ]
            }
        },
        "replicaPolicy": "{\n  \"Version\":\"2012-10-17\",\n  \"Statement\":[{\n
 \"Effect\":\"Allow\",\n    \"Principal\":{\"AWS\":\"arn:aws:iam::123456789012:user/
Alice\"},\n    \"Action\":\"kms:*\",\n    \"Resource\":\"*\"\n  }, {\n    \"Effect
\":\"Allow\",\n    \"Principal\":{\"AWS\":\"arn:aws:iam::012345678901:user/Bob\"},\n
    \"Action\":\"kms:CreateGrant\",\n    \"Resource\":\"*\"\n  }, {\n    \"Effect\":
\"Allow\",\n    \"Principal\":{\"AWS\":\"arn:aws:iam::012345678901:user/Charlie\"},\n
  \"Action\":\"kms:Encrypt\",\n    \"Resource\":\"*\"\n}]\n}",
    },
    "requestID": "abcdef68-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "fedcba44-6773-4f96-8763-1993aec9ae6a",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

RetireGrant

Nell'esempio seguente viene illustrata una voce di log AWS CloudTrail generata chiamando l'operazione RetireGrant. Per informazioni su come ritirare le concessioni, consulta Ritirare e revocare le concessioni.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
```

```
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2022-09-01T19:39:33Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "RetireGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "grantId": "abcde1237f76e4ba7987489ac329fbfba6ad343d6f7075dbd1ef191f0120514a"
    },
    "requestID": "1d274d57-5697-462c-a004-f25fcc29fa26",
    "eventID": "0771bcfb-3e24-4332-9ac8-e1c06563eecf",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


RevokeGrant

Nell'esempio seguente viene illustrata una voce di log AWS CloudTrail generata chiamando l'operazione RevokeGrant. Per informazioni su come revocare le concessioni, consulta Ritirare e revocare le concessioni.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
```

```
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2022-09-01T19:35:17Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "RevokeGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "grantId": "abcde1237f76e4ba7987489ac329fbfba6ad343d6f7075dbd1ef191f0120514a"
    },
    "responseElements": null,
    "requestID": "59d94c03-c5b7-428d-ae6e-f2c4b47d2917",
    "eventID": "07a23a39-6526-4ae2-b31e-d35fbe9e24ee",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


RotateKey

Nell'esempio seguente viene illustrata una voce di log AWS CloudTrail dell'operazione che ruota una AWS KMS key. AWS KMS chiama questa operazione quando è il momento di ruotare una chiave KMS su cui è abilitata la rotazione automatica delle chiavi. Quando abiliti la rotazione automatica delle chiavi (EnableKeyRotation), AWS KMS ruota la chiave KMS 365 giorni dopo e successivamente ogni 365 giorni.

CloudTrail le voci di registro per questa operazione registrate a partire da dicembre 2022 includono l'ARN della chiave KMS interessata nel `responseElements.keyId` valore, anche se questa operazione non restituisce l'ARN della chiave.

Per un esempio della voce di CloudTrail registro che registra l'`EnableKeyRotation`operazione, vedere. EnableKeyRotation Per informazioni sulla rotazione delle chiavi KMS, consulta Rotazione delle AWS KMS keys.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "111122223333",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2021-01-14T01:41:59Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "RotateKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": {
        "keyId":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "eventID": "a24b3967-ddad-417f-9b22-2332b918db06",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "111122223333",
    "serviceEventDetails": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    }
}
```

ScheduleKeyDeletion

Questi esempi mostrano le voci di AWS CloudTrail registro relative all'ScheduleKeyDeletionoperazione.

Per un esempio della voce di CloudTrail registro che viene scritta quando la chiave viene eliminata, vedereDeleteKey. Per informazioni sull'eliminazione delle AWS KMS keys, consulta Eliminazione di AWS KMS keys.

Nell'esempio seguente viene registrata una richiesta `ScheduleKeyDeletion` di una chiave KMS a Regione singola.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::111122223333:user/Alice",
            "accountId": "111122223333",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice"
    },
    "eventTime": "2021-03-23T18:58:30Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "ScheduleKeyDeletion",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "pendingWindowInDays": 20,
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": {
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "keyState": "PendingDeletion",
        "deletionDate": "Apr 12, 2021 18:58:30 PM"
    },
    "requestID": "ee408f36-ea01-422b-ac14-b0f147c68334",
    "eventID": "3c4226b0-1e81-48a8-a333-7fa5f3cbd118",
    "readOnly": false,
    "resources": [
        {
```

```
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

Nell'esempio seguente viene registrata una richiesta `ScheduleKeyDeletion` di una chiave KMS multi-Regione con chiavi di replica.

Poiché AWS KMS non eliminerà una chiave multi-regione fino a quando tutte le sue chiavi di replica non vengono eliminate, nel campo `responseElements` il `keyState` è `PendingReplicaDeletion` e il campo `deletionDate` viene omesso.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::111122223333:user/Alice",
            "accountId": "111122223333",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice"
    },
    "eventTime": "2021-10-28T17:59:05Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "ScheduleKeyDeletion",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "pendingWindowInDays": 30,
        "keyId": "mrk-1234abcd12ab34cd56ef1234567890ab"
    },
    "responseElements": {
        "keyId": "arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
        "keyState": "PendingReplicaDeletion",
        "pendingWindowInDays": 30
    },
```

```
    "requestID": "12341411-d846-42a6-a476-b1cbe3011f89",
    "eventID": "abcda5f-396d-494c-9380-0c47860df5f1",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Nell'esempio seguente viene registrata una richiesta `ScheduleKeyDeletion` di una chiave KMS in un archivio delle chiavi personalizzate AWS CloudHSM.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::111122223333:user/Alice",
            "accountId": "111122223333",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice"
    },
    "eventTime": "2021-10-26T23:25:25Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "ScheduleKeyDeletion",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321",
        "pendingWindowInDays": 30
    },
    "responseElements": {
```

```
        "keyId": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321",
        "deletionDate": "Nov 2, 2021, 11:25:25 PM",
        "keyState": "PendingDeletion",
        "pendingWindowInDays": 30
    },
    "additionalEventData": {
        "customKeyStoreId": "cks-1234567890abcdef0",
        "clusterId": "cluster-1a23b4cdefg",
        "backingKeys": "[{\"keyHandle\":\"01\",\"backingKeyId\":\"backing-key-id\"}]"
    },
    "requestID": "abcd9f60-2c9c-4a0b-a456-d5d998f7f321",
    "eventID": "ca01996a-01b0-4edd-bbbb-25d7b6d1a6fa",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Sign

Questi esempi mostrano le voci di log AWS CloudTrail per l'operazione Sign.

L'esempio seguente mostra una voce di CloudTrail registro per un'operazione Sign che utilizza una chiave RSA KMS asimmetrica per generare una firma digitale per un file.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
```

```
        "userName": "Alice"
    },
    "eventTime": "2022-03-07T22:36:44Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Sign",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "messageType": "RAW",
        "keyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
        "signingAlgorithm": "RSASSA_PKCS1_V1_5_SHA_256"
    },
    "responseElements": null,
    "requestID": "8d0b35e0-46cf-48b9-be99-bf2ebc9ab9fb",
    "eventID": "107b3cac-b125-4556-9702-12a2b9afcff7",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


SynchronizeMultiRegionKey

L'esempio seguente mostra una voce di log AWS CloudTrail generata quando AWS KMS sincronizza una chiave per più Regioni. La sincronizzazione coinvolge le chiamate tra Regioni diverse per copiare le proprietà condivise di una chiave primaria in più Regioni alle relative chiavi di replica. AWS KMS sincronizza periodicamente le chiavi in più Regioni per garantire che tutte le chiavi in più Regioni correlate abbiano lo stesso materiale chiave.

L'`resources`elemento della voce di CloudTrail registro include la chiave ARN della chiave primaria multiregionale, inclusa la sua. Regione AWS Le chiavi di replica in più Regioni correlate e le relative Regioni non sono elencate in questa voce di log.

CloudTrail le voci di registro per questa operazione registrate a partire da dicembre 2022 includono l'ARN della chiave KMS interessata nel `responseElements.keyId` valore, anche se questa operazione non restituisce l'ARN della chiave.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "111122223333",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2020-11-18T02:04:37Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "SynchronizeMultiRegionKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": {
        "keyId":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "12345681-de97-42e9-bed0-b02ae1abd8dc",
    "eventID": "abcdec99-2b5c-4670-9521-ddb8f031e146",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


TagResource

L'esempio seguente mostra una voce di AWS CloudTrail registro di una chiamata all'TagResourceoperazione per aggiungere un tag con una chiave di tag `Department` e un valore di tag di`IT`.

Per un esempio di una voce di `UntagResource` CloudTrail registro che viene scritta quando la chiave viene ruotata, vedeteUntagResource. Per informazioni sull'assegnazione di tag per AWS KMS keys, consulta Chiavi di tagging.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2020-07-01T21:19:25Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "TagResource",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "tags": [
            {
                "tagKey": "Department",
                "tagValue": "IT"
            }
        ]
    },
    "responseElements": null,
    "requestID": "b942584a-f77d-4787-9feb-b9c5be6e746d",
    "eventID": "0a091b9b-0df5-4cf9-b667-6f2879532b8f",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
```

```
    "recipientAccountId": "111122223333"
}
```

UntagResource

L'esempio seguente mostra una voce di AWS CloudTrail registro di una chiamata all'UntagResourceoperazione per eliminare un tag con una chiave di tag di`Dept`.

CloudTrail le voci di registro per questa operazione registrate a partire da dicembre 2022 includono l'ARN della chiave KMS interessata nel `responseElements.keyId` valore, anche se questa operazione non restituisce l'ARN della chiave.

Per un esempio di voce di `TagResource` CloudTrail registro, vedere. TagResource Per informazioni sull'assegnazione di tag per AWS KMS keys, consulta Chiavi di tagging.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2020-07-01T21:19:19Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "UntagResource",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "tagKeys": [
            "Dept"
        ]
    },
    "responseElements": {
        "keyId":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
```

```
    "requestID": "cb1d507b-6015-47f4-812b-179713af8068",
    "eventID": "0b00f4b0-036e-411d-aa75-87eb4a35a4b3",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

UpdateAlias

L'esempio seguente mostra una voce di AWS CloudTrail registro relativa all'UpdateAliasoperazione. L'elemento `resources` include i campi per l'alias e le risorse della chiave KMS. Per informazioni sulla creazione di alias in AWS KMS, consulta Creazione di un alias.

CloudTrail le voci di registro per questa operazione registrate a partire da dicembre 2022 includono l'ARN della chiave KMS interessata nel `responseElements.keyId` valore, anche se questa operazione non restituisce l'ARN della chiave.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
         "principalId": "EX_PRINCIPAL_ID",
         "arn": "arn:aws:iam::111122223333:user/Alice",
         "accountId": "111122223333",
         "accessKeyId": "EXAMPLE_KEY_ID",
         "userName": "Alice"
    },
    "eventTime": "2020-11-13T23:18:15Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "UpdateAlias",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "aliasName": "alias/my_alias",
```

```
        "targetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": {
        "keyId":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "d9472f40-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "f72d3993-864f-48d6-8f16-e26e1ae8dff0",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-west-2:111122223333:alias/my_alias"
        },
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

UpdateCustomKeyStore

Nell'esempio seguente viene mostrata una voce di log AWS CloudTrail generata chiamando l'operazione `UpdateCustomKeyStore` per aggiornare l'ID cluster per un archivio chiavi personalizzate. Per informazioni sulla modifica degli archivi delle chiavi personalizzate, consultare Modifica delle impostazioni di un archivio delle chiavi di AWS CloudHSM.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
```

```
    "eventTime": "2021-10-21T20:17:32Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "UpdateCustomKeyStore",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "customKeyStoreId": "cks-1234567890abcdef0",
        "clusterId": "cluster-1a23b4cdefg"
    },
    "responseElements": null,
    "additionalEventData": {
        "customKeyStoreName": "ExampleKeyStore",
        "clusterId": "cluster-1a23b4cdefg"
    },
    "requestID": "abcde9e1-f1a3-4460-a423-577fb6e695c9",
    "eventID": "114b61b9-0ea6-47f5-a9d2-4f2bdd0017d5",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333"
}
```


UpdateKeyDescription

Nell'esempio seguente viene illustrata una voce di log AWS CloudTrail generata chiamando l'operazione UpdateKeyDescription.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2022-09-01T19:22:40Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "UpdateKeyDescription",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
```

```
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "description": "New key description"
    },
    "responseElements": null,
    "requestID": "8c3c1f8b-336d-4896-b034-4eb9916bc9b3",
    "eventID": "f5f3d548-2e9e-4658-8427-9dcb5b1ea791",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

UpdatePrimaryRegion

L'esempio seguente mostra le voci di AWS CloudTrail registro generate richiamando l'UpdatePrimaryRegionoperazione su una chiave multiregionale.

L'`UpdatePrimaryRegion`operazione scrive due voci di CloudTrail registro: una nella regione con la chiave primaria multiregionale convertita in una chiave di replica e una nella regione con una chiave di replica multiarea convertita in una chiave primaria.

CloudTrail le voci di registro per questa operazione registrate a partire da dicembre 2022 includono l'ARN della chiave KMS interessata nel `responseElements.keyId` valore, anche se questa operazione non restituisce l'ARN della chiave.

L'esempio seguente mostra una voce di CloudTrail registro relativa alla regione `UpdatePrimaryRegion` in cui la chiave multiregionale è passata da una chiave primaria a una chiave di replica (us-west-2). Il campo `primaryRegion` mostra la Regione che ora ospita la chiave primaria (ap-northeast-1).

```
{
```

```
    "eventVersion": "1.08",
    "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::111122223333:user/Alice",
            "accountId": "111122223333",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice"
    },
    "eventTime": "2021-03-10T20:23:37Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "UpdatePrimaryRegion",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "mrk-1234abcd12ab34cd56ef1234567890ab",
        "primaryRegion": "ap-northeast-1"
    },
    "responseElements": {
        "keyId":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "ee408f36-ea01-422b-ac14-b0f147c68334",
    "eventID": "3c4226b0-1e81-48a8-a333-7fa5f3cbd118",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```


L'esempio seguente rappresenta la voce di CloudTrail registro relativa alla regione `UpdatePrimaryRegion` in cui la chiave multiregionale è passata da una chiave di replica a una chiave primaria (ap-northeast-1). Questa voce di log non identifica la Regione principale precedente.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::111122223333:user/Alice",
            "accountId": "111122223333",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "invokedBy": "kms.amazonaws.com"
    },
    "eventTime": "2021-03-10T20:23:37Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "UpdatePrimaryRegion",
    "awsRegion": "ap-northeast-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "arn:aws:kms:ap-northeast-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
        "primaryRegion": "ap-northeast-1"
    },
    "responseElements": {
        "keyId":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "ee408f36-ea01-422b-ac14-b0f147c68334",
    "eventID": "091e6be5-737f-43c6-8431-e3679d6d0619",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```

VerifyMac

L'esempio seguente mostra una voce di AWS CloudTrail registro relativa all'VerifyMacoperazione.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
```

```
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
     },
    "eventTime": "2022-03-31T19:25:54Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "VerifyMac",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "macAlgorithm": "HMAC_SHA_384",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": null,
    "requestID": "f35da560-edff-4d6e-9b40-fb306fa9ef1e",
    "eventID": "6b464487-6dea-44cd-84ad-225d7450c975",
    "readOnly": true,
    "resources": [
        {
           "accountId": "111122223333",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Verifica

Questi esempi mostrano le voci di log AWS CloudTrail per l'operazione Verify.

L'esempio seguente mostra una voce di CloudTrail registro per un'operazione Verify che utilizza una chiave RSA KMS asimmetrica per verificare una firma digitale.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
```

```
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2022-03-07T22:50:41Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Verify",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "signingAlgorithm": "RSASSA_PKCS1_V1_5_SHA_256",
        "keyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
        "messageType": "RAW"
    },
    "responseElements": null,
    "requestID": "c73ab82a-af82-4750-ae2c-b6bb790e9c28",
    "eventID": "3b4331cd-5b7b-4de5-bf5f-82ec22f0dac0",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Esempio uno di Amazon EC2

L'esempio seguente registra la creazione di un volume crittografato da parte di un principale IAM utilizzando la chiave di volume predefinita nella console di gestione Amazon EC2.

L'esempio seguente mostra una voce di CloudTrail registro in cui l'utente Alice crea un volume crittografato con una chiave di volume predefinita nella console di gestione Amazon EC2. Il

record del file di log di EC2 include un campo `volumeId` con un valore di `"vol-13439757"`. Il record AWS KMS contiene un campo `encryptionContext` con un valore di `"aws:ebs:id": "vol-13439757"`. Analogamente, il `principalId` e l'`accountId` tra i due record corrispondono. I record riflettono il fatto che la creazione di un volume crittografato genera una chiave di dati utilizzata per crittografare il contenuto del volume.

```
{
  "Records": [
     {
      "eventVersion": "1.02",
      "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::111122223333:user/Alice",
            "accountId": "111122223333",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice"
        },
      "eventTime": "2014-11-05T20:50:18Z",
      "eventSource": "ec2.amazonaws.com",
      "eventName": "CreateVolume",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "AWS Internal",
      "requestParameters": {
        "size": "10",
        "zone": "us-east-1a",
        "volumeType": "gp2",
        "encrypted": true
      },
      "responseElements": {
        "volumeId": "vol-13439757",
        "size": "10",
        "zone": "us-east-1a",
        "status": "creating",
        "createTime": 1415220618876,
        "volumeType": "gp2",
        "iops": 30,
        "encrypted": true
      },
      "requestID": "1565210e-73d0-4912-854c-b15ed349e526",
      "eventID": "a3447186-135f-4b00-8424-bc41f1a93b4f",
      "eventType": "AwsApiCall",
```

```
      "recipientAccountId": "123456789012"
    },
    {
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
      },
      "eventTime": "2014-11-05T20:50:19Z",
      "eventSource": "kms.amazonaws.com",
      "eventName": "GenerateDataKeyWithoutPlaintext",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "&AWS; Internal",
      "requestParameters": {
        "encryptionContext": {
          "aws:ebs:id": "vol-13439757"
        },
        "numberOfBytes": 64,
        "keyId": "alias/aws/ebs"
      },
      "responseElements": null,
      "requestID": "create-123456789012-758241111-1415220618",
      "eventID": "4bd2a696-d833-48cc-b72c-05e61b608399",
      "readOnly": true,
      "resources": [
        {
          "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
          "accountId": "111122223333"
        }
      ],
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    }
  ]
}
```

Esempio due di Amazon EC2

Nell'esempio seguente, un principale IAM che esegue un'istanza Amazon EC2 crea e monta un volume di dati crittografato in una chiave KMS. Questa azione genera più record di CloudTrail registro.

Quando il volume viene creato, Amazon EC2, agendo per conto del cliente, ottiene una chiave dati crittografata da AWS KMS (`GenerateDataKeyWithoutPlaintext`). Quindi crea un'autorizzazione (`CreateGrant`) che gli consente di decrittografare la chiave dati. Quando il volume è montato, Amazon EC2 chiama AWS KMS per decrittare la chiave dati (`Decrypt`).

`instanceId` dell'istanza Amazon EC2, `"i-81e2f56c"`, viene visualizzato nell'evento `RunInstances`. Lo stesso ID dell'istanza qualifica l'elemento `granteePrincipal` dell'autorizzazione creato (`"111122223333:aws:ec2-infrastructure:i-81e2f56c"`) e il ruolo assunto che è l'entità nella chiamata `Decrypt` (`"arn:aws:sts::111122223333:assumed-role/aws:ec2-infrastructure/i-81e2f56c"`).

L'ARN della chiave KMS che protegge il volume dei dati, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`, viene mostrato in tutte e tre le chiamate AWS KMS (`CreateGrant`, `GenerateDataKeyWithoutPlaintext` e `Decrypt`).


```
{
  "Records": [
    {
      "eventVersion": "1.02",
      "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::111122223333:user/Alice",
            "accountId": "111122223333",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice"
      },
      "eventTime": "2014-11-05T21:35:27Z",
      "eventSource": "ec2.amazonaws.com",
      "eventName": "RunInstances",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "AWS Internal",
      "requestParameters": {
        "instancesSet": {
```

```
          "items": [
            {
              "imageId": "ami-b66ed3de",
              "minCount": 1,
              "maxCount": 1
            }
          ]
        },
        "groupSet": {
          "items": [
            {
              "groupId": "sg-98b6e0f2"
            }
          ]
        },
        "instanceType": "m3.medium",
        "blockDeviceMapping": {
          "items": [
            {
              "deviceName": "/dev/xvda",
              "ebs": {
                "volumeSize": 8,
                "deleteOnTermination": true,
                "volumeType": "gp2"
              }
            },
            {
              "deviceName": "/dev/sdb",
              "ebs": {
                "volumeSize": 8,
                "deleteOnTermination": false,
                "volumeType": "gp2",
                "encrypted": true
              }
            }
          ]
        },
        "monitoring": {
          "enabled": false
        },
        "disableApiTermination": false,
        "instanceInitiatedShutdownBehavior": "stop",
        "clientToken": "XdKUT141516171819",
        "ebsOptimized": false
```

```
    },
    "responseElements": {
      "reservationId": "r-5ebc9f74",
      "ownerId": "111122223333",
      "groupSet": {
        "items": [
          {
            "groupId": "sg-98b6e0f2",
            "groupName": "launch-wizard-2"
          }
        ]
      },
      "instancesSet": {
        "items": [
          {
            "instanceId": "i-81e2f56c",
            "imageId": "ami-b66ed3de",
            "instanceState": {
              "code": 0,
              "name": "pending"
            },
            "amiLaunchIndex": 0,
            "productCodes": {

            },
            "instanceType": "m3.medium",
            "launchTime": 1415223328000,
            "placement": {
              "availabilityZone": "us-east-1a",
              "tenancy": "default"
            },
            "monitoring": {
              "state": "disabled"
            },
            "stateReason": {
              "code": "pending",
              "message": "pending"
            },
            "architecture": "x86_64",
            "rootDeviceType": "ebs",
            "rootDeviceName": "/dev/xvda",
            "blockDeviceMapping": {

            },
```

```
            "virtualizationType": "hvm",
            "hypervisor": "xen",
            "clientToken": "XdKUT1415223327917",
            "groupSet": {
              "items": [
                {
                  "groupId": "sg-98b6e0f2",
                  "groupName": "launch-wizard-2"
                }
              ]
            },
            "networkInterfaceSet": {

            },
            "ebsOptimized": false
          }
        ]
      }
    },
    "requestID": "41c4b4f7-8bce-4773-bf0e-5ae3bb5cbce2",
    "eventID": "cd75a605-2fee-4fda-b847-9c3d330ebaae",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
  },
  {
    "eventVersion": "1.02",
    "userIdentity": {
          "type": "IAMUser",
          "principalId": "EX_PRINCIPAL_ID",
          "arn": "arn:aws:iam::111122223333:user/Alice",
          "accountId": "111122223333",
          "accessKeyId": "EXAMPLE_KEY_ID",
          "userName": "Alice"
    },
    "eventTime": "2014-11-05T21:35:35Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
      "constraints": {
        "encryptionContextSubset": {
          "aws:ebs:id": "vol-f67bafb2"
```

```
          }
        },
        "granteePrincipal": "111122223333:aws:ec2-infrastructure:i-81e2f56c",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
      },
      "responseElements": {
        "grantId": "abcde1237f76e4ba7987489ac329fbfba6ad343d6f7075dbd1ef191f0120514a"
      },
      "requestID": "41c4b4f7-8bce-4773-bf0e-5ae3bb5cbce2",
      "eventID": "c1ad79e3-0d3f-402a-b119-d5c31d7c6a6c",
      "readOnly": false,
      "resources": [
        {
          "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
          "accountId": "111122223333"
        }
      ],
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.02",
      "userIdentity": {
          "type": "IAMUser",
          "principalId": "EX_PRINCIPAL_ID",
          "arn": "arn:aws:iam::111122223333:user/Alice",
          "accountId": "111122223333",
          "accessKeyId": "EXAMPLE_KEY_ID",
          "userName": "Alice"
      },
      "eventTime": "2014-11-05T21:35:32Z",
      "eventSource": "kms.amazonaws.com",
      "eventName": "GenerateDataKeyWithoutPlaintext",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "AWS Internal",
      "requestParameters": {
        "encryptionContext": {
          "aws:ebs:id": "vol-f67bafb2"
        },
        "numberOfBytes": 64,
        "keyId": "alias/aws/ebs"
```

```
      },
      "responseElements": null,
      "requestID": "create-111122223333-758247346-1415223332",
      "eventID": "ac3cab10-ce93-4953-9d62-0b6e5cba651d",
      "readOnly": true,
      "resources": [
        {
          "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
          "accountId": "111122223333"
        }
      ],
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "111122223333:aws:ec2-infrastructure:i-81e2f56c",
        "arn": "arn:aws:sts::111122223333:assumed-role/aws:ec2-infrastructure/
i-81e2f56c",
        "accountId": "111122223333",
        "accessKeyId": "",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-11-05T21:35:38Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "111122223333:aws:ec2-infrastructure",
            "arn": "arn:aws:iam::111122223333:role/aws:ec2-infrastructure",
            "accountId": "111122223333",
            "userName": "aws:ec2-infrastructure"
          }
        }
      },
      "eventTime": "2014-11-05T21:35:47Z",
      "eventSource": "kms.amazonaws.com",
      "eventName": "Decrypt",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "requestParameters": {
```

```
        "encryptionContext": {
          "aws:ebs:id": "vol-f67bafb2"
        }
      },
      "responseElements": null,
      "requestID": "b4b27883-6533-11e4-b4d9-751f1761e9e5",
      "eventID": "edb65380-0a3e-4123-bbc8-3d1b7cff49b0",
      "readOnly": true,
      "resources": [
        {
          "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
          "accountId": "111122223333"
        }
      ],
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    }
  ]
}
```

Monitoraggio con Amazon CloudWatch

Puoi monitorare i tuoi dati AWS KMS keys utilizzando Amazon CloudWatch, un AWS servizio che raccoglie ed elabora dati grezzi AWS KMS trasformandoli in metriche leggibili quasi in tempo reale. Questi dati sono registrati per un periodo di due settimane, in modo da accedere a informazioni cronologiche e comprendere meglio l'utilizzo delle chiavi KMS e le loro modifiche nel corso del tempo.

Puoi usare Amazon CloudWatch per avvisarti di eventi importanti, come i seguenti.

- Il materiale chiave importato in una chiave KMS si avvicina alla data di scadenza.
- Viene ancora utilizzata una chiave KMS in attesa di eliminazione.
- Il materiale chiave di una chiave KMS è stato ruotato automaticamente.
- È stata eliminata una chiave KMS.

Puoi anche creare un CloudWatch allarme Amazon che ti avvisi quando la frequenza delle richieste raggiunge una determinata percentuale del valore di quota. Per i dettagli, consulta Gestisci le tariffe di richiesta AWS KMS API utilizzando Service Quotas e Amazon CloudWatch nel blog sulla AWSsicurezza.

Argomenti

Parametri e dimensioni di AWS KMS

AWS KMSpredefinisce i CloudWatch parametri di Amazon per semplificare il monitoraggio dei dati critici e la creazione di allarmi. Puoi visualizzare le AWS KMS metriche utilizzando l' CloudWatch API AWS Management Console e Amazon.

Questa sezione elenca ogni AWS KMS metrica e le relative dimensioni e fornisce alcune linee guida di base per la creazione di CloudWatch allarmi basati su tali metriche e dimensioni.

> **Note**
>
> Nome del gruppo di dimensioni:
> Per visualizzare una metrica nella CloudWatch console Amazon, nella sezione Metriche, seleziona il nome del gruppo di dimensioni. Quindi, puoi filtrare in base a Metric name (Nome parametro). Questo argomento include il nome del parametro e il nome del gruppo di dimensioni per ogni parametro AWS KMS.

Argomenti

SecondsUntilKeyMaterialExpiration

Il numero di secondi rimanenti fino alla scadenza del materiale della chiave importato in una chiave KMS. Questo parametro è valido solo per le chiavi KMS con un materiale della chiave importato (un'origine del materiale della chiave di `EXTERNAL`) e una data di scadenza.

Utilizza questo parametro per tenere traccia del tempo che rimane fino alla scadenza del materiale della chiave importato. Quando questo periodo di tempo scende al di sotto di una soglia definita, puoi reimportare il materiale della chiave con una nuova data di scadenza. Il parametro `SecondsUntilKeyMaterialExpiration` è specifico per una chiave KMS. Non puoi utilizzare questo parametro per monitorare più chiavi KMS o chiavi KMS che potresti creare in futuro. Per assistenza sulla creazione di un CloudWatch allarme per monitorare questa metrica, consulta. Creazione di un CloudWatch avviso di scadenza del materiale chiave importato

La statistica più utile per questo parametro è `Minimum`, che indica la quantità minima di tempo rimanente per tutti i punti dati nel periodo statistico specificato. L'unica unità valida per questo periodo è `Seconds`.

Nome del gruppo di dimensioni: Per-Key Metrics (Parametri per chiave)

Dimensioni per **`SecondsUntilKeyMaterialExpiration`**

Dimensione	Descrizione relativa ad AWS
KeyId	Valore per ogni chiave KMS.

ExternalKeyStoreThrottle

Il numero di richieste di operazioni di crittografia sulle chiavi KMS in ogni archivio delle chiavi esterne limitato da AWS KMS (risponde con un'eccezione `ThrottlingException`). Questo parametro si applica solo agli archivi delle chiave esterne.

La `ExternalKeyStoreThrottle` metrica si applica solo alle chiavi KMS in un archivio di chiavi esterno e solo alle richieste di operazioni crittografiche e all'operazione. DescribeKey AWS KMSlimita queste richieste quando il tasso di richiesta supera la quota di richieste di archivio chiavi personalizzato per l'archivio di chiavi esterno. Questo parametro non include la limitazione (della larghezza di banda della rete) da parte del proxy dell'archivio delle chiavi esterne o del gestore delle chiavi esterne.

Utilizza questo parametro per verificare e modificare il valore della quota di richiesta dell'archivio delle chiavi personalizzate. Se tale parametro indica che AWS KMS limita di frequente le richieste per queste chiavi KMS, potresti prendere in considerazione la possibilità di richiedere un aumento del valore della quota di richiesta dell'archivio delle chiavi personalizzate. Per ricevere assistenza, consulta Richiesta di un aumento di quota nella Guida per l'utente delle Service Quotas.

Se ricevi frequentemente errori `KMSInvalidStateException` con un messaggio che descrive il rifiuto della richiesta "a causa di un tasso di richieste molto elevato" o "perché il proxy dell'archivio delle chiavi esterne non ha risposto in tempo", ciò potrebbe indicare che il gestore delle chiavi esterne o il proxy non è in grado di sostenere la frequenza di richieste corrente. Se possibile, riduci il tasso di richiesta. Potresti anche prendere in considerazione la possibilità di richiedere una riduzione del valore della quota di richiesta dell'archivio delle chiavi personalizzate. La riduzione di tale valore potrebbe aumentare la limitazione (della larghezza di banda della rete) e il valore del parametro `ExternalKeyStoreThrottle`, tuttavia indica che AWS KMS rifiuta rapidamente le richieste in eccesso prima che vengano inviate al proxy dell'archivio delle chiavi esterne o al gestore delle chiavi esterne. Per richiedere una riduzione della quota, consulta la sezione Centro AWS Support e crea un caso.

Nome del gruppo di dimensioni: Keystore Throttle Metrics (Parametri di limitazione del keystore)

Dimensione	Descrizione
CustomKeyStoreId	Valore per ogni archivio delle chiavi esterne.
KmsOperation	Valore per ogni operazione API AWS KMS. Questo parametro si applica solo alle operazioni di crittografia e all'operazione `DescribeKey` sulle chiavi KMS in un archivio delle chiavi esterne.
KeySpec	Valore per ogni tipo di chiave KMS. L'unica specifica della chiave supportata per le chiavi KMS in un archivio delle chiavi esterne è SYMMETRIC_DEFAULT.

XksProxyCertificateDaysToExpire

Il numero di giorni che mancano alla scadenza del certificato TLS per l'endpoint proxy dell'archivio delle chiavi esterne (`XksProxyUriEndpoint`). Questo parametro si applica solo agli archivi delle chiave esterne.

Usa questa metrica per creare un CloudWatch allarme che ti avvisi della scadenza imminente del tuo certificato TLS. Alla scadenza del certificato, AWS KMS non è in grado di comunicare con il proxy dell'archivio delle chiavi esterne. Tutti i dati protetti dalle chiavi KMS nell'archivio delle chiavi esterne diventano inaccessibili fino al rinnovo del certificato.

Dal momento che la scadenza di un certificato potrebbe impedirti di accedere alle risorse crittografate, un avviso relativo al certificato potrebbe risultare utile. Configura l'allarme in modo che l'organizzazione abbia la possibilità di rinnovare il certificato prima della sua scadenza.

Nome del gruppo di dimensioni: XKS Proxy Certificate Metrics (Parametri del certificato proxy XKS)

Dimensione	Descrizione
CustomKeyStoreId	Valore per ogni archivio delle chiavi esterne.
CertificateName	Nome del soggetto (CN) nel certificato TLS.

XksProxyCredentialAge

Il numero di giorni trascorsi dell'associazione delle credenziali di autenticazione proxy (`XksProxyAuthenticationCredential`) all'archivio delle chiavi esterne. Questo conteggio inizia quando inserisci le credenziali di autenticazione come parte della creazione o dell'aggiornamento dell'archivio delle chiavi esterne. Questo parametro si applica solo agli archivi delle chiave esterne.

Questo valore è progettato per ricordarti l'età delle credenziali di autenticazione. Tuttavia, poiché il conteggio inizia dal momento in cui associ le credenziali all'archivio delle chiavi esterne e non dalla loro data di creazione, l'indicazione dell'età potrebbe non essere accurata.

Usa questa metrica per creare un CloudWatch allarme che ti ricordi di ruotare le credenziali di autenticazione proxy del key store esterno.

Nome del gruppo di dimensioni: Per-Keystore Metrics (Parametri per keystore)

Dimensione	Descrizione
CustomKeyStoreId	Valore per ogni archivio delle chiavi esterne.

XksProxyErrors

Il numero di eccezioni relative alle richieste AWS KMS indirizzate al proxy dell'archivio delle chiavi esterne. Questo conteggio include le eccezioni che il proxy dell'archivio delle chiavi esterne restituisce ad AWS KMS e gli errori di timeout che si verificano quando il proxy non risponde ad AWS KMS entro l'intervallo di 250 millisecondi. Questo parametro si applica solo agli archivi delle chiave esterne.

Utilizza questo parametro per tenere traccia del tasso di errore delle chiavi KMS nell'archivio delle chiavi esterne. Rivela gli errori più frequenti, in modo da consentirti di assegnare priorità diverse agli interventi tecnici. Ad esempio, le chiavi KMS che generano alti tassi di errori irreversibili potrebbero indicare un problema con la configurazione dell'archivio delle chiavi esterne. Per visualizzare la configurazione dell'archivio delle chiavi esterne, consulta Visualizzazione di un archivio delle chiavi esterne. Per modificare le impostazioni dell'archivio delle chiavi esterne, consulta Modifica delle proprietà dell'archivio delle chiavi esterne.

Nome del gruppo di dimensioni: XKS Proxy Error Metrics (Parametri di errore del proxy XKS)

Dimensione	Descrizione
CustomKeyStoreId	Valore per ogni archivio delle chiavi esterne.
KmsOperation	Valore per ogni operazione API AWS KMS che ha generato una richiesta al proxy XKS.
XksOperation	Valore per ogni operazione API proxy dell'archivio delle chiavi esterne.
KeySpec	Valore per ogni tipo di chiave KMS. L'unica specifica della chiave supportata per le chiavi KMS in un archivio delle chiavi esterne è SYMMETRIC_DEFAULT.
ErrorType	Valori: • Errori non irreversibili: possono essere temporanei, come gli errori di rete. • Errori irreversibili: possono indicare un problema con la configurazione dell'archivio delle chiavi personalizzate o con i componenti esterni. • N/D: la richiesta è andata a buon fine; nessun errore

Dimensione	Descrizione
Exception Name	Valori: • Nome dell'eccezione • Nessuno: la richiesta è andata a buon fine; nessun errore

XksExternalKeyManagerStates

Conteggio del numero di istanze del gestore delle chiavi esterne in ciascuno dei seguenti stati di integrità: `Active`, `Degraded` e `Unavailable`. Le informazioni per questo parametro provengono dal proxy associato a ogni archivio delle chiavi esterne. Questo parametro si applica solo agli archivi delle chiave esterne.

Di seguito sono riportati gli stati di integrità delle istanze del gestore delle chiavi esterne associate a un archivio delle chiavi esterne. Ogni proxy dell'archivio delle chiavi esterne potrebbe utilizzare indicatori diversi per misurare gli stati di integrità del gestore delle chiavi esterne. Per ulteriori informazioni, consulta la documentazione del proxy dell'archivio delle chiavi esterne.

- `Active`: il gestore delle chiavi esterne è integro.
- `Degraded`: il gestore delle chiavi esterne non è integro, ma può comunque servire il traffico
- `Unavailable`: il gestore delle chiavi esterne non è in grado di servire il traffico.

Utilizza questa metrica per creare un CloudWatch allarme che ti avvisi in caso di istanze di key manager esterne danneggiate e non disponibili. Per determinare lo stato di ogni istanza, consulta i log del proxy dell'archivio delle chiavi esterne.

Nome del gruppo di dimensioni: XKS External Key Manager Metrics (Parametri del gestore chiavi esterne di XKS)

Dimensione	Descrizione
CustomKey StoreId	Valore per ogni archivio delle chiavi esterne.

Dimensione	Descrizione
XksExternalKeyManagerState	Valore per ogni stato di integrità.

XksProxyLatency

Il numero di millisecondi necessari a un proxy dell'archivio delle chiavi esterne per rispondere a una richiesta AWS KMS. Se la richiesta è scaduta, il valore registrato è il limite di timeout di 250 millisecondi. Questo parametro si applica solo agli archivi delle chiave esterne.

Utilizza questo parametro per valutare le prestazioni del proxy dell'archivio delle chiavi esterne e del gestore delle chiavi esterne. Ad esempio, se il proxy è spesso prossimo al timeout per le operazioni di crittografia e decrittografia, rivolgiti all'amministratore del proxy.

Le risposte lente potrebbero anche indicare che il gestore delle chiavi esterne non è in grado di gestire il traffico delle richieste corrente. AWS KMS consiglia la gestione di 1.800 richieste di operazioni di crittografia al secondo per il gestore delle chiavi esterne. Se il gestore delle chiavi esterne non è in grado di gestire 1.800 richieste al secondo, prendi in considerazione la possibilità di richiedere una riduzione della quota di richieste per le chiavi KMS in un archivio delle chiavi personalizzate. Le richieste relative alle operazioni di crittografia che utilizzano le chiavi KMS nell'archivio delle chiavi esterne anticiperanno rapidamente l'errore (fail fast) con un'eccezione di limitazione (della larghezza di banda della rete), anziché essere elaborate e successivamente rifiutate dal proxy o dal gestore delle chiavi esterne.

Nome del gruppo di dimensioni: XKS Proxy Latency Metrics (Parametri di latenza del proxy XKS)

Dimensione	Descrizione
CustomKeyStoreId	Valore per ogni archivio delle chiavi esterne.
KmsOperation	Valore per ogni operazione API AWS KMS che ha generato una richiesta al proxy XKS.
XksOperation	Valore per ogni operazione API proxy dell'archivio delle chiavi esterne.

Dimensione	Descrizione
KeySpec	Valore per ogni tipo di chiave KMS. L'unica specifica della chiave supportata per le chiavi KMS in un archivio delle chiavi esterne è SYMMETRIC_DEFAULT.

Visualizzazione dei parametri AWS KMS

Puoi visualizzare le AWS KMS metriche utilizzando l' CloudWatch API AWS Management Console e Amazon.

Per visualizzare le metriche utilizzando la console CloudWatch

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Se necessario, modifica la regione. Nella barra di navigazione seleziona la regione in cui si trovano le risorse AWS.
3. Nel pannello di navigazione, seleziona Metrics (Parametri), All metrics (Tutti i parametri).
4. Nella scheda Browse (Sfoglia), cerca `KMS`, quindi scegli KMS.
5. Scegli il nome del gruppo di dimensioni del parametro da visualizzare.

   Ad esempio, per il parametro `SecondsUntilKeyMaterialExpiration`, scegli Per-Key Metrics (Parametri per chiave).
6. Per un grafico del valore del parametro, scegli il nome del parametro, quindi scegli `Add to graph`. Per convertire il grafico lineare in un valore, scegli Line (Linea), quindi scegli Number (Numero).

Per visualizzare i parametri utilizzando l'API Amazon CloudWatch

Per visualizzare le AWS KMS metriche utilizzando l' CloudWatch API, invia una ListMetricsrichiesta con `Namespace` set to. `AWS/KMS` L'esempio seguente mostra come eseguire questa operazione con l'AWS Command Line Interface (AWS CLI).

```
$  aws cloudwatch list-metrics --namespace AWS/KMS

{
    "Metrics": [
        {
            "Namespace": "AWS/KMS",
```

```
            "MetricName": "SecondsUntilKeyMaterialExpiration",
            "Dimensions": [
                {
                    "Name": "KeyId",
                    "Value": "1234abcd-12ab-34cd-56ef-1234567890ab"
                }
            ]
        },
        {
            "Namespace": "AWS/KMS",
            "MetricName": "ExtenalKeyStoreThrottle",
            "Dimensions": [
                {
                    "Name": "CustomKeyStoreId",
                    "Value": "cks-1234567890abcdef0"
                },
                {
                    "Name": "KmsOperation",
                    "Value": "Encrypt"
                },
                {
                    "Name": "KeySpec",
                    "Value": "SYMMETRIC_DEFAULT"
                }
            ]
        },
        {
            "Namespace": "AWS/KMS",
            "MetricName": "XksProxyCertificateDaysToExpire",
            "Dimensions": [
                {
                    "Name": "CustomKeyStoreId",
                    "Value": "cks-1234567890abcdef0"
                },
                {
                    "Name": "CertificateName",
                    "Value": "myproxy.xks.example.com"
                }
            ]
        },
        {
            "Namespace": "AWS/KMS",
            "MetricName": "XksProxyCredentialAge",
            "Dimensions": [
```

```
                {
                    "Name": "CustomKeyStoreId",
                    "Value": "cks-1234567890abcdef0"
                }
            ]
        },
        {
            "Namespace": "AWS/KMS",
            "MetricName": "XksProxyErrors",
            "Dimensions": [
                {
                    "Name": "CustomKeyStoreId",
                    "Value": "cks-1234567890abcdef0"
                },
                {
                    "Name": "KmsOperation",
                    "Value": "Decrypt"
                },
                {
                    "Name": "XksOperation",
                    "Value": "Decrypt"
                },
                {
                     "Name": "KeySpec",
                     "Value": "SYMMETRIC_DEFAULT"
                },
                {
                    "Name": "ErrorType",
                    "Value": "Retryable errors"
                },
                {
                     "Name": "ExceptionName",
                     "Value": "KMSInvalidStateException"
                }
            ]
        },
        {
            "Namespace": "AWS/KMS",
            "MetricName": "XksProxyHsmStates",
            "Dimensions": [
                {
                    "Name": "CustomKeyStoreId",
                    "Value": "cks-1234567890abcdef0"
                },
```

```
                {
                    "Name": "XksProxyHsmState",
                    "Value": "Active"
                }
            ]
        },
        {
            "Namespace": "AWS/KMS",
            "MetricName": "XksProxyLatency",
            "Dimensions": [
                {
                    "Name": "CustomKeyStoreId",
                    "Value": "cks-1234567890abcdef0"
                },
                {
                    "Name": "KmsOperation",
                    "Value": "Decrypt"
                },
                {
                    "Name": "XksOperation",
                    "Value": "Decrypt"
                },
                {
                     "Name": "KeySpec",
                     "Value": "SYMMETRIC_DEFAULT"
                }
            ]
        }
    ]
}
```

Creazione di CloudWatch allarmi per monitorare le chiavi KMS

Puoi creare un CloudWatch allarme Amazon in base a una AWS KMS metrica. L'allarme invia un messaggio e-mail quando il valore di un parametro supera una soglia specificata nella configurazione dell'allarme. L'allarme può inviare un messaggio e-mail a un argomento Servizio di notifica semplice Amazon (Amazon Simple Notification Service (Amazon SNS)) o alla policy di Dimensionamento automatico Amazon EC2. Per informazioni dettagliate sugli CloudWatch allarmi, consulta Using Amazon CloudWatch alarms nella Amazon CloudWatch User Guide

Crea un avviso per la scadenza del materiale della chiave importato

Puoi utilizzare la `SecondsUntilKeyMaterialExpiration`metrica per creare un CloudWatch allarme che ti avvisi quando il materiale chiave importato in una chiave KMS sta per scadere.

Quando importi il materiale della chiave in una chiave KMS, puoi specificare una data e un'ora in cui tale materiale scade. Quando il materiale della chiave scade, AWS KMS elimina tale materiale e la chiave KMS diventa inutilizzabile. Per utilizzare di nuovo la chiave KMS, devi importare nuovamente lo stesso materiale della chiave.

Per istruzioni, consulta Creazione di un CloudWatch avviso di scadenza del materiale chiave importato.

Creazione di un allarme per l'utilizzo di chiavi KMS che hanno l'eliminazione in sospeso

Quando programmi l'eliminazione di una chiave KMS, AWS KMS applica un periodo di attesa prima di procedere all'eliminazione. È possibile usare il periodo di attesa per assicurarsi che la chiave KMS non sia necessaria ora o in futuro. Puoi anche configurare un CloudWatch allarme per avvisarti se una persona o un'applicazione tenta di utilizzare la chiave KMS in un'operazione crittografica durante il periodo di attesa. Se si riceve una notifica da parte di un allarme, è possibile annullare l'eliminazione della chiave KMS.

Per istruzioni, consulta Creazione di un allarme che rileva l'uso di una chiave KMS in attesa di eliminazione.

Creazione di un allarme per monitorare un archivio delle chiavi esterne

È possibile creare CloudWatch allarmi in base alle metriche degli archivi di chiavi esterni e alle chiavi KMS degli archivi di chiavi esterni.

Ad esempio, ti consigliamo di impostare un CloudWatch allarme per avvisarti quando il certificato TLS per il tuo archivio di chiavi esterno sta per scadere (XksProxyCertificateDaysToExpire), quando il tuo proxy dell'archivio chiavi esterno segnala che le istanze del gestore di chiavi esterno sono in uno stato degradato o non disponibile (). XksProxyHsmStates

Per istruzioni, consultare Monitoraggio di un archivio delle chiavi esterne.

Monitoraggio con Amazon EventBridge

Puoi utilizzare Amazon EventBridge (precedentemente Amazon CloudWatch Events) per avvisarti dei seguenti eventi importanti nel ciclo di vita delle tue chiavi KMS.

- Il materiale chiave di una chiave KMS è stato ruotato automaticamente.
- Il materiale chiave importante in una chiave KMS scaduta.
- Una chiave KMS che era stata pianificata per l'eliminazione è stata eliminata.

AWS KMSsi integra con Amazon EventBridge per avvisarti di eventi importanti che influiscono sulle tue chiavi KMS. Ogni evento è rappresentato in JSON (JavaScriptObject Notation) e include il nome dell'evento, la data e l'ora in cui si è verificato l'evento e l'evento interessato. Puoi raccogliere questi eventi e configurare regole che li instradino verso uno o più destinazioni, come funzioni AWS Lambda, argomenti Amazon SNS, code Amazon SQS, flussi di dati Amazon Kinesis o destinazioni integrate.

Per ulteriori informazioni sull'utilizzo EventBridge con altri tipi di eventi, inclusi quelli emessi AWS CloudTrail quando registra una richiesta API di lettura/scrittura, consulta la Amazon EventBridge User Guide.

I seguenti argomenti descrivono gli EventBridge eventi che genera. AWS KMS

Rotazione KMS CMK

AWS KMS supporta la rotazione automatica del materiale della chiave nelle chiavi KMS di crittografia simmetrica. La rotazione annuale del materiale della chiave è facoltativa per le chiavi gestite dal cliente. Il materiale della chiave per le Chiavi gestite da AWS viene ruotato automaticamente ogni anno.

Ogni volta che AWS KMS ruota il materiale chiave, invia un `KMS CMK Rotation` evento a EventBridge. AWS KMSgenera questo evento con il massimo impegno.

Di seguito è illustrato un esempio di questo evento.

```
{
  "version": "0",
  "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
  "detail-type": "KMS CMK Rotation",
  "source": "aws.kms",
  "account": "111122223333",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  ],
```

```
  "detail": {
    "key-id": "1234abcd-12ab-34cd-56ef-1234567890ab"
  }
}
```

Scadenza del materiale chiave importato di KMS

Quando importi il materiale chiave in una chiave KMS, è possibile specificare un'ora in cui tale materiale scade. Quando il materiale chiave scade, AWS KMS elimina il materiale chiave e invia un evento corrispondente `KMS Imported Key Material Expiration` a. EventBridge AWS KMSgenera questo evento con la massima diligenza possibile.

Di seguito è illustrato un esempio di questo evento.

```
{
  "version": "0",
  "id": "9da9af57-9253-4406-87cb-7cc400e43465",
  "detail-type": "KMS Imported Key Material Expiration",
  "source": "aws.kms",
  "account": "111122223333",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  ],
  "detail": {
    "key-id": "1234abcd-12ab-34cd-56ef-1234567890ab"
  }
}
```

Eliminazione di KMS CMK

Quando programmi l'eliminazione di una chiave KMS, AWS KMS applica un periodo di attesa prima di procedere all'eliminazione. Al termine del periodo di attesa, AWS KMS elimina la chiave KMS e invia un `KMS CMK Deletion` evento a. EventBridge AWS KMSgarantisce questo EventBridge evento. A seguito dei tentativi, potrebbero generarsi più eventi in pochi secondi che eliminano la stessa chiave KMS.

Di seguito è illustrato un esempio di questo evento.

```
{
```

```
  "version": "0",
  "id": "e9ce3425-7d22-412a-a699-e7a5fc3fbc9a",
  "detail-type": "KMS CMK Deletion",
  "source": "aws.kms",
  "account": "111122223333",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  ],
  "detail": {
    "key-id": "1234abcd-12ab-34cd-56ef-1234567890ab"
  }
}
```

Creazione di risorse AWS KMScon AWS CloudFormation

AWS Key Management Service è integrato con AWS CloudFormation, un servizio che ti consente di modellare e configurare le tue risorse AWS in modo da dedicare meno tempo alla creazione e alla gestione delle risorse e dell'infrastruttura. È possibile creare un modello che descriva le chiavi KMS e gli alias e AWS CloudFormation si occuperà del provisioning e della configurazione di queste risorse per conto dell'utente. Per informazioni sul AWS KMS supporto per CloudFormation, consulta il riferimento al tipo di risorsa KMS nella Guida per l'AWS CloudFormationutente.

Quando usi AWS CloudFormation, puoi riutilizzare il modello per configurare le risorse AWS KMS in modo coerente e continuo. Basta descrivere le risorse una volta sola, dopodiché si può effettuare il provisioning di tali risorse quante volte si vuole in più Account AWS e regioni.

Per eseguire l'assegnazione e la configurazione delle risorse per AWS KMS e altri servizi AWS, devi conoscere i modelli AWS CloudFormation. I modelli sono file di testo formattati in JSON o YAML. Questi modelli descrivono le risorse di cui intendi effettuare il provisioning negli stack AWS CloudFormation. Se non hai familiarità con JSON o YAML, puoi usare AWS CloudFormationDesigner per iniziare a utilizzare i modelli AWS CloudFormation. Per ulteriori informazioni, consulta Che cos'è AWS CloudFormationDesigner? nella Guida per l'utente di AWS CloudFormation.

Regioni

AWS KMS CloudFormation le risorse sono supportate in tutte le regioni in cui AWS CloudFormation è supportata.

Risorse AWS KMS in modelli AWS CloudFormation

AWS KMS supporta le seguenti risorse AWS CloudFormation.

- `AWS::KMS::Key` crea una chiave KMS simmetrica o asimmetrica. È possibile utilizzare questa risorsa per creare una chiave KMS primaria simmetrica o asimmetrica multi-regione. Per creare una chiave di replica multi-regione, utilizzare la risorsa `AWS::KMS::ReplicaKey`. Non puoi utilizzare questa risorsa per creare chiavi KMS con materiale chiave importato o chiavi KMS in un archivio delle chiavi personalizzate.
- `AWS::KMS::Alias` crea un alias e lo associa a una chiave KMS. La chiave KMS può essere definita nel modello o creata da un altro meccanismo.
- `AWS::KMS::ReplicaKey` crea una chiave di replica in più Regioni. Per creare una chiave primaria in più Regioni, utilizzare la risorsa `AWS::KMS::Key`. Non è possibile utilizzare questa risorsa per replicare le chiavi multi-regione con materiale chiave importato. Per informazioni dettagliate sulle chiavi in più Regioni, consulta Chiavi multi-regione in AWS KMS.

> **Important**
>
> Se si modifica il valore di una proprietà `KeyUsage`, `KeySpec` o `MultiRegion`, su una chiave KMS esistente, quest'ultima viene pianificata per l'eliminazione e viene creata una nuova chiave KMS con il valore specificato.
> Durante la pianificazione per l'eliminazione, la chiave KMS esistente diventa inutilizzabile. Se non annulli l'eliminazione pianificata della chiave KMS esistente al di fuori di AWS CloudFormation, tutti i dati crittografati sotto la chiave KMS esistente diventano irrecuperabili quando la chiave KMS viene eliminata.

Le chiavi KMS create dal modello sono risorse effettive nel tuo Account AWS. Le entità principali autorizzate possono utilizzare e gestire le chiavi KMS create dal modello, utilizzando il modello, la console AWS KMS o le API AWS KMS. Quando si elimina una chiave KMS dal modello, la chiave KMS viene pianificata per l'eliminazione utilizzando un periodo di attesa specificato in anticipo.

Puoi ad esempio usare un modello AWS CloudFormation per creare una chiave KMS di prova con policy chiave, specifiche chiave, utilizzo della chiave, alias e i tag che preferisci. È possibile eseguirlo nella suite di test, esaminare i risultati e quindi utilizzare il modello per pianificare la chiave di prova per l'eliminazione. Successivamente, è possibile eseguire nuovamente il modello per creare una chiave di prova con le stesse proprietà.

Oppure è possibile utilizzare un modello AWS CloudFormation per definire una particolare configurazione della chiave KMS che soddisfi le regole aziendali e gli standard di sicurezza. È quindi possibile utilizzare tale modello ogni volta che è necessario creare una chiave KMS. Non devi preoccuparti delle chiavi configurate in modo errato. Se la configurazione preferita viene modificata, è possibile utilizzare il modello per aggiornare le chiavi KMS. Ad esempio, il modello consente di abilitare in modo semplice la rotazione automatica dei tasti su tutte le chiavi KMS definite dal modello.

Per ulteriori informazioni sulle risorse AWS KMS, inclusi esempi, consulta la documentazione di riferimento sui tipi di risorse KMS nella Guida per l'utente di AWS CloudFormation.

Ulteriori informazioni su AWS CloudFormation

Per ulteriori informazioni su AWS CloudFormation, consulta le seguenti risorse:

- AWS CloudFormation
- Guida per l'utente di AWS CloudFormation
- Documentazione di riferimento dell'API AWS CloudFormation
- Guida per l'utente dell'interfaccia a riga di comando di AWS CloudFormation

Eliminazione di AWS KMS keys

L'eliminazione di una AWS KMS key è un'operazione distruttiva e potenzialmente pericolosa. Infatti, elimina il materiale della chiave e tutti i metadati associati alla chiave KMS ed è irreversibile. Dopo l'eliminazione di una chiave KMS, non è più possibile decrittare i dati crittografati usando tale chiave KMS, che quindi non possono più essere recuperati. (Le uniche eccezioni sono rappresentate da chiavi di replica multi-regione e chiavi KMS asimmetriche e HMAC con materiale della chiave importato.) Questo rischio è significativo per le chiavi KMS asimmetriche utilizzate per la crittografia in cui, senza avvertenze o errori, gli utenti possono continuare a generare con la chiave pubblica testi criptati che non possono essere decrittografati dopo l'eliminazione della chiave privata da AWS KMS.

Dovresti eliminare una chiave KMS solo quando hai la certezza di non doverla più utilizzare. In caso di dubbio, valuta la possibilità di disabilitare la chiave KMS invece di eliminarla. Puoi riabilitare una chiave KMS disabilitata e annullare l'eliminazione pianificata di una chiave KMS, ma non puoi recuperare una chiave KMS eliminata.

È possibile solamente pianificare l'eliminazione di una chiave gestita dal cliente. Non è possibile eliminare Chiavi di proprietà di AWS o Chiavi gestite da AWS.

Prima di eliminare una chiave KMS, potresti voler sapere in che modo numerosi testi cifrati sono stati crittografati per quella chiave KMS. AWS KMS non archivia queste informazioni né i testi cifrati. Per ottenere queste informazioni, devi determinare l'utilizzo passato di una chiave KMS. Per assistenza, vai a Stabilire l'utilizzo passato di una chiave KMS.

AWS KMS non elimina mai le chiavi KMS a meno che non le pianifichi esplicitamente per l'eliminazione e il periodo di attesa obbligatorio scada.

Potresti scegliere di eliminare una chiave KMS per uno o più dei seguenti motivi:

- Per completare il ciclo di vita delle chiavi per le chiavi KMS che non sono più necessarie
- Per evitare i costi di gestione delle chiavi KMS inutilizzate
- Per ridurre il numero di chiavi KMS conteggiate nella quota di risorse delle chiavi KMS

> **Note**
>
> Se chiudi il tuo Account AWS, le tue chiavi KMS diventano inaccessibili e non ti vengono più fatturate.

AWS KMS registra una voce nel log AWS CloudTrail quando pianifichi l'eliminazione della chiave KMS e quando la chiave KMS viene effettivamente eliminata.

Per informazioni sull'eliminazione di chiavi primarie e di replica multi-regione, consulta Eliminazione di chiavi multiregione.

Argomenti

- Informazioni sul periodo di attesa
- Eliminazione delle chiavi KMS asimmetriche
- Eliminazione di chiavi multi-regione
- Eliminazione di chiavi KMS con materiale della chiave importato
- Controllo dell'accesso per l'eliminazione delle chiavi
- Pianificazione e annullamento dell'eliminazione di chiavi
- Creazione di un allarme che rileva l'uso di una chiave KMS in attesa di eliminazione
- Stabilire l'utilizzo passato di una chiave KMS

Informazioni sul periodo di attesa

Poiché eliminare una chiave KMS è un'operazione distruttiva e potenzialmente pericolosa, AWS KMS richiede di impostare un periodo di attesa di 7-30 giorni. Il periodo di attesa predefinito è di 30 giorni.

Tuttavia, il periodo di attesa effettivo potrebbe essere fino a 24 ore più lungo di quello pianificato. Per ottenere la data e l'ora effettive in cui la chiave KMS verrà eliminata, utilizzare l'DescribeKeyoperazione. O nella console AWS KMS, nella pagina dei dettagli per la chiave KMS, nella sezione Configurazione generale, consulta Data di eliminazione pianificata. Assicurati di segnare il fuso orario.

Durante il periodo di attesa, lo stato della chiave KMS e quello della chiave è In attesa di eliminazione.

- Una chiave KMS che è in attesa di eliminazione non può essere utilizzata in nessuna operazione di crittografia.
- AWS KMS non ruota il materiale chiavi delle chiavi KMS in attesa di eliminazione.

Al termine del periodo di attesa, AWS KMS elimina la chiave KMS, i relativi alias e tutti i relativi metadati AWS KMS.

La pianificazione dell'eliminazione di una chiave KMS potrebbe non influire immediatamente sulle chiavi di dati crittografate dalla chiave KMS. Per informazioni dettagliate, vedi In che modo le chiavi KMS inutilizzabili influiscono sulle chiavi dati.

Utilizza il periodo di attesa per assicurarti che la chiave KMS non sia necessaria ora o in futuro. Puoi configurare un CloudWatch allarme Amazon per avvisarti se una persona o un'applicazione tenta di utilizzare la chiave KMS durante il periodo di attesa. Per ripristinare la chiave KMS, puoi annullare l'eliminazione della chiave prima del termine del periodo di attesa. Dopo il termine del periodo di attesa, non puoi annullare l'eliminazione della chiave e AWS KMS elimina la chiave KMS.

Eliminazione delle chiavi KMS asimmetriche

Gli utenti autorizzati possono eliminare chiavi KMS simmetriche o asimmetriche. La procedura per pianificare l'eliminazione di queste chiavi KMS è la stessa per entrambi i tipi di chiave. Tuttavia, poiché la chiave pubblica di una chiave KMS asimmetrica può essere scaricata e utilizzata al di fuori di AWS KMS, l'operazione comporta notevoli rischi aggiuntivi, soprattutto per le chiavi KMS asimmetriche utilizzate per la crittografia (l'utilizzo della chiave è `ENCRYPT_DECRYPT`).

- Quando pianifichi l'eliminazione di una chiave KMS, lo stato della chiave KMS cambia in In attesa di eliminazione e la chiave KMS non può essere utilizzata nelle operazioni di crittografia. Tuttavia, la pianificazione dell'eliminazione non ha alcun effetto sulle chiavi pubbliche al di fuori di AWS KMS. Gli utenti che dispongono della chiave pubblica possono continuare a utilizzarle per crittografare i messaggi. Non ricevono alcuna notifica del cambiamento dello stato della chiave. A meno che l'eliminazione non venga annullata, il testo cifrato creato con la chiave pubblica non può essere decrittato.
- Allarmi, log e altre strategie che rilevano il tentativo di utilizzo di chiavi KMS in attesa di eliminazione non possono rilevare l'utilizzo della chiave pubblica al di fuori di AWS KMS.
- Quando la chiave KMS viene eliminata, tutte le azioni AWS KMS che riguardano la chiave KMS hanno esito negativo. Tuttavia, gli utenti che dispongono della chiave pubblica possono continuare a utilizzarla per crittografare i messaggi. Questi testi cifrati non possono essere decrittati.

Se devi eliminare una chiave KMS asimmetrica con un utilizzo di chiave`ENCRYPT_DECRYPT`, utilizza le voci di CloudTrail registro per determinare se la chiave pubblica è stata scaricata e condivisa. In caso affermativo, verifica che la chiave pubblica non venga utilizzata al di fuori di AWS KMS. Valuta l'opportunità di disattivare la chiave KMS anziché di eliminarla.

Il rischio rappresentato dall'eliminazione di una chiave asimmetrica è ridotto per le chiavi KMS asimmetriche con materiale della chiave importato. Per informazioni dettagliate, vedi Eliminazione di una chiave KMS con il materiale della chiave importato.

Eliminazione di chiavi multi-regione

Gli utenti autorizzati possono pianificare l'eliminazione delle chiavi primarie e di replica multi-regione. Tuttavia, AWS KMS non eliminerà una chiave primaria multi-regione che ha una chiave di replica. Inoltre, finché esiste la chiave primaria, è possibile ricreare una chiave di replica multi-regione eliminata. Per informazioni dettagliate, vedi Eliminazione di chiavi multiregione.

Eliminazione di chiavi KMS con materiale della chiave importato

Gli utenti autorizzati possono pianificare l'eliminazione delle chiavi KMS con materiale della chiave importato. Questa azione elimina definitivamente la chiave KMS, il relativo materiale e tutti i metadati associati alla chiave KMS.

Non puoi creare una nuova chiave KMS di crittografia simmetrica in grado di decrittografare i testi criptati di una chiave di crittografia simmetrica eliminata con materiale della chiave importato, neppure se disponi di una copia del relativo materiale della chiave. Tuttavia, se disponi del materiale della

chiave, puoi ricreare efficacemente una chiave KMS asimmetrica o una chiave KMS HMAC con il materiale della chiave importato. Per informazioni dettagliate, vedi Eliminazione di una chiave KMS con il materiale della chiave importato.

Controllo dell'accesso per l'eliminazione delle chiavi

Se utilizzi le policy IAM per concedere le autorizzazioni AWS KMS, tutte le identità IAM che dispongono dell'accesso di amministratore AWS (`"Action": "*"`) o dell'accesso completo a AWS KMS (`"Action": "kms:*"`) sono già autorizzate a pianificare e annullare l'eliminazione di chiavi KMS. Per consentire agli amministratori delle chiavi di pianificare e annullare l'eliminazione delle chiavi nella relativa policy, utilizza la console AWS KMS o l'API AWS KMS.

In genere, solo gli amministratori delle chiavi sono in grado di pianificare o annullare l'eliminazione delle chiavi. Tuttavia, puoi concedere queste autorizzazioni ad altre identità IAM aggiungendo `kms:ScheduleKeyDeletion` e `kms:CancelKeyDeletion` alla policy della chiave o a una policy IAM. Puoi anche utilizzare la chiave `kms:ScheduleKeyDeletionPendingWindowInDays`condition per limitare ulteriormente i valori che i principali possono specificare nel parametro di una richiesta. `PendingWindowInDays` ScheduleKeyDeletion

Consentire agli amministratori delle chiavi di pianificare e annullare l'eliminazione delle chiavi (console)

Per concedere agli amministratori delle chiavi l'autorizzazione per pianificare e annullare l'eliminazione delle chiavi.

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.
4. Scegli l'alias o l'ID chiave della chiave KMS di cui intendi modificare le autorizzazioni.
5. Scegli la scheda Key policy (Policy delle chiavi).
6. Il passaggio successivo è diverso per la visualizzazione predefinita e la visualizzazione della policy della policy delle chiavi. La visualizzazione predefinita è disponibile solo se utilizzi la policy delle chiavi di console predefinita. In caso contrario, è disponibile solo la visualizzazione della policy.

Quando è disponibile la visualizzazione predefinita, nella scheda Key policy (Policy delle chiavi) viene visualizzato il pulsante Switch to policy view (Passa alla visualizzazione della policy) o Switch to default view (Passa alla visualizzazione predefinita).

- Nella visualizzazione predefinita:
  - In Key deletion (Eliminazione chiave), seleziona Allow key administrators to delete this key (Consenti agli amministratori delle chiavi di eliminare questa chiave).
- Nella visualizzazione della policy:
  a. Scegli Modifica.
  b. Nell'istruzione della policy per gli amministratori delle chiavi, aggiungi le autorizzazioni `kms:ScheduleKeyDeletion` e `kms:CancelKeyDeletion` all'elemento `Action`.

```
{
  "Sid": "Allow access for Key Administrators",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:user/KMSKeyAdmin"},
  "Action": [
    "kms:Create*",
    "kms:Describe*",
    "kms:Enable*",
    "kms:List*",
    "kms:Put*",
    "kms:Update*",
    "kms:Revoke*",
    "kms:Disable*",
    "kms:Get*",
    "kms:Delete*",
    "kms:ScheduleKeyDeletion",
    "kms:CancelKeyDeletion"
  ],
  "Resource": "*"
}
```

  c. Seleziona Salvataggio delle modifiche.

Consentire agli amministratori delle chiavi l'autorizzazione per pianificare e annullare l'eliminazione delle chiavi (AWS CLI)

Puoi utilizzare la AWS Command Line Interface per aggiungere le autorizzazioni per la pianificazione e l'annullamento dell'eliminazione di chiavi.

Per aggiungere l'autorizzazione per pianificare e annullare l'eliminazione di chiavi

1. Utilizzare il comando `aws kms get-key-policy` per recuperare la policy delle chiavi esistente, quindi salvare il documento di policy in un file.
2. Apri il documento della policy nell'editor di testo preferito. Nell'istruzione della policy per gli amministratori delle chiavi, aggiungi le autorizzazioni `kms:ScheduleKeyDeletion` e `kms:CancelKeyDeletion`. L'esempio seguente mostra un'istruzione di policy con queste due autorizzazioni:

```
{
  "Sid": "Allow access for Key Administrators",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:user/KMSKeyAdmin"},
  "Action": [
    "kms:Create*",
    "kms:Describe*",
    "kms:Enable*",
    "kms:List*",
    "kms:Put*",
    "kms:Update*",
    "kms:Revoke*",
    "kms:Disable*",
    "kms:Get*",
    "kms:Delete*",
    "kms:ScheduleKeyDeletion",
    "kms:CancelKeyDeletion"
  ],
  "Resource": "*"
}
```

3. Utilizza il comando `aws kms put-key-policy` per applicare la policy chiave alla chiave KMS.

Pianificazione e annullamento dell'eliminazione di chiavi

Le procedure seguenti descrivono come pianificare e annullare l'eliminazione di una chiave in una AWS KMS keys per Regione singola (chiave KMS) in AWS KMS utilizzando la AWS Management Console, AWS CLI e AWS SDK for Java.

Per informazioni sulla pianificazione dell'eliminazione delle chiavi multi-regioni, consulta Eliminazione di chiavi multiregione.

> **Warning**
>
> L'eliminazione di una chiave KMS è un'operazione distruttiva e potenzialmente pericolosa. Dovresti procedere solo quando hai la certezza di non dover più utilizzare la chiave KMS e che non ne avrai bisogno in futuro. In caso di dubbio, dovresti disabilitare la chiave KMS invece di eliminarla.

Prima di eliminare una chiave KMS, devi disporre delle autorizzazioni necessarie. Per informazioni su come concedere queste autorizzazioni agli amministratori delle chiavi, consulta Controllo dell'accesso per l'eliminazione delle chiavi. Puoi anche utilizzare la chiave di condizione `kms:ScheduleKeyDeletionPendingWindowInDays` per limitare ulteriormente il periodo di attesa, applicando, ad esempio, un periodo di attesa minimo.

AWS KMS registra una voce nel log AWS CloudTrail quando pianifichi l'eliminazione della chiave KMS e quando la chiave KMS viene effettivamente eliminata.

Pianificazione e annullamento dell'eliminazione di chiavi (console)

Nella AWS Management Console, è possibile pianificare e annullare l'eliminazione di più chiavi KMS contemporaneamente.

Per pianificare l'eliminazione di chiavi

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.

Non è possibile pianificare l'eliminazione di Chiavi gestite da AWS o Chiavi di proprietà di AWS.

4. Scegli la casella di controllo accanto alla chiave KMS da eliminare.
5. Scegliere Key actions (Operazioni sulle chiavi), Schedule key deletion (Pianifica eliminazione chiave).
6. Leggere l'avviso e le informazioni sull'annullamento dell'eliminazione durante il periodo di attesa. Se decidi di annullare l'eliminazione, nella parte inferiore della pagina scegli Annulla.
7. Per Waiting period (in days) (Periodo di attesa (in giorni)), immettere un numero di giorni compreso tra 7 e 30.
8. Controlla le chiavi KMS che stai eliminando.
9. Scegli la casella di controllo accanto a Confirm you want to schedule this key for deletion in ***<number of days>*** days (Conferma di voler pianificare l'eliminazione della chiave tra <number of days> giorni).
10. Scegliere Schedule deletion (Pianifica eliminazione).

Lo stato della chiave KMS diventa In attesa di eliminazione.

Per annullare l'eliminazione di chiavi

1. Aprire la console AWS KMS all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.
4. Scegli la casella di controllo accanto alla chiave KMS da ripristinare.
5. Scegliere Key actions (Operazioni sulle chiavi), Cancel key deletion (Annulla eliminazione chiave).

Lo stato della chiave KMS cambia da In attesa di eliminazione a Disabilitata. Per utilizzare la chiave KMS è necessario abilitarla.

Pianificazione e annullamento dell'eliminazione di chiavi (AWS CLI)

Utilizza il comando `aws kms schedule-key-deletion` per pianificare l'eliminazione di una chiave gestita dal cliente, come mostrato nel seguente esempio.

Non è possibile pianificare l'eliminazione di Chiave gestita da AWS o Chiave di proprietà di AWS.

```
$ aws kms schedule-key-deletion --key-id 1234abcd-12ab-34cd-56ef-1234567890ab --
pending-window-in-days 10
```

Quando utilizzata correttamente, la AWS CLI restituisce un output come quello mostrato nell'esempio seguente:

```
{
    "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "DeletionDate": 1598304792.0,
    "KeyState": "PendingDeletion",
    "PendingWindowInDays": 10
}
```

Utilizzare il comando `aws kms cancel-key-deletion` per annullare l'eliminazione di chiavi dalla AWS CLI, come mostrato nel seguente esempio.

```
$ aws kms cancel-key-deletion --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

Quando utilizzata correttamente, la AWS CLI restituisce un output come quello mostrato nell'esempio seguente:

```
{
    "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
}
```

Lo stato della chiave KMS cambia da In attesa di eliminazione a Disabilitata. Per utilizzare la chiave KMS è necessario abilitarla.

Pianificazione e annullamento dell'eliminazione di chiavi (AWS SDK for Java)

L'esempio seguente mostra come pianificare l'eliminazione di una chiave gestita dal cliente con AWS SDK for Java. Questo esempio richiede di aver precedentemente creato un'istanza `AWSKMSClient` come `kms`.

```
String KeyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

int PendingWindowInDays = 10;
```

```
ScheduleKeyDeletionRequest scheduleKeyDeletionRequest =
new
 ScheduleKeyDeletionRequest().withKeyId(KeyId).withPendingWindowInDays(PendingWindowInDays);
kms.scheduleKeyDeletion(scheduleKeyDeletionRequest);
```

L'esempio seguente mostra come annullare l'eliminazione di una chiave con AWS SDK for Java. Questo esempio richiede di aver precedentemente creato un'istanza `AWSKMSClient` come `kms`.

```
String KeyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

CancelKeyDeletionRequest cancelKeyDeletionRequest =
new CancelKeyDeletionRequest().withKeyId(KeyId);
kms.cancelKeyDeletion(cancelKeyDeletionRequest);
```

Lo stato della chiave KMS cambia da In attesa di eliminazione a Disabilitata. Per utilizzare la chiave KMS è necessario abilitarla.

Creazione di un allarme che rileva l'uso di una chiave KMS in attesa di eliminazione

Puoi combinare le funzionalità di AWS CloudTrail Amazon CloudWatch Logs e Amazon Simple Notification Service (Amazon SNS) per creare un CloudWatch allarme Amazon che ti avvisa quando qualcuno nel tuo account tenta di utilizzare una chiave KMS in attesa di eliminazione. Se ricevi questa notifica, potresti voler annullare l'eliminazione della chiave KMS e riconsiderare la decisione di eliminarla.

Le seguenti procedure creano un allarme che ti avvisa ogni volta che il messaggio di errore "*Key ARN* `is pending deletion`" viene scritto nei tuoi file di registro. CloudTrail Questo messaggio di errore indica che una persona o un'applicazione ha cercato di utilizzare la chiave KMS in una operazione di crittografia. Poiché la notifica è collegata al messaggio di errore, non viene attivata quando utilizzi operazioni API consentite sulle chiavi KMS in attesa di eliminazione, ad esempio `ListKeys`, `CancelKeyDeletion` e `PutKeyPolicy`. Per visualizzare un elenco delle operazioni API AWS KMS che restituiscono questo messaggio di errore, consulta Stati chiave delle chiavi AWS KMS.

L'e-mail di notifica che ricevi non include la chiave KMS o l'operazione di crittografia. Puoi trovare tali informazioni nel file di registro di CloudTrail. L'e-mail segnala invece che lo stato dell'allarme è

stato modificato da OK ad Alarm (Allarme). Per ulteriori informazioni sugli CloudWatch allarmi e sui cambiamenti di stato, consulta Using Amazon CloudWatch alarms nella Amazon CloudWatch User Guide.

> **Warning**
>
> Questo CloudWatch allarme Amazon non è in grado di rilevare l'uso della chiave pubblica di una chiave KMS asimmetrica al di fuori di. AWS KMS Per informazioni dettagliate sui rischi particolari derivanti dall'eliminazione delle chiavi KMS asimmetriche utilizzate per la crittografia a chiave pubblica, inclusa la creazione di testi cifrati che non possono essere decrittati, consulta Eliminazione delle chiavi KMS asimmetriche.

Argomenti

Requisiti per un allarme CloudWatch

Prima di creare un CloudWatch allarme, devi creare un AWS CloudTrail percorso e configurare CloudTrail la distribuzione dei file di CloudTrail log ad Amazon CloudWatch Logs. Hai anche bisogno di un argomento Amazon SNS per la notifica degli allarmi.

- Creazione di un trail CloudTrail.

  CloudTrail viene abilitato automaticamente sul tuo account al Account AWS momento della creazione dell'account. Tuttavia, per una registrazione continua di eventi nell'account, inclusi gli eventi per AWS KMS, crea un trail.

- Configura CloudTrail per consegnare i tuoi file di registro CloudWatch Logs.

  Configura la consegna dei tuoi file di CloudTrail registro ai CloudWatch registri. Ciò consente a CloudWatch Logs di monitorare i log per le richieste AWS KMS API che tentano di utilizzare una chiave KMS in attesa di eliminazione.

- Creazione di un argomento Amazon SNS.

  Quando l'allarme si attiva, ti avvisa inviando un messaggio e-mail a un indirizzo e-mail in un argomento Amazon Simple Notification Service (Amazon SNS).

Creazione dell'allarme CloudWatch

In questa procedura, crei un filtro metrico del gruppo di CloudWatch log che trova le istanze dell'eccezione di eliminazione in sospeso. Quindi, si crea un CloudWatch allarme basato sulla metrica del gruppo di log. Per informazioni sui filtri delle metriche dei gruppi di log, consulta Creazione di metriche da eventi di log utilizzando filtri nella Amazon CloudWatch Logs User Guide.

1. Crea un filtro CloudWatch metrico che analizzi i log. CloudTrail

   Segui le istruzioni in Creazione di un filtro di parametri per un gruppo di log utilizzando i seguenti valori obbligatori. Per gli altri campi, accetta i valori predefiniti e immetti i nomi come richiesto.

Campo	Valore
Modello di filtro	`{ $.eventSource = kms* && $.errorMessage = "* is pending deletion."}`
Valore del parametro	1

2. Crea un CloudWatch allarme basato sul filtro metrico creato nel passaggio 1.

   Segui le istruzioni riportate in Creazione di un CloudWatch allarme basato su un filtro metrico di gruppo di log utilizzando i seguenti valori obbligatori. Per gli altri campi, accetta i valori predefiniti e immetti i nomi come richiesto.

Campo	Valore
Filtro di parametri	Il nome del filtro di parametri che hai creato nella fase 1.
Tipo di soglia	Statico
Condizioni	Ogni volta che *`nome parametro`* è maggiore di 1
Punti dati da segnalare	1 di 1

Campo	Valore
Trattamento dei dati mancanti	Considera dati mancanti come buoni (non superano la soglia)

Dopo aver completato questa procedura, riceverai una notifica ogni volta che il nuovo CloudWatch allarme entra nello stato. `ALARM` Se ricevi una notifica per questo allarme, per crittografare o decrittografare i dati è possibile che sia ancora necessaria una chiave KMS pianificata per l'eliminazione. In questo caso, annulla l'eliminazione della chiave KMS e riconsidera la decisione di eliminarla.

Stabilire l'utilizzo passato di una chiave KMS

Prima di eliminare una chiave KMS, potresti voler sapere in che modo numerosi testi cifrati sono stati crittografati per quella chiave. AWS KMS non archivia queste informazioni né i testi cifrati. Sapere in che modo una chiave KMS è stata utilizzata in passato potrebbe aiutarti a decidere se ti servirà in futuro. In questo argomento vengono suggerite diverse strategie che consentono di determinare l'utilizzo passato di una chiave KMS.

> **Warning**
>
> Queste strategie per determinare l'utilizzo passato e corrente sono efficaci solo per gli utenti AWS e le operazioni AWS KMS. Non sono in grado di rilevare l'uso della chiave pubblica di una asimmetrica al di fuori di AWS KMS. Per informazioni dettagliate sui rischi particolari derivanti dall'eliminazione delle chiavi KMS asimmetriche utilizzate per la crittografia a chiave pubblica, inclusa la creazione di testi cifrati che non possono essere decrittati, consulta Eliminazione delle chiavi KMS asimmetriche.

Argomenti

- Analisi delle autorizzazioni della chiave KMS per determinare l'ambito dell'utilizzo potenziale
- Analisi dei log AWS CloudTrail per determinare l'utilizzo effettivo

Analisi delle autorizzazioni della chiave KMS per determinare l'ambito dell'utilizzo potenziale

Stabilire chi o cosa ha attualmente accesso a una chiave KMS potrebbe aiutarti a determinare in quale misura è stata utilizzata la chiave KMS e se è ancora necessaria. Per ulteriori informazioni su come determinare chi o cosa ha attualmente accesso a una chiave KMS, consulta Determinazione dell'accesso a una AWS KMS keys.

Analisi dei log AWS CloudTrail per determinare l'utilizzo effettivo

Potresti voler utilizzare la cronologia di utilizzo di una chiave KMS per stabilire se in una determinata chiave KMS sono crittografati i testi cifrati.

Tutte le attività API AWS KMS vengono registrate nei file di log AWS CloudTrail. Se hai creato un CloudTrail percorso nella regione in cui si trova la tua chiave KMS, puoi esaminare i tuoi file di CloudTrail registro per visualizzare una cronologia di tutte le attività dell'AWS KMSAPI per una particolare chiave KMS. Se un trail non è disponibile, è comunque possibile visualizzare gli eventi recenti nella cronologia degli eventi CloudTrail . Per informazioni dettagliate sulle modalità di AWS KMS utilizzo CloudTrail, consulta. Registrazione delle chiamate API AWS KMS con AWS CloudTrail

Gli esempi seguenti mostrano le voci di CloudTrail registro generate quando viene utilizzata una chiave KMS per proteggere un oggetto archiviato in Amazon Simple Storage Service (Amazon S3). In questo esempio, l'oggetto viene caricato in Amazon S3 utilizzando le informazioni riportate in Protezione dei dati utilizzando la crittografia lato server con chiavi KMS (SSE-KMS). Quando carichi un oggetto in Amazon S3 con SSE-KMS, specifichi la chiave KMS da utilizzare per proteggere l'oggetto. Amazon S3 utilizza l'AWS KMSGenerateDataKeyoperazione per richiedere una chiave dati univoca per l'oggetto e questo evento di richiesta viene registrato CloudTrail con una voce simile alla seguente:


```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROACKCEVSQ6C2EXAMPLE:example-user",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admins/example-user",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
```

```
        "creationDate": "2015-09-10T23:12:48Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/Admins",
        "accountId": "111122223333",
        "userName": "Admins"
      }
    },
    "invokedBy": "internal.amazonaws.com"
  },
  "eventTime": "2015-09-10T23:58:18Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "GenerateDataKey",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "internal.amazonaws.com",
  "userAgent": "internal.amazonaws.com",
  "requestParameters": {
    "encryptionContext": {"aws:s3:arn": "arn:aws:s3:::example_bucket/example_object"},
    "keySpec": "AES_256",
    "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  "responseElements": null,
  "requestID": "cea04450-5817-11e5-85aa-97ce46071236",
  "eventID": "80721262-21a5-49b9-8b63-28740e7ce9c9",
  "readOnly": true,
  "resources": [{
    "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "accountId": "111122223333"
  }],
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}
```

Quando in un secondo momento scarichi questo oggetto da Amazon S3, Amazon S3 invia una richiesta `Decrypt` a AWS KMS per decrittare la chiave di dati dell'oggetto utilizzando la chiave KMS specificata. Quando esegui questa operazione, i tuoi file di CloudTrail registro includono una voce simile alla seguente:

```
{
```

```
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROACKCEVSQ6C2EXAMPLE:example-user",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admins/example-user",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2015-09-10T23:12:48Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/Admins",
        "accountId": "111122223333",
        "userName": "Admins"
      }
    },
    "invokedBy": "internal.amazonaws.com"
  },
  "eventTime": "2015-09-10T23:58:39Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "Decrypt",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "internal.amazonaws.com",
  "userAgent": "internal.amazonaws.com",
  "requestParameters": {
    "encryptionContext": {"aws:s3:arn": "arn:aws:s3:::example_bucket/example_object"}},
  "responseElements": null,
  "requestID": "db750745-5817-11e5-93a6-5b87e27d91a0",
  "eventID": "ae551b19-8a09-4cfc-a249-205ddba330e3",
  "readOnly": true,
  "resources": [{
    "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "accountId": "111122223333"
  }],
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}
```

L'attività delle API di AWS KMS viene registrata da CloudTrail. Esaminando queste voci di registro, potresti essere in grado di determinare l'utilizzo passato di una chiave KMS specifica e ciò potrebbe aiutarti a decidere se eliminarla o meno.

Per vedere altri esempi di come l'attività delle AWS KMS API viene visualizzata nei file di CloudTrail registro, vai aRegistrazione delle chiamate API AWS KMS con AWS CloudTrail. Per ulteriori informazioni su questo argomento, CloudTrail consulta la Guida per AWS CloudTrail l'utente.

Stati chiave delle chiavi AWS KMS

UnA AWS KMS keyha sempre uno stato della chiave. Le operazioni sulla chiave KMS e sul relativo ambiente possono modificare lo stato della chiave, in modo transitorio o fino a quando un'altra operazione non modifica lo stato della chiave.

La tabella in questa sezione mostra come gli stati chiave influiscono sulle chiamate alle operazioni API AWS KMS. Come risultato dello stato della chiave, si prevede che un'operazione su una chiave KMS abbia esito positivo (#), esito negativo (X), o esito positivo solo in determinate condizioni (?). Il risultato spesso differisce per le chiavi KMS con il materiale della chiave importato.

Questa tabella include solo le operazioni API che utilizzano una chiave KMS. Altre operazioni, ad esempio CreateKeye ListKeys, vengono omesse.

Argomenti

- Stato chiave e tipi di chiave KMS
- Tabella dello stato delle chiavi

Stato chiave e tipi di chiave KMS

Il tipo di chiave KMS determina gli stati della chiave che può avere.

- Tutte le chiavi KMS possono essere incluse negli stati `Enabled`, `Disabled` e `PendingDeletion`.
- La maggior parte delle chiavi KMS viene creata nello stato `Enabled`. Le chiavi KMS con il materiale chiave importato vengono create nello stato `PendingImport`.
- Lo stato `PendingImport` si applica unicamente alle chiavi KMS con materiale chiave importato.
- Lo stato `Unavailable` si applica unicamente a una chiave KMS in un archivi delle chiavi personalizzate. Una chiave KMS in un archivio delle chiavi di AWS CloudHSM è `Unavailable`

quando l'archivio delle chiavi personalizzate viene disconnesso intenzionalmente dal relativo cluster AWS CloudHSM. Una chiave KMS in un archivio delle chiavi esterne è `Unavailable` quando l'archivio delle chiavi personalizzate viene disconnesso intenzionalmente dal relativo proxy dell'archivio delle chiavi esterne. Puoi visualizzare e gestire chiavi KMS non disponibili, ma non puoi utilizzarle nelle operazioni di crittografia.

Lo stato di una chiave KMS in un archivio delle chiavi personalizzate non è influenzato dalle modifiche apportate al relativo materiale della chiave. Una chiave KMS in un archivio delle chiavi di AWS CloudHSM non è influenzata dalle modifiche apportate al materiale della chiave associato nel cluster AWS CloudHSM. Una chiave KMS in un archivio delle chiavi esterne non è influenzata dalle modifiche apportate alla relativa chiave esterna in un gestore delle chiavi esterne. Se il materiale della chiave è disattivato o eliminato, lo stato della chiave KMS non cambia, ma le operazioni di crittografia che utilizzano la chiave KMS avranno esito negativo.

- Gli stati della chiave `Creating`, `Updating` e`PendingReplicaDeletion` si applicano solo alle chiavi multiregione.
  - Una chiave di replica multiregione si trova nello stato della chiave `Creating` transitorio mentre è in fase di creazione. Questo processo potrebbe essere ancora in corso al termine dell'ReplicateKeyoperazione. Una volta completato il processo di replica, la chiave di replica si trova nello stato `Enabled` o `PendingImport`.
  - Le chiavi multi-regione si trovano nello stato della chiave `Updating` transitorio durante l'aggiornamento della Regione primaria. Questo processo potrebbe essere ancora in corso al termine dell'UpdatePrimaryRegionoperazione. Al termine del processo di aggiornamento, le chiavi primarie e di replica riprendono lo stato della chiave `Enabled`.
  - Quando si pianificherà l'eliminazione di una chiave primaria multiregione che dispone di chiavi di replica, la chiave primaria si trova nello stato `PendingReplicaDeletion` finché non vengono eliminate tutte le chiavi di replica. Lo stato della chiave diventa `PendingDeletion`. Per informazioni dettagliate, vedi Eliminazione di chiavi multiregione.

Tabella dello stato delle chiavi

Nella tabella seguente viene illustrato l'effetto dello stato chiave di una chiave KMS sulle operazioni AWS KMS.

Le descrizioni delle note a piè di pagina numerate ([n]) si trovano alla fine di questo argomento.

> **Note**
>
> Potrebbe essere necessario scorrere orizzontalmente o verticalmente per visualizzare tutti i dati di questa tabella.

API	Abilitato	Disabilitato	In attesa di eliminazione In attesa di eliminazione della replica	In attesa di importazione	Non disponibile	Creazione	Aggiornamento in corso
CancelKeyDeletion	 [4]	 [4]		 [4]	 [4], [13]	 [4]	 [4]
CreateAlias			 [3]				
CreateGrant		 [1]	 [2] o [3]	 [5]		 [14]	
Decrypt		 [1]	 [2] o [3]	 [5]	 [11]	 [14]	
DeleteAlias							

API	Abilitato	Disabilitato	In attesa di eliminazione In attesa di eliminazione della replica	In attesa di importazione	Non disponibile	Creazione	Aggiornamento in corso
DeleteImportedKeyMaterial	✓ [9]	✓ [9]	✓ [9]	✓ (nessun effetto)	N/D	⊗ [14]	⊗ [15]
DescribeKey	✓	✓	✓	✓	✓	✓	✓
DisableKey	✓	✓	⊗ [3]	⊗ [5]	✓ [12]	⊗ [14]	⊗ [15]
DisableKeyRotation	? [7]	⊗ [1] o [7]	⊗ [3] o [7]	⊗ [6]	⊗ [7]	⊗ [14]	? [7]
EnableKey	✓	✓	⊗ [3]	⊗ [5]	✓ [12]	⊗ [14]	⊗ [15]
EnableKeyRotation	? [7]	⊗ [1] o [7]	⊗ [3] o [7]	⊗ [6]	⊗ [7]	⊗ [14]	? [7]

API	Abilitato	Disabilitato	In attesa di eliminazione In attesa di eliminazione della replica	In attesa di importazione	Non disponibile	Creazione	Aggiornamento in corso
Crittografa	✓	⊗ [1]	⊗ [2] o [3]	⊗ [5]	⊗ [11]	⊗ [14]	✓
GenerateDataKey	✓	⊗ [1]	⊗ [2] o [3]	⊗ [5]	⊗ [11]	⊗ [14]	✓
GenerateDataKeyPair	✓	⊗ [1]	⊗ [2] o [3]	⊗ [5]	⊗ [11]	⊗ [14]	✓
GenerateDataKeyPairWithoutPlaintext	✓	⊗ [1]	⊗ [2] o [3]	⊗ [5]	⊗ [11]	⊗ [14]	✓
GenerateDataKeyWithoutPlaintext	✓	⊗ [1]	⊗ [2] o [3]	⊗ [5]	⊗ [11]	⊗ [14]	✓
GenerateMac	✓	⊗ [1]	⊗ [2] o [3]	N/D	N/D	⊗ [14]	✓

API	Abilitato	Disabilitato	In attesa di eliminazione In attesa di eliminazione della replica	In attesa di importazione	Non disponibile	Creazione	Aggiornamento in corso
GetKeyPolicy							
GetKeyRotationStatus	 [7]	 [7]	 [7]	 [6]	 [7]	 [7]	 [7]
GetParametersForImport	 [9]	 [9]	 [8] o [9]		 [9]	 [14]	 [15]
GetPublicKey		 [1]	 [2] o [3]	N/D	N/D	 [14]	
ImportKeyMaterial	 [9]	 [9]	 [8] o [9]		 [9]	 [14]	
ListAliases							
ListGrants							

API	Abilitato	Disabilitato	In attesa di eliminazione In attesa di eliminazione della replica	In attesa di importazione	Non disponibile	Creazione	Aggiornamento in corso
ListKeyPolicies	✓	✓	✓	✓	✓	✓	✓
ListResourceTags	✓	✓	✓	✓	✓	✓	✓
PutKeyPolicy	✓	✓	✓	✓	✓	✓	✓
ReEncrypt	✓	⊗ [1]	⊗ [2] o [3]	⊗ [5]	⊗ [11]	⊗ [14]	✓
ReplicateKey	✓	⊗ [1]	⊗ [2] o [3]	⊗ [5]	N/D	⊗ [14]	⊗ [15]
RetireGrant	✓	✓	✓	✓	✓	✓	✓
RevokeGrant	✓	✓	✓	✓	✓	✓	✓
ScheduleKeyDeletion	✓	✓	⊗ [3]	✓	✓	✓	⊗ [15]

API	Abilitato	Disabilitato	In attesa di eliminazione In attesa di eliminazione della replica	In attesa di importazione	Non disponibile	Creazione	Aggiornamento in corso
Sign	✓	⊗ [1]	⊗ [2] o [3]	N/D	N/D	⊗ [14]	✓
TagResource	✓	✓	⊗ [3]	✓	✓	✓	✓
UntagResource	✓	✓	⊗ [3]	✓	✓	✓	✓
UpdateAlias	✓	✓	? [10]	✓	✓	✓	✓
UpdateKeyDescription	✓	✓	⊗ [3]	✓	✓	✓	✓
UpdatePrimaryRegion	✓	⊗ [1]	⊗ [2] o [3]	⊗ [5]	N/D	⊗ [14]	✓

API	Abilitato	Disabilitato	In attesa di eliminazione In attesa di eliminazione della replica	In attesa di importazione	Non disponibile	Creazione	Aggiornamento in corso
Verifica	✓	⊗ [1]	⊗ [2] o [3]	N/D	N/D	⊗ [14]	✓
VerifyMac	✓	⊗ [1]	⊗ [2] o [3]	N/D	N/D	⊗ [14]	✓

Dettagli tabella

- [1] `DisabledException: <key ARN> is disabled.`
- [2] `DisabledException: <key ARN> is pending deletion (or pending replica deletion).`
- [3] `KMSInvalidStateException: <key ARN> is pending deletion (or pending replica deletion).`
- [4] `KMSInvalidStateException: <key ARN> is not pending deletion (or pending replica deletion).`
- [5] `KMSInvalidStateException: <key ARN> is pending import.`
- [6] `UnsupportedOperationException: <key ARN> origin is EXTERNAL which is not valid for this operation.`
- [7] Se la chiave KMS ha importato materiale della chiave o si trova in un archivio delle chiavi personalizzate: `UnsupportedOperationException`.
- [8] Se la chiave KMS ha importato il materiale della chiave: `KMSInvalidStateException`

- [9] Se la chiave KMS non può avere o non ha materiale della chiave importato: `UnsupportedOperationException`.
- [10] Se la chiave KMS di origine è in attesa di eliminazione, il comando viene completato. Se la chiave KMS di destinazione è in attesa di eliminazione, il comando ha esito negativo con l'errore: `KMSInvalidStateException : <key ARN> is pending deletion.`
- [11] `KMSInvalidStateException: <key ARN> is unavailable.` Non puoi eseguire questa operazione su una chiave KMS non disponibile.
- [12] L'operazione riesce, ma lo stato di chiave della chiave KMS non cambia finché questa non diventa disponibile.
- [13] Quando una chiave KMS in un archivio delle chiavi personalizzate è in attesa di eliminazione, il relativo stato rimane `PendingDeletion` anche se la chiave KMS diventa non disponibile. Ciò ti consente di annullare l'eliminazione della chiave KMS in qualsiasi momento durante il periodo di attesa.
- [14] `KMSInvalidStateException: <key ARN> is creating.` AWS KMS genera questa eccezione mentre sta replicando una chiave multi-regione (`ReplicateKey`).
- [15] `KMSInvalidStateException: <key ARN> is updating.` AWS KMS genera questa eccezione mentre aggiorna la regione primaria di una chiave multi-regione (`UpdatePrimaryRegion`).

Autenticazione e controllo degli accessi per AWS KMS

Per utilizzare AWS KMS, l'utente deve disporre di credenziali che AWS può utilizzare per autenticare le richieste. Le credenziali devono includere le autorizzazioni per accedere alle risorse AWS, una AWS KMS keys e gli alias. Nessun principale AWS dispone di autorizzazioni per una chiave KMS a meno che tale autorizzazione non venga fornita esplicitamente e mai negata. Non sono disponibili autorizzazioni implicite o automatiche per l'utilizzo o la gestione di una chiave KMS.

Il modo principale per gestire l'accesso alle risorse AWS KMS è mediante le policy. Le policy sono documenti che descrivono quali principali possono accedere a quali risorse. Le policy allegate a un'identità IAM sono definite policy basate su identità (o policy IAM), mentre quelle collegate ad altri tipi di risorse vengono definite policy di risorse. Le policy di risorse AWS KMS per le chiavi KMS sono dette policy delle chiavi. Tutte le chiavi KMS dispongono di una policy delle chiavi.

Per controllare l'accesso agli alias AWS KMS, utilizzare le policy IAM. Per consentire ai principali di creare gli alias, è necessario fornire l'autorizzazione all'alias in una policy IAM e l'autorizzazione alla chiave in una policy delle chiavi. Per informazioni dettagliate, vedi Controllo dell'accesso agli alias.

Per controllare l'accesso alle chiavi KMS, è possibile utilizzare i seguenti meccanismi delle policy.

- Policy delle chiavi: ogni chiave KMS ha una policy delle chiavi. Le policy delle chiavi sono il meccanismo principale per controllare l'accesso a una chiave KMS. Puoi utilizzare la sola policy delle chiavi per il controllo dell'accesso, per cui l'accesso alla chiave KMS nella sua interezza è definito in un unico documento (la policy delle chiavi). Per ulteriori informazioni sull'utilizzo delle policy delle chiavi, consulta Policy delle chiavi.
- Policy IAM: è possibile utilizzare le policy IAM insieme alla policy delle chiavi e alle concessioni per controllare l'accesso a una chiave KMS. Il controllo dell'accesso eseguito in questo modo consente di gestire tutte le autorizzazioni delle identità IAM in IAM. Per utilizzare una policy IAM per consentire l'accesso a una chiave KMS, la policy delle chiavi deve consentirla esplicitamente. Per ulteriori informazioni sull'utilizzo di policy IAM consulta Policy IAM.
- Concessioni: è possibile utilizzare le concessioni insieme alla policy delle chiavi e alle policy IAM per consentire l'accesso a una chiave KMS. Il controllo dell'accesso eseguito in questo modo ti consente di accedere alla chiave KMS nella policy delle chiavi e di permettere alle identità di delegare l'accesso ad altri utenti. Per ulteriori informazioni sull'utilizzo di concessioni, consulta Concessioni in AWS KMS.

Le chiavi KMS appartengono all'account AWS in cui sono state create. Tuttavia, nessuna identità o principale, incluso l'utente root dell'account AWS, ha il permesso di utilizzare o gestire una chiave KMS a meno che tale autorizzazione non sia esplicitamente fornita in una policy delle chiavi, una policy IAM o una concessione. L'identità IAM che crea una chiave KMS non è considerata il proprietario della chiave e non dispone automaticamente dell'autorizzazione a utilizzare o gestire la chiave KMS creata. Come qualsiasi altra identità, il creatore di chiavi deve ottenere l'autorizzazione tramite una policy chiave, una policy IAM o una concessione. Tuttavia, le identità che hanno l'autorizzazione `kms:CreateKey` possono impostare la policy chiave iniziale e concedersi l'autorizzazione all'utilizzo o alla gestione della chiave.

Nelle sezioni seguenti vengono fornite informazioni dettagliate su come utilizzare AWS Identity and Access Management (IAM) e le autorizzazioni AWS KMS per contribuire a proteggere le risorse tramite il controllo degli accessi.

Argomenti

Concetti del controllo degli accessi di AWS KMS

Scopri i concetti utilizzati nelle discussioni sul controllo degli accessi in AWS KMS.

Argomenti

- Autenticazione
- Autorizzazione
- Autenticazione con identità
- Gestione dell'accesso con policy
- Risorse AWS KMS

Autenticazione

L'autenticazione è il processo di verifica della tua identità. Per inviare una richiesta a AWS KMS, devi accedere ad AWS utilizzando le tue credenziali AWS.

Autorizzazione

L'autorizzazione consente di inviare richieste per creare, gestire o utilizzare risorse AWS KMS. Ad esempio, devi avere l'autorizzazione per utilizzare una chiave KMS in un'operazione di crittografia.

Usa policy delle chiavi, policy IAM e concessioni per controllare gli accessi alle risorse AWS KMS. Ogni chiave KMS deve avere una policy delle chiavi. Se la policy delle chiavi lo consente, puoi anche utilizzare le policy IAM e le concessioni per consentire ai principali l'accesso alla chiave KMS. Per affinare l'autorizzazione, puoi utilizzare le chiavi di condizione che consentono o negano l'accesso solo quando una richiesta o una risorsa soddisfa le condizioni specificate. Puoi permettere l'accesso ai principali attendibili in altri Account AWS.

Autenticazione con identità

L'autenticazione è la procedura di accesso ad AWS con le credenziali di identità. Devi essere autenticato (connesso a AWS) come utente root Utente root dell'account AWS, come utente IAM o assumere un ruolo IAM.

Puoi accedere ad AWS come identità federata utilizzando le credenziali fornite attraverso un'origine di identità. Gli utenti AWS IAM Identity Center (Centro identità IAM), l'autenticazione Single Sign-On (SSO) dell'azienda e le credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Se accedi ad AWS tramite la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere alla AWS Management Console o al portale di accesso AWS. Per ulteriori informazioni sull'accesso ad AWS, consulta la sezione Come accedere al tuo Account AWS nella Guida per l'utente di Accedi ad AWS.

Se accedi ad AWS in modo programmatico, AWS fornisce un Software Development Kit (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le richieste utilizzando le tue credenziali. Se non utilizzi gli strumenti AWS, devi firmare le richieste personalmente. Per ulteriori informazioni sulla firma delle richieste, consulta Firma delle richieste AWS nella Guida per l'utente IAM.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. AWS consiglia ad esempio di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza dell'account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA) in AWS nella Guida per l'utente di IAM.

Utente root di un Account AWS

Quando crei un Account AWS, inizi con una singola identità di accesso che ha accesso completo a tutti i Servizi AWS e le risorse nell'account. Tale identità è detta utente root Account AWS ed è possibile accedervi con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzarle per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente di IAM.

Identità federata

Come best practice, richiedi agli utenti umani, compresi quelli che richiedono l'accesso di amministratore, di utilizzare la federazione con un provider di identità per accedere a Servizi AWSutilizzando credenziali temporanee.

Un'identità federata è un utente della directory degli utenti aziendali, un provider di identità Web, AWS Directory Service, la directory Identity Center o qualsiasi utente che accede ai Servizi AWS utilizzando le credenziali fornite tramite un'origine di identità. Quando le identità federate accedono agli Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. È possibile creare utenti e gruppi in IAM Identity Center oppure connettersi e sincronizzarsi con un gruppo di utenti e gruppi nell'origine di identità per utilizzarli in tutte le applicazioni e gli Account AWS. Per ulteriori informazioni sul Centro identità IAM, consulta Cos'è Centro identità IAM? nella Guida per l'utente di AWS IAM Identity Center.

Utenti e gruppi IAM

Un utente IAM è una identità all'interno del tuo Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, per casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente di IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato Amministratori IAM e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità all'interno di un Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. È possibile assumere temporaneamente un ruolo IAM nella AWS Management Console mediante lo scambio di ruoli. È possibile assumere un ruolo chiamando un'azione AWS CLI o API AWS oppure utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente di IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente di IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un

ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per ulteriori informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center.

- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, per alcuni dei Servizi AWS, è possibile collegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.
- Accesso multi-servizio: alcuni Servizi AWS utilizzano funzionalità in altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Inoltro delle sessioni di accesso (FAS): quando si utilizza un utente o un ruolo IAM per eseguire operazioni in AWS, tale utente o ruolo viene considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che effettua la chiamata a un Servizio AWS, combinate con il Servizio AWS richiedente, per effettuare richieste a servizi a valle. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che necessita di interazioni con altri Servizi AWS o risorse per essere portata a termine. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM assunto da un servizio per eseguire operazioni per conto dell'utente. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati ai servizi sono visualizzati nell'account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

- Applicazioni in esecuzione su Amazon EC2: è possibile utilizzare un ruolo IAM per gestire credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 che eseguono richieste di AWS CLIo dell'API AWS. Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un ruolo AWS a un'istanza EC2, affinché sia disponibile per tutte le relative applicazioni, puoi creare un profilo dell'istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente di IAM.

Gestione dell'accesso con policy

Per controllare l'accesso a AWS è possibile creare policy e collegarle a identità o risorse AWS. Una policy è un oggetto in AWS che, quando associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste policy quando un principale IAM (utente, utente root o sessione ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle policy viene archiviata in AWSsotto forma di documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente di IAM.

Gli amministratori possono utilizzare le policy AWSJSON per specificare l'accesso ai diversi elementi. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. Successivamente l'amministratore può aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'azione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dalla AWS Management Console, la AWS CLI o l'API AWS.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono incorporate direttamente in un singolo utente, gruppo o ruolo. Le policy gestite sono policy autonome che possono essere collegate a più utenti, gruppi e ruoli in Account AWS. Le policy gestite includono le policy gestite da AWS e le policy gestite dal cliente. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente di IAM.

Policy basate su risorse

Una policy delle chiavi AWS KMS è una policy basata sulle risorse che controlla l'accesso a una chiave KMS. Ogni chiave KMS deve avere una policy delle chiavi. Puoi utilizzare un altro meccanismo di autorizzazione per consentire l'accesso alla chiave KMS, ma solo se la policy delle chiavi lo consente. (Puoi utilizzare una policy IAM per negare l'accesso a una chiave KMS anche se la policy delle chiavi non lo consente esplicitamente).

Le policy basate sulle risorse sono documenti di policy JSON che colleghi a una risorsa, come una chiave KMS, per controllare l'accesso a una risorsa specifica. Le policy basate su risorse stabiliscono quali operazioni uno specifico principale può eseguire, su quale risorsa e in quali condizioni. Non specifichi la risorsa in una policy basata sulle risorse, ma devi specificare un principale, ad esempio account, utenti, ruoli, utenti federati o Servizi AWS. Le policy basate sulle risorse sono policy inline che si trovano nel servizio che gestisce la risorsa. Non puoi utilizzare le policy gestite da AWS da IAM, come una policy gestita da `AWSKeyManagementServicePowerUser` in una policy basata sulle risorse.

Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3, AWS WAF e Amazon VPC sono esempi di servizi che supportano le ACL. Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

AWS KMS non supporta le ACL.

Altri tipi di policy

AWS supporta altri tipi di policy meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzione avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.
- Policy di controllo dei servizi (SCP): le SCP sono policy JSON che specificano il numero massimo di autorizzazioni per un'organizzazione o unità organizzativa (OU) in AWS Organizations. AWS Organizationsè un servizio per il raggruppamento e la gestione centralizzata degli Account AWSmultipli di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. La SCP limita le autorizzazioni per le entità negli account membri, compreso ogni Utente root dell'account AWS. Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations.
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente di IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per informazioni su come AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella Guida per l'utente di IAM.

Risorse AWS KMS

In AWS KMS, la risorsa primaria è una AWS KMS key. AWS KMS supporta anche un alias, una risorsa indipendente che fornisce un nome descrittivo per una chiave KMS. Alcune operazioni AWS KMS ti consentono di utilizzare un alias per identificare una chiave KMS.

Ogni istanza di una chiave KMS o un alias ha un Amazon Resource Name (ARN) univoco con un formato standard. Nelle risorse AWS KMS, il nome del servizio AWS è `kms`.

- AWS KMS key

  Formato ARN:

  `arn:`*`AWS partition name`*`:`*`AWS service name`*`:`*`Regione AWS`*`:`*`Account AWS ID`*`:key/`*`key ID`*

  Esempio di ARN:

  ```
  arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
  ```

- Alias

  Formato ARN:

  `arn:`*`AWS partition name`*`:`*`AWS service name`*`:`*`Regione AWS`*`:`*`Account AWS ID`*`:alias/`*`alias name`*

  Esempio di ARN:

  ```
  arn:aws:kms:us-west-2:111122223333:alias/example-alias
  ```

AWS KMS fornisce un set di operazioni API da utilizzare con le risorse AWS KMS. Per ulteriori informazioni sull'identificazione delle chiavi KMS nelle operazioni API AWS Management Console e AWS KMS, consulta Identificatori chiave () KeyId. Per visualizzare un elenco di operazioni AWS KMS, consulta la documentazione di riferimento delle API AWS Key Management Service.

Policy delle chiavi in AWS KMS

Una policy della chiave è una policy delle risorse per una AWS KMS key. Le policy chiave sono lo strumento principale per controllare l'accesso alle chiavi KMS. Ogni chiave KMS deve avere

esattamente una policy chiave. Le istruzioni nella policy delle chiavi determinano chi dispone dell'autorizzazione per utilizzare la chiave KMS e come questa può essere utilizzata. Puoi anche usare le policy IAM e le concessioni per controllare l'accesso alla chiave KMS, ma ogni chiave KMS deve avere un documento di policy delle chiavi.

Nessun principale AWS, neanche l'utente root o il creatore delle chiavi, dispone di autorizzazioni per una chiave KMS a meno che non sia esplicitamente consentito e mai negato, in una policy delle chiavi, in una policy IAM o in una concessione.

A meno che la policy delle chiavi non lo consenta esplicitamente, non è possibile utilizzare le policy IAM per permettere l'accesso a una chiave KMS. Senza l'autorizzazione dalla policy delle chiavi, le policy IAM che consentono le autorizzazioni non hanno alcun effetto. È possibile utilizzare una policy IAM per negare un'autorizzazione a una chiave KMS senza l'autorizzazione da una policy delle chiavi. Per impostazione predefinita, la policy delle chiavi di default abilita le policy IAM. Per abilitare le policy IAM nella policy delle chiavi, aggiungere l'istruzione della policy descritta in Consente l'accesso a Account AWS e abilita le policy IAM.

A differenza delle policy IAM, che sono globali, le policy chiave sono regionali. Una policy delle chiavi controlla l'accesso a una sola chiave KMS nella stessa regione. Non ha alcun effetto sulle chiavi KMS in altre regioni.

Argomenti

- Creazione di una policy delle chiavi
- Policy delle chiavi predefinita
- Visualizzazione di una policy di chiave
- Modifica di una policy delle chiavi
- Autorizzazioni per i servizi AWS nelle policy delle chiavi

Creazione di una policy delle chiavi

È possibile creare e gestire le policy chiave nella AWS KMS console, utilizzando operazioni AWS KMS API CreateKey, ad esempio e ReplicateKeyPutKeyPolicy, o utilizzando un AWS CloudFormationmodello.

Quando si crea una chiave KMS nella console AWS KMS, l'utente viene guidato attraverso le fasi di creazione di una policy delle chiavi basata sulla policy delle chiavi di default per la console.

Quando utilizzi le API `CreateKey` o `ReplicateKey`, se non specifichi una policy della chiave, le API applicano la policy della chiave predefinita per le chiavi create a livello di programmazione. Quando usi l'API `PutKeyPolicy`, devi specificare una policy della chiave.

Ogni documento di policy può avere una o più istruzioni di policy. L'esempio seguente mostra un documento di policy della chiave valido con un'istruzione della policy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Describe the policy statement",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:user/Alice"
      },
      "Action": "kms:DescribeKey",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:KeySpec": "SYMMETRIC_DEFAULT"
        }
      }
    }
  ]
}
```

Argomenti

- Formato della policy della chiave
- Elementi in una policy della chiave
- Esempi di policy delle chiavi

Formato della policy della chiave

Un documento di policy della chiave deve rispettare le seguenti regole:

- Fino a 32 kilobyte (32.768 byte)
- L'elemento `Sid` in un'istruzione di policy della chiave non può includere spazi. Gli spazi sono vietati nell'elemento `Sid` di un documento di policy IAM.

Un documento di policy della chiave può includere solo i seguenti caratteri:

- Caratteri ASCII stampabili
- I caratteri stampabili nel set di caratteri Basic Latin e Latin-1 Supplement
- I caratteri speciali di tabulazione (`\u0009`), avanzamento di riga (`\u000A`) e ritorno a capo (`\u000D`)

Elementi in una policy della chiave

Un documento di policy delle chiavi deve avere i seguenti elementi:

Versione

Specifica la versione del documento della policy della chiave. Impostare la versione su `2012-10-17` (la versione più recente).

Dichiarazione

Include le istruzioni della policy. Un documento di policy delle chiavi deve avere almeno un'istruzione.

Ogni istruzione in una policy della chiave può contenere fino a sei elementi. Gli elementi `Effect`, `Principal`, `Action` e `Resource` sono obbligatori.

Sid

(Facoltativo) L'identificatore di istruzione (`Sid`) è una stringa arbitraria che è possibile utilizzare per descrivere l'istruzione. Il `Sid` in una policy della chiave può includere spazi. Non è possibile includere spazi nell'elemento `Sid` di una policy IAM.

Effetto

(Obbligatorio) Specifica se concedere o negare le autorizzazioni nell'istruzione di policy. I valori validi sono `Allow` e `Deny`. Se non concedi esplicitamente l'accesso a una chiave KMS, l'accesso viene implicitamente rifiutato. È anche possibile negare esplicitamente l'accesso a una chiave KMS. È possibile eseguire questa operazione per accertarsi che un utente non sia in grado di accedervi, anche quando l'accesso viene concesso da un'altra policy.

Principale

(Obbligatorio) Il principale è l'identità che ottiene le autorizzazioni specificate nell'istruzione di policy. È possibile specificare Account AWS, utenti IAM, ruoli IAM e alcuni servizi AWS come

principali in una policy delle chiavi. I gruppi di utenti IAM non sono un principale valido in alcun tipo di policy.

Un valore asterisco, ad esempio `"AWS": "*"`, rappresenta tutte le identità AWS in tutti gli account.

> **Important**
>
> Non impostare il principale su un asterisco (*) in un'istruzione della policy della chiave che consenta autorizzazioni, a meno che non utilizzi condizioni per limitare la policy della chiave. Un asterisco dà ogni identità in ogni Account AWS l'autorizzazione a utilizzare la chiave KMS, a meno che un'altra istruzione di policy lo neghi esplicitamente. Gli utenti in altri Account AWS possono utilizzare la tua chiave KMS ogni qualvolta dispongono delle autorizzazioni corrispondenti nel loro account.

> **Note**
>
> Le best practice di IAM disincentivano l'uso di utenti IAM con credenziali a lungo termine. Quando possibile, utilizza i ruoli IAM che forniscono credenziali temporanee. Per i dettagli, consulta la sezione Best practice di sicurezza in IAM nella Guida per l'utente IAM.

Quando il principale in una istruzione di policy delle chiavi è un principale Account AWS espresso come `arn:aws:iam::111122223333:root"`, l'istruzione non fornisce l'autorizzazione ad alcun principale IAM. Invece, fornisce l'autorizzazione Account AWS per utilizzare le policy IAM per delegare le autorizzazioni specificate nella policy delle chiavi. (Un principale in formato `arn:aws:iam::111122223333:root"` non rappresenta l'utente root dell'account AWS, nonostante l'uso di "root" nell'identificatore dell'account. Tuttavia, il principale dell'account rappresenta l'account e i relativi amministratori, incluso l'utente root dell'account.)

Quando il principale è un altro Account AWS o i relativi principali, le autorizzazioni sono valide solo quando l'account è abilitato nella regione con la chiave KMS e la policy delle chiavi KMS. Per informazioni sulle regioni non abilitate per impostazione predefinita ("regioni attivate"), consulta Gestione delle Regioni AWS nella Riferimenti generali di AWS.

Per consentire a un Account AWS diverso o ai relativi principali l'uso di una chiave KMS, è necessario fornire l'autorizzazione in una policy delle chiavi e in una policy IAM nell'altro account. Per informazioni dettagliate, vedi Autorizzazione per gli utenti in altri account di utilizzare una chiave KMS.

Azione

(Obbligatorio) Specificano le operazioni API da permettere o negare. Ad esempio, l'operazione `kms:Encrypt` corrisponde all'operazione AWS KMSEncrypt. È possibile elencare più di un'operazione in un'istruzione di policy. Per ulteriori informazioni, consultare Riferimento per le autorizzazioni.

Risorsa

(Obbligatorio) In una policy della chiave, il valore dell'elemento Resource (Risorsa) è `"*"`, che significa "questa chiave KMS". L'asterisco (`"*"`) identifica la chiave KMS a cui è collegata la policy delle chiavi.

> **Note**
>
> Se l'elemento `Resource` obbligatorio non è presente nell'istruzione della policy delle chiavi, l'istruzione non avrà alcun effetto. Una istruzione di policy delle chiavi senza un elemento `Resource` non si applica ad alcuna chiave KMS.
> Quando manca un `Resource` elemento in una dichiarazione di policy chiave, la AWS KMS console segnala correttamente un errore, ma le PutKeyPolicyAPI CreateKeye hanno successo, anche se l'informativa è inefficace.

Condition

(Facoltativo) Le condizioni specificano i requisiti da soddisfare affinché una policy della chiave diventi effettiva. Con le condizioni, AWS può valutare il contesto di una richiesta API per determinare se la policy vale o meno.

Per specificare le condizioni, per impostazione predefinita è necessario utilizzare chiavi di condizione. AWS KMS supporta chiavi di condizione globali AWS e chiavi di condizione AWS KMS. Per supportare il controllo dell'accesso basato su attributi (ABAC), AWS KMS fornisce chiavi di condizione che controllano l'accesso a una chiave KMS in base a tag e alias. Per informazioni dettagliate, vedi ABAC per AWS KMS.

Il formato per una condizione è:

```
"Condition": {"condition operator": {"condition key": "condition value"}}
```

come per esempio:

```
"Condition": {"StringEquals": {"kms:CallerAccount": "111122223333"}}
```

Per informazioni sulla sintassi delle policy AWS, consulta Documentazione di riferimento sulle policy IAMAWS nella Guida per l'utente di IAM.

Esempi di policy delle chiavi

L'esempio seguente mostra una policy della chiave completa per una chiave KMS di crittografia simmetrica. È utile come riferimento mentre leggi i concetti della policy delle chiavi in questo capitolo. Questa policy delle chiavi combina le istruzioni di policy di esempio della sezione precedente sulla policy delle chiavi predefinita in un'unica policy delle chiavi che ottiene quanto segue:

- Concede all'Account AWS di esempio, 111122223333, l'accesso completo alla chiave KMS. Concede all'account e ai relativi amministratori, incluso l'utente root dell'account (per le emergenze), l'uso delle policy IAM nell'account per consentire l'accesso alla chiave KMS.
- Consente al ruolo IAM `ExampleAdminRole` di amministrare la chiave KMS.
- Permette al ruolo IAM `ExampleUserRole` di utilizzare la chiave KMS.

```
{
    "Id": "key-consolepolicy",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow access for Key Administrators",
            "Effect": "Allow",
```

```
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/ExampleAdminRole"
            },
            "Action": [
                "kms:Create*",
                "kms:Describe*",
                "kms:Enable*",
                "kms:List*",
                "kms:Put*",
                "kms:Update*",
                "kms:Revoke*",
                "kms:Disable*",
                "kms:Get*",
                "kms:Delete*",
                "kms:TagResource",
                "kms:UntagResource",
                "kms:ScheduleKeyDeletion",
                "kms:CancelKeyDeletion"
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/ExampleUserRole"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow attachment of persistent resources",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/ExampleUserRole"
            },
            "Action": [
                "kms:CreateGrant",
```

```
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                }
            }
        }
    ]
}
```

Policy delle chiavi predefinita

Quando si crea una chiave KMS, è possibile specificare la policy delle chiavi per la nuova chiave KMS. Se non ne fornisci una, AWS KMS la crea per te. La policy delle chiavi predefinita utilizzata da AWS KMS varia a seconda che la chiave venga creata nella console AWS KMS o se si utilizza l'API AWS KMS.

La policy delle chiavi predefinita al momento della creazione di una chiave KMS a livello di programmazione

Quando si crea una chiave KMS a livello di programmazione con l'API AWS KMS (anche usando gli SDK AWS, AWS Command Line Interface o AWS Tools for PowerShell) e non si specifica una policy delle chiavi, AWS KMS applica una policy delle chiavi predefinita molto semplice. Questa policy delle chiavi predefinita incluse un'unica istruzione della policy che fornisce all'Account AWS che possiede la chiave KMS l'autorizzazione per utilizzare le policy IAM per consentire l'accesso a tutte le operazioni AWS KMS sulla chiave KMS. Per ulteriori informazioni su questa istruzione di policy, consulta Consente l'accesso a Account AWS e abilita le policy IAM.

La policy delle chiavi prefefinita al momento della creazione di una chiave KMS con la AWS Management Console

Quando si crea una chiave KMS tramite la AWS Management Console, la policy delle chiavi inizia con l'istruzione della policy che consente l'accesso all'Account AWS e abilita le policy IAM. La console aggiunge quindi una istruzione per gli amministratori delle chiavi, una istruzione per gli utenti delle chiavi e (per la maggior parte dei tipi di chiavi) un'istruzione che consente ai principali di utilizzare la chiave KMS con altri servizi AWS. È possibile utilizzare le funzionalità della console AWS

KMS per specificare gli utenti e i ruoli IAM e gli Account AWS che sono amministratori delle chiavi e quelli che sono utenti delle chiavi (o entrambi).

Autorizzazioni

- Consente l'accesso a Account AWS e abilita le policy IAM
- Consente agli amministratori delle chiavi di amministrare la chiave KMS
- Consente agli utenti della chiave di utilizzare la chiave KMS
  - Consente agli utenti della chiave di utilizzare una chiave KMS per le operazioni di crittografia
  - Consente agli utenti della chiave di utilizzare la chiave KMS con i servizi AWS

Consente l'accesso a Account AWS e abilita le policy IAM

La seguente istruzione delle policy delle chiavi predefinita è fondamentale.

- Fornisce all'Account AWS che possiede la chiave KMS l'accesso completo alla chiave KMS.

  A differenza di altre policy di risorse AWS, una policy delle chiavi AWS KMS non fornisce automaticamente l'autorizzazione all'account o alle relative identità. Per concedere l'autorizzazione agli amministratori di account, la policy delle chiavi deve includere un'istruzione esplicita che fornisce l'autorizzazione, come questa.
- Consente all'account di utilizzare le policy IAM per consentire l'accesso alla chiave KMS, oltre alla policy delle chiavi.

  Senza questa autorizzazione, le policy IAM che consentono l'accesso alla chiave sono inefficaci, anche se le policy IAM che negano l'accesso alla chiave sono ancora valide.
- Riduce il rischio che la chiave diventi ingestibile fornendo l'autorizzazione per il controllo degli accessi agli amministratori dell'account, incluso l'utente root dell'account, che non può essere eliminato.

La seguente istruzione della policy delle chiavi è l'unica policy delle chiavi predefinita per le chiavi KMS create a livello di programmazione. È la prima istruzione di policy nella policy delle chiavi predefinita per le chiavi KMS create nella console AWS KMS.

```
{
  "Sid": "Enable IAM User Permissions",
  "Effect": "Allow",
```

```
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:root"
   },
  "Action": "kms:*",
  "Resource": "*"
}
```

Consente alle policy IAM di controllare l'accesso alla chiave KMS.

L'istruzione della policy delle chiavi illustrata sopra fornisce all'Account AWS che possiede la chiave l'autorizzazione per utilizzare le policy IAM, nonché le policy delle chiavi, per consentire tutte le operazioni (`kms:*`) sulla chiave KMS.

Il principale in questa istruzione della policy delle chiavi è il principale dell'account, rappresentato da un ARN nel formato `arn:aws:iam::account-id:root`. Il principale dell'account rappresenta l'account AWS e i relativi amministratori.

Quando il principale in una istruzione di policy delle chiavi è il principale dell'account, l'istruzione della policy non fornisce al principale IAM l'autorizzazione a utilizzare la chiave KMS. Consente invece all'account di utilizzare le policy IAM per delegare le autorizzazioni specificate nell'istruzione della policy. Questa istruzione di policy delle chiavi predefinita consente all'account di utilizzare le policy IAM per delegare l'autorizzazione per tutte le operazioni (`kms:*`) sulla chiave KMS.

Riduce il rischio che la chiave KMS diventi ingestibile.

A differenza di altre policy di risorse AWS, una policy delle chiavi AWS KMS non fornisce automaticamente l'autorizzazione all'account o ai relativi principali. Per fornire l'autorizzazione a qualsiasi principale, incluso il principale dell'account, è necessario utilizzare una istruzione della policy delle chiavi che fornisca esplicitamente l'autorizzazione. Non è richiesto di concedere al principale dell'account, o a qualsiasi principale, l'accesso alla chiave KMS. Tuttavia, l'accesso al principale dell'account aiuta a evitare che la chiave diventi ingestibile.

Ad esempio, si supponga di creare una policy delle chiavi che dia a un solo utente l'accesso alla chiave KMS. Se questo utente viene eliminato, la chiave diventa ingestibile e diventa necessario contattare AWS Support per ottenere di nuovo l'accesso alla chiave KMS.

L'istruzione della policy delle chiavi illustrata sopra fornisce l'autorizzazione per controllare la chiave al principale dell'account, che rappresenta l'Account AWS e i relativi amministratori, incluso l'utente root dell'account. L'utente root dell'account è l'unico principale che non può essere

eliminato a meno che non si elimini l'Account AWS. Le best practice IAM scoraggiano l'operazione per conto dell'utente root dell'account, tranne in caso di emergenza. Tuttavia, potrebbe essere necessario agire come utente root dell'account se si eliminano tutti gli altri utenti e ruoli con accesso alla chiave KMS.

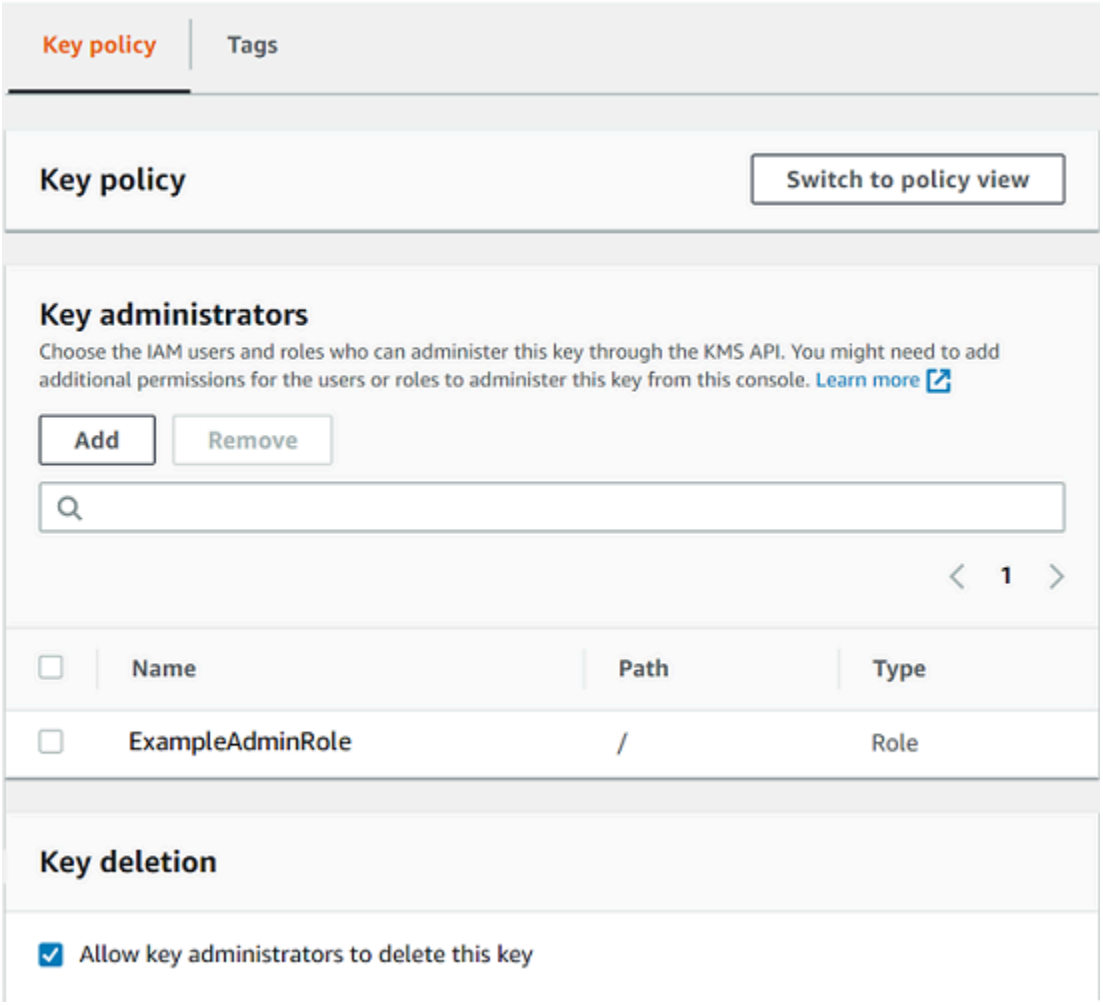
Consente agli amministratori delle chiavi di amministrare la chiave KMS

La policy delle chiavi predefinita creata dalla console consente di scegliere gli utenti e i ruoli IAM nell'account e renderli amministratori delle chiavi. Questa istruzione si chiama istruzione degli amministratori delle chiavi. Gli amministratori delle chiavi dispongono delle autorizzazioni per gestire la chiave KMS, ma non dispongono delle autorizzazioni per utilizzare la chiave KMS nelle operazioni di crittografia. È possibile aggiungere utenti e ruoli IAM all'elenco degli amministratori delle chiavi quando si crea la chiave KMS nella visualizzazione di default o nella visualizzazione della policy.

> **Warning**
>
> Poiché gli amministratori delle chiavi dispongono dell'autorizzazione per modificare la policy delle chiavi, possono concedere a loro stessi e ad altri le autorizzazioni AWS KMS non specificate in questa policy.
> I principali che dispongono dell'autorizzazione per gestire tag e alias possono anche controllare l'accesso a una chiave KMS. Per informazioni dettagliate, vedi ABAC per AWS KMS.

> **Note**
>
> Le best practice di IAM disincentivano l'uso di utenti IAM con credenziali a lungo termine. Quando possibile, utilizza i ruoli IAM che forniscono credenziali temporanee. Per i dettagli, consulta la sezione Best practice di sicurezza in IAM nella Guida per l'utente IAM.

L'esempio seguente mostra l'istruzione degli amministratori della chiave nella visualizzazione predefinita della console AWS KMS.



L'esempio seguente mostra un esempio di istruzione degli amministratori della chiave nella visualizzazione della policy della console AWS KMS. Questa istruzione degli amministratori della chiave si riferisce a una chiave KMS di crittografia simmetrica mono-regione.

```
{
  "Sid": "Allow access for Key Administrators",
  "Effect": "Allow",
  "Principal": {"AWS":"arn:aws:iam::111122223333:role/ExampleAdminRole"},
  "Action": [
    "kms:Create*",
    "kms:Describe*",
    "kms:Enable*",
    "kms:List*",
    "kms:Put*",
    "kms:Update*",
    "kms:Revoke*",
    "kms:Disable*",
```

```
    "kms:Get*",
    "kms:Delete*",
    "kms:TagResource",
    "kms:UntagResource",
    "kms:ScheduleKeyDeletion",
    "kms:CancelKeyDeletion"
  ],
  "Resource": "*"
}
```

L'istruzione predefinita degli amministratori della chiave per la chiave KMS più comune, una chiave KMS di crittografia simmetrica mono-regione, concede le seguenti autorizzazioni. Per informazioni dettagliate su ciascuna autorizzazione, consultare AWS KMS autorizzazioni.

Quando si utilizza la console AWS KMS per creare una chiave KMS, la console aggiunge gli utenti e i ruoli specificati all'elemento `Principal` nell'istruzione degli amministratori della chiave.

Molte di queste autorizzazioni contengono il carattere jolly (*), che concede tutte le autorizzazioni che iniziano con il verbo specificato. Di conseguenza, quando AWS KMS aggiunge nuove operazioni API, gli amministratori della chiave sono automaticamente autorizzati a utilizzarle. Non è necessario aggiornare le policy della chiave per includere le nuove operazioni. Se si preferisce limitare gli amministratori della chiave a un set fisso di operazioni API, è possibile modificare la policy della chiave.

`kms:Create*`

Consente `kms:CreateAlias` e `kms:CreateGrant`. (L'autorizzazione `kms:CreateKey` è valida solo in una policy IAM.)

`kms:Describe*`

Consente `kms:DescribeKey`. L'autorizzazione `kms:DescribeKey` è richiesta per visualizzare la pagina dei dettagli della chiave per una chiave KMS nella AWS Management Console.

`kms:Enable*`

Permette `kms:EnableKey`. Per le chiavi KMS di crittografia simmetrica, consente anche `kms:EnableKeyRotation`.

`kms:List*`

Permette `kms:ListGrants`, `kms:ListKeyPolicies` e `kms:ListResourceTags`. (Le autorizzazioni `kms:ListAliases` e `kms:ListKeys`, che sono necessarie per visualizzare le chiavi KMS nella AWS Management Console, sono valide solo nelle policy IAM.)

`kms:Put*`

Consente `kms:PutKeyPolicy`. Questa autorizzazione consente agli amministratori della chiave di modificare la policy della chiave per questa chiave KMS.

`kms:Update*`

Consente `kms:UpdateAlias` e `kms:UpdateKeyDescription`. Per le chiavi multi-Regione, consente `kms:UpdatePrimaryRegion` su questa chiave KMS.

`kms:Revoke*`

Concede `kms:RevokeGrant`, che permette agli amministratori della chiave di eliminare una concessione anche se non sono un principale per il ritiro nella concessione.

`kms:Disable*`

Permette `kms:DisableKey`. Per le chiavi KMS di crittografia simmetrica, consente anche `kms:DisableKeyRotation`.

`kms:Get*`

Permette `kms:GetKeyPolicy` e `kms:GetKeyRotationStatus`. Per le chiavi KMS con materiale chiave importato, consente `kms:GetParametersForImport`. Per le chiavi KMS asimmetriche, consente `kms:GetPublicKey`. L'autorizzazione `kms:GetKeyPolicy` è richiesta per visualizzare la policy della chiave per una chiave KMS nella AWS Management Console.

`kms:Delete*`

Consente `kms:DeleteAlias`. Per le chiavi con materiale chiave importato, consente `kms:DeleteImportedKeyMaterial`. L'autorizzazione `kms:Delete*` non consente agli amministratori della chiave di eliminare la chiave KMS (`ScheduleKeyDeletion`).

`kms:TagResource`

Consente `kms:TagResource`, per cui gli amministratori della chiave possono aggiungere tag alla chiave KMS. Poiché i tag possono essere utilizzati anche per controllare l'accesso alla chiave KMS, questa autorizzazione può consentire agli amministratori di permettere o negare l'accesso alla chiave KMS. Per informazioni dettagliate, vedi ABAC per AWS KMS.

`kms:UntagResource`

Consente `kms:UntagResource`, per cui gli amministratori della chiave possono eliminare tag dalla chiave KMS. Poiché i tag possono essere utilizzati per controllare l'accesso alla chiave, questa autorizzazione può consentire agli amministratori di permettere o negare l'accesso alla chiave KMS. Per informazioni dettagliate, vedi ABAC per AWS KMS.

`kms:ScheduleKeyDeletion`

Consente `kms:ScheduleKeyDeletion`, per cui gli amministratori della chiave possono eliminare questa chiave KMS. Per eliminare questa autorizzazione, deseleziona l'opzione Consenti agli amministratori della chiave di eliminare questa chiave.

`kms:CancelKeyDeletion`

Consente `kms:CancelKeyDeletion`, per cui gli amministratori della chiave possono annullare l'eliminazione di questa chiave KMS. Per eliminare questa autorizzazione, deseleziona l'opzione Consenti agli amministratori della chiave di eliminare questa chiave.

AWS KMS aggiunge le seguenti autorizzazioni all'istruzione predefinita degli amministratori chiave al momento della creazione di chiavi per uso speciale.

`kms:ImportKeyMaterial`

L'autorizzazione `kms:ImportKeyMaterial` consente agli amministratori della chiave di importare il materiale chiave nella chiave KMS. Questa autorizzazione è inclusa nella policy delle chiavi solo quando crei una chiave KMS senza materiale della chiave.

`kms:ReplicateKey`

L'autorizzazione `kms:ReplicateKey` consente agli amministratori della chiave di creare una replica di una chiave primaria multi-Regione in un'altra Regione AWS. Questa autorizzazione è inclusa nella policy della chiave solo quando si crea una chiave primaria o di replica multi-Regione.

`kms:UpdatePrimaryRegion`

L'autorizzazione `kms:UpdatePrimaryRegion` consente agli amministratori della chiave di modificare una replica di una chiave multi-Regione in una chiave primaria multi-Regione. Questa

autorizzazione è inclusa nella policy della chiave solo quando si crea una chiave primaria o di replica multi-Regione.

Consente agli utenti della chiave di utilizzare la chiave KMS

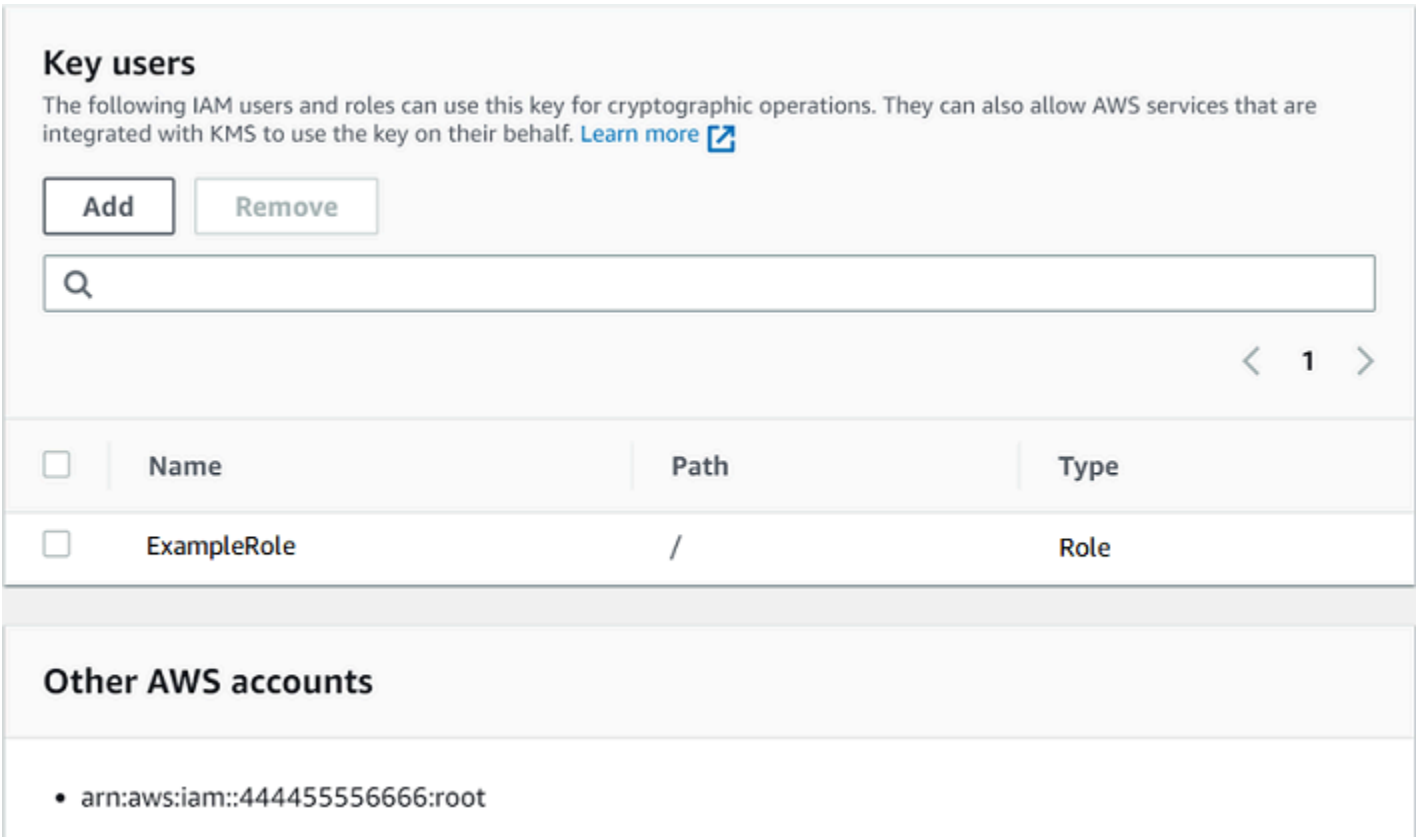
La policy della chiave predefinita creata dalla console per le chiavi KMS di crittografia simmetrica consente di scegliere gli utenti IAM e i ruoli IAM nell'account e negli Account AWS esterni e di renderli utenti della chiave.

La console aggiunge due istruzioni di policy alla policy delle chiavi per gli utenti della chiave.

- Utilizzare direttamente la chiave KMS — La prima istruzione di policy delle chiavi consente agli utenti della chiave di utilizzare la chiave KMS direttamente per tutte le operazioni di crittografia per quel tipo di chiave KMS.
- Utilizzare la chiave KMS con servizi AWS: la seconda istruzione di policy fornisce agli utenti della chiave il permesso di consentire ai servizi AWS che sono integrati con AWS KMS di utilizzare la chiave KMS per loro conto per proteggere le risorse, ad esempio i bucket di Amazon S3 e le tabelle di Amazon DynamoDB.

Puoi aggiungere utenti IAM, ruoli IAM e Account AWS esterni all'elenco degli utenti della chiave quando crei la chiave KMS. È anche possibile modificare l'elenco con la visualizzazione predefinita della console per le policy delle chiavi, come illustrato nella seguente immagine. La visualizzazione predefinita per le policy delle chiavi si trova nella pagina dei dettagli delle chiavi. Per ulteriori informazioni su come consentire agli utenti in altri Account AWS di utilizzare la chiave KMS, consulta Autorizzazione per gli utenti in altri account di utilizzare una chiave KMS.

> **Note**
>
> Le best practice di IAM disincentivano l'uso di utenti IAM con credenziali a lungo termine. Quando possibile, utilizza i ruoli IAM che forniscono credenziali temporanee. Per i dettagli, consulta la sezione Best practice di sicurezza in IAM nella Guida per l'utente IAM.



Le istruzioni degli amministratori della chiave predefinite per una chiave KMS simmetrica a Regione singola concedono le seguenti autorizzazioni. Per informazioni dettagliate su ciascuna autorizzazione, consultare AWS KMS autorizzazioni.

Quando si utilizza la console AWS KMS per creare una chiave KMS, la console aggiunge gli utenti e i ruoli specificati all'elemento `Principal` in ciascuna istruzione degli amministratori della chiave.

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {"AWS": [
    "arn:aws:iam::111122223333:role/ExampleRole",
    "arn:aws:iam::444455556666:root"
  ]},
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
```

```
  "Resource": "*"
},
{
  "Sid": "Allow attachment of persistent resources",
  "Effect": "Allow",
  "Principal": {"AWS": [
    "arn:aws:iam::111122223333:role/ExampleRole",
    "arn:aws:iam::444455556666:root"
  ]},
  "Action": [
    "kms:CreateGrant",
    "kms:ListGrants",
    "kms:RevokeGrant"
  ],
  "Resource": "*",
  "Condition": {"Bool": {"kms:GrantIsForAWSResource": true}}
}
```

Consente agli utenti della chiave di utilizzare una chiave KMS per le operazioni di crittografia

Gli utenti della chiave sono autorizzati a utilizzare direttamente la chiave KMS in tutte le operazioni di crittografia supportate nella chiave KMS. Possono inoltre utilizzare l'DescribeKeyoperazione per ottenere informazioni dettagliate sulla chiave KMS nella AWS KMS console o utilizzare le AWS KMS operazioni API.

Per impostazione predefinita, la console AWS KMS aggiunge istruzioni per gli utenti di chiave come quelle contenute negli esempi seguenti alla policy delle chiavi predefinita. Dato che supportano diverse operazioni API, le operazioni nelle istruzioni della policy per le chiavi KMS di crittografia simmetrica, le chiavi KMS HMAC, le chiavi asimmetriche per la crittografia a chiave pubblica e le chiavi KMS asimmetriche per la firma e la verifica sono leggermente diverse.

Chiavi KMS di crittografia simmetrica

La console aggiunge l'istruzione seguente alla policy della chiave per le chiavi KMS di crittografia simmetrica.

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleKeyUserRole"},
```

```
  "Action": [
    "kms:Decrypt",
    "kms:DescribeKey",
    "kms:Encrypt",
    "kms:GenerateDataKey*",
    "kms:ReEncrypt*"
  ],
  "Resource": "*"
}
```

Chiavi KMS HMAC

La console aggiunge l'istruzione seguente alla policy della chiave per le chiavi KMS HMAC.

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleKeyUserRole"},
  "Action": [
    "kms:DescribeKey",
    "kms:GenerateMac",
    "kms:VerifyMac"
  ],
  "Resource": "*"
}
```

Chiavi KMS asimmetriche per la crittografia a chiave pubblica

La console aggiunge l'istruzione seguente alla policy delle chiavi per le chiavi KMS asimmetriche con un utilizzo di chiave Encrypt and decrypt (Crittografia e decrittografia).

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleKeyUserRole"
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:DescribeKey",
    "kms:GetPublicKey"
```

```
  ],
  "Resource": "*"
}
```

Chiavi KMS asimmetriche per la firma e la verifica

La console aggiunge l'istruzione seguente alla policy delle chiavi per le chiavi KMS asimmetriche con un utilizzo di chiave Sign and verify (Firma e verifica).

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleKeyUserRole"},
  "Action": [
    "kms:DescribeKey",
    "kms:GetPublicKey",
    "kms:Sign",
    "kms:Verify"
  ],
  "Resource": "*"
}
```

Le operazioni in queste istruzioni forniscono agli utenti della chiave le autorizzazioni seguenti.

`kms:Encrypt`

Permette agli utenti della chiave di crittografare i dati con questa chiave KMS.

`kms:Decrypt`

Permette agli utenti della chiave di decrittare i dati con questa chiave KMS.

`kms:DescribeKey`

Permette agli utenti della chiave di ottenere informazioni dettagliate su questa chiave KMS, compresi gli identificatori, la data di creazione e lo stato della chiave. Consente inoltre agli utenti della chiave di visualizzare i dettagli sulla chiave KMS nella console AWS KMS.

`kms:GenerateDataKey*`

Permette agli utenti della chiave di richiedere una chiave di dati simmetrica o una coppia di chiavi di dati asimmetriche per operazioni di crittografia sul lato client. La console utilizza il carattere jolly * per rappresentare l'autorizzazione per le seguenti operazioni

API: GenerateDataKey, GenerateDataKeyWithoutPlaintextGenerateDataKeyPair, e. GenerateDataKeyPairWithoutPlaintext Queste autorizzazioni sono valide solo per le chiavi KMS di crittografia simmetrica che crittografano le chiavi di dati.

km: GenerateMac

Consente agli utenti della chiave di utilizzare una chiave KMS HMAC per generare un tag HMAC.

km: GetPublicKey

Permette agli utenti della chiave di scaricare la chiave pubblica della chiave KMS asimmetrica. Le parti con cui condividi questa chiave pubblica possono crittografare i dati al di fuori di AWS KMS. Questi testi cifrati possono essere decriptati solo chiamando l'operazione Decrypt in AWS KMS.

km: * ReEncrypt

Permette agli utenti della chiave di crittografare nuovamente i dati originariamente crittografati con questa chiave KMS o di utilizzare questa chiave KMS per ricrittografare dati crittografati in precedenza. L'ReEncryptoperazione richiede l'accesso alle chiavi KMS di origine e di destinazione. A tal fine, puoi concedere l'autorizzazione `kms:ReEncryptFrom` sulla chiave KMS di origine e l'autorizzazione `kms:ReEncryptTo` sulla chiave KMS di destinazione. Per semplicità, però, la console consente `kms:ReEncrypt*` (con il carattere jolly `*`) su entrambe le chiavi KMS.

kms:Sign

Permette agli utenti della chiave di firmare messaggi con questa chiave KMS.

kms:Verify

Permette agli utenti della chiave di verificare le firme con questa chiave KMS.

km: VerifyMac

Consente agli utenti della chiave di utilizzare una chiave KMS HMAC per verificare un tag HMAC.

Consente agli utenti della chiave di utilizzare la chiave KMS con i servizi AWS

La policy delle chiavi predefinita nella console, inoltre, concede agli utenti della chiave le autorizzazioni di cui hanno bisogno per proteggere i dati nei servizi AWS che utilizzano concessioni. I servizi AWS spesso utilizzano le concessioni per ottenere autorizzazioni specifiche e limitate per utilizzare una chiave KMS.

Questa istruzione di policy delle chiavi consente all'utente della chiave di creare, visualizzare e revocare concessioni sulla chiave KMS, ma solo quando la richiesta di operazione di concessione

proviene da un servizio AWS integrato con AWS KMS. La condizione kms: GrantIsFor AWSResource policy non consente all'utente di chiamare direttamente queste operazioni di concessione. Quando l'utente della chiave lo consente, un servizio AWS può creare una concessione per conto dell'utente che consente al servizio di utilizzare la chiave KMS per proteggere i dati dell'utente.

Gli utenti della chiave hanno bisogno di queste autorizzazioni di concessione per utilizzare la loro chiave KMS con i servizi integrati, ma queste autorizzazioni non sono sufficienti. Gli utenti della chiave hanno bisogno dell'autorizzazione anche per utilizzare i servizi integrati. Per ulteriori informazioni su come garantire agli utenti l'accesso a un servizio AWS che si integra con AWS KMS, consulta la documentazione relativa al servizio integrato.

```
{
  "Sid": "Allow attachment of persistent resources",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleKeyUserRole"},
  "Action": [
    "kms:CreateGrant",
    "kms:ListGrants",
    "kms:RevokeGrant"
  ],
  "Resource": "*",
  "Condition": {"Bool": {"kms:GrantIsForAWSResource": true}}
}
```

Ad esempio, gli utenti della chiave possono utilizzare queste autorizzazioni sulla chiave KMS nei modi seguenti.

- Utilizza questa chiave KMS con Amazon Elastic Block Store (Amazon EBS) e Amazon Elastic Compute Cloud (Amazon EC2) per allegare un volume EBS crittografato a un'istanza EC2. L'utente della chiave offre implicitamente a Amazon EC2 l'autorizzazione a utilizzare la chiave KMS per collegare il volume crittografato all'istanza. Per ulteriori informazioni, consultare Come Amazon Elastic Block Store (Amazon EBS) usa AWS KMS.
- Utilizza questa chiave KMS con Amazon Redshift per avviare un cluster crittografato. L'utente della chiave offre implicitamente a Amazon Redshift l'autorizzazione a utilizzare la chiave KMS per avviare il cluster crittografato e creare snapshot crittografate. Per ulteriori informazioni, consultare Come Amazon Redshift utilizza AWS KMS.
- Utilizzare questa chiave KMS con altri servizi AWS integrati con AWS KMS che utilizzano concessioni per creare, gestire o utilizzare le risorse crittografate con quei servizi.

La policy delle chiavi predefinita consente agli utenti della chiave di delegare l'autorizzazione di concessione a tutti i servizi integrati che utilizzano le concessioni. È tuttavia possibile creare una policy delle chiavi personalizzata che limita l'autorizzazione ai servizi AWSspecificati. Per ulteriori informazioni, consulta la chiave di condizione km: ViaService.

Visualizzazione di una policy di chiave

Puoi visualizzare la politica delle chiavi per una chiave gestita dal AWS KMS cliente o Chiave gestita da AWSnel tuo account utilizzando AWS Management Console o l'GetKeyPolicyoperazione nell'AWS KMSAPI. Non è possibile utilizzare queste tecniche per visualizzare la policy delle chiavi di una chiave KMS in un Account AWS diverso.

Per ulteriori informazioni sulle policy delle chiavi AWS KMS consulta Policy delle chiavi in AWS KMS. Per informazioni su come determinare quali utenti e ruoli hanno accesso a una chiave KMS, consulta the section called “Determinazione dell'accesso”.

Argomenti

- Visualizzazione di una policy delle chiavi (console)
- Visualizzazione di una policy delle chiavi (API AWS KMS)

Visualizzazione di una policy delle chiavi (console)

Gli utenti autorizzati possono visualizzare la policy delle chiavi per unaChiave gestita da AWS o una chiave gestita dal cliente nella scheda Key policy (Policy delle chiavi) della AWS Management Console.

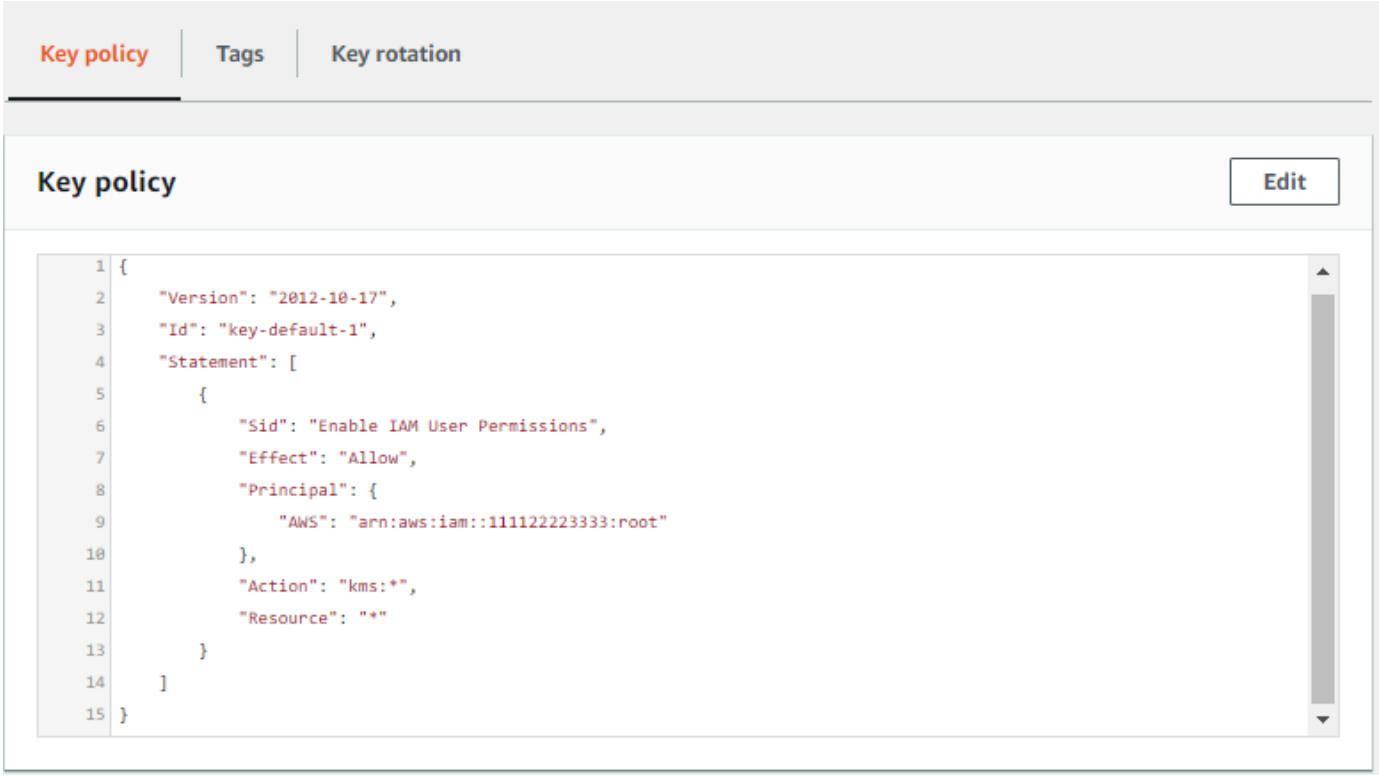
Per visualizzare la politica chiave per una chiave KMS inAWS Management Console, devi disporre delle autorizzazioni kms: ListAliases, kms: DescribeKey e kms:. GetKeyPolicy

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Per visualizzare le chiavi nell'account creato e gestito per te da AWS, nel riquadro di navigazione, seleziona chiavi gestite AWS. Per visualizzare le chiavi nell'account creato e gestito dall'utente, nel riquadro di navigazione, seleziona Chiavi gestite dal cliente.

4. Nell'elenco di chiavi KMS, scegliere l'alias o l'ID chiave della chiave KMS che si intende esaminare.
5. Scegli la scheda Policy della chiave.

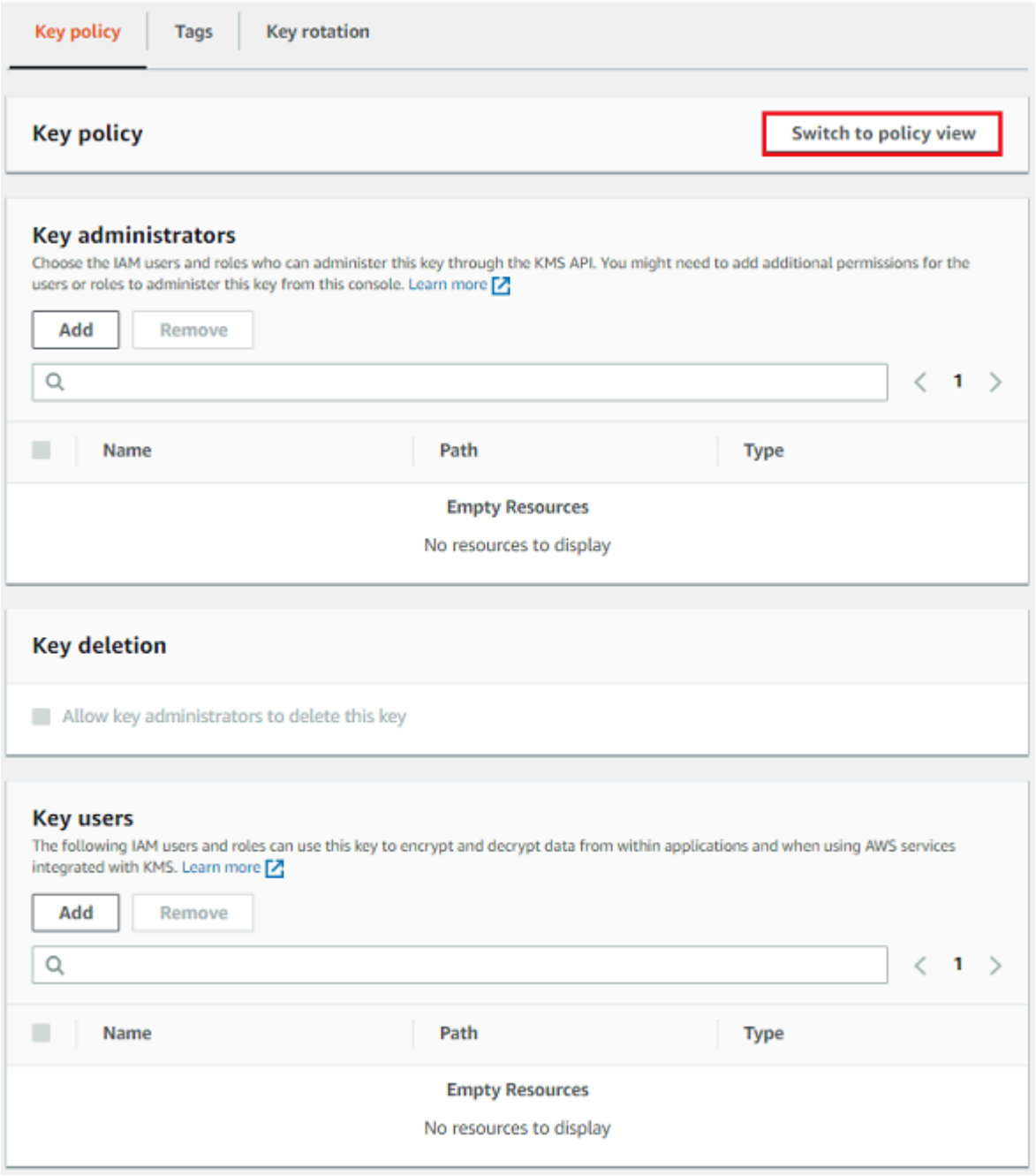
   Nella tab Policy chiave è possibile che venga visualizzato il documento della policy delle chiavi. Si tratta della visualizzazione policy. Nelle istruzioni della policy delle chiavi è possibile visualizzare i principali a cui la policy ha concesso l'accesso alla chiave KMS e le operazioni che tali entità possono eseguire.

   Nell'esempio seguente viene illustrata la visualizzazione policy per la policy di chiave predefinita.



   Se invece la chiave KMS è stata creata nella AWS Management Console, verrà visualizzata la visualizzazione predefinita con le sezioni per Amministratori della chiave, Eliminazione della chiave e Utenti della chiave. Per visualizzare il documento di policy delle chiavi, scegliere Switch to policy view (Passa alla visualizzazione policy).

   Nell'esempio seguente viene illustrata la visualizzazione predefinita per la policy di chiave predefinita.



Visualizzazione di una policy delle chiavi (API AWS KMS)

Per ottenere la politica chiave per una chiave KMS nel tuoAccount AWS, usa l'operazione nell'API. GetKeyPolicyAWS KMS Non è possibile utilizzare questa operazione per visualizzare una policy di chiave in un account diverso.

L'esempio seguente utilizza il get-key-policycomando contenuto in AWS Command Line Interface (AWS CLI), ma puoi utilizzare qualsiasi AWS SDK per effettuare questa richiesta.

Il parametro `PolicyName` è obbligatorio, anche se l'unico valore valido è `default`. Inoltre, questo comando richiede l'output nel testo, anziché in JSON, per rendere la visualizzazione più semplice.

Prima di eseguire questo comando, sostituisci l'ID chiave di esempio con un ID valido dell'account.

```
$ aws kms get-key-policy --key-id 1234abcd-12ab-34cd-56ef-1234567890ab --policy-name
 default --output text
```

La risposta deve essere simile a quella seguente, che restituisce la policy di chiave predefinita.

```
{
  "Version" : "2012-10-17",
  "Id" : "key-consolepolicy-3",
  "Statement" : [ {
    "Sid" : "Enable IAM User Permissions",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "arn:aws:iam::111122223333:root"
    },
    "Action" : "kms:*",
    "Resource" : "*"
  } ]
}
```

Modifica di una policy delle chiavi

Puoi modificare la politica chiave per una chiave KMS nel tuo Account AWS utilizzando l'PutKeyPolicyoperazione AWS Management Console o. Non è possibile utilizzare queste tecniche per modificare la policy delle chiavi di una chiave KMS in un Account AWS diverso.

Quando modifichi una policy delle chiavi, ricorda le seguenti regole:

- Puoi visualizzare la policy delle chiavi per una Chiave gestita da AWS o per una chiave gestita dal cliente, ma puoi modificare la policy delle chiavi solo per una chiave gestita dal cliente. Le policy delle Chiavi gestite da AWS vengono create e gestite dal servizio AWS che ha creato la chiave KMS nel tuo account. Non puoi visualizzare o modificare la policy delle chiavi per una Chiave di proprietà di AWS.
- È possibile aggiungere o rimuovere utenti IAM, ruoli IAM e Account AWS nella policy delle chiavi e modificare le operazioni consentite o non consentite per quei principali. Per ulteriori informazioni

sui metodi per specificare principali e autorizzazioni in una policy delle chiavi, consulta Policy delle chiavi.

- Non puoi aggiungere gruppi IAM a una policy delle chiavi, ma puoi aggiungere più utenti IAM e ruoli IAM. Per ulteriori informazioni, consulta Autorizzazione per più principali IAM di accedere a una chiave KMS.
- Se aggiungi Account AWS esterni a una policy delle chiavi, devi anche utilizzare le policy IAM negli account esterni per fornire autorizzazioni agli utenti, ai gruppi o ai ruoli IAM in tali account. Per ulteriori informazioni, consulta Autorizzazione per gli utenti in altri account di utilizzare una chiave KMS.
- Il documento di policy delle chiavi risultante non può superare i 32 KB (32.768 byte).

Argomenti

Come modificare una policy delle chiavi

Puoi modificare una policy chiavi in tre diversi modi, ognuno dei quali è illustrato nelle seguenti sezioni.

Argomenti

Utilizzo della visualizzazione predefinita della AWS Management Console

Puoi utilizzare la console per modificare una policy delle chiavi mediante un'interfaccia grafica denominata visualizzazione predefinita.

Se le procedure seguenti non corrispondono a ciò che viene visualizzato nella console, è possibile che questa policy delle chiavi non sia stata creata con la console oppure che sia stata modificata in un modo non supportato dalla visualizzazione predefinita della console. In questo caso, segui i passaggi descritti in Utilizzo della visualizzazione policy della AWS Management Console o Uso dell'API AWS KMS.

1. Visualizza la policy delle chiavi per una chiave gestita dal cliente come descritto in Visualizzazione di una policy delle chiavi (console). (Non è possibile modificare la policy delle chiavi di Chiavi gestite da AWS.)
2. Decidere cosa modificare.

   - Per aggiungere o rimuovere amministratori delle chiavi e per consentire o impedire agli amministratori di eliminare la chiave KMS, utilizza i controlli nella sezione Key Administrators della pagina. Gli amministratori delle chiavi gestiscono la chiave KMS, possono abilitare e disabilitare la stessa, impostare la policy delle chiavi e abilitare la rotazione delle chiavi.
   - Per aggiungere o rimuovere utenti della chiave e per consentire o non consentire ai Account AWS esterni di utilizzare la chiave KMS, utilizza i controlli nella sezione Utenti della chiave della pagina. Gli utenti della chiave possono utilizzare la chiave KMS nelle operazioni di crittografia, ad esempio crittografia, decrittografia, ricrittografia e generazione di chiavi di dati.

Utilizzo della visualizzazione policy della AWS Management Console

Puoi utilizzare la console per modificare un documento di policy delle chiavi mediante la visualizzazione policy della console.

1. Visualizza la policy delle chiavi per una chiave gestita dal cliente come descritto in Visualizzazione di una policy delle chiavi (console). (Non è possibile modificare la policy delle chiavi di Chiavi gestite da AWS.)
2. Nella sezione Policy della chiave, scegli Passa alla visualizzazione della policy.
3. Modificare il documento di policy delle chiavi, quindi scegliere Save changes (Salva le modifiche).

Uso dell'API AWS KMS

Puoi utilizzare l'PutKeyPolicyoperazione per modificare la politica chiave di una chiave KMS nel tuo. Account AWS Non è possibile utilizzare questa API per una chiave KMS in un Account AWS differente.

1. Utilizza l'GetKeyPolicyoperazione per ottenere il documento di politica chiave esistente, quindi salva il documento di politica chiave in un file. Per il codice di esempio in più linguaggi di programmazione, consulta Recupero di una policy delle chiavi.
2. Aprire il documento di policy delle chiavi in un editor di testo, modificarlo e salvare il file.

3. Utilizza l'PutKeyPolicyoperazione per applicare il documento di policy chiave aggiornato alla chiave KMS. Per il codice di esempio in più linguaggi di programmazione, consulta Impostazione di una policy delle chiavi.

Per un esempio di copia di una politica chiave da una chiave KMS a un'altra, vedi l'GetKeyPolicy esempio nel Command Reference. AWS CLI

Autorizzazione per più principali IAM di accedere a una chiave KMS

I gruppi IAM non sono principali validi in una policy chiave. Per consentire a più utenti e ruoli di accedere a una chiave KMS, procedi in uno dei seguenti modi:

- Usa un ruolo IAM come principale nella policy delle chiavi. Più utenti autorizzati possono assumere il ruolo secondo necessità. Per i dettagli, consulta Ruoli IAM nella Guida per l'utente IAM.

  Sebbene sia possibile collegare più utenti IAM in una policy delle chiavi, questa procedura non è consigliata perché richiede l'aggiornamento della policy delle chiavi ogni volta che l'elenco di utenti autorizzati viene modificato. Inoltre, le best practice di IAM disincentivano l'uso di utenti IAM con credenziali a lungo termine. Per i dettagli, consulta la sezione Best practice di sicurezza in IAM nella Guida per l'utente IAM.
- Utilizza una policy IAM per collegare l'autorizzazione a un gruppo IAM. Per fare ciò, assicurati che la policy delle chiavi includa la dichiarazione che consente alle policy IAM di consentire l'accesso alla chiave KMS, crea una policy IAM che consenta l'accesso alla chiave KMS e quindi collega tale policy a un gruppo IAM che contenga gli utenti IAM autorizzati. L'utilizzo di questo approccio non richiede l'aggiornamento di policy quando l'elenco degli utenti autorizzati viene modificato. È sufficiente aggiungere o rimuovere tali utenti dal gruppo IAM appropriato. Per i dettagli, consulta la sezione Gruppi di utenti IAM nella Guida per l'utente IAM

Per ulteriori informazioni sull'utilizzo congiunto delle policy delle chiavi AWS KMS e delle policy IAM, consulta Risoluzione dei problemi di accesso alla chiave.

Autorizzazioni per i servizi AWS nelle policy delle chiavi

Molti servizi AWS utilizzano AWS KMS keys per proteggere le risorse che gestiscono. Quando un servizio utilizza Chiavi di proprietà di AWS o Chiavi gestite da AWS, il servizio stabilisce e mantiene le policy della chiave per queste chiavi KMS.

Tuttavia, quando si utilizza una chiave gestita dal cliente con un servizio AWS, è l'utente che imposta e mantiene la policy della chiave. Tale policy della chiave deve concedere al servizio le autorizzazioni minime necessarie per proteggere la risorsa per conto dell'utente. Si consiglia di seguire il principio del privilegio minimo: concedere al servizio soltanto le autorizzazioni necessarie. È possibile farlo in modo efficace scoprendo di quali autorizzazioni il servizio ha bisogno e utilizzando le chiavi di condizione globali AWS e le chiavi di condizione AWS KMS per perfezionare le autorizzazioni.

Per trovare le autorizzazioni richieste dal servizio su una chiave gestita dal cliente, consultare la documentazione di crittografia per il servizio. Ad esempio, per le autorizzazioni richieste da Amazon Elastic Block Store (Amazon EBS), consultare Autorizzazioni per gli utenti IAM nella Guida per l'utente di Amazon EC2 per le istanze Linux e nella Guida per l'utente di Amazon EC2 per le istanze Windows. Per le autorizzazioni richieste da Secrets Manager, consultare Autorizzazione dell'uso della chiave KMS nella Guida per l'utente di AWS Secrets Manager.

Implementazione di autorizzazioni con privilegio minimo

Quando si concede a un servizio AWS l'autorizzazione di utilizzare una chiave KMS, assicurarsi che l'autorizzazione sia valida solo per le risorse a cui il servizio deve accedere per conto dell'utente. Questa strategia del privilegio minimo aiuta a prevenire l'uso non autorizzato di una chiave KMS quando le richieste passano tra servizi AWS diversi.

Per implementare una strategia del privilegio minimo, si consiglia di utilizzare le chiavi di condizione del contesto di crittografia AWS KMS e l'ARN di origine globale o le chiavi di condizione dell'account di origine.

Utilizzo delle chiavi di condizione del contesto di crittografia

Il modo più efficace per implementare autorizzazioni con privilegi minimi durante l'utilizzo delle risorse AWS KMS è includere le chiavi di condizione kms:EncryptionContext:context-key o kms:EncryptionContextKeys nella policy che permette ai principali di chiamare le operazioni di crittografia di AWS KMS. Queste chiavi di condizione sono particolarmente efficaci perché associano l'autorizzazione al contesto di crittografia che è legato al testo criptato quando la risorsa è crittografata.

Utilizza le chiavi delle condizioni del contesto di crittografia solo quando l'azione nella dichiarazione politica è CreateGranto un'operazione crittografica AWS KMS simmetrica che accetta un `EncryptionContext` parametro, come operazioni come Decrypt o Decrypt. GenerateDataKey (Per un elenco delle operazioni supportate, consultare kms:EncryptionContext:context-key o kms:EncryptionContextKeys). Se si utilizzano queste chiavi di condizione per consentire altre operazioni, ad esempio, l'autorizzazione verrà negata DescribeKey.

Impostare il valore sul contesto di crittografia utilizzato dal servizio quando crittografa la risorsa. Queste informazioni sono generalmente disponibili nel capitolo Sicurezza della documentazione del servizio. Ad esempio, il contesto di crittografia di AWS Proton identifica la risorsa AWS Proton e il relativo modello associato. Il contesto di crittografia di AWS Secrets Manager identifica il segreto e la sua versione. Il contesto di crittografia per Amazon Location identifica la localizzazione o la raccolta.

Il seguente esempio di istruzione della chiave delle policy permette ad Amazon Location Service di creare concessioni per conto di utenti autorizzati. Questa informativa limita l'autorizzazione utilizzando le chiavi kms: ViaService, kms: CallerAccount e `kms:EncryptionContext:`*`context-key`* condition per legare l'autorizzazione a una particolare risorsa tracker.

```
{
  "Sid": "Allow Amazon Location to create grants on behalf of authorized users",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/LocationTeam"
  },
  "Action": "kms:CreateGrant",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ViaService": "geo.us-west-2.amazonaws.com",
      "kms:CallerAccount": "111122223333",
      "kms:EncryptionContext:aws:geo:arn": "arn:aws:geo:us-west-2:111122223333:tracker/
SAMPLE-Tracker"
    }
  }
}
```

Utilizzo delle chiavi di condizione **`aws:SourceArn`** o **`aws:SourceAccount`**

Quando il principale in un'istruzione della policy della chiave è un principale del servizio AWS, consigliamo vivamente di utilizzare le chiavi di condizione globale aws:SourceArn o aws:SourceAccount oltre alla chiave di condizione `kms:EncryptionContext:`*`context-key`*. I valori dell'ARN e dell'account sono inclusi nel contesto di autorizzazione solo quando una richiesta arriva a AWS KMS da un altro servizio AWS. Questa combinazione di condizioni implementa autorizzazioni meno privilegiate ed evita un potenziale scenario "confused deputy". I principali del servizio in genere non vengono utilizzati come principali in una policy della chiave, ma alcuni servizi AWS, come ad esempio AWS CloudTrail, lo richiedono.

Per utilizzare le chiavi di condizione globali `aws:SourceArn` o `aws:SourceAccount`, impostare il valore sul nome della risorsa Amazon (ARN) o sull'account della risorsa crittografata. Ad esempio, nell'istruzione di una policy della chiave che fornisce l'autorizzazione AWS CloudTrail per crittografare un percorso, impostare sull'ARN del percorso il valore di `aws:SourceArn`. Quando possibile, utilizzare `aws:SourceArn`, che è più specifico. Impostare il valore sull'ARN o un modello ARN con caratteri jolly. Se non si conosce l'ARN della risorsa, utilizzare `aws:SourceAccount`.

> **Note**
>
> Se una risorsa ARN include caratteri non consentiti in una policy della chiave AWS KMS, non puoi utilizzare tale risorsa ARN nel valore della chiave di condizione `aws:SourceArn`. Devi invece utilizzare la chiave di condizione `aws:SourceAccount`. Per maggiori informazioni sulle regole delineate nel documento delle policy delle chiavi, consulta la sezione Formato della policy della chiave.

Nell'esempio seguente di policy della chiave, il principale che ottiene le autorizzazioni è il principale del servizio AWS CloudTrail, `cloudtrail.amazonaws.com`. Per implementare il privilegio minimo, questa policy utilizza le chiavi di condizione `aws:SourceArn` e `kms:EncryptionContext:`*`context-key`*. L'informativa consente di CloudTrail utilizzare la chiave KMS per generare la chiave dati che utilizza per crittografare un trail. Le condizioni `aws:SourceArn` e `kms:EncryptionContext:`*`context-key`* sono valutate in modo indipendente. Qualsiasi richiesta di utilizzare la chiave KMS per l'operazione specificata deve soddisfare entrambe le condizioni.

Per limitare l'autorizzazione del servizio al percorso `finance` nell'account di esempio (111122223333) e nella Regione `us-west-2`, questa istruzione di policy definisce la condizione della chiave `aws:SourceArn` per l'ARN di un particolare percorso. L'istruzione condition utilizza l'ArnEqualsoperatore per garantire che ogni elemento dell'ARN venga valutato indipendentemente durante la corrispondenza. L'esempio utilizza anche la chiave di condizione `kms:EncryptionContext:`*`context-key`* per limitare l'autorizzazione ai percorsi in un determinato account e Regione.

Prima di utilizzare questa policy della chiave, è necessario sostituire l'ID dell'account, la Regione e il nome del percorso di esempio con valori validi riferiti al proprio account.

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Sid": "Allow CloudTrail to encrypt logs",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "kms:GenerateDataKey",
      "Resource": "*",
      "Condition": {
        "ArnEquals": {
          "aws:SourceArn": [
            "arn:aws:cloudtrail:us-west-2:111122223333:trail/finance"
          ]
        },
        "StringLike": {
          "kms:EncryptionContext:aws:cloudtrail:arn": [
            "arn:aws:cloudtrail:*:111122223333:trail/*"
          ]
        }
      }
    }
  ]
}
```

Utilizzo delle policy IAM con AWS KMS

Puoi utilizzare le policy IAM, insieme a policy chiave, concessioni e policy di endpoint VPC, per controllare l'accesso alle AWS KMS keys in AWS KMS.

> **Note**
>
> Per utilizzare una policy IAM per controllare l'accesso a una chiave KMS, la policy chiave per la chiave KMS deve concedere all'account l'autorizzazione all'utilizzo delle policy IAM. In particolare, la policy chiave deve includere l'istruzione di policy che abilita le policy IAM.
> In questa sezione viene illustrato come utilizzare le policy IAM per controllare l'accesso alle operazioni AWS KMS. Per informazioni più generiche su IAM, consulta la Guida per l'utente di IAM.

Tutte le chiavi KMS devono disporre di una policy chiave. Le policy IAM sono facoltativi. Per utilizzare una policy IAM per controllare l'accesso a una chiave KMS, la policy chiave per la chiave KMS deve concedere all'account l'autorizzazione all'utilizzo delle policy IAM. In particolare, la policy chiave deve includere l'istruzione di policy che abilita le policy IAM.

Le policy IAM possono controllare l'accesso a qualsiasi operazione AWS KMS. A differenza delle policy chiave, le policy IAM possono controllare l'accesso a più chiavi KMS e fornire autorizzazioni per le operazioni di diversi servizi AWS correlati. Ma le policy IAM sono particolarmente utili per controllare l'accesso alle operazioni CreateKey, ad esempio quelle che non possono essere controllate da una policy chiave perché non coinvolgono alcuna chiave KMS particolare.

Se si accede a AWS KMS tramite un endpoint Amazon Virtual Private Cloud (Amazon VPC), è inoltre possibile utilizzare una policy di endpoint VPC per limitare l'accesso alle risorse AWS KMS quando si utilizza l'endpoint. Ad esempio, quando si utilizza l'endpoint VPC, è possibile consentire solo alle entità principali nell'Account AWS di accedere alle chiavi gestite dal cliente. Per informazioni dettagliate, vedi Controllo dell'accesso all'endpoint VPC.

Per informazioni sulla scrittura e sulla formattazione di un documento di policy JSON, consulta la Documentazione di riferimento sulla policy IAM JSON nella Guida per l'utente di IAM.

Argomenti

Panoramica delle policy IAM

Puoi utilizzare policy IAM nei seguenti modi:

- Allegare una policy di autorizzazioni a un ruolo per la federazione o le autorizzazioni tra più account – Puoi collegare una policy IAM a un ruolo IAM per abilitare la federazione delle identità, consentire autorizzazioni tra più account o concedere autorizzazioni ad applicazioni eseguite su istanze EC2. Per ulteriori informazioni sui vari casi d'uso per i ruoli IAM, consulta Ruoli IAM nella Guida per l'utente di IAM.

- Allegare una policy di autorizzazioni a un utente o a un gruppo – Puoi collegare una policy che consente a un utente o a un gruppo di utenti di richiamare operazioni AWS KMS. Tuttavia, le best practice IAM consigliano di utilizzare identità con credenziali temporanee, come i ruoli IAM, quando possibile.

Di seguito viene illustrato un esempio di policy IAM con autorizzazioni AWS KMS. Questa policy consente alle identità IAM a cui è collegata di ottenere tutte le chiavi KMS e gli alias.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:ListKeys",
      "kms:ListAliases"
    ],
    "Resource": "*"
  }
}
```

Come tutte le policy IAM, questa policy non ha un elemento `Principal`. Quando colleghi una policy IAM a un'identità IAM, tale identità ottiene le autorizzazioni specificate nella policy.

Per una tabella che mostra tutte le operazioni API di AWS KMS e le risorse a cui si applicano, consulta la Riferimento per le autorizzazioni.

Best practice per le policy IAM

Rendere sicuro l'accesso alle AWS KMS keys è fondamentale per la sicurezza di tutte le risorse AWS. Le chiavi KMS vengono utilizzate per proteggere molte risorse sensibili nell'Account AWS. Prenditi il tempo necessario per progettare le policy chiave, le policy IAM, le concessioni e le policy degli endpoint VPC che controllano l'accesso alle chiavi KMS.

Nelle istruzioni delle policy IAM che controllano l'accesso alle chiavi KMS, utilizza il principio del privilegio minimo. Assegna ai principali IAM solo le autorizzazioni necessarie solo per quelle chiavi KMS che devono utilizzare o gestire.

Le seguenti best practice si applicano alle policy IAM che controllano l'accesso alle chiavi AWS KMS e agli alias. Per una guida generale alle best practice delle policy IAM, consulta la sezione Best practice di sicurezza in IAM nella Guida per l'utente IAM.

Utilizzo delle policy delle chiavi

Quando possibile, concedi le autorizzazioni nelle policy chiave che interessano una chiave KMS anziché in una policy IAM applicabile a molte chiavi KMS, incluse quelle di altri Account AWS. Ciò è particolarmente importante per le autorizzazioni sensibili come kms: PutKeyPolicy e kms: ScheduleKeyDeletion ma anche per le operazioni crittografiche che determinano la protezione dei dati.

CreateKey Limita le autorizzazioni

Concedi il permesso di creare chiavi (kms: CreateKey) solo ai principali che ne hanno bisogno. I principali che creano una chiave KMS impostano anche le policy delle chiavi, in modo che possano concedere a se stessi e agli altri l'autorizzazione per utilizzare e gestire le chiavi KMS che creano. Quando concedi questa autorizzazione, è consigliabile limitarla utilizzando le condizioni delle policy. Ad esempio, puoi utilizzare la KeySpec condizione kms: per limitare l'autorizzazione alle chiavi KMS di crittografia simmetrica.

Specificare le chiavi KMS in una policy IAM

Come best practice, specifica l'ARN di chiave di ciascuna chiave KMS a cui si applica l'autorizzazione nell'elemento `Resource` dell'istruzione della policy. Questa procedura limita l'autorizzazione per le chiavi KMS a quella richiesta dal principale. Ad esempio, questo elemento `Resource` elenca solo le chiavi KMS che il principale deve utilizzare.

```
"Resource": [
    "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321"
]
```

Se non è possibile specificare le chiavi KMS, utilizza un valore `Resource` che limita l'accesso alle chiavi KMS in un Account AWS e in una Regione attendibili, ad esempio `arn:aws:kms:`*`region`*`:`*`account`*`:key/*`. In alternativa, limita l'accesso alle chiavi KMS a tutte le Regioni (*) di un Account AWS attendibile, ad esempio `arn:aws:kms:*:`*`account`*`:key/*`.

Non puoi utilizzare un ID chiave, un nome aliaso l'ARN dell'alias per rappresentare una chiave KMS nel campo `Resource` di una policy IAM. Se si specifica un alias ARN, la policy si applica all'alias e non alla chiave KMS. Per informazioni generali sulle policy IAM, consulta Controllo dell'accesso agli alias.

Evita "Resource": "*" in una policy IAM

Utilizza i caratteri jolly (*) in modo giudizioso. In una policy delle chiavi, il carattere jolly nell'elemento `Resource` rappresenta la chiave KMS a cui è collegata la policy delle chiavi. Tuttavia, in una policy IAM, il carattere jolly da solo nell'elemento `Resource` (`"Resource": "*"`) applica le autorizzazioni a tutte le chiavi KMS in tutti gli account Account AWS che l'account del principale dispone dell'autorizzazione a utilizzare. Ciò potrebbe includere le chiavi KMS in altri Account AWS, nonché le chiavi KMS nell'account del principale.

Ad esempio, per utilizzare una chiave KMS in un altro Account AWS, un principale richiede l'autorizzazione dalla policy chiave della chiave KMS nell'account esterno e da una policy IAM nel proprio account. Supponiamo che un account arbitrario ti abbia concesso l'autorizzazione Account AWS kms:Decrypt sulle sue chiavi KMS. In tal caso, una policy IAM nell'account che concede a un ruolo l'autorizzazione `kms:Decrypt` per tutte le chiavi KMS (`"Resource": "*"`) soddisferebbe la parte IAM del requisito. Di conseguenza, i principali che possono assumere tale ruolo possono ora decrittare i testi cifrati utilizzando la chiave KMS nell'account non attendibile. Le voci relative alle loro operazioni vengono visualizzate nei CloudTrail registri di entrambi gli account.

In particolare, evita di utilizzare `"Resource": "*"` in un'istruzione della policy che consente le seguenti operazioni API. Queste operazioni possono essere chiamate nelle chiavi KMS di altri Account AWS.

- DescribeKey
- GetKeyRotationStatus
- Operazioni crittografiche (Encrypt, Decrypt,,,,,, GenerateDataKey, GenerateDataKeyPair, GenerateDataKeyWithoutPlaintextSign GenerateDataKeyPairWithoutPlaintextGetPublicKey, ReEncryptVerify)
- CreateGrant, ListGrants, ListRetirableGrants, RetireGrant, RevokeGrant

Quando utilizzare "Resource": "*"

In una policy IAM usi un carattere jolly nell'elemento `Resource` solo per le autorizzazioni che lo richiedono. Solo le seguenti autorizzazioni richiedono l'elemento `"Resource": "*"`.

- km: CreateKey
- km: GenerateRandom
- km: ListAliases
- km: ListKeys

- Autorizzazioni per archivi di chiavi personalizzati, come kms: CreateCustomKeyStore e kms:. ConnectCustomKeyStore

> **Note**
>
> Le autorizzazioni per le operazioni con alias (kms:CreateAlias, kms:, kms: UpdateAlias DeleteAlias) devono essere allegate all'alias e alla chiave KMS. Puoi utilizzare `"Resource": "*"` in una policy IAM per rappresentare gli alias e le chiavi KMS oppure per specificare gli alias e le chiavi KMS nell'elemento `Resource`. Per alcuni esempi, consulta Controllo dell'accesso agli alias.

Negli esempi riportati in questo argomento vengono fornite ulteriori informazioni e indicazioni per la progettazione di policy IAM per le chiavi KMS. Per indicazioni e best practice generali su AWS KMS, consultare Best practice su AWS Key Management Service (PDF). Per le best practice su IAM per tutte le risorse AWS, consulta Best practice sulla sicurezza in IAM nella Guida per l'utente di IAM.

Specificazione delle chiavi KMS nelle istruzioni della policy IAM

Puoi utilizzare una policy IAM per consentire a un principale di utilizzare o gestire le chiavi KMS. Le chiavi KMS sono specificate nell'elemento `Resource` dell'istruzione della policy.

- Per specificare una chiave KMS in un'istruzione delle policy IAM, devi utilizzare l'ARN della chiave. Non è possibile utilizzare un ID chiave, un nome alias o l'ARN di alias per identificare una chiave KMS in un'istruzione della policy IAM.

  Ad esempio: `"Resource": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"`

  Per controllare l'accesso a una chiave KMS in base ai relativi alias, usa le chiavi di condizione kms: o kms:. RequestAlias ResourceAliases Per informazioni dettagliate, vedi ABAC per AWS KMS.

  Utilizzate un alias ARN come risorsa solo in una dichiarazione di policy che controlla l'accesso alle operazioni di alias, ad esempio CreateAlias, o. UpdateAliasDeleteAlias Per informazioni dettagliate, vedi Controllo dell'accesso agli alias.
- Per specificare più chiavi KMS nell'account e nella regione, utilizza i caratteri jolly (*) nelle posizioni dell'ID risorsa e della regione dell'ARN di chiave.

Ad esempio, per specificare tutte le chiavi KMS nella Regione Stati Uniti occidentali (Oregon) di un account, utilizza `"Resource": "arn:aws:kms:us-west-2:111122223333:key/*"`. Per specificare tutte le chiavi KMS in tutte le Regioni dell'account, utilizza `"Resource": "arn:aws:kms:*:111122223333:key/*"`.

- Per rappresentare tutte le chiavi KMS, utilizza solo un carattere jolly (`"*"`). Utilizza questo formato per operazioni che non utilizzano alcuna chiave KMS particolare, vale a dire CreateKey, GenerateRandome. ListAliasesListKeys

Quando scrivi le istruzioni delle policy, come best practice è consigliabile limitare le chiavi KMS a quelle che i principali devono utilizzare, anziché concedere loro l'accesso a tutte le chiavi KMS.

Ad esempio, la seguente dichiarazione di policy IAM consente al principale di richiamare le operazioni DescribeKeyGenerateDataKey,, Decrypt solo sulle chiavi KMS elencate nell'`Resource`elemento dell'informativa politica. La specifica delle chiavi KMS in base all'ARN della chiave, che è una best practice, garantisce che le autorizzazioni siano limitate solo alle chiavi KMS indicate.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:DescribeKey",
      "kms:GenerateDataKey",
      "kms:Decrypt"
    ],
    "Resource": [
      "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321"
    ]
  }
}
```

Per applicare l'autorizzazione a tutte le chiavi KMS in un determinato Account AWS attendibile, puoi utilizzare i caratteri jolly (*) nelle posizioni della Regione e dell'ID chiave. Ad esempio, la seguente istruzione di policy consente al principale di richiamare le operazioni specificate in tutte le chiavi KMS in due account di esempio attendibili.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:DescribeKey",
      "kms:GenerateDataKey",
      "kms:GenerateDataKeyPair"
    ],
    "Resource": [
      "arn:aws:kms:*:111122223333:key/*",
      "arn:aws:kms:*:444455556666:key/*"
    ]
  }
}
```

Inoltre puoi utilizzare un carattere jolly (`"*"`) da solo nell'elemento `Resource`. Poiché consente l'accesso a tutte le chiavi KMS che l'account ha l'autorizzazione di utilizzare, è consigliato principalmente per le operazioni senza una particolare chiave KMS e per le istruzioni `Deny`. Puoi inoltre utilizzarlo nelle istruzioni di policy che consentono esclusivamente operazioni di sola lettura meno sensibili. Per determinare se un'operazione AWS KMS coinvolge una particolare chiave KMS, cerca il valore Chiave KMS nella colonna Risorse della tabella in the section called “Riferimento per le autorizzazioni”.

Ad esempio, l'istruzione di policy riportata di seguito utilizza un effetto `Deny` per impedire ai principali di utilizzare le operazioni specificate per qualsiasi chiave KMS. Viene utilizzato un carattere jolly nell'elemento `Resource` per rappresentare tutte le chiavi KMS.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": [
      "kms:CreateKey",
      "kms:PutKeyPolicy",
      "kms:CreateGrant",
      "kms:ScheduleKeyDeletion"
    ],
    "Resource": "*"
  }
}
```

Nell'istruzione di policy seguente viene utilizzato un carattere jolly da solo per rappresentare tutte le chiavi KMS. Tuttavia consente solo operazioni di sola lettura meno sensibili e operazioni che non si applicano a nessuna particolare chiave KMS.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:CreateKey",
      "kms:ListKeys",
      "kms:ListAliases",
      "kms:ListResourceTags"
    ],
    "Resource": "*"
  }
}
```

Autorizzazioni necessarie per l'uso della console AWS KMS

Per utilizzare la console AWS KMS, gli utenti devono disporre di un set di autorizzazioni minimo che gli consenta di utilizzare le risorse AWS KMS nel loro Account AWS. Oltre a queste autorizzazioni AWS KMS, gli utenti devono disporre delle autorizzazioni per elencare gli utenti IAM e i ruoli IAM. Se decidi di creare una policy IAM più restrittiva delle autorizzazioni minime richieste, la console AWS KMS non funzionerà come previsto per gli utenti con tale policy IAM.

Per le autorizzazioni minime necessarie per consentire a un utente l'accesso in sola lettura alla console AWS KMS, consulta Consentire a un utente di visualizzare le chiavi KMS nella console AWS KMS.

Per consentire agli utenti di utilizzare la AWS KMS console per creare e gestire le chiavi KMS, allega la policy AWSKeyManagementServicePowerUsergestita all'utente, come descritto nella sezione seguente.

Non è necessario concedere autorizzazioni minime di console per gli utenti che utilizzano l'API AWS KMS tramite gli SDK AWS, AWS Command Line Interface o AWS Tools for PowerShell. Tuttavia, è necessario concedere a questi utenti l'autorizzazione per utilizzare l'API. Per ulteriori informazioni, consulta Riferimento per le autorizzazioni.

Policy gestita da AWS per utenti esperti

È possibile utilizzare una policy gestita da `AWSKeyManagementServicePowerUser` per assegnare ai principali IAM dell'account le autorizzazioni di un utente esperto. Gli utenti esperti possono creare chiavi KMS, utilizzare e gestire le chiavi KMS da loro create e visualizzare tutte le chiavi KMS e le identità IAM. I principali che dispongono della policy gestita `AWSKeyManagementServicePowerUser` possono ottenere le autorizzazioni anche da altre origini, incluse le policy delle chiavi, altre policy IAM e concessioni.

`AWSKeyManagementServicePowerUser` è una policy IAM gestite da AWS. Per ulteriori informazioni sulle policy gestite da AWS, consulta Policy gestite da AWS nella Guida per l'utente di IAM.

> **Note**
>
> Le autorizzazioni in questa policy specifiche di una chiave KMS, ad esempio `kms:TagResource` e `kms:GetKeyRotationStatus`, sono efficaci solo quando la policy delle chiavi per quella chiave KMS consente esplicitamente all'Account AWS di utilizzare policy IAM per controllare l'accesso alla chiave. Per determinare se un'autorizzazione è specifica di una chiave KMS, consultare AWS KMS autorizzazioni e cercare un valore di chiave KMS nella colonna Resources (Risorse).
>
> Questa policy fornisce all'utente esperto le autorizzazioni per qualsiasi chiave KMS con una policy delle chiavi che consenta l'operazione. Per autorizzazioni multi-account, come `kms:DescribeKey` e `kms:ListGrants`, ciò potrebbe includere chiavi KMS in Account AWS non attendibili. Per informazioni dettagliate, consulta Best practice per le policy IAM e Autorizzazione per gli utenti in altri account di utilizzare una chiave KMS. Per determinare se un'autorizzazione è valida per le chiavi KMS in altri account, consultare AWS KMS autorizzazioni e cercare un valore Yes (Sì) nella colonna Cross-account use (Utilizzo per più account).
>
> Per consentire ai responsabili di visualizzare la AWS KMS console senza errori, il principale necessita del tag: GetResources permission, che non è incluso nella `AWSKeyManagementServicePowerUser` policy. È possibile concedere questa autorizzazione in una policy IAM separata.

La policy IAM gestita da AWSKeyManagementServicePower deve includere le seguenti autorizzazioni:

- Consente ai principali di creare chiavi KMS. Poiché questo processo include l'impostazione della policy delle chiavi, gli utenti possono concedere a se stessi e ad altri l'autorizzazione per utilizzare e gestire le chiavi KMS create.
- Consente ai principali di creare ed eliminare alias e tag in tutte le chiavi KMS. La modifica di un tag o alias può consentire o negare l'autorizzazione all'utilizzo e alla gestione della chiave KMS. Per informazioni dettagliate, vedi ABAC per AWS KMS.
- Consente ai principali di ottenere informazioni dettagliate su tutte le chiavi KMS, compreso l'ARN della chiave, la configurazione di crittografia, la policy delle chiavi, gli alias, i tag e lo stato di rotazione.
- Consente ai principali di elencare utenti, gruppi e ruoli IAM.
- Questa policy non consente ai principali di utilizzare o gestire le chiavi KMS che non hanno creato. Tuttavia, possono modificare alias e tag su tutte le chiavi KMS, il che potrebbe consentire o negare loro l'autorizzazione all'utilizzo o alla gestione di una chiave KMS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:CreateAlias",
                "kms:CreateKey",
                "kms:DeleteAlias",
                "kms:Describe*",
                "kms:GenerateRandom",
                "kms:Get*",
                "kms:List*",
                "kms:TagResource",
                "kms:UntagResource",
                "iam:ListGroups",
                "iam:ListRoles",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Esempi di policy IAM

Questa sezione include esempi di policy IAM che concedono autorizzazioni per varie azioni AWS KMS.

> **Important**
>
> Alcune delle autorizzazioni nelle seguenti policy sono consentite solo quando anche la policy delle chiavi della chiave KMS le consente. Per ulteriori informazioni, consulta Riferimento per le autorizzazioni.

Per informazioni sulla scrittura e sulla formattazione di un documento di policy JSON, consulta la Documentazione di riferimento sulla policy IAM JSON nella Guida per l'utente di IAM.

Esempi

- Consentire a un utente di visualizzare le chiavi KMS nella console AWS KMS
- Consentire a un utente di creare chiavi KMS
- Consentire a un utente di eseguire la crittografa e la decrittografa con qualsiasi chiave KMS in un Account AWS specifico
- Consentire a un utente di eseguire la crittografa e la decrittografa con qualsiasi chiave KMS in un Account AWS specifico e in una Regione
- Consentire a un utente di eseguire la crittografia e la decrittazione con chiavi KMS specifiche
- Impedire a un utente di disabilitare o eliminare le chiavi KMS

Consentire a un utente di visualizzare le chiavi KMS nella console AWS KMS

La policy IAM seguente consente agli utenti di accedere in sola lettura alla console AWS KMS. Gli utenti che dispongono di queste autorizzazioni possono visualizzare tutte le chiavi KMS nel proprio Account AWS, ma non possono creare o modificare le chiavi KMS.

Per visualizzare le chiavi KMS nelle pagine Chiavi gestite da AWSe nelle pagine delle chiavi gestite dal cliente, i principali richiedono le GetResources autorizzazioni kms: ListKeys, kms: e tag: ListAliases, anche se le chiavi non hanno tag o alias. Le autorizzazioni rimanenti, in particolare kms: DescribeKey, sono necessarie per visualizzare le colonne e i dati opzionali della tabella delle chiavi KMS nelle pagine di dettaglio delle chiavi KMS. Le ListRoles autorizzazioni iam: ListUsers e iam:

sono necessarie per visualizzare la politica chiave nella visualizzazione predefinita senza errori. Per visualizzare i dati nella pagina Custom key store e i dettagli sulle chiavi KMS negli archivi chiavi personalizzati, i mandanti necessitano anche dell'autorizzazione kms:. DescribeCustomKeyStores

Se limiti l'accesso alla console di un utente a particolari chiavi KMS, la console visualizza un errore per ogni chiave KMS che non è visibile.

Questa policy include due istruzioni di policy. L'elemento `Resource` nella prima istruzione di policy consente le autorizzazioni specificate per tutte le chiavi KMS in tutte le regioni dell'Account AWS di esempio. I visualizzatori della console non hanno bisogno di un accesso aggiuntivo perché la console AWS KMS visualizza solo le chiavi KMS nell'account del principale. Questo vale anche se hanno l'autorizzazione per visualizzare le chiavi KMS in altri Account AWS. Le autorizzazioni AWS KMS e IAM rimanenti richiedono un elemento `"Resource": "*"` perché non si applicano a nessuna particolare chiave KMS.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadOnlyAccessForAllKMSKeysInAccount",
      "Effect": "Allow",
      "Action": [
        "kms:GetPublicKey",
        "kms:GetKeyRotationStatus",
        "kms:GetKeyPolicy",
        "kms:DescribeKey",
        "kms:ListKeyPolicies",
        "kms:ListResourceTags",
        "tag:GetResources"
      ],
      "Resource": "arn:aws:kms:*:111122223333:key/*"
    },
    {
      "Sid": "ReadOnlyAccessForOperationsWithNoKMSKey",
      "Effect": "Allow",
      "Action": [
        "kms:ListKeys",
        "kms:ListAliases",
        "iam:ListRoles",
        "iam:ListUsers"
      ],
      "Resource": "*"
```

```
    }
  ]
}
```

Consentire a un utente di creare chiavi KMS

La seguente policy IAM consente a un utente di creare chiavi KMS di tutti i tipi. Il valore dell'elemento `Resource` è `*` perché l'operazione `CreateKey` non utilizza particolari risorse AWS KMS (chiavi KMS o alias).

Per limitare l'utente a particolari tipi di chiavi KMS, usa le chiavi di condizione kms:KeySpec, kms: e kms: KeyUsage. KeyOrigin

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "kms:CreateKey",
    "Resource": "*"
  }
}
```

I principali che creano le chiavi potrebbero richiedere alcune autorizzazioni correlate.

- kms: PutKeyPolicy — I responsabili che dispongono dell'`kms:CreateKey`autorizzazione possono impostare la politica chiave iniziale per la chiave KMS. Tuttavia, il `CreateKey` chiamante deve disporre di kms: PutKeyPolicy permission, che gli consente di modificare la politica della chiave KMS, oppure deve specificare il `BypassPolicyLockoutSafetyCheck` parametro di`CreateKey`, che non è consigliato. Il chiamante `CreateKey` può ottenere l'autorizzazione `kms:PutKeyPolicy` per la chiave KMS da una policy IAM o può includere questa autorizzazione nella policy chiavi della chiave KMS che sta creando.
- kms: TagResource — Per aggiungere tag alla chiave KMS durante l'`CreateKey`operazione, il `CreateKey` chiamante deve disporre dell'autorizzazione kms: in una policy IAM. TagResource Includere questa autorizzazione nella policy delle chiavi della nuova chiave KMS non è sufficiente. Tuttavia, se il chiamante `CreateKey` include `kms:TagResource` nella policy delle chiavi iniziale, può aggiungere i tag in una chiamata separata dopo la creazione della chiave KMS.
- kms: CreateAlias — I principali che creano una chiave KMS nella AWS KMS console devono avere l'CreateAliasautorizzazione kms: sulla chiave KMS e sull'alias. La console effettua due chiamate,

una a `CreateKey` e una a `CreateAlias`. È necessario fornire l'autorizzazione per l'alias in una policy IAM. Puoi fornire l'autorizzazione chiave KMS in una policy delle chiavi o in una policy IAM. Per informazioni dettagliate, vedi Controllo dell'accesso agli alias.

Oltre a `kms:CreateKey`, la policy IAM seguente fornisce l'autorizzazione `kms:TagResource` per tutte le chiavi KMS nell'Account AWS e l'autorizzazione `kms:CreateAlias` per tutti gli alias dell'account. Include anche alcune utili autorizzazioni di sola lettura che possono essere fornite solo in una policy IAM.

Questa policy IAM non include l'autorizzazione `kms:PutKeyPolicy` o altre autorizzazioni che possono essere impostate in una policy delle chiavi. Come best practice, è consigliabile impostare queste autorizzazioni nella policy delle chiavi che si applica esclusivamente a una chiave KMS.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IAMPermissionsForParticularKMSKeys",
      "Effect": "Allow",
      "Action": "kms:TagResource",
      "Resource": "arn:aws:kms:*:111122223333:key/*"
    },
    {
      "Sid": "IAMPermissionsForParticularAliases",
      "Effect": "Allow",
      "Action": "kms:CreateAlias",
      "Resource": "arn:aws:kms:*:111122223333:alias/*"
    },
    {
      "Sid": "IAMPermissionsForAllKMSKeys",
      "Effect": "Allow",
      "Action": [
        "kms:CreateKey",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource": "*"
    }
  ]
}
```

Consentire a un utente di eseguire la crittografa e la decrittografa con qualsiasi chiave KMS in un Account AWS specifico

La policy IAM seguente consente a un utente di crittografare e decrittare i dati con qualsiasi chiave KMS nell'Account AWS 111122223333.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:Encrypt",
      "kms:Decrypt"
    ],
    "Resource": "arn:aws:kms:*:111122223333:key/*"
  }
}
```

Consentire a un utente di eseguire la crittografa e la decrittografa con qualsiasi chiave KMS in un Account AWS specifico e in una Regione

La policy IAM seguente consente a un utente di crittografare e decrittare i dati con qualsiasi chiave KMS nell' Account AWS 111122223333 nella Regione Stati Uniti occidentali (Oregon).

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:Encrypt",
      "kms:Decrypt"
    ],
    "Resource": [
      "arn:aws:kms:us-west-2:111122223333:key/*"
    ]
  }
}
```

Consentire a un utente di eseguire la crittografia e la decrittazione con chiavi KMS specifiche

La policy IAM seguente consente a un utente di crittografare e decrittare i dati con le due chiavi KMS specificate nell'elemento `Resource`. Per specificare una chiave KMS in un'istruzione della policy IAM, devi utilizzare l'ARN chiave della chiave KMS.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:Encrypt",
      "kms:Decrypt"
    ],
    "Resource": [
      "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321"
    ]
  }
}
```

Impedire a un utente di disabilitare o eliminare le chiavi KMS

La policy IAM seguente impedisce a un utente di disabilitare o eliminare le chiavi KMS, anche quando un'altra policy IAM o una policy delle chiavi lo consente. Una policy che nega autorizzazioni in modo esplicito sostituisce tutte le altre policy, anche quelle che concedono le stesse autorizzazioni. Per ulteriori informazioni, consulta Risoluzione dei problemi di accesso alla chiave.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": [
      "kms:DisableKey",
      "kms:ScheduleKeyDeletion"
    ],
    "Resource": "*"
  }
}
```

Concessioni in AWS KMS

Una concessione è uno strumento delle policy che permette ai principali AWS di usare le chiavi KMS nelle operazioni di crittografia. Può anche consentire loro di visualizzare una chiave KMS (`DescribeKey`) e creare e gestire concessioni. Quando autorizzi l'accesso a una chiave KMS, le concessioni vengono prese in considerazione insieme alle policy chiave e alle policy IAM. I privilegi vengono spesso utilizzati per le autorizzazioni temporanee perché è possibile crearne una, utilizzarne le autorizzazioni ed eliminarla senza modificare le policy chiave o le policy IAM.

Le concessioni sono comunemente utilizzate dai servizi AWS che si integrano con AWS KMS per crittografare i tuoi dati inattivi. Il servizio crea una concessione per conto di un utente nell'account, ne utilizza le autorizzazioni e la revoca non appena l'attività è completata. Per informazioni dettagliate su come i servizi AWS usano le concessioni, consulta In che modo i servizi AWS utilizzano AWS KMS o l'argomento Crittografia dei dati inattivi nella guida per l'utente o nella guida per gli sviluppatori del servizio.

Per esempi di codice che illustrano l'utilizzo delle concessioni in diversi linguaggi di programmazione, consulta Utilizzo delle concessioni.

Argomenti

Informazioni sulle concessioni

Le concessioni sono un meccanismo di controllo degli accessi molto flessibile e utile. Quando crei una concessione per una chiave KMS, la concessione consente al principale beneficiario di chiamare le operazioni di concessione specificate nella chiave KMS a condizione che siano soddisfatte tutte le condizioni specificate nella concessione.

- Ogni concessione consente l'accesso a una sola chiave KMS. È possibile creare una concessione per una chiave KMS in un Account AWS diverso.
- Una concessione può consentire l'accesso a una chiave KMS, ma non negare l'accesso.

- Ogni concessione ha un beneficiario principale. Il principale beneficiario può rappresentare una o più identità nello stesso Account AWS della chiave KMS o in un account diverso.
- Una concessione può consentire solo operazioni di concessione. Le operazioni di concessione devono essere supportate dalla chiave KMS nella concessione. Se si specifica un'operazione non supportata, la CreateGrantrichiesta ha esito negativo con un'`ValidationError`eccezione.
- Il principale beneficiario può utilizzare le autorizzazioni concesse dalla concessione senza specificarla, proprio come se le autorizzazioni provenissero da una policy chiave o da una policy IAM. Tuttavia, siccome l'API AWS KMS segue un modello di consistenza finale, quando crei, ritiri o revochi una concessione, potrebbe verificarsi un breve ritardo prima che la modifica sia disponibile in AWS KMS. Per utilizzare immediatamente le autorizzazioni in una concessione, usa un token di concessione.
- Un principale autorizzato può eliminare la concessione (ritirala o revocala). L'eliminazione di una concessione elimina tutte le autorizzazioni consentite dalla concessione. Non è necessario individuare le policy da aggiungere o rimuovere per annullare la concessione.
- AWS KMS limita il numero di concessione per ogni chiave KMS. Per informazioni dettagliate, vedi Concessioni per chiave KMS: 50.000.

Prestare attenzione quando si creano concessione e quando si concede ad altri l'autorizzazione di creare concessione. L'autorizzazione a creare sovvenzioni ha implicazioni sulla sicurezza, proprio come consentire a kms: l'PutKeyPolicyautorizzazione a impostare le politiche.

- Gli utenti con l'autorizzazione a creare concessioni per una chiave KMS (`kms:CreateGrant`) possono utilizzare una concessione per permettere agli utenti e ai ruoli, inclusi i servizi AWS, di utilizzare la chiave KMS. I principi possono essere identità nel tuo Account AWS o identità in un altro account o organizzazione.
- Le concessioni possono consentire solo un sottoinsieme di operazioni AWS KMS. È possibile utilizzare le concessioni per consentire ai principali di visualizzare la chiave KMS, utilizzarla nelle operazioni di crittografia e creare e ritirare i concessioni. Per informazioni dettagliate, consulta .Operazioni di concessione. È possibile utilizzare anche i vincoli di concessione per limitare le autorizzazioni nell'ambito di una concessione per una chiave crittografica simmetrica.
- Le entità principali possono ottenere l'autorizzazione per creare concessioni da una policy chiave o da una policy IAM. I principali che ottengono l'autorizzazione `kms:CreateGrant` da una policy possono creare concessioni per qualunque operazione di concessione sulla chiave KMS. Questi principali non sono tenuti ad avere l'autorizzazione che stanno concedendo sulla chiave. Quando

si consente un'autorizzazione `kms:CreateGrant` in una policy, è possibile utilizzare le condizioni della policy per limitare questa autorizzazione.

- I principali possono inoltre ottenere l'autorizzazione per creare concessioni da una concessione. Questi principali possono delegare solo le autorizzazioni concesse, anche se dispongono di altre autorizzazioni da una policy. Per informazioni dettagliate, vedi Concessione dell'autorizzazione CreateGrant .

Per informazioni sui concetti relativi alle concessioni, consulta Terminologia sulle concessioni.

Concetti delle concessioni

Per utilizzare le concessioni in modo efficace, è necessario comprendere i termini e i concetti che AWS KMS usa.

Vincoli di concessione

Condizione che limita le autorizzazioni nella concessione. Attualmente, AWS KMS supporta i vincoli di concessioni basati sul contesto di crittografia nella richiesta di un'operazione di crittografia. Per informazioni dettagliate, vedi Utilizzo dei vincoli di concessione.

ID concessione

L'identificatore univoco di una concessione per una chiave KMS. Puoi utilizzare un ID di concessione, insieme a un identificatore chiave, per identificare una concessione in una RetireGrantrichiesta or. RevokeGrant

Operazioni di concessione

Le operazioni AWS KMS che puoi consentire in una concessione. Se si specificano altre operazioni, la CreateGrantrichiesta ha esito negativo con un'`ValidationError`eccezione. Queste sono anche le operazioni che accettano un token di concessione. Per informazioni dettagliate sulla modifica di queste autorizzazioni, consulta AWS KMS autorizzazioni.

Queste operazioni di concessione rappresentano effettivamente l'autorizzazione per l'utilizzo dell'operazione. Pertanto, per l'operazione `ReEncrypt`, puoi specificare `ReEncryptFrom`, `ReEncryptTo` o entrambi `ReEncrypt*`.

Le operazioni di concessione sono:

- Operazioni di crittografia

- Decrypt
- Encrypt
- GenerateDataKey
- GenerateDataKeyPair
- GenerateDataKeyPairWithoutPlaintext
- GenerateDataKeyWithoutPlaintext
- GenerateMac
- ReEncryptFrom
- ReEncryptTo
- Sign
- Verify
- VerifyMac

- Altre operazioni
  - CreateGrant
  - DescribeKey
  - GetPublicKey
  - RetireGrant

Le operazioni di concessione che autorizzi devono essere supportate dalla chiave KMS nella concessione. Se si specifica un'operazione non supportata, la CreateGrantrichiesta ha esito negativo con un'`ValidationError`eccezione. Ad esempio, le concessioni per le chiavi KMS di crittografia simmetrica non possono permettere le operazioni Sign, Verify, `GenerateMac` o `VerifyMac` Le concessioni per le chiavi KMS asimmetriche non possono permettere operazioni che generano chiavi di dati o coppie di chiavi di dati.

Concessione di token

L'API AWS KMS segue un modello di consistenza finale. Quando crei una concessione, potrebbe verificarsi un breve ritardo prima che la modifica sia disponibile in AWS KMS. Generalmente, occorrono pochissimi secondi per la propagazione della modifica nel sistema, ma in alcuni casi possono essere necessari diversi minuti. Se provi a utilizzare una concessione prima della propagazione in tutto il sistema, potrebbe verificarsi un errore di accesso negato. Un token di concessione consente di fare riferimento alla concessione e di utilizzare immediatamente le autorizzazioni di concessione.

Un grant token (token di concessione) è una stringa univoca, non segreta, di lunghezza variabile, codificata in base64 che rappresenta una concessione. È possibile utilizzare il token di concessione per identificare la concessione in qualsiasi operazione di concessione. Tuttavia, poiché il valore del token è un hash digest, non rivela alcun dettaglio sulla concessione.

Un token di concessione è progettato in modo da poter essere utilizzato solo quando la concessione si è propagata in AWS KMS. Dopo di che, l'assegnatario principale può utilizzare l'autorizzazione nella concessione senza fornire un token di concessione o qualsiasi altra prova della concessione. È possibile utilizzare un token di concessione in qualsiasi momento, ma una volta che la concessione è consistente, AWS KMS utilizza la concessione per determinare le autorizzazioni, non il token di concessione.

Ad esempio, il comando seguente richiama l'GenerateDataKeyoperazione. Utilizza un token di concessione per rappresentare la concessione che dà al chiamante (l'assegnatario principale) il permesso di chiamare `GenerateDataKey` sulla chiave KMS specificata.

```
$ aws kms generate-data-key \
        --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
        --key-spec AES_256 \
        --grant-token $token
```

Puoi anche utilizzare un token di concessione per identificare una concessione in qualsiasi operazione che gestisce le concessioni. Ad esempio, il preside uscente può utilizzare un token di concessione in una chiamata all'RetireGrantoperazione.

```
$ aws kms retire-grant \
        --grant-token $token
```

`CreateGrant` è l'unica operazione che restituisce un token di concessione. Non è possibile ottenere un token di concessione da nessun'altra AWS KMS operazione o dall'evento di CloudTrail registro relativo all' CreateGrant operazione. Le ListRetirableGrantsoperazioni ListGrantsand restituiscono l'ID della concessione, ma non un token di concessione.

Per informazioni dettagliate, vedi Utilizzo di un token di concessione.

Principale assegnatario

Le identità che ottengono le autorizzazioni specificate nella concessione. Ogni concessione ha un principale beneficiario che può rappresentare più identità.

L'assegnatario principale può essere qualsiasi principale AWS, incluso un Account AWS (radice), un utente IAM, un ruolo IAM, un ruolo o utente federato o un utente del ruolo assunto. L'assegnatario principale può essere nello stesso account della chiave KMS o in un account diverso. Tuttavia, l'assegnatario principale della concessione non può essere un principale del servizio, un gruppo IAM, o un'organizzazione AWS.

> **Note**
>
> Le best practice di IAM disincentivano l'uso di utenti IAM con credenziali a lungo termine. Quando possibile, utilizza i ruoli IAM che forniscono credenziali temporanee. Per i dettagli, consulta la sezione Best practice di sicurezza in IAM nella Guida per l'utente IAM.

Ritiro (di una concessione)

Termina una concessione. Ritiri una concessione al termine dell'utilizzo delle autorizzazioni.

Sia la revoca che il ritiro di una concessione eliminano la concessione. Ma il ritiro può essere fatto da un principale specificato nella concessione. La revoca viene in genere eseguita da un amministratore della chiave. Per informazioni dettagliate, vedi Ritirare e revocare le concessioni.

Principale per il ritiro

Un principale che può ritirare una concessione. È possibile specificare un principale per il ritiro in una concessione, ma non è obbligatorio. Il principale per il ritiro può essere qualsiasi principale AWS, tra cui Account AWS, utenti IAM, ruoli IAM, utenti federati e utenti dei ruoli assunti. Il principale per il ritiro può essere nello stesso account della chiave KMS o in un account diverso.

> **Note**
>
> Le best practice di IAM disincentivano l'uso di utenti IAM con credenziali a lungo termine. Quando possibile, utilizza i ruoli IAM che forniscono credenziali temporanee. Per i dettagli, consulta la sezione Best practice di sicurezza in IAM nella Guida per l'utente IAM.

Oltre al principale per il ritiro specificato nella concessione, una concessione può essere ritirata dall'Account AWS in cui la concessione è stata creata. Se la concessione consente l'operazione `RetireGrant`, l'assegnatario principale può ritirare la concessione. Inoltre, l'Account AWS o un Account AWS che rappresenta l'assegnatario principale può delegare l'autorizzazione a ritirare

una concessione a un principale IAM nello stesso Account AWS. Per informazioni dettagliate, vedi Ritirare e revocare le concessioni.

Revoca (di una concessione)

Termina una concessione. Revochi una concessione per negare attivamente le autorizzazioni consentite dalla concessione.

Sia la revoca che il ritiro di una concessione eliminano la concessione. Ma il ritiro può essere fatto da un principale specificato nella concessione. La revoca viene in genere eseguita da un amministratore della chiave. Per informazioni dettagliate, vedi Ritirare e revocare le concessioni.

Consistenza finale (per le concessioni)

L'API AWS KMS segue un modello di consistenza finale. Quando crei, ritiri o revochi una concessione, potrebbe verificarsi un breve ritardo prima che la modifica sia disponibile in AWS KMS. Generalmente, occorrono pochissimi secondi per la propagazione della modifica nel sistema, ma in alcuni casi possono essere necessari diversi minuti.

Potresti apprendere di questo breve ritardo se ricevi errori imprevisti. Ad esempio, se tenti di gestire una nuova concessione o utilizzi le autorizzazioni in una nuova concessione prima che la concessione sia nota in AWS KMS, potresti ricevere un errore di accesso negato. Se ritiri o revochi una concessione, l'assegnatario principale potrebbe ancora essere in grado di utilizzare le autorizzazioni per un breve periodo fino a quando la concessione non viene completamente eliminata. La strategia tipica è quella di riprovare la richiesta, e alcuni SDK AWS includono backoff automatico e logica di ripetizione.

AWS KMS dispone di funzioni per mitigare questo breve ritardo.

- Per utilizzare immediatamente le autorizzazioni in una nuova concessione, usa un token di concessione. È possibile utilizzare un token di concessione per fare riferimento a una concessione in qualsiasi operazione di concessione. Per istruzioni, consulta Utilizzo di un token di concessione.
- L'CreateGrantoperazione ha un `Name` parametro che impedisce alle operazioni di nuovo tentativo di creare concessioni duplicate.

> **Note**
>
> I token di concessione sostituiscono la validità della concessione fino a quando tutti gli endpoint del servizio non sono stati aggiornati con il nuovo stato della concessione. Nella maggior parte dei casi, la consistenza finale sarà raggiunta entro cinque minuti.

Per ulteriori informazioni, consulta Consistenza finale di AWS KMS.

Best practice per le concessioni AWS KMS

AWS KMS consiglia le seguenti best practice durante la creazione, l'utilizzo e la gestione delle concessioni.

- Limita le autorizzazioni nella concessione a quelle richieste dall'assegnatario principale. Utilizzare il principio di accesso meno privilegiato.
- Utilizza un assegnatario principale specifico, ad esempio un ruolo IAM, e concedigli l'autorizzazione di utilizzare solo le operazioni API richieste.
- Usa il contesto di crittografia Vincoli di concessione per garantire che i chiamanti utilizzino la chiave KMS per lo scopo previsto. Per informazioni dettagliate su come utilizzare il contesto di crittografia in una richiesta di protezione dei dati, consulta Come proteggere l'integrità dei dati crittografati utilizzando AWS Key Management Service e EncryptionContext nel blog sulla AWS sicurezza.

  > **Tip**
  >
  > Utilizza il vincolo di EncryptionContextEqualconcessione ogni volta che è possibile. Il vincolo di EncryptionContextSubsetconcessione è più difficile da usare correttamente. Se devi utilizzarlo, leggi attentamente la documentazione e testa il vincolo di concessione per assicurarti che funzioni come previsto.

- Eliminare concessioni duplicate. Le concessioni duplicate hanno lo stesso ARN chiave, le stesse azioni API, lo stesso assegnatario principale, lo stesso contesto di crittografia e lo stesso nome. Se ritiri o revochi la concessione originale ma lasci i duplicati, le concessioni duplicate rimanenti rappresentano escalation involontarie di privilegi. Per evitare di duplicare le concessioni quando riprovi una richiesta `CreateGrant`, utilizza il parametro `Name`. Per rilevare sovvenzioni duplicate, utilizzate l'operazione. ListGrants Se crei accidentalmente una concessione duplicata, ritirala o revocala il prima possibile.

  > **Note**
  >
  > Le concessioni per chiavi gestite da AWS potrebbero sembrare duplicate ma avere diversi assegnatari principali.
  > Il campo `GranteePrincipal` nella risposta `ListGrants` contiene solitamente il principal dell'assegnatario della concessione. Tuttavia, quando il principale dell'assegnatario della

concessione è un servizio AWS, il campo `GranteePrincipal` contiene il principale del servizio, che potrebbe rappresentare più principali dell'assegnatario diversi.

- Ricorda che le concessioni non scadono automaticamente. Ritira o revoca la concessione non appena l'autorizzazione non sarà più necessaria. Le concessioni che non vengono eliminate potrebbero creare un rischio per la sicurezza delle risorse crittografate.

Creazione di concessioni

Prima di creare una concessione, scopri le opzioni per la personalizzazione della concessione. È possibile utilizzare vincoli di concessione per limitare le autorizzazioni nella concessione. Scopri di più sulla concessione dell'autorizzazione `CreateGrant`. Le entità principali che ricevono l'autorizzazione per creare concessioni da una concessione sono limitate nelle concessioni che possono creare.

Argomenti

- Creazione di una concessione
- Utilizzo dei vincoli di concessione
- Concessione dell'autorizzazione CreateGrant

Creazione di una concessione

Per creare una sovvenzione, chiama l'CreateGrantoperazione. Specifica una chiave KMS, un assegnatario principale e un elenco di operazioni di concessione consentite. È inoltre possibile designare un principale per il ritiro opzionale. Per personalizzare la concessione, puoi usare i parametri `Constraints` opzionali per definire i vincoli di concessione

Quando si crea, si ritira o si revoca una concessione, potrebbe verificarsi un breve ritardo, in genere meno di cinque minuti, prima che la modifica sia disponibile in AWS KMS. Per ulteriori informazioni, consulta Consistenza finale (per concessioni).

Ad esempio, il comando `CreateGrant` seguente crea una concessione che consente agli utenti autorizzati ad assumere il ruolo `keyUserRole` di chiamare l'operazione Decrypt sulla chiave KMS simmetrica specificata. La concessione utilizza il parametro `RetiringPrincipal` per designare un'entità principale che può ritirare la concessione. Include anche un vincolo di concessione che consente l'autorizzazione solo quando il contesto di crittografia nella richiesta include `"Department": "IT"`.

```
$  aws kms create-grant \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/keyUserRole \
    --operations Decrypt \
    --retiring-principal arn:aws:iam::111122223333:role/adminRole \
    --constraints EncryptionContextSubset={Department=IT}
```

Se il tuo codice tenta di nuovo l'operazione `CreateGrant` o utilizza un SDK AWS che rinvia automaticamente le richieste, utilizza il parametro opzionale Nome per impedire la creazione di concessioni duplicate. Se AWS KMS ottiene una richiesta `CreateGrant` per una concessione con le stesse proprietà di una concessione esistente, incluso il nome, riconosce la richiesta come un nuovo tentativo e non crea una nuova concessione. Non puoi utilizzare il valore `Name` per identificare la concessione in qualsiasi operazione AWS KMS.

> **Important**
>
> Non includere informazioni riservate o sensibili nel nome della concessione. Può apparire in testo semplice nei CloudTrail log e in altri output.

```
$ aws kms create-grant \
    --name IT-1234abcd-keyUserRole-decrypt \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/keyUserRole \
    --operations Decrypt \
    --retiring-principal arn:aws:iam::111122223333:role/adminRole \
    --constraints EncryptionContextSubset={Department=IT}
```

Per esempi di codice che illustrano l'utilizzo delle concessioni in diversi linguaggi di programmazione, consulta Utilizzo delle concessioni.

Utilizzo dei vincoli di concessione

I vincoli di concessione stabiliscono condizioni relative alle autorizzazioni che la concessione dà all'assegnatario principale. I vincoli di concessione sostituiscono le chiavi di condizione in una policy chiave o in una policy IAM. Ogni valore del vincolo di concessione può includere fino a 8 coppie del contesto di crittografia. Il valore del contesto di crittografia in ogni vincolo di concessione non può superare i 384 caratteri.

> **Important**
>
> Non includere informazioni riservate o sensibili in questo campo. Questo campo può essere visualizzato in testo semplice nei CloudTrail log e in altri output.

AWS KMS supporta due vincoli di concessione, `EncryptionContextEquals` e `EncryptionContextSubset`, entrambi i quali stabiliscono i requisiti per il contesto di crittografia in una richiesta di un'operazione di crittografia.

I vincoli di concessione del contesto di crittografia sono progettati per essere utilizzati con operazioni di concessione che dispongono di un parametro contesto di crittografia.

- I vincoli di contesto di crittografia sono validi solo in una concessione per una chiave KMS di crittografia simmetrica. Le operazioni di crittografia con altre chiavi KMS non supportano un contesto di crittografia.
- Il vincolo di contesto di crittografia viene ignorato per le operazioni `DescribeKey` e `RetireGrant`. `DescribeKey` e `RetireGrant` non dispongono di un parametro di contesto di crittografia, ma è possibile includere queste operazioni in una concessione con un vincolo di contesto di crittografia.
- È possibile utilizzare un vincolo di contesto di crittografia in una concessione per l'operazione `CreateGrant`. Il vincolo del contesto di crittografia richiede che tutte le concessioni create con l'autorizzazione `CreateGrant` hanno un vincolo di contesto di crittografia altrettanto rigoroso o più rigoroso.

AWS KMS supporta i seguenti vincoli di concessione del contesto di crittografia.

EncryptionContextEquals

Utilizza `EncryptionContextEquals` per specificare il contesto di crittografia esatto per le richieste consentite.

`EncryptionContextEquals` richiede che le coppie del contesto di crittografia nella richiesta corrispondano in modo esatto a livello di maiuscole e minuscole alle coppie del contesto di crittografia nel vincolo di concessione. Le coppie possono essere visualizzate in qualsiasi ordine, ma le chiavi e i valori in ciascuna coppia non possono variare.

Ad esempio, se il vincolo di concessione `EncryptionContextEquals` richiede la coppia del contesto di crittografia `"Department": "IT"`, la concessione consente le richieste del tipo specificato solo quando il contesto di crittografia nella richiesta è esattamente `"Department": "IT"`.

EncryptionContextSubset

Utilizza `EncryptionContextSubset` per richiedere che le richieste includano particolari coppie di contesto di crittografia.

`EncryptionContextSubset` richiede che le richieste includano tutte le coppie del contesto di crittografia nel vincolo di concessione (corrispondenti in modo esatto a livello di maiuscole e minuscole), ma la richiesta può avere anche altre coppie di contesto di crittografia. Le coppie possono essere visualizzate in qualsiasi ordine, ma le chiavi e i valori in ciascuna coppia non possono variare.

Ad esempio, se il vincolo di concessione `EncryptionContextSubset` richiede la coppia del contesto di crittografia `Department=IT`, la concessione consente le richieste del tipo specificato quando il contesto di crittografia nella richiesta è `"Department": "IT"`, o include `"Department": "IT"` insieme ad altre coppie di contesto di crittografia, come `"Department": "IT","Purpose": "Test"`.

Per specificare un vincolo di contesto di crittografia in una concessione per una chiave KMS di crittografia simmetrica, utilizzate il parametro nell'operazione. `Constraints` CreateGrant La concessione creata da questo comando concede agli utenti autorizzati ad assumere il ruolo `keyUserRole` l'autorizzazione a chiamare l'operazione API Decrypt. Tuttavia, tale autorizzazione è valida solo quando il contesto di crittografia nella richiesta `Decrypt` è una coppia di contesto di crittografia `"Department": "IT"`.

```
$ aws kms create-grant \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/keyUserRole \
    --operations Decrypt \
    --retiring-principal arn:aws:iam::111122223333:role/adminRole \
    --constraints EncryptionContextEquals={Department=IT}
```

La concessione risultante è simile alla seguente. Tieni presente che l'autorizzazione concessa al ruolo `keyUserRole` è valida solo quando la richiesta `Decrypt` usa la stessa coppia del contesto di

crittografia specificata nel vincolo di concessione. Per trovare le concessioni su una chiave KMS, usa l'operazione. ListGrants

```
$ aws kms list-grants --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
{
    "Grants": [
        {
            "Name": "",
            "IssuingAccount": "arn:aws:iam::111122223333:root",
            "GrantId":
 "abcde1237f76e4ba7987489ac329fbfba6ad343d6f7075dbd1ef191f0120514a",
            "Operations": [
                "Decrypt"
            ],
            "GranteePrincipal": "arn:aws:iam::111122223333:role/keyUserRole",
            "Constraints": {
                "EncryptionContextEquals": {
                    "Department": "IT"
                }
            },
            "CreationDate": 1568565290.0,
            "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "RetiringPrincipal": "arn:aws:iam::111122223333:role/adminRole"
        }
    ]
}
```

Per soddisfare il vincolo di concessione `EncryptionContextEquals`, il contesto di crittografia nella richiesta per l'operazione `Decrypt` deve essere una coppia `"Department": "IT"`. Una richiesta dall'assegnatario principale come la seguente soddisferebbe il vincolo di concessione `EncryptionContextEquals`.

```
$ aws kms decrypt \
    --key-id arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab\
    --ciphertext-blob fileb://encrypted_msg \
    --encryption-context Department=IT
```

Quando il vincolo di concessione è `EncryptionContextSubset`, le coppie del contesto di crittografia nella richiesta devono includere le coppie del contesto di crittografia nel vincolo di

concessione, ma la richiesta può includere anche altre coppie di contesto di crittografia. Il seguente vincolo di concessione richiede che una delle coppie di contesto di crittografia nella richiesta sia `"Deparment": "IT"`.

```
"Constraints": {
   "EncryptionContextSubset": {
       "Department": "IT"
   }
}
```

La seguente richiesta dall'assegnatario principale soddisferebbe entrambi i vincoli di concessione `EncryptionContextEqual` e `EncryptionContextSubset` di questo esempio.

```
$ aws kms decrypt \
    --key-id arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --ciphertext-blob fileb://encrypted_msg \
    --encryption-context Department=IT
```

Tuttavia, una richiesta come la seguente da parte dell'assegnatario principale soddisferebbe il vincolo di concessione`EncryptionContextSubset`, ma fallirebbe il vincolo di concessione `EncryptionContextEquals`.

```
$ aws kms decrypt \
    --key-id arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --ciphertext-blob fileb://encrypted_msg \
    --encryption-context Department=IT,Purpose=Test
```

I servizi AWS spesso utilizzano vincoli di contesto di crittografia nelle concessioni che concedono loro l'autorizzazione per utilizzare chiavi KMS nel tuo account Account AWS. Ad esempio, Amazon DynamoDB utilizza una concessione come la seguente per ottenere l'autorizzazione a utilizzare la Chiave gestita da AWS per DynamoDB nel tuo account. Il vincolo di concessione `EncryptionContextSubset` in questa concessione rende le autorizzazioni nella concessione valide solo quando il contesto di crittografia nella richiesta include coppie `"tableName": "Services"` e `"subscriberID": "111122223333"`. Questo vincolo di concessione significa che la concessione consente a DynamoDB di utilizzare la chiave KMS specificata solo per una determinata tabella nel tuo Account AWS.

Per ottenere questo risultato, esegui l'ListGrantsoperazione su Chiave gestita da AWS per DynamoDB nel tuo account.

```
$ aws kms list-grants --key-id 0987dcba-09fe-87dc-65ba-ab0987654321

{
    "Grants": [
        {
            "Operations": [
                "Decrypt",
                "Encrypt",
                "GenerateDataKey",
                "ReEncryptFrom",
                "ReEncryptTo",
                "RetireGrant",
                "DescribeKey"
            ],
            "IssuingAccount": "arn:aws:iam::111122223333:root",
            "Constraints": {
                "EncryptionContextSubset": {
                    "aws:dynamodb:tableName": "Services",
                    "aws:dynamodb:subscriberId": "111122223333"
                }
            },
            "CreationDate": 1518567315.0,
            "KeyId": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321",
            "GranteePrincipal": "dynamodb.us-west-2.amazonaws.com",
            "RetiringPrincipal": "dynamodb.us-west-2.amazonaws.com",
            "Name": "8276b9a6-6cf0-46f1-b2f0-7993a7f8c89a",
            "GrantId":
 "1667b97d27cf748cf05b487217dd4179526c949d14fb3903858e25193253fe59"
        }
    ]
}
```

Concessione dell'autorizzazione CreateGrant

Una concessione può includere l'autorizzazione per chiamare l'operazione `CreateGrant`. Ma quando un assegnatario principale ottiene l'autorizzazione di chiamare `CreateGrant` da una concessione, piuttosto che da una policy, tale autorizzazione è limitata.

- L'assegnatario principale può solo creare concessioni che consentono alcune o tutte le operazioni nella concessione primaria.
- I vincoli di concessione nelle concessioni che creano devono essere almeno altrettanto rigorosi di quelli della concessione primaria.

Queste limitazioni non si applicano ai principali che ottengono l'autorizzazione `CreateGrant` da una policy, anche se le loro autorizzazioni possono essere limitate dalle condizioni della policy.

Ad esempio, considera una concessione che consente al principale della concessione di chiamare le operazioni `GenerateDataKey`, `Decrypt` e `CreateGrant`. Chiamiamo una concessione che consente all'autorizzazione `CreateGrant` a una concessione primaria.

```
# The original grant in a ListGrants response.
{
    "Grants": [
        {
            "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "CreationDate": 1572216195.0,
            "GrantId":
 "abcde1237f76e4ba7987489ac329fbfba6ad343d6f7075dbd1ef191f0120514a",
            "Operations": [
                "GenerateDataKey",
                "Decrypt",
                "CreateGrant
            ]
            "RetiringPrincipal": "arn:aws:iam::111122223333:role/adminRole",
            "Name": "",
            "IssuingAccount": "arn:aws:iam::111122223333:root",
            "GranteePrincipal": "arn:aws:iam::111122223333:role/keyUserRole",
            "Constraints": {
                "EncryptionContextSubset": {
                    "Department": "IT"
                }
            },
        }
    ]
}
```

L'assegnatario principale, exampleUser, può utilizzare questa autorizzazione per creare una concessione che include un sottoinsieme delle operazioni specificate nella concessione originale, ad

esempio `CreateGrant` e `Decrypt`. La concessione secondaria non può includere altre operazioni, come `ScheduleKeyDeletion` o `ReEncrypt`.

Inoltre, i vincoli nelle concessioni secondarie devono essere altrettanto o più restrittivi di quelli della concessione primaria. Ad esempio, la concessione figlio può aggiungere coppie a un vincolo `EncryptionContextSubset` nella concessione padre, ma non può rimuoverle. La concessione figlio può modificare un vincolo `EncryptionContextSubset` in un vincolo `EncryptionContextEquals`, ma non viceversa.

Ad esempio, l'assegnatario principale della concessione può utilizzare l'autorizzazione `CreateGrant` che ha ottenuto dalla concessione primaria per creare la seguente concessione secondaria. Le operazioni nella concessione secondaria sono un sottoinsieme di operazioni della concessione primaria e i vincoli di concessione sono più restrittivi.

```
# The child grant in a ListGrants response.
{
    "Grants": [
        {
            "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "CreationDate": 1572249600.0,
            "GrantId":
 "fedcba9999c1e2e9876abcde6e9d6c9b6a1987650000abcee009abcdef40183f",
            "Operations": [
                "CreateGrant"
                "Decrypt"
            ]
            "RetiringPrincipal": "arn:aws:iam::111122223333:user/exampleUser",
            "Name": "",
            "IssuingAccount": "arn:aws:iam::111122223333:root",
            "GranteePrincipal": "arn:aws:iam::111122223333:user/anotherUser",
            "Constraints": {
IAM best practices discourage the use of IAM users with long-term credentials. Whenever
                      possible, use IAM roles, which provide temporary credentials. For
 details,
                      see Security best practices in IAM in the IAM User Guide.
        "EncryptionContextEquals": {
                    "Department": "IT"
                }
            },
        }
    ]
```

```
}
```

L'assegnatario principale nella concessione secondaria, `anotherUser`, può utilizzare il la sua autorizzazione `CreateGrant` per creare concessioni. Tuttavia, le concessioni che `anotherUser` crea devono includere le operazioni nella sua concessione primaria o in un sottoinsieme e i vincoli di concessione devono essere uguali o più severi.

Gestione delle concessioni

Le entità con le autorizzazioni richieste possono visualizzare, utilizzare ed eliminare (ritirare o revocare) le concessioni. Per perfezionare le autorizzazioni per la creazione e la gestione delle concessioni, AWS KMS supporta diverse condizioni di policy che è possibile utilizzare nelle policy chiave e nelle policy IAM.

Argomenti

Controllo dell'accesso alle concessioni

È possibile controllare l'accesso alle operazioni che creano e gestiscono concessioni nelle policy chiave, nelle policy IAM e nelle concessioni. I principali che ottengono l'autorizzazione `CreateGrant` da una concessione hanno autorizzazioni di concessione più limitate.

Operazione API	Policy chiave o policy IAM	Grant
CreateGrant	✓	✓
ListGrants	✓	-
ListRetirableGrants	✓	-
Ritiro di concessioni	(Limitato. Consulta Ritirare e revocare le concessioni)	✓

Operazione API	Policy chiave o policy IAM	Grant
RevokeGrant	✓	-

Quando usi una policy chiave o una policy IAM per controllare l'accesso alle operazioni che creano e generano concessioni, puoi utilizzare una o più condizioni di policy seguenti per limitare l'autorizzazione. AWS KMS supporta tutte le chiavi di condizione correlate alle concessioni indicate di seguito. Per informazioni dettagliate ed esempi, consulta AWS KMS chiavi di condizione.

km: GrantConstraintType

Consente ai principali di creare una concessione solo quando la concessione include il vincolo di concessione specificato.

km: GrantIsFor AWSResource

Permette ai principali di chiamare `CreateGrant`, `ListGrants` o `RevokeGrant` solo quando un servizio AWS integrato con AWS KMS invia la richiesta per conto del principale.

km: GrantOperations

Consente ai principali di creare una concessione, ma limita la concessione alle operazioni specificate.

km: GranteePrincipal

Consente ai principali di creare una concessione solo per l'assegnatario principale specificato.

km: RetiringPrincipal

Consente ai principali di creare una concessione solo quando la concessione specifica un particolare principale per il ritiro.

Visualizzazione di concessioni

Per visualizzare la concessione, usa l'ListGrantsoperazione. È necessario specificare la chiave KMS a cui si applicano le concessioni. È inoltre possibile filtrare l'elenco delle concessioni in base all'ID concessione o all'assegnatario principale. Per ulteriori esempi, consulta Visualizzazione di una concessione.

Per visualizzare tutte le sovvenzioni nella regione Account AWS e con un particolare capitale uscente, usa. ListRetirableGrants Le risposte includono dettagli su ogni concessione.

> **Note**
>
> Il campo `GranteePrincipal` nella risposta `ListGrants` contiene solitamente il principal dell'assegnatario della concessione. Tuttavia, quando il principale dell'assegnatario della concessione è un servizio AWS, il campo `GranteePrincipal` contiene il principale del servizio, che potrebbe rappresentare più principali dell'assegnatario diversi.

Ad esempio, il comando seguente elenca tutte le concessioni per una chiave KMS.

```
$  aws kms list-grants --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
{
    "Grants": [
        {
            "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "CreationDate": 1572216195.0,
            "GrantId":
 "abcde1237f76e4ba7987489ac329fbfba6ad343d6f7075dbd1ef191f0120514a",
            "Constraints": {
                "EncryptionContextSubset": {
                    "Department": "IT"
                }
            },
            "RetiringPrincipal": "arn:aws:iam::111122223333:role/adminRole",
            "Name": "",
            "IssuingAccount": "arn:aws:iam::111122223333:root",
            "GranteePrincipal": "arn:aws:iam::111122223333:user/exampleUser",
            "Operations": [
                "Decrypt"
            ]
        }
    ]
}
```

Utilizzo di un token di concessione

L'API AWS KMS segue un modello di consistenza finale. Quando si crea una concessione, la concessione potrebbe non essere effettiva immediatamente. Potrebbe verificarsi un breve ritardo prima che la modifica sia disponibile in AWS KMS. Generalmente, occorrono pochissimi secondi per la propagazione della modifica nel sistema, ma in alcuni casi possono essere necessari diversi

minuti. Una volta che la concessione è stata propagata in tutto il sistema, il principale assegnatario può utilizzare le autorizzazioni nella concessione senza specificare il token di concessione o una prova della concessione. Tuttavia, se una concessione è talmente nuova da non essere ancora nota a tutti in AWS KMS, l'esito della richiesta potrebbe essere negativo con un errore `AccessDeniedException`.

Per utilizzare immediatamente le autorizzazioni in una nuova concessione, utilizza il token di concessione per la concessione. Salva il token di concessione restituito dall'CreateGrantoperazione. Quindi invia il token di concessione nella richiesta per l'operazione AWS KMS. È possibile inviare un token di concessione a qualsiasi operazione di concessione AWS KMS e puoi inviare più token di concessione nella stessa richiesta.

L'esempio seguente utilizza l'`CreateGrant`operazione per creare una concessione che consenta le operazioni GenerateDataKeye Decrypt. Salva il token di concessione che `CreateGrant` restituisce nella variabile `token`. Quindi, in una chiamata all'operazione `GenerateDataKey`, utilizza il token di concessione nella variabile `token`.

```
# Create a grant; save the grant token
$ token=$(aws kms create-grant \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:user/appUser \
    --retiring-principal arn:aws:iam::111122223333:user/acctAdmin \
    --operations GenerateDataKey Decrypt \
    --query GrantToken \
    --output text)

# Use the grant token in a request
$ aws kms generate-data-key \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --key-spec AES_256 \
    --grant-tokens $token
```

I principali con autorizzazione possono utilizzare un token di concessione anche per ritirare una nuova concessione, anche prima che la concessione sia disponibile in AWS KMS. (L'operazione `RevokeGrant` non accetta un token di concessione.) Per informazioni dettagliate, vedi Ritirare e revocare le concessioni.

```
# Retire the grant
$ aws kms retire-grant --grant-token $token
```

Ritirare e revocare le concessioni

Per eliminare una concessione, ritirarla o revocarla.

Le RevokeGrantoperazioni RetireGrantand sono molto simili tra loro. Entrambe le operazioni eliminano una concessione, eliminando le autorizzazioni consentite dalla concessione. La differenza principale tra queste operazioni è il modo in cui sono autorizzate.

RevokeGrant

Come la maggior parte delle operazioni AWS KMS, l'accesso all'operazione `RevokeGrant` è controllata tramite le policy chiave e le policy IAM. L'RevokeGrantAPI può essere richiamata da qualsiasi principale con `kms:RevokeGrant` autorizzazione. Questa autorizzazione è inclusa nelle autorizzazioni standard concesse agli amministratori delle chiavi. In genere, gli amministratori revocano una concessione per negare le autorizzazioni consentite dalla concessione.

RetireGrant

La concessione determina chi può ritirarla. Questa struttura consente di controllare il ciclo di vita di una concessione senza modificare le policy chiave o le policy IAM. In genere, si ritira una concessione quando si è terminato di utilizzare le relative autorizzazioni.

Una concessione può essere ritirata da un principale per il ritiro opzionale specificato nella concessione. L'assegnatario principale può anche ritirare la concessione, ma solo se è anche un principale per il ritiro o se la concessione include l'operazione `RetireGrant`. Come backup, l'Account AWS in cui la concessione è stata creata può ritirare la concessione.

C'è un'autorizzazione `kms:RetireGrant` che può essere utilizzata nelle policy IAM, ma dispone di un'utilità limitata. I principali specificati nella concessione possono ritirare una concessione senza l'autorizzazione `kms:RetireGrant`. L'autorizzazione `kms:RetireGrant` da sola non consente ai principali di ritirare una concessione. L'autorizzazione `kms:RetireGrant` non è efficace in una policy chiave.

- Per negare l'autorizzazione al ritiro di una concessione, puoi utilizzare un'azione `Deny` con l'autorizzazione `kms:RetireGrant`.
- L'Account AWS che possiede la chiave KMS può delegare l'autorizzazione `kms:RetireGrant` al principale IAM nell'account.
- Se il principale per il ritiro è un Account AWS diverso, gli amministratori dell'altro account possono utilizzare `kms:RetireGrant` per delegare l'autorizzazione a ritirare la concessione al principale IAM in tale account.

L'API AWS KMS segue un modello di consistenza finale. Quando crei, ritiri o revochi una concessione, potrebbe verificarsi un breve ritardo prima che la modifica sia disponibile in AWS KMS. Generalmente, occorrono pochissimi secondi per la propagazione della modifica nel sistema, ma in alcuni casi possono essere necessari diversi minuti. Se è necessario eliminare immediatamente una nuova concessione, prima che sia disponibile in AWS KMS, usa un token di concessione per ritirare la concessione. Non è possibile utilizzare un token di concessione per revocare una concessione.

Connessione a AWS KMS mediante un endpoint VPC

Ora puoi connetterti direttamente a AWS KMS attraverso un endpoint VPC di interfaccia nel tuo cloud privato virtuale (VPC). Quando utilizzi un endpoint VPC di interfaccia, la comunicazione tra il VPC e AWS KMS avviene completamente all'interno della rete AWS.

AWS KMS supporta gli endpoint Amazon Virtual Private Cloud (Amazon VPC) basati su AWS PrivateLink. Ogni endpoint VPC è rappresentato da una o più interfacce di rete elastiche (ENI) con indirizzi IP privati nelle sottoreti del VPC.

L'endpoint VPC di interfaccia connette il tuo VPC direttamente ad AWS KMS senza alcun Internet gateway, dispositivo NAT, connessione VPN o connessione AWS Direct Connect. Le istanze presenti nel VPC non richiedono indirizzi IP pubblici per comunicare con AWS KMS.

Regioni

AWS KMS supporta gli endpoint VPC e le policy degli endpoint VPC in tutte le Regioni AWS in cui AWS KMS è disponibile.

Argomenti

- Considerazioni sugli endpoint VPC dell'AWS KMS
- Creazione di un endpoint VPC per AWS KMS
- Connessione a un endpoint VPC AWS KMS
- Controllo dell'accesso all'endpoint VPC
- Utilizzo di un endpoint VPC in un'istruzione di policy
- Registrazione dell'endpoint VPC

Considerazioni sugli endpoint VPC dell'AWS KMS

Prima di impostare un endpoint VPC dell'interfaccia per AWS KMS, consulta l'argomento Proprietà e limitazioni degli endpoint dell'interfaccia nella Guida AWS PrivateLink.

Il supporto AWS KMS per un endpoint VPC include quanto segue.

- Puoi utilizzare l'endpoint VPC per richiamare tutte le operazioni API AWS KMS dal VPC.
- Puoi creare un endpoint VPC di interfaccia che si collega all'endpoint di una regione AWS KMS o a un endpoint FIPS AWS KMS.
- È possibile utilizzare i registri AWS CloudTrail per eseguire una verifica sull'utilizzo delle chiavi KMS tramite l'endpoint VPC. Per informazioni dettagliate, vedi Registrazione dell'endpoint VPC.

Creazione di un endpoint VPC per AWS KMS

Puoi creare un endpoint VPC per AWS KMS utilizzando la console Amazon VPC o l'API Amazon VPC. Per ulteriori informazioni, consulta la sezione Creazione di un endpoint di interfaccia nella Guida per l'utente di AWS PrivateLink.

- Per creare un endpoint VPC per l'AWS KMS, utilizza il seguente nome di servizio:

  ```
  com.amazonaws.region.kms
  ```

  Ad esempio, nella regione Stati Uniti occidentali (Oregon) (`us-west-2`), il nome del servizio sarebbe:

  ```
  com.amazonaws.us-west-2.kms
  ```

- Per creare un endpoint VPC che si collega a un endpoint FIPS AWS KMS, usa il seguente nome di servizio:

  ```
  com.amazonaws.region.kms-fips
  ```

  Ad esempio, nella regione Stati Uniti occidentali (Oregon) (`us-west-2`), il nome del servizio sarebbe:

  ```
  com.amazonaws.us-west-2.kms-fips
  ```

Per semplificare l'utilizzo dell'endpoint VPC, puoi abilitare un nome DNS privato per l'endpoint VPC. Se selezioni l'opzione Enable DNS Name (Abilita nome DNS), il nome host DNS standard AWS KMS si risolve nell'endpoint VPC. Ad esempio, `https://kms.us-west-2.amazonaws.com` si risolverebbe in un endpoint VPC connesso al nome del servizio `com.amazonaws.us-west-2.kms`.

Questa opzione rende più semplice utilizzare l'endpoint VPC. La AWS CLI e gli SDK AWS utilizzano per impostazione predefinita il nome host DNS standard dell'AWS KMS, pertanto hai bisogno di specificare l'URL dell'endpoint VPC nelle applicazioni e nei comandi.

Per ulteriori informazioni, consulta la sezione Accesso a un servizio tramite un endpoint di interfaccia nella Guida di AWS PrivateLink.

Connessione a un endpoint VPC AWS KMS

È possibile connettersi a AWS KMS tramite l'endpoint VPC utilizzando un SDK AWS, l'AWS CLI o AWS Tools for PowerShell. Per specificare l'endpoint VPC, utilizzare il nome DNS.

Ad esempio, il comando list-keys utilizza il parametro `endpoint-url` per specificare l'endpoint VPC. Per utilizzare un comando come questo, sostituisci l'ID dell'endpoint VPC con uno presente nel tuo account.

```
$ aws kms list-keys --endpoint-url https://vpce-1234abcdf5678c90a-09p7654s-us-east-1a.ec2.us-east-1.vpce.amazonaws.com
```

Se hai attivato nomi host privati al momento della creazione dell'endpoint VPC, non è necessario specificare l'URL dell'endpoint VPC nella configurazione dell'applicazione o nei comandi della CLI. Il nome host DNS standard AWS KMS viene risolto nell'endpoint VPC. La AWS CLI e gli SDK usano questo nome host per impostazione predefinita, quindi puoi iniziare a utilizzare l'endpoint VPC per connetterti a un endpoint regionale AWS KMS senza modificare nulla negli script e nelle applicazioni.

Per utilizzare nomi host privati, gli attributi `enableDnsHostnames` e `enableDnsSupport` del VPC devono essere impostati su `true`. Per impostare questi attributi, utilizzare l'ModifyVpcAttributeoperazione. Per informazioni dettagliate, consulta la sezione Visualizzazione e aggiornamento degli attributi DNS per il VPC nella Guida per l'utente di Amazon VPC.

Controllo dell'accesso all'endpoint VPC

Per controllare l'accesso all'endpoint VPC per AWS KMS collegare una policy di endpoint VPC all'endpoint VPC. La policy di endpoint determina se i principali possono utilizzare l'endpoint VPC per chiamare le operazioni AWS KMS sulle risorse AWS KMS.

Puoi creare una policy di endpoint VPC quando crei l'endpoint e puoi modificare la policy di endpoint VPC in qualsiasi momento. Utilizza la console di gestione VPC o le operazioni CreateVpcEndpointo ModifyVpcEndpoint. Puoi inoltre creare e modificare una policy di endpoint VPC utilizzando un modello di AWS CloudFormation. Per informazioni sull'utilizzo della console di gestione VPC, consulta la sezione Creazione di un endpoint di interfaccia e Modifica di un endpoint di interfaccia nella Guida di AWS PrivateLink.

> **Note**
>
> AWS KMS supporta le policy di endpoint VPC da luglio 2020. Gli endpoint VPC per AWS KMS creati prima di tale data hanno la policy di endpoint VPC predefinita, ma è possibile modificarla in qualsiasi momento.

Per informazioni sulla scrittura e sulla formattazione di un documento di policy JSON, consulta la Documentazione di riferimento sulla policy IAM JSON nella Guida per l'utente di IAM.

Argomenti

Informazioni sulle policy di endpoint VPC

Affinché una richiesta AWS KMS che utilizza un endpoint VPC abbia esito positivo, il principale richiede autorizzazioni da due origini:

- Una policy chiave, una policy IAM o una concessione deve concedere l'autorizzazione al principale per chiamare l'operazione sulla risorsa (chiave KMS o alias).
- Una policy di endpoint VPC deve concedere l'autorizzazione al principale per utilizzare l'endpoint per effettuare la richiesta.

Ad esempio, una policy chiave potrebbe concedere al principale un'autorizzazione per chiamare Decrypt in una determinata chiave KMS. Tuttavia, la policy di endpoint VPC potrebbe non consentire a tale principale di chiamare `Decrypt` sulla chiave KMS utilizzando l'endpoint.

Oppure una policy DisableKeysugli endpoint VPC potrebbe consentire a un principale di utilizzare l'endpoint per richiamare determinate chiavi KMS. Tuttavia se il principale non dispone di tali autorizzazioni da una policy delle chiavi, una policy IAM o una concessione, la richiesta non riesce.

Policy di endpoint VPC predefinita

Ogni endpoint VPC dispone di una policy di endpoint VPC, ma non è necessario specificare la policy. Se non specifichi una policy, la policy di endpoint predefinita consente tutte le operazioni effettuate da tutte i principali su tutte le risorse dell'endpoint.

Tuttavia, per le risorse AWS KMS, il principale deve disporre anche dell'autorizzazione per richiamare l'operazione da una policy delle chiavi, una policy IAM o una concessione. Pertanto, in pratica, la policy predefinita indica che se un principale dispone dell'autorizzazione per chiamare un'operazione su una risorsa, può anche chiamarla utilizzando l'endpoint.

```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Principal": "*",
      "Resource": "*"
    }
  ]
}
```

Per permettere ai principali di utilizzare l'endpoint VPC solo per un sottoinsieme di operazioni consentite, crea o modifica la policy di endpoint VPC.

Creazione di una policy degli endpoint VPC

Una policy di endpoint VPC determina se un principale dispone dell'autorizzazione per utilizzare l'endpoint VPC per eseguire operazioni su una risorsa. Per le risorse AWS KMS, il principale deve inoltre disporre dell'autorizzazione per eseguire le operazioni da una policy delle chiavi, una policy IAM o una concessione.

Ogni istruzione della policy di endpoint VPC richiede i seguenti elementi:

- Il principale che può eseguire operazioni.
- Le azioni che possono essere eseguite
- Le risorse sui cui si possono eseguire le azioni

L'istruzione della policy non specifica l'endpoint VPC. Si applica invece a qualsiasi endpoint VPC a cui è collegata la policy. Per ulteriori informazioni, consulta Controllo degli accessi ai servizi con endpoint VPC nella Guida per l'utente di Amazon VPC.

Di seguito è riportato l'esempio di una policy di endpoint VPC per AWS KMS. Quando è collegata a un endpoint VPC, questa policy consente a `ExampleUser` di utilizzare l'endpoint VPC per chiamare le operazioni specificate sulla chiave KMS specificata. Prima di utilizzare una policy come questa, sostituisci il principale e l'ARN di chiave dell'esempio con valori validi del tuo account.

```
{
   "Statement":[
      {
         "Sid": "AllowDecryptAndView",
         "Principal": {"AWS": "arn:aws:iam::111122223333:user/ExampleUser"},
         "Effect":"Allow",
         "Action": [
             "kms:Decrypt",
             "kms:DescribeKey",
             "kms:ListAliases",
             "kms:ListKeys"
          ],
         "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
      }
   ]
}
```

AWS CloudTrail registra tutte le operazioni che utilizzano l'endpoint VPC. Tuttavia, CloudTrail i registri non includono le operazioni richieste dai responsabili in altri account o le operazioni per le chiavi KMS in altri account.

Pertanto, puoi creare una policy di endpoint VPC che impedisca ai principali negli account esterni di utilizzare l'endpoint VPC per chiamare qualsiasi operazione AWS KMS su qualsiasi chiave dell'account locale.

L'esempio seguente utilizza la chiave aws: PrincipalAccount global condition per negare l'accesso a tutti i principali per tutte le operazioni su tutte le chiavi KMS a meno che il principale non si trovi nell'account locale. Prima di utilizzare una policy come questa, sostituisci l'ID account dell'esempio con uno valido.

```
{
```

```
  "Statement": [
    {
      "Sid": "AccessForASpecificAccount",
      "Principal": {"AWS": "*"},
      "Action": "kms:*",
      "Effect": "Deny",
      "Resource": "arn:aws:kms:*:111122223333:key/*",
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalAccount": "111122223333"
        }
      }
    }
  ]
}
```

Visualizzazione di una policy di endpoint VPC

Per visualizzare la policy degli endpoint VPC per un endpoint, utilizza la console di gestione VPC o l'operazione. DescribeVpcEndpoints

Il comando AWS CLI seguente ottiene la policy per l'endpoint con l'ID endpoint VPC specificato.

Prima di eseguire questo comando, sostituisci l'ID endpoint dell'esempio con un ID valido del tuo account.

```
$ aws ec2 describe-vpc-endpoints \
--query 'VpcEndpoints[?VpcEndpointId==`vpce-1234abcdf5678c90a`].[PolicyDocument]'
--output text
```

Utilizzo di un endpoint VPC in un'istruzione di policy

Puoi controllare l'accesso alle risorse AWS KMS e alle operazioni quando la richiesta proviene dal VPC o utilizza un endpoint VPC. A tale scopo, utilizza una delle seguenti chiavi di condizione globale in una policy delle chiavi o una policy IAM.

- Usa la chiave di condizione `aws:sourceVpce` per concedere o limitare l'accesso in base all'endpoint VPC.
- Usa la chiave di condizione `aws:sourceVpc` per concedere o limitare l'accesso in base al VPC che ospita l'endpoint privato.

> **Note**
>
> Fai attenzione durante la creazione delle policy IAM e delle policy delle chiavi basate sull'endpoint VPC. Se un'istruzione di policy richiede che le richieste provengano da un determinato VPC o endpoint VPC, le richieste provenienti da servizi AWS integrati che usano una risorsa AWS KMS per tuo conto potrebbero non andare a buon fine. Per assistenza, consulta Utilizzo delle condizioni di endpoint VPC nelle policy con autorizzazioni AWS KMS. Inoltre, la chiave di condizione `aws:sourceIP` non è efficace quando la richiesta proviene da un endpoint Amazon VPC. Per limitare le richieste a un endpoint VPC, utilizza il comando `aws:sourceVpce` o le chiavi di condizione `aws:sourceVpc`. Per ulteriori informazioni, consulta la sezione Gestione delle identità e degli accessi per endpoint VPC e servizi endpoint VPC nella Guida di AWS PrivateLink.

Puoi utilizzare queste chiavi di condizione globali per controllare l'accesso a AWS KMS keys (chiavi KMS), agli alias e a operazioni del genere CreateKeyche non dipendono da alcuna risorsa particolare.

Ad esempio, la seguente policy delle chiavi di esempio consente a un utente di eseguire alcune operazioni di crittografia con una chiave KMS solo quando la richiesta utilizza l'endpoint VPC specificato. Quando un utente invia una richiesta all'endpoint VPC di AWS KMS, l'ID della richiesta viene confrontato con il valore della chiave di condizione `aws:sourceVpce` nella policy. Se non corrisponde, la richiesta viene rifiutata.

Per usare una policy come questa, sostituisci il placeholder dell'ID Account AWS e degli ID degli endpoint VPC con i valori validi per il tuo account.

```
{
    "Id": "example-key-1",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Enable IAM policies",
            "Effect": "Allow",
            "Principal": {"AWS":["111122223333"]},
            "Action": ["kms:*"],
            "Resource": "*"
        },
        {
            "Sid": "Restrict usage to my VPC endpoint",
```

```
            "Effect": "Deny",
            "Principal": "*",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:sourceVpce": "vpce-1234abcdf5678c90a"
                }
            }
        }

    ]
}
```

Puoi anche utilizzare la chiave di condizione `aws:sourceVpc` per limitare l'accesso alle tue chiavi KMS in base al VPC in cui risiede l'endpoint VPC.

I seguenti comandi di esempio della policy delle chiavi consentono i comandi che gestiscono la chiave KMS solo quando la loro provenienza è `vpc-12345678`. Inoltre, consente i comandi che utilizzano la chiave KMS per le operazioni di crittografia solo quando provengono da `vpc-2b2b2b2b`. Puoi usare una policy come questa se un'applicazione è in esecuzione in un VPC, ma devi utilizzare un secondo VPC separato per le funzioni di gestione.

Per usare una policy come questa, sostituisci il placeholder dell'ID Account AWS e degli ID degli endpoint VPC con i valori validi per il tuo account.

```
{
    "Id": "example-key-2",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow administrative actions from vpc-12345678",
            "Effect": "Allow",
            "Principal": {"AWS": "111122223333"},
            "Action": [
                "kms:Create*","kms:Enable*","kms:Put*","kms:Update*",
                "kms:Revoke*","kms:Disable*","kms:Delete*",
```

```
                "kms:TagResource", "kms:UntagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:sourceVpc": "vpc-12345678"
                }
            }
        },
        {
            "Sid": "Allow key usage from vpc-2b2b2b2b",
            "Effect": "Allow",
            "Principal": {"AWS": "111122223333"},
            "Action": [
                "kms:Encrypt","kms:Decrypt","kms:GenerateDataKey*"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:sourceVpc": "vpc-2b2b2b2b"
                }
            }
        },
        {
            "Sid": "Allow read actions from everywhere",
            "Effect": "Allow",
            "Principal": {"AWS": "111122223333"},
            "Action": [
                "kms:Describe*","kms:List*","kms:Get*"
            ],
            "Resource": "*",
        }
    ]
}
```

Registrazione dell'endpoint VPC

AWS CloudTrail registra tutte le operazioni che utilizzano l'endpoint VPC. Quando una richiesta a AWS KMS utilizza un endpoint VPC, l'ID dell'endpoint VPC appare nella voce di log AWS CloudTrail che registra la richiesta. Puoi utilizzare l'ID dell'endpoint per effettuare l'audit dell'uso dei tuoi endpoint VPC di AWS KMS.

Tuttavia, CloudTrail i registri non includono le operazioni richieste dai responsabili in altri account o le richieste di AWS KMS operazioni su chiavi KMS e alias in altri account. Inoltre, per proteggere il VPC, le richieste negate da una policy di endpoint VPC che altrimenti sarebbero state consentite, non vengono registrate in AWS CloudTrail.

Ad esempio, questa voce di log di esempio registra una richiesta GenerateDataKey che utilizza l'endpoint VPC. Il campo `vpcEndpointId` viene visualizzato alla fine della voce di log.

```
{
  "eventVersion":"1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "accountId": "111122223333",
    "userName": "Alice"
  },
  "eventTime":"2018-01-16T05:46:57Z",
  "eventSource":"kms.amazonaws.com",
  "eventName":"GenerateDataKey",
  "awsRegion":"eu-west-1",
  "sourceIPAddress":"172.01.01.001",
  "userAgent":"aws-cli/1.14.23 Python/2.7.12 Linux/4.9.75-25.55.amzn1.x86_64
 botocore/1.8.27",
  "requestParameters":{
    "keyId":"1234abcd-12ab-34cd-56ef-1234567890ab",
    "numberOfBytes":128
  },
  "responseElements":null,
  "requestID":"a9fff0bf-fa80-11e7-a13c-afcabff2f04c",
  "eventID":"77274901-88bc-4e3f-9bb6-acf1c16f6a7c",
  "readOnly":true,
  "resources":[{
    "ARN":"arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "accountId":"111122223333",
    "type":"AWS::KMS::Key"
  }],
  "eventType":"AwsApiCall",
  "recipientAccountId":"111122223333",
  "vpcEndpointId": "vpce-1234abcdf5678c90a"
```

```
}
```

Chiavi di condizione per AWS KMS

È possibile specificare le condizioni nelle politiche chiave e nelle politiche IAM che controllano l'accesso alle AWS KMS risorse. L'istruzione di policy diventa effettiva solo quando le condizioni sono true. Ad esempio, potresti decidere che un'istruzione di una policy diventi effettiva solo dopo una data specifica. In alternativa, è possibile impostare un'istruzione di policy per controllare l'accesso solo quando viene visualizzato un valore specifico in una richiesta API.

Per specificare le condizioni, puoi utilizzare le chiavi di condizione nell'elemento `Condition` di un'istruzione di policy con gli operatori della condizione IAM. Alcune chiavi di condizione si applicano in generale a AWS, altre sono specifiche a AWS KMS.

I valori delle chiavi condizionali devono rispettare i caratteri e le regole di codifica delle policy AWS KMS chiave e delle policy IAM. Per maggiori informazioni sulle regole delineate nel documento delle policy delle chiavi, consulta la sezione Formato della policy della chiave. Per informazioni dettagliate sulle regole delineate nel documento delle policy IAM, consulta la sezione Requisiti del nome IAM nella Guida per l'utente di IAM.

Argomenti

- AWS chiavi di condizione globali
- AWS KMS chiavi di condizione
- AWS KMS chiavi di condizione per AWS Nitro Enclaves

AWS chiavi di condizione globali

AWS definisce le chiavi di condizione globali, un insieme di chiavi di condizioni politiche per tutti i AWS servizi che utilizzano IAM per il controllo degli accessi. AWS KMS supporta tutte le chiavi di condizione globali. È possibile utilizzarli nelle politiche AWS KMS chiave e nelle politiche IAM.

Ad esempio, puoi utilizzare la chiave aws: PrincipalArn global condition per consentire l'accesso a una AWS KMS key (chiave KMS) solo quando il principale nella richiesta è rappresentato dall'Amazon Resource Name (ARN) nel valore della chiave di condizione. Per supportare il controllo degli accessi basato sugli attributi (ABAC) in AWS KMS, puoi utilizzare la chiave di condizione globale aws:ResourceTag/tag-key in una policy IAM per consentire l'accesso alle chiavi KMS con un tag particolare.

Per evitare che un AWS servizio venga utilizzato come sostituto confuso in una policy in cui il principale è un responsabile del AWS servizio, puoi utilizzare le chiavi di condizione o global condition. aws:SourceArnaws:SourceAccount Per informazioni dettagliate, vedi Utilizzo delle chiavi di condizione `aws:SourceArn` o `aws:SourceAccount`.

Per informazioni sulle chiavi di condizione AWS globali, inclusi i tipi di richieste in cui sono disponibili, consulta AWS Global Condition Context Keys nella IAM User Guide. Per esempi di utilizzo delle chiavi di condizione globali nelle policy IAM, consulta Controllo dell'accesso alle richieste e Controllo delle chiavi di tag nella Guida per l'utente di IAM.

Negli argomenti seguenti vengono fornite linee guida speciali per l'utilizzo delle chiavi di condizione basate su indirizzi IP e endpoint VPC.

Argomenti

- Utilizzo della condizione con indirizzo IP nelle policy con autorizzazioni AWS KMS
- Utilizzo delle condizioni di endpoint VPC nelle policy con autorizzazioni AWS KMS

Utilizzo della condizione con indirizzo IP nelle policy con autorizzazioni AWS KMS

Puoi utilizzarli AWS KMS per proteggere i tuoi dati in un AWS servizio integrato. Tuttavia, fai attenzione quando specifichi gli operatori di condizione dell'indirizzo IP o la chiave di `aws:SourceIp` condizione nella stessa dichiarazione di politica che consente o nega l'accesso. AWS KMSAd esempio, la politica in AWS: Denies Access to AWS Based on the Source IP limita AWS le azioni alle richieste provenienti dall'intervallo IP specificato.

Considera questo scenario:

1. Alleghi una policy come quella mostrata in AWS: Denies Access to AWS Based on the Source IP a un'identità IAM. Imposti il valore della chiave di condizione `aws:SourceIp` sull'intervallo di indirizzi IP per l'azienda dell'utente. Questa identità IAM ha altre policy collegate che gli consentono di utilizzare Amazon EBS, Amazon EC2 e AWS KMS.
2. L'identità cerca di collegare un volume EBS crittografato a un'istanza EC2. Questa operazione ha esito negativo con un errore di autorizzazione anche se l'utente ha l'autorizzazione a utilizzare tutti i servizi rilevanti.

La fase 2 non riesce perché la richiesta AWS KMS di decrittografia della chiave dati crittografata del volume proviene da un indirizzo IP associato all'infrastruttura Amazon EC2. Per avere successo, la richiesta deve provenire dall'indirizzo IP dell'utente di origine. Poiché la policy nella fase 1 nega

esplicitamente tutte le richieste provenienti da indirizzi IP diversi da quelli specificati, ad Amazon EC2 viene negata l'autorizzazione a decrittografare la chiave di dati crittografata del volume EBS.

Inoltre, la chiave di condizione `aws:sourceIP` non è efficace quando la richiesta proviene da un endpoint Amazon VPC. Per limitare le richieste a un endpoint VPC, incluso un endpoint VPCAWS KMS, utilizza `aws:sourceVpce` o le chiavi di condizione `aws:sourceVpc`. Per maggiori informazioni, consulta Endpoint VPC - Controllo dell'uso degli endpoint nella Guida per l'utente di Amazon VPC.

Utilizzo delle condizioni di endpoint VPC nelle policy con autorizzazioni AWS KMS

AWS KMS supporta gli endpoint Amazon Virtual Private Cloud (Amazon VPC) alimentati da. AWS PrivateLink Puoi utilizzare le seguenti chiavi di condizione globale nelle policy chiave e nelle policy IAM per controllare l'accesso alle AWS KMS risorse quando la richiesta proviene da un VPC o utilizza un endpoint VPC. Per informazioni dettagliate, vedi Utilizzo di un endpoint VPC in un'istruzione di policy.

- `aws:SourceVpc` limita l'accesso alle richieste dal VPC specificato.
- `aws:SourceVpce` limita l'accesso alle richieste dall'endpoint VPC specificato.

Se utilizzi queste chiavi condizionali per controllare l'accesso alle chiavi KMS, potresti inavvertitamente negare l'accesso ai servizi che utilizzi per AWS tuo conto. AWS KMS

Fai attenzione a evitare una situazione come quella illustrata nell'esempio delle chiavi di condizione con indirizzo IP. Se limiti le richieste di una chiave KMS a un endpoint VPC o VPC, le chiamate AWS KMS da un servizio integrato, come Amazon S3 o Amazon EBS, potrebbero non riuscire. Questo può accadere anche se la richiesta dell'origine sostanzialmente proviene dal VPC o dall'endpoint VPC.

AWS KMS chiavi di condizione

AWS KMS fornisce un set di chiavi di condizione che è possibile utilizzare nelle politiche chiave e nelle politiche IAM. Queste chiavi di condizione sono specifiche per AWS KMS. Ad esempio, puoi utilizzare la chiave di condizione `kms:EncryptionContext:`*`context-key`* per richiedere un contesto di crittografia specifico per controllare l'accesso a una chiave KMS di crittografia simmetrica.

Condizioni per una richiesta di operazione API

Molte chiavi AWS KMS condizionali controllano l'accesso a una chiave KMS in base al valore di un parametro nella richiesta di un' AWS KMS operazione. Ad esempio, puoi utilizzare la chiave kms:

KeySpec condition in una policy IAM per consentire l'uso dell'CreateKeyoperazione solo quando il valore del `KeySpec` parametro nella `CreateKey` richiesta è. `RSA_4096`

Questo tipo di condizione funziona anche quando il parametro non è presente nella richiesta, ad esempio quando si usa il valore predefinito del parametro. Ad esempio, puoi utilizzare la chiave di condizione kms:KeySpec per consentire agli utenti di usare l'operazione `CreateKey` solo quando il valore del parametro `KeySpec` è `SYMMETRIC_DEFAULT`, che è il valore predefinito. Questa condizione consente le richieste che hanno il parametro `KeySpec` con il valore `SYMMETRIC_DEFAULT` e le richieste che non hanno alcun parametro `KeySpec`.

Condizioni per le chiavi KMS utilizzate nelle operazioni API

Alcune chiavi AWS KMS condizionali possono controllare l'accesso alle operazioni in base a una proprietà della chiave KMS utilizzata nell'operazione. Ad esempio, puoi utilizzare la KeyOrigin condizione kms: per consentire ai responsabili di GenerateDataKeyrichiamare una chiave KMS solo quando la `Origin` chiave KMS è. `AWS_KMS` Per scoprire se una chiave di condizione può essere utilizzata in questo modo, osserva la descrizione della chiave di condizione.

L'operazione deve essere un'operazione delle risorse delle chiavi KMS, ossia un'operazione autorizzata per una determinata chiave KMS. Per identificare le operazioni delle risorse delle chiavi KMS, nella tabella Azioni e risorse, cerca un valore della `KMS key` nella colonna `Resources` per l'operazione. Se si utilizza questo tipo di chiave condizionale con un'operazione non autorizzata per una particolare risorsa chiave KMS, ad esempio ListKeys, l'autorizzazione non è efficace perché la condizione non può mai essere soddisfatta. Non c'è nessuna risorsa chiave KMS coinvolta nell'autorizzazione dell'operazione `ListKeys` e nessuna proprietà `KeySpec`.

Gli argomenti seguenti descrivono ogni chiave di AWS KMS condizione e includono esempi di istruzioni sulle politiche che illustrano la sintassi delle politiche.

Utilizzo di operatori con chiavi di condizione

Quando una condizione di policy confronta due set di valori, ad esempio il set di tag in una richiesta e il set di tag in una policy, è necessario spiegare AWS come confrontare i set. Per farlo, IAM definisce due operatori, `ForAnyValue` e `ForAllValues`. Utilizza gli operatori solo con le chiavi di condizione multivalore che li richiedono. Non utilizzare operatori con chiavi di condizione a valore singolo. Testa sempre in modo approfondito le istruzioni di policy prima di avvalertene in un ambiente di produzione.

Le chiavi di condizione sono a valore singolo o multivalore. Per determinare se una chiave di AWS KMS condizione è a valore singolo o multivalore, consultate la colonna Tipo di valore nella descrizione della chiave di condizione.

- Le chiavi di condizione a valore singolo hanno al massimo un valore nel contesto di autorizzazione (la richiesta o la risorsa). Ad esempio, poiché ogni chiamata API può provenire da una sola Account AWS, kms: CallerAccount è una chiave di condizione a valore singolo. Non utilizzare operatori con una chiave di condizione a valore singolo.
- Le chiavi di condizione multivalore hanno più valori nel contesto di autorizzazione (la richiesta o la risorsa). Ad esempio, poiché ogni chiave KMS può avere più alias, kms: ResourceAliases può avere più valori. Le chiavi di condizione multivalore richiedono un operatore.

Si noti che la differenza tra chiavi di condizione a valore singolo e multivalore dipende dal numero di valori nel contesto di autorizzazione e non dal numero di valori nella condizione di policy.

> **Warning**
>
> L'utilizzo di un operatore con una chiave di condizione a valore singolo può creare un'istruzione di policy eccessivamente permissiva (o eccessivamente restrittiva). Utilizza gli operatori solo con le chiavi di condizione multivalore.
> Se crei o aggiorni una politica che include un operatore `ForAllValues` set con le chiavi kms:EncryptionContext: context-key o `aws:RequestTag/`*`tag-key`* condition, AWS KMS restituisce il seguente messaggio di errore:
> `OverlyPermissiveCondition: Using the ForAllValues set operator with a single-valued condition key matches requests without the specified [encryption context or tag] or with an unspecified [encryption context or tag]. To fix, remove ForAllValues.`

Per informazioni dettagliate su `ForAnyValue` e sugli operatori `ForAllValues`, consulta Utilizzo di più chiavi e valori nella Guida per l'utente di IAM. Per informazioni sul rischio di utilizzare l'operatore *`ForAllValues`* set con una condizione a valore singolo, consulta Avviso di sicurezza: ForAllValues con chiave a valore singolo nella Guida per l'utente IAM.

Argomenti

- km: BypassPolicyLockoutSafetyCheck
- km: CallerAccount
- kms: (obsoletoCustomerMasterKeySpec)
- kms: CustomerMasterKeyUsage (obsoleto)
- km: DataKeyPairSpec

- km: EncryptionAlgorithm
- kms:: chiave contestuale EncryptionContext
- km: EncryptionContextKeys
- km: ExpirationModel
- km: GrantConstraintType
- km: GrantIsFor AWSResource
- km: GrantOperations
- km: GranteePrincipal
- km: KeyOrigin
- km: KeySpec
- km: KeyUsage
- km: MacAlgorithm
- km: MessageType
- km: MultiRegion
- km: MultiRegionKeyType
- km: PrimaryRegion
- km: ReEncryptOnSameKey
- km: RequestAlias
- km: ResourceAliases
- km: ReplicaRegion
- km: RetiringPrincipal
- km: ScheduleKeyDeletionPendingWindowInDays
- km: SigningAlgorithm
- km: ValidTo
- km: ViaService
- km: WrappingAlgorithm
- km: WrappingKeySpec

km: BypassPolicyLockoutSafetyCheck

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy
`kms:BypassPolicyLockoutSafetyCheck`	Booleano	A valore singolo	`CreateKey` `PutKeyPolicy`	Solo policy IAM Policy delle chiavi e policy IAM

Il tasto `kms:BypassPolicyLockoutSafetyCheck` condition controlla l'accesso alle PutKeyPolicyoperazioni CreateKeyand in base al valore del `BypassPolicyLockoutSafetyCheck` parametro nella richiesta.

La seguente istruzione di policy IAM di esempio impedisce agli utenti di aggirare il controllo di sicurezza di blocco della policy rifiutando l'autorizzazione a creare le chiavi KMS quando il valore del parametro `BypassPolicyLockoutSafetyCheck` nella richiesta `CreateKey` è `true`.

```
{
  "Effect": "Deny",
  "Action": [
    "kms:CreateKey",
    "kms:PutKeyPolicy"
  ],
  "Resource": "*",
  "Condition": {
    "Bool": {
      "kms:BypassPolicyLockoutSafetyCheck": true
    }
  }
}
```

È inoltre possibile utilizzare la chiave di condizione `kms:BypassPolicyLockoutSafetyCheck` in una policy IAM o della chiave per controllare l'accesso all'operazione `PutKeyPolicy`. La seguente istruzione di policy di esempio da una policy delle chiavi impedisce agli utenti di aggirare il controllo di sicurezza di blocco della policy durante la modifica della policy di una chiave KMS.

Invece di utilizzare un `Deny` esplicito, questa istruzione di policy utilizza `Allow` con l'operatore di condizione Null per consentire l'accesso solo quando la richiesta non include il parametro `BypassPolicyLockoutSafetyCheck`. Quando il parametro non viene utilizzato, il valore predefinito è `false`. Questa istruzione di policy leggermente più debole può essere sostituita nel raro caso in cui un bypass sia necessario.

```
{
  "Effect": "Allow",
  "Action": "kms:PutKeyPolicy",
  "Resource": "*",
  "Condition": {
    "Null": {
      "kms:BypassPolicyLockoutSafetyCheck": true
    }
  }
}
```

Consulta anche

- km: KeySpec
- km: KeyOrigin
- km: KeyUsage

km: CallerAccount

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy
`kms:CallerAccount`	Stringa	A valore singolo	Operazioni delle risorse delle chiavi KMS Operazioni dell'archivio delle chiavi personalizzate	Policy delle chiavi e policy IAM

È possibile utilizzare questa chiave di condizione per consentire o negare l'accesso a tutte le identità (utenti e ruoli) in un Account AWS. Nelle policy delle chiavi, è possibile utilizzare l'elemento `Principal` per specificare le identità per le quali vale l'istruzione di policy. La sintassi per l'elemento `Principal` non fornisce un modo per specificare tutte le identità in un Account AWS. Ma puoi ottenere questo effetto combinando questa chiave di condizione con un `Principal` elemento che specifica tutte le AWS identità.

È possibile utilizzarlo per controllare l'accesso a qualsiasi operazione di risorsa chiave KMS, ovvero a qualsiasi AWS KMS operazione che utilizza una particolare chiave KMS. Per identificare le operazioni delle risorse delle chiavi KMS, nella tabella Azioni e risorse, cerca un valore della `KMS key` nella colonna `Resources` per l'operazione. È valido anche per le operazioni che gestiscono gli archivi delle chiavi personalizzate.

Ad esempio, la seguente istruzione di policy chiave dimostra come utilizzare la chiave di condizione `kms:CallerAccount`. Questa dichiarazione rientra nella politica chiave Chiave gestita da AWS per Amazon EBS. Combina un `Principal` elemento che specifica tutte le AWS identità con la chiave di `kms:CallerAccount` condizione per consentire in modo efficace l'accesso a tutte le identità in 111122223333. Account AWS Contiene una chiave di AWS KMS condizione aggiuntiva (`kms:ViaService`) per limitare ulteriormente le autorizzazioni permettendo solo le richieste provenienti da Amazon EBS. Per ulteriori informazioni, consulta km: ViaService.

```
{
  "Sid": "Allow access through EBS for all principals in the account that are
 authorized to use EBS",
  "Effect": "Allow",
  "Principal": {"AWS": "*"},
  "Condition": {
    "StringEquals": {
      "kms:CallerAccount": "111122223333",
      "kms:ViaService": "ec2.us-west-2.amazonaws.com"
    }
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:CreateGrant",
    "kms:DescribeKey"
  ],
  "Resource": "*"
```

```
}
```

kms: (obsoletoCustomerMasterKeySpec)

La chiave di condizione `kms:CustomerMasterKeySpec` è obsoleta. Usa invece la chiave kms: condition. KeySpec

Le chiavi di condizione `kms:CustomerMasterKeySpec` e `kms:KeySpec` funzionano allo stesso modo. Solo i nomi differiscono. Ti consigliamo di utilizzare `kms:KeySpec`. Tuttavia, per evitare di interrompere le modifiche, AWS KMS supporta entrambe le chiavi di condizione.

kms: CustomerMasterKeyUsage (obsoleto)

La chiave di condizione `kms:CustomerMasterKeyUsage` è obsoleta. Usa invece la chiave kms: condition. KeyUsage

Le chiavi di condizione `kms:CustomerMasterKeyUsage` e `kms:KeyUsage` funzionano allo stesso modo. Solo i nomi differiscono. Ti consigliamo di utilizzare `kms:KeyUsage`. Tuttavia, per evitare di interrompere le modifiche, AWS KMS supporta entrambe le chiavi di condizione.

km: DataKeyPairSpec

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy
`kms:DataKeyPairSpec`	Stringa	A valore singolo	`GenerateDataKeyPair` `GenerateDataKeyPairWithoutPlaintext`	Policy delle chiavi e policy IAM

È possibile utilizzare questa chiave di condizione per controllare l'accesso alle GenerateDataKeyPairWithoutPlaintextoperazioni GenerateDataKeyPairand in base al valore del `KeyPairSpec` parametro nella richiesta. Ad esempio, è possibile consentire agli utenti di generare solo determinati tipi di coppie di chiavi di dati.

La seguente istruzione di policy delle chiavi di esempio utilizza la chiave di condizione `kms:DataKeyPairSpec` per consentire agli utenti di usare la chiave KMS per generare solo coppie di chiavi di dati RSA.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": [
    "kms:GenerateDataKeyPair",
    "kms:GenerateDataKeyPairWithoutPlaintext"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:DataKeyPairSpec": "RSA*"
    }
  }
}
```

Consulta anche

- km: KeySpec
- the section called “km: EncryptionAlgorithm”
- the section called “kms:: chiave contestuale EncryptionContext”
- the section called “km: EncryptionContextKeys”

km: EncryptionAlgorithm

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy

`kms:EncryptionAlgorithm`	Stringa	A valore singolo	`Decrypt`
			`Encrypt`
			`GenerateDataKey`
				Policy delle chiavi e policy IAM

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy

			`GenerateDataKeyPair`
			
			`GenerateDataKeyPairWithoutPlaintext`
			
			`GenerateDataKeyWithoutPlaintext`
			
			`ReEncrypt`	

È possibile utilizzare la chiave di condizione `kms:EncryptionAlgorithm` per controllare l'accesso alle operazioni di crittografia in base all'algoritmo di crittografia usato nell'operazione. Per le ReEncryptoperazioni Encrypt, Decrypt and, controlla l'accesso in base al valore del EncryptionAlgorithmparametro nella richiesta. Per le operazioni che generano chiavi di dati e coppie di chiavi di dati, controlla l'accesso in base all'algoritmo di crittografia utilizzato per crittografare la chiave di dati.

Questa chiave condizionale non ha alcun effetto sulle operazioni eseguite all'esterno AWS KMS, come la crittografia con la chiave pubblica in una coppia di chiavi KMS asimmetrica all'esterno di. AWS KMS

EncryptionAlgorithm parametro in una richiesta

Per consentire agli utenti di utilizzare solo un particolare algoritmo di crittografia con una chiave KMS, usa un'istruzione di policy con un effetto `Deny` e un operatore di condizione `StringNotEquals`. Ad esempio, la seguente istruzione di policy delle chiavi di esempio impedisce ai principali che possono assumere il ruolo `ExampleRole` di utilizzare questa chiave KMS nelle operazioni di crittografia specificate a meno che l'algoritmo di crittografia nella richiesta non sia `RSAES_OAEP_SHA_256`, un algoritmo di crittografia asimmetrica utilizzato con le chiavi KMS RSA.

A differenza di un'istruzione di policy che consente a un utente di utilizzare un particolare algoritmo di crittografia, un'istruzione di policy con un doppio negativo come questa impedisce ad altre policy e concessioni per questa chiave KMS di autorizzare il ruolo a utilizzare altri algoritmi di crittografia. Il `Deny` in questa istruzione di policy chiave ha la precedenza sulle policy delle chiavi o policy IAM con effetto `Allow`, nonché su tutte le concessioni per questa chiave KMS e i relativi principali.

```
{
  "Sid": "Allow only one encryption algorithm with this asymmetric KMS key",
  "Effect": "Deny",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*"
  ],
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "kms:EncryptionAlgorithm": "RSAES_OAEP_SHA_256"
    }
  }
}
```

Algoritmo di crittografia utilizzato per l'operazione

È possibile utilizzare anche la chiave di condizione `kms:EncryptionAlgorithm` per controllare l'accesso alle operazioni basate sull'algoritmo di crittografia utilizzato nell'operazione, anche quando l'algoritmo non è specificato nella richiesta. Ciò consente di richiedere o vietare l'algoritmo `SYMMETRIC_DEFAULT`, che potrebbe non essere specificato in una richiesta perché è il valore predefinito.

Questa funzione ti consente di usare la chiave di condizione `kms:EncryptionAlgorithm` per controllare l'accesso alle operazioni che generano chiavi di dati e coppie di chiavi di dati. Queste operazioni utilizzano soltanto chiavi KMS di crittografia simmetrica e l'algoritmo `SYMMETRIC_DEFAULT`.

Ad esempio, questa policy IAM limita le sue entità principali alla crittografia simmetrica. Nega l'accesso a qualsiasi chiave KMS nell'account di esempio per le operazioni di crittografia a meno che l'algoritmo di crittografia specificato nella richiesta o utilizzato

nell'operazione non sia SYMMETRIC_DEFAULT. `GenerateDataKey*`Incluse le aggiunte GenerateDataKeyGenerateDataKeyWithoutPlaintextGenerateDataKeyPair,, e GenerateDataKeyPairWithoutPlaintextalle autorizzazioni. La condizione non ha alcun effetto su queste operazioni perché utilizzano sempre un algoritmo di crittografia simmetrica.

```
{
  "Sid": "AllowOnlySymmetricAlgorithm",
  "Effect": "Deny",
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*"
  ],
  "Resource": "arn:aws:kms:us-west-2:111122223333:key/*",
  "Condition": {
    "StringNotEquals": {
      "kms:EncryptionAlgorithm": "SYMMETRIC_DEFAULT"
    }
  }
}
```

Consulta anche

- the section called “km: MacAlgorithm”
- km: SigningAlgorithm

kms:: chiave contestuale EncryptionContext

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy

`kms:EncryptionContext: context-key`	Stringa	A valore singolo	`CreateGrant`
			`Encrypt`
			`Decrypt`
			`GenerateDataKey`
				Policy delle chiavi e policy IAM

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy

			`GenerateDataKeyPair`
			
			`GenerateDataKeyPairWithoutPlaintext`
			
			`GenerateDataKeyWithoutPlaintext`
			
			`ReEncrypt`	

È possibile utilizzare la chiave di condizione `kms:EncryptionContext:`*`context-key`* per controllare l'accesso a una chiave KMS di crittografia simmetrica in base al contesto di crittografia in una richiesta per un'operazione di crittografia. Utilizza questa chiave di condizione per valutare sia la chiave sia il valore nella coppia del contesto di crittografia. Per valutare solo le chiavi del contesto di crittografia o richiedere un contesto di crittografia indipendentemente dalle chiavi o dai valori, usa la chiave kms: EncryptionContextKeys condition.

> **Note**
>
> I valori delle chiavi di condizione devono rispettare le regole sul numero di caratteri delle policy delle chiavi e delle policy IAM. Alcuni caratteri che sono validi in un contesto di crittografia non sono validi nelle policy. Potrebbe non essere possibile utilizzare questa chiave di condizione per esprimere tutti i valori validi del contesto di crittografia. Per maggiori informazioni sulle regole delineate nel documento delle policy delle chiavi, consulta la sezione Formato della policy della chiave. Per informazioni dettagliate sulle regole delineate nel documento delle policy IAM, consulta la sezione Requisiti del nome IAM nella Guida per l'utente di IAM.

Non è possibile specificare un contesto di crittografia in un'operazione di crittografia con una chiave KMS asimmetrica o una chiave KMS HMAC. Gli algoritmi asimmetrici e gli algoritmi MAC non supportano un contesto di crittografia.

Per utilizzare la chiave di condizione kms:EncryptionContext: context-key, sostituisci il segnaposto della chiave *contestuale con la chiave* di contesto di crittografia. Sostituisci il segnaposto *context-value* con il valore del contesto di crittografia.

```
"kms:EncryptionContext:context-key": "context-value"
```

Ad esempio, la seguente chiave di condizione specifica un contesto di crittografia in cui la chiave è `AppName` e il valore è `ExampleApp` (`AppName = ExampleApp`).

```
"kms:EncryptionContext:AppName": "ExampleApp"
```

Si tratta di una chiave di condizione a valore singolo. La chiave nella chiave di condizione specifica una particolare chiave di contesto di crittografia (context-key). Sebbene sia possibile includere più coppie di contesto di crittografia in ogni richiesta API, la coppia di contesto di crittografia con la context-key specificata può avere un solo valore. Ad esempio, la chiave di condizione `kms:EncryptionContext:Department` si applica solo alle coppie di contesto di crittografia con una chiave `Department` e qualsiasi coppia di contesto di crittografia data con la chiave `Department` può avere solo un valore.

Non utilizzare un operatore con la chiave di condizione `kms:EncryptionContext:`*`context-key`*. Se crei un'istruzione di policy con un'azione `Allow`, la chiave di condizione `kms:EncryptionContext:`*`context-key`* e l'operatore `ForAllValues`, la condizione consente le richieste senza contesto di crittografia e senza le richieste con coppie di contesto di crittografia che non sono specificate nella condizione di policy.

> **Warning**
>
> Non utilizzare un operatore `ForAnyValue` or `ForAllValues` con una chiave di condizione a valore singolo. Questi operatori possono creare una condizione di policy che non richiede valori che intendi richiedere e consente valori che intendi vietare.
> Se crei o aggiorni una politica che include un operatore *`ForAllValues`* set con la chiave contestuale kms::, restituisce il seguente messaggio di erroreEncryptionContext: AWS KMS `OverlyPermissiveCondition:EncryptionContext: Using the ForAllValues set operator with a single-valued condition key matches requests`

```
    without the specified encryption context or with an unspecified
    encryption context. To fix, remove ForAllValues.
```

Per richiedere una particolare coppia di contesto di crittografia, utilizzare la chiave di condizione `kms:EncryptionContext:`*`context-key`* con l'operatore `StringEquals`.

La seguente istruzione di policy chiave di esempio consente alle entità principali che possono assumere il ruolo per utilizzare la chiave KMS in una richiesta `GenerateDataKey` solo quando il contesto di crittografia nella richiesta include la coppia `AppName:ExampleApp`. Altre coppie di contesto di crittografia sono consentite.

Il nome della chiave non fa distinzione tra maiuscole e minuscole. La distinzione tra maiuscole e minuscole che fa il valore è determinata dall'operatore della condizione, ad esempio `StringEquals`. Per informazioni dettagliate, vedi Distinzione tra maiuscole e minuscole della condizione del contesto.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:AppName": "ExampleApp"
    }
  }
}
```

Per richiedere una coppia di contesti di crittografia e vietare tutte le altre coppie di contesti di crittografia, usa sia kms:EncryptionContext: context-key che nell'informativa sulla politica. `kms:EncryptionContextKeys` La seguente istruzione di policy chiave utilizza la chiave di condizione `kms:EncryptionContext:AppName` per richiedere la coppia di contesto di crittografia `AppName=ExampleApp` nella richiesta. Utilizza inoltre una chiave di condizione `kms:EncryptionContextKeys` con l'operatore `ForAllValues` per consentire solo la chiave di contesto di crittografia `AppName`.

L'operatore `ForAllValues` limita le chiavi di contesto di crittografia nella richiesta a `AppName`. Se la condizione `kms:EncryptionContextKeys` con l'operatore `ForAllValuese` è stata

utilizzata da sola in un'istruzione di policy, questo operatore consentirebbe le richieste senza contesto di crittografia. Tuttavia, se la richiesta non avesse un contesto di crittografia, la condizione `kms:EncryptionContext:AppName` avrebbe esito negativo. Per dettagli sull'operatore `ForAllValues`, consulta Utilizzo di più chiavi e valori nella Guida per l'utente di IAM.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/KeyUsers"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:AppName": "ExampleApp"
    },
    "ForAllValues:StringEquals": {
      "kms:EncryptionContextKeys": [
        "AppName"
      ]
    }
  }
}
```

È inoltre possibile utilizzare questa chiave di condizione per negare l'accesso a una chiave KMS per una determinata operazione. La seguente istruzione di policy della chiave di esempio utilizza un effetto `Deny` per impedire all'entità principale di utilizzare la chiave KMS se il contesto di crittografia nella richiesta include una coppia di contesto di crittografia `Stage=Restricted`. Questa condizione consente una richiesta con altre coppie di contesto di crittografia, incluse le coppie di contesto di crittografia con la chiave `Stage` e altri valori, come `Stage=Test`.

```
{
  "Effect": "Deny",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:Stage": "Restricted"
```

```
    }
  }
}
```

Utilizzo di più coppie di contesto di crittografia

È possibile richiedere o vietare più coppie di contesto di crittografia. È inoltre possibile richiedere una delle diverse coppie di contesto di crittografia. Per informazioni dettagliate sulla logica utilizzata per interpretare queste condizioni, consulta Creazione di una condizione con più chiavi o valori nella Guida per l'utente di IAM.

> **Note**
>
> Le versioni precedenti di questo argomento mostravano istruzioni politiche che utilizzavano *`ForAnyValue`* e *`ForAllValues`* impostavano gli operatori con la chiave di condizione kms:: EncryptionContext context-key. L'utilizzo di un operatore con una chiave di condizione a valore singolo può comportare policy che consentono richieste senza contesto di crittografia e coppie di contesto di crittografia non specificate.
> Ad esempio, una condizione di policy con l'effetto `Allow`, l'operatore `ForAllValues` e la chiave di condizione `"kms:EncryptionContext:Department": "IT"` non limita il contesto di crittografia alla coppia "Department=IT". Permette richieste senza contesto di crittografia e richieste con coppie di contesto di crittografia non specificate, come `Stage=Restricted`.
> Rivedi le tue politiche ed elimina l'operatore set da qualsiasi condizione con kms:: context-key. EncryptionContext I tentativi di creare o aggiornare una policy con questo formato hanno esito negativo con un'eccezione `OverlyPermissiveCondition`. Per risolvere il problema, è necessario eliminare l'operatore.

Per richiedere più coppie di contesto di crittografia, elenca le coppie nella stessa condizione. La seguente istruzione di policy della chiave di esempio richiede due coppie di contesto di crittografia, `Department=IT` e `Project=Alpha`. Poiché le condizioni hanno chiavi diverse (`kms:EncryptionContext:Department` and `kms:EncryptionContext:Project`), sono implicitamente collegate da un operatore AND. Altre coppie di contesto di crittografia sono consentite, ma non obbligatorie.

```
{
  "Effect": "Allow",
```

```
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:Decrypt",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:Department": "IT",
      "kms:EncryptionContext:Project": "Alpha"
    }
  }
}
```

Per richiedere una coppia di contesto di crittografia OPPURE un'altra coppia, inserire ciascuna chiave di condizione in un'istruzione di policy separata. La seguente policy chiave di esempio richiede coppie `Department=IT` o `Project=Alpha`, o entrambe. Altre coppie di contesto di crittografia sono consentite, ma non obbligatorie.

```
{
 "Effect": "Allow",
 "Principal": {
  "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
 },
 "Action": "kms:GenerateDataKey",
 "Resource": "*",
 "Condition": {
  "StringEquals": {
   "kms:EncryptionContext:Department": "IT"
  }
 }
},
{
 "Effect": "Allow",
 "Principal": {
  "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
 },
 "Action": "kms:GenerateDataKey",
 "Resource": "*",
 "Condition": {
  "StringEquals": {
   "kms:EncryptionContext:Project": "Alpha"
  }
 }
```

```
}
```

Per richiedere coppie di crittografia particolari ed escludere tutte le altre coppie di contesto di crittografia, usa sia kms:EncryptionContext: context-key che nella dichiarazione politica. `kms:EncryptionContextKeys` La seguente dichiarazione di policy chiave utilizza la condizione kms:EncryptionContext: context-key per richiedere un contesto di crittografia con entrambe le coppie. *`Department=IT`* `Project=Alpha` Utilizza una chiave di condizione `kms:EncryptionContextKeys` con l'operatore `ForAllValues` per consentire solo le chiavi di contesto di crittografia `Department` e `Project`.

L'operatore `ForAllValues` limita le chiavi di contesto di crittografia nella richiesta a `Department` e `Project`. Se fosse usato da solo in una condizione, questo operatore di set consentirebbe richieste senza contesto di crittografia, ma in questa configurazione, la chiave contestuale kms:EncryptionContext: in questa condizione fallirebbe.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:Department": "IT",
      "kms:EncryptionContext:Project": "Alpha"
    },
    "ForAllValues:StringEquals": {
      "kms:EncryptionContextKeys": [
        "Department",
        "Project"
      ]
    }
  }
}
```

È inoltre possibile vietare più coppie di contesto di crittografia. La seguente istruzione di policy della chiave di esempio utilizza un effetto `Deny` per impedire all'entità principale di utilizzare le chiavi KMS se il contesto di crittografia nella richiesta include una coppia `Stage=Restricted` o `Stage=Production`.

Valori multipli (`Restricted` e `Production`) per la stessa chiave (`kms:EncryptionContext:Stage`) sono implicitamente collegati da un'OR. Per informazioni dettagliate, consulta Logica di valutazione per condizioni con più chiavi o valori nella Guida per l'utente di IAM.

```
{
  "Effect": "Deny",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:Stage": [
         "Restricted",
         "Production"
      ]
    }
  }
}
```

Distinzione tra maiuscole e minuscole della condizione del contesto

Il contesto di crittografia specificato in un'operazione di decrittografia deve essere una corrispondenza esatta, che fa distinzione tra maiuscole e minuscole per il contesto di crittografia specificato nell'operazione di crittografia. Solo l'ordine delle coppie in un contesto di crittografia con più coppie può variare.

Tuttavia, nelle condizioni della policy, la chiave di condizione non fa distinzione tra maiuscole e minuscole. Se il valore della condizione fa distinzione tra minuscole e maiuscole viene determinato dall'operatore della condizione della policy che utilizzi, ad esempio `StringEquals` o `StringEqualsIgnoreCase`.

Per questo motivo, la chiave di condizione, che include il prefisso `kms:EncryptionContext:` e la sostituzione *`context-key`*, non fa distinzione tra minuscole e maiuscole. Una policy che utilizza questa condizione non controlla se i caratteri degli elementi della chiave di condizione sono in maiuscolo o minuscolo. Se il valore della condizione fa distinzione tra minuscole e maiuscole, ovvero la sostituzione di *`context-value`*, viene determinato dall'operatore della condizione della policy.

Ad esempio, la seguente istruzione di policy consente l'operazione quando il contesto di crittografia include una chiave Appname, senza considerare se i caratteri sono in minuscolo o maiuscolo. La condizione `StringEquals` richiede che `ExampleApp` sia scritto con caratteri maiuscoli come specificato.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:Decrypt",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:Appname": "ExampleApp"
    }
  }
}
```

Per richiedere una chiave contestuale di crittografia con distinzione tra maiuscole e minuscole, usa la condizione kms: EncryptionContextKeys policy con un operatore di condizione con distinzione tra maiuscole e minuscole, ad esempio. `StringEquals` In questa condizione della policy, poiché la chiave di contesto di crittografia è il valore della condizione della policy; la distinzione tra minuscole e maiuscole è determinata dall'operatore della condizione.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "kms:EncryptionContextKeys": "AppName"
    }
  }
}
```

Per richiedere una valutazione con distinzione tra maiuscole e minuscole sia della chiave che del valore del contesto di crittografia, utilizza insieme le condizioni della politica

`kms:EncryptionContextKeys` e kms:EncryptionContext: contestuale nella stessa dichiarazione di policy. L'operatore condizione con distinzione tra maiuscole e minuscole (come `StringEquals`) si applica sempre al valore della condizione. La chiave di contesto di crittografia (ad esempio `AppName`) è il valore della condizione `kms:EncryptionContextKeys`. Il valore del contesto di crittografia (ad esempio*`ExampleApp`*) è il valore della condizione kms:: context-key. EncryptionContext

Ad esempio, nella seguente istruzione della policy della chiave di esempio, in quanto l'operatore `StringEquals` fa distinzione tra minuscole e maiuscole, sia la chiave del contesto di crittografia sia il valore del contesto di crittografia fanno distinzione tra minuscole e maiuscole.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "kms:EncryptionContextKeys": "AppName"
    },
    "StringEquals": {
      "kms:EncryptionContext:AppName": "ExampleApp"
    }
  }
}
```

Utilizzo di variabili in una condizione del contesto di crittografia

La chiave e il valore in una coppia del contesto di crittografia devono essere stringhe letterali semplici. Non possono essere integer o oggetti o un qualsiasi tipo non completamente risolto. Se usi un tipo diverso, ad esempio un numero intero o un float, lo AWS KMS interpreta come una stringa letterale.

```
"encryptionContext": {
    "department": "10103.0"
}
```

Tuttavia, il valore della chiave di condizione `kms:EncryptionContext:`*`context-key`* può essere una variabile della policy IAM. Queste variabili di policy vengono risolte in fase di esecuzione

(runtime) in base ai valori nella richiesta. Ad esempio, `aws:CurrentTime` restituisce l'ora della richiesta e `aws:username` restituisce il nome descrittivo dell'intermediario.

Puoi utilizzare queste variabili di policy per creare un'istruzione di policy con una condizione che richiede informazioni molto specifiche in un contesto di crittografia, ad esempio il nome utente dell'intermediario. Dal momento che contiene una variabile, puoi utilizzare la stessa istruzione di policy per tutti gli utenti che possono assumere il ruolo. Non è necessario scrivere un'istruzione di policy separata per ogni utente.

Considera una situazione in cui desideri che tutti gli utenti che possono assumere un ruolo utilizzino la stessa chiave KMS per crittografare e decrittare i dati. Tuttavia, vuoi consentire loro di decrittografare solo i dati che hanno crittografato. Inizia richiedendo che ogni richiesta AWS KMS includa un contesto di crittografia in cui la chiave è `user` e il valore è il nome AWS utente del chiamante, come il seguente.

```
"encryptionContext": {
    "user": "bob"
}
```

Quindi, per applicare questo requisito, puoi utilizzare un'istruzione di policy come quella nell'esempio seguente. Questa istruzione di policy concede al ruolo `TestTeam` l'autorizzazione per crittografare e decrittare i dati con la chiave KMS. Tuttavia, l'autorizzazione è valida solo quando il contesto di crittografia nella richiesta include una coppia `"user": "`*`<username>`*`"`. Per rappresentare il nome utente, la condizione utilizza la variabile della policy `aws:username`.

Quando la richiesta viene valutata, il nome utente dell'intermediario sostituisce la variabile nella condizione. Pertanto, la condizione richiede un contesto di crittografia `"user": "bob"` per "bob" e `"user": "alice"` per "alice".

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/TestTeam"
  },
  "Action": [
    "kms:Decrypt",
    "kms:Encrypt"
  ],
  "Resource": "*",
  "Condition": {
```

```
    "StringEquals": {
      "kms:EncryptionContext:user": "${aws:username}"
    }
  }
}
```

Puoi utilizzare una variabile di policy IAM solo nel valore della coppia di chiavi di condizione `kms:EncryptionContext:`*`context-key`*. Non è possibile utilizzare una variabile nella chiave.

Puoi anche utilizzare le chiavi di contesto specifiche del provider nelle variabili. Queste chiavi di contesto identificano in modo univoco gli utenti che hanno effettuato l'accesso AWS utilizzando la federazione delle identità Web.

Come tutte le variabili, queste possono essere utilizzate solo nella condizione `kms:EncryptionContext:`*`context-key`* della policy, non nel contesto di crittografia effettivo. Inoltre, possono essere utilizzate solo nel valore della condizione, non nella chiave.

Ad esempio, la seguente istruzione della policy delle chiavi è simile a quella precedente. Tuttavia, la condizione richiede un contesto di crittografia in cui la chiave è `sub` e il valore identifica in modo univoco un utente connesso a un pool di utenti Amazon Cognito. Per dettagli sull'identificazione di utenti e ruoli in Amazon Cognito, consulta Ruoli IAM nella Guida per sviluppatori di Amazon Cognito.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/TestTeam"
  },
  "Action": [
    "kms:Decrypt",
    "kms:Encrypt"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
       "kms:EncryptionContext:sub": "${cognito-identity.amazonaws.com:sub}"
    }
  }
}
```

Consulta anche

- the section called “km: EncryptionContextKeys”

- the section called “km: GrantConstraintType”

km: EncryptionContextKeys

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy

`kms:EncryptionContextKeys`	Stringa (elenco)	Multivalore	`CreateGrant`
			`Decrypt`
			`Encrypt`
			`GenerateDataKey`
			`GenerateDataKeyPair`
			`GenerateDataKeyPairWithoutPlaintext`
			`GenerateDataKeyWithoutPlaintext`
			`ReEncrypt`
				Policy delle chiavi e policy IAM

È possibile utilizzare la chiave di condizione `kms:EncryptionContextKeys` per controllare l'accesso a una chiave KMS di crittografia simmetrica in base al contesto di crittografia in una richiesta per un'operazione di crittografia. Utilizza questa chiave di condizione per valutare solo la chiave in ciascuna coppia del contesto di crittografia. Per valutare sia la chiave sia il valore nel contesto di crittografia, usa la chiave di condizione `kms:EncryptionContext:`*`context-key`*.

Non è possibile specificare un contesto di crittografia in un'operazione di crittografia con una chiave KMS asimmetrica o una chiave KMS HMAC. Gli algoritmi asimmetrici e gli algoritmi MAC non supportano un contesto di crittografia.

> **Note**
>
> I valori delle chiavi condizionali, inclusa una chiave di contesto di crittografia, devono essere conformi ai caratteri e alle regole di codifica delle politiche AWS KMS chiave. Potrebbe non essere possibile utilizzare questa chiave di condizione per esprimere tutte le chiavi valide nel contesto di crittografia. Per maggiori informazioni sulle regole delineate nel documento delle policy delle chiavi, consulta la sezione Formato della policy della chiave. Per informazioni dettagliate sulle regole delineate nel documento delle policy IAM, consulta la sezione Requisiti del nome IAM nella Guida per l'utente di IAM.

Si tratta di una chiave di condizione multivalore. È possibile specificare più coppie di contesto di crittografia in ogni richiesta API. `kms:EncryptionContextKeys` confronta le chiavi del contesto di crittografia nella richiesta con il set di chiavi del contesto di crittografia nella policy. Per determinare il modo in cui questi set vengono confrontati, devi fornire un operatore `ForAnyValue` o `ForAllValues` nella condizione di policy. Per dettagli sugli operatori, consulta Utilizzo di più chiavi e valori nella Guida per l'utente di IAM.

- `ForAnyValue`: almeno una chiave di contesto di crittografia nella richiesta deve corrispondere a una chiave di contesto di crittografia nella condizione della policy. Sono consentite altre chiavi di contesto di crittografia. Se la richiesta non dispone di contesto di crittografia, la condizione non viene soddisfatta.
- `ForAllValues`: ogni chiave di contesto di crittografia nella richiesta deve corrispondere a una chiave di contesto di crittografia nella condizione della policy. Questo operatore limita le chiavi di contesto di crittografia a quelle nella condizione della policy. Non richiede alcuna chiave di contesto di crittografia, ma vieta le chiavi di contesto di crittografia non specificate.

La seguente istruzione di policy della chiave di esempio utilizza la chiave di condizione `kms:EncryptionContextKeys`con l'operatore `ForAnyValue`. Questa istruzione di policy utilizza una chiave KMS per le operazioni specificate, ma solo quando almeno una delle coppie del contesto di crittografia nella richiesta include la chiave `AppName`, indipendentemente dal suo valore.

Ad esempio, questa istruzione di policy chiave consente una richiesta `GenerateDataKey` con due coppie di contesto di crittografia, `AppName=Helper` e `Project=Alpha`, perché la prima coppia di contesto di crittografia soddisfa la condizione. Una richiesta con solo `Project=Alpha` o senza contesto di crittografia avrebbe esito negativo.

Poiché l'operazione di StringEqualscondizione fa distinzione tra maiuscole e minuscole, questa dichiarazione di policy richiede l'ortografia e la minuscola della chiave di contesto di crittografia. Tuttavia, è possibile utilizzare un operatore della condizione che ignora se la chiave ha caratteri in minuscolo o maiuscolo, ad esempio `StringEqualsIgnoreCase`.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": [
    "kms:Encrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "kms:EncryptionContextKeys": "AppName"
    }
  }
}
```

Inoltre, è possibile utilizzare la chiave di condizione `kms:EncryptionContextKeys` per richiedere un qualsiasi contesto di crittografia nelle operazioni di crittografia che utilizzano la chiave KMS.

La seguente istruzione di policy della chiave di esempio utilizza la chiave di condizione `kms:EncryptionContextKeys` con Null condition operator per consentire l'accesso alla chiave KMS solo quando il contesto di crittografia nella richiesta dell'API è diverso da null. Questa condizione non verifica le chiavi o i valori del contesto di crittografia. Verifica solo che il contesto di crittografia esista.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
```

```
  "Action": [
    "kms:Encrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*",
  "Condition": {
    "Null": {
      "kms:EncryptionContextKeys": false
    }
  }
}
```

Consulta anche

- kms:: chiave contestuale EncryptionContext
- km: GrantConstraintType

km: ExpirationModel

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy
`kms:ExpirationModel`	Stringa	A valore singolo	`ImportKeyMaterial`	Policy delle chiavi e policy IAM

Il tasto `kms:ExpirationModel` condition controlla l'accesso all'ImportKeyMaterialoperazione in base al valore del ExpirationModelparametro nella richiesta.

`ExpirationModel` è un parametro opzionale che determina se il materiale della chiave importato scade. I valori validi sono `KEY_MATERIAL_EXPIRES` e `KEY_MATERIAL_DOES_NOT_EXPIRE`. Il valore predefinito è `KEY_MATERIAL_EXPIRES`.

La data e l'ora di scadenza sono determinate dal valore del ValidToparametro. Il parametro `ValidTo` è obbligatorio a meno che il valore del parametro `ExpirationModel` non sia `KEY_MATERIAL_DOES_NOT_EXPIRE`. Puoi anche utilizzare la chiave kms: ValidTo condition per richiedere una data di scadenza particolare come condizione per l'accesso.

La seguente istruzione di policy di esempio utilizza la chiave di condizione `kms:ExpirationModel` per consentire agli utenti di importare materiale della chiave in una chiave KMS solo quando la richiesta include il parametro `ExpirationModel` e il suo valore è `KEY_MATERIAL_DOES_NOT_EXPIRE`.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:ImportKeyMaterial",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ExpirationModel": "KEY_MATERIAL_DOES_NOT_EXPIRE"
    }
  }
}
```

È inoltre possibile utilizzare la chiave di condizione `kms:ExpirationModel` per consentire agli utenti di importare il materiale chiave solo quando il materiale della chiave scade. La seguente istruzione di policy di esempio utilizza la chiave di condizione `kms:ExpirationModel` con Null condition operator per consentire agli utenti di importare materiale chiave solo quando la richiesta non include il parametro `ExpirationModel`. Il valore predefinito per ExpirationModel è`KEY_MATERIAL_EXPIRES`.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:ImportKeyMaterial",
  "Resource": "*",
  "Condition": {
    "Null": {
      "kms:ExpirationModel": true
    }
  }
}
```

Consulta anche

- km: ValidTo
- km: WrappingAlgorithm
- km: WrappingKeySpec

km: GrantConstraintType

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy
`kms:GrantConstraintType`	Stringa	A valore singolo	`CreateGrant`	Policy delle chiavi e policy IAM

È possibile utilizzare questa chiave di condizione per controllare l'accesso all'CreateGrantoperazione in base al tipo di vincolo di concessione nella richiesta.

Quando crei una concessione, opzionalmente è possibile specificare un vincolo di concessione per consentire le operazioni che la concessione consente solo quando è presente un determinato contesto di crittografia. Il vincolo di concessione può essere di due tipi: `EncryptionContextEquals` o `EncryptionContextSubset`. È possibile utilizzare questa chiave di condizione per controllare che la richiesta contenga uno dei due tipi.

> **Important**
>
> Non includere informazioni riservate o sensibili in questo campo. Questo campo può essere visualizzato in testo semplice nei CloudTrail log e in altri output.

La seguente istruzione di policy delle chiavi di esempio utilizza la chiave di condizione `kms:GrantConstraintType` per consentire agli utenti di creare concessioni solo quando la richiesta include un vincolo di concessione `EncryptionContextEquals`. L'esempio illustra un'istruzione di policy in una policy delle chiavi.

```
{
  "Effect": "Allow",
  "Principal": {
```

```
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:CreateGrant",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:GrantConstraintType": "EncryptionContextEquals"
    }
  }
}
```

Consulta anche

- kms:: chiave contestuale EncryptionContext
- km: EncryptionContextKeys
- km: GrantIsFor AWSResource
- km: GrantOperations
- km: GranteePrincipal
- km: RetiringPrincipal

km: GrantIsFor AWSResource

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy

`kms:GrantIsForAWSResource`	Booleano	A valore singolo	`CreateGrant`
			`ListGrants`
			`RevokeGrant`
				Policy delle chiavi e policy IAM

Consente o nega l'CreateGrantautorizzazione per RevokeGrantle operazioni solo quando un AWS servizio integrato con AWS KMS richiama l'operazione per conto dell'utente. ListGrants Questa condizione di policy non consente all'utente di chiamare direttamente queste operazioni di concessione.

La seguente istruzione di policy della chiave di esempio utilizza la chiave di condizione `kms:GrantIsForAWSResource`. Consente AWS ai servizi integrati con AWS KMS, come Amazon EBS, di creare sovvenzioni su questa chiave KMS per conto del committente specificato.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:CreateGrant",
  "Resource": "*",
  "Condition": {
    "Bool": {
      "kms:GrantIsForAWSResource": true
    }
  }
}
```

Consulta anche

- km: GrantConstraintType
- km: GrantOperations
- km: GranteePrincipal
- km: RetiringPrincipal

km: GrantOperations

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy
`kms:GrantOperations`	Stringa	Multivalore	`CreateGrant`	Policy delle chiavi e policy IAM

È possibile utilizzare questa chiave di condizione per controllare l'accesso all'CreateGrantoperazione in base alle operazioni di concessione contenute nella richiesta. Ad esempio, è possibile consentire

agli utenti di creare concessioni che delegano l'autorizzazione di crittografare ma non decrittografare. Per ulteriori informazioni sulle autorizzazioni, consulta Utilizzo di concessioni

Questa è una chiave di condizione multivalore. `kms:GrantOperations` confronta l'insieme delle operazioni di concessione nella richiesta `CreateGrant` all'insieme di operazioni di concessione nella policy. Per determinare il modo in cui questi set vengono confrontati, devi fornire un operatore `ForAnyValue` o `ForAllValues` nella condizione di policy. Per dettagli sugli operatori, consulta Utilizzo di più chiavi e valori nella Guida per l'utente di IAM.

- `ForAnyValue`: almeno un'operazione di concessione nella richiesta deve corrispondere a una delle operazioni di concessione nella condizione di policy. Sono ammesse altre operazioni di concessione.
- ForAllValues: Ogni operazione di concessione nella richiesta deve corrispondere a un'operazione di concessione nella condizione della politica. Questo operatore limita le operazioni di concessione a quelle specificate nella condizione della policy. Non richiede alcuna operazione di concessione, ma vieta le operazioni di concessione non specificate.

  ForAllValues restituisce true anche quando non ci sono operazioni di concessione nella richiesta, ma `CreateGrant` non le consente. Se il parametro `Operations` è mancante o ha un valore nullo, la richiesta `CreateGrant` ha esito negativo.

La seguente istruzione di policy delle chiavi di esempio utilizza la chiave di condizione `kms:GrantOperations` per creare concessioni solo quando le operazioni di concessione sono `Encrypt`, `ReEncryptTo` o entrambi. Se la concessione include altre operazioni, la richiesta `CreateGrant` ha esito negativo.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:CreateGrant",
  "Resource": "*",
  "Condition": {
    "ForAllValues:StringEquals": {
      "kms:GrantOperations": [
        "Encrypt",
        "ReEncryptTo"
      ]
```

```
    }
  }
}
```

Se si modifica l'operatore nella condizione di policy in `ForAnyValue`, l'istruzione di policy richiederebbe che almeno una delle operazioni di concessione nella concessione sia `Encrypt` o `ReEncryptTo`, ma consentirebbe altre operazioni di concessione, come `Decrypt` o `ReEncryptFrom`.

Consulta anche

- km: GrantConstraintType
- km: GrantIsFor AWSResource
- km: GranteePrincipal
- km: RetiringPrincipal

km: GranteePrincipal

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy
`kms:GranteePrincipal`	Stringa	A valore singolo	`CreateGrant`	Policy IAM e della chiave

È possibile utilizzare questa chiave di condizione per controllare l'accesso all'CreateGrantoperazione in base al valore del GranteePrincipalparametro nella richiesta. Ad esempio, è possibile creare autorizzazioni per utilizzare una chiave KMS solo quando il principale assegnatario nella richiesta `CreateGrant` corrisponde al principale specificato nell'istruzione della condizione.

Per specificare il principale beneficiario, utilizza l'Amazon Resource Name (ARN) di un principale. AWS I principali validi includono utenti IAM Account AWS, ruoli IAM, utenti federati e utenti assunti. Per informazioni sulla sintassi ARN per un principale, consulta IAM ARNs nella IAM User Guide.

La seguente istruzione di policy delle chiavi di esempio utilizza la chiave di condizione `kms:GranteePrincipal` per creare autorizzazioni per una chiave KMS solo quando il principale assegnatario nella concessione è `LimitedAdminRole`.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:CreateGrant",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:GranteePrincipal": "arn:aws:iam::111122223333:role/LimitedAdminRole"
    }
  }
}
```

Consulta anche

- km: GrantConstraintType
- km: GrantIsFor AWSResource
- km: GrantOperations
- km: RetiringPrincipal

km: KeyOrigin

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy
`kms:KeyOrigin`	Stringa	A valore singolo	`CreateKey` Operazioni delle risorse delle chiavi KMS	Policy IAM Policy delle chiavi e policy IAM

La chiave di condizione `kms:KeyOrigin` controlla l'accesso alle operazioni in base al valore della proprietà `Origin` della chiave KMS creata o utilizzata nell'operazione. Funziona come una condizione di risorsa o una condizione di richiesta.

È possibile utilizzare questa chiave di condizione per controllare l'accesso all'CreateKeyoperazione in base al valore del parametro Origin nella richiesta. I valori validi di `Origin` sono `AWS_KMS`, `AWS_CLOUDHSM` ed `EXTERNAL`.

Ad esempio, è possibile creare una chiave KMS solo quando il materiale chiave viene generato in AWS KMS (`AWS_KMS`), solo quando il materiale chiave viene generato in un AWS CloudHSM cluster associato a un archivio chiavi personalizzato (`AWS_CLOUDHSM`) o solo quando il materiale chiave viene importato da una fonte esterna (`EXTERNAL`).

L'esempio seguente di dichiarazione politica chiave utilizza la chiave `kms:KeyOrigin` condition per creare una chiave KMS solo quando AWS KMS crea il materiale chiave.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
      },
      "Action": "kms:CreateKey",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:KeyOrigin": "AWS_KMS"
        }
      }
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
      },
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:GenerateDataKeyPair",
        "kms:GenerateDataKeyPairWithoutPlaintext",
        "kms:ReEncrypt*"
      ],
      "Resource": "arn:aws:kms:us-west-2:111122223333:key/*",
```

```
      "Condition": {
        "StringEquals": {
          "kms:KeyOrigin": "AWS_CLOUDHSM"
        }
      }
    }
  ]
}
```

La chiave di condizione `kms:KeyOrigin` può essere utilizzata anche per controllare l'accesso alle operazioni che utilizzano o gestiscono una chiave KMS in base alla proprietà `Origin` della chiave KMS utilizzata per l'operazione. L'operazione deve essere un'operazione delle risorse delle chiavi KMS, ossia un'operazione autorizzata per una determinata chiave KMS. Per identificare le operazioni delle risorse delle chiavi KMS, nella tabella Azioni e risorse, cerca un valore della `KMS key` nella colonna `Resources` per l'operazione.

Ad esempio, la policy IAM seguente consente ai principali di eseguire le operazioni specificate sulle risorse chiave KMS, ma solo con le chiavi KMS nell'account che sono state create in un archivio chiavi personalizzato.

```
{
  "Effect": "Allow",
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:GenerateDataKey",
    "kms:GenerateDataKeyWithoutPlaintext",
    "kms:GenerateDataKeyPair",
    "kms:GenerateDataKeyPairWithoutPlaintext",
    "kms:ReEncrypt*"
  ],
  "Resource": "arn:aws:kms:us-west-2:111122223333:key/*",
  "Condition": {
    "StringEquals": {
      "kms:KeyOrigin": "AWS_CLOUDHSM"
    }
  }
}
```

Consulta anche

- km: BypassPolicyLockoutSafetyCheck

- km: KeySpec
- km: KeyUsage

km: KeySpec

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy
`kms:KeySpec`	Stringa	A valore singolo	`CreateKey` Operazioni delle risorse delle chiavi KMS	Policy IAM Policy delle chiavi e policy IAM

La chiave di condizione `kms:KeySpec` controlla l'accesso alle operazioni in base al valore della proprietà `KeySpec` della chiave KMS creata o utilizzata nell'operazione.

È possibile utilizzare questa chiave di condizione in una policy IAM per controllare l'accesso all'CreateKeyoperazione in base al valore del KeySpecparametro in una `CreateKey` richiesta. Ad esempio, puoi utilizzare questa condizione per permettere agli utenti di creare solo chiavi KMS di crittografia simmetrica o solo chiavi KMS HMAC.

La seguente istruzione di policy IAM di esempio utilizza la chiave di condizione `kms:KeySpec` per permettere ai principali di creare solo chiavi KMS asimmetriche RSA. L'autorizzazione è valida solo quando `KeySpec` nella richiesta inizia con `RSA_`.

```
{
  "Effect": "Allow",
  "Action": "kms:CreateKey",
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:KeySpec": "RSA_*"
    }
  }
}
```

La chiave di condizione `kms:KeySpec` può essere utilizzata anche per controllare l'accesso alle operazioni che utilizzano o gestiscono una chiave KMS in base alla proprietà `KeySpec` della chiave KMS utilizzata per l'operazione. L'operazione deve essere un'operazione delle risorse delle chiavi KMS, ossia un'operazione autorizzata per una determinata chiave KMS. Per identificare le operazioni delle risorse delle chiavi KMS, nella tabella Azioni e risorse, cerca un valore della `KMS key` nella colonna `Resources` per l'operazione.

Ad esempio, la policy IAM seguente permette ai principali di eseguire le operazioni specificate sulle risorse chiave KMS, ma solo con le chiavi KMS di crittografia simmetrica presenti nell'account.

```
{
  "Effect": "Allow",
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:DescribeKey"
  ],
  "Resource": "arn:aws:kms:us-west-2:111122223333:key/*",
  "Condition": {
    "StringEquals": {
      "kms:KeySpec": "SYMMETRIC_DEFAULT"
    }
  }
}
```

Consulta anche

- km: BypassPolicyLockoutSafetyCheck
- kms: (obsoletoCustomerMasterKeySpec)
- km: DataKeyPairSpec
- km: KeyOrigin
- km: KeyUsage

km: KeyUsage

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy
`kms:KeyUsage`	Stringa	A valore singolo	`CreateKey` Operazioni delle risorse delle chiavi KMS	Policy IAM Policy delle chiavi e policy IAM

La chiave di condizione `kms:KeyUsage` controlla l'accesso alle operazioni in base al valore della proprietà `KeyUsage` della chiave KMS creata o utilizzata nell'operazione.

È possibile utilizzare questa chiave di condizione per controllare l'accesso all'CreateKeyoperazione in base al valore del KeyUsageparametro nella richiesta. I valori validi di `KeyUsage` sono `ENCRYPT_DECRYPT`, `SIGN_VERIFY` ed `GENERATE_VERIFY_MAC`.

Ad esempio, puoi creare una chiave KMS solo quando `KeyUsage` è `ENCRYPT_DECRYPT` o negare l'autorizzazione a un utente quando `KeyUsage` è `SIGN_VERIFY`.

La seguente istruzione di policy IAM di esempio utilizza la chiave di condizione `kms:KeyUsage` per creare una chiave KMS solo quando `KeyUsage` è `ENCRYPT_DECRYPT`.

```
{
  "Effect": "Allow",
  "Action": "kms:CreateKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:KeyUsage": "ENCRYPT_DECRYPT"
    }
  }
}
```

La chiave di condizione `kms:KeyUsage` può essere utilizzata anche per controllare l'accesso alle operazioni che utilizzano o gestiscono una chiave KMS in base alla proprietà `KeyUsage` della chiave KMS nell'operazione. L'operazione deve essere un'operazione delle risorse delle chiavi KMS, ossia un'operazione autorizzata per una determinata chiave KMS. Per identificare le operazioni delle

risorse delle chiavi KMS, nella tabella Azioni e risorse, cerca un valore della `KMS key` nella colonna `Resources` per l'operazione.

Ad esempio, la policy IAM seguente consente ai principali di eseguire le operazioni specificate sulle risorse chiave KMS, ma solo con le chiavi KMS nell'account che vengono utilizzate per la firma e la verifica.

```
{
  "Effect": "Allow",
  "Action": [
    "kms:CreateGrant",
    "kms:DescribeKey",
    "kms:GetPublicKey",
    "kms:ScheduleKeyDeletion"
  ],
  "Resource": "arn:aws:kms:us-west-2:111122223333:key/*",
  "Condition": {
    "StringEquals": {
      "kms:KeyUsage": "SIGN_VERIFY"
    }
  }
}
```

Consulta anche

- km: BypassPolicyLockoutSafetyCheck
- kms: CustomerMasterKeyUsage (obsoleto)
- km: KeyOrigin
- km: KeySpec

km: MacAlgorithm

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy
`kms:MacAlgorithm`	Stringa	A valore singolo	`GenerateMac` `VerifyMac`	Policy delle chiavi e policy IAM

È possibile utilizzare il tasto `kms:MacAlgorithm` condition per controllare l'accesso alle VerifyMacoperazioni GenerateMacand in base al valore del `MacAlgorithm` parametro nella richiesta.

La seguente policy della chiave di esempio permette agli utenti che possono assumere il ruolo `testers` di utilizzare la chiave KMS HMAC per generare e verificare i tag HMAC solo quando l'algoritmo MAC nella richiesta è `HMAC_SHA_384` o `HMAC_SHA_512`. Questa policy utilizza due istruzioni della policy separate, ciascuna con una propria condizione. Se si specificano più algoritmi MAC in una singola istruzione di condizione, la condizione richiede entrambi gli algoritmi anziché l'uno o l'altro.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/testers"
      },
      "Action": [
        "kms:GenerateMac",
        "kms:VerifyMac"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:MacAlgorithm": "HMAC_SHA_384"
        }
      }
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/testers"
      },
      "Action": [
        "kms:GenerateMac",
        "kms:VerifyMac"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
```

```
          "kms:MacAlgorithm": "HMAC_SHA_512"
        }
      }
    }
  ]
}
```

Consulta anche

- the section called “km: EncryptionAlgorithm”
- km: SigningAlgorithm

km: MessageType

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy
`kms:MessageType`	Stringa	A valore singolo	`Sign` `Verify`	Policy delle chiavi e policy IAM

La chiave di condizione `kms:MessageType` controlla l'accesso alle operazioni Sign e Verify in base al valore del parametro `MessageType` nella richiesta. I valori validi di `MessageType` sono `RAW` e `DIGEST`.

Ad esempio, la seguente istruzione di policy delle chiavi utilizza la chiave di condizione `kms:MessageType` per utilizzare una chiave KMS asimmetrica per firmare un messaggio, ma non un digest di messaggi.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:Sign",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:MessageType": "RAW"
```

```
    }
  }
}
```

Consulta anche

- the section called “km: SigningAlgorithm”

km: MultiRegion

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy
`kms:MultiRegion`	Booleano	A valore singolo	`CreateKey` Operazioni delle risorse delle chiavi KMS	Policy delle chiavi e policy IAM

È possibile utilizzare questa chiave di condizione per consentire operazioni solo su chiavi di regione singola o solo su chiavi multiregione. Il tasto `kms:MultiRegion` condition controlla l'accesso alle AWS KMS operazioni sulle chiavi KMS e all'CreateKeyoperazione in base al valore della `MultiRegion` proprietà della chiave KMS. I valori validi sono `true` (multiregione) e `false` (singola Regione). Tutte le chiavi KMS hanno una proprietà `MultiRegion`.

Ad esempio, la seguente istruzione di policy IAM usa la chiave di condizione `kms:MultiRegion` per consentire ai principali di creare solo chiavi a singola Regione.

```
{
  "Effect": "Allow",
  "Action": "kms:CreateKey",
  "Resource": "*",
  "Condition": {
    "Bool": {
      "kms:MultiRegion": false
    }
  }
}
```

km: MultiRegionKeyType

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy
`kms:MultiRegionKeyType`	Stringa	A valore singolo	`CreateKey` Operazioni delle risorse delle chiavi KMS	Policy delle chiavi e policy IAM

È possibile utilizzare questa chiave di condizione per consentire operazioni solo su chiavi multiregione primarie o solo su chiavi multiregione di replica. Il tasto `kms:MultiRegionKeyType` condition controlla l'accesso alle AWS KMS operazioni sulle chiavi KMS e l'CreateKeyoperazione in base alla `MultiRegionKeyType` proprietà della chiave KMS. I valori validi sono `PRIMARY` e `REPLICA`. Solo le chiavi multiregione hanno una proprietà `MultiRegionKeyType`.

In genere si utilizza la chiave di condizione `kms:MultiRegionKeyType` in una policy di IAM per controllare l'accesso a più chiavi KMS. Tuttavia, poiché una determinata chiave multiregione può diventare primaria o di replica, è possibile utilizzare questa condizione in una policy chiave per consentire un'operazione solo quando la chiave multiregione specifica è una chiave primaria o di replica.

Ad esempio, la seguente istruzione di policy IAM utilizza la chiave di condizione `kms:MultiRegionKeyType` per consentire ai principali di pianificare e annullare l'eliminazione delle chiavi solo su chiavi di replica multiregione nell' Account AWSspecificato.

```
{
  "Effect": "Allow",
  "Action": [
    "kms:ScheduleKeyDeletion",
    "kms:CancelKeyDeletion"
  ],
  "Resource": "arn:aws:kms:*:111122223333:key/*",
  "Condition": {
    "StringEquals": {
      "kms:MultiRegionKeyType": "REPLICA"
    }
  }
```

```
}
```

Per consentire o negare l'accesso a tutte le chiavi multiregione, è possibile utilizzare entrambi i valori o un valore null con `kms:MultiRegionKeyType`. Tuttavia, la chiave kms: MultiRegion condition è consigliata a tale scopo.

km: PrimaryRegion

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy
`kms:PrimaryRegion`	Stringa (elenco)	A valore singolo	`UpdatePrimaryRegion`	Policy delle chiavi e policy IAM

È possibile utilizzare questa chiave di condizione per limitare le regioni di destinazione in un'UpdatePrimaryRegionoperazione. Queste sono quelle Regioni AWS che possono ospitare le tue chiavi primarie multiregionali.

Il tasto `kms:PrimaryRegion` condition controlla l'accesso all'UpdatePrimaryRegionoperazione in base al valore del `PrimaryRegion` parametro. Il `PrimaryRegion` parametro specifica la chiave Regione AWS di replica multiregionale che viene promossa a primaria. Il valore della condizione è costituito da uno o più Regione AWS nomi, ad esempio or, `us-east-1` o da schemi di denominazione delle regioni`ap-southeast-2`, ad esempio `eu-*`

Ad esempio, la seguente istruzione di policy chiave utilizza la chiave di condizione `kms:PrimaryRegion` per consentire ai principali di aggiornare la Regione primaria di una chiave multiregione in una delle quattro Regioni specificate.

```
{
  "Effect": "Allow",
  "Action": "kms:UpdatePrimaryRegion",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/Developer"
  },
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:PrimaryRegion": [
```

```
          "us-east-1",
          "us-west-2",
          "eu-west-3",
          "ap-southeast-2"
        ]
      }
    }
}
```

km: ReEncryptOnSameKey

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy
`kms:ReEncryptOnSameKey`	Booleano	A valore singolo	`ReEncrypt`	Policy delle chiavi e policy IAM

È possibile utilizzare questa chiave di condizione per controllare l'accesso all'ReEncryptoperazione a seconda che la richiesta specifichi una chiave KMS di destinazione che sia la stessa utilizzata per la crittografia originale.

Ad esempio, la seguente istruzione di policy delle chiavi utilizza la chiave di condizione `kms:ReEncryptOnSameKey` per ricrittografare solo quando la chiave KMS di destinazione corrisponde alla chiave utilizzata per la crittografia originale.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:ReEncrypt*",
  "Resource": "*",
  "Condition": {
    "Bool": {
      "kms:ReEncryptOnSameKey": true
    }
  }
}
```

km: RequestAlias

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy
`kms:RequestAlias`	Stringa (elenco)	A valore singolo	Operazioni di crittografia DescribeKey GetPublicKey	Policy delle chiavi e policy IAM

È possibile utilizzare questa chiave di condizione per consentire un'operazione solo quando la richiesta utilizza un determinato alias per identificare la chiave KMS. La chiave di condizione `kms:RequestAlias` controlla l'accesso a una chiave KMS utilizzata in un'operazione di crittografia, `GetPublicKey` oppure una `DescribeKey` basata sull'alias che identifichi la chiave KMS nella richiesta. (Questa condizione politica non ha alcun effetto sull'GenerateRandomoperazione perché l'operazione non utilizza una chiave o un alias KMS.)

Questa condizione supporta il controllo degli accessi basato sugli attributi (ABAC) in AWS KMS, che consente di controllare l'accesso alle chiavi KMS in base ai tag e agli alias di una chiave KMS. È possibile utilizzare tag e alias per consentire o negare l'accesso a una chiave KMS senza modificare policy o concessioni. Per informazioni dettagliate, vedi ABAC per AWS KMS.

Per specificare l'alias in questa condizione di policy, utilizza un nome alias, ad esempio `alias/project-alpha`, o un modello di nome alias, ad esempio `alias/*test*`. Non è possibile specificare un ARN alias nel valore di questa chiave di condizione.

Per soddisfare questa condizione, il valore del parametro `KeyId` nella richiesta deve corrispondere a un nome alias o un ARN alias. Se la richiesta utilizza un identificatore chiave, non soddisfa la condizione, anche se identifica la stessa chiave KMS.

Ad esempio, la seguente dichiarazione di politica chiave consente al principale di richiamare l'operazione sulla chiave KMS. GenerateDataKey Tuttavia questo è consentito solo quando il valore del parametro `KeyId` nella richiesta è `alias/finance-key` o un ARN alias con quel nome alias, ad esempio `arn:aws:kms:us-west-2:111122223333:alias/finance-key`.

```
{
```

```
  "Sid": "Key policy using a request alias condition",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/developer"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:RequestAlias": "alias/finance-key"
    }
  }
}
```

Non è possibile utilizzare questa chiave di condizione per controllare l'accesso alle operazioni di alias, come CreateAliaso. DeleteAlias Per informazioni sul controllo dell'accesso a tutte le operazioni alias, consulta Controllo dell'accesso agli alias.

km: ResourceAliases

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy
`kms:ResourceAliases`	Stringa (elenco)	Multivalore	Operazioni delle risorse delle chiavi KMS	Solo policy IAM

Utilizza questa chiave di condizione per controllare l'accesso a una chiave KMS in base agli alias associati alla chiave KMS. L'operazione deve essere un'operazione delle risorse delle chiavi KMS, ossia un'operazione autorizzata per una determinata chiave KMS. Per identificare le operazioni delle risorse delle chiavi KMS, nella tabella Azioni e risorse, cerca un valore della `KMS key` nella colonna `Resources` per l'operazione.

Questa condizione supporta il controllo degli accessi basato su attributi (ABAC) in AWS KMS. Con ABAC è possibile controllare l'accesso alle chiavi KMS in base ai tag assegnati a una chiaveKMS e agli alias associati a una chiave KMS. È possibile utilizzare tag e alias per consentire o negare l'accesso a una chiave KMS senza modificare policy o concessioni. Per informazioni dettagliate, vedi ABAC per AWS KMS.

Un alias deve essere univoco in una regione Account AWS and, ma questa condizione consente di controllare l'accesso a più chiavi KMS nella stessa regione (utilizzando l'operatore Regioni AWS di `StringLike` confronto) o a più chiavi KMS in diversi account.

> **Note**
>
> La ResourceAliases condizione kms: è efficace solo quando la chiave KMS è conforme agli alias per quota di chiavi KMS. Se una chiave KMS supera questa quota, alle entità principali autorizzate a usare la chiave KMS tramite la condizione `kms:ResourceAliases` viene negato l'accesso alla chiave KMS.

Per specificare l'alias in questa condizione di policy, utilizza un nome alias, ad esempio `alias/project-alpha`, o un modello di nome alias, ad esempio `alias/*test*`. Non è possibile specificare un ARN alias nel valore di questa chiave di condizione. Per soddisfare la condizione, la chiave KMS utilizzata nell'operazione deve avere l'alias specificato. Non importa se o come la chiave KMS viene identificata nella richiesta per l'operazione.

Si tratta di una chiave di condizione multivalore che confronta il set di alias associato a una chiave KMS con il set di alias nella policy. Per determinare il modo in cui questi set vengono confrontati, devi fornire un operatore `ForAnyValue` o `ForAllValues` nella condizione di policy. Per dettagli sugli operatori, consulta Utilizzo di più chiavi e valori nella Guida per l'utente di IAM.

- ForAnyValue: Almeno un alias associato alla chiave KMS deve corrispondere a un alias nella condizione della politica. Sono consentiti altri alias. Se la chiave KMS non dispone di alias, la condizione non viene soddisfatta.
- ForAllValues: Ogni alias associato alla chiave KMS deve corrispondere a un alias nella politica. Questo operatore limita gli alias associati alla chiave KMS a quelli nella condizione della policy. Non richiede alcun alias, ma vieta alias non specificati.

Ad esempio, la seguente dichiarazione di policy IAM consente al principale di richiamare l'GenerateDataKeyoperazione su qualsiasi chiave KMS specificata Account AWS associata all'alias. `finance-key` (Le policy chiave delle chiavi KMS interessate devono inoltre consentire all'account del principale di utilizzarle per questa operazione.) Per indicare che la condizione è soddisfatta quando uno dei molti alias che potrebbero essere associati alla chiave KMS è `alias/finance-key`, la condizione utilizza il set di operatori `ForAnyValue`.

Poiché la condizione `kms:ResourceAliases` si basa sulla risorsa, non sulla richiesta, una chiamata a `GenerateDataKey` ha esito positivo per qualsiasi chiave KMS associata all'alias `finance-key`, anche se la richiesta utilizza un ID chiave o un ARN della chiave per identificare la chiave KMS.

```
{
  "Sid": "AliasBasedIAMPolicy",
  "Effect": "Allow",
  "Action": "kms:GenerateDataKey",
  "Resource": [
    "arn:aws:kms:*:111122223333:key/*",
    "arn:aws:kms:*:444455556666:key/*"
  ],
  "Condition": {
    "ForAnyValue:StringEquals": {
      "kms:ResourceAliases": "alias/finance-key"
    }
  }
}
```

L'istruzione della policy IAM di esempio seguente consente all'entità principale di abilitare e disabilitare le chiavi KMS, ma solo quando tutti gli alias delle chiavi KMS includono "`Test`"». Questa istruzione di policy utilizza due condizioni. La condizione con l'operatore `ForAllValues` richiede che tutti gli alias associati alla chiave KMS includano "Test". La condizione con l'operatore `ForAnyValue` richiede che la chiave KMS abbia almeno un alias con "Test". Senza la condizione `ForAnyValue`, questa istruzione di policy consentirebbe all'entità principaledi utilizzare chiavi KMS prive di alias.

```
{
  "Sid": "AliasBasedIAMPolicy",
  "Effect": "Allow",
  "Action": [
    "kms:EnableKey",
    "kms:DisableKey"
  ],
  "Resource": "arn:aws:kms:*:111122223333:key/*",
  "Condition": {
    "ForAllValues:StringLike": {
      "kms:ResourceAliases": [
        "alias/*Test*"
      ]
    },
```

```
    "ForAnyValue:StringLike": {
      "kms:ResourceAliases": [
        "alias/*Test*"
      ]
    }
  }
}
```

km: ReplicaRegion

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy
`kms:ReplicaRegion`	Stringa (elenco)	A valore singolo	`ReplicateKey`	Policy delle chiavi e policy IAM

È possibile utilizzare questa chiave di condizione per limitare il numero Regioni AWS in cui un principale può replicare una chiave multiregionale. La chiave `kms:ReplicaRegion` condizionale controlla l'accesso all'ReplicateKeyoperazione in base al valore del ReplicaRegionparametro nella richiesta. Questo parametro specifica la Regione AWS per la nuova Chiave di replica.

Il valore della condizione è costituito da uno o più Regione AWS nomi, ad esempio `us-east-1` o`ap-southeast-2`, o da modelli di nomi, ad esempio`eu-*`. Per un elenco dei nomi di tali Regioni AWS AWS KMS supporti, consulta AWS Key Management Service endpoints e quote in. Riferimenti generali di AWS

Ad esempio, la seguente dichiarazione di politica chiave utilizza la chiave `kms:ReplicaRegion` condition per consentire ai principali di richiamare l'ReplicateKeyoperazione solo quando il valore del `ReplicaRegion` parametro è una delle regioni specificate.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/Administrator"
  },
  "Action": "kms:ReplicateKey"
  "Resource": "*",
  "Condition": {
```

```
    "StringEquals": {
      "kms:ReplicaRegion": [
         "us-east-1",
         "eu-west-3",
         "ap-southeast-2"
      ]
    }
  }
}
```

Questa chiave condizionale controlla l'accesso solo all'ReplicateKeyoperazione. Per controllare l'accesso all'UpdatePrimaryRegionoperazione, usa il tasto kms: PrimaryRegion condition.

km: RetiringPrincipal

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy
`kms:RetiringPrincipal`	Stringa (elenco)	A valore singolo	`CreateGrant`	Policy delle chiavi e policy IAM

È possibile utilizzare questa chiave di condizione per controllare l'accesso all'CreateGrantoperazione in base al valore del RetiringPrincipalparametro nella richiesta. Ad esempio, puoi creare autorizzazioni per utilizzare una chiave KMS solo quando `RetiringPrincipal` nella richiesta `CreateGrant` corrisponde a `RetiringPrincipal` nell'istruzione della condizione.

Per specificare il principale che va in pensione, utilizza l'Amazon Resource Name (ARN) di AWS un principale. I principali validi includono utenti IAM Account AWS, ruoli IAM, utenti federati e utenti assunti. Per informazioni sulla sintassi ARN per un principale, consulta IAM ARNs nella IAM User Guide.

L'esempio seguente di dichiarazione politica chiave consente a un utente di creare concessioni per la chiave KMS. La chiave `kms:RetiringPrincipal` condizionale limita l'autorizzazione alle `CreateGrant` richieste in cui il principale beneficiario della concessione ritirante è il. `LimitedAdminRole`

```
{
```

```
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:CreateGrant",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:RetiringPrincipal": "arn:aws:iam::111122223333:role/LimitedAdminRole"
    }
  }
}
```

Consulta anche

- km: GrantConstraintType
- km: GrantIsFor AWSResource
- km: GrantOperations
- km: GranteePrincipal

km: ScheduleKeyDeletionPendingWindowInDays

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy
`kms:ScheduleKeyDeletionPendingWindowInDays`	Numerico	A valore singolo	`ScheduleKeyDeletion`	Policy delle chiavi e policy IAM

È possibile utilizzare questa chiave di condizione per limitare i valori che i principali possono specificare nel `PendingWindowInDays` parametro di una ScheduleKeyDeletionrichiesta.

`PendingWindowInDays`Speciifica il numero di giorni che AWS KMS attendono prima di eliminare una chiave. AWS KMS consente di specificare un periodo di attesa compreso tra 7 e 30 giorni, ma è possibile utilizzare la chiave di `kms:ScheduleKeyDeletionPendingWindowInDays` condizione

per limitare ulteriormente il periodo di attesa, ad esempio imporre un periodo di attesa minimo entro l'intervallo valido.

Ad esempio, la seguente istruzione della policy della chiave utilizza la chiave di condizione `kms:ScheduleKeyDeletionPendingWindowInDays` per impedire ai principali di pianificare l'eliminazione della chiave se il periodo di attesa è minore o uguale a 21 giorni.

```
{
  "Effect": "Deny",
  "Action": "kms:ScheduleKeyDeletion",
  "Principal": "*",
  "Resource": "*",
  "Condition" : {
      "NumericLessThanEquals" : {
        "kms:ScheduleKeyDeletionPendingWindowInDays" : "21"
      }
  }
}
```

km: SigningAlgorithm

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy
`kms:SigningAlgorithm`	Stringa	A valore singolo	`Sign` `Verify`	Policy delle chiavi e policy IAM

È possibile utilizzare il tasto `kms:SigningAlgorithm` condition per controllare l'accesso alle operazioni di firma e verifica in base al valore del SigningAlgorithmparametro nella richiesta. Questa chiave condizionale non ha effetto sulle operazioni eseguite all'esterno AWS KMS, come la verifica delle firme con la chiave pubblica in una coppia di chiavi KMS asimmetrica all'esterno di. AWS KMS

La seguente policy delle chiavi di esempio consente agli utenti che possono assumere il ruolo `testers` di utilizzare la chiave KMS per firmare i messaggi solo quando l'algoritmo di firma utilizzato per la richiesta è un algoritmo RSASSA_PSS, ad esempio `RSASSA_PSS_SHA512`.

```
{
```

```
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/testers"
  },
  "Action": "kms:Sign",
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:SigningAlgorithm": "RSASSA_PSS*"
    }
  }
}
```

Consulta anche

- km: EncryptionAlgorithm
- the section called “km: MacAlgorithm”
- the section called “km: MessageType”

km: ValidTo

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy
`kms:ValidTo`	Timestamp	A valore singolo	`ImportKeyMaterial`	Policy delle chiavi e policy IAM

Il tasto `kms:ValidTo` condition controlla l'accesso all'ImportKeyMaterialoperazione in base al valore del ValidToparametro nella richiesta, che determina quando scade il materiale chiave importato. Il valore viene espresso in formato Unix.

Come impostazione predefinita, il parametro `ValidTo` è obbligatorio in una richiesta `ImportKeyMaterial`. Tuttavia, se il valore del ExpirationModelparametro è`KEY_MATERIAL_DOES_NOT_EXPIRE`, il `ValidTo` parametro non è valido. Puoi anche usare la chiave kms: ExpirationModel condition per richiedere il `ExpirationModel` parametro o un valore di parametro specifico.

La seguente istruzione di policy di esempio consente a un utente di importare il materiale della chiave in una chiave KMS. La chiave di condizione `kms:ValidTo` limita l'autorizzazione alle richieste `ImportKeyMaterial` nelle quali il valore `ValidTo` è minore o uguale a `1546257599.0` (31 dicembre 2018, 23:59:59).

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:ImportKeyMaterial",
  "Resource": "*",
  "Condition": {
    "NumericLessThanEquals": {
      "kms:ValidTo": "1546257599.0"
    }
  }
}
```

Consulta anche

- km: ExpirationModel
- km: WrappingAlgorithm
- km: WrappingKeySpec

km: ViaService

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy
`kms:ViaService`	Stringa	A valore singolo	Operazioni delle risorse delle chiavi KMS	Policy delle chiavi e policy IAM

La chiave `kms:ViaService` condition limita l'uso di una chiave KMS alle richieste provenienti da AWS servizi specifici. È possibile specificare uno o più servizi in ciascuna chiave di condizione `kms:ViaService`. L'operazione deve essere un'operazione delle risorse delle chiavi KMS, ossia

un'operazione autorizzata per una determinata chiave KMS. Per identificare le operazioni delle risorse delle chiavi KMS, nella tabella Azioni e risorse, cerca un valore della `KMS key` nella colonna `Resources` per l'operazione.

Ad esempio, la seguente istruzione di una policy chiave utilizza la chiave di condizione `kms:ViaService` per consentire l'utilizzo di una chiave gestita dal cliente per le azioni specificate solo quando la richiesta proviene da Amazon EC2 o Amazon RDS nella Regione Stati Uniti occidentali (Oregon) per conto di `ExampleRole`.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:CreateGrant",
    "kms:ListGrants",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ViaService": [
        "ec2.us-west-2.amazonaws.com",
        "rds.us-west-2.amazonaws.com"
      ]
    }
  }
}
```

Puoi inoltre utilizzare una chiave di condizione `kms:ViaService` per negare l'autorizzazione a utilizzare una chiave KMS quando la richiesta proviene da determinati servizi. Ad esempio, la seguente istruzione di policy da una policy delle chiavi utilizza una chiave di condizione `kms:ViaService` per evitare che una chiave gestita dal cliente venga utilizzata per le operazioni `Encrypt` quando la richiesta proviene da AWS Lambda per conto di `ExampleRole`.

```
{
```

```
  "Effect": "Deny",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": [
    "kms:Encrypt"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ViaService": [
          "lambda.us-west-2.amazonaws.com"
      ]
    }
  }
}
```

Important

Quando si utilizza la chiave di condizione `kms:ViaService`, il servizio effettua la richiesta per conto di un principale in Account AWS. Questi principali devono disporre delle autorizzazioni seguenti:

- Autorizzazione a utilizzare la chiave KMS. Il principale deve concedere le autorizzazioni al servizio integrato in modo che il servizio possa utilizzare la chiave gestita dal cliente per conto del principale. Per ulteriori informazioni, consulta In che modo i servizi AWS utilizzano AWS KMS.
- Autorizzazione a utilizzare il servizio integrato. Per informazioni dettagliate su come fornire agli utenti l'accesso a un AWS servizio che si integra con AWS KMS, consulta la documentazione del servizio integrato.

Tutte le Chiavi gestite da AWS utilizzano una chiave di condizione `kms:ViaService` nel documento della policy delle chiavi. Questa condizione consente alla chiave KMS di essere utilizzata solo per le richieste che provengono dal servizio che ha creato la chiave KMS. Per vedere la politica chiave di an Chiave gestita da AWS, usa l'GetKeyPolicyoperazione.

La chiave di condizione `kms:ViaService` è valida nelle istruzioni IAM e della policy delle chiavi. I servizi specificati devono essere integrati con AWS KMS e supportare la chiave di condizione `kms:ViaService`.

I servizi che supportano la chiave di condizione **`kms:ViaService`**

La tabella seguente elenca AWS i servizi che sono integrati AWS KMS e supportano l'uso della chiave di `kms:ViaService` condizione nelle chiavi gestite dal cliente. I servizi in questa tabella potrebbero non essere disponibili in tutte le aree. Utilizza il `.amazonaws.com` suffisso del AWS KMS ViaService nome in tutte le AWS partizioni.

> **Note**
>
> Potrebbe essere necessario scorrere orizzontalmente o verticalmente per visualizzare tutti i dati di questa tabella.

Nome servizio	AWS KMS ViaService nome
AWS App Runner	`apprunner.` *`AWS_region`* `.amazonaws.com`
AWS AppFabric	`appfabric.` *`AWS_region`* `.amazonaws.com`
Amazon AppFlow	`appflow.`*`AWS_region`* `.amazonaws.com`
AWS Application Migration Service	`mgn.`*`AWS_region`* `.amazonaws.com`
Amazon Athena	`athena.`*`AWS_region`* `.amazonaws.com`
AWS Audit Manager	`auditmanager.` *`AWS_region`* `.amazonaws.com`
Amazon Aurora	`rds.`*`AWS_region`* `.amazonaws.com`
AWS Backup	`backup.`*`AWS_region`* `.amazonaws.com`
AWS Backup Gateway	`backup-gateway.` *`AWS_region`* `.amazonaws.com`
SDK Amazon Chime	`chimevoiceconnector.` *`AWS_region`* `.amazonaws.com`

Nome servizio	AWS KMS ViaService nome
AWS CodeArtifact	`codeartifact.` *`AWS_region`* `.amazonaws.com`
CodeGuru Revisore Amazon	`codeguru-reviewer.` *`AWS_region`* `.amazonaws.com`
Amazon Comprehend	`comprehend.` *`AWS_region`* `.amazonaws.com`
Amazon Connect	`connect.`*`AWS_region`* `.amazonaws.com`
Customer Profiles Amazon Connect	`profile.`*`AWS_region`* `.amazonaws.com`
Amazon Q in Connect	`wisdom.`*`AWS_region`* `.amazonaws.com`
AWS Database Migration Service (AWS DMS)	`dms.`*`AWS_region`* `.amazonaws.com`
AWS Directory Service	`directoryservice.` *`AWS_region`* `.amazonaws.com`
Amazon DynamoDB	`dynamodb.` *`AWS_region`* `.amazonaws.com`
Amazon DocumentDB	`docdb-elastic.` *`AWS_region`* `.amazonaws.com`
Amazon EC2 Systems Manager (SSM)	`ssm.`*`AWS_region`* `.amazonaws.com`
Amazon Elastic Block Store (Amazon EBS)	`ec2.`*`AWS_region`* `.amazonaws.com` (solo EBS)
Amazon Elastic Container Registry (Amazon ECR)	`ecr.`*`AWS_region`* `.amazonaws.com`
Amazon Elastic File System (Amazon EFS)	`elasticfilesystem.` *`AWS_region`* `.amazonaws.com`

Nome servizio	AWS KMS ViaService nome
Amazon ElastiCache	Includi entrambi ViaService i nomi nel valore della chiave condizionale: • elasticache. *AWS_region* .amazonaws.com • dax.*AWS_region* .amazonaws.com
AWS Elemental MediaTailor	mediatailor. *AWS_region* .amazonaws.com
AWS Risoluzione dell'entità	entityresolution. *AWS_region* .amazonaws.com
Amazon FinSpace	finspace. *AWS_region* .amazonaws.com
Amazon Forecast	forecast. *AWS_region* .amazonaws.com
Amazon FSx	fsx.*AWS_region* .amazonaws.com
AWS Glue	glue.*AWS_region* .amazonaws.com
AWS Ground Station	groundstation. *AWS_region* .amazonaws.com
Amazon GuardDuty	malware-protection. *AWS_region* .amazonaws.com
AWS HealthLake	healthlake. *AWS_region* .amazonaws.com
AWS IoT SiteWise	iotsitewise. *AWS_region* .amazonaws.com
Amazon Kendra	kendra.*AWS_region* .amazonaws.com

Nome servizio	AWS KMS ViaService nome
Amazon Keyspaces (per Apache Cassandra)	`cassandra.` *`AWS_region`* `.amazonaws.com`
Amazon Kinesis	`kinesis.`*`AWS_region`*` .amazonaws.com`
Amazon Data Firehose	`firehose.` *`AWS_region`* `.amazonaws.com`
Flusso di video Amazon Kinesis	`kinesisvideo.` *`AWS_region`* `.amazonaws.com`
AWS Lambda	`lambda.`*`AWS_region`*` .amazonaws.com`
Amazon Lex	`lex.`*`AWS_region`*` .amazonaws.com`
AWS License Manager	`license-manager.` *`AWS_region`* `.amazonaws.com`
Servizio di posizione Amazon	`geo.`*`AWS_region`*` .amazonaws.com`
Amazon Lookout per le apparecchiature	`lookoutequipment.` *`AWS_region`* `.amazonaws.com`
Amazon Lookout per le metriche	`lookoutmetrics.` *`AWS_region`* `.amazonaws.com`
Amazon Lookout per Vision	`lookoutvision.` *`AWS_region`* `.amazonaws.com`
Amazon Macie	`macie.`*`AWS_region`*` .amazonaws.com`
AWS Mainframe Modernization	`m2.`*`AWS_region`*` .amazonaws.com`
Blockchain gestita da Amazon	`managedblockchain.` *`AWS_region`* `.amazonaws.com`
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	`kafka.`*`AWS_region`*` .amazonaws.com`

Nome servizio	AWS KMS ViaService nome
Amazon Managed Workflows for Apache Airflow (MWAA)	`airflow.AWS_region .amazonaws.com`
Amazon MemoryDB per Redis	`memorydb. AWS_region .amazonaws.com`
Amazon Monitron	`monitron. AWS_region .amazonaws.com`
Amazon MQ	`mq.AWS_region .amazonaws.com`
Amazon Neptune	`rds.AWS_region .amazonaws.com`
Amazon Nimble Studio	`nimble.AWS_region .amazonaws.com`
AWS HealthOmics	`omics.AWS_region .amazonaws.com`
OpenSearch Servizio Amazon	`es.AWS_region .amazonaws.com , aoss.AWS_region .amazonaws.com`
AWS Proton	`proton.AWS_region .amazonaws.com`
Database Amazon Quantum Ledger (Amazon QLDB)	`qldb.AWS_region .amazonaws.com`
Performance Insights di Amazon RDS	`rds.AWS_region .amazonaws.com`
Amazon Redshift	`redshift. AWS_region .amazonaws.com`
Editor di query Amazon Redshift V2	`sqlworkbench. AWS_region .amazonaws.com`
Amazon Redshift Serverless	`redshift-serverless. AWS_region .amazonaws.com`
Amazon Rekognition	`rekognition. AWS_region .amazonaws.com`

Nome servizio	AWS KMS ViaService nome
Amazon Relational Database Service (Amazon RDS)	`rds.`*`AWS_region`*` .amazonaws.com`
Datastore replicato di Amazon	`ards.`*`AWS_region`*` .amazonaws.com`
Amazon SageMaker	`sagemaker.`*`AWS_region`*` .amazonaws.com`
AWS Secrets Manager	`secretsmanager.`*`AWS_region`*` .amazonaws.com`
Amazon Security Lake	`securitylake.`*`AWS_region`*` .amazonaws.com`
Amazon Simple Email Service (Amazon SES)	`ses.`*`AWS_region`*` .amazonaws.com`
Servizio di notifica semplice Amazon (Amazon Simple Notification Service (Amazon SNS))	`sns.`*`AWS_region`*` .amazonaws.com`
Amazon Simple Queue Service (Amazon SQS)	`sqs.`*`AWS_region`*` .amazonaws.com`
Amazon Simple Storage Service (Amazon S3)	`s3.`*`AWS_region`*` .amazonaws.com`
AWS Snowball	`importexport.`*`AWS_region`*` .amazonaws.com`
AWS Storage Gateway	`storagegateway.`*`AWS_region`*` .amazonaws.com`
AWS Systems Manager Incident Manager	`ssm-incidents.`*`AWS_region`*` .amazonaws.com`
AWS Systems Manager Incident Manager Contatti	`ssm-contacts.`*`AWS_region`*` .amazonaws.com`
Amazon Timestream	`timestream.`*`AWS_region`*` .amazonaws.com`

Nome servizio	AWS KMS ViaService nome
Amazon Translate	`translate.` *`AWS_region`* `.amazonaws.com`
Accesso verificato da AWS	`verified-access.` *`AWS_region`* `.amazonaws.com`
Amazon WorkMail	`workmail.` *`AWS_region`* `.amazonaws.com`
Amazon WorkSpaces	`workspaces.` *`AWS_region`* `.amazonaws.com`
Amazon WorkSpaces Thin Client	`thinclient.` *`AWS_region`* `.amazonaws.com`
Amazon WorkSpaces Web	`workspaces-web.` *`AWS_region`* `.amazonaws.com`
AWS X-Ray	`xray.`*`AWS_region`* `.amazonaws.com`

km: WrappingAlgorithm

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy
`kms:WrappingAlgorithm`	Stringa	A valore singolo	`GetParametersForImport`	Policy delle chiavi e policy IAM

Questa chiave di condizione controlla l'accesso all'GetParametersForImportoperazione in base al valore del WrappingAlgorithmparametro nella richiesta. È possibile utilizzare questa condizione per richiedere che i principali utilizzino un determinato algoritmo per crittografare il materiale chiave durante il processo di importazione. Le richieste della chiave pubblica e del token di importazione non riescono se viene specificato un diverso algoritmo di wrapping.

La seguente istruzione di policy chiave di esempio utilizza la chiave di condizione `kms:WrappingAlgorithm` per fornire all'utente l'autorizzazione a richiamare l'operazione `GetParametersForImport`, ma gli impedisce di utilizzare l'algoritmo di wrapping `RSAES_OAEP_SHA_1`. Quando `WrappingAlgorithm` nella richiesta `GetParametersForImport` è`RSAES_OAEP_SHA_1`, l'operazione non riesce.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:GetParametersForImport",
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "kms:WrappingAlgorithm": "RSAES_OAEP_SHA_1"
    }
  }
}
```

Consulta anche

- km: ExpirationModel
- km: ValidTo
- km: WrappingKeySpec

km: WrappingKeySpec

AWS KMS chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy
`kms:WrappingKeySpec`	Stringa	A valore singolo	`GetParametersForImport`	Policy delle chiavi e policy IAM

Questa chiave di condizione controlla l'accesso all'GetParametersForImportoperazione in base al valore del WrappingKeySpecparametro nella richiesta. È possibile utilizzare questa condizione per

richiedere che i principali utilizzino un determinato tipo di chiave pubblica durante il processo di importazione. Se la richiesta specifica un tipo di chiave diversa, ha esito negativo.

Poiché l'unico valore valido per il valore del parametro `WrappingKeySpec` è `RSA_2048`, impedendo agli utenti di utilizzare questo valore efficacemente, si impedisce loro di utilizzare l'operazione `GetParametersForImport`.

La seguente istruzione di policy di esempio utilizza la chiave di condizione `kms:WrappingAlgorithm` per richiedere che `WrappingKeySpec` nella richiesta sia `RSA_4096`.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:GetParametersForImport",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:WrappingKeySpec": "RSA_4096"
    }
  }
}
```

Consulta anche

- km: ExpirationModel
- km: ValidTo
- km: WrappingAlgorithm

AWS KMS chiavi di condizione per AWS Nitro Enclaves

AWS Nitro Enclaves è una funzionalità di Amazon EC2 che consente di creare ambienti di elaborazione isolati chiamati enclavi per proteggere ed elaborare dati altamente sensibili. AWS KMS fornisce chiavi di condizione per supportare Nitro Enclaves. AWS Queste chiavi di condizioni sono valide solo per le richieste di Nitro AWS KMS Enclave.

Quando richiami le operazioni Decrypt o GenerateRandomAPI con il documento di attestazione firmato da un'enclave, queste API crittografano il testo in chiaro nella risposta utilizzando la

chiave pubblica del documento di attestazione e restituiscono testo cifrato anziché testo semplice. GenerateDataKeyGenerateDataKeyPair Questo testo criptato può essere decrittato solo utilizzando la chiave privata nell'enclave. Per ulteriori informazioni, consulta Come AWS Nitro Enclaves usa AWS KMS.

Le seguenti chiavi di condizione consentono di limitare le autorizzazioni per queste operazioni in base al contenuto del documento di attestazione firmato. Prima di consentire un'operazione, AWS KMS confronta il documento di attestazione dell'enclave con i valori di queste chiavi di condizione. AWS KMS

km: 384 RecipientAttestation ImageSha

AWS KMS Chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy

`kms:RecipientAttestation:ImageSha384`	Stringa	A valore singolo	`Decrypt`
			`GenerateDataKey`
			`GenerateDataKeyPair`
			`GenerateRandom`
				Policy delle chiavi e policy IAM

La chiave di condizione `kms:RecipientAttestation:ImageSha384` controlla l'accesso a `Decrypt`, `GenerateDataKey`, `GenerateDataKeyPair` e `GenerateRandom` con una chiave KMS quando il digest immagine del documento di attestazione firmato nella richiesta corrisponde al valore nella chiave di condizione. Il valore `ImageSha384` corrisponde a PCR0 nel documento di attestazione. Questa chiave condizionale è efficace solo quando il `Recipient` parametro nella richiesta specifica un documento di attestazione firmato per un'enclave AWS Nitro.

Questo valore è incluso anche negli CloudTraileventi per le richieste alle enclavi Nitro. AWS KMS

> **Note**
>
> Questa chiave di condizione è valida nelle istruzioni delle policy delle chiavi e nelle istruzioni delle policy IAM, anche se non viene visualizzata nella console IAM o nella Documentazione di riferimento dell'autorizzazione del servizio IAM.

Ad esempio, la seguente dichiarazione di politica chiave consente al `data-processing` ruolo di utilizzare la chiave KMS per Decrypt,, e le operazioni. GenerateDataKeyGenerateDataKeyPairGenerateRandom La chiave di condizione `kms:RecipientAttestation:ImageSha384` consente le operazioni solo quando il valore del digest immagine (PCR0) del documento di attestazione nella richiesta corrisponde al valore del digest nella condizione. Questa chiave condizionale è efficace solo quando il `Recipient` parametro nella richiesta specifica un documento di attestazione firmato per un'enclave Nitro. AWS

Se la richiesta non include un documento di attestazione valido proveniente da un'enclave AWS Nitro, l'autorizzazione viene negata perché questa condizione non è soddisfatta.

```
{
  "Sid" : "Enable enclave data processing",
  "Effect" : "Allow",
  "Principal" : {
    "AWS" : "arn:aws:iam::111122223333:role/data-processing"
  },
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey",
    "kms:GenerateDataKeyPair",
    "kms:GenerateRandom"
  ],
  "Resource" : "*",
  "Condition": {
    "StringEqualsIgnoreCase": {
      "kms:RecipientAttestation:ImageSha384":
 "9fedcba8abcdef7abcdef6abcdef5abcdef4abcdef3abcdef2abcdef1abcdef1abcdef0abcdef1abcdef2abcdef3a
    }
  }
}
```

kms: PCR RecipientAttestation <PCR_ID>

AWS KMS Chiavi di condizione	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy

`kms:RecipientAttestation:PCR<PCR_ID>`	Stringa	A valore singolo	`Decrypt`
			`GenerateDataKey`
			`GenerateDataKeyPair`
			`GenerateRandom`
				Policy delle chiavi e policy IAM

La chiave di condizione `kms:RecipientAttestation:PCR<PCR_ID>` controlla l'accesso a `Decrypt`, `GenerateDataKey`, `GenerateDataKeyPair` e `GenerateRandom` con una chiave KMS solo quando i registri di configurazione della piattaforma (PCR) dal documento di attestazione firmato nella richiesta corrispondono ai registri PCR nella chiave di condizione. Questa chiave condizionale è efficace solo quando il `Recipient` parametro nella richiesta specifica un documento di attestazione firmato da un'enclave AWS Nitro.

Questo valore è incluso anche negli CloudTraileventi che rappresentano le richieste per le enclavi Nitro. AWS KMS

> **Note**
>
> Questa chiave di condizione è valida nelle istruzioni delle policy delle chiavi e nelle istruzioni delle policy IAM, anche se non viene visualizzata nella console IAM o nella Documentazione di riferimento dell'autorizzazione del servizio IAM.

Per specificare un valore PCR, utilizzare il formato seguente. Concatena l'ID PCR al nome della chiave di condizione. Il valore PCR deve essere una stringa esadecimale minuscola di un massimo di 96 byte.

```
"kms:RecipientAttestation:PCRPCR_ID": "PCR_value"
```

Ad esempio, la seguente chiave di condizione specifica un valore particolare per PCR1, che corrisponde all'hash del kernel utilizzato per l'enclave e il processo di bootstrap.

```
kms:RecipientAttestation:PCR1:
 "0x1abcdef2abcdef3abcdef4abcdef5abcdef6abcdef7abcdef8abcdef9abcdef8abcdef7abcdef6abcdef5abcdef
```

Il seguente esempio di istruzione della policy della chiave consente al ruolo `data-processing` di utilizzare la chiave KMS per l'operazione Decrypt.

La chiave di condizione `kms:RecipientAttestation:PCR` in questa istruzione consente l'operazione solo quando il valore PCR1 nel documento di attestazione firmato nella richiesta corrisponde al valore `kms:RecipientAttestation:PCR1` nella condizione. Usa l'operatore di policy `StringEqualsIgnoreCase` per richiedere un confronto senza distinzione tra maiuscole e minuscole dei valori PCR.

Se la richiesta non include un documento di attestazione, l'autorizzazione viene negata perché questa condizione non è soddisfatta.

```
{
  "Sid" : "Enable enclave data processing",
  "Effect" : "Allow",
  "Principal" : {
    "AWS" : "arn:aws:iam::111122223333:role/data-processing"
  },
  "Action": "kms:Decrypt",
  "Resource" : "*",
  "Condition": {
    "StringEqualsIgnoreCase": {
      "kms:RecipientAttestation:PCR1":
 "0x1de4f2dcf774f6e3b679f62e5f120065b2e408dcea327bd1c9dddaea6664e7af79355814748447674530 82c6f15
    }
  }
}
```

ABAC per AWS KMS

Il controllo dell'accesso basato su attributi (Attribute-Based Access Control, ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. AWS KMS supporta ABAC

consentendo di controllare l'accesso alle chiavi gestite dal cliente in base ai tag e agli alias associati alle chiavi KMS. Le chiavi di condizione tag e alias che abilitano ABAC in AWS KMS forniscono un modo potente e flessibile per autorizzare le entità a utilizzare le chiavi KMS senza modificare le policy o gestire le concessioni. Ma occorre usare queste funzionalità con cura in modo che ai principali non sia inavvertitamente autorizzato o negato l'accesso.

Se si utilizza ABAC, tenere presente che l'autorizzazione per gestire tag e alias è ora un'autorizzazione di controllo di accesso. Assicurarsi di conoscere i tag e gli alias esistenti in tutte le chiavi KMS prima di distribuire una policy che dipende da tag o alias. Prendere ragionevoli precauzioni quando si aggiungono, eliminano e aggiornano gli alias e quando si taggano e si rimuovono i tag delle chiavi. Assegna le autorizzazioni per gestire tag e alias solo alle entità che ne hanno bisogno e limita i tag e gli alias che possono gestire.

> **Note**
>
> Quando usi ABAC per AWS KMS, presta attenzione quando concedi ai principali l'autorizzazione per gestire tag e alias. La modifica di un tag o di un alias potrebbe consentire o negare l'autorizzazione a una chiave KMS. Gli amministratori chiave che non dispongono dell'autorizzazione per modificare le policy chiave o creare concessioni possono controllare l'accesso alle chiavi KMS se dispongono dell'autorizzazione per gestire tag o alias.
> È possibile che occorrano fino a cinque minuti affinché le modifiche a tag e alias diventano effettive per l'autorizzazione delle chiavi KMS. Le modifiche recenti potrebbero essere visibili nelle operazioni API prima che influiscano sull'autorizzazione.
> Per controllare l'accesso a una chiave KMS in base al relativo alias, è necessario utilizzare una chiave di condizione. Non è possibile utilizzare un alias per rappresentare una chiave KMS nell'elemento `Resource` di un'istruzione di policy. Quando viene visualizzato un alias nell'elemento `Resource`, l'istruzione di policy si applica all'alias e non alla chiave KMS associata.

Ulteriori informazioni

- Per informazioni dettagliate sul supporto AWS KMS per ABAC, inclusi gli esempi, consulta Utilizzo degli alias per controllare l'accesso alle chiavi KMS e Utilizzo dei tag per controllare l'accesso alle chiavi KMS.
- Per informazioni generali sull'utilizzo dei tag per controllare l'accesso alle risorse AWS, consulta Cos'è ABAC per AWS? e Controllo degli accessi alle risorse AWS con i tag per le risorse nella Guida per l'utente di IAM.

Chiavi di condizione ABAC per AWS KMS

Per autorizzare l'accesso alle chiavi del servizio di gestione delle chiavi in base ai relativi tag e alias, utilizzare le seguenti chiavi di condizione in una policy chiave o in una policy IAM.

Chiavi di condizione ABAC	Descrizione	Tipo di policy	Operazioni AWS KMS
seghe: ResourceTag	Il tag (chiave e valore) sulla chiave KMS corrisponde al tag (chiave e valore) o al modello di tag nella policy	Solo policy IAM	Operazioni delle risorse delle chiavi KMS [2]
aws:RequestTag//tag-key	Il tag (chiave e valore) nella richiesta corrisponde al tag (chiave e valore) o al modello di tag nella policy	Policy chiave e policy IAM[1]	TagResource, UntagResource
aws: TagKeys	Le chiavi tag nella richiesta corrispon dono alle chiavi tag nella policy	Policy chiave e policy IAM[1]	TagResource, UntagResource
km: ResourceAliases	Gli alias associati alla chiave KMS corrispon dono agli alias o ai modelli di alias nella policy	Solo policy IAM	Operazioni delle risorse delle chiavi KMS [2]
km: RequestAlias	L'alias che rappresen ta la chiave KMS nella richiesta corrisponde agli alias o ai modelli di alias nella policy.	Policy chiave e policy IAM[1]	Operazioni crittogra fiche, DescribeK eyGetPublicKey

[1]Qualsiasi chiave di condizione che può essere utilizzata in una policy chiave può essere utilizzata anche in una policy IAM, ma solo se la policy chiave lo consente.

[2]Un'operazione delle risorse delle chiavi KMS è un'operazione autorizzata per una determinata chiave KMS. Per identificare le operazioni delle risorse delle chiavi KMS, nella tabella delle autorizzazioni AWS KMS, cerca un valore della chiave KMS nella colonna `Resources`per l'operazione.

Ad esempio, è possibile utilizzare queste chiavi di condizione per creare le seguenti policy.

- Una policy IAM con `kms:ResourceAliases` che consente di utilizzare le chiavi KMS con un particolare alias o modello di alias. Questa differisce leggermente dalle policy che si basano sui tag: sebbene sia possibile utilizzare modelli di alias in una policy, ogni alias deve essere univoco in un Account AWS e una Regione. In questo modo è possibile applicare una policy a un set selezionato di chiavi KMS senza elencare gli ARN chiave delle chiavi KMS nell'istruzione di policy. Per aggiungere o rimuovere chiavi KMS dal set, modificare l'alias della chiave KMS.
- Una policy chiave con `kms:RequestAlias` che consente ai principali di utilizzare una chiave KMS in un'operazione `Encrypt`, ma solo quando la richiesta `Encrypt` utilizza tale alias per identificare la chiave KMS.
- Una policy IAM con `aws:ResourceTag/`*`tag-key`* che nega l'autorizzazione a utilizzare le chiavi KMS con una chiave di tag e un valore di tag specifici. Ciò consente di applicare una policy a un set selezionato di chiavi KMS senza elencare gli ARN chiave delle chiavi KMS nell'istruzione di policy. Per aggiungere o rimuovere le chiavi del servizio di gestione delle chiavi dal set, taggare o rimuovere la chiave KMS.
- Una policy IAM con `aws:RequestTag/`*`tag-key`* che consente ai gruppi di eliminare solo i tag della chiave KMS `"Purpose"="Test"`.
- Una policy IAM con `aws:TagKeys` che nega l'autorizzazione ad aggiungere o eliminare un tag a una chiave KMS con una chiave tag `Restricted`.

ABAC rende la gestione degli accessi flessibile e scalabile. Ad esempio, puoi utilizzare la chiave di condizione `aws:ResourceTag/`*`tag-key`* per creare una policy IAM che consente ai principali di utilizzare una chiave KMS per le operazioni specificate solo quando la chiave KMS ha un tag `Purpose=Test`. La policy si applica a tutte le chiavi KMS in tutte le Regioni dell'Account AWS.

Quando è collegata a un utente o a un ruolo, la policy IAM seguente consente alle entità principali di utilizzare tutte le chiavi KMS esistenti con un tag `Purpose=Test` per le operazioni specificate. Per fornire questo accesso a chiavi KMS nuove o esistenti, non è necessario modificare le policy. È

sufficiente collegare il tag `Purpose=Test` alle chiavi KMS. Allo stesso modo, per rimuovere questo accesso dalle chiavi KMS con un tag `Purpose=Test`, modifica o elimina il tag.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AliasBasedIAMPolicy",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "arn:aws:kms:*:111122223333:key/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Purpose": "Test"
        }
      }
    }
  ]
}
```

Tuttavia, se si utilizza questa funzione, fare attenzione nella gestione di tag e alias. L'aggiunta, la modifica o l'eliminazione di un tag o di un alias può inavvertitamente consentire o negare l'accesso a una chiave KMS. Gli amministratori chiave che non dispongono dell'autorizzazione per modificare le policy chiave o creare concessioni possono controllare l'accesso alle chiavi KMS se dispongono dell'autorizzazione per gestire tag e alias. Per mitigare questo rischio, considera di limitare le autorizzazioni per la gestione di tag e alias. Ad esempio, potrebbe essere necessario consentire solo ai principali di gestire la gestione dei tag `Purpose=Test`. Per informazioni dettagliate, consulta Utilizzo degli alias per controllare l'accesso alle chiavi KMS e Utilizzo dei tag per controllare l'accesso alle chiavi KMS.

Tag o alias?

AWS KMS supporta ABAC con tag e alias. Entrambe le opzioni offrono una strategia di controllo degli accessi flessibile e scalabile, ma sono leggermente diverse l'una dall'altra.

Potresti decidere di usare tag o usare alias in base ai particolari modelli di utilizzo AWS. Ad esempio, se sono già state concesse autorizzazioni di assegnazione di tag alla maggior parte degli amministratori, potrebbe essere più semplice controllare una strategia di autorizzazione basata sugli alias. Oppure, se stai per raggiungere la quota di alias per chiave KMS, potresti preferire una strategia di autorizzazione basata sui tag.

I seguenti vantaggi sono di interesse generale.

Vantaggi del controllo degli accessi basato su tag

- Stesso meccanismo di autorizzazione per diversi tipi di risorse AWS.

  Puoi utilizzare lo stesso tag o codice tag per controllare l'accesso a più tipi di risorse, ad esempio un cluster Amazon Relational Database Service (Amazon RDS), un volume Amazon Elastic Block Store (Amazon EBS) e una chiave KMS. Questa funzione consente diversi modelli di autorizzazione più flessibili rispetto ai tradizionali controlli di accesso basati sui ruoli.
- Autorizzare l'accesso a un gruppo di chiavi KMS.

  È possibile utilizzare i tag per gestire l'accesso a un gruppo di chiavi KMS nello stesso Account AWS e nella stessa Regione. Assegnare lo stesso tag o chiave di tag alle chiavi KMS scelte. Quindi crea una semplice dichiarazione easy-to-maintain politica basata sul tag o sulla chiave del tag. Per aggiungere o rimuovere una chiave KMS dal gruppo di autorizzazioni, aggiungere o rimuovere il tag. Non è necessario modificare la policy.

Vantaggi del controllo degli accessi basato su alias

- Autorizza l'accesso alle operazioni di crittografia in base agli alias.

  La maggior parte delle condizioni delle policy basate sulla richiesta per gli attributi, incluso aws:RequestTag/tag-key, influiscono solo sulle operazioni che aggiungono, modificano o eliminano l'attributo. Ma la chiave kms: RequestAlias condition controlla l'accesso alle operazioni crittografiche in base all'alias utilizzato per identificare la chiave KMS nella richiesta. Ad esempio, è possibile concedere a un'entità principale l'autorizzazione per utilizzare una chiave KMS in u'operazione `Encrypt` ma solo quando il valore del parametro `KeyId` è `alias/restricted-key-1`. Per soddisfare questa condizione, è necessario quanto segue:
  - La chiave KMS deve essere associata a tale alias.
  - La richiesta deve utilizzare l'alias per identificare la chiave KMS.

- Il principale deve disporre dell'autorizzazione per utilizzare la chiave KMS soggetta alla condizione `kms:RequestAlias`.

Ciò è particolarmente utile se le applicazioni utilizzano comunemente nomi alias o ARN alias per fare riferimento alle chiavi KMS.

- Fornisci autorizzazioni molto limitate.

L'alias deve essere univoco in un Account AWS e in una Regione. Di conseguenza, concedere ai principali l'accesso a una chiave KMS basata su un alias può essere molto più restrittivo rispetto a concedere loro l'accesso basato su un tag. Diversamente dagli alias, i tag possono essere assegnati a più chiavi KMS nello stesso account e nella stessa Regione. Se si sceglie, è possibile utilizzare un modello alias, ad esempio `alias/test*`, per consentire agli entità principali di accedere a un gruppo di chiavi KMS nello stesso account e nella stessa Regione. Tuttavia, l'autorizzazione o la negazione dell'accesso a un alias specifico consente un controllo molto rigoroso sulle chiavi KMS.

Risoluzione dei problemi ABAC per AWS KMS

Controllare l'accesso alle chiavi KMS in base ai tag e agli alias è comodo e potente. Tuttavia, è incline a alcuni errori prevedibili che vorrai prevenire.

Accesso modificato a causa della modifica dei tag

Se un tag viene eliminato o il relativo valore viene modificato, ai principali che hanno accesso a una chiave KMS basata solo su tale tag verrà negato l'accesso alla chiave KMS. Ciò può verificarsi anche quando un tag incluso in un'istruzione di policy di negazione viene aggiunto a una chiave KMS. L'aggiunta di un tag relativo alla policy a una chiave KMS può consentire l'accesso a principali a cui è necessario negare l'accesso a una chiave KMS.

Si supponga, ad esempio, che un principale abbia accesso a una chiave KMS in base al tag `Project=Alpha`, ad esempio l'autorizzazione fornita dalla seguente istruzione della policy IAM di esempio.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IAMPolicyWithResourceTag",
```

```
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:ap-southeast-1:111122223333:key/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Project": "Alpha"
        }
      }
    }
  ]
}
```

Se il tag viene eliminato dalla chiave KMS o il valore del tag viene modificato, l'entità principale non dispone più dell'autorizzazione per utilizzare la chiave KMS per le operazioni specificate. Ciò potrebbe diventare evidente quando il responsabile tenta di leggere o scrivere dati in un AWS servizio che utilizza una chiave gestita dal cliente. Per tracciare la modifica del tag, rivedi i CloudTrail log o le immissioni. TagResourceUntagResource

Per ripristinare l'accesso senza aggiornare la policy, modifica i tag sulla chiave KMS. Questa azione ha un impatto minimo diverso dal breve periodo in cui sta entrando in vigore AWS KMS. Per evitare un errore come questo, dai le autorizzazioni per l'assegnazione e l'eliminazione di tag solo ai principali che ne hanno bisogno e limita le autorizzazioni per l'assegnazione di tag ai tag che devono gestire. Prima di modificare un tag, cerca le policy per rilevare l'accesso che dipende dal tag e ottenere le chiavi KMS in tutte le Regioni che dispongono del tag. Potresti prendere in considerazione la creazione di un CloudWatch allarme Amazon quando vengono modificati determinati tag.

Modifica dell'accesso a causa della modifica degli alias

Se un alias viene eliminato o associato a una chiave KMS diversa, ai principali che hanno accesso alla chiave KMS basata solo su tale alias verrà negato l'accesso alla chiave KMS. Ciò può verificarsi anche quando un alias associato a una chiave KMS è incluso in un'istruzione della policy di negazione. L'aggiunta di un alias relativo alla policy a una chiave KMS può inoltre consentire l'accesso a principali a cui è necessario negare l'accesso a una chiave KMS.

Ad esempio, la seguente dichiarazione politica IAM utilizza la chiave kms: ResourceAliases condition per consentire l'accesso alle chiavi KMS in diverse regioni dell'account con uno qualsiasi degli alias specificati.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AliasBasedIAMPolicy",
      "Effect": "Allow",
      "Action": [
        "kms:List*",
        "kms:Describe*",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:*:111122223333:key/*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "kms:ResourceAliases": [
            "alias/ProjectAlpha",
            "alias/ProjectAlpha_Test",
            "alias/ProjectAlpha_Dev"
          ]
        }
      }
    }
  ]
}
```

Per tracciare la modifica dell'alias, esamina i CloudTrail log e le CreateAliasimmissioni. UpdateAliasDeleteAlias

Per ripristinare l'accesso senza aggiornare la policy, modifica gli alias associati alla chiave KMS. Poiché ogni alias può essere associato a una sola chiave KMS in un account e in una Regione, la gestione degli alias è un po' più difficile della gestione dei tag. Il ripristino dell'accesso ad alcune entità principali a una chiave KMS può negare l'accesso alla stessa o ad altre entità principali a una chiave KMS diversa.

Per evitare questo errore, assegna autorizzazioni di gestione degli alias solo alle entità principali che ne hanno bisogno e limita le autorizzazioni per la gestione degli alias agli alias che devono gestire. Prima di aggiornare o eliminare un alias, cerca le policy per rilevare l'accesso che dipende dall'alias e trova le chiavi KMS in tutte le Regioni associate all'alias.

Accesso negato a causa di quota alias

Gli utenti autorizzati a utilizzare una chiave KMS entro una ResourceAliases condizione kms: riceveranno un'`AccessDenied`eccezione se la chiave KMS supera gli alias predefiniti per quota di chiavi KMS per quell'account e quella regione.

Per ripristinare l'accesso, elimina gli alias associati alla chiave KMS in modo da rispettare la quota. In alternativa, utilizza un meccanismo alternativo per consentire agli utenti di accedere alla chiave KMS.

Modifica dell'autorizzazione ritardata

Le modifiche apportate a tag e alias possono richiedere fino a cinque minuti per influenzare l'autorizzazione delle chiavi KMS. Di conseguenza, una modifica di tag o alias potrebbe riflettersi nelle risposte delle operazioni API prima che influiscano sull'autorizzazione. Questo ritardo è probabilmente più lungo del breve ritardo finale di coerenza che colpisce la maggior parte delle operazioni AWS KMS.

Ad esempio, potrebbe esserci una policy IAM che consente a determinate entità principali di utilizzare una chiave KMS con un tag `"Purpose"="Test"`. Quindi aggiungi il tag `"Purpose"="Test"` su una chiave KMS. Sebbene l'TagResourceoperazione sia stata completata e la ListResourceTagsrisposta confermi che il tag è assegnato alla chiave KMS, i responsabili potrebbero non avere accesso alla chiave KMS per un massimo di cinque minuti.

Per evitare errori, inserisci questo ritardo previsto nel tuo codice.

Richieste non riuscite a causa di aggiornamenti alias

Quando aggiorni un alias, associ un alias esistente a una chiave KMS diversa.

La decrittografia e ReEncryptle richieste che specificano il nome alias o l'alias ARN potrebbero non riuscire perché l'alias è ora associato a una chiave KMS che non crittografava il testo cifrato. Questa situazione in genere restituisce `IncorrectKeyException` o `NotFoundException`. O se la richiesta non ha un parametro `KeyId` o `DestinationKeyId`, l'operazione potrebbe avere esito negativo con l'eccezione `AccessDenied` perché il chiamante non ha più accesso alla chiave KMS che ha crittografato il testo cifrato.

È possibile tracciare la modifica esaminando i log e le voci di registro. CloudTrail CreateAliasUpdateAliasDeleteAlias È inoltre possibile utilizzare il valore del `LastUpdatedDate` campo nella ListAliasesrisposta per rilevare una modifica.

Ad esempio, la seguente risposta di ListAliasesesempio mostra che l'`ProjectAlpha_Test`alias nella `kms:ResourceAliases` condizione è stato aggiornato. Di conseguenza, le entità principali che hanno un accesso basato sugli alias perdono l'accesso alla chiave KMS associata in precedenza. Al contrario, hanno accesso alla nuova chiave KMS associata.

```
$ aws kms list-aliases --query 'Aliases[?starts_with(AliasName, `alias/ProjectAlpha`)]'

{
    "Aliases": [
        {
            "AliasName": "alias/ProjectAlpha_Test",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/ProjectAlpha_Test",
            "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
            "CreationDate": 1566518783.394,
            "LastUpdatedDate": 1605308931.903
        },
        {
            "AliasName": "alias/ProjectAlpha_Restricted",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/
ProjectAlpha_Restricted",
            "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
            "CreationDate": 1553410800.010,
            "LastUpdatedDate": 1553410800.010
        }
    ]
}
```

Non è semplice rimediare a questa modifica. È possibile aggiornare nuovamente l'alias per associarlo alla chiave KMS originale. Tuttavia, prima di agire, è necessario considerare l'effetto di tale modifica sulla chiave KMS attualmente associata. Se le entità utilizzavano quest'ultima chiave KMS nelle operazioni di crittografia, potrebbe essere necessario continuare ad accedervi. In questo caso, è possibile aggiornare la policy per assicurarsi che le entità principali dispongano dell'autorizzazione per utilizzare entrambe le chiavi KMS.

È possibile evitare un errore come questo: prima di aggiornare un alias, cerca le policy per rilevare l'accesso che dipende dall'alias. Quindi ottieni le chiavi KMS in tutte le Regioni associate all'alias. Assegna autorizzazioni di gestione degli alias solo alle entità principali che ne hanno bisogno e limita le autorizzazioni per la gestione degli alias agli alias che devono gestire.

Autorizzazione per gli utenti in altri account di utilizzare una chiave KMS

Puoi consentire a utenti o ruoli in un Account AWS diverso di usare una chiave KMS nel tuo account. L'accesso tra account richiede l'autorizzazione nella policy chiave della chiave dKMS e in una policy IAM nell'account dell'utente esterno.

L'autorizzazione tra account è valida solo per le seguenti operazioni:

- Operazioni di crittografia
- CreateGrant
- DescribeKey
- GetKeyRotationStatus
- GetPublicKey
- ListGrants
- RetireGrant
- RevokeGrant

Se concedi a un utente in un account diverso l'autorizzazione per altre operazioni, tali autorizzazioni non hanno effetto. Ad esempio, se concedi a un account principale kms: ListKeys permission in una policy IAM o kms: ScheduleKeyDeletion permission on a KMS key in una key policy chiave, i tentativi dell'utente di richiamare tali operazioni sulle tue risorse continuano a fallire.

Per informazioni dettagliate sull'utilizzo delle chiavi KMS in account diversi per le operazioni AWS KMS, consulta la colonna Utilizzo tra account in AWS KMS autorizzazioni e Utilizzo delle chiavi KMS in altri account. C'è anche una sezione Utilizzo tra account in ogni descrizione API nella Documentazione di riferimento dell'API AWS Key Management Service.

> **Warning**
>
> Fai attenzione a concedere ai principali le autorizzazioni per utilizzare le chiavi KMS. Quando possibile, segui il principio del privilegio minimo. Offri agli utenti l'accesso solo alle chiavi KMS necessarie solo per le operazioni che richiedono.
> Inoltre, presta cautela nell'utilizzare qualsiasi chiave KMS sconosciuta, in particolare una chiave KMS in un account diverso. Gli utenti malintenzionati potrebbero concederti le

autorizzazioni per utilizzare la loro chiave KMS e ottenere informazioni su di te o sul tuo account.
Per informazioni sull'utilizzo delle policy per proteggere le risorse dell'account, consulta Best practice per le policy IAM.

Per concedere l'autorizzazione a utilizzare una chiave KMS a utenti e ruoli in un altro account, è necessario utilizzare due diversi tipi di policy:

- La policy chiave per la chiave KMS deve fornire all'account esterno (o utenti e ruoli nell'account esterno) l'autorizzazione per utilizzare la chiave KMS. La policy delle chiavi si trova nell'account proprietario della chiave KMS.
- Le policy IAM nell'account esterno devono delegare le autorizzazioni delle policy delle chiavi ai relativi utenti e ruoli. Queste policy sono impostate nell'account esterno e concedono autorizzazioni agli utenti e ai ruoli in tale account.

La policy chiave determina chi può avere accesso alla chiave KMS. La policy IAM determina chi ha accesso alla chiave KMS. Né la policy chiave né la policy IAM sono sufficienti, è necessario modificarle entrambe.

Per modificare la politica chiave, puoi utilizzare la Policy View in AWS Management Console o utilizzare le CreateKeyoperazioni or. PutKeyPolicy Per informazioni sull'impostazione della policy delle chiavi durante la creazione di una chiave KMS, consulta Creazione di chiavi KMS utilizzabili da altri account.

Per informazioni sulla modifica delle policy IAM, consulta Utilizzo delle policy IAM con AWS KMS.

Per un esempio che mostra come la policy chiave e le policy IAM collaborano per consentire l'utilizzo di una chiave KMS in un altro account, consulta Esempio 2: un utente assume un ruolo con l'autorizzazione per l'utilizzo di una chiave KMS in un altro Account AWS.

Puoi visualizzare le operazioni AWS KMS tra account risultanti nella chiave KMS nei logs AWS CloudTrail. Le operazioni che usano le chiavi KMS in altri account vengono registrate sia nell'account del chiamante che nell'account del proprietario della chiave KMS.

Argomenti

- Fase 1: aggiungere una dichiarazione di policy delle chiavi nell'account locale
- Fase 2: aggiungere le policy IAM nell'account esterno

- Creazione di chiavi KMS utilizzabili da altri account
- Autorizzazione per l'utilizzo di chiavi KMS esterne con Servizi AWS
- Utilizzo delle chiavi KMS in altri account

> **Note**
>
> Gli esempi in questo argomento mostrano come utilizzare insieme una policy chiave e una policy IAM per fornire e limitare l'accesso a una chiave KMS. Questi esempi generici non hanno lo scopo di rappresentare le autorizzazioni che un particolare Servizio AWS richiede per una chiave KMS. Per informazioni sulle autorizzazioni richieste da un Servizio AWS, consulta l'argomento relativo alla crittografia nella documentazione del servizio.

Fase 1: aggiungere una dichiarazione di policy delle chiavi nell'account locale

La policy delle chiavi per una chiave KMS è il principale determinante di chi può accedere alla chiave KMS e quali operazioni può eseguire. La policy della chiave è sempre definita nell'account proprietario della chiave KMS. A differenza delle policy IAM, le policy delle chiavi non specificano una risorsa. La risorsa è la chiave KMS associata alla policy delle chiavi. Nel processo di assegnazione delle autorizzazioni multi-account, la policy delle chiavi per la chiave KMS deve fornire all'account esterno (o utenti e ruoli nell'account esterno) l'autorizzazione per utilizzare la chiave KMS.

Per concedere a un account esterno l'autorizzazione per utilizzare la chiave KMS, aggiungi una dichiarazione alla policy delle chiavi che specifica l'account esterno. Nell'elemento `Principal` della policy delle chiavi, immetti l'Amazon Resource Name (ARN) dell'account esterno.

Quando specifichi un account esterno in una policy chiave, gli amministratori IAM nell'account esterno possono utilizzare le policy IAM per delegare tali autorizzazioni a qualsiasi utente e ruolo nell'account esterno. Possono anche decidere quali delle operazioni specificate nella policy delle chiavi possono eseguire gli utenti e i ruoli.

Le autorizzazioni concesse all'account esterno e alle relative entità principali sono valide solo se l'account esterno è abilitato nella Regione che ospita la chiave KMS e le relative policy chiave. Per informazioni sulle regioni non abilitate per impostazione predefinita ("regioni attivate"), consulta Gestione delle Regioni AWS nella Riferimenti generali di AWS.

Ad esempio, supponiamo che tu voglia permettere all'account 444455556666 di utilizzare una chiave KMS di crittografia simmetrica nell'account 111122223333. A tale scopo, aggiungi una dichiarazione di policy come quella nell'esempio seguente alla policy delle chiavi per la chiave KMS nell'account 111122223333. Questa istruzione di policy concede all'account esterno, 444455556666, l'autorizzazione per utilizzare la chiave KMS nelle operazioni di crittografia per le chiavi KMS di crittografia simmetrica.

> **Note**
>
> L'esempio seguente rappresenta un esempio di policy delle chiavi per la condivisione di una chiave KMS con un altro account. Sostituisci i valori `Sid`, `Principal` e `Action` di esempio con valori validi per l'uso previsto della tua chiave KMS.

```
{
    "Sid": "Allow an external account to use this KMS key",
    "Effect": "Allow",
    "Principal": {
        "AWS": [
            "arn:aws:iam::444455556666:root"
        ]
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*"
}
```

Invece di concedere l'autorizzazione all'account esterno, puoi specificare particolari utenti e ruoli esterni nella policy delle chiavi. Tuttavia, tali utenti e ruoli non possono utilizzare la chiave KMS finché gli amministratori IAM nell'account esterno non collegano le policy IAM appropriate alle loro identità. Le policy IAM possono concedere l'autorizzazione a tutti o a un sottoinsieme di utenti e ruoli esterni specificati nella policy delle chiavi. Inoltre, possono consentire tutte o un sottoinsieme delle operazioni specificate nella policy delle chiavi.

La specifica delle identità in una policy delle chiavi limita le autorizzazioni che gli amministratori IAM nell'account esterno possono fornire. Tuttavia, rende più complessa la gestione delle policy con due account. Ad esempio, supponiamo che sia necessario aggiungere un utente o un ruolo. È necessario aggiungere tale identità alla policy delle chiavi nell'account proprietario della chiave KMS e creare policy IAM nell'account dell'identità.

Per specificare particolari utenti o ruoli esterni in una policy delle chiavi, nell'elemento `Principal` immettere l'Amazon Resource Name (ARN) di un utente o un ruolo nell'account esterno.

Ad esempio, la seguente istruzione di policy delle chiavi di esempio consente a `ExampleRole` nell'account `444455556666` di utilizzare una chiave KMS nell'account `111122223333`. Questa istruzione di policy della chiave concede all'account esterno, `444455556666`, l'autorizzazione per utilizzare la chiave KMS nelle operazioni di crittografia per le chiavi KMS di crittografia simmetrica.

> **Note**
>
> L'esempio seguente rappresenta un esempio di policy delle chiavi per la condivisione di una chiave KMS con un altro account. Sostituisci i valori `Sid`, `Principal` e `Action` di esempio con valori validi per l'uso previsto della tua chiave KMS.

```
{
    "Sid": "Allow an external account to use this KMS key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::444455556666:role/ExampleRole"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*"
}
```

> **Note**
>
> Non impostare il principale su un asterisco (*) in un'istruzione della policy della chiave che consenta autorizzazioni, a meno che non utilizzi condizioni per limitare la policy della chiave. Un asterisco dà ogni identità in ogni Account AWS l'autorizzazione a utilizzare la chiave KMS, a meno che un'altra istruzione di policy lo neghi esplicitamente. Gli utenti in altri Account AWS possono utilizzare la tua chiave KMS ogni qualvolta dispongono delle autorizzazioni corrispondenti nel loro account.

È inoltre necessario decidere quali autorizzazioni concedere all'account esterno. Per l'elenco delle autorizzazioni sulle chiavi KMS, consulta AWS KMS autorizzazioni.

Puoi concedere all'account esterno l'autorizzazione per utilizzare la chiave KMS nelle operazioni di crittografia e utilizzare la chiave KMS con i servizi AWS integrati con AWS KMS. A tale scopo, utilizza la sezione Key Users (Utenti chiave) di AWS Management Console. Per informazioni dettagliate, vedi Creazione di chiavi KMS utilizzabili da altri account.

Per specificare altre autorizzazioni nelle policy delle chiavi, modifica il documento della policy delle chiavi. Ad esempio, potresti voler concedere agli utenti l'autorizzazione per decrittare ma non crittografare, oppure l'autorizzazione per visualizzare la chiave KMS ma non utilizzarla. Per modificare il documento di policy chiave, è possibile utilizzare la Policy View nelle PutKeyPolicyoperazioni AWS Management Console CreateKeyo nelle operazioni.

Fase 2: aggiungere le policy IAM nell'account esterno

La policy delle chiavi nell'account proprietario della chiave KMS imposta l'intervallo valido per le autorizzazioni. Tuttavia, gli utenti e i ruoli nell'account esterno non possono utilizzare la chiave KMS finché non si collegano alle policy IAM che delegano tali autorizzazioni o utilizzano le concessioni per gestire l'accesso alla chiave KMS. Le policy IAM sono impostate nell'account esterno.

Se la policy delle chiavi concede l'autorizzazione all'account esterno, puoi collegare le policy IAM a qualsiasi utente o ruolo nell'account. Tuttavia, se la policy delle chiavi concede l'autorizzazione a determinati utenti o ruoli, la policy IAM può concedere tali autorizzazioni solo a tutti o a un sottoinsieme degli utenti e dei ruoli specificati. Se una policy IAM concede alla chaive KMS l'accesso ad altri utenti o ruoli esterni, non ha alcun effetto.

La policy delle chiavi limita anche le operazioni nella policy IAM. La policy IAM può delegare tutte le operazioni o un sottoinsieme di quelle specificate nella policy delle chiavi. Se la policy IAM elenca le operazioni che non sono specificate nella policy delle chiavi, tali autorizzazioni non sono valide.

La policy IAM dell'esempio seguente consente al principale di utilizzare la chiave KMS nell'account `111122223333` per le operazioni di crittografia. Per concedere questa autorizzazione a utenti e ruoli nell'account `444455556666`, collega la policy agli utenti o ai ruoli nell'account `444455556666`.

> **Note**
>
> L'esempio seguente rappresenta un esempio di policy IAM per la condivisione di una chiave KMS con un altro account. Sostituisci i valori `Sid`, `Resource` e `Action` di esempio con valori validi per l'uso previsto della tua chiave KMS.

```
{
    "Sid": "AllowUseOfKeyInAccount111122223333",
    "Effect": "Allow",
    "Action": [
      "kms:Encrypt",
      "kms:Decrypt",
      "kms:ReEncrypt*",
      "kms:GenerateDataKey*",
      "kms:DescribeKey"
    ],
    "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
}
```

Tieni presente quanto segue riguardo a questa policy:

- A differenza delle policy delle chiavi, le istruzioni delle policy IAM non contengono l'elemento `Principal`. Nelle policy IAM, il principale è implicito nell'identità a cui è collegata la policy.
- L'elemento `Resource` nella policy IAM identifica la chiave KMS che l'entità principale può utilizzare. Per specificare una chiave KMS, aggiungi l'ARN chiave all'elemento `Resource`.
- È possibile specificare più di una chiave KMS nell'elemento `Resource`. Tuttavia, se non specifichi particolari chiavi KMS nell'elemento `Resource`, potresti inavvertitamente concedere l'accesso a più chiavi KMS del previsto.

- Per consentire all'utente esterno di utilizzare la chiave KMS con i servizi AWS che si integrano con AWS KMS, potrebbe essere necessario aggiungere autorizzazioni alla policy delle chiavi o alla policy IAM. Per informazioni dettagliate, vedi Autorizzazione per l'utilizzo di chiavi KMS esterne con Servizi AWS.

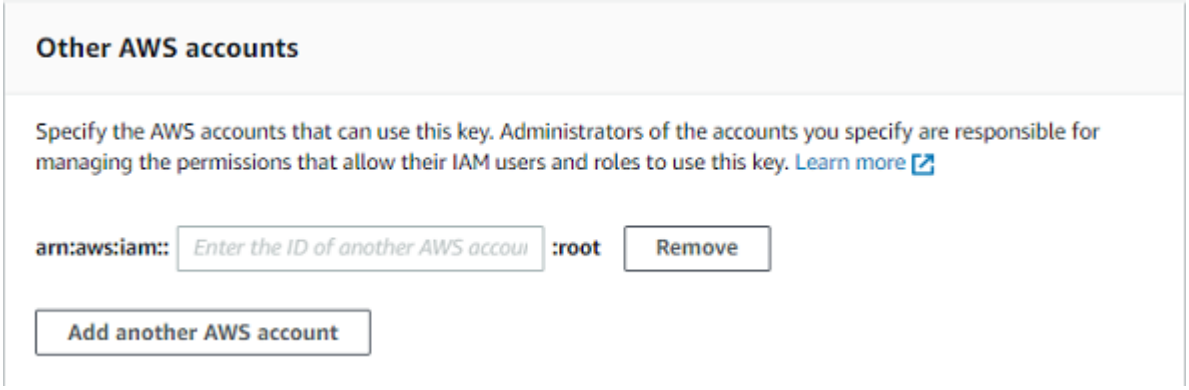
Per ulteriori informazioni sull'utilizzo di policy IAM, consulta Policy IAM.

Creazione di chiavi KMS utilizzabili da altri account

Quando si utilizza l'CreateKeyoperazione per creare una chiave KMS, è possibile utilizzare il relativo `Policy` parametro per specificare una politica chiave che consenta a un account esterno, o a utenti e ruoli esterni, l'autorizzazione a utilizzare la chiave KMS. È inoltre necessario aggiungere policy IAM nell'account esterno che delegano queste autorizzazioni agli utenti e ai ruoli dell'account, anche quando gli utenti e i ruoli sono specificati nella policy delle chiavi. È possibile modificare la politica delle chiavi in qualsiasi momento utilizzando l'PutKeyPolicyoperazione.

Quando crei una chiave KMS nella AWS Management Console, crei anche la relativa policy chiave. Quando selezioni le identità nelle sezioni Amministratori delle chiavi e Utenti delle chiavi, AWS KMS aggiunge istruzioni di policy per tali identità alla policy chiave della chiave KMS.

La sezione Key Users (Utenti chiave) consente inoltre di aggiungere account esterni come utenti delle chiavi.



Quando immetti l'ID account di un account esterno, AWS KMS aggiunge due istruzioni alla policy delle chiavi. Questa operazione influisce solo sulla policy delle chiavi. Gli utenti e i ruoli nell'account esterno non possono utilizzare la chiave KMS finché non colleghi le policy IAM per concedere loro alcune o tutte queste autorizzazioni.

La prima istruzione di policy chiave concede all'account esterno l'autorizzazione per utilizzare la chiave KMS nelle operazioni di crittografia.

> **Note**
>
> Gli esempi seguenti rappresentano un esempio di policy delle chiavi per la condivisione di una chiave KMS con un altro account. Sostituisci i valori `Sid`, `Principal` e `Action` di esempio con valori validi per l'uso previsto della tua chiave KMS.

```
{
    "Sid": "Allow use of the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::444455556666:root"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*"
}
```

La seconda istruzione di policy chiave consente all'account esterno di creare, visualizzare e revocare concessioni sulla chiave KMS, ma solo quando la richiesta proviene da un servizio AWS integrato con AWS KMS. Queste autorizzazioni consentono altri servizi AWS che crittografano i dati utente di utilizzare la chiave KMS.

Queste autorizzazioni sono progettate per le chiavi KMS che crittografano i dati degli utenti nei AWS servizi, come Amazon. WorkMail Questi servizi in genere utilizzano concessioni per ottenere le autorizzazioni necessarie per utilizzare la chiave KMS per conto dell'utente. Per informazioni dettagliate, vedi Autorizzazione per l'utilizzo di chiavi KMS esterne con Servizi AWS.

```
{
    "Sid": "Allow attachment of persistent resources",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::444455556666:root"
    },
    "Action": [
        "kms:CreateGrant",
```

```
            "kms:ListGrants",
            "kms:RevokeGrant"
        ],
        "Resource": "*",
        "Condition": {
            "Bool": {
                "kms:GrantIsForAWSResource": "true"
            }
        }
    }
```

Se queste autorizzazioni non soddisfano le tue esigenze, puoi modificarle nella visualizzazione delle politiche della console o utilizzando l'operazione. PutKeyPolicy Puoi indicare utenti e ruolo esterni specifici anziché concedere l'autorizzazione all'account esterno. Puoi modificare le operazioni specificate dalla policy. Inoltre, puoi utilizzare le condizioni globali e di policy AWS KMS per perfezionare le autorizzazioni.

Autorizzazione per l'utilizzo di chiavi KMS esterne con Servizi AWS

Puoi concedere a un utente in un account diverso l'autorizzazione per utilizzare la chiave KMS con un servizio integrato con AWS KMS. Ad esempio, un utente in un account esterno può utilizzare la chiave KMS per crittografare gli oggetti in un bucket Amazon S3 o per crittografare i segreti archiviati in AWS Secrets Manager.

La policy delle chiavi deve fornire all'utente esterno o all'account dell'utente esterno l'autorizzazione per utilizzare la chiave KMS. Inoltre, è necessario collegare policy IAM all'identità che concede all'utente l'autorizzazione per utilizzare il Servizio AWS. Il servizio potrebbe richiedere che gli utenti dispongano di autorizzazioni aggiuntive nella policy chiave o nella policy IAM. Per un elenco delle autorizzazioni richieste dal Servizio AWS per una chiave gestita dal cliente, consulta l'argomento relativo alla protezione dei dati nel capitolo sulla sicurezza della guida per l'utente o la guida per gli sviluppatori del servizio.

Utilizzo delle chiavi KMS in altri account

Se si dispone dell'autorizzazione per utilizzare una chiave KMS in un Account AWS diverso, è possibile utilizzare la chiave KMS nella AWS Management Console, negli SDK AWS, in AWS CLI e in AWS Tools for PowerShell.

Per identificare una chiave KMS in un account diverso in un comando della shell o in una richiesta API, utilizzare i seguenti identificatori chiave.

- Per le operazioni di crittografia, e DescribeKeyGetPublicKey, utilizzare la chiave ARN o l'alias ARN della chiave KMS.
- Per CreateGrant, GetKeyRotationStatusListGrants, e RevokeGrant, usa la chiave ARN della chiave KMS.

Se si immette solo un ID chiave o un nome alias, AWS presume che la chiave KMS sia nell'account.

La console AWS KMS non visualizza le chiavi KMS in altri account, anche se si dispone dell'autorizzazione per utilizzarle. Inoltre, gli elenchi di chiavi KMS visualizzati nelle console di altri servizi AWS non includono chiavi KMS in altri account.

Per specificare una chiave KMS in un account diverso nella console di un servizio AWS, è necessario immettere l'ARN della chiave o l'ARN dell'alias della chiave KMS. L'identificatore chiave richiesto varia a seconda del servizio e potrebbe differire tra la console del servizio e le relative operazioni API. Per dettagli, consultare la documentazione del servizio.

Utilizzo di ruoli collegati ai servizi per AWS KMS

AWS Key Management Service utilizza ruoli collegati al servizio AWS Identity and Access Management (IAM). Un ruolo collegato al servizio è un tipo di ruolo IAM univoco collegato direttamente a AWS KMS. I ruoli collegati ai servizi sono definiti da AWS KMS e includono tutte le autorizzazioni richieste dal servizio per eseguire chiamate agli altri servizi AWS per tuo conto.

Un ruolo collegato ai servizi semplifica la configurazione di AWS KMS perché non dovrai più aggiungere manualmente le autorizzazioni necessarie. AWS KMS definisce le autorizzazioni dei relativi ruoli associati ai servizi e, salvo diversamente definito, AWS KMS potrà assumere solo i propri ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. Questa procedura protegge le risorse di AWS KMS perché impedisce la rimozione involontaria delle autorizzazioni di accesso alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consultare Servizi AWS che funzionano con IAM e cercare i servizi che riportano Sì nella colonna Ruolo collegato ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni del ruolo collegato ai servizi per store delle chiavi personalizzate AWS KMS

AWS KMSutilizza un ruolo collegato al servizio denominato AWSServiceRoleForKeyManagementServiceCustomKeyStoresper supportare gli archivi di chiavi personalizzati. Questo ruolo collegato ai servizi dà a AWS KMS l'autorizzazione per visualizzare i cluster AWS CloudHSM e creare l'infrastruttura di rete a supporto di una connessione tra l'archivio chiavi personalizzato e il relativo cluster AWS CloudHSM. AWS KMS crea questo ruolo solo quando crei un archivio delle chiavi personalizzate. Non è possibile creare direttamente questo ruolo collegato ai servizi.

Il ruolo collegato ai servizi AWSServiceRoleForKeyManagementServiceCustomKeyStores considera attendibile `cks.kms.amazonaws.com` ai fini dell'assunzione del ruolo. Di conseguenza, solo AWS KMS può assumere questo ruolo collegato ai servizi.

Le autorizzazioni nel ruolo sono limitate alle operazioni che AWS KMS esegue per connettere uno store delle chiavi personalizzate a un cluster AWS CloudHSM. Non fornisce a AWS KMS autorizzazioni aggiuntive. Ad esempio, AWS KMS non dispone dell'autorizzazione per creare, gestire o eliminare cluster AWS CloudHSM, HSM o backup.

Per ulteriori informazioni sul ruolo AWSServiceRoleForKeyManagementServiceCustomKeyStores, tra cui un elenco di autorizzazioni e istruzioni su come visualizzare il ruolo, modificare la descrizione del ruolo, eliminare il ruolo e ricrearlo con AWS KMS, consulta Autorizzazione di AWS KMS per gestire risorse AWS CloudHSM e Amazon EC2.

Autorizzazioni del ruolo collegato ai servizi per chiavi AWS KMS multiregione.

AWS KMSutilizza un ruolo collegato al servizio denominato AWSServiceRoleForKeyManagementServiceMultiRegionKeysper supportare chiavi multiregionali. Questo ruolo collegato ai servizi dà a AWS KMS l'autorizzazione per sincronizzare le modifiche al materiale chiave di una chiave primaria multiregione alle relative chiavi di replica. AWS KMS crea questo ruolo solo quando crei una chiave primaria multiregione. Non è possibile creare direttamente questo ruolo collegato ai servizi.

Il ruolo collegato ai servizi AWSServiceRoleForKeyManagementServiceMultiRegionKeys considera attendibile `mrk.kms.amazonaws.com` ai fini dell'assunzione del ruolo. Di conseguenza, solo AWS KMS può assumere questo ruolo collegato ai servizi. Le autorizzazioni nel ruolo sono limitate

alle azioni che AWS KMS esegue per mantenere sincronizzato il materiale chiave nelle chiavi multiregione correlate. Non fornisce a AWS KMS autorizzazioni aggiuntive.

Per ulteriori informazioni sul ruolo AWSServiceRoleForKeyManagementServiceMultiRegionKeys, tra cui un elenco di autorizzazioni e istruzioni su come visualizzare il ruolo, modificare la descrizione del ruolo, eliminare il ruolo e ricrearlo con AWS KMS, consulta Autorizzazione di AWS KMS per sincronizzare le chiavi multi-regione.

Aggiornamenti di AWS KMSalle policy gestite da AWS

Visualizza i dettagli sugli aggiornamenti alle policy gestite da AWS per AWS KMS da quando questo servizio ha iniziato a tenere traccia delle modifiche. Per gli avvisi automatici sulle modifiche apportate a questa pagina, sottoscrivere il feed RSS nella pagina Cronologia dei documenti di AWS KMS

Modifica	Descrizione	Data
AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy: aggiornamento a policy esistente	AWS KMSha aggiunto `ec2:DescribeVpcs` `ec2:DescribeNetworkAcls` , e `ec2:DescribeNetworkInterfaces` le autorizzazioni per monitorare le modifiche nel VPC che contiene AWS CloudHSM il cluster in modo da AWS KMS fornire messaggi di errore chiari in caso di errori.	10 novembre 2023
AWS KMS ha iniziato il rilevamento delle modifiche	AWS KMS ha iniziato il rilevamento delle modifiche per le relative policy gestite da AWS.	10 novembre 2023

Utilizzo del protocollo TLS post-quantistico ibrido con AWS KMS

AWS Key Management Service (AWS KMS) supporta un'opzione di scambio di chiavi post-quantistiche ibride per il protocollo di crittografia di rete TLS (Transport Layer Security). È possibile utilizzare questa opzione TLS quando ci si connette agli endpoint API AWS KMS. Offriamo questa caratteristica prima che gli algoritmi post-quantistici siano standardizzati in modo da poter iniziare a testare l'effetto di questi protocolli di scambio di chiavi sulle chiamate AWS KMS. Queste caratteristiche opzionali di scambio di chiavi post-quantistiche ibride sono sicure almeno quanto la crittografia TLS che utilizziamo oggi e potrebbero fornire ulteriori vantaggi per la sicurezza a lungo termine. Tuttavia, influenzano la latenza e il throughput rispetto ai protocolli di scambio di chiavi classici in uso oggi.

I dati inviati a AWS Key Management Service (AWS KMS) vengono protetti in transito dalla crittografia fornita da una connessione TLS (Transport Layer Security). Le classiche suite di crittografia supportate da AWS KMS per le sessioni TLS rendono gli attacchi di forza bruta sui meccanismi di scambio delle chiavi irrealizzabili con la tecnologia attuale. Tuttavia, se il calcolo quantistico su larga scala diventa una realtà in futuro, le classiche suite di crittografia utilizzate nei meccanismi di scambio delle chiavi TLS saranno suscettibili a questi attacchi. Se stai sviluppando applicazioni che si basano sulla riservatezza a lungo termine dei dati trasferiti su una connessione TLS, dovresti considerare un piano per la migrazione alla crittografia post-quantistica prima che i computer quantistici su larga scala diventino disponibili per l'uso. AWS sta lavorando per prepararsi a questo futuro, e vogliamo che anche voi siate ben preparati.

Per proteggere i dati crittografati oggi contro potenziali attacchi futuri, AWS sta partecipando con la comunità crittografica allo sviluppo di algoritmi resistenti alla quantistica o post-quantistici. Abbiamo implementato le suite di crittografia di scambio di chiavi post-quantistiche ibride in AWS KMS che combinano elementi classici e post-quantistici per assicurare che la connessione TLS sia potente almeno quanto lo sarebbe con le suite di crittografia classiche.

Queste suite di crittografia ibride sono disponibili per l'utilizzo sui carichi di lavoro di produzione nella maggior parte delle Regioni AWS. Tuttavia, poiché le caratteristiche di prestazioni e i requisiti di larghezza di banda delle suite di crittografia ibride sono diversi da quelli dei classici meccanismi di scambio di chiavi, si consiglia di testarli nelle chiamate API AWS KMS in condizioni diverse.

Feedback

Come sempre, la tua opinione e la partecipazione nei nostri repository open source è molto importante. Vorremmo soprattutto sapere come la tua infrastruttura interagisce con questa nuova variante del traffico TLS.

- Per fornire un feedback su questo argomento, usa il link Feedback nell'angolo in alto a destra di questa pagina.
- Stiamo sviluppando queste suite di crittografia ibride in open source nel s2n-tlsrepository di. GitHub Per fornire feedback sulla fruibilità delle suite crittografia o condividere nuove condizioni o risultati di test, creare un problema nel repository s2n-tls.
- Stiamo scrivendo esempi di codice per l'utilizzo del TLS post-quantistico ibrido nel repository. AWS KMS aws-kms-pq-tls-example GitHub Per porre domande o condividere idee sulla configurazione del client HTTP o del client AWS KMS per utilizzare le suite di crittografia ibrida, creare un problema nel repository aws-kms-pq-tls-example.

Regioni AWS supportate

Il TLS post-quantistico per AWS KMS è disponibile in tutte le Regioni AWS supportate da AWS KMS, ad eccezione delle regioni Cina (Pechino) e Cina (Ningxia).

> **Note**
>
> AWS KMS non supporta il protocollo TLS post-quantistico ibrido per gli endpoint FIPS in AWS GovCloud (US).

Per un elenco degli endpoint AWS KMS per ogni Regione AWS, consulta Endpoint e quote AWS Key Management Service nella Riferimenti generali di Amazon Web Services. Per ulteriori informazioni sugli endpoint FIPS, consulta Endpoint FIPS nella Riferimenti generali di Amazon Web Services.

Informazioni sullo scambio di chiavi post-quantistiche ibride in TLS

AWS KMS supporta le suite di crittografia di scambio di chiavi post-quantistiche ibride. Puoi utilizzare Common Runtime AWS SDK for Java 2.x e AWS su sistemi Linux per configurare un client HTTP in modo che utilizzi queste suite di crittografia. Quindi, ogni volta che ci si connette a un endpoint AWS KMS con il client HTTP, vengono utilizzate le suite di crittografia ibrida.

Questo client HTTP utilizza s2n-tls, che è un'implementazione open source del protocollo TLS. Le suite di crittografia ibride utilizzate da s2n-tls sono implementate solo per lo scambio di chiavi, non per la crittografia dei dati diretta. Durante lo scambio di chiavi, il client e il server calcolano la chiave che utilizzeranno per crittografare e decrittografare i dati in rete.

Gli algoritmi utilizzati da s2n-tls sono un ibrido che combina la curva ellittica Diffie-Hellman (ECDH), un normale algoritmo di scambio di chiavi utilizzato oggi in TLS, con Kyber, un algoritmo di crittografia a chiave pubblica che l'istituto nazionale per gli standard e la tecnologia (NIST) ha designato come primo standard per l'algoritmo di accordo chiave post-quantistico. Questo algoritmo ibrido utilizza ciascuno degli algoritmi in modo indipendente per generare una chiave. Quindi combina crittograficamente le due chiavi. Con s2n-tls, puoi configurare un client HTTP con una preferenza per il protocollo TLS post-quantistico, che inserisce ECDH con Kyber in prima posizione nell'elenco delle preferenze. Gli algoritmi di scambio di chiavi classici sono inclusi nell'elenco delle preferenze per garantire la compatibilità, ma sono inferiori nell'ordine delle preferenze.

Se le ricerche in corso riveleranno che l'algoritmo Kyber non dispone dell'efficacia post-quantistica prevista, la chiave ibrida sarà comunque efficace quanto la singola chiave ECDH attualmente in uso. Fino al completamento della ricerca sugli algoritmi post-quantistici, si consiglia di utilizzare algoritmi ibridi, piuttosto che utilizzare esclusivamente algoritmi post-quantistici.

Utilizzo del protocollo TLS post-quantistico ibrido con AWS KMS

È possibile utilizzare il protocollo TLS post-quantistico ibrido per le chiamate a AWS KMS. Quando si configura l'ambiente di test del client HTTP, tenere presente le seguenti informazioni:

Crittografia in transito

Le suite di crittografia ibrida in s2n-tls vengono utilizzate solo per la crittografia in transito. Proteggono i dati durante il trasferimento dal client all'endpoint AWS KMS. AWS KMS non utilizza queste suite di crittografia per crittografare i dati nelle AWS KMS keys.

Invece, quando AWS KMS esegue la crittografia dei dati con le chiavi KMS, utilizza la crittografia simmetrica con chiavi a 256 bit e l'algoritmo Advanced Encryption Standard in Galois Counter Mode (AES-GCM), che è già resistente alla quantistica. Attacchi teorici futuri di calcolo quantistico su larga scala su testi cifrati creati con chiavi AES-GCM a 256 bit riducono l'effettiva sicurezza della chiave a 128 bit. Questo livello di sicurezza è sufficiente per rendere impossibili gli attacchi di forza bruta su testi cifrati AWS KMS.

Sistemi supportati

L'uso delle suite di crittografia ibride in s2n-tls al momento è supportato solo su sistemi Linux. Inoltre, queste suite di crittografia sono supportate solo negli SDK che supportano il Common Runtime, AWS ad esempio AWS SDK for Java 2.x. Per vedere un esempio, consulta Come configurare il protocollo TLS post-quantistico ibrido.

Endpoint AWS KMS

Quando si utilizzano le suite di crittografia ibrida, utilizzare l'endpoint AWS KMS standard. Le suite di crittografia ibrida in s2n-tls non sono compatibili con gli endpoint convalidati FIPS 140-2 per AWS KMS.

Quando configuri un client HTTP con preferenza per le connessioni TLS post-quantistiche con s2n-tls, le crittografie post-quantistiche sono al primo posto nell'elenco delle preferenze di crittografia. Tuttavia, l'elenco delle preferenze include le crittografie classiche non ibride in posizioni inferiori nell'ordine di preferenza per la compatibilità. Quando configuri un client HTTP affinché preferisca il protocollo TLS post-quantistico con un endpoint convalidato AWS KMS FIPS 140-2, s2n-tls negozia una crittografia di scambio di chiavi non ibrida classica.

Per un elenco degli endpoint AWS KMS per ogni Regione AWS, consulta Endpoint e quote AWS Key Management Service in Riferimenti generali di Amazon Web Services. Per ulteriori informazioni sugli endpoint FIPS, consulta Endpoint FIPS nella Riferimenti generali di Amazon Web Services.

Prestazioni previste

I nostri primi test di benchmark indicano che le suite di crittografia ibrida in s2n-tls sono più lente delle classiche suite di crittografia TLS. L'effetto varia in base al profilo di rete, alla velocità della CPU, al numero di core e alla frequenza delle chiamate. Per i risultati dei test delle prestazioni, consulta Come ottimizzare TLS per la crittografia ibrida post-quantistica con Kyber.

Come configurare il protocollo TLS post-quantistico ibrido

In questa procedura, aggiungi una dipendenza Maven per il client HTTP AWS Common Runtime. Quindi, configura un client HTTP che preferisca il protocollo TLS post-quantistico. Quindi, creare un client AWS KMS che utilizza il client HTTP.

Per un esempio completo di configurazione e utilizzo del protocollo TLS post-quantistico ibrido con AWS KMS, consultare il repository aws-kms-pq-tls-example.

> **Note**
>
> Il client HTTP AWS Common Runtime, disponibile in anteprima, è diventato disponibile a livello generale a febbraio 2023. In tale versione, la classe `tlsCipherPreference` e il parametro del metodo `tlsCipherPreference()` vengono sostituiti dal parametro del metodo `postQuantumTlsEnabled()`. Se stavi usando questo esempio durante l'anteprima, devi aggiornare il codice.

1. Aggiungere il AWS Common Runtime del cliente alle dipendenze di Maven. Si consiglia di utilizzare l'ultima versione disponibile.

   Ad esempio, questa istruzione aggiunge la versione `2.20.0` del client AWS Common Runtime alle dipendenze di Maven.

   ```
   <dependency>
       <groupId>software.amazon.awssdk</groupId>
       <artifactId>aws-crt-client</artifactId>
       <version>2.20.0</version>
   </dependency>
   ```

2. Per abilitare le suite di crittografia post-quantistica ibrida, aggiungere AWS SDK for Java 2.x al progetto e inizializzarlo. Quindi abilita le suite di crittografia post-quantistica ibrida come mostrato nell'esempio seguente.

   Questo codice utilizza il parametro del metodo `postQuantumTlsEnabled()` per configurare un client HTTP AWS Common Runtime che preferisce la suite di crittografia post-quantistica ibrida consigliata, ECDH con Kyber. Quindi utilizza il client HTTP configurato per creare un'istanza del client asincrono AWS KMS, `KmsAsyncClient`. Una volta completato questo codice, tutte le richieste API AWS KMS sull'istanza `KmsAsyncClient` utilizzano un protocollo TLS post-quantistico ibrido.

   ```
   // Configure HTTP client
   SdkAsyncHttpClient awsCrtHttpClient = AwsCrtAsyncHttpClient.builder()
              .postQuantumTlsEnabled(true)
              .build();

   // Create the AWS KMS async client
   KmsAsyncClient kmsAsync = KmsAsyncClient.builder()
             .httpClient(awsCrtHttpClient)
             .build();
   ```

3. Testa le chiamate AWS KMS con il protocollo TLS post-quantistico ibrido.

   Quando si richiamano le operazioni API AWS KMS sul client AWS KMS configurato, le chiamate vengono trasmesse all'endpoint AWS KMS utilizzando il protocollo TLS post-quantistico ibrido. Per testare la configurazione, esegui una chiamata API AWS KMS, ad esempio `ListKeys`.

   ```
   ListKeysReponse keys = kmsAsync.listKeys().get();
   ```

Test del protocollo TLS post-quantistico ibrido con AWS KMS

Si consiglia di eseguire i seguenti test con suite di crittografia ibrida sulle applicazioni che richiamano AWS KMS.

- Eseguire test di carico e benchmark. Le suite di crittografia ibrida funzionano in modo diverso rispetto agli algoritmi di scambio di chiavi tradizionali. Potrebbe essere necessario modificare i timeout della connessione per consentire tempi di handshake più lunghi. In caso di esecuzione all'interno di una funzione AWS Lambda, aumentare l'impostazione del timeout di esecuzione.
- Provare a connettersi da posizioni diverse. A seconda del percorso di rete utilizzato dalla richiesta, è possibile scoprire che host intermedi, proxy o firewall con deep packet inspection (DPI) bloccano la richiesta. Ciò potrebbe derivare dall'utilizzo delle nuove suite di crittografia nella ClientHelloparte dell'handshake TLS o dai messaggi di scambio di chiavi più grandi. In caso di difficoltà con la risoluzione di questi problemi, contattare il team di sicurezza o gli amministratori IT per aggiornare la configurazione pertinente e sbloccare le nuove suite di crittografia TLS.

Ulteriori informazioni sul protocollo TLS post-quantistico in AWS KMS

Per ulteriori informazioni sull'utilizzo del protocollo TLS post-quantistico ibrido in AWS KMS, consultare le risorse seguenti.

- Per ulteriori informazioni sulla crittografia post-quantistica su AWS, inclusi collegamenti a post di blog e articoli di ricerca, consulta la sezione Crittografia post-quantistica.
- Per informazioni su s2n-tls, consultare Introduzione di s2n-tls, una nuova implementazione TLS open source e Utilizzo di s2n-tls.
- Per informazioni sul client HTTP AWS Common Runtime, consulta la sezione Configurazione del client HTTP basato su CRT AWS nella Guida per gli sviluppatori AWS SDK for Java 2.x.
- Per informazioni sul progetto di crittografia post-quantistica presso il National Institute for Standards and Technology (NIST), consultare Post-Quantum Cryptography (Crittografia post-quantistica).
- Per informazioni sulla standardizzazione della crittografia post-quantistica del NIST, consulta la sezione Standardizzazione della crittografia post-quantistica.

Determinazione dell'accesso a una AWS KMS keys

Per determinare il livello di chi o cosa ha attualmente accesso a una AWS KMS key, è necessario esaminare la policy chiave della chiave KMS, tutte le concessioni che si applicano alla chiave KMS

e potenzialmente tutte le policy AWS Identity and Access Management (IAM). Ciò potrebbe essere necessario per determinare la portata dell'utilizzo potenziale di una chiave KMS oppure per aiutarti a soddisfare i requisiti di conformità o di verifica. I seguenti argomenti aiutano a generare un elenco completo dei principali AWS (identità) che attualmente hanno accesso a una chiave KMS.

Argomenti

Analisi della policy delle chiavi

Le policy chiave sono lo strumento principale per controllare l'accesso alle chiavi KMS. Ogni chiave KMS ha esattamente una policy chiave.

Quando una policy delle chiavi è costituita da o include la policy chiave predefinita, la policy chiave consente agli amministratori IAM dell'account di utilizzare le policy IAM per controllare l'accesso alla chiave KMS. Inoltre, se la policy delle chiavi concede a un altro Account AWS l'autorizzazione per utilizzare la chiave KMS, gli amministratori IAM dell'account esterno possono utilizzare le policy IAM per delegare tali autorizzazioni. Per determinare l'elenco completo dei principali che possono accedere alla chiave KMS, esamina le policy IAM.

Per visualizzare la politica chiave di una chiave gestita AWS KMS dal cliente o Chiave gestita da AWSnel tuo account, utilizza AWS Management Console o l'GetKeyPolicyoperazione nell'AWS KMSAPI. Per visualizzare la policy delle chiavi, è necessario disporre delle autorizzazioni `kms:GetKeyPolicy` per la chiave KMS. Per istruzioni sulla visualizzazione delle policy delle chiave per una chiave KMS, consulta the section called “Visualizzazione di una policy di chiave”.

Esamina il documento di policy delle chiavi e prendi nota di tutti i principali specificati in ciascun elemento `Principal` dell'istruzione di policy. In un'istruzione della policy con un effetto `Allow`, gli utenti IAM, i ruoli IAM e l'Account AWS nell'elemento `Principal` hanno accesso a questa chiave KMS.

> **Note**
>
> Non impostare il principale su un asterisco (*) in un'istruzione della policy della chiave che consenta autorizzazioni, a meno che non utilizzi condizioni per limitare la policy della chiave.

> Un asterisco dà ogni identità in ogni Account AWS l'autorizzazione a utilizzare la chiave KMS, a meno che un'altra istruzione di policy lo neghi esplicitamente. Gli utenti in altri Account AWS possono utilizzare la tua chiave KMS ogni qualvolta dispongono delle autorizzazioni corrispondenti nel loro account.

I seguenti esempi utilizzano le istruzioni di policy incluse nella policy delle chiavi predefinita per mostrare come eseguire questa operazione.

Example Istruzione di policy 1

```
{
  "Sid": "Enable IAM User Permissions",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
  "Action": "kms:*",
  "Resource": "*"
}
```

Nell'istruzione della policy 1, `arn:aws:iam::111122223333:root` è un principale dell'account AWS che si riferisce all'Account AWS 111122223333. (Non è l'utente root dell'account). Per impostazione predefinita, un'istruzione della policy come questa è inclusa nel documento della policy delle chiavi quando crei una nuova chiave KMS con la AWS Management Console o quando crei una nuova chiave KMS in modo programmatico ma non fornisci una policy delle chiavi.

Un documento di policy delle chiavi con un'istruzione che consente l'accesso all'Account AWS consente policy IAM nell'account per concedere l'accesso alla chiave KMS. Pertanto, gli utenti e i ruoli nell'account potrebbero avere accesso alla chiave KMS anche se non sono elencati in modo esplicito come principali nel documento di policy delle chiavi. Esamina tutte le policy IAM in tutti gli Account AWS elencati come principali per determinare se consentono l'accesso a questa chiave KMS.

Example Istruzione di policy 2

```
{
  "Sid": "Allow access for Key Administrators",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:role/KMSKeyAdmins"},
  "Action": [
```

```
    "kms:Describe*",
    "kms:Put*",
    "kms:Create*",
    "kms:Update*",
    "kms:Enable*",
    "kms:Revoke*",
    "kms:List*",
    "kms:Disable*",
    "kms:Get*",
    "kms:Delete*",
    "kms:ScheduleKeyDeletion",
    "kms:CancelKeyDeletion"
  ],
  "Resource": "*"
}
```

Nella dichiarazione politica 2, `arn:aws:iam::111122223333:role/KMSKeyAdmins` fa riferimento al ruolo IAM denominato KMS KeyAdmins in Account AWS 111122223333. Gli utenti autorizzati ad assumere questo ruolo sono autorizzati ad eseguire le operazioni elencate nell'istruzione della policy, che sono le operazioni amministrative per la gestione di una chiave KMS.

Example Istruzione di policy 3

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:role/EncryptionApp"},
  "Action": [
    "kms:DescribeKey",
    "kms:GenerateDataKey*",
    "kms:Encrypt",
    "kms:ReEncrypt*",
    "kms:Decrypt"
  ],
  "Resource": "*"
}
```

Nella dichiarazione politica 3, `arn:aws:iam::111122223333:role/EncryptionApp` fa riferimento al ruolo IAM denominato EncryptionApp in 111122223333. Account AWS I principali autorizzati ad assumere questo ruolo sono autorizzati a eseguire le operazioni riportate nell'istruzione della policy, che includono le operazioni di crittografia per una chiave KMS di crittografia simmetrica.

Example Istruzione di policy 4

```
{
  "Sid": "Allow attachment of persistent resources",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:role/EncryptionApp"},
  "Action": [
    "kms:ListGrants",
    "kms:CreateGrant",
    "kms:RevokeGrant"
  ],
  "Resource": "*",
  "Condition": {"Bool": {"kms:GrantIsForAWSResource": true}}
}
```

Nella dichiarazione politica 4, `arn:aws:iam::111122223333:role/EncryptionApp` fa riferimento al ruolo IAM denominato EncryptionApp in Account AWS 111122223333. I principali autorizzati ad assumere questo ruolo sono autorizzati a eseguire le operazioni elencate nell'istruzione della policy. Queste operazioni, quando combinate con le operazioni consentite nell'Esempio di istruzione 3 della policy, sono quelle necessarie per delegare l'utilizzo della chiave KMS alla maggior parte dei servizi AWS che si integrano con AWS KMS, in particolare i servizi che utilizzano concessioni. Il GrantIsFor AWSResource valore kms: nell'`Condition`elemento assicura che la delega sia consentita solo quando il delegato è un AWS servizio che si integra AWS KMS e utilizza le concessioni per l'autorizzazione.

Per informazioni sui diversi modi in cui è possibile specificare un principale in un documento della policy chiave, consulta Specifica un principale nella Guida per l'utente IAM.

Per ulteriori informazioni sulle policy delle chiavi AWS KMS consulta Policy delle chiavi in AWS KMS.

Analisi delle policy IAM

Oltre alla policy delle chiavi e alle concessioni, puoi anche utilizzare le policy IAM per consentire l'accesso a una chiave KMS. Per ulteriori informazioni sull'utilizzo congiunto delle policy IAM e delle policy chiave, consulta Risoluzione dei problemi di accesso alla chiave.

Per determinare quali principali hanno attualmente accesso a una chiave KMS tramite le policy IAM, puoi utilizzare lo strumento Simulatore di policy IAM basato su browser o puoi effettuare richieste all'API IAM.

Modi per esaminare le policy IAM

- Analisi delle policy IAM con il simulatore di policy IAM
- Analisi delle policy IAM con l'API IAM

Analisi delle policy IAM con il simulatore di policy IAM

Il simulatore di policy IAM può aiutarti a scoprire i principali che possono accedere a una chiave KMS tramite una policy IAM.

Per utilizzare il simulatore di policy IAM per determinare l'accesso a una chiave KMS

1. Accedere alla AWS Management Console, quindi aprire il simulatore di policy IAM all'indirizzo https://policysim.aws.amazon.com/.
2. Nel riquadro Users, Groups, and Roles (Utenti, gruppi e ruoli), scegliere l'utente, il gruppo o il ruolo del quale si intende simulare le policy.
3. (Opzionale) Deseleziona la casella di controllo accanto a qualsiasi policy che desideri omettere dalla simulazione. Per simulare tutte le policy, lascia tutte le policy selezionate.
4. Nel riquadro Policy Simulator (Simulatore di policy), seguire la procedura riportata di seguito:
   a. Per Select service (Seleziona servizio), scegliere Key Management Service.
   b. Per simulare delle specifiche operazioni AWS KMS per Select actions (Seleziona operazioni), scegliere le operazioni da simulare. Per simulare tutte le operazioni AWS KMS, scegliere Select All (Seleziona tutto).
5. (Opzionale) Il simulatore di policy simula l'accesso a tutte le chiavi KMS per impostazione predefinita. Per simulare l'accesso a una determinata chiave KMS, scegli Impostazioni di simulazione, quindi digita l'Amazon Resource Name (ARN) della chiave KMS da simulare.
6. Scegliere Run Simulation (Esegui simulazione).

È possibile visualizzare i risultati della simulazione nella sezione Results (Risultati). Ripeti le fasi da 2 a 6 per ogni utente, gruppo e ruolo nell'Account AWS.

Analisi delle policy IAM con l'API IAM

È possibile utilizzare l'API IAM per esaminare le policy IAM a livello di codice. Le seguenti fasi forniscono una panoramica generale su come eseguire questa operazione:

1. Per ogni account Account AWS elencato come principale nella policy chiave (ovvero, ogni AWSaccount principal specificato in questo formato:`"Principal": {"AWS":`

`"arn:aws:iam::111122223333:root"}`), utilizza ListRoleslе operazioni ListUsersand nell'API IAM per inserire tutti gli utenti e i ruoli nell'account.

2. Per ogni utente e ruolo nell'elenco, utilizza l'SimulatePrincipalPolicyoperazione nell'API IAM, passando i seguenti parametri:
   - Per `PolicySourceArn`specificare il nome ARN (Amazon Resource Name) di un utente o un ruolo dal tuo elenco. Puoi specificare un solo `PolicySourceArn` per ogni richiesta `SimulatePrincipalPolicy`, pertanto è necessario chiamare questa operazione più volte, una volta per ogni utente e ruolo nell'elenco.
   - Per l'elenco `ActionNames`, specificare ogni operazione API AWS KMS da simulare. Per simulare tutte le operazioni API AWS KMS utilizzare `kms:*`. Per testare singole operazioni API AWS KMS, precedere ciascuna operazione API da "`kms:`", ad esempio, "`kms:ListKeys`". Per un elenco completo delle operazioni API AWS KMS, consulta Azioni nella Documentazione di riferimento dell'API AWS Key Management Service.
   - (Opzionale) Per determinare se gli utenti o i ruoli possono accedere a KMS specifiche, utilizza il parametro `ResourceArns` per specificare un elenco di nomi delle risorse Amazon (ARN) delle chiavi KMS. Per determinare se gli utenti o i ruoli possono accedere a una chiave KMS, ometti il parametro `ResourceArns`.

IAM risponde a ogni richiesta `SimulatePrincipalPolicy` con una valutazione: `allowed`, `explicitDeny` o `implicitDeny`. Per ogni tipo di risposta che contiene una valutazione `allowed`, la risposta include il nome dell'operazione API AWS KMS specifica consentita Eventualmente, include l'ARN della chiave KMS usata nella valutazione.

Analisi delle concessioni

Le concessioni sono meccanismi avanzati per specificare le autorizzazioni che tu o un servizio AWS integrato con AWS KMS potete utilizzare per specificare come e quando una chiave KMS può essere utilizzata. Le concessioni sono collegate a una chiave KMS; ogni concessione, inoltre, contiene il principale che riceve l'autorizzazione per utilizzare la chiave KMS e un elenco di operazioni consentite. Le concessioni sono un'alternativa alla policy delle chiavi e sono utili per casi d'uso specifici. Per ulteriori informazioni, consulta Concessioni in AWS KMS.

Per ottenere un elenco di concessioni per una chiave KMS, usa l'AWS KMSListGrantsoperazione. Puoi esaminare le concessioni per una chiave KMS per determinare chi o cosa dispone attualmente dell'autorizzazione per utilizzare la chiave KMS tramite tali concessioni. L'esempio seguente è una

rappresentazione JSON di una concessione che è stata ottenuta dal comando list-grants nella AWS CLI.

```
{"Grants": [{
  "Operations": ["Decrypt"],
  "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
  "Name": "0d8aa621-43ef-4657-b29c-3752c41dc132",
  "RetiringPrincipal": "arn:aws:iam::123456789012:root",
  "GranteePrincipal": "arn:aws:sts::111122223333:assumed-role/aws:ec2-infrastructure/
i-5d476fab",
  "GrantId": "dc716f53c93acacf291b1540de3e5a232b76256c83b2ecb22cdefa26576a2d3e",
  "IssuingAccount": "arn:aws:iam::111122223333:root",
  "CreationDate": 1.444151834E9,
  "Constraints": {"EncryptionContextSubset": {"aws:ebs:id": "vol-5cccfb4e"}}
}]}
```

Per scoprire chi o cosa dispone dell'autorizzazione per utilizzare la chiave KMS, cerca l'elemento `"GranteePrincipal"`. Nell'esempio precedente, il principale della concessione è un utente del ruolo assunto associato all'istanza EC2 i-5d476fab. L'infrastruttura di EC2 utilizza questo ruolo per collegare il volume EBS crittografato vol-5cccfb4e all'istanza. In questo caso, il ruolo dell'infrastruttura di EC2 dispone dell'autorizzazione per utilizzare la chiave KMS perché in precedenza avevi creato un volume EBS crittografato protetto da questa chiave KMS. e avevi collegato il volume a un'istanza EC2.

L'esempio seguente è un'altra rappresentazione JSON di una concessione che è stata ottenuta dal comando list-grants nella AWS CLI. Nell'esempio seguente, il principale della concessione è un altro Account AWS.

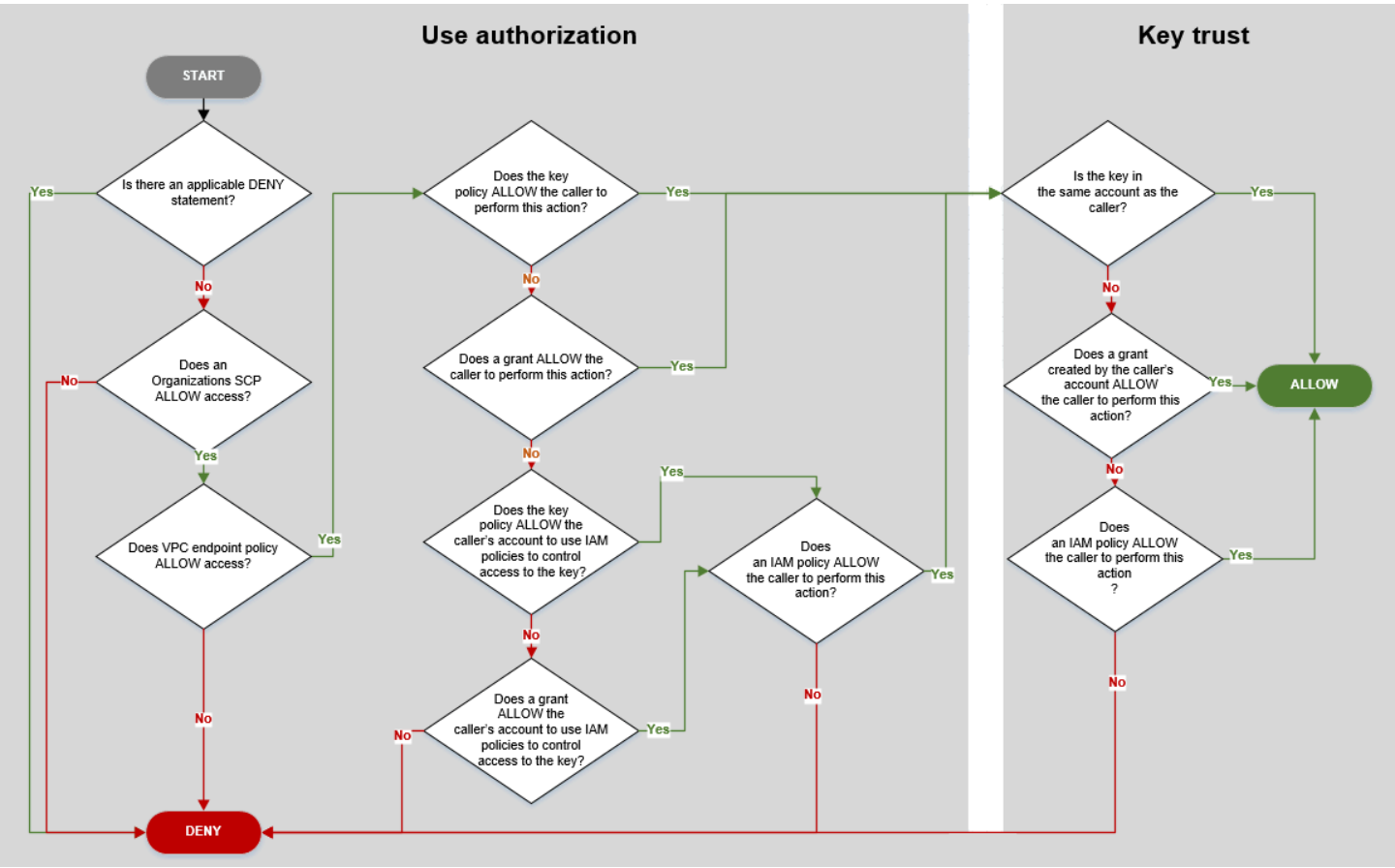
```
{"Grants": [{
  "Operations": ["Encrypt"],
  "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
  "Name": "",
  "GranteePrincipal": "arn:aws:iam::444455556666:root",
  "GrantId": "f271e8328717f8bde5d03f4981f06a6b3fc18bcae2da12ac38bd9186e7925d11",
  "IssuingAccount": "arn:aws:iam::111122223333:root",
  "CreationDate": 1.444151269E9
}]}
```

Risoluzione dei problemi di accesso alla chiave

Quando autorizzi l'accesso a una chiave KMS, AWS KMS valuta quanto segue:

- La policy chiave collegata alla chiave KMS. La policy chiave è sempre definita nell'Account AWS e nella Regione che posseggono la chiave KMS.
- Tutte le policy IAM collegate al ruolo o all'utente da cui proviene la richiesta. Le policy IAM che regolano l'uso da parte di un principale di una chiave KMS sono sempre definite nell'Account AWS del principale.
- Tutte le concessioni applicabili alla chiave KMS.
- Altri tipi di policy che potrebbero essere applicate alla richiesta di utilizzare la chiave KMS, ad esempio le policy di controllo dei servizi AWS Organizations e le policy di endpoint VPC. Queste policy sono facoltative e consentono tutte le operazioni per impostazione predefinita, ma puoi utilizzarle per limitare le autorizzazioni altrimenti concesse ai principali.

AWS KMS valuta questi meccanismi di policy insieme per determinare se l'accesso alla chiave KMS è consentito o meno. A tale scopo, AWS KMS utilizza un processo simile a quello illustrato nel seguente diagramma di flusso. Il seguente diagramma di flusso fornisce una rappresentazione visiva del processo di valutazione delle policy.



Questo diagramma di flusso è diviso in due parti. Le parti appaiono in sequenza, ma sono in genere valutate nello stesso momento.

- L'autorizzazione di utilizzo determina se è consentito l'utilizzo di una chiave KMS in base alla policy delle chiavi, alle policy IAM, alle concessioni e ad altre policy applicabili.
- Attendibilità della chiave determina se è necessario considerare attendibile una chiave KMS che è consentito utilizzare. In generale, si considerano attendibili le risorse nell'Account AWS. Ma è anche sicuro utilizzare le chiavi KMS con un Account AWS separato se esiste una concessione o una policy IAM nell'account che consente di utilizzare la chiave KMS.

Puoi usare questo diagramma di flusso per scoprire perché a un intermediario è stata concessa o negata l'autorizzazione a usare una chiave KMS. È anche possibile utilizzarlo per valutare le policy e le autorizzazioni. Ad esempio, il diagramma mostra che a un intermediario può essere negato l'accesso tramite una dichiarazione `DENY` esplicita o tramite l'assenza di una dichiarazione `ALLOW` esplicita, nella policy della chiave, nella policy IAM o nella concessione.

Il diagramma di flusso è in grado di spiegare alcuni scenari comuni.

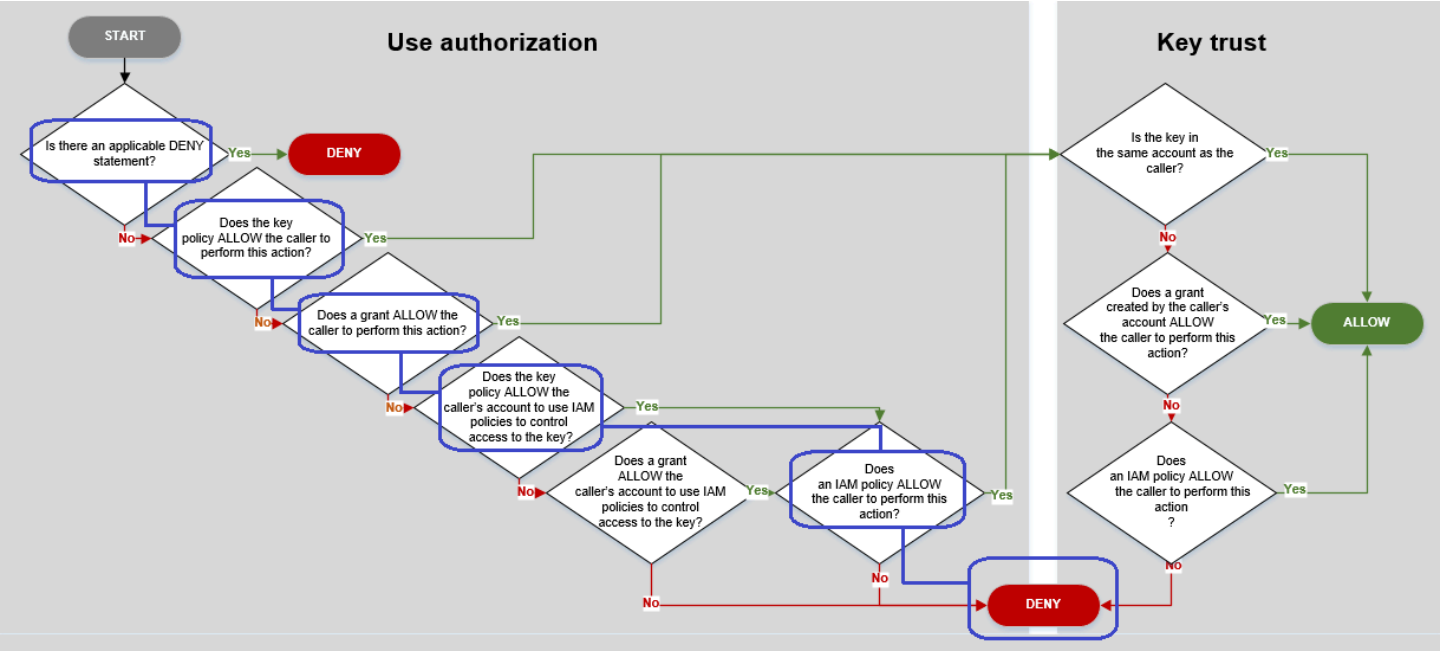
Esempi di autorizzazione

- Esempio 1: all'utente viene negato l'accesso a una chiave KMS nel proprio Account AWS
- Esempio 2: un utente assume un ruolo con l'autorizzazione per l'utilizzo di una chiave KMS in un altro Account AWS

Esempio 1: all'utente viene negato l'accesso a una chiave KMS nel proprio Account AWS

Alice è un utente IAM nell'Account AWS 111122223333. Le è stato negato l'accesso a una chiave KMS nello stesso Account AWS. Perché Alice non è in grado di utilizzare la chiave KMS?

In questo caso, ad Alice è negato l'accesso alla chiave KMS perché non vi è alcuna policy delle chiavi, policy IAM o concessione che le offre le autorizzazioni necessarie. La policy delle chiavi della chiave KMS consente all'Account AWS di utilizzare le policy IAM per controllare l'accesso alla chiave KMS, ma nessuna policy IAM fornisce ad Alice l'autorizzazione per utilizzare la chiave KMS.



Considerare le relative policy per questo esempio.

- La chiave KMS che Alice desidera utilizzare ha la policy delle chiavi predefinita. Questa policy consente all'Account AWS che possiede la chiave KMS di utilizzare le policy IAM per controllare l'accesso alla chiave KMS. Questa policy soddisfa la condizione nel diagramma La policy della chiave CONSENTE agli intermediari di utilizzare le policy IAM per controllare l'accesso alla chiave?.

```
{
  "Version" : "2012-10-17",
  "Id" : "key-test-1",
  "Statement" : [ {
    "Sid" : "Delegate to IAM policies",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "arn:aws:iam::111122223333:root"
    },
    "Action" : "kms:*",
    "Resource" : "*"
  } ]
}
```

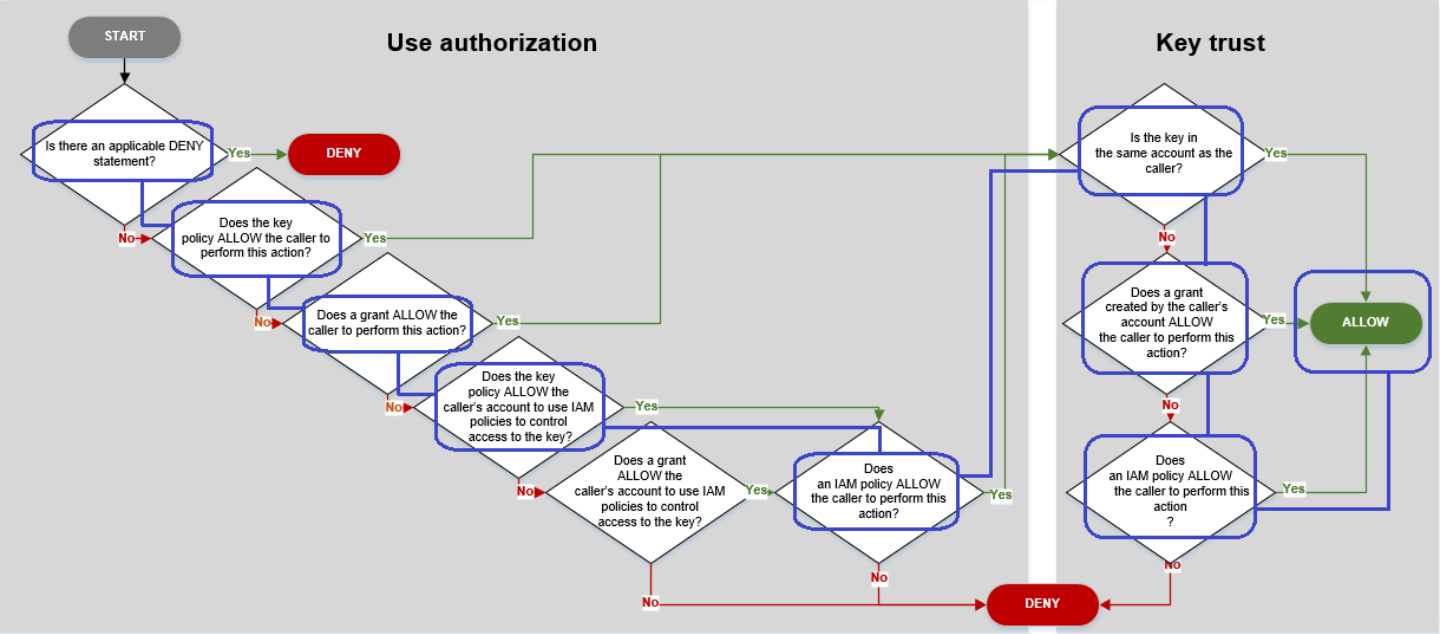
- Non vi è alcuna policy delle chiavi, policy IAM o concessione che consente ad Alice di utilizzare la chiave KMS. Pertanto, ad Alice è negata l'autorizzazione di utilizzare la chiave KMS.

Esempio 2: un utente assume un ruolo con l'autorizzazione per l'utilizzo di una chiave KMS in un altro Account AWS

Bob è un utente nell'account 1 (111122223333). Può utilizzare una chiave KMS nell'account 2 (444455556666) nelle operazioni di crittografia. In che modo è possibile?

> **Tip**
>
> Durante la valutazione di autorizzazioni tra più account, ricordare che la policy della chiave è specificata nell'account della chiave KMS. La policy IAM è specificato nell'account dell'intermediario, anche quando l'autore si trova in un altro account. Per informazioni dettagliate su come fornire l'accesso tra account alle chiavi KMS, consulta Autorizzazione per gli utenti in altri account di utilizzare una chiave KMS.

- La policy delle chiavi per la chiave KMS consente all'account 2 di utilizzare le policy IAM per controllare l'accesso alla chiave KMS.
- La policy chiave per la chiave KMS nell'account 2 consente all'account 1 di utilizzare la chiave KMS nelle operazioni di crittografia. Tuttavia, l'account 1 deve utilizzare le policy IAM in modo da fornire ai principali l'accesso alla chiave KMS.
- Una policy IAM nell'account 1 consente al ruolo `Engineering` di utilizzare la chiave KMS nell'account 2 per operazioni di crittografia.
- Bob, un utente nell'account 1, ha l'autorizzazione per assumere il ruolo `Engineering`.
- Bob può considerare affidabile questa chiave KMS, anche se non si trova nel suo account, una policy IAM nel suo account gli fornisce un'autorizzazione esplicita a utilizzare questa chiave KMS.



Vediamo le policy che consentono a Bob, un utente nell'account 1, di utilizzare la chiave KMS nell'account 2.

- La policy delle chiavi per la chiave KMS consente all'account 2 (444455556666, l'account proprietario della chiave KMS) di utilizzare le policy IAM per controllare l'accesso alla chiave KMS. Questa policy delle chiavi consente inoltre all'account 1 (111122223333) di utilizzare la chiave KMS nelle operazioni di crittografia (specificate nell'elemento `Action` dell'istruzione della policy). Tuttavia, nessuno nell'account 1 può utilizzare la chiave KMS nell'account 2 finché l'account 1 definisce le policy IAM che offrono ai principali l'accesso alla chiave KMS.

  Nel diagramma di flusso, questa policy della chiave nell'account 2 soddisfa la condizione La policy della chiave CONSENTE all'account dell'intermediario di utilizzare le policy IAM per controllare l'accesso alla chiave?.

```
{
    "Id": "key-policy-acct-2",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Permission to use IAM policies",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::444455556666:root"
            },
            "Action": "kms:*",
```

```
            "Resource": "*"
        },
        {
            "Sid": "Allow account 1 to use this KMS key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncryptFrom",
                "kms:ReEncryptTo",
                "kms:GenerateDataKey",
                "kms:GenerateDataKeyWithoutPlaintext",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        }
    ]
}
```

- Una policy IAM nell'Account AWS del chiamante (account 1, 111122223333) concede al principale l'autorizzazione per eseguire operazioni di crittografia tramite la chiave KMS nell'account 2 (444455556666). L'elemento `Action` delega al principale le stesse autorizzazioni che la policy della chiave nell'account 2 ha fornito all'account 1. Per dare queste autorizzazioni al ruolo `Engineering` nell'account 1, questa policy in linea è incorporata nel ruolo `Engineering`.

  Le policy IAM tra più account come questa sono efficaci solo quando la policy della chiave per la chiave KMS nell'account 2 offre all'account 1 l'autorizzazione per utilizzare la chiave KMS. Inoltre, l'account 1 può dare ai propri principal solo l'autorizzazione per eseguire le azioni che la policy della chiave ha dato all'account.

  Nel diagramma di flusso, questo soddisfa la condizione Una policy IAM consente all'intermediario di eseguire questa azione?.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
```

```
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncryptFrom",
                "kms:ReEncryptTo",
                "kms:GenerateDataKey",
                "kms:GenerateDataKeyWithoutPlaintext",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-
west-2:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab"
            ]
        }
    ]
}
```

- Ultimo elemento obbligatorio è la definizione del ruolo `Engineering` nell'account 1. Il `AssumeRolePolicyDocument` nel ruolo consente a Bob di assumere il ruolo `Engineering`.

```
{
    "Role": {
        "Arn": "arn:aws:iam::111122223333:role/Engineering",
        "CreateDate": "2019-05-16T00:09:25Z",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": {
                "Principal": {
                    "AWS": "arn:aws:iam::111122223333:user/bob"
                },
                "Effect": "Allow",
                "Action": "sts:AssumeRole"
            }
        },
        "Path": "/",
        "RoleName": "Engineering",
        "RoleId": "AROA4KJY2TU23Y7NK62MV"
    }
}
```

AWS KMS autorizzazioni

Questa tabella è progettata per aiutarti a comprendere AWS KMS le autorizzazioni in modo da poter controllare l'accesso alle tue risorse. AWS KMS Le definizioni delle intestazioni di colonna vengono visualizzate sotto la tabella.

Per ulteriori informazioni sulle AWS KMS autorizzazioni, consulta la sezione Azioni, risorse e chiavi di condizione relativa all' AWS Key Management Serviceargomento del Service Authorization Reference. Tuttavia, questo argomento non riporta tutte le chiavi di condizione che possono essere utilizzate per rifinire ogni autorizzazione.

> **Note**
>
> Potrebbe essere necessario scorrere orizzontalmente o verticalmente per visualizzare tutti i dati della tabella.

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
CancelKeyDeletion `kms:CancelKeyDeletion`	Policy delle chiavi	No	Chiave KMS	Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
				aws:ResourceTag/tag-key (chiave di condizione AWS globale) km: ViaService
ConnectCustomKeyStore `kms:ConnectCustomKeyStore`	Policy IAM	No	*	km: CallerAccount

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
CreateAlias `kms:CreateAlias` Per utilizzare questa operazione, il chiamante necessita dell'auto rizzazione `kms:CreateAlias` su due risorse: • L'alias (in una policy IAM) • La chiave KMS (in una policy chiave) Per informazioni dettaglia te, vedi Controllo dell'accesso agli alias.	Policy IAM (per l'alias)	No	Alias	Nessuna (in caso di controllo dell'accesso all'alias)
	Policy chiave (per la chiave KMS)	No	Chiave KMS	Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizion eAWS globale) km: ViaService
CreateCustomKeyStore `kms:CreateCustomKeyStore`	Policy IAM	No	*	km: CallerAccount

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
CreateGrant `kms:CreateGrant`	Policy delle chiavi	Sì	Chiave KMS	Condizioni per il contesto di crittografia: kms:: chiave contestuale EncryptionContext km: EncryptionContextKeys Condizioni di concessione: km: GrantConstraintType km: GranteePrincipal km: GrantIsFor AWSResource km: GrantOperations km: RetiringPrincipal Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
				km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizione eAWS globale) km: ViaService
CreateKey `kms:CreateKey`	Policy IAM	No	*	km: BypassPolicyLockoutSafetyCheck km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ViaService aws:RequestTag/tag-key (chiave di condizione eAWS globale) aws:ResourceTag/tag-key (chiave di condizione globale)AWS aws: TagKeys (chiave di condizioneAWS globale)

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
Decrypt `kms:Decrypt`	Policy delle chiavi	Sì	Chiave KMS	Condizioni per le operazioni di crittografia km: EncryptionAlgorithm km: RequestAlias Condizioni per il contesto di crittografia: kms:: chiave contestuale EncryptionContext km: EncryptionContextKeys Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizione AWS globale)

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
				km: ViaService
DeleteAlias `kms:DeleteAlias`	Policy IAM (per l'alias)	No	Alias	Nessuna (in caso di controllo dell'accesso all'alias)
Per utilizzare questa operazione, il chiamante necessita dell'auto rizzazione `kms:Delet eAlias` su due risorse: • L'alias (in una policy IAM) • La chiave KMS (in una policy chiave) Per informazioni dettaglia te, vedi Controllo dell'accesso agli alias.	Policy chiave (per la chiave KMS)	No	Chiave KMS	Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizion eAWS globale) km: ViaService
DeleteCustomKeyStore `kms:DeleteCustomKe yStore`	Policy IAM	No	*	km: CallerAccount

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
DeleteImportedKeyMaterial `kms:DeleteImportedKeyMaterial`	Policy delle chiavi	No	Chiave KMS	Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizione AWS globale) km: ViaService
DescribeCustomKeyStores `kms:DescribeCustomKeyStores`	Policy IAM	No	*	km: CallerAccount

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
DescribeKey `kms:DescribeKey`	Policy delle chiavi	Sì	Chiave KMS	Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizione AWS globale) km: ViaService Altre condizioni: km: RequestAlias

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
DisableKey `kms:DisableKey`	Policy delle chiavi	No	Chiave KMS	Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizione AWS globale) km: ViaService

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
DisableKeyRotation `kms:DisableKeyRotation`	Policy delle chiavi	No	Chiave KMS	Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizione AWS globale) km: ViaService
DisconnectCustomKeyStore `kms:DisconnectCustomKeyStore`	Policy IAM	No	*	km: CallerAccount

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
EnableKey `kms:EnableKey`	Policy delle chiavi	No	Chiave KMS	Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizione globale AWS) km: ViaService

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
EnableKeyRotation `kms:EnableKeyRotation`	Policy delle chiavi	No	Chiave KMS (solo simmetrica)	Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizione AWS globale) km: ViaService

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
Encrypt `kms:Encrypt`	Policy delle chiavi	Sì	Chiave KMS	Condizioni per le operazioni di crittografia km: EncryptionAlgorithm km: RequestAlias Condizioni per il contesto di crittografia: kms:: chiave contestuale EncryptionContext km: EncryptionContextKeys Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizione AWS globale)

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
				km: ViaService

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
GenerateDataKey `kms:GenerateDataKey`	Policy delle chiavi	Sì	Chiave KMS (solo simmetrica)	Condizioni per le operazioni di crittografia km: EncryptionAlgorithm km: RequestAlias Condizioni per il contesto di crittografia: kms:: chiave contestuale EncryptionContext km: EncryptionContextKeys Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizioneAWS globale)

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
				km: ViaService

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
GenerateDataKeyPair `kms:GenerateDataKeyPair`	Policy delle chiavi	Sì	Chiave KMS (solo simmetrica) Genera coppie di chiavi di dati asimmetriche protette da una chiave KMS di crittografia simmetrica.	Condizioni per coppie di chiavi di dati: km: DataKeyPairSpec Condizioni per le operazioni di crittografia km: EncryptionAlgorithm km: RequestAlias Condizioni per il contesto di crittografia: kms:: chiave contestuale EncryptionContext km: EncryptionContextKeys Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
				km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizione AWS globale) km: ViaService

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
GenerateDataKeyPairWithoutPlaintext `kms:GenerateDataKeyPairWithoutPlaintext`	Policy delle chiavi	Sì	Chiave KMS (solo simmetrica) Genera coppie di chiavi di dati asimmetriche protette da una chiave KMS di crittografia simmetrica.	Condizioni per coppie di chiavi di dati: km: DataKeyPairSpec Condizioni per le operazioni di crittografia km: EncryptionAlgorithm km: RequestAlias Condizioni per il contesto di crittografia: kms:: chiave contestuale EncryptionContext km: EncryptionContextKeys Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
				km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizione AWS globale) km: ViaService

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
GenerateDataKeyWithoutPlaintext `kms:GenerateDataKeyWithoutPlaintext`	Policy delle chiavi	Sì	Chiave KMS (solo simmetrica)	Condizioni per le operazioni di crittografia km: EncryptionAlgorithm km: RequestAlias Condizioni per il contesto di crittografia: kms:: chiave contestuale EncryptionContext km: EncryptionContextKeys Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizioneAWS globale)

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
				km: ViaService
GenerateMac `kms:GenerateMac`	Policy delle chiavi	Sì	Chiave KMS	Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizione globale AWS) km: ViaService Condizioni per le operazioni di crittografia: km: MacAlgorithm km: RequestAlias
GenerateRandom `kms:GenerateRandom`	Policy IAM	N/D	*	Nessuno

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
GetKeyPolicy `kms:GetKeyPolicy`	Policy delle chiavi	No	Chiave KMS	Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizione AWS globale) km: ViaService

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
GetKeyRotationStatus `kms:GetKeyRotationStatus`	Policy delle chiavi	Sì	Chiave KMS (solo simmetrica)	Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizione AWS globale) km: ViaService

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
GetParametersForImport `kms:GetParametersForImport`	Policy delle chiavi	No	Chiave KMS	km: WrappingAlgorithm km: WrappingKeySpec Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizione AWS globale) km: ViaService

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
GetPublicKey `kms:GetPublicKey`	Policy delle chiavi	Sì	Chiave KMS (solo asimmetrica)	Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizione AWS globale) km: ViaService Altre condizioni: km: RequestAlias

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
ImportKeyMaterial `kms:ImportKeyMaterial`	Policy delle chiavi	No	Chiave KMS	Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizione AWS globale) km: ViaService Altre condizioni: km: ExpirationModel km: ValidTo
ListAliases `kms:ListAliases`	Policy IAM	No	*	Nessuno

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
ListGrants `kms:ListGrants`	Policy delle chiavi	Sì	Chiave KMS	Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizione AWS globale) km: ViaService Altre condizioni: km: GrantIsForAWSResource

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
ListKeyPolicies `kms:ListKeyPolicies`	Policy delle chiavi	No	Chiave KMS	Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizione AWS globale) km: ViaService
ListKeys `kms:ListKeys`	Policy IAM	No	*	Nessuno

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
ListResourceTags `kms:ListResourceTags`	Policy delle chiavi	No	Chiave KMS	Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizione AWS globale) km: ViaService

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
ListRetirableGrants `kms:ListRetirableGrants`	Policy IAM	L'entità principale specificata deve trovarsi nell'account locale, ma l'operazione restituisce concessioni in tutti gli account.	*	Nessuno

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
PutKeyPolicy `kms:PutKeyPolicy`	Policy delle chiavi	No	Chiave KMS	Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizione AWS globale) km: ViaService Altre condizioni: km: BypassPolicyLockoutSafetyCheck

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione

ReEncrypt
 	
`kms:ReEncryptFrom`
 	
`kms:ReEncryptTo`
 	
Per utilizzare questa operazione, il chiamante necessita dell'auto rizzazione per due chiavi KMS:
 	
• `kms:ReEnc ryptFrom` sulla chiave KMS usata per la decrittografia
• `kms:ReEncryptTo` sulla chiave KMS utilizzata per la crittogra fia
	Policy delle chiavi	Sì	Chiave KMS	Condizioni per le operazioni di crittografia
				
				km: EncryptionAlgorithm
				
				km: RequestAlias
				
				Condizioni per il contesto di crittografia:
				
				kms:: chiave contestuale EncryptionContext
				
				km: EncryptionContextK eys
				
				Condizioni per le operazioni delle chiavi KMS:
				
				km: CallerAccount
				
				km: KeySpec
				
				km: KeyUsage
				
				km: KeyOrigin
				
				km: MultiRegion
				
				km: MultiRegionKeyType
				
				km: ResourceAliases
				
				aws:ResourceTag/tag-key (chiave di condizion eAWS globale)

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
				km: ViaService Altre condizioni: km: ReEncryptOnSameKey
ReplicateKey `kms:ReplicateKey` Per utilizzare questa operazione, il chiamante necessita delle seguenti autorizzazioni: • `kms:ReplicateKey` sulla chiave primaria multiregione • `kms:CreateKey` in una policy IAM nella Regione di replica	Policy delle chiavi	No	Chiave KMS	Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizione AWS globale) km: ViaService Altre condizioni: km: ReplicaRegion

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
RetireGrant `kms:RetireGrant` L'autorizzazione per ritirare una concessione è determinata principal mente dalla concessione. Una policy da sola non può consentire l'accesso a questa operazione. Per ulteriori informazi oni, consulta Ritirare e revocare le concessioni.	Policy IAM Questa autorizza zione non è valida in una policy chiave.	Sì	Chiave KMS	km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizion eAWS globale)

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
RevokeGrant `kms:RevokeGrant`	Policy delle chiavi	Sì	Chiave KMS	Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizione globale AWS) km: ViaService Altre condizioni: km: GrantIsForAWSResource

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
ScheduleKeyDeletion `kms:ScheduleKeyDeletion`	Policy delle chiavi	No	Chiave KMS	Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizione globale) AWS km: ViaService

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
Sign `kms:Sign`	Policy delle chiavi	Sì	Chiave KMS (solo asimmetrica)	Condizioni per la firma e la verifica: km: MessageType km: RequestAlias km: SigningAlgorithm Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizione AWS globale) km: ViaService

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
TagResource `kms:TagResource`	Policy delle chiavi	No	Chiave KMS	Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizioneAWS globale) km: ViaService Condizioni per l'assegnazione di tag: aws:RequestTag/tag-key (chiave di condizioneAWS globale) aws: TagKeys (chiave di condizioneAWS globale)

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
UntagResource `kms:UntagResource`	Policy delle chiavi	No	Chiave KMS	Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizione AWS globale) km: ViaService Condizioni per l'assegnazione di tag: aws:RequestTag/tag-key (chiave di condizione AWS globale) aws: TagKeys (chiave di condizioneAWS globale)

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
UpdateAlias `kms:UpdateAlias` Per utilizzare questa operazione, il chiamante necessita dell'auto rizzazione `kms:UpdateAlias` su tre risorse: • L'alias • La chiave KMS attualmente associata • La chiave KMS appena associata Per informazioni dettaglia te, vedi Controllo dell'accesso agli alias.	Policy IAM (per l'alias)	No	Alias	Nessuna (in caso di controllo dell'accesso all'alias)
	Policy chiave (per le chiavi KMS)	No	Chiave KMS	Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizion eAWS globale) km: ViaService
UpdateCustomKeyStore `kms:UpdateCustomKeyStore`	Policy IAM	No	*	km: CallerAccount

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
UpdateKeyDescription `kms:UpdateKeyDescription`	Policy delle chiavi	No	Chiave KMS	Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizione AWS globale) km: ViaService

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
UpdatePrimaryRegion `kms:UpdatePrimaryRegion` Per utilizzare questa operazione, il chiamante necessita dell'autorizzazione `kms:UpdatePrimaryRegion` sulla chiave primaria multiregione, che diventerà una chiave di replica, e sulla chiave di replica multiregione che diventerà la chiave primaria.	Policy delle chiavi	No	Chiave KMS	Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizione AWS globale) km: ViaService Altre condizioni: km: PrimaryRegion

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
Verify `kms:Verify`	Policy delle chiavi	Sì	Chiave KMS (solo asimmetrica)	Condizioni per la firma e la verifica: km: MessageType km: RequestAlias km: SigningAlgorithm Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizione AWS globale) km: ViaService

Azioni e autorizzazioni	Tipo di policy	Utilizzo per più account	Risorse (per policy IAM)	AWS KMS tasti di condizione
VerifyMac `kms:VerifyMac`	Policy delle chiavi	Sì	Chiave KMS	Condizioni per le operazioni delle chiavi KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (chiave di condizione AWS globale) km: ViaService Condizioni per le operazioni di crittografia: km: MacAlgorithm km: RequestAlias

Descrizioni delle colonne

Le colonne nella tabella forniscono le seguenti informazioni:

- Azioni e autorizzazioni elenca ogni operazione AWS KMS API e l'autorizzazione che consente l'operazione. È possibile specificare l'operazione nell'elemento `Action` di un'istruzione di policy.

- Tipo di policy indica se l'autorizzazione può essere utilizzata in una policy chiave o in una policy IAM.

  Policy chiave significa che puoi specificare l'autorizzazione nella policy chiave. Quando la policy chiave contiene l'istruzione di policy che consente policy IAM, puoi specificare l'autorizzazione in una policy IAM.

  Policy IAM significa che puoi specificare l'autorizzazione solo in una policy IAM.

- Utilizzo tra account mostra le operazioni che gli utenti autorizzati possono eseguire sulle risorse in un Account AWSdiverso.

  Un valore di Sì significa che le entità principali possono eseguire l'operazione sulle risorse in un Account AWSdiverso.

  Un valore di No significa che le entità principali possono eseguire l'operazione solo sulle risorse nel proprio Account AWS.

  Se si concede a un'entità in un account diverso un'autorizzazione che non può essere utilizzata su una risorsa tra account, l'autorizzazione non è valida. Ad esempio, se concedi a un responsabile di un altro account kms: l'TagResourceautorizzazione a utilizzare una chiave KMS nel tuo account, i suoi tentativi di taggare la chiave KMS nel tuo account falliranno.

- Resources elenca le AWS KMS risorse a cui si applicano le autorizzazioni. AWS KMS supporta due tipi di risorse: una chiave KMS e un alias. In una policy delle chiavi, il valore dell'elemento `Resource` è sempre `*`, che indica la chiave KMS collegata alla policy delle chiavi.

  Utilizza i seguenti valori per rappresentare una AWS KMS risorsa in una policy IAM.

  Chiave KMS

  Quando la risorsa è una chiave KMS utilizza l'ARN chiave. Per assistenza, consulta the section called “Individuazione dell'ID e dell'ARN della chiave”.

  `arn:`*`AWS_partition_name`*`:kms:`*`AWS_Region`*`:`*`AWS_account_ID`*`:key/`*`key_ID`*

  Per esempio:

  arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

Alias

Quando la risorsa è un alias, utilizza l'ARN dell'alias. Per assistenza, consulta the section called "Individuazione del nome e dell'ARN dell'alias".

`arn:AWS_partition_name:kms:AWS_region:AWS_account_ID:alias/alias_name`

Per esempio:

arn:aws:kms:us-west- 2:111122223333:alias/ ExampleAlias

***** (asterisco)

Quando l'autorizzazione non si applica a una determinata risorsa (chiave KMS o alias) utilizza un asterisco (`*`).

In una policy IAM per un' AWS KMS autorizzazione, un asterisco nell'elemento indica tutte le risorse (chiavi e alias KMS). `Resource` AWS KMS Puoi anche utilizzare un asterisco nell'`Resource`elemento quando l' AWS KMS autorizzazione non si applica a particolari chiavi o alias KMS. Ad esempio, quando si consente o si nega l'autorizzazione `kms:CreateKey` o `kms:ListKeys`, è possibile impostare l'elemento `Resource` su `*` o su una variante specifica dell'account, ad esempio `arn:AWS_partition_name:kms:AWS_region:AWS_account_ID:*`.

- AWS KMS condition keys elenca le chiavi di AWS KMS condizione che è possibile utilizzare per controllare l'accesso all'operazione. Puoi specificare condizioni nell'elemento `Condition` di una policy. Per ulteriori informazioni, consulta AWS KMS chiavi di condizione. Questa colonna include anche le chiavi di condizioneAWS globali supportate da AWS KMS, ma non da tutti i AWS servizi.

Test delle autorizzazioni

Per utilizzare AWS KMS, devi disporre di credenziali che AWS può utilizzare per autenticare le richieste API. Le credenziali devono includere l'autorizzazione per accedere alle chiavi KMS e agli alias. Le autorizzazioni sono determinate dalle policy delle chiavi, dalle policy IAM, dalle concessioni e dai controlli di accesso multi-account. Oltre a controllare l'accesso alle chiavi KMS, puoi controllare l'accesso al tuo CloudHSM e ai tuoi archivi di chiavi personalizzate.

Puoi specificare il parametro dell'API `DryRun` per controllare se disponi delle autorizzazioni necessarie a utilizzare le chiavi AWS KMS. Puoi utilizzare anche `DryRun` per controllare se i parametri della richiesta in una chiamata API AWS KMS sono specificati correttamente.

Argomenti

Qual è il DryRun parametro?

`DryRun` è un parametro dell'API opzionale specificato per controllare se l'esito delle chiamate API AWS KMS sarà positivo. Usa `DryRun` per testare la chiamata API, prima di effettuare realmente la chiamata a AWS KMS. Puoi effettuare i controlli seguenti:

- che disponi delle autorizzazioni necessarie per utilizzare le chiavi AWS KMS;
- che hai specificato correttamente i parametri nella chiamata.

AWS KMS supporta l'utilizzo del parametro `DryRun` in determinate azioni dell'API:

- CreateGrant
- Decrypt
- Encrypt
- GenerateDataKey
- GenerateDataKeyPair
- GenerateDataKeyPairWithoutPlaintext
- GenerateDataKeyWithoutPlaintext
- GenerateMac
- ReEncrypt
- RetireGrant
- RevokeGrant
- Sign
- Verify
- VerifyMac

L'utilizzo del parametro `DryRun` comporterà dei costi e verrà fatturato come richiesta API standard. Per ulteriori informazioni sui prezzi di AWS KMS, consulta Prezzi di AWS Key Management Service.

Tutte le richieste API con il parametro `DryRun` si applicano alla quota della richiesta API e possono comportare un'eccezione di limitazione della larghezza di banda della rete se superi la quota della richiesta API. Ad esempio, la chiamata Decrypt con `DryRun` o senza `DryRun` viene conteggiata sulla stessa quota delle operazioni crittografiche. Per ulteriori informazioni, consulta Limitazione delle richieste AWS KMS.

Ogni chiamata indirizzata a un'operazione dell'API AWS KMS viene acquisita come evento e registrata in un log di AWS CloudTrail. L'output di tutte le operazioni che specificano il `DryRun` parametro viene visualizzato nel CloudTrail registro. Per ulteriori informazioni, consulta Registrazione delle chiamate API AWS KMS con AWS CloudTrail.

Specificazione DryRun con l'API

Per utilizzare `DryRun`, specifica il parametro `–dry-run` nei comandi della AWS CLI e nelle chiamate API AWS KMS che supportano il parametro. In tal modo, AWS KMS controllerà se l'esito della chiamata sarà positivo. L'esito delle chiamate AWS KMS che utilizzano `DryRun` sarà sempre negativo e verrà restituito un messaggio con informazioni sul motivo dell'esito negativo della chiamata. Il messaggio può includere le seguenti eccezioni:

- `DryRunOperationException`: l'esito della richiesta sarebbe stato positivo se non fosse stato specificato `DryRun`.
- `ValidationException`: l'esito della richiesta è negativo perché è stato specificato un parametro dell'API errato.
- `AccessDeniedException`: non disponi delle autorizzazioni per l'esecuzione dell'azione dell'API specificata sulla risorsa KMS.

Ad esempio, il comando seguente utilizza l'CreateGrantoperazione e crea una concessione che consente agli utenti autorizzati ad assumere il `keyUserRole` ruolo di chiamare l'operazione Decrypt su una chiave KMS simmetrica specificata. Il parametro `DryRun` è specificato.

```
$  aws kms create-grant \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/keyUserRole \
    --operations Decrypt \
    --dry-run
```

Chiavi per uso speciale

AWS Key Management Service (AWS KMS) supporta diversi tipi di chiavi per usi diversi.

Quando crei una AWS KMS key, per impostazione predefinita ottieni una chiave KMS di crittografia simmetrica. In AWS KMS, una chiave KMS di crittografia simmetrica rappresenta una chiave AES-GCM a 256 bit utilizzata per la crittografia e la decrittografia, tranne nelle regioni della Cina, dove rappresenta una chiave simmetrica a 128 bit simmetrica che utilizza la crittografia SM4. Il materiale della chiave simmetrica mantiene sempre AWS KMS crittografato. A meno che la tua attività non richieda esplicitamente chiavi HMAC o di crittografia asimmetrica, le chiavi KMS di crittografia simmetrica, grazie alle quali AWS KMS è sempre crittografato, sono una scelta valida. Inoltre, i servizi AWS integrati con AWS KMS usano soltanto chiavi KMS di crittografia simmetrica per crittografare i dati. Questi servizi non supportano la crittografia con chiavi KMS asimmetriche.

Puoi utilizzare una chiave KMS di crittografia simmetrica in AWS KMS per crittografare, decrittografare e crittografare nuovamente i dati, generare chiavi di dati e coppie di chiavi di dati e generare stringhe di byte casuali. Puoi importare il materiale della chiave di tua proprietà in una chiave KMS di crittografia simmetrica e creare chiavi KMS di crittografia simmetrica negli archivi delle chiavi personalizzate. Per una tabella di confronto delle operazioni eseguibili sulle chiavi KMS simmetriche e asimmetriche, consulta la sezione Documentazione di riferimento dei tipi di chiave.

AWS KMS supporta anche i seguenti tipi di chiavi KMS per scopi speciali:

- Chiavi RSA asimmetriche per la crittografia delle chiavi pubbliche
- Chiavi RSA ed ECC asimmetriche per la firma e la verifica
- Chiavi SM2 asimmetriche (solo regioni della Cina) per la crittografia a chiave pubblica o firma e verifica
- Chiavi HMAC per generare e verificare i codici di autenticazione dei messaggi basati su hash
- Chiavi a più regionimulti-regione (simmetriche e asimmetriche) che funzionano come copie della stessa chiave in Regioni AWS diverse
- Chiavi con materiale chiave importato fornito dall'utente
- Chiavi in un archivio delle chiavi personalizzate che è supportato da un cluster AWS CloudHSM o da un gestore delle chiavi esterne al di fuori di AWS.

Scelta di un tipo di chiave KMS

AWS KMS supporta diversi tipi di chiavi KMS: chiavi crittografiche simmetrica, chiavi HMAC simmetriche, chiavi crittografiche asimmetrica e chiavi di firma asimmetrica.

Le chiavi KMS differiscono perché contengono materiali crittografici diversi.

- Chiave KMS di crittografia simmetrica: rappresenta una chiave crittografica AES-GCM a 256 bit, tranne nelle regioni della Cina, dove rappresenta una chiave crittografica SM4 a 128 bit. Il materiale della chiave simmetrica mantiene sempre AWS KMS crittografato. Per utilizzare la chiave KMS di crittografia simmetrica devi richiamare AWS KMS.

  Le chiavi crittografiche simmetrica, che sono le chiavi KMS predefinite, sono ideali per la maggior parte dei casi d'uso. Se hai bisogno di una chiave KMS per proteggere i tuoi dati in un Servizio AWS, utilizza una chiave crittografica simmetrica a meno che non ti venga richiesto di utilizzare un altro tipo di chiave.
- Chiave KMS asimmetrica: rappresenta una coppia di chiavi, una pubblica e una privata, correlate matematicamente utilizzabili per la crittografia e la decrittazione o per la firma e la verifica, ma non per entrambe le azioni. Grazie alla chiave privata il servizio AWS KMS non è mai in chiaro. Puoi utilizzare la chiave pubblica all'interno di AWS KMS, chiamando le azioni API AWS KMS, o scaricare la chiave pubblica e usarla all'esterno di AWS KMS.
- Chiave KMS HMAC (simmetrica): rappresenta una chiave simmetrica di lunghezza variabile utilizzata per generare e verificare i codici di autenticazione dei messaggi basati su hash. Il materiale della chiave di una chiave KMS HMAC mantiene sempre AWS KMS crittografato. Per utilizzare la chiave KMS HMAC, devi richiamare AWS KMS.

Il tipo di chiave KMS creato dipende in gran parte dalla modalità di utilizzo della chiave KMS, dai requisiti di sicurezza e dai requisiti di autorizzazione. Tieni presente che quando crei la chiave KMS, la configurazione crittografica della chiave KMS, tra cui la specifica e l'utilizzo della chiave, viene stabilita in fase di creazione della chiave KMS e non può essere modificata.

Utilizza le indicazioni che seguono per determinare quale tipo di chiave KMS è necessario in base al caso d'uso.

Crittografia e decrittografia dei dati

Utilizza una chiave KMS simmetrica per la maggior parte dei casi d'uso che richiedono la crittografia e la decrittazione dei dati. L'algoritmo di crittografia simmetrica utilizzato da AWS KMS

è veloce, efficiente e garantisce la riservatezza e l'autenticità dei dati. Supporta la crittografia autenticata con dati autenticati aggiuntivi (AAD), definiti come contesto di crittografia. Questo tipo di chiave KMS richiede che sia il mittente che il destinatario dei dati crittografati dispongano di credenziali AWS valide per chiamare AWS KMS.

Se il tuo caso d'uso prevede che gli utenti adottino la crittografia all'esterno di AWS poiché non possono chiamare AWS KMS, le chiavi KMS asimmetriche costituiscono una valida scelta. Puoi distribuire la parte pubblica della chiave KMS asimmetrica per consentire a questi utenti di crittografare i dati. E le applicazioni che devono decriptare quei dati possono utilizzare la parte privata della chiave KMS asimmetrica all'interno di AWS KMS.

Firma dei messaggi e verifica delle firme

Per firmare i messaggi e verificare le firme, è necessario utilizzare una chiave KMS asimmetrica. Puoi utilizzare una chiave KMS con una specifica della chiave che rappresenta una coppia di chiavi RSA, una coppia di chiavi basate su curva ellittica (ECC) o una coppia di chiavi SM2 (solo regioni della Cina). La specifica della chiave scelta è determinata dall'algoritmo di firma che desideri utilizzare. Gli algoritmi di firma ECDSA supportati dalle coppie di chiavi ECC sono consigliati rispetto agli algoritmi di firma RSA. Tuttavia, potrebbe essere necessario utilizzare una determinata specifica della chiave e un algoritmo di firma per supportare gli utenti che verificano le firme all'esterno di AWS.

Esecuzione della crittografia a chiave pubblica

Per eseguire la crittografia a chiave pubblica, è necessario utilizzare una chiave KMS asimmetrica con una specifica della chiave RSA o una specifica della chiave SM2 (solo regioni della Cina). Per crittografare i dati in AWS KMS con la chiave pubblica di una coppia di chiavi KMS, utilizza l'operazione Encrypt (crittografa). Puoi anche scaricare la chiave pubblica e condividerla con le parti che devono crittografare i dati all'esterno di AWS KMS.

Quando scarichi la chiave pubblica di una chiave KMS asimmetrica, puoi utilizzarla all'esterno di AWS KMS. Tuttavia, non è più soggetta ai controlli di sicurezza che proteggono la chiave KMS in AWS KMS. Ad esempio, non puoi utilizzare le policy né le concessioni delle chiavi AWS KMS per controllare l'utilizzo della chiave pubblica. Né puoi controllare se la chiave viene utilizzata solo per la crittografia e la decrittografia tramite gli algoritmi di crittografia supportati da AWS KMS. Per ulteriori dettagli, consulta la pagina sulle considerazioni speciali per il download delle chiavi pubbliche.

Per decriptare i dati crittografati con la chiave pubblica all'esterno di AWS KMS, chiamare l'azione Decrypt. L'operazione `Decrypt` non riesce se i dati sono stati crittografati con una

chiave pubblica di una chiave KMS con l'utilizzo della chiave di `SIGN_VERIFY`. Avrà anche esito negativo se i dati sono stati crittografati utilizzando un algoritmo che AWS KMS non supporta per le specifiche delle chiavi selezionate. Per ulteriori informazioni sulle specifiche principali e sugli algoritmi supportati, consulta Asymmetric key specs (specifiche delle chiavi asimmetriche).

Per evitare questi errori, chiunque utilizzi una chiave pubblica all'esterno di AWS KMS deve archiviare la configurazione della chiave. La AWS KMS console e la GetPublicKeyrisposta forniscono le informazioni da includere quando si condivide la chiave pubblica.

Generazione e verifica dei codici HMAC

Per generare e verificare i codici di autenticazione dei messaggi basati su hash, utilizza una chiave KMS HMAC. Quando crei una chiave HMAC in AWS KMS, AWS KMS crea e protegge il materiale della chiave e si assicura che utilizzi gli algoritmi MAC corretti per la tua chiave. I codici HMAC possono essere utilizzati anche come numeri pseudo-casuali e, in alcuni scenari, per la firma simmetrica e la tokenizzazione.

Le chiavi KMS HMAC sono chiavi simmetriche. Quando crei una chiave KMS HMAC nella console AWS KMS, scegli il tipo di chiave `Symmetric`.

Utilizzo con i servizi AWS

Per creare una chiave KMS da utilizzare con un servizio AWS integrato con AWS KMS, consulta la documentazione relativa al servizio. I servizi AWS che crittografano i dati richiedono una chiave KMS di crittografia simmetrica.

Oltre a queste considerazioni, le operazioni crittografiche sulle chiavi KMS con specifiche della chiave diverse hanno prezzi e quote di richieste differenti. Per informazioni sui prezzi di AWS KMS, consulta la pagina dei prezzi di AWS Key Management Service. Per informazioni sulle quote di richieste, consulta Quote di richieste.

Selezione dell'utilizzo della chiave

L'utilizzo della chiave di una chiave KMS determina se la chiave KMS viene usata per la crittografia e la decrittografia, per la firma e la verifica delle firme oppure per la generazione e la verifica di tag HMAC. Ogni chiave KMS ha un solo utilizzo. L'utilizzo di una chiave KMS per più di un tipo di operazioni rende il prodotto di tutte le operazioni più vulnerabile agli attacchi.

Come illustrato nella tabella seguente, le chiavi KMS di crittografia simmetrica possono essere utilizzate solo per la crittografia e la decrittografia. Le chiavi KMS HMAC possono essere utilizzate

solo per generare e verificare i codici HMAC. Le chiavi KMS basate su curva ellittica (ECC) possono essere utilizzate solo per la firma e la verifica. La scelta dell'utilizzo della chiave deve essere effettuata solo per le chiavi KMS RSA.

Utilizzo valido per i tipi di chiavi KMS

Tipo di chiave KMS	Encrypt and decrypt (Crittografa e decripta) ENCRYPT_DECRYPT	Sign and Verify (Firma e verifica) SIGN_VERIFY	Genera e verifica MAC GENERATE_VERIFY_MAC
Chiavi KMS di crittografia simmetrica	✓	⊗	⊗
Chiavi KMS HMAC (simmetriche)	⊗	⊗	✓
Chiavi KMS asimmetriche con coppie di chiavi RSA	✓	✓	⊗
Chiavi KMS asimmetriche con coppie di chiavi ECC	⊗	✓	⊗
Chiavi KMS asimmetriche con coppie di chiavi SM2 (solo regioni della Cina)	✓	✓	⊗

Nella console AWS KMS, scegli innanzitutto il tipo di chiave (simmetrica o asimmetrica) e l'utilizzo della chiave. Il tipo di chiave scelto determina quali opzioni di utilizzo della chiave verranno visualizzate. L'utilizzo della chiave scelto determina quali specifiche della chiave, se previste, verranno visualizzate.

Per scegliere un utilizzo della chiave nella console AWS KMS:

- Per le chiavi KMS di crittografia simmetrica (impostazione predefinita), scegli Encrypt and decrypt (Crittografa e decrittografa).
- Per le chiavi KMS HMAC, scegli Generate and verify MAC (Genera e verifica MAC).
- Per le chiavi KMS con materiale della chiave basata su curva ellittica (ECC), scegli Sign and verify (Firma e verifica).
- Per le chiavi KMS con materiale della chiave RSA, scegli Encrypt and decrypt (Crittografa e decrittografa) o Sign and verify (Firma e verifica).
- Per le chiavi KMS con materiale della chiave SM2, scegli Encrypt and decrypt (crittografa e decrittografa) o Sign and verify (Firma e verifica). La specifica della chiave SM2 è disponibile solo nelle regioni della Cina.

Per consentire ai mandanti di creare chiavi KMS solo per un particolare utilizzo di chiavi, usa la chiave kms: KeyUsage condition. Puoi inoltre utilizzare la `kms:KeyUsage` chiave di condizione per consentire ali principali di chiamare operazioni API per una chiave KMS in base al relativo utilizzo della chiave. Ad esempio, puoi consentire l'autorizzazione a disabilitare una chiave KMS solo se l'utilizzo della chiave è SIGN_VERIFY.

Selezione delle specifiche della chiave

Quando crei una chiave KMS asimmetrica o una chiave KMS HMAC, selezioni la relativa specifica della chiave. La specifica della chiave, che è una proprietà di ogni AWS KMS key, rappresenta la configurazione crittografica della tua chiave KMS. La specifica della chiave viene scelta in fase di creazione della chiave KMS e non può essere modificata in seguito. Se hai selezionato la specifica della chiave errata, elimina la chiave KMS e creane una nuova.

> **Note**
>
> La specifica della chiave per una chiave del servizio di gestione delle chiavi era nota come "specifica chiave master cliente". Il `CustomerMasterKeySpec` parametro dell'CreateKeyoperazione è obsoleto. Utilizza invece il parametro `KeySpec`. La risposta delle DescribeKeyoperazioni `CreateKey` and include un `CustomerMasterKeySpec` membro `KeySpec` and con lo stesso valore.

La specifica della chiave determina se la chiave KMS è simmetrica o asimmetrica, il tipo di materiale della chiave nella chiave KMS, gli algoritmi di crittografia, gli algoritmi di firma o gli algoritmi del codice

di autenticazione dei messaggi (MAC) supportati da AWS KMS per la chiave KMS. La specifica della chiave scelta è in genere determinata dal caso d'uso e dai requisiti normativi. Tuttavia, le operazioni crittografiche sulle chiavi KMS con specifiche diverse della chiave ECC hanno prezzi differenti e sono soggette a varie quote. Per i dettagli sui prezzi, vedere Prezzi di AWS Key Management Service. Per informazioni sulle quote di richieste, consulta Quote di richieste.

Per determinare le specifiche chiave che i responsabili del tuo account possono utilizzare per le chiavi KMS, usa la chiave kms: KeySpec condition.

AWS KMS supporta le seguenti specifiche della chiave per le chiavi KMS:

Specifica della chiave crittografica simmetrica (impostazione predefinita)

- SYMMETRIC_DEFAULT

Specifiche della chiave HMAC

- HMAC_224
- HMAC_256
- HMAC_384
- HMAC_512

Specifiche della chiave RSA (crittografia e decrittografia o firma e verifica)

- RSA_2048
- RSA_3072
- RSA_4096

Specifiche della chiave basata su curva ellittica

- Coppie di chiavi basate su curva ellittica asimmetriche consigliate da NIST (firma e verifica)
  - ECC_NIST_P256 (secp256r1)
  - ECC_NIST_P384 (secp384r1)
  - ECC_NIST_P521 (secp521r1)
- Altre coppie di chiavi asimmetriche basate su curva ellittica (firma e verifica)
  - ECC_SECG_P256K1 (secp256k1), comunemente usate per la criptovaluta.

Specifiche della chiave SM2 (crittografia e decrittografia o firma e verifica)

- SM2 (solo regioni della Cina)

Chiavi asimmetriche in AWS KMS

AWS KMS supporta chiavi KMS asimmetriche che rappresentano una coppia di chiavi pubblica e privata RSA, a curva ellittica (ECC) o SM2 (solo regioni della Cina) correlate matematicamente. Queste coppie di chiavi sono generate nei moduli di sicurezza hardware AWS KMS certificati ai sensi del Programma di convalida dei moduli crittografici FIPS 140-2, tranne nelle Regioni Cina (Pechino) e Cina (Ningxia). La chiave privata non lascia mai i moduli HSM AWS KMS non crittografati. In alternativa, è possibile scaricare la chiave pubblica e utilizzarla all'esterno di AWS. È possibile creare chiavi KMS asimmetriche per eseguire la crittografia e la decrittazione o la firma e la verifica, ma non per entrambe le operazioni.

È possibile creare e gestire le chiavi KMS nell'Account AWS, nonché impostare le policy chiave, le policy IAM e le concessioni che controllano l'accesso alle chiavi KMS, abilitare e disabilitare le chiavi KMS, creare tag e alias ed eliminare le chiavi KMS. È possibile controllare tutte le operazioni che utilizzano o gestiscono le chiavi KMS in AWS nei registri AWS CloudTrail.

AWS KMS fornisce inoltre coppie di chiavi dati asimmetriche progettate per essere utilizzate per la crittografia lato client all'esterno di AWS KMS. La chiave privata in una coppia di chiavi dati simmetriche è protetta da una chiave KMS di crittografia simmetrica in AWS KMS.

In questo argomento viene descritto il funzionamento delle chiavi KMS asimmetriche, vengono illustrate le differenze rispetto ad altre chiavi KMS e viene spiegato come decidere il tipo di chiave KMS necessario per proteggere i dati. Viene inoltre spiegato come funzionano le coppie di chiavi dati asimmetriche e come usarle all'esterno di AWS KMS.

Regioni

Le chiavi KMS simmetriche e le coppie di chiavi di dati asimmetriche sono supportate in tutte le Regioni Regioni AWS supportate da AWS KMS.

Ulteriori informazioni

- Per creare chiavi KMS asimmetriche, consultare Creazione di chiavi KMS asimmetriche. Per creare chiavi KMS di crittografia simmetrica, consulta la sezione Creazione di chiavi.
- Per creare chiavi KMS asimmetriche multi-regione, consulta la sezione Creazione di chiavi multiregione.
- Per scoprire se una chiave KMS è simmetrica o asimmetrica, consulta Individuazione di chiavi KMS asimmetriche.

- Per una tabella di confronto delle operazioni dell'API AWS KMS applicabili a ciascun tipo di chiave KMS, consulta the section called “Documentazione di riferimento dei tipi di chiave”.
- Per controllare l'accesso alle specifiche della chiave, l'utilizzo della chiave, gli algoritmi di crittografia e gli algoritmi di firma che i principali dell'account possono utilizzare per le chiavi KMS, consulta the section called “AWS KMS chiavi di condizione”.
- Per informazioni sulle quote di richieste applicabili ai diversi tipi di chiavi KMS, consulta the section called “Quote di richieste”.
- Per informazioni su come firmare messaggi e verificare le firme con chiavi KMS asimmetriche, consulta Firma digitale con le nuove chiavi asimmetriche di AWS KMS nel Blog di AWS sulla sicurezza.

Argomenti

Chiavi KMS asimmetriche

Puoi creare una chiave KMS asimmetrica in AWS KMS. Una chiave KMS asimmetrica rappresenta una coppia di chiavi, una pubblica e una privata, correlate matematicamente. Puoi distribuire la chiave pubblica anche a qualcuno che non consideri attendibile, ma la chiave privata deve essere tenuta segreta.

In una chiave KMS asimmetrica la chiave privata viene creata in AWS KMS e fa in modo che il servizio AWS KMS non sia mai in chiaro. Per utilizzare la chiave privata, è necessario chiamare AWS KMS. Puoi utilizzare la chiave pubblica all'interno di AWS KMS chiamando le azioni API AWS KMS. In alternativa, puoi scaricare la chiave pubblica e utilizzarla all'esterno di AWS KMS.

Se il tuo caso d'uso prevede che gli utenti adottino la crittografia all'esterno di AWS poiché non possono chiamare AWS KMS, le chiavi KMS asimmetriche costituiscono una valida scelta. Tuttavia, se stai creando una chiave KMS per crittografare i dati archiviati o gestiti in un servizio AWS, utilizza una chiave KMS di crittografia simmetrica. I servizi AWS integrati con AWS KMS usano

soltanto chiavi KMS di crittografia simmetrica per crittografare i dati. Questi servizi non supportano la crittografia con chiavi KMS asimmetriche.

AWS KMS supporta tre tipi di chiavi KMS asimmetriche.

- Chiavi KMS RSA: chiave KMS con una coppia di chiavi RSA per eseguire la crittografia e la decrittografia o la firma e la verifica (ma non entrambe le azioni). AWS KMS supporta lunghezze di chiave differenti per diversi requisiti di sicurezza.
- Chiavi KMS basate su curva ellittica (ECC): chiave KMS con una coppia di chiavi basate su curva ellittica per la firma e la verifica. AWS KMS supporta diverse curve di uso comune.
- Chiavi KMS SM2 (solo regioni della Cina): una chiave KMS con una coppia di chiavi SM2 per eseguire la crittografia e la decrittografia o la firma e la verifica (non entrambe le azioni).

Per maggiori informazioni sulla configurazione della chiave asimmetrica, consulta la sezione Scelta di un tipo di chiave KMS. Per informazioni tecniche sugli algoritmi di crittografia e firma supportati da AWS KMS per le chiavi KMS RSA, consulta le specifiche della chiave RSA. Per informazioni tecniche sugli algoritmi di firma supportati da AWS KMS per le chiavi KMS ECC, consulta le specifiche della chiave basata su curva ellittica. Per informazioni tecniche sugli algoritmi di crittografia e firma supportati da AWS KMS per le chiavi KMS SM2 (solo regioni della Cina), consulta le specifiche della chiave SM2.

Per una tabella di confronto delle azioni eseguibili su chiavi KMS simmetriche e asimmetriche, consulta Confronto tra chiavi KMS simmetriche e asimmetriche. Per informazioni su come determinare se una chiave KMS è simmetrica o asimmetrica, consulta Individuazione di chiavi KMS asimmetriche.

Regioni

Le chiavi KMS simmetriche e le coppie di chiavi di dati asimmetriche sono supportate in tutte le Regioni Regioni AWS supportate da AWS KMS.

Creazione di chiavi KMS asimmetriche

Puoi creare chiavi KMS asimmetriche nella AWS KMS console, utilizzando l'CreateKeyAPI o utilizzando un modello. AWS CloudFormation Una chiave KMS asimmetrica rappresenta una coppia di chiavi pubbliche e private che può essere utilizzata per la crittografia o la firma. La chiave privata rimane all'interno di AWS KMS. Per scaricare la chiave pubblica per usarla al di fuori di AWS KMS, consultare Download delle chiavi pubbliche.

Se stai creando una chiave KMS per crittografare i dati archiviati o gestiti in un servizio AWS, utilizza una chiave KMS di crittografia simmetrica. I servizi AWS integrati con AWS KMS non supportano le chiavi KMS asimmetriche. Per informazioni su come decidere se creare una chiave KMS simmetrica o asimmetrica, consulta la sezione Scelta di un tipo di chiave KMS.

Per informazioni sulle autorizzazioni richieste per la creazione di chiavi KMS, consultare Autorizzazioni per la creazione di chiavi KMS.

Argomenti

- Creazione di chiavi KMS asimmetriche (console)
- Creazione di chiavi asimmetriche KMS (API AWS KMS)

Creazione di chiavi KMS asimmetriche (console)

Puoi utilizzare la AWS Management Console per creare AWS KMS keys asimmetriche (chiavi KMS). Ogni chiave KMS asimmetrica rappresenta una coppia di chiavi pubbliche e private.

> **Important**
>
> Non includere informazioni riservate o sensibili nell'alias, nella descrizione o nei tag. Questi campi possono apparire in testo semplice nei CloudTrail log e in altri output.

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.
4. Scegliere Create key (Crea chiave).
5. Per creare una chiave KMS asimmetrica, in Key type (Tipo di chiave) scegli Asymmetric (Asimmetrica).

   Per informazioni su come creare una chiave KMS di crittografia simmetrica nella console AWS KMS, consulta la sezione Creazione di chiavi KMS di crittografia simmetrica (console).
6. Per creare una chiave KMS asimmetrica per la crittografia a chiave pubblica, in Key usage (Utilizzo chiave) scegliere Encrypt and decrypt (Crittografa e decritta). In alternativa, per creare

una chiave KMS asimmetrica per la firma dei messaggi e la verifica delle firme, in Key usage (Utilizzo chiave) scegliere Sign and verify (Firma e verifica).

Per informazioni sulla scelta di un valore di utilizzo chiave, consulta Selezione dell'utilizzo della chiave.

7. Seleziona le specifiche (Key spec (Specifiche chiave)) per la tua chiave KMS asimmetrica.

   Spesso la scelta delle specifiche chiave è determinata da requisiti normativi, di sicurezza o aziendali. Potrebbe essere influenzata anche dalla dimensione dei messaggi che è necessario crittografare o firmare. In generale, le chiavi di crittografia più lunghe sono più resistenti agli attacchi a forza bruta.

   Per informazioni sulla scelta di una specifica di chiave, consulta Selezione delle specifiche della chiave.

8. Seleziona Avanti.

9. Digita un alias per la chiave KMS. Un nome di alias non può iniziare con **`aws/`**. Il prefisso **`aws/`** è riservato da Amazon Web Services per rappresentare le Chiavi gestite da AWS nel tuo account.

   Un record alias è un nome che può essere utilizzato per identificare la chiave KMS nella console e in alcune API AWS KMS. È consigliabile scegliere un alias che indica il tipo di dati che desideri proteggere o l'applicazione che desideri utilizzare con la chiave KMS.

   Gli alias sono obbligatori quando si crea una chiave KMS nella AWS Management Console. Non è possibile specificare un alias quando si utilizza l'CreateKeyoperazione, ma è possibile utilizzare la console o l'CreateAliasoperazione per creare un alias per una chiave KMS esistente. Per informazioni dettagliate, vedi Utilizzo di alias.

10. (Facoltativo) Digita una descrizione per la chiave KMS.

    Inserire una descrizione che illustra il tipo di dati che si desidera proteggere o l'applicazione che si desidera utilizzare con la chiave KMS.

    Puoi aggiungere una descrizione ora o aggiornarla in qualsiasi momento, a meno che lo stato della chiave non sia `Pending Deletion` o `Pending Replica Deletion`. Per aggiungere, modificare o eliminare la descrizione di una chiave gestita dal cliente esistente, modifica la descrizione nella AWS Management Console o utilizza l'operazione. UpdateKeyDescription

11. (Facoltativo) Digitare una chiave di tag e un valore di tag facoltativo. Per aggiungere più di un tag alla chiave KMS scegli Add tag (Aggiungi tag).

Quando aggiungi i tag alle risorse AWS, AWS genera un report di allocazione dei costi in cui l'utilizzo e i costi sono aggregati in base ai tag. I tag possono essere utilizzati anche per controllare l'accesso a una chiave KMS. Per informazioni sull'assegnazione di tag delle chiavi KMS, consulta Chiavi di tagging e ABAC per AWS KMS.

12. Seleziona Next (Successivo).
13. Seleziona i ruoli e gli utenti IAM che possono gestire la chiave KMS.

> **Note**
>
> Questa policy delle chiavi fornisce all'Account AWS il controllo completo di questa chiave KMS. Consente agli amministratori dell'account di utilizzare policy IAM per concedere ad altri principali l'autorizzazione per la gestione della chiave KMS. Per informazioni dettagliate, vedi the section called “Policy delle chiavi predefinita”.
> Le best practice di IAM disincentivano l'uso di utenti IAM con credenziali a lungo termine. Quando possibile, utilizza i ruoli IAM che forniscono credenziali temporanee. Per i dettagli, consulta la sezione Best practice di sicurezza in IAM nella Guida per l'utente IAM.

14. (Facoltativo) Per impedire ai ruoli e agli utenti IAM selezionati di eliminare questa chiave KMS, nella sezione Eliminazione chiave nella parte inferiore della pagina, deseleziona la casella di controllo Consenti agli amministratori delle chiavi di eliminare questa chiave.
15. Seleziona Next (Successivo).
16. Seleziona i ruoli e gli utenti IAM che possono utilizzare la chiave KMS per operazioni di crittografia.

> **Note**
>
> Questa policy delle chiavi fornisce all'Account AWS il controllo completo di questa chiave KMS. Consente agli amministratori dell'account di utilizzare le policy IAM per fornire ad altri principali l'autorizzazione per utilizzare la chiave KMS nelle operazioni di crittografia. Per informazioni dettagliate, vedi the section called “Policy delle chiavi predefinita”.
> Le best practice di IAM disincentivano l'uso di utenti IAM con credenziali a lungo termine. Quando possibile, utilizza i ruoli IAM che forniscono credenziali temporanee. Per i dettagli, consulta la sezione Best practice di sicurezza in IAM nella Guida per l'utente IAM.

17. (Facoltativo) È possibile consentire ad altri Account AWS di utilizzare questa chiave KMS per operazioni di crittografia. A questo proposito, nella sezione Altri Account AWS, nella parte inferiore della pagina, scegli Aggiungi un altro Account AWS e inserisci il numero di identificazione Account AWS di un account esterno. Per aggiungere più account esterni, ripetere questo passaggio.

    > **Note**
    >
    > Per consentire ai principali negli account esterni di utilizzare la chiave KMS, gli amministratori dell'account esterno devono creare policy IAM che forniscono tali autorizzazioni. Per ulteriori informazioni, consultare Autorizzazione per gli utenti in altri account di utilizzare una chiave KMS.

18. Seleziona Next (Successivo).
19. Esaminare le principali impostazioni scelte. È comunque possibile tornare indietro e modificare tutte le impostazioni.
20. Scegli Termina per creare la chiave KMS.

Creazione di chiavi asimmetriche KMS (API AWS KMS)

È possibile utilizzare l'CreateKeyoperazione per creare un'asimmetriaAWS KMS key. Questi esempi utilizzano la AWS Command Line Interface (AWS CLI), ma puoi usare anche qualsiasi linguaggio di programmazione supportato.

Quando crei una chiave KMS asimmetrica devi specificare il parametro `KeySpec` che determina il tipo di chiavi create. Inoltre, è necessario specificare un valore `KeyUsage` per ENCRYPT_DECRYPT o SIGN_VERIFY. Una volta creata la chiave KMS, non è più possibile modificare queste proprietà.

L'`CreateKey`operazione non consente di specificare un alias, ma è possibile utilizzare l'CreateAliasoperazione per creare un alias per la nuova chiave KMS.

> **Important**
>
> Non includere informazioni riservate o sensibili nei campi `Description` o `Tags`. Questi campi possono apparire in testo semplice nei CloudTrail log e in altri output.

Nell'esempio seguente viene utilizzata l'operazione `CreateKey` per creare una chiave KMS asimmetrica di chiavi RSA a 4096-bit progettata per la crittografia a chiave pubblica.

```
$ aws kms create-key --key-spec RSA_4096 --key-usage ENCRYPT_DECRYPT
{
    "KeyMetadata": {
        "KeyState": "Enabled",
        "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "KeyManager": "CUSTOMER",
        "Description": "",
        "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "CreationDate": 1569973196.214,
        "MultiRegion": false,
        "KeySpec": "RSA_4096",
        "CustomerMasterKeySpec": "RSA_4096",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "EncryptionAlgorithms": [
            "RSAES_OAEP_SHA_1",
            "RSAES_OAEP_SHA_256"
        ],
        "AWSAccountId": "111122223333",
        "Origin": "AWS_KMS",
        "Enabled": true
    }
}
```

Il comando di esempio che segue crea una chiave KMS asimmetrica che rappresenta una coppia di chiavi ECDSA utilizzata per la firma e la verifica. Non è possibile creare una coppia di chiavi a curva ellittica per la crittografia e la decrittografia.

```
$ aws kms create-key --key-spec ECC_NIST_P521 --key-usage SIGN_VERIFY
{
    "KeyMetadata": {
        "KeyState": "Enabled",
        "KeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
        "CreationDate": 1570824817.837,
        "Origin": "AWS_KMS",
        "SigningAlgorithms": [
            "ECDSA_SHA_512"
        ],
```

```
        "Arn": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321",
        "AWSAccountId": "111122223333",
        "KeySpec": "ECC_NIST_P521",
        "CustomerMasterKeySpec": "ECC_NIST_P521",
        "KeyManager": "CUSTOMER",
        "Description": "",
        "Enabled": true,
        "MultiRegion": false,
        "KeyUsage": "SIGN_VERIFY"
    }
}
```

Download delle chiavi pubbliche

Puoi visualizzare, copiare e scaricare la chiave pubblica da una coppia di chiavi KMS asimmetriche utilizzando la AWS Management Console o l'API AWS KMS. È necessario disporre dell'autorizzazione `kms:GetPublicKey` per la chiave KMS asimmetrica.

Ogni coppia di chiavi KMS asimmetriche è composta da una chiave privata, che non lascia mai AWS KMS in chiaro, e da una chiave pubblica che è possibile scaricare e condividere.

Potresti condividere una chiave pubblica per consentire ad altri di crittografare esternamente a AWS KMS dati che puoi decrittare solo con la tua chiave privata. Oppure per consentire ad altri di verificare esternamente a AWS KMS una firma digitale generata con la chiave privata.

Quando usi la chiave pubblica nella chiave KMS asimmetrica all'interno di AWS KMS, ottieni l'autenticazione, l'autorizzazione e la registrazione che fanno parte di ogni operazione AWS KMS. Si riduce anche il rischio di crittografare dati che non possono essere decrittati. Queste caratteristiche non hanno efficacia al di fuori di AWS KMS. Per informazioni dettagliate, vedi Considerazioni speciali per il download delle chiavi pubbliche.

> **Tip**
>
> Ti interessano le chiavi di dati o le chiavi SSH? In questo argomento viene descritto come gestire le chiavi asimmetriche in AWS Key Management Service, dove la chiave privata non è esportabile. Per le coppie di chiavi di dati esportabili in cui la chiave privata è protetta da una chiave KMS con crittografia simmetrica, vedere. GenerateDataKeyPair Per assistenza con il download della chiave pubblica associata a un'istanza Amazon EC2, consulta la sezione

Recupero della chiave pubblica nella Guida per l'utente di Amazon EC2 per istanze Linux e nella Guida per l'utente di Amazon EC2 per istanze Windows.

Argomenti

Considerazioni speciali per il download delle chiavi pubbliche

Per proteggere le chiavi KMS, AWS KMS fornisce controlli di accesso, crittografia autenticata e log dettagliati di ogni operazione. AWS KMS consente anche di impedire in modo temporaneo o permanente l'uso di chiavi KMS. Infine, le operazioni AWS KMS sono concepite per ridurre al minimo il rischio di crittografia dei dati che non possono essere decrittati. Queste funzionalità non sono disponibili quando si utilizzano chiavi pubbliche scaricate al di fuori di AWS KMS.

Autorizzazione

Le policy delle chiavi e le policy IAM che controllano l'accesso alla chiave KMS in AWS KMS non hanno alcun effetto sulle operazioni eseguite esternamente ad AWS. Qualsiasi utente che può ottenere la chiave pubblica può utilizzarla al di fuori di AWS KMS, anche se non dispone dell'autorizzazione per crittografare i dati o per verificare le firme con la chiave KMS.

Limitazioni d'uso delle chiavi

Le limitazioni d'uso delle chiavi non hanno validità al di fuori di AWS KMS. Se chiami l'operazione Encrypt con una chiave KMS con `KeyUsage` pari a `SIGN_VERIFY`, l'operazione AWS KMS ha esito negativo. Tuttavia, se esegui la crittografia dei dati al di fuori di AWS KMS con una chiave pubblica di una chiave KMS con `KeyUsage` pari a `SIGN_VERIFY`, non è possibile decrittare i dati.

Restrizioni sugli algoritmi

Le restrizioni sugli algoritmi di crittografia e firma supportati da AWS KMS non hanno validità al di fuori di AWS KMS. Se esegui la crittografia dei dati con la chiave pubblica di una chiave KMS al di fuori di AWS KMS e usi un algoritmo di crittografia non supportato da AWS KMS, non è possibile decrittare i dati.

Disattivazione ed eliminazione di chiavi KMS

Le operazioni che è possibile eseguire per impedire l'uso della chiave KMS in un'operazione di crittografia all'interno di AWS KMS non impediscono l'uso della chiave pubblica al di fuori di AWS KMS. Ad esempio, la disattivazione di una chiave KMS, la pianificazione dell'eliminazione di una chiave KMS, l'eliminazione di una chiave KMS o l'eliminazione del materiale di chiave da una chiave KMS non hanno alcun effetto su una chiave pubblica esterna a AWS KMS. Se elimini una chiave KMS asimmetrica oppure elimini o perdi il materiale della chiave, i dati crittografati con una chiave pubblica esternamente a AWS KMS non sono recuperabili.

Registrazione

I log AWS CloudTrail che registrano ogni operazione AWS KMS, inclusi la richiesta, la risposta, la data, l'ora e l'utente autorizzato, non registrano l'utilizzo della chiave pubblica al di fuori di AWS KMS.

Verifica offline con coppie di chiavi SM2 (solo regioni della Cina)

Per verificare la firma al di fuori di AWS KMS con una chiave pubblica SM2, è necessario specificare l'ID distintivo. Per impostazione predefinita, AWS KMS utilizza `1234567812345678` come ID distintivo. Per ulteriori informazioni, consulta Offline verification with SM2 key pairs (China Regions only) (verifica offline con coppie di chiavi SM2 (solo regioni della Cina)).

Download di una chiave pubblica (console)

Puoi utilizzare la AWS Management Console per visualizzare, copiare e scaricare la chiave pubblica da una chiave KMS asimmetrica nel tuo Account AWS. Per scaricare la chiave pubblica da una chiave KMS asimmetrica in un Account AWS diverso, utilizza l'API AWS KMS.

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.
4. Scegli l'alias o l'ID chiave di una chiave KMS asimmetrica.
5. Scegli la tab Configurazione crittografica. Registra i valori dei campi Specifica della chiave, Utilizzo della chiave e Algoritmi di crittografia o Algoritmi di firma. Questi valori serviranno per utilizzare la chiave pubblica al di fuori di AWS KMS. Assicurarsi di condividere queste informazioni quando si condivide la chiave pubblica.

6. Scegliere la scheda Public key (Chiave pubblica).
7. Per copiare la chiave pubblica negli Appunti, scegliere Copy (Copia). Per scaricare la chiave pubblica in un file, scegliere Download (Scarica).

Download di una chiave pubblica (API AWS KMS)

L'GetPublicKeyoperazione restituisce la chiave pubblica in una chiave KMS asimmetrica. Restituisce inoltre informazioni critiche necessarie per utilizzare correttamente la chiave pubblica al di fuori di AWS KMS, inclusi gli algoritmi di utilizzo della chiave e di crittografia. Assicurati di salvare questi valori e di condividerli ogni volta che condividi la chiave pubblica.

Gli esempi in questa sezione utilizzano AWS Command Line Interface (AWS CLI), ma puoi usare anche qualsiasi linguaggio di programmazione supportato.

Per specificare una chiave KMS, utilizza l'ID chiave, l'ARN di chiave, il nome dell'alias o l'ARN di alias. Quando utilizzi un nome alias, aggiungi il prefisso alias/. Per specificare una chiave KMS in un Account AWS diverso devi utilizzare l'ARN di chiave o alias.

Prima di eseguire questo comando, sostituisci il nome alias di esempio con un identificatore valido per la chiave KMS. Per eseguire questo comando, è necessario disporre delle autorizzazioni `kms:GetPublicKey` per la chiave KMS.

```
$ aws kms get-public-key --key-id alias/example_RSA_3072

{
    "KeySpec": "RSA_3072",
    "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "KeyUsage": "ENCRYPT_DECRYPT",
    "EncryptionAlgorithms": [
        "RSAES_OAEP_SHA_1",
        "RSAES_OAEP_SHA_256"
    ],
    "PublicKey": "MIIBojANBgkqhkiG..."
}
```

Individuazione di chiavi KMS asimmetriche

Per determinare se una determinata chiave KMS è simmetrica o asimmetrica, individua il tipo di chiave o la specifica della chiave. Puoi usare la console AWS KMS o l'API AWS KMS.

Alcuni di questi metodi mostrano anche altri aspetti della configurazione crittografica di una chiave KMS, incluso l'utilizzo della chiave e gli algoritmi di crittografia o la firma supportati dalla chiave KMS. Puoi visualizzare la configurazione crittografica di una chiave KMS esistente, ma non puoi modificarla.

Per informazioni generali sulla visualizzazione delle chiavi KMS, inclusi l'ordinamento, il filtraggio e la scelta delle colonne per la visualizzazione della console, consulta Visualizzazione della chiave KMS nella console.

Argomenti

- Individuazione del tipo di chiave nella tabella delle chiavi KMS
- Individuazione del tipo di chiave nella pagina dei dettagli
- Individuazione delle specifiche della chiave utilizzando l'API AWS KMS

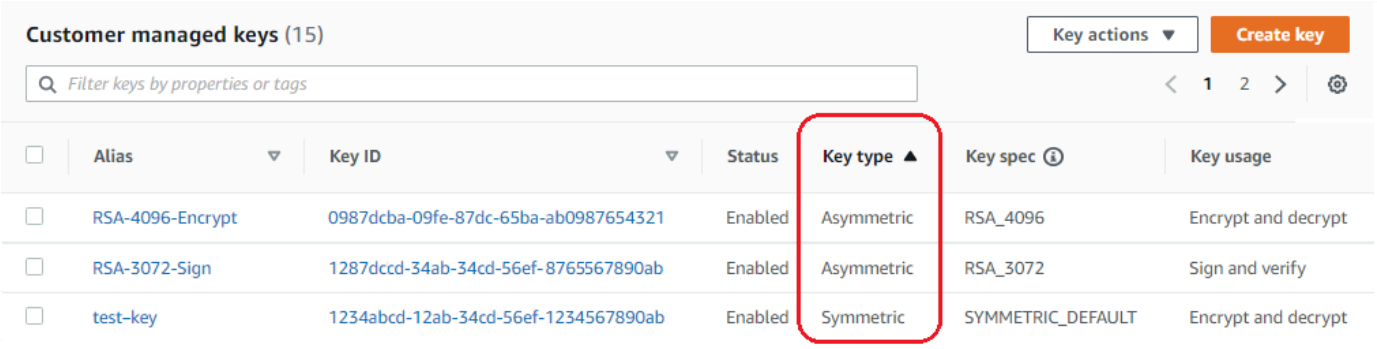
Individuazione del tipo di chiave nella tabella delle chiavi KMS

Nella console AWS KMS, la colonna Tipo di chiave indica se ogni chiave KMS è simmetrica o asimmetrica. È possibile aggiungere una colonna Tipo di chiave alla tabella delle chiavi KMS nelle pagine Chiavi gestite dal cliente o Chiavi gestite da AWS nella console.

Per individuare le chiavi KMS simmetriche e asimmetriche nella tabella delle chiavi KMS, utilizza la procedura seguente.

1. Aprire la console AWS KMS all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il selettore della regione nell'angolo superiore destro della pagina.
3. Per visualizzare le chiavi nell'account creato e gestito dall'utente, nel riquadro di navigazione, seleziona Chiavi gestite dal cliente. Per visualizzare le chiavi nell'account creato e gestito per te da AWS, nel riquadro di navigazione, seleziona AWS chiavi gestite dal cliente.
4. Le colonne Tipo di chiave indicano se ogni chiave KMS è simmetrica o asimmetrica. È inoltre possibile ordinare e filtrare in base al valore Key type (Tipo di chiave).

   Se la colonna Tipo di chiave non viene visualizzata nella tabella delle chiavi KMS, scegli l'icona a forma di ingranaggio nell'angolo in alto a destra della pagina, scegli Tipo di chiave e quindi seleziona Conferma. È inoltre possibile aggiungere le colonne Key spec (Specifica della chiave) e Key usage (Utilizzo della chiave).



Individuazione del tipo di chiave nella pagina dei dettagli

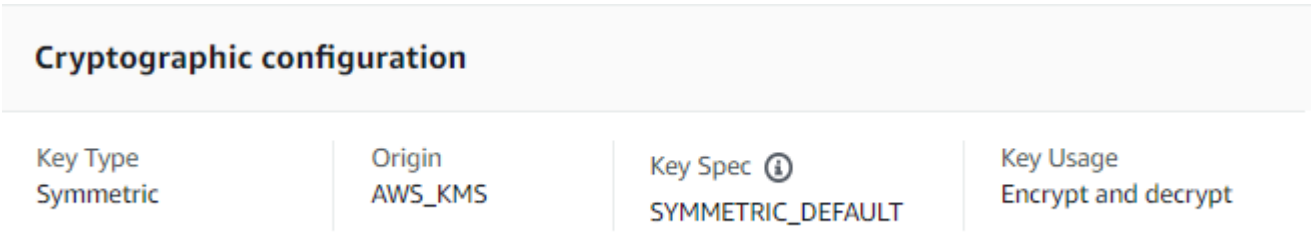
Nella console AWS KMS, la pagina dei dettagli di ogni chiave KMS include una sezione Cryptographic Configuration (Configurazione crittografica) in cui sono visualizzati il tipo di chiave (simmetrica o asimmetrica) e altri dettagli crittografici relativi alla chiave KMS.

Per individuare le chiavi KMS simmetriche e asimmetriche nella pagina dei dettagli di una chiave KMS, utilizza la procedura seguente.

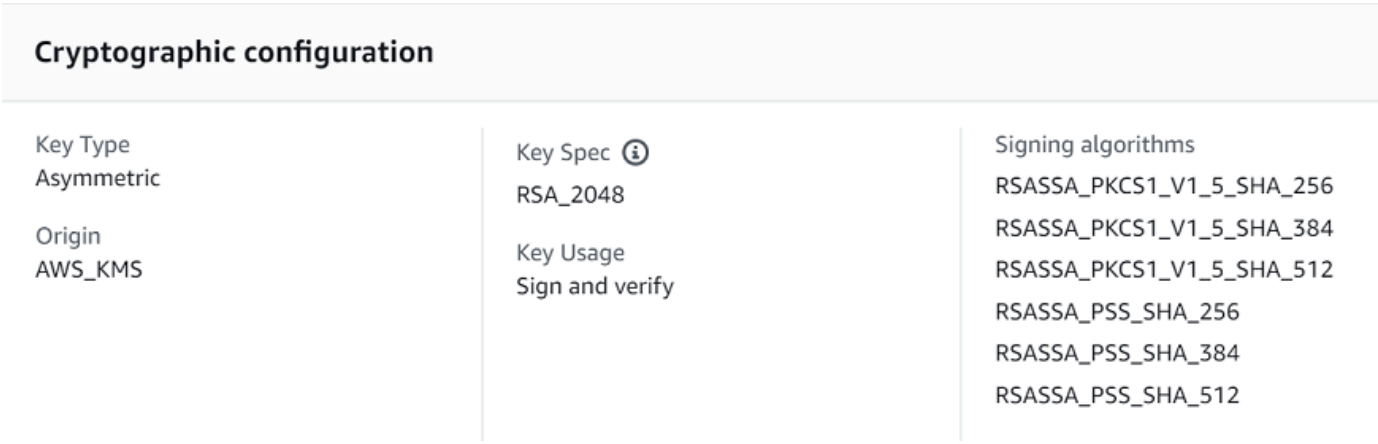
1. Aprire la console AWS KMS all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il selettore della regione nell'angolo superiore destro della pagina.
3. Per visualizzare le chiavi nell'account creato e gestito dall'utente, nel riquadro di navigazione, seleziona Chiavi gestite dal cliente. Per visualizzare le chiavi nell'account creato e gestito per te da AWS, nel riquadro di navigazione, seleziona AWS chiavi gestite dal cliente.
4. Scegli l'alias o l'ID chiave di una chiave KMS.
5. Seleziona la scheda Configurazione crittografica. Le schede si trovano al di sotto della sezione Configurazione generale.

   La sezione Configurazione crittografica include il Tipo di chiave, che indica se è simmetrica o asimmetrica. Visualizza anche altri dettagli sulla chiave KMS, incluso Key Usage (Utilizzo della chiave), che indica se una chiave KMS può essere utilizzata per crittografia e decrittazione o firma e verifica. Per le chiavi KMS asimmetriche, visualizza gli algoritmi di crittografia o gli algoritmi di firma supportati dalla chiave KMS.

   Ad esempio, la seguente è una scheda di esempio di Cryptographic configuration (Configurazione di crittografia) per una chiave KMS di crittografia simmetrica.



Di seguito è riportato una sezione Configurazione crittografica di esempio per una chiave KMS RSA asimmetrica utilizzata per la firma e la verifica.



Individuazione delle specifiche della chiave utilizzando l'API AWS KMS

Per determinare se una chiave KMS è simmetrica o asimmetrica, usa l'operazione. DescribeKey Il campo `KeySpec` nella risposta contiene le specifiche della chiave della chiave KMS. Per una chiave KMS di crittografia simmetrica, il valore di `KeySpec` è `SYMMETRIC_DEFAULT`. Gli altri valori indicano una chiave KMS asimmetrica o una chiave KMS HMAC.

> **Note**
>
> Il membro `CustomerMasterKeySpec` è obsoleto. Utilizza invece `KeySpec`. Per evitare l'interruzione delle modifiche, la risposta `DescribeKey` include i membri `KeySpec` e `CustomerMasterKeySpec` con lo stesso valore.

Ad esempio, `DescribeKey` restituisce la seguente risposta per una chiave KMS di crittografia simmetrica. Il valore di `KeySpec` è `SYMMETRIC_DEFAULT`.

```
{
```

```
  "KeyMetadata": {
    "AWSAccountId": "111122223333",
    "KeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
    "Arn": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321",
    "CreationDate": 1496966810.831,
    "Enabled": true,
    "Description": "",
    "KeyState": "Enabled",
    "Origin": "AWS_KMS",
    "KeyManager": "CUSTOMER",
    "MultiRegion": false,
    "KeySpec": "SYMMETRIC_DEFAULT",
    "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
    "KeyUsage": "ENCRYPT_DECRYPT",
    "EncryptionAlgorithms": [
        "SYMMETRIC_DEFAULT"
    ]
  }
}
```

La risposta `DescribeKey` per una chiave KMS RSA asimmetrica utilizzata per la firma e la verifica è simile a questo esempio. Il valore `KeySpec` è RSA_2048 e la `KeyUsage` è`SIGN_VERIFY`. L'elemento `SigningAlgorithms` elenca gli algoritmi di firma validi per la chiave KMS.

```
{
  "KeyMetadata": {
    "AWSAccountId": "111122223333",
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "CreationDate": 1571767572.317,
    "CustomerMasterKeySpec": "RSA_2048",
    "Enabled": false,
    "Description": "",
    "KeyState": "Disabled",
    "Origin": "AWS_KMS",
    "MultiRegion": false,
    "KeyManager": "CUSTOMER",
    "KeySpec": "RSA_2048",
    "KeyUsage": "SIGN_VERIFY",
    "SigningAlgorithms": [
        "RSASSA_PKCS1_V1_5_SHA_256",
```

```
        "RSASSA_PKCS1_V1_5_SHA_384",
        "RSASSA_PKCS1_V1_5_SHA_512",
        "RSASSA_PSS_SHA_256",
        "RSASSA_PSS_SHA_384",
        "RSASSA_PSS_SHA_512"
    ]
  }
}
```

Specifiche delle chiavi asimmetriche

Negli argomenti che seguono vengono fornite informazioni tecniche sulle specifiche delle chiavi supportate da AWS KMS per le chiavi KMS asimmetriche. Le informazioni sulla specifica della chiave SYMMETRIC_DEFAULT per le chiavi di crittografia simmetrica sono incluse a fini di confronto.

Argomenti

- Specifiche della chiave RSA
- Specifiche della chiave basata su curva ellittica
- Specifica della chiave SM2 (solo regioni della Cina)
- Specifica della chiave SYMMETRIC_DEFAULT

Specifiche della chiave RSA

Quando utilizzi una specifica della chiave RSA, AWS KMS crea una chiave KMS asimmetrica con una coppia di chiavi RSA. Grazie alla chiave privata il servizio AWS KMS non è mai in chiaro. Puoi utilizzare la chiave pubblica all'interno di AWS KMS o scaricare la chiave pubblica per usarla all'esterno di AWS KMS.

> **Warning**
>
> Quando si crittografano i dati al di fuori di AWS KMS, assicurarsi di poter decrittare il testo cifrato. Se si utilizza la chiave pubblica da una chiave KMS che è stata eliminata da AWS KMS, la chiave pubblica da una chiave KMS configurata per la firma e la verifica o un algoritmo di crittografia che non è supportato dalla chiave KMS, i dati non sono recuperabili.

In AWS KMS puoi utilizzare chiavi KMS asimmetriche con coppie di chiavi RSA per eseguire la crittografia e la decrittazione o la firma e la verifica, ma non per entrambe le azioni. Questa proprietà,

nota come utilizzo della chiave, viene determinata separatamente dalla specifica della chiave; tuttavia è preferibile che tu la definisca prima di selezionare la specifica.

AWS KMS supporta le seguenti specifiche della chiave RSA per la crittografia e la decrittografia o la firma e la verifica:

- RSA_2048
- RSA_3072
- RSA_4096

Le specifiche della chiave RSA differiscono in base alla lunghezza di bit della chiave RSA. La specifica della chiave RSA scelta potrebbe essere determinata dai tuoi standard di sicurezza o dai requisiti della tua attività. In generale, usa la chiave più grande che ritieni pratica e conveniente per la tua attività. Le operazioni crittografiche sulle chiavi KMS con specifiche della chiave RSA diverse hanno prezzi differenti. Per informazioni sui prezzi AWS KMS, consulta Prezzi di AWS Key Management Service. Per informazioni sulle quote di richieste, consulta Quote di richieste.

Specifiche della chiave RSA per la crittografia e la decrittografia

Quando una chiave KMS asimmetrica RSA viene utilizzata per la crittografia e la decrittazione, esegui la crittografia con la chiave pubblica e la decrittazione con la chiave privata. Quando chiami l'operazione `Encrypt` in AWS KMS per una chiave KMS RSA, AWS KMS utilizza la chiave pubblica nella coppia di chiavi RSA e l'algoritmo di crittografia specificato per crittografare i dati. Per decrittare il testo cifrato, chiama l'operazione `Decrypt` e specifica la stessa chiave KMS e lo stesso algoritmo di crittografia. AWS KMS utilizza quindi la chiave privata nella coppia di chiavi RSA per decrittare i dati.

Puoi inoltre scaricare la chiave pubblica e utilizzarla per crittografare i dati all'esterno di AWS KMS. Assicurati di utilizzare un algoritmo di crittografia supportato da AWS KMS per le chiavi KMS RSA. Per decrittare il testo cifrato, chiama la funzione `Decrypt` con la stessa chiave KMS e lo stesso algoritmo di crittografia.

AWS KMS supporta due algoritmi di crittografia per le chiavi KMS con specifiche della chiave RSA. Questi algoritmi, definiti in PKCS #1 v2.2, differiscono per la funzione hash che usano internamente. In AWS KMS gli algoritmi RSAES_OAEP utilizzano sempre la stessa funzione hash sia per scopi di hashing che per la funzione di generazione della maschera (MGF1). Occorre specificare un algoritmo di crittografia quando chiami le azioni Encrypt e Decrypt. Puoi scegliere un algoritmo diverso per ogni richiesta.

Algoritmi di crittografia supportati per le specifiche della chiave RSA

Algoritmo di crittografia	Descrizione dell'algoritmo
RSAES_OAEP_SHA_1	PKCS #1 v2.2, sezione 7.1. Crittografia RSA con riempimento OAEP che utilizza SHA-1 sia per l'hash sia per la funzione di generazione della maschera MGF1 insieme a un'etichetta vuota.
RSAES_OAEP_SHA_256	PKCS #1, sezione 7.1. Crittografia RSA con riempimento OAEP che utilizza SHA-256 sia per l'hash sia per la funzione di generazione della maschera MGF1 insieme a un'etichetta vuota.

Non puoi configurare una chiave KMS per utilizzare un particolare algoritmo di crittografia. Tuttavia, puoi utilizzare la condizione kms: EncryptionAlgorithm policy per specificare gli algoritmi di crittografia che i principali possono utilizzare con la chiave KMS.

Per ottenere gli algoritmi di crittografia per una chiave KMS, visualizza la configurazione crittografica della chiave KMS nella console o utilizza l'operazione. AWS KMS DescribeKey AWS KMSfornisce inoltre le specifiche della chiave e gli algoritmi di crittografia quando scarichi la chiave pubblica, nella AWS KMS console o utilizzando l'operazione. GetPublicKey

Potresti scegliere una specifica della chiave RSA in base alla lunghezza dei dati in chiaro che puoi crittografare in ogni richiesta. Nella tabella che segue vengono illustrate le dimensioni massime, in byte, del testo in chiaro che puoi crittografare in una singola chiamata all'azione Encrypt. I valori differiscono con la specifica della chiave e l'algoritmo di crittografia. Per eseguire un confronto, puoi utilizzare una chiave KMS di crittografia simmetrica per crittografare fino a 4.096 byte contemporaneamente.

Per calcolare la lunghezza massima del testo in chiaro in byte per questi algoritmi, utilizzare la seguente formula: (*`dimensione_chiave_in_bit`* /8) - (2 * *`lunghezza_hash_in_bit`*/8) - 2. Ad esempio, per RSA_2048 con SHA-256, la dimensione massima del testo in chiaro in byte è (2048/8) - (2 * 256/8) -2 = 190.

Dimensione massima del testo in chiaro (in byte) in un'azione Encrypt

	Algoritmo di crittografia	
Specifica della chiave	RSAES_OAEP_SHA_1	RSAES_OAEP_SHA_256
RSA_2048	214	190
RSA_3072	342	318
RSA_4096	470	446

Specifiche della chiave RSA per la firma e la verifica

Quando una chiave KMS asimmetrica RSA viene utilizzata per la firma e la verifica, generi la firma per un messaggio con la chiave privata e verifichi la firma con la chiave pubblica.

Quando chiami l'operazione `Sign` in AWS KMS per una chiave KMS asimmetrica, per generare una firma, AWS KMS utilizza la chiave privata nella coppia di chiavi RSA, nel messaggio e nell'algoritmo di firma specificato. Per verificare la firma, chiamare l'azione Verify. Specifica la firma, oltre alla stessa chiave KMS, allo stesso messaggio e algoritmo di firma. AWS KMS utilizza quindi la chiave pubblica nella coppia di chiavi RSA per verificare la firma. Puoi inoltre scaricare la chiave pubblica e utilizzarla per verificare la firma all'esterno di AWS KMS.

AWS KMS supporta gli algoritmi di firma seguenti per le chiavi KMS con specifica della chiave RSA. Devi specificare un algoritmo di firma quando chiami le operazioni Sign (firma) e Verify (verifica). Puoi scegliere un algoritmo diverso per ogni richiesta. Quando si firma con coppie di chiavi RSA, sono preferiti gli algoritmi RSASSA-PSS. Includiamo algoritmi RSASSA-PKCS1-v1_5 per la compatibilità con le applicazioni esistenti.

Algoritmi di firma supportati per le specifiche della chiave RSA

Algoritmo di firma	Descrizione dell'algoritmo
RSASSA_PSS_SHA_256	PKCS #1 v2.2, sezione 8.1, firma RSA con riempimento PSS che utilizza SHA-256 sia per il digest del messaggio sia per la funzione di generazione della maschera MGF1 insieme a un valore salt a 256 bit

Algoritmo di firma	Descrizione dell'algoritmo
RSASSA_PSS_SHA_384	PKCS #1 v2.2, sezione 8.1, firma RSA con riempimento PSS che utilizza SHA-384 sia per il digest del messaggio sia per la funzione di generazione della maschera MGF1 insieme a un valore salt a 384 bit
RSASSA_PSS_SHA_512	PKCS #1 v2.2, sezione 8.1, firma RSA con riempimento PSS che utilizza SHA-512 sia per il digest del messaggio sia per la funzione di generazione della maschera MGF1 insieme a un valore salt a 512 bit
RSASSA_PKCS1_V1_5_SHA_256	PKCS #1 v2.2, sezione 8.2, firma RSA con riempimento PKCS #1v1.5 e SHA-256
RSASSA_PKCS1_V1_5_SHA_384	PKCS #1 v2.2, sezione 8.2, firma RSA con riempimento PKCS #1v1.5 e SHA-384
RSASSA_PKCS1_V1_5_SHA_512	PKCS #1 v2.2, sezione 8.2, firma RSA con riempimento PKCS #1v1.5 e SHA-512

Non puoi configurare una chiave KMS per utilizzare algoritmi di firma particolari. Tuttavia, puoi utilizzare la condizione kms: SigningAlgorithm policy per specificare gli algoritmi di firma che i principali possono utilizzare con la chiave KMS.

Per ottenere gli algoritmi di firma per una chiave KMS, visualizza la configurazione crittografica della chiave KMS nella console o utilizzando l'operazione. AWS KMS DescribeKey AWS KMSfornisce anche le specifiche della chiave e gli algoritmi di firma quando scarichi la chiave pubblica, nella AWS KMS console o utilizzando l'operazione. GetPublicKey

Specifiche della chiave basata su curva ellittica

Quando utilizzi una specifica della chiave basata su curva ellittica (ECC), AWS KMS crea una chiave KMS asimmetrica con una coppia di chiavi ECC per la firma e la verifica. La chiave privata che genera la firma non lascia mai AWS KMS in chiaro. Puoi utilizzare la chiave pubblica per verificare le firme all'interno di AWS KMS o scaricare la chiave pubblica da utilizzare all'esterno di AWS KMS.

AWS KMS supporta le seguenti specifiche della chiave ECC per le chiavi KMS asimmetriche.

- Coppia di chiavi asimmetriche basate su curva ellittica consigliate da NIST (firma e verifica)
  - ECC_NIST_P256 (secp256r1)
  - ECC_NIST_P384 (secp384r1)
  - ECC_NIST_P521 (secp521r1)
- Altre coppie di chiavi asimmetriche basate su curva ellittica (firma e verifica)
  - ECC_SECG_P256K1 (secp256k1), comunemente usate per le criptovalute.

La specifica della chiave ECC scelta potrebbe essere determinata dai tuoi standard di sicurezza o dai requisiti della tua attività. In generale, utilizza la curva con il maggior numero di punti che ritieni pratica e conveniente per la tua attività.

Se stai creando una chiave KMS asimmetrica da utilizzare con le criptovalute, usa la specifica della chiave ECC_SECG_P256K1. Puoi utilizzare anche questa specifica della chiave per altri scopi, ma è necessaria per il Bitcoin e le altre criptovalute.

Le chiave KMS con specifiche diverse della chiave ECC hanno prezzi differenti e sono soggette a varie quote di richieste. Per informazioni sui prezzi di AWS KMS, consulta la pagina dei prezzi di AWS Key Management Service. Per informazioni sulle quote di richieste, consulta Quote di richieste.

Nella tabella che segue vengono illustrati gli algoritmi di firma supportati da AWS KMS per ciascuna delle specifiche della chiave ECC. Non puoi configurare una chiave KMS per utilizzare algoritmi di firma particolari. Tuttavia, puoi utilizzare la condizione kms: SigningAlgorithm policy per specificare gli algoritmi di firma che i principali possono utilizzare con la chiave KMS.

Algoritmi di firma supportati per le specifiche della chiave ECC

Specifica della chiave	Algoritmo di firma	Descrizione dell'algoritmo
ECC_NIST_P256	ECDSA_SHA_256	NIST FIPS 186-4, sezione 6.4, firma ECDSA che utilizza la curva specificata dalla chiave e l'algoritmo SHA-256 per il digest del messaggio.
ECC_NIST_P384	ECDSA_SHA_384	NIST FIPS 186-4, sezione 6.4, firma ECDSA che utilizza la

Specifica della chiave	Algoritmo di firma	Descrizione dell'algoritmo
		curva specificata dalla chiave e l'algoritmo SHA-384 per il digest del messaggio.
ECC_NIST_P521	ECDSA_SHA_512	NIST FIPS 186-4, sezione 6.4, firma ECDSA che utilizza la curva specificata dalla chiave e l'algoritmo SHA-512 per il digest del messaggio.
ECC_SECG_P256K1	ECDSA_SHA_256	NIST FIPS 186-4, sezione 6.4, firma ECDSA che utilizza la curva specificata dalla chiave e l'algoritmo SHA-256 per il digest del messaggio.

Specifica della chiave SM2 (solo regioni della Cina)

La specifica della chiave SM2 è una specifica chiave di curva ellittica definita all'interno della serie di specifiche GM/T pubblicata dall'ufficio di Stato cinese per la crittografia commerciale (OSCCA, Office of State Commercial Cryptography Administration). La specifica della chiave SM2 è disponibile solo nelle regioni della Cina. Quando utilizzi una specifica della chiave SM2, AWS KMS crea una chiave KMS asimmetrica con una coppia di chiavi SM2. Puoi utilizzare la coppia di chiavi SM2 all'interno di AWS KMS o scaricare la chiave pubblica per usarla all'esterno di AWS KMS.

A differenza delle specifiche della chiave ECC, è possibile utilizzare una chiave KMS SM2 per la firma e la verifica o per crittografia e decrittografia. È necessario specificare il parametro sull'utilizzo della chiave in fase di creazione della chiave KMS e non può essere modificata in seguito.

AWS KMS supporta i seguenti algoritmi di crittografia e firma SM2:

- Algoritmo di crittografia SM2PKE

  SM2PKE è un algoritmo di crittografia basato su curva ellittica definito da OSCCA in GM/T 0003.4-2012.

- Algoritmo di firma SM2DSA

  SM2DSA è un algoritmo di firma basato su curva ellittica definito da OSCCA in GM/T 0003.2-2012. SM2DSA richiede un ID distintivo che viene sottoposto a hash con l'algoritmo di hashing SM3 e quindi combinato con il messaggio, o il digest del messaggio, a cui è stato passato AWS KMS. Questo valore concatenato viene quindi sottoposto a hashing e firmato da AWS KMS.

Operazioni offline con SM2 (solo regioni della Cina)

È possibile scaricare la chiave pubblica della coppia di chiavi SM2 per l'utilizzo in operazioni offline, ovvero al di fuori di AWS KMS. Tuttavia, quando si utilizza la chiave pubblica SM2 offline, potrebbe essere necessario eseguire manualmente conversioni e calcoli aggiuntivi. Le operazioni di SM2DSA potrebbero richiedere un ID distintivo o il calcolo di un digest del messaggio. Le operazioni di crittografia SM2PKE potrebbero richiedere la conversione dell'output di testo criptato non elaborato in un formato che AWS KMS può accettare.

Per aiutarti in queste operazioni, la classe `SM2OfflineOperationHelper` per Java fornisce metodi che eseguono le attività per tuo conto. È possibile utilizzare questa classe helper come modello per altri fornitori di crittografia.

> **Important**
>
> Il codice di riferimento `SM2OfflineOperationHelper` è progettato per essere compatibile con Bouncy Castle versione 1.68. Per assistenza con altre versioni, contatta bouncycastle.org.

Verifica offline con coppie di chiavi SM2 (solo regioni della Cina)

Per verificare la firma al di fuori di AWS KMS con una chiave pubblica SM2, è necessario specificare l'ID distintivo. Quando passi un messaggio non elaborato, `MessageType:RAW`, all'API Sign (firma), AWS KMS utilizza l'ID distintivo predefinito, `1234567812345678`, definito dall'OSCCA in GM/T 0009-2012. Non puoi specificare il tuo ID distintivo all'interno di AWS KMS.

Tuttavia, se si sta generando un messaggio digest al di fuori di AWS, puoi specificare il tuo ID distintivo, quindi passare il digest del messaggio, `MessageType:DIGEST`, a AWS KMS per la firma. A tale scopo, modifica il valore `DEFAULT_DISTINGUISHING_ID` in classe

`SM2OfflineOperationHelper`. L'ID distintivo specificato può essere qualsiasi stringa lunga fino a 8.192 caratteri. Dopo che AWS KMS ha firmato il digest del messaggio, è che necessario che il digest del messaggio o il messaggio e l'ID distintivo utilizzato per calcolare il digest lo verifichino offline.

Classe **`SM2OfflineOperationHelper`**

All'interno di AWS KMS, le conversioni di testo criptato non elaborato e i calcoli del digest dei messaggi SM2DSA avvengono automaticamente. Non tutti i fornitori di crittografia implementano SM2 allo stesso modo. Alcune librerie, come OpenSSL versioni 1.1.1 e successive, eseguono queste operazioni automaticamente. AWS KMS ha confermato questo comportamento in fase di test con OpenSSL versione 3.0. Utilizza la seguente classe `SM2OfflineOperationHelper` con librerie, come Bouncy Castle, che richiedono di eseguire manualmente queste conversioni e calcoli.

La classe `SM2OfflineOperationHelper` fornisce metodi per le seguenti operazioni offline:

- Calcolo del digest del messaggio

  Per generare un digest del messaggio offline da utilizzare per la verifica offline o da passare a AWS KMS per la firma, utilizza il metodo `calculateSM2Digest`. Il metodo `calculateSM2Digest` genera un digest dei messaggi con l'algoritmo di hashing SM3. L'GetPublicKeyAPI restituisce la chiave pubblica in formato binario. È necessario analizzare la chiave binaria in un file Java PublicKey. Fornisci il messaggio alla chiave pubblica analizzata. Il metodo combina automaticamente il tuo messaggio con l'ID distintivo predefinito, `1234567812345678`, ma è possibile impostare il proprio ID distintivo modificando il valore `DEFAULT_DISTINGUISHING_ID`.

- Verify

  Per verificare la firma offline, usa il metodo `offlineSM2DSAVerify`. Il metodo `offlineSM2DSAVerify` utilizza il digest del messaggio calcolato dall'ID distintivo specificato e il messaggio originale fornito per verificare la firma digitale. L'GetPublicKeyAPI restituisce la chiave pubblica in formato binario. È necessario analizzare la chiave binaria in un file Java PublicKey. Fornisci alla chiave pubblica analizzata il messaggio originale e la firma che desideri verificare. Per ulteriori dettagli, consulta .Offline verification with SM2 key pairs (verifica offline con coppie di chiavi SM2).

- Encrypt

  Per crittografare il testo normale offline utilizza il metodo `offlineSM2PKEEncrypt`. Questo metodo garantisce che il testo criptato sia in un formato che AWS KMS può decrittografare. Il metodo `offlineSM2PKEEncrypt` crittografa il testo normale e quindi converte il testo criptato

grezzo prodotto da SM2PKE nel formato ASN.1. L'GetPublicKeyAPI restituisce la chiave pubblica in formato binario. È necessario analizzare la chiave binaria in un file Java PublicKey. Fornisci alla chiave pubblica analizzata il testo normale che desideri crittografare.

Se non sei sicuro di dover eseguire la conversione, usa la seguente operazione OpenSSL per testare il formato del tuo testo criptato. Se l'operazione non riesce, è necessario convertire il testo criptato nel formato ASN.1.

```
openssl asn1parse -inform DER -in ciphertext.der
```

Per impostazione predefinita, la classe `SM2OfflineOperationHelper` usa l'ID distintivo predefinito, `1234567812345678`, quando si generano digest di messaggi per le operazioni SM2DSA.

```
package com.amazon.kms.utils;

import javax.crypto.BadPaddingException;
import javax.crypto.Cipher;
import javax.crypto.IllegalBlockSizeException;
import javax.crypto.NoSuchPaddingException;
import java.io.IOException;
import java.math.BigInteger;
import java.nio.ByteBuffer;
import java.nio.charset.StandardCharsets;
import java.security.InvalidKeyException;
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;
import java.security.NoSuchProviderException;
import java.security.PrivateKey;
import java.security.PublicKey;

import org.bouncycastle.crypto.CryptoException;
import org.bouncycastle.jce.interfaces.ECPublicKey;

import java.util.Arrays;

import org.bouncycastle.asn1.ASN1EncodableVector;
import org.bouncycastle.asn1.ASN1Integer;
import org.bouncycastle.asn1.DEROctetString;
import org.bouncycastle.asn1.DERSequence;
import org.bouncycastle.asn1.gm.GMNamedCurves;
```

```
import org.bouncycastle.asn1.x9.X9ECParameters;
import org.bouncycastle.crypto.CipherParameters;
import org.bouncycastle.crypto.params.ParametersWithID;
import org.bouncycastle.crypto.params.ParametersWithRandom;
import org.bouncycastle.crypto.signers.SM2Signer;
import org.bouncycastle.jcajce.provider.asymmetric.util.ECUtil;

public class SM2OfflineOperationHelper {
    // You can change the DEFAULT_DISTINGUISHING_ID value to set your own
 distinguishing ID,
    // the DEFAULT_DISTINGUISHING_ID can be any string up to 8,192 characters long.
    private static final byte[] DEFAULT_DISTINGUISHING_ID =
 "1234567812345678".getBytes(StandardCharsets.UTF_8);
    private static final X9ECParameters SM2_X9EC_PARAMETERS =
 GMNamedCurves.getByName("sm2p256v1");

    // ***calculateSM2Digest***
    // Calculate message digest
    public static byte[] calculateSM2Digest(final PublicKey publicKey, final byte[]
 message) throws
            NoSuchProviderException, NoSuchAlgorithmException {
        final ECPublicKey ecPublicKey = (ECPublicKey) publicKey;

        // Generate SM3 hash of default distinguishing ID, 1234567812345678
        final int entlenA = DEFAULT_DISTINGUISHING_ID.length * 8;
        final byte [] entla = new byte[] { (byte) (entlenA & 0xFF00), (byte) (entlenA &
 0x00FF) };
        final byte [] a = SM2_X9EC_PARAMETERS.getCurve().getA().getEncoded();
        final byte [] b = SM2_X9EC_PARAMETERS.getCurve().getB().getEncoded();
        final byte [] xg = SM2_X9EC_PARAMETERS.getG().getXCoord().getEncoded();
        final byte [] yg = SM2_X9EC_PARAMETERS.getG().getYCoord().getEncoded();
        final byte[] xa = ecPublicKey.getQ().getXCoord().getEncoded();
        final byte[] ya = ecPublicKey.getQ().getYCoord().getEncoded();
        final byte[] za = MessageDigest.getInstance("SM3", "BC")
                .digest(ByteBuffer.allocate(entla.length +
 DEFAULT_DISTINGUISHING_ID.length + a.length + b.length + xg.length + yg.length +
                        xa.length +
 ya.length).put(entla).put(DEFAULT_DISTINGUISHING_ID).put(a).put(b).put(xg).put(yg).put(xa).put
                        .array());

        // Combine hashed distinguishing ID with original message to generate final
 digest
        return MessageDigest.getInstance("SM3", "BC")
```

```
                .digest(ByteBuffer.allocate(za.length +
message.length).put(za).put(message)
                        .array());
    }

    // ***offlineSM2DSAVerify***
    // Verify digital signature with SM2 public key
    public static boolean offlineSM2DSAVerify(final PublicKey publicKey, final byte []
message,
            final byte [] signature) throws InvalidKeyException {
        final SM2Signer signer = new SM2Signer();
        CipherParameters cipherParameters =
ECUtil.generatePublicKeyParameter(publicKey);
        cipherParameters = new ParametersWithID(cipherParameters,
DEFAULT_DISTINGUISHING_ID);
        signer.init(false, cipherParameters);
        signer.update(message, 0, message.length);
        return signer.verifySignature(signature);
    }

    // ***offlineSM2PKEEncrypt***
    // Encrypt data with SM2 public key
    public static byte[] offlineSM2PKEEncrypt(final PublicKey publicKey, final byte []
plaintext) throws
            NoSuchPaddingException, NoSuchAlgorithmException, NoSuchProviderException,
InvalidKeyException,
            BadPaddingException, IllegalBlockSizeException, IOException {
        final Cipher sm2Cipher = Cipher.getInstance("SM2", "BC");
        sm2Cipher.init(Cipher.ENCRYPT_MODE, publicKey);

        // By default, Bouncy Castle returns raw ciphertext in the c1c2c3 format
        final byte [] cipherText = sm2Cipher.doFinal(plaintext);

        // Convert the raw ciphertext to the ASN.1 format before passing it to AWS KMS
        final ASN1EncodableVector asn1EncodableVector = new ASN1EncodableVector();
        final int coordinateLength = (SM2_X9EC_PARAMETERS.getCurve().getFieldSize() +
7) / 8 * 2 + 1;
        final int sm3HashLength = 32;
        final int xCoordinateInCipherText = 33;
        final int yCoordinateInCipherText = 65;
        byte[] coords = new byte[coordinateLength];
        byte[] sm3Hash = new byte[sm3HashLength];
        byte[] remainingCipherText = new byte[cipherText.length - coordinateLength -
sm3HashLength];
```

```
        // Split components out of the ciphertext
        System.arraycopy(cipherText, 0, coords, 0, coordinateLength);
        System.arraycopy(cipherText, cipherText.length - sm3HashLength, sm3Hash, 0,
 sm3HashLength);
        System.arraycopy(cipherText, coordinateLength, remainingCipherText,
 0,cipherText.length - coordinateLength - sm3HashLength);

        // Build standard SM2PKE ASN.1 ciphertext vector
        asn1EncodableVector.add(new ASN1Integer(new BigInteger(1,
 Arrays.copyOfRange(coords, 1, xCoordinateInCipherText))));
        asn1EncodableVector.add(new ASN1Integer(new BigInteger(1,
 Arrays.copyOfRange(coords, xCoordinateInCipherText, yCoordinateInCipherText))));
        asn1EncodableVector.add(new DEROctetString(sm3Hash));
        asn1EncodableVector.add(new DEROctetString(remainingCipherText));

        return new DERSequence(asn1EncodableVector).getEncoded("DER");
    }
}
```

Specifica della chiave SYMMETRIC_DEFAULT

La specifica della chiave di default, SYMMETRIC_DEFAULT, è la specifica della chiave per le chiavi KMS di crittografia simmetrica. Quando selezioni il tipo di chiave Symmetric (Simmetrica) e l'utilizzo della chiave Encrypt and decrypt (Crittografa e decrittografa) nella console AWS KMS, viene selezionata la specifica della chiave `SYMMETRIC_DEFAULT`. Nell'CreateKeyoperazione, se non si specifica un `KeySpec` valore, viene selezionato SYMMETRIC_DEFAULT. Se non hai motivo di utilizzare una specifica della chiave diversa, SYMMETRIC_DEFAULT è una scelta valida.

SYMMETRIC_DEFAULT attualmente rappresenta AES-256-GCM, un algoritmo simmetrico basato su Advanced Encryption Standard (AES) in Galois Counter Mode (GCM) con chiavi a 256 bit, standard del settore per la crittografia sicura. Il testo cifrato generato da questo algoritmo supporta ulteriori dati autenticati (AAD), ad esempio un contesto di crittografia, e GCM fornisce un controllo di integrità aggiuntivo sul testo cifrato. Per dettagli tecnici, consulta Dettagli crittografici su AWS Key Management Service.

AES-256-GCM garantisce la protezione attuale e futura dei dati crittografati. I crittografi considerano questo algoritmo resistente alla quantistica. Attacchi teorici futuri di calcolo quantistico su larga scala su testi cifrati creati con chiavi AES-GCM a 256 bit riducono l'effettiva sicurezza della chiave a 128 bit. Tuttavia, questo livello di sicurezza è sufficiente per rendere impossibili gli attacchi a forza bruta su testi cifrati di AWS KMS.

È l'unica eccezione nelle regioni della Cina, dove SYMMETRIC_DEFAULT rappresenta una chiave simmetrica a 128 bit che utilizza la crittografia SM4. È possibile creare una chiave SM4 a 128 bit solo nelle regioni della Cina. Non puoi creare una chiave KMS AES-GCM a 256 bit in Cina.

Puoi utilizzare una chiave KMS di crittografia simmetrica in AWS KMS per crittografare, decrittografare e crittografare nuovamente i dati, e per proteggere le chiavi dati e le coppie di chiavi dati generate. I servizi AWS integrati con AWS KMS utilizzano chiavi KMS di crittografia simmetrica per la crittografia dei dati a riposo. Puoi importare il materiale della chiave di tua proprietà in una chiave KMS di crittografia simmetrica e creare chiavi KMS di crittografia simmetrica negli archivi delle chiavi personalizzate. Per una tabella di confronto delle azioni eseguibili su chiavi KMS simmetriche e asimmetriche, consulta Confronto tra chiavi KMS simmetriche e asimmetriche.

Per informazioni dettagliate su AWS KMS e sulle chiavi di crittografia simmetrica, consulta la sezione Dettagli della crittografia di AWS Key Management Service.

Chiavi HMAC in AWS KMS

Le chiavi KMS con codice di autenticazione dei messaggi basato su hash (HMAC) sono chiavi simmetriche utilizzate per generare e verificare gli HMAC all'interno di AWS KMS. Il materiale della chiave univoco associato a ciascuna chiave KMS HMAC fornisce la chiave privata richiesta dagli algoritmi HMAC. È possibile utilizzare una chiave KMS HMAC con le operazioni `GenerateMac` e `VerifyMac` per verificare l'integrità e l'autenticità dei dati all'interno di AWS KMS.

Gli algoritmi HMAC combinano una funzione hash crittografica e una chiave segreta condivisa. Prendono un messaggio e una chiave segreta, come il materiale della chiave in una chiave KMS HMAC, e restituiscono un codice univoco di dimensioni fisse o tag. Se un solo carattere del messaggio cambia o se la chiave segreta non è identica, il tag risultante è completamente diverso. Richiedendo una chiave segreta, HMAC fornisce anche autenticità; è impossibile generare un tag HMAC identico senza la chiave segreta. Gli HMAC a volte vengono chiamati firme simmetriche, perché funzionano come firme digitali, ma utilizzano una sola chiave sia per la firma sia per la verifica.

Le chiavi KMS HMAC e gli algoritmi HMAC utilizzati da AWS KMS sono conformi agli standard di settore definiti in RFC 2104. L'AWS KMSGenerateMacoperazione genera tag HMAC standard. Le chiavi KMS HMAC sono generate nei moduli di sicurezza hardware AWS KMS certificati ai sensi del Programma di convalida dei moduli crittografici FIPS 140-2, tranne nelle Regioni Cina (Pechino) e Cina (Ningxia), e mantengono AWS KMS sempre crittografato. Per utilizzare una chiave KMS HMAC, è necessario richiamare AWS KMS.

Le chiavi KMS HMAC sono utilizzate per determinare l'autenticità di un messaggio, come un token Web JSON (JWT), le informazioni della carta di credito tokenizzate o una password inviata. Possono essere utilizzati anche come funzioni di derivazione chiave (KDF) sicure, specialmente nelle applicazioni che richiedono chiavi deterministiche.

Le chiavi KMS HMAC offrono un vantaggio rispetto agli HMAC del software applicativo perché il materiale della chiave viene generato e utilizzato interamente all'interno di AWS KMS, in base ai controlli dell'accesso impostati per la chiave.

> **Tip**
>
> Le best practice consigliano di limitare la durata dell'efficacia di qualsiasi meccanismo di firma, incluso un HMAC. Ciò scoraggia un attacco in cui l'attore utilizza un messaggio firmato per stabilire la validità ripetutamente o molto tempo dopo la sostituzione del messaggio. I tag HMAC non includono un timestamp, ma puoi includere un timestamp nel token o nel messaggio per rilevare più facilmente quando è il momento di aggiornare l'HMAC.

Gli utenti autorizzati possono creare, gestire e utilizzare le chiavi KMS HMAC nel tuo account AWS. Ciò include le operazioni di abilitazione e disabilitazione delle chiavi, impostazione e modifica di alias e tag e pianificazione dell'eliminazione delle chiavi KMS HMAC. Inoltre, puoi controllare gli accessi alle chiavi KMS HMAC utilizzando le policy della chiave, le policy IAM e le concessioni. È possibile controllare tutte le operazioni che utilizzano o gestiscono le chiavi KMS HMAC all'interno di AWS nei registri AWS CloudTrail. Puoi creare chiavi KMS HMAC con materiale della chiave importato. Inoltre, puoi creare chiavi KMS HMAC multi-regione, che si comportano come copie della stessa chiave KMS HMAC in più Regioni AWS.

Le chiavi KMS HMAC supportano solo le operazioni crittografiche `GenerateMac` e `VerifyMac`. Non è possibile utilizzare le chiavi KMS HMAC per crittografare i dati o firmare messaggi o utilizzare qualsiasi altro tipo di chiave KMS nelle operazioni HMAC. Quando utilizzi l'operazione `GenerateMac`, fornisci un messaggio fino a 4.096 byte, una chiave KMS HMAC e l'algoritmo MAC compatibile con la specifica della chiave HMAC, e `GenerateMac` calcola il tag HMAC. Per verificare un tag HMAC, è necessario fornire il tag HMAC e lo stesso messaggio, la chiave KMS HMAC e l'algoritmo MAC utilizzato da `GenerateMac` per calcolare il tag HMAC originale. L'operazione `VerifyMac` calcola il tag HMAC e verifica che sia identico al tag HMAC fornito. Se il tag HMAC inserito non corrisponde a quello calcolato, la verifica non riesce.

Le chiavi KMS HMAC non supportano la rotazione automatica delle chiavi e non puoi creare una chiave KMS HMAC in un archivio di chiavi personalizzate.

Se crei una chiave KMS per crittografare i dati in un servizio AWS, utilizza una chiave crittografica simmetrica. Non puoi utilizzare una chiave KMS HMAC.

Regioni

Le chiavi KMS HMAC sono supportate in tutte le Regioni AWS supportate da AWS KMS.

Ulteriori informazioni

- Per assistenza nella scelta di un tipo di chiave KMS, consulta la sezione Scelta di un tipo di chiave KMS.
- Per una tabella di confronto delle operazioni dell'API AWS KMS supportate per ciascun tipo di chiave KMS, consulta la sezione Documentazione di riferimento dei tipi di chiave.
- Per informazioni sulla creazione di chiavi KMS HMAC multi-regione, consulta la sezione Chiavi multi-regione in AWS KMS.
- Per esaminare la differenza nella policy della chiave predefinita configurata dalla console AWS KMS per le chiavi KMS HMAC, consulta la sezione the section called “Consente agli utenti della chiave di utilizzare la chiave KMS con i servizi AWS”.
- Per informazioni sui prezzi delle chiavi KMS HMAC, consulta la pagina Prezzi di AWS Key Management Service.
- Per informazioni sulle quote applicabili alle chiavi KMS HMAC, consulta le sezioni Quote delle risorse e Quote di richieste.
- Per informazioni sull'eliminazione delle chiavi KMS HMAC, consulta la sezione Eliminazione di AWS KMS keys.
- Per informazioni sull'utilizzo di HMAC per creare token Web JSON, consulta la sezione Come proteggere gli HMAC in AWS KMS nel Blog sulla sicurezza di AWS.
- Ascolta il podcast: Introduzione a HMAC per AWS Key Management Service sul Podcast ufficiale AWS.

Argomenti

- Visualizzazione delle chiavi KMS HMAC

Specifiche della chiave per le chiavi KMS HMAC

AWS KMS supporta chiavi HMAC simmetriche di lunghezze diverse. La scelta della specifica della chiave può dipendere da requisiti normativi, di sicurezza o aziendali. La lunghezza della chiave determina l'algoritmo MAC utilizzato nelle VerifyMacoperazioni GenerateMace nelle operazioni. In generale, le chiavi più lunghe sono più sicure. Usa la chiave più lunga funzionale per il tuo caso d'uso.

Specifica della chiave HMAC	Algoritmo MAC
HMAC_224	HMAC_SHA_224
HMAC_256	HMAC_SHA_256
HMAC_384	HMAC_SHA_384
HMAC_512	HMAC_SHA_512

Creazione di chiavi KMS HMAC

Puoi creare chiavi KMS HMAC nella console AWS KMS, tramite l'API CreateKey o utilizzando un modello AWS CloudFormation.

AWS KMS supporta molteplici specifiche della chiave per le chiavi KMS HMAC. La scelta della specifica della chiave può essere determinata da requisiti normativi, di sicurezza o aziendali. In generale, le chiavi più lunghe sono più resistenti agli attacchi a forza bruta.

> **Important**
>
> Non includere informazioni riservate o sensibili nell'alias, nella descrizione o nei tag. Questi campi possono apparire in testo semplice nei CloudTrail log e in altri output.

Se stai creando una chiave KMS per crittografare i dati in un servizio AWS, utilizza una chiave KMS di crittografia simmetrica. I servizi AWS integrati con AWS KMS non supportano le chiavi

KMS asimmetriche né le chiavi KMS HMAC. Per informazioni sulla creazione di una chiave KMS di crittografia simmetrica, consulta la sezione Creazione di chiavi.

Ulteriori informazioni

- Per determinare quale tipo di chiave KMS creare, consulta la sezione Scelta di un tipo di chiave KMS.
- Per creare una chiave KMS HMAC primaria multi-regione, è possibile utilizzare le procedure descritte in questo argomento. Per replicare una chiave HMAC multi-regione, consulta la sezione the section called “Creazione di chiavi di replica”.
- Per informazioni sulle autorizzazioni richieste per la creazione di chiavi KMS, consultare Autorizzazioni per la creazione di chiavi KMS.
- Per informazioni sull'utilizzo di un AWS CloudFormation modello per creare una chiave KMS HMAC, consulta AWS::KMS::Keyla Guida per l'AWS CloudFormationutente.

Argomenti

- Creazione di chiavi KMS HMAC (console)
- Creazione di chiavi KMS HMAC (API AWS KMS)

Creazione di chiavi KMS HMAC (console)

Per creare chiavi KMS HMAC puoi utilizzare la AWS Management Console. Le chiavi KMS HMAC sono chiavi simmetriche con un utilizzo della chiave Generate and verify MAC (Genera e verifica MAC). È possibile anche creare chiavi HMAC multi-regione.

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.
4. Scegliere Create key (Crea chiave).
5. Alla voce Key type (Tipo di chiave), scegliere Symmetric (Simmetrica).

   Le chiavi KMS HMAC sono simmetriche. Usa la stessa chiave per generare e verificare i tag HMAC.
6. Per Key usage (Utilizzo della chiave), scegli Generate and verify MAC (Genera e verifica MAC).

Generate and verify MAC (Genera e verifica MAC) è l'unico utilizzo valido per le chiavi KMS HMAC.

> **Note**
>
> Key usage (Utilizzo della chiave) viene visualizzato per le chiavi simmetriche solo quando le chiavi KMS HMAC sono supportate nella regione selezionata.

7. Seleziona un valore Key spec (Specifica della chiave) per la tua chiave KMS HMAC.

   La scelta della specifica della chiave può essere determinata da requisiti normativi, di sicurezza o aziendali. In generale, le chiavi più lunghe sono più sicure.

8. Per creare una chiave HMAC primaria multi-regione, in Advanced options (Opzioni avanzate) scegli Multi-Region key (Chiave multi-regione). Le proprietà condivise che definisci per questa chiave KMS, come il tipo di chiave e l'utilizzo della chiave, saranno condivise con le relative chiavi di replica. Per informazioni dettagliate, vedi Creazione di chiavi multiregione.

   Non è possibile utilizzare questa procedura per creare una chiave di replica. Per creare una chiave HMAC di replica multi-regione, segui le istruzioni per creare una chiave di replica.

9. Seleziona Avanti.

10. Inserisci un alias per la chiave KMS. Un nome di alias non può iniziare con **`aws/`**. Il prefisso **`aws/`** è riservato da Amazon Web Services per rappresentare le Chiavi gestite da AWS nel tuo account.

    Ti consigliamo di utilizzare un alias che identifichi la chiave KMS come chiave HMAC, ad esempio `HMAC/test-key`. In questo modo è più semplice identificare le chiavi HMAC nella console AWS KMS, dove puoi ordinare e filtrare le chiavi per tag e alias, ma non in base alla specifica o all'utilizzo delle chiavi.

    Gli alias sono obbligatori quando si crea una chiave KMS nella AWS Management Console. Non è possibile specificare un alias quando si utilizza l'CreateKeyoperazione, ma è possibile utilizzare la console o l'CreateAliasoperazione per creare un alias per una chiave KMS esistente. Per informazioni dettagliate, vedi Utilizzo di alias.

11. (Facoltativo) Inserisci una descrizione per la chiave KMS.

    Inserire una descrizione che illustra il tipo di dati che si desidera proteggere o l'applicazione che si desidera utilizzare con la chiave KMS.

Puoi aggiungere una descrizione ora o aggiornarla in qualsiasi momento, a meno che lo stato della chiave non sia `Pending Deletion` o `Pending Replica Deletion`. Per aggiungere, modificare o eliminare la descrizione di una chiave gestita dal cliente esistente, modifica la descrizione nella AWS Management Console o utilizza l'operazione. UpdateKeyDescription

12. (Facoltativo) Inserisci un tag della chiave e un valore facoltativo. Per aggiungere più di un tag alla chiave KMS scegli Add tag (Aggiungi tag).

    Puoi anche aggiungere un tag che identifica la chiave come chiave HMAC, ad esempio `Type=HMAC`. In questo modo è più semplice identificare le chiavi HMAC nella console AWS KMS, dove puoi ordinare e filtrare le chiavi per tag e alias, ma non in base alla specifica o all'utilizzo delle chiavi.

    Quando aggiungi i tag alle risorse AWS, AWS genera un report di allocazione dei costi in cui l'utilizzo e i costi sono aggregati in base ai tag. I tag possono essere utilizzati anche per controllare l'accesso a una chiave KMS. Per informazioni sull'assegnazione di tag delle chiavi KMS, consulta Chiavi di tagging e ABAC per AWS KMS.
13. Seleziona Next (Successivo).
14. Seleziona i ruoli e gli utenti IAM che possono gestire la chiave KMS.

    > **Note**
    >
    > Questa policy delle chiavi fornisce all'Account AWS il controllo completo di questa chiave KMS. Consente agli amministratori dell'account di utilizzare policy IAM per concedere ad altri principali l'autorizzazione per la gestione della chiave KMS. Per informazioni dettagliate, vedi the section called “Policy delle chiavi predefinita”.
    > Le best practice di IAM disincentivano l'uso di utenti IAM con credenziali a lungo termine. Quando possibile, utilizza i ruoli IAM che forniscono credenziali temporanee. Per i dettagli, consulta la sezione Best practice di sicurezza in IAM nella Guida per l'utente IAM.
15. (Facoltativo) Per impedire ai ruoli e agli utenti IAM selezionati di eliminare questa chiave KMS, nella sezione Eliminazione chiave nella parte inferiore della pagina, deseleziona la casella di controllo Consenti agli amministratori delle chiavi di eliminare questa chiave.
16. Seleziona Next (Successivo).
17. Seleziona i ruoli e gli utenti IAM che possono utilizzare la chiave KMS per operazioni di crittografia.

> **Note**
>
> Questa policy delle chiavi fornisce all'Account AWS il controllo completo di questa chiave KMS. Consente agli amministratori dell'account di utilizzare le policy IAM per fornire ad altri principali l'autorizzazione per utilizzare la chiave KMS nelle operazioni di crittografia. Per informazioni dettagliate, vedi the section called “Policy delle chiavi predefinita”.
> Le best practice di IAM disincentivano l'uso di utenti IAM con credenziali a lungo termine. Quando possibile, utilizza i ruoli IAM che forniscono credenziali temporanee. Per i dettagli, consulta la sezione Best practice di sicurezza in IAM nella Guida per l'utente IAM.

18. (Facoltativo) È possibile consentire ad altri Account AWS di utilizzare questa chiave KMS per operazioni di crittografia. A questo proposito, nella sezione Altri Account AWS, nella parte inferiore della pagina, scegli Aggiungi un altro Account AWS e inserisci il numero di identificazione Account AWS di un account esterno. Per aggiungere più account esterni, ripetere questo passaggio.

> **Note**
>
> Per consentire ai principali negli account esterni di utilizzare la chiave KMS, gli amministratori dell'account esterno devono creare policy IAM che forniscono tali autorizzazioni. Per ulteriori informazioni, consultare Autorizzazione per gli utenti in altri account di utilizzare una chiave KMS.

19. Seleziona Next (Successivo).
20. Esaminare le principali impostazioni scelte. È comunque possibile tornare indietro e modificare tutte le impostazioni.
21. Scegli Finish (Termina) per creare la chiave KMS HMAC.

Creazione di chiavi KMS HMAC (API AWS KMS)

È possibile utilizzare l'CreateKeyoperazione per creare una chiave KMS HMAC. Questi esempi utilizzano la AWS Command Line Interface (AWS CLI), ma puoi usare anche qualsiasi linguaggio di programmazione supportato.

Quando crei una chiave KMS HMAC, devi specificare il parametro `KeySpec` che determina il tipo di chiave KMS. Inoltre, devi specificare il valore `KeyUsage` di GENERATE_VERIFY_MAC, anche se è l'unico valore valido per l'utilizzo della chiave per le chiavi HMAC. Per creare una chiave KMS HMAC multi-regione, aggiungi il parametro `MultiRegion` con un valore `true`. Una volta creata la chiave KMS, non è più possibile modificare queste proprietà.

L'`CreateKey`operazione non consente di specificare un alias, ma è possibile utilizzare l'CreateAliasoperazione per creare un alias per la nuova chiave KMS. Ti consigliamo di utilizzare un alias che identifichi la chiave KMS come chiave HMAC, ad esempio `HMAC/test-key`. In questo modo è più semplice identificare le chiavi HMAC nella console AWS KMS, dove puoi ordinare e filtrare le chiavi per alias, ma non in base alla specifica o all'utilizzo delle chiavi.

Se tenti di creare una chiave KMS HMAC in una Regione AWS in cui le chiavi HMAC non sono supportate, l'operazione `CreateKey` restituisce un'eccezione `UnsupportedOperationException`

Gli esempi seguenti utilizzano l'operazione `CreateKey` per creare una chiave KMS HMAC a 512 bit.

```
$ aws kms create-key --key-spec HMAC_512 --key-usage GENERATE_VERIFY_MAC
{
    "KeyMetadata": {
        "KeyState": "Enabled",
        "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "KeyManager": "CUSTOMER",
        "Description": "",
        "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "CreationDate": 1669973196.214,
        "MultiRegion": false,
        "KeySpec": "HMAC_512",
        "CustomerMasterKeySpec": "HMAC_512",
        "KeyUsage": "GENERATE_VERIFY_MAC",
        "MacAlgorithms": [
            "HMAC_SHA_512"
        ],
        "AWSAccountId": "111122223333",
        "Origin": "AWS_KMS",
        "Enabled": true
    }
}
```

Controllo dell'accesso alle chiavi KMS HMAC

Per controllare l'accesso a una chiave KMS HMAC è necessario utilizzare una policy della chiave, richiesta per ogni chiave KMS. Puoi utilizzare anche le policy IAM e le concessioni.

La policy della chiave di default per le chiavi HMAC create nella console AWS KMS fornisce agli utenti della chiave l'autorizzazione a richiamare le operazioni `GenerateMac` e `VerifyMac`. Tuttavia, non include l'istruzione della policy della chiave progettata per l'utilizzo delle concessioni con i servizi AWS. Se crei chiavi HMAC utilizzando l'operazione `CreateKey`, devi specificare queste autorizzazioni nella policy della chiave o in una policy IAM.

Per perfezionare e limitare le autorizzazioni alle chiavi HMAC puoi utilizzare le chiavi di condizione globali AWS e le chiavi di condizione AWS KMS. Ad esempio, puoi utilizzare la chiave di condizione `kms:ResourceAliases` per controllare l'accesso alle operazioni AWS KMS in base agli alias associati a una chiave HMAC. Le seguenti condizioni delle policy AWS KMS sono utili per le policy relative alle chiavi HMAC.

- Usa una chiave di condizione `kms:MacAlgorithm` per limitare gli algoritmi che i principali possono richiedere quando richiamano le operazioni `GenerateMac` e `VerifyMac`. Ad esempio, è possibile permettere ai principali di richiamare le operazioni `GenerateMac`ma solo quando l'algoritmo MAC nella richiesta è `HMAC_SHA_384`.
- Usa una chiave di condizione `kms:KeySpec` per permettere o impedire ai principali di creare determinati tipi di chiavi HMAC. Ad esempio, per consentire ai principali di creare solo chiavi HMAC, è possibile consentire l'CreateKeyoperazione, ma utilizzare la `kms:KeySpec` condizione per consentire solo chiavi con una specifica `HMAC_384` chiave.

  Puoi utilizzare la chiave di condizione `kms:KeySpec` anche per controllare l'accesso ad altre operazioni su una chiave KMS in base alla specifica della chiave. Ad esempio, puoi permettere ai principali di pianificare e annullare l'eliminazione della chiave solo sulle chiavi KMS con una specifica della chiave `HMAC_256`.
- Usa la chiave di condizione `kms:KeyUsage` per permettere o impedire ai principali di creare determinati tipi di chiavi HMAC. Ad esempio, per consentire ai principali di creare solo chiavi HMAC, è possibile consentire l'CreateKeyoperazione, ma utilizzare la `kms:KeyUsage` condizione per consentire solo le chiavi che utilizzano una chiave. `GENERATE_VERIFY_MAC`

  Puoi utilizzare la chiave di condizione `kms:KeyUsage` anche per controllare l'accesso ad altre operazioni su una chiave KMS in base all'utilizzo della chiave. Ad esempio, puoi

permettere ai principali di abilitare e disabilitare solo le chiavi KMS con un utilizzo della chiave `GENERATE_VERIFY_MAC`.

Puoi anche creare concessioni per le operazioni `GenerateMac` e `VerifyMac`, che sono operazioni di concessione. Tuttavia, non puoi utilizzare vincoli di concessione del contesto di crittografia in una concessione per una chiave HMAC. Il formato dei tag HMAC non supporta i valori del contesto di crittografia.

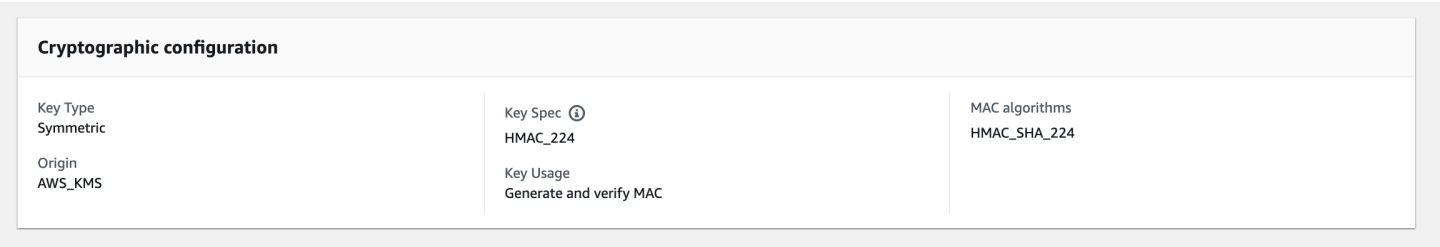
Visualizzazione delle chiavi KMS HMAC

Puoi visualizzare le chiavi KMS HMAC nella console AWS KMS o tramite l'API DescribeKey. Puoi monitorare l'uso delle tue chiavi HMAC KMS nei AWS CloudTraillog e in Amazon. CloudWatch Per istruzioni di base sulla visualizzazione delle chiavi KMS, consulta la sezione Visualizzazione di chiavi.

È possibile distinguere le chiavi KMS HMAC da altri tipi di chiavi KMS in base alla specifica della chiave, che inizia con `HMAC`, o al suo utilizzo, che è sempre Generate and verify MAC (Genera e verifica MAC, `GENERATE_VERIFY_MAC`).

Le chiavi KMS HMAC sono incluse nella tabella sulla pagina Customer managed keys (Chiavi gestite dal cliente) della console AWS KMS. Tuttavia, non è possibile ordinare o filtrare le chiavi KMS in base alla specifica o all'utilizzo della chiave. Per semplificare la ricerca delle chiavi HMAC, puoi assegnare loro un alias o un tag distintivo. In questo modo, potrai ordinare o filtrare le chiavi in base all'alias o al tag.

Nella pagina dei dettagli della chiave di una chiave KMS HMAC puoi trovare i dettagli di configurazione nella scheda Cryptographic configuration (Configurazione di crittografia).



Chiavi multi-regione in AWS KMS

AWS KMS supporta le chiavi multi-regione, che sono AWS KMS keys in diversi Regioni AWS che possono essere utilizzate in modo intercambiabile, come se avessi la stessa chiave in più regioni. Ogni set di chiavi multi-regione correlate ha lo stesso materiale della chiave e ID chiave, in modo da

poter crittografare i dati in un Regione AWS e decrittarli in un altro Regione AWS senza crittografare nuovamente o effettuare una chiamata tra regioni a AWS KMS.

Come tutte le chiavi KMS, le chiavi multi-regione non lasciano mai AWS KMS non crittografato. È possibile creare chiavi multi-regione simmetriche o asimmetriche per la crittografia o la firma, creare chiavi multi-regione HMAC per la generazione e la verifica dei tag HMAC e creare chiavi multi-regione con materiale della chiave importato o materiale della chiave generato da AWS KMS. È necessario gestire ogni chiave multi-regione in modo indipendente, inclusa la creazione di alias e tag, l'impostazione delle policy chiave e delle concessioni e l'abilitazione e la disabilitazione selettiva. È possibile utilizzare chiavi multi-regione in tutte le operazioni di crittografia che è possibile eseguire con le chiavi di singola regione.

Le chiavi multi-regione sono una soluzione flessibile e potente per molti scenari comuni di sicurezza dei dati.

Ripristino di emergenza

In un'architettura di backup e ripristino, le chiavi multi-regione consentono di elaborare i dati crittografati senza interruzioni anche in caso di una interconnessione Regione AWS. I dati mantenuti nelle regioni di backup possono essere decrittati nella regione di backup e i dati appena crittografati nella regione di backup possono essere decrittati nella regione principale quando tale regione viene ripristinata.

Gestione globale dei dati

Le aziende che operano a livello globale necessitano di dati distribuiti a livello globale e che siano disponibili in modo coerente in Regioni AWS. È possibile creare chiavi multi-regione in tutte le aree geografiche in cui risiedono i dati, quindi utilizzare le chiavi come se fossero una chiave singola regione senza la latenza di una chiamata tra regioni diverse o il costo di una nuova crittografia dei dati sotto una chiave diversa in ogni regione.

Applicazioni per la firma distribuita

Le applicazioni che richiedono funzionalità di firma tra regioni diverse possono utilizzare chiavi di firma asimmetriche multi-regione per generare firme digitali identiche in modo coerente e ripetuto in diverse Regioni AWS.

Se utilizzi il concatenamento dei certificati con un unico archivio attendibile globale (per una singola autorità di certificazione radice (CA) e CA intermedia regionali firmate dalla CA principale, non sono necessarie chiavi multi-regione. Tuttavia, se il sistema non supporta CA intermedie,

ad esempio la firma delle applicazioni, è possibile utilizzare le chiavi multi-regione per garantire coerenza alle certificazioni internazionali.

Applicazioni in modalità attivo-attivo che si estendono su più regioni

Alcuni carichi di lavoro e applicazioni possono estendersi su più regioni in architetture di modalità attivo-attivo. Per queste applicazioni, le chiavi multi-regione possono ridurre la complessità fornendo lo stesso materiale chiave per le operazioni simultanee di crittografia e decrittografia sui dati che potrebbero essere spostati oltre i confini della regione.

È possibile utilizzare chiavi multi-regione con file crittografati lato client, ad esempio AWS Encryption SDK, il Client di crittografia DynamoDB, e file crittografato lato client Amazon S3. Per un esempio di utilizzo delle chiavi multi-regioni con le tabelle globali di Amazon DynamoDB e DynamoDB Encryption Client, vedere file crittografato di dati globali lato client con AWS KMSchiavi multi-regione nel Blog sulla sicurezzaAWS.

servizi AWS che si integrano con AWS KMS per la crittografia a riposo o le firme digitali attualmente trattano le chiavi multi-regione come se fossero chiavi a singola regione. Potrebbero riavvolgere o crittografare i dati spostati tra le regioni. Ad esempio, la replica tra regioni di Amazon S3 decritta e crittografa nuovamente i dati sotto una chiave KMS nell'area di destinazione, anche durante la replica di oggetti protetti da una chiave multi-regione.

Le chiavi multi-regione non sono globali. Creare una chiave primaria multi-regione e quindi replicarla in Regioni selezionate all'interno di una partizione AWS. Puoi quindi gestire la chiave multi-regione in ogni regione in modo indipendente. Né AWS né AWS KMS crea o replica automaticamente chiavi multi-regione in qualsiasi regione per tuo conto. Chiavi gestite da AWS, le chiavi KMS che i servizi AWS creano nel tuo account per te, sono sempre chiavi di singola regione.

Non è possibile convertire una chiave di regione singola esistente in una chiave multi-regione. Questo design garantisce che tutti i dati protetti con le chiavi esistenti di regione singola mantengano le stesse proprietà di residenza e sovranità dei dati.

Per la maggior parte delle esigenze di sicurezza dei dati, l'isolamento regionale e la tolleranza ai guasti delle risorse regionali rendono standard le chiavi di una singola regione AWS KMS la soluzione più adatta. Tuttavia, quando è necessario crittografare o firmare i dati in applicazioni lato client in più regioni, è possibile che le chiavi multi-regione siano la soluzione.

Regioni

Le chiavi multi-regione sono supportate in tutte le Regioni AWS that AWS KMS supporta tranne Cina (Pechino) e Cina (Ningxia).

Prezzi e quote

Ogni chiave di un set di chiavi multi-regione viene conteggiata come una chiave KMS per i prezzi e le quote. Le quote di AWS KMS sono calcolate separatamente per ogni regione di un account. L'utilizzo e la gestione delle chiavi multi-regione in ogni regione conteggiano per le quote per quella regione.

Tipi di chiavi KMS supportati

È possibile creare i seguenti tipi di chiavi KMS multiregione:

- Chiavi KMS di crittografia simmetrica
- Chiavi KMS asimmetriche
- Chiavi KMS HMAC
- Chiavi KMS con materiale della chiave importato

Non è possibile creare chiavi multi-regione in un archivio delle chiavi personalizzate.

Argomenti

- Controllo dell'accesso alle chiavi multi-regione
- Creazione di chiavi multi-regione
- Visualizzazione delle chiavi multi-regione
- Gestione delle chiavi multi-regione
- Importazione di materiale della chiave in chiavi multi-regione
- Eliminazione di chiavi multi-regione

Considerazioni sulla protezione per le chiavi multi-regione

Utilizza una chiave multi-regione AWS KMS solo quando ne hai bisogno. Le chiavi multi-regione offrono una soluzione flessibile e scalabile per carichi di lavoro che spostano dati crittografati tra Regioni AWS o hanno bisogno di un accesso tra regioni. Considera una chiave multi-regione se hai bisogno di condividere, spostare o eseguire il backup di dati protetti tra regioni o creare firme digitali identiche di applicazioni che operano in diverse regioni.

Tuttavia, il processo di creazione di una chiave multi-regione sposta il materiale chiave su limiti Regione AWS all'interno di AWS KMS. Il testo cifrato generato da una chiave multi-regione può potenzialmente essere decrittato da più chiavi correlate in più posizioni geografiche. I servizi e le risorse isolate a livello regionale offrono vantaggi significativi. Ogni Regione AWS è isolata e indipendente dalle altre regioni. Le regioni forniscono la tolleranza ai guasti, la stabilità e la resilienza e possono anche ridurre la latenza. Consentono di creare risorse ridondanti che restano disponibili e non influenzate da un'interruzione in un'altra regione. Nello stato AWS KMS, assicurano anche che ogni testo cifrato possa essere decrittato da una sola chiave.

Le chiavi multi-regione sollevano anche nuove considerazioni sulla sicurezza:

- Il controllo dell'accesso e l'applicazione della policy di sicurezza dei dati è più complesso con le chiavi multi-regione. È necessario assicurarsi che la policy sia controllata in modo coerente sulla chiave in più aree isolate. E devi usare la policy per applicare i limiti, invece di fare affidamento su chiavi separate.

  Ad esempio, è necessario impostare le condizioni di policy sui dati per impedire ai team del ciclo paghe di una regione di leggere i dati del ciclo paghe per una regione diversa. Inoltre, è necessario utilizzare il controllo di accesso per impedire uno scenario in cui una chiave multi-regione in una regione protegge i dati di un tenant e una chiave multi-regione correlata in un'altra regione protegge i dati di un tenant diverso.
- Anche la verifica delle chiavi in tutte le regioni è più complesso. Con le chiavi multi-regione, è necessario esaminare e riconciliare le attività di verifica in più regioni per ottenere una comprensione completa delle attività chiave sui dati protetti.
- La conformità ai requisiti di residenza dei dati può essere più complessa. Con le regioni isolate, è possibile garantire la residenza dei dati e la conformità alla sovranità dei dati. Le chiavi KMS in una determinata regione possono decrittare i dati sensibili solo in tale regione. I dati crittografati in una regione possono rimanere completamente protetti e inaccessibili in qualsiasi altra regione.

  Per verificare la residenza dei dati e la sovranità dei dati con chiavi multi-regione, è necessario implementare policy di accesso e compilare eventi AWS CloudTrail in più regioni.

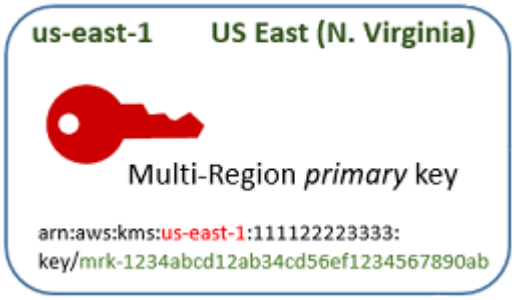
Per semplificare la gestione del controllo degli accessi su chiavi multiregionali, l'autorizzazione a replicare una chiave multiregionale (kms: ReplicateKey) è separata dall'autorizzazione standard per creare chiavi (kms:). CreateKey Inoltre, AWS KMS supporta diverse condizioni di policy per le chiavi multi-regione, tra cui `kms:MultiRegion`, che consente o nega l'autorizzazione a creare, utilizzare o gestire chiavi multi-regione e `kms:ReplicaRegion`, che limita le regioni in cui è possibile replicare

una chiave multi-regione. Per informazioni dettagliate, vedi Controllo dell'accesso alle chiavi multi-regione.

Come funzionano le chiavi multi-regione

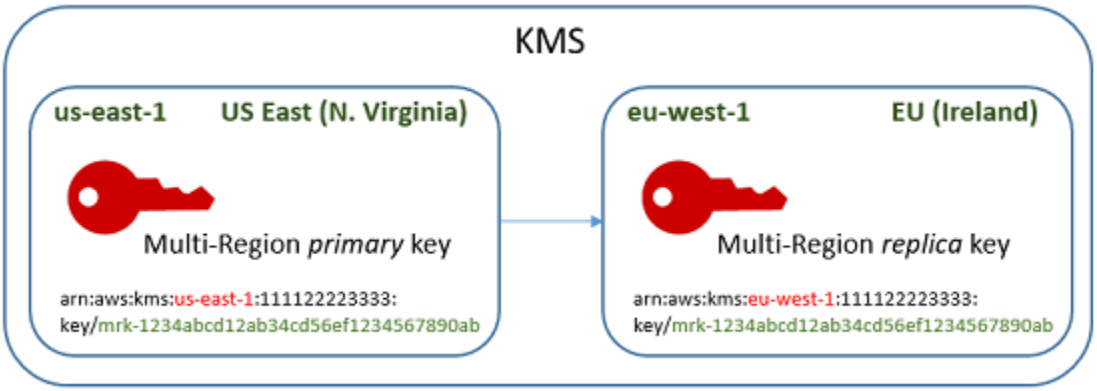
Si inizia creando una chiave primaria multi-regione simmetrica o asimmetrica in un Regione AWS che AWS KMS supporta, come gli Stati Uniti orientali (Virginia settentrionale). È possibile decidere se una chiave è di regione singola o multi-regione solo al momento della creazione. Non è possibile modificare questa proprietà in un secondo momento. Come per qualsiasi chiave KMS, è possibile impostare una policy delle chiavi per la chiave multi-regione ed è possibile creare concessioni e aggiungere alias e tag per la categorizzazione e l'autorizzazione. (Queste sono proprietà indipendenti che non sono condiviei o sincronizzate con altre chiavi.) È possibile utilizzare la chiave primaria multi-regione nelle operazioni di crittografia per la crittografia o la firma.

È possibile creare una chiave primaria multiregionale nella AWS KMS console o utilizzando l'CreateKeyAPI con il parametro impostato su. `MultiRegion` `true` Si noti che le chiavi multi-regione hanno un ID chiave distintivo che inizia con `mrk-`. Puoi utilizzare il prefisso `mrk-` per identificare gli MRK a livello di programmazione.



Se scegli, puoi replicare la chiave primaria multi-regione in una o più diverse Regioni AWS nella stessa partizione AWS come Europa (Irlanda). Quando lo fai, AWS KMS crea una chiave di replica nella regione specificata con lo stesso ID chiave e altre proprietà condivise come chiave primaria. Trasporta in modo sicuro il materiale chiave attraverso il confine della regione e lo associa alla nuova chiave KMS nella regione di destinazione, il tutto all'interno di AWS KMS. Il risultato è due chiavi multi-regione correlate, una chiave primaria e una chiave di replica, che possono essere utilizzate in modo intercambiabile.

È possibile creare una chiave di replica multiregionale nella AWS KMS console o utilizzando l'API. ReplicateKey



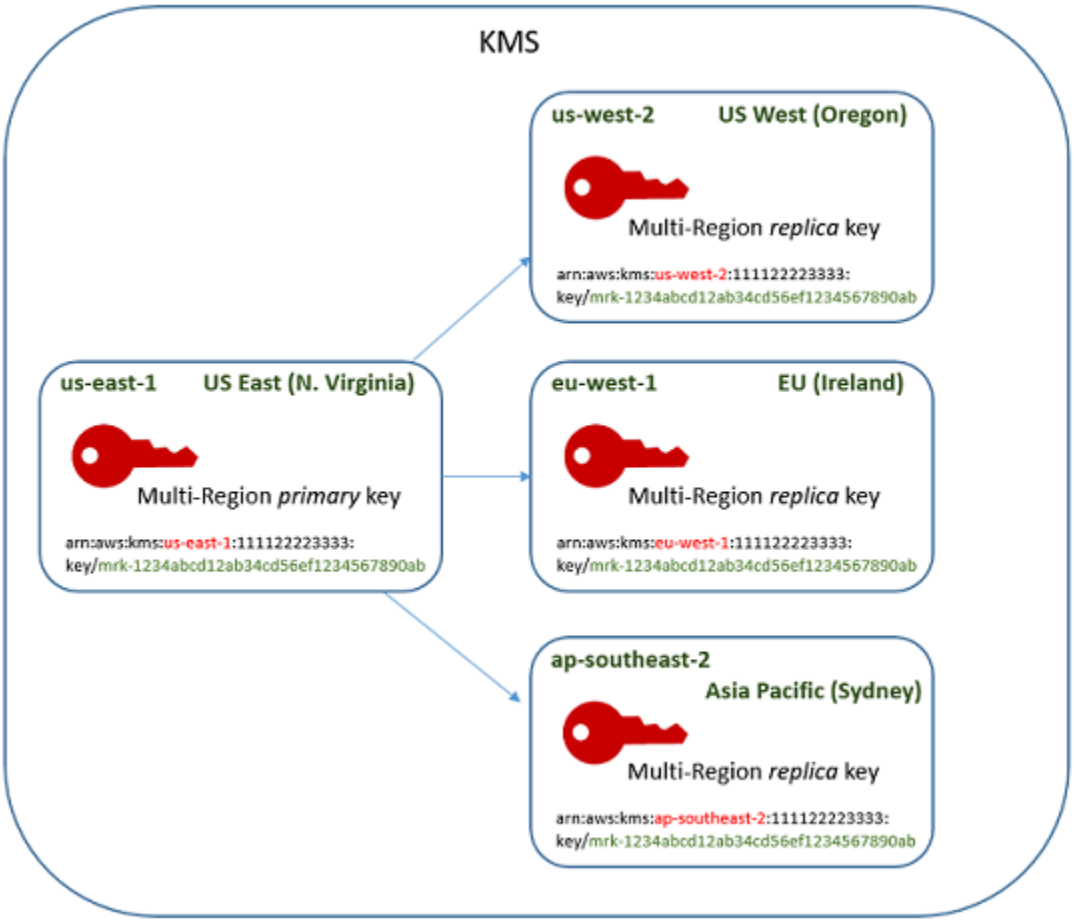
La risultante chiave di replica multi-regione è una chiave KMS completamente funzionale con le stesse proprietà condivise come chiave primaria. Per tutti gli altri aspetti, si tratta di una chiave KMS indipendente con descrizione, policy delle chiavi, concessioni, alias e tag propri. L'attivazione o la disattivazione di una chiave multi-regione non ha alcun effetto sulle chiavi multi-regione. È possibile utilizzare le chiavi primarie e di replica in modo indipendente nelle operazioni di crittografia o coordinarne l'utilizzo. Ad esempio, è possibile crittografare i dati con la chiave primaria nella regione Stati Uniti orientali (Virginia settentrionale), spostare i dati nella regione Europa (Irlanda) e utilizzare la chiave di replica per decrittare i dati.

Le chiavi multi-regione correlate hanno lo stesso ID chiave. I loro ARN della chiave (nomi delle risorse Amazon) differiscono solo nel campo Regione. Ad esempio, la chiave primaria multi-regione e le chiavi di replica potrebbero avere i seguenti di esempi di ARN della chiave. L'ID chiave, l'ultimo elemento nell'ARN della chiave, è identico. Entrambe le chiavi hanno l'ID chiave distintivo delle chiavi multi-regione, che inizia con mrk-.

```
Primary key: arn:aws:kms:us-
east-1:111122223333:key/mrk-1234abcd12ab34cd56ef12345678990ab
Replica key: arn:aws:kms:eu-
west-1:111122223333:key/mrk-1234abcd12ab34cd56ef12345678990ab
```

Per l'interoperabilità è necessario disporre dello stesso ID chiave. Durante la crittografia, AWS KMS associa l'ID chiave della chiave KMS al testo cifrato in modo che il testo cifrato possa essere decrittato solo con tale chiave KMS o una chiave KMS con lo stesso ID chiave. Questa caratteristica rende anche facili da riconoscere le chiavi multi-regione correlate e rende più facile utilizzarle in modo intercambiabile. Ad esempio, quando le si utilizzano in un'applicazione, è possibile fare riferimento alle chiavi multi-regione correlate tramite il relativo ID chiave condivisa. Quindi, se necessario, specificare la regione o l'ARN per distinguerli.

Man mano che le esigenze dei dati cambiano, è possibile replicare la chiave primaria ad altri Regioni AWS nella stessa partizione, come gli Stati Uniti occidentali (Oregon) e Asia Pacifico (Sydney). Il risultato è quattro chiavi multi-regione correlate con lo stesso materiale della chiave e gli stessi ID chiave, come illustrato nel diagramma seguente. Gestisci le chiavi in modo indipendente. Puoi usarle indipendentemente o in modo coordinato. Ad esempio, è possibile crittografare i dati con la chiave di replica in Asia Pacifico (Sydney), spostare i dati in Stati Uniti occidentali (Oregon) e decrittarli con la chiave di replica in Stati Uniti occidentali (Oregon).



Altre considerazioni per le chiavi multi-regione includono le seguenti.

Sincronizzazione delle proprietà condivise — Se una proprietà condivisa delle modifiche delle chiavi multi-regione, AWS KMS sincronizza automaticamente la modifica dalla chiave primaria a tute le sue chiavi di replica. Non è possibile richiedere o forzare una sincronizzazione delle proprietà condivise. AWS KMS rileva e sincronizza tutte le modifiche. Tuttavia, è possibile controllare la sincronizzazione utilizzando l'SynchronizeMultiRegionKeyevento nei log. CloudTrail

Ad esempio, se si abilita la rotazione automatica delle chiavi su una chiave primaria simmetrica multi-regione, AWS KMS copia tale impostazione su tutte le chiavi di replica. Quando il materiale

chiave viene ruotato, la rotazione viene sincronizzata tra tutte le chiavi multi-regione correlate, in modo che continuino ad avere lo stesso materiale chiave corrente e ad accedere a tutte le versioni precedenti del materiale chiave. Se si crea una nuova chiave di replica, la chiave contiene lo stesso materiale corrente di tutte le chiavi multi-regione correlate e l'accesso a tutte le versioni precedenti del materiale chiave. Per dettagli, consulta Rotazione di chiavi multiregione.

Modifica della chiave primaria — Ogni set di chiavi multi-regione deve avere esattamente una chiave primaria. La chiave primaria è l'unica chiave che può essere replicata. È anche la fonte delle proprietà condivise delle chiavi di replica. Tuttavia, è possibile modificare la chiave primaria in una replica e promuovere una delle chiavi di replica in primaria. È possibile eseguire questa operazione in modo da poter eliminare una chiave primaria per più aree da una determinata regione o individuare la chiave primaria in una regione più vicina agli amministratori di progetto. Per informazioni dettagliate, vedi Aggiornamento della Regione principale.

Eliminazione di chiavi multi-regione — Come tutte le chiavi KMS, è necessario pianificare l'eliminazione delle chiavi multi-regione prima che AWS KMS li elimini. Mentre la chiave è in attesa di eliminazione, non è possibile utilizzarla in nessuna operazione di crittografia. Tuttavia, AWS KMS non eliminerà una chiave primaria multi-regione finché non verranno eliminate tutte le chiavi di replica. Per informazioni dettagliate, vedi Eliminazione di chiavi multiregione.

Concetti

I termini e i concetti seguenti sono utilizzati con le chiavi multi-regione.

Chiave multi-regione

Una chiave multi-regione è una di un set di chiavi KMS con lo stesso ID chiave e materiale chiave (e altre proprietà condivise) in diversi Regioni AWS. Ogni chiave multi-regione è una chiave KMS completamente funzionante che può essere utilizzata indipendentemente dalle relative chiavi multi-regione correlate. Poiché tutte le chiavi multi-regione correlate hanno lo stesso ID chiave e materiale chiave, sono interoperabili, ovvero qualsiasi chiave multi-regione correlata in qualsiasi Regione AWS può decrittare il testo cifrato da qualsiasi altra chiave multi-regione correlata.

Puoi impostare la proprietà multi-regione di una chiave KMS al momento della sua creazione. Non è possibile modificare la proprietà multi-Regione su una chiave esistente. Non è possibile convertire una chiave a Regione singola in chiave multi-Regione o convertire una chiave multi-Regione in una chiave a Regione singola. Per spostare i carichi di lavoro esistenti in scenari multi-Regione, è necessario crittografare nuovamente i dati o creare nuove firme con nuove chiavi multi-Regione.

Una chiave multi-regione può essere simmetrica o asimmetrica e può utilizzare materiale della chiave AWS KMS o materiale chiave importato. Non è possibile creare chiavi multi-regione in un archivio delle chiavi personalizzate.

In una serie di chiavi multi-regione correlate, c'è esattamente una chiave primaria in qualsiasi momento. È possibile creare chiavi di replica di quella chiave primaria in altri Regioni AWS. È possibile anche aggiornare l'area principale, che modifica la chiave primaria in una chiave di replica e modifica una chiave di replica specificata nella chiave primaria. Tuttavia, è possibile mantenere solo una chiave primaria o una chiave di replica in ogni Regione AWS. Tutte le regioni devono trovarsi nella stessa partizione AWS.

È possibile avere più set di chiavi multi-regione correlate nello stesso o in un diverso Regioni AWS. Sebbene le chiavi multi-regione correlate siano interoperabili, le chiavi multi-regione non correlate non sono interoperabili.

Chiave primaria

Una chiave primaria multi-regione è una chiave KMS che può essere replicata in altri Regioni AWS nella stessa partizione. Ogni set di chiavi multi-regione ha una sola chiave primaria.

Una chiave primaria differisce da una chiave di replica nei seguenti modi:

- Solo una chiave primaria può essere replicata.
- La chiave primaria è la fonte per le proprietà condivise delle sue chiavi di replica, incluso il materiale della chiave e l'ID chiave.
- Puoi abilitare e disabilitare la rotazione automatica delle chiavi solo su una chiave primaria.
- È possibile pianificare l'eliminazione di una chiave primaria in qualsiasi momento. Ma AWS KMS non eliminerà una chiave primaria finché non verranno eliminate tutte le chiavi di replica.

Tuttavia, le chiavi primarie e di replica non differiscono in alcuna proprietà crittografica. È possibile utilizzare una chiave primaria e le relative chiavi di replica in modo intercambiabile.

Non è necessario replicare una chiave primaria. È possibile utilizzarlo come qualsiasi chiave KMS e replicarlo se e quando è utile. Tuttavia, poiché le chiavi multi-regione dispongono di proprietà di protezione diverse dalle chiavi di regione singola, si consiglia di creare una chiave multi-regione solo quando si prevede di replicarla.

Chiave di replica

Una chiave di replica multi-regione è una chiave KMS che ha lo stesso ID chiave e materiale della chiave come sua chiave primaria e chiavi di replica correlate, ma esiste in una Regione AWS diversa.

Una chiave di replica è una chiave KMS completamente funzionale con policy di chiave, privilegi, alias, tag e altre proprietà. Non è una copia o un puntatore alla chiave primaria o a qualsiasi altra chiave. È possibile utilizzare una chiave di replica anche se la chiave primaria e tutte le chiavi di replica correlate sono disabilitate. È inoltre possibile convertire una chiave di replica in una chiave primaria e una chiave primaria in una chiave di replica. Una volta creata, una chiave di replica si basa sulla sua chiave primaria solo per rotazione delle chiavi e aggiornamento della regione primaria.

Le chiavi primarie e di replica non differiscono nelle proprietà crittografiche. È possibile utilizzare una chiave primaria e le relative chiavi di replica in modo intercambiabile. I dati crittografati da una chiave primaria o di replica possono essere decrittati dalla stessa chiave o da qualsiasi chiave primaria o di replica correlata.

Replica

È possibile replicare una chiave primaria multi-regione in un altro Regione AWS nella stessa partizione. Quando si esegue questa operazione, AWS KMS crea una chiave di replica multi-regione nella regione specificata con lo stesso ID chiave e altre proprietà condivise come chiave primaria. Quindi trasporta in modo sicuro il materiale chiave attraverso il confine della regione e lo associa alla nuova chiave di replica, il tutto all'interno di AWS KMS.

Proprietà condivise

Proprietà condivise sono proprietà di una chiave multi-regione primaria che sono condivise con le relative chiavi di replica. AWS KMS crea le chiavi di replica con gli stessi valori di proprietà condivisa di quelli della chiave primaria. Quindi, sincronizza periodicamente i valori delle proprietà condivise della chiave primaria con le relative chiavi di replica. Non è possibile impostare queste proprietà su una chiave di replica.

Di seguito sono riportate le proprietà condivise delle chiavi multi-regione.

- ID chiave — (L'elemento `Region` del ARN della chiave differisce.)
- Materiale della chiave
- Origine del materiale della chiave

- Specifica della chiave e algoritmi di crittografia
- Utilizzo delle chiavi
- Rotazione automatica delle chiavi, è possibile abilitare e disabilitare la rotazione automatica delle chiavi solo sulla chiave primaria. Le nuove chiavi di replica vengono create con tutte le versioni del materiale della chiave condivisa. Per informazioni dettagliate, vedi Rotazione di chiavi multiregione.

È inoltre possibile considerare le designazioni primarie e di replica delle chiavi multi-regione correlate come proprietà condivise. Quando crei nuove chiavi di replica o aggiorni la chiave primaria, AWS KMS sincronizza la modifica con tutte le chiavi multi-regione correlate. Una volta completate queste modifiche, tutte le chiavi multi-regione elencano in modo accurato la chiave primaria e le chiavi di replica.

Tutte le altre proprietà delle chiavi multi-regione sono proprietà indipendenti, compresa la descrizione, la policy delle chiavi, le concessioni, gli stati chiave abilitati e disabilitati, gli alias, e i tag. Puoi impostare gli stessi valori per queste proprietà su tutte le chiavi multi-regione correlate, ma se si modifica il valore di una proprietà indipendente, AWS KMS non lo sincronizza.

È possibile tenere traccia della sincronizzazione delle proprietà condivise delle chiavi multi-regione. Nel tuo AWS CloudTrail registro, cerca l'SynchronizeMultiRegionKeyevento.

Controllo dell'accesso alle chiavi multi-regione

È possibile utilizzare chiavi multi-regione in scenari di conformità, ripristino di emergenza e backup più complessi con le chiavi di singola regione. Tuttavia, poiché le proprietà di protezione delle chiavi multi-regione sono significativamente diverse da quelle delle chiavi di regione singola, si consiglia di prestare attenzione quando si autorizza la creazione, la gestione e l'utilizzo di chiavi multi-regione.

> **Note**
>
> Dichiarazioni di policy IAM esistenti con caratteri jolly nel campo `Resource` ora si applicano sia alle chiavi di regione singola che a quelle multi-regione. Per limitarli alle chiavi KMS a regione singola o alle chiavi multiregione, usa la chiave kms: condition. MultiRegion

Utilizza gli strumenti di autorizzazione per impedire la creazione e l'utilizzo di chiavi multi-regione in qualsiasi scenario in cui una singola regione è sufficiente. Consenti ai principali di replicare una chiave multi-regione solo nelle Regioni AWS che li richiedono. Concedere l'autorizzazione per le chiavi multi-regione solo ai principali che ne hanno bisogno e solo per le attività che le richiedono.

È possibile utilizzare le policy delle chiavi, le policy IAM e le concessioni per consentire ai principali IAM di gestire e utilizzare le chiavi multi-regione nel Account AWS. Ogni chiave multi-regione è una risorsa indipendente con una chiave univoca ARN e una policy delle chiavi. È necessario stabilire e gestire una policy delle chiavi per ogni chiave e assicurarsi che le policy IAM nuove ed esistenti implementino la strategia di autorizzazione.

Argomenti

- Nozioni di base sull'autorizzazione per le chiavi multi-regione
- Autorizzazione degli amministratori e degli utenti delle chiavi multi-regione
- Autorizzazione di AWS KMS per sincronizzare le chiavi multi-regione

Nozioni di base sull'autorizzazione per le chiavi multi-regione

Quando si progettano policy delle chiavi e policy IAM per chiavi multi-regione, considerare i seguenti principi.

- Policy delle chiavi — Ogni chiave multi-regione è una risorsa della chiave KMS indipendente con la propria Policy delle chiavi. È possibile applicare la stessa policy o una policy delle chiavi diversa a ogni chiave nel set di chiavi multi-regione correlate. Policy delle chiavi non sono proprietà condivise di chiavi multi-regione. AWS KMS non copia o sincronizza le policy delle chiavi tra le chiavi multi-regione correlate.

  Quando si crea una chiave di replica nel AWS KMS, la console visualizza la policy delle chiavi corrente della chiave primaria per comodità. È possibile utilizzare questa policy delle chiavi, modificarla o eliminarla e sostituirla. Ma anche se accetti la policy delle chiavi primaria invariata, AWS KMS non sincronizza le policy. Ad esempio, se si modifica la policy delle chiavi della chiave primaria, la policy delle chiavi della chiave di replica rimane invariato.
- Politica chiave predefinita: quando si creano chiavi multiregionali utilizzando le `ReplicateKey` operazioni CreateKeyand, viene applicata la politica chiave predefinita a meno che non si specifichi una politica chiave nella richiesta. Si tratta della stessa policy delle chiavi predefinita applicata alle chiavi di singola regione.
- Policy IAM — Come per tutte le chiavi KMS, è possibile utilizzare le policy IAM per controllare l'accesso alle chiavi multi-regione solo quando la policy delle chiavi lo consente. Policy IAM applica a tutte le Regioni AWS per impostazione predefinita. Tuttavia, puoi utilizzare chiavi condizionali, come aws: RequestedRegion, per limitare le autorizzazioni a una particolare regione.

Per creare chiavi primarie e di replica, i principali devono disporre di autorizzazione `kms:CreateKey` in una policy IAM che si applica alla regione in cui viene creata la chiave.

- Concessioni — le concessioni AWS KMS sono regionali. Ogni concessione consente autorizzazioni per una chiave KMS. È possibile utilizzare le concessioni per consentire le autorizzazioni a una chiave primaria o a una chiave di replica multi-regione. Tuttavia, non è possibile utilizzare una singola concessione per consentire le autorizzazioni a più chiavi KMS, anche se sono chiavi multi-regione correlate.
- ARN della chiave — Ogni chiave multi-regione ha un ARN della chiave unico. Gli ARN della chiave delle chiavi multi-regione correlate hanno la stessa partizione, account e ID chiave, ma regioni diverse.

  Per applicare un'istruzione delle policy IAM a una determinata chiave multi-regione, utilizza il relativo ARN della chiave o un pattern di ARN della chiave che include la regione. Per applicare un'istruzione di policy IAM a tutte le chiavi multi-regione correlate, utilizza un carattere jolly (*) nell'elemento Regione dell'ARN, come mostrato nell'esempio seguente.

```
{
  "Effect": "Allow",
  "Action": [
    "kms:Describe*",
    "kms:List*"
  ],
  "Resource": {
      "arn:aws:kms:*::111122223333:key/mrk-1234abcd12ab34cd56ef1234567890ab"
  }
}
```

  Per applicare una dichiarazione di policy a tutte le chiavi multiregionali presenti nella tua aziendaAccount AWS, puoi utilizzare la condizione kms: MultiRegion policy o un modello di ID chiave che includa il prefisso distintivo. `mrk-`
- Ruolo collegato ai servizi: i responsabili che creano chiavi primarie multiregionali devono disporre dell'autorizzazione iam:. CreateServiceLinkedRole

  Per sincronizzare le proprietà condivise delle chiavi multi-regione correlate, AWS KMS assume un Ruolo collegato ai servizi IAM. AWS KMS crea il ruolo collegato ai servizi nel Account AWS ogni volta che crei una chiave primaria multi-regione. (Se il ruolo esiste, AWS KMS lo ricrea, cosa che non ha alcun effetto dannoso.) Il ruolo è valido in tutte le Regioni. AWS KMSPer consentire la

creazione (o la ricreazione) del ruolo collegato al servizio, i responsabili che creano chiavi primarie multiregionali devono disporre dell'autorizzazione iam:. CreateServiceLinkedRole

Autorizzazione degli amministratori e degli utenti delle chiavi multi-regione

I principali che creano e gestiscono chiavi multi-regione necessitano delle seguenti autorizzazioni nelle regioni primarie e di replica:

- `kms:CreateKey`
- `kms:ReplicateKey`
- `kms:UpdatePrimaryRegion`
- `iam:CreateServiceLinkedRole`

Creazione di una chiave primaria

Per creare una chiave primaria multiregionale, il principale necessita delle CreateServiceLinkedRole autorizzazioni kms: CreateKey e iam: in una policy IAM efficace nella regione della chiave primaria. I principali che dispongono di queste autorizzazioni possono creare chiavi di regione singola e multi-regione a meno che non si limitino le autorizzazioni.

L'`iam:CreateServiceLinkedRole`autorizzazione consente di AWS KMS creare il AWSServiceRoleForKeyManagementServiceMultiRegionKeysruolo per sincronizzare le proprietà condivise delle relative chiavi multiregionali.

Ad esempio, questa policy IAM consente a un principale di creare qualsiasi tipo di chiave KMS.

```
{
  "Version": "2012-10-17",
  "Statement":{
      "Action": [
        "kms:CreateKey",
        "iam:CreateServiceLinkedRole"
      ],
      "Effect":"Allow",
      "Resource":"*"
  }
}
```

Per consentire o negare l'autorizzazione alla creazione di chiavi primarie multiregionali, usa la chiave kms: condition. MultiRegion I valori validi sono `true` (Chiave multi-regione) o `false` (Chiave di singola regione). Ad esempio, la seguente istruzione di policy IAM utilizza un'operazione `Deny` con la chiave di condizione `kms:MultiRegion` per impedire ai principali di creare chiavi multi-regione.

```
{
  "Version": "2012-10-17",
  "Statement":{
      "Action":"kms:CreateKey",
      "Effect":"Deny",
      "Resource":"*",
      "Condition": {
          "Bool": "kms:MultiRegion": true
      }
  }
}
```

Replica delle chiavi

Per creare una chiave di replica multi-regione, il principale richiede le seguenti autorizzazioni:

- kms: ReplicateKey autorizzazione nella politica chiave della chiave primaria.
- kms: CreateKey autorizzazione in una politica IAM efficace nella regione della chiave di replica.

Presta attenzione quando consenti queste autorizzazioni. Consentono ai principali di creare chiavi KMS e le policy delle chiavi che ne autorizzano l'utilizzo. L'autorizzazione `kms:ReplicateKey` autorizza inoltre il trasferimento di materiale chiave oltre i confini della regione all'interno di AWS KMS.

Per limitare il numero Regioni AWS di repliche di una chiave multiregionale, usa la chiave kms: condition. ReplicaRegion Limita solo l'autorizzazione `kms:ReplicateKey`. Altrimenti, non ha efficacia. Ad esempio, la seguente policy delle chiavi consente al principale di replicare questa chiave primaria, ma solo nelle regioni specificate.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/Administrator"
  },
  "Action": "kms:ReplicateKey",
```

```
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ReplicaRegion": [
         "us-east-1",
         "eu-west-3",
         "ap-southeast-2"
      ]
    }
  }
}
```

Aggiornamento della regione primaria

I principali autorizzati possono convertire una chiave di replica in una chiave primaria, modificando la chiave primaria precedente in una replica. Questa azione è nota come aggiornamento della regione primaria. Per aggiornare la regione principale, la principale necessita dell'UpdatePrimaryRegionautorizzazione kms: in entrambe le regioni. Puoi fornire queste autorizzazioni in una policy delle chiavi o in una policy IAM.

- `kms:UpdatePrimaryRegion` sulla chiave primaria. Questa autorizzazione deve essere valida nella regione chiave primaria.
- `kms:UpdatePrimaryRegion` sulla chiave di replica. Questa autorizzazione deve essere valida nella regione chiave di replica.

Ad esempio, la seguente policy delle chiavi consente agli utenti che possono assumere il ruolo di Amministratore di aggiornare la regione primaria della chiave KMS. Questa chiave KMS può essere la chiave primaria o una chiave di replica in questa operazione.

```
{
  "Effect": "Allow",
  "Resource": "*",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/Administrator"
  },
  "Action": "kms:UpdatePrimaryRegion"
}
```

Per limitare la Regioni AWS capacità di ospitare una chiave primaria, usa la chiave kms: PrimaryRegion condition. Ad esempio, la seguente istruzione della policy IAM consente ai principali di

aggiornare la regione primaria delle chiavi multi-regione nel Account AWS, ma solo quando la nuova regione primaria è una delle regioni specificate.

```
{
  "Effect": "Allow",
  "Action": "kms:UpdatePrimaryRegion",
  "Resource": {
      "arn:aws:kms:*:111122223333:key/*"
  },
  "Condition": {
    "StringEquals": {
      "kms:PrimaryRegion": [
         "us-west-2",
         "sa-east-1",
         "ap-southeast-1"
      ]
    }
  }
}
```

Utilizzo e gestione di chiavi multi-regione

Per impostazione predefinita, i principali che dispongono dell'autorizzazione per utilizzare e gestire le chiavi KMS in un Account AWS e Regione hanno anche l'autorizzazione per utilizzare e gestire chiavi multi-regione. Tuttavia, puoi utilizzare la chiave kms: MultiRegion condition per consentire solo chiavi a regione singola o solo chiavi multiregione. Oppure usa la chiave kms: MultiRegionKeyType condition per consentire solo chiavi primarie multiregionali o solo chiavi di replica. Entrambi i tasti condizionali controllano l'accesso all'CreateKeyoperazione e a qualsiasi operazione che utilizza una chiave KMS esistente, come Encrypt o. EnableKey

La seguente istruzione di policy IAM utilizza la chiave di condizione `kms:MultiRegion` per impedire ai principali di utilizzare o gestire qualsiasi chiave multi-regione.

```
{
  "Effect": "Deny",
  "Action": "kms:*",
  "Resource": "*",
  "Condition": {
    "Bool": "kms:MultiRegion": true
  }
}
```

In questo esempio, l'istruzione di policy IAM utilizza la condzione `kms:MultiRegionKeyType` per consentire ai principali di pianificare e annullare l'eliminazione delle chiavi, ma solo sulle chiavi di replica multi-regione.

```
{
  "Effect": "Allow",
  "Action": [
    "kms:ScheduleKeyDeletion",
    "kms:CancelKeyDeletion"
  ],
  "Resource": {
      "arn:aws:kms:us-west-2:111122223333:key/*"
  },
  "Condition": {
    "StringEquals": "kms:MultiRegionKeyType": "REPLICA"
  }
}
```

Autorizzazione di AWS KMS per sincronizzare le chiavi multi-regione

Per supportare Chiavi multi-regione, AWS KMS utilizza un ruolo collegato al servizio IAM. Questo ruolo dà a AWS KMS i permessi necessari per sincronizzare le proprietà condivise. È possibile visualizzare l'SynchronizeMultiRegionKey CloudTrail evento che registra la AWS KMS sincronizzazione delle proprietà condivise nei registri. AWS CloudTrail

Informazioni sul ruolo collegato ai servizi per le chiavi multi-regione

Un ruolo collegato ai servizi è un ruolo IAM che concede a un servizio AWS l'autorizzazione per chiamare altri servizi AWS a tuo nome. È concepito per facilitare l'utilizzo delle funzionalità di molteplici servizi AWS integrati senza la necessità di creare e gestire policy IAM complesse.

Per le chiavi multiregionali, AWS KMS crea il ruolo AWSServiceRoleForKeyManagementServiceMultiRegionKeyscollegato al servizio con la policy. AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy Questa policy dà al ruolo l'autorizzazione `kms:SynchronizeMultiRegionKey`, che consente di sincronizzare le proprietà condivise delle chiavi multi-regione.

Poiché solo il ruolo AWSServiceRoleForKeyManagementServiceMultiRegionKeyscollegato al servizio è affidabile`mrk.kms.amazonaws.com`, solo AWS KMS può assumere questo ruolo collegato al servizio. Questo ruolo è limitato alle operazioni che AWS KMS deve sincronizzare le proprietà

condivise in più regioni. Non fornisce a AWS KMS autorizzazioni aggiuntive. Ad esempio, AWS KMS non dispone dell'autorizzazione per creare, replicare o eliminare chiavi KMS.

Per ulteriori informazioni su come i servizi AWS utilizzano ruoli collegati ai servizi, consulta la pagina Uso di ruoli collegati ai servizi nella Guida per l'utente di IAM.

Creazione del ruolo collegato ai servizi

AWS KMScrea automaticamente il ruolo AWSServiceRoleForKeyManagementServiceMultiRegionKeyscollegato al servizio nel tuo Account AWS quando crei una chiave multiregionale, se il ruolo non esiste già. Non è possibile creare o ricreare direttamente questo ruolo collegato ai servizi.

Modifica della descrizione di un ruolo collegato ai servizi

Non è possibile modificare il nome del ruolo o le dichiarazioni politiche nel ruolo AWSServiceRoleForKeyManagementServiceMultiRegionKeyscollegato al servizio, ma è possibile modificare la descrizione del ruolo. Per istruzioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione del ruolo collegato ai servizi

AWS KMSnon elimina il ruolo AWSServiceRoleForKeyManagementServiceMultiRegionKeyscollegato al servizio dal tuo Account AWS e non puoi eliminarlo. Tuttavia, AWS KMS non assume il AWSServiceRoleForKeyManagementServiceMultiRegionKeysruolo né utilizza alcuna delle sue autorizzazioni a meno che non si disponga di chiavi multiregionali nella propria regione. Account AWS

Creazione di chiavi multiregione

È possibile creare chiavi multiregione nella console o tramite l'API AWS KMS.

La proprietà multi-Regione impostata con questa procedura è immutabile. Non è possibile convertire una chiave a Regione singola in chiave multi-Regione o convertire una chiave multi-Regione in una chiave a Regione singola.

Argomenti

- Creazione di chiavi primarie multiregione
- Creazione di chiavi di replica multiregione

Creazione di chiavi primarie multiregione

È possibile creare chiavi primarie multiregione nella console AWS KMS o tramite l'API AWS KMS. È possibile creare la chiave primaria in qualsiasi Regione AWS dove AWS KMS supporta le chiavi multiregione.

Per creare una chiave primaria multiregionale, il principale necessita delle stesse autorizzazioni di cui ha bisogno per creare qualsiasi chiave KMS, inclusa l'CreateKeyautorizzazione kms: in una policy IAM. Il preside necessita anche dell'autorizzazione iam:. CreateServiceLinkedRole Puoi usare la chiave kms: MultiRegionKeyType condition per consentire o negare l'autorizzazione alla creazione di chiavi primarie multiregionali.

Queste istruzioni creano una chiave primaria multiregione con materiale chiave generato da AWS KMS. Per creare una chiave primaria multiregione con materiale chiave importato, consulta Creazione di una chiave primaria con materiale chiave importato.

Argomenti

- Creazione di chiavi primarie multiregione (console)
- Creazione di chiavi primarie multiregione (API AWS KMS)

Creazione di chiavi primarie multiregione (console)

Per creare una chiave primaria multiregione nella console AWS KMS, utilizza la stessa procedura che utilizzeresti per creare qualsiasi chiave KMS. Seleziona una chiave multiregione in Opzioni avanzate. Per istruzioni complete, consulta Creazione di chiavi.

> **Important**
>
> Non includere informazioni riservate o sensibili nell'alias, nella descrizione o nei tag. Questi campi possono apparire in testo semplice nei CloudTrail log e in altri output.

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.
4. Scegliere Create key (Crea chiave).

5. Selezionare un tipo di chiave simmetrico o asimmetrico. Le chiavi simmetriche sono le chiavi di default.

   È possibile creare chiavi simmetriche e asimmetriche multi-regione, incluse le chiavi KMS HMAC multi-regione, che sono simmetriche.

6. Seleziona l'utilizzo della chiave. Encrypt and decrypt (Crittografa e decrittografa) è l'utilizzo di default.

   Per assistenza, consulta le sezioni the section called “Creazione di chiavi”, the section called “Creazione di chiavi KMS asimmetriche” o the section called “Creazione di chiavi HMAC”.

7. Espandere Advanced options (Opzioni avanzate).

8. Alla voce Origine del materiale chiave, per far sì che AWS KMS generi il materiale chiave che le chiavi primarie e di replica condivideranno, scegli KMS. Se importi il materiale della chiave nelle chiavi primarie e di replica, scegli External (Import key material) (Esterna (Importa materiale della chiave)).

9. Alla voce Replica multiregione, scegli Consenti la replica di questa chiave in altre Regioni.

   Non è possibile modificare questa impostazione dopo aver creato la chiave KMS.

10. Digita un alias per la chiave primaria.

    Gli alias non sono una proprietà condivisa delle chiavi multiregione. È possibile assegnare alla chiave primaria multiregione e alle relative repliche gli stessi alias o alias diversi. AWS KMS non sincronizza gli alias delle chiavi multiregione.

    > **Note**
    >
    > L'aggiunta, l'eliminazione o l'aggiornamento di un alias può consentire o negare l'autorizzazione alla chiave KMS. Per informazioni dettagliate, consulta ABAC per AWS KMS e Utilizzo degli alias per controllare l'accesso alle chiavi KMS.

11. (Facoltativo) Digita una descrizione della chiave primaria.

    Le descrizioni non sono una proprietà condivisa delle chiavi multiregione. È possibile assegnare alla chiave primaria multiregione e alle relative repliche le stesse descrizioni o descrizioni diverse. AWS KMS non sincronizza le descrizioni delle chiavi multiregione.

12. (Facoltativo) Digitare una tag di chiave e un valore di tag facoltativo. Per assegnare più di un tag alla chiave primaria, scegli Aggiungi tag.

I tag non sono una proprietà condivisa delle chiavi multiregione. È possibile assegnare alla chiave primaria multiregione e alle relative repliche gli stessi tag o tag diversi. AWS KMS non sincronizza i tag delle chiavi multiregione. Puoi modificare i tag nelle chiaviKMS in qualsiasi momento.

> **Note**
>
> L'applicazione o l'eliminazione di un tag chiave KMS può consentire o negare l'autorizzazione alla chiave KMS. Per informazioni dettagliate, consulta ABAC per AWS KMS e Utilizzo dei tag per controllare l'accesso alle chiavi KMS.

13. Seleziona i ruoli e gli utenti IAM che possono gestire la chiave primaria.

> **Note**
>
> Le policy IAM possono fornire ad altri ruoli e utenti IAM l'autorizzazione per gestire la chiave KMS.
> Le best practice di IAM disincentivano l'uso di utenti IAM con credenziali a lungo termine. Quando possibile, utilizza i ruoli IAM che forniscono credenziali temporanee. Per i dettagli, consulta la sezione Best practice di sicurezza in IAM nella Guida per l'utente IAM.

Questo passaggio avvia il processo di creazione di una policy chiave per la chiave primaria. Le policy chiave non sono una proprietà condivisa delle chiavi multiregione. È possibile assegnare alla chiave primaria multiregione e alle relative repliche le stesse policy chiave o policy chiave diverse. AWS KMS non sincronizza le policy chiave delle chiavi multiregione. È possibile modificare la policy chiave di una chiave KMS in qualsiasi momento.

14. Completa la procedura per la creazione della policy delle chiavi, inclusa la selezione degli utenti della chiave. Dopo aver revisionato la policy chiave, seleziona Fine per creare la chiave KMS.

Creazione di chiavi primarie multiregione (API AWS KMS)

Per creare una chiave primaria multiregionale, utilizzare l'CreateKeyoperazione. Usa il parametro `MultiRegion` con valore `True`.

Ad esempio, il seguente comando crea una chiave primaria multiregione nellaRegione AWS del chiamante (us-east-1). Accetta valori predefiniti per tutte le altre proprietà, inclusa la policy chiave. I valori predefiniti per le chiavi primarie multiregione sono gli stessi dei valori predefiniti per tutte le altre chiavi KMS, inclusa la proprietà policy chiave predefinita. Questa procedura crea una chiave di crittografia simmetrica, la chiave KMS di default.

La risposta include l'elemento `MultiRegion` e l'elemento `MultiRegionConfiguration` con sottoelementi e valori tipici per una chiave primaria multiregione senza chiavi di replica. L'ID chiave di una chiave multiregione inizia sempre con `mrk-`.

> **Important**
>
> Non includere informazioni riservate o sensibili nei campi `Description` o `Tags`. Questi campi possono apparire in testo semplice nei CloudTrail log e in altri output.

```
$ aws kms create-key --multi-region
{
    "KeyMetadata": {
        "Origin": "AWS_KMS",
        "KeyId": "mrk-1234abcd12ab34cd56ef1234567890ab",
        "Description": "",
        "KeyManager": "CUSTOMER",
        "Enabled": true,
        "KeySpec": "SYMMETRIC_DEFAULT",
        "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "KeyState": "Enabled",
        "CreationDate": 1606329032.475,
        "Arn": "arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
        "AWSAccountId": "111122223333",
        "EncryptionAlgorithms": [
            "SYMMETRIC_DEFAULT"
        ],
        "MultiRegion": true,
        "MultiRegionConfiguration": {
            "MultiRegionKeyType": "PRIMARY",
            "PrimaryKey": {
                "Arn": "arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
```

```
                "Region": "us-east-1"
            },
            "ReplicaKeys": [ ]
        }
    }
}
```

Creazione di chiavi di replica multiregione

È possibile creare una chiave di replica multiarea nella AWS KMS console, utilizzando l'ReplicateKeyoperazione o utilizzando un AWS CloudFormation modello. Non è possibile utilizzare l'CreateKeyoperazione per creare una chiave di replica.

È possibile utilizzare queste procedure per replicare qualsiasi chiave primaria multi-regione, incluse le chiavi KMS di crittografia simmetrica, le chiavi KMS asimmetriche e le chiavi KMS HMAC.

Al termine di questa operazione, la nuova chiave di replica presenta uno stato chiave `Creating`. Questo stato della chiave cambia in `Enabled` (o PendingImport) dopo alcuni secondi al termine del processo di creazione della nuova chiave di replica. Quando lo stato della chiave è `Creating`, puoi visualizzare e gestire la chiave, ma non utilizzarla per operazioni di crittografia. Se state creando e utilizzando la chiave di replica a livello di codice, riprovate `KMSInvalidStateException` o richiamate DescribeKeyper verificarne `KeyState` il valore prima di utilizzarla.

Se si elimina accidentalmente una chiave di replica, è possibile utilizzare questa procedura per ricrearla. Se si replica la stessa chiave primaria nella stessa regione, la nuova chiave di replica creata avrà le stesse proprietà condivise della chiave di replica originale.

> **Important**
>
> Non includere informazioni riservate o sensibili nell'alias, nella descrizione o nei tag. Questi campi possono apparire in testo semplice nei CloudTrail log e in altri output.

Ulteriori informazioni

- Per creare una chiave di replica multiregione con materiale chiave importato, consulta Creazione di una chiave di replica con materiale chiave importato.
- Per utilizzare un AWS CloudFormation modello per creare una chiave di replica, consulta AWS::KMS::ReplicaKeyla Guida per l'AWS CloudFormationutente.

Argomenti

- Regioni di replica
- Creazione di chiavi di replica (console)
- Creazione di una chiave di replica (API AWS KMS)

Regioni di replica

In genere, scegli di replicare una chiave multiregione in una Regione AWS in base al tuo modello di business e ai requisiti normativi. Ad esempio, puoi replicare una chiave nelle Regioni in cui conservi le tue risorse. In alternativa, per soddisfare i requisiti di ripristino di emergenza, è possibile replicare una chiave in Regioni geograficamente distanti.

Di seguito sono riportati i requisiti AWS KMS per le Regioni di replica. Se la Regione scelta non è conforme a questi requisiti, i tentativi di replicare una chiave hanno esito negativo.

- Una chiave multiregione correlata per Regione: non è possibile creare una chiave di replica nella stessa Regione della chiave primaria o nella stessa Regione di un'altra replica della chiave primaria.

  Se si prova a replicare una chiave primaria in una regione che ha già una replica di quella chiave primaria, il tentativo avrà esito negativo. Se la chiave di replica corrente nella regione si trova nello stato delle chiavi `PendingDeletion`, è possibile annullare l'eliminazione della chiave di replica oppure attendere fino a quando la chiave di replica non viene eliminata.
- Più chiavi multiregione non correlate nella stessa Regione — È possibile avere più chiavi multiregione non correlate nella stessa Regione. Ad esempio, è possibile avere due chiavi primarie multiregione nella Regione `us-east-1`. Ciascuna delle chiavi primarie può avere una chiave di replica nella Regione `us-west-2`.
- Regioni nella stessa partizione — La Regione della chiave di replica deve trovarsi nella stessa partizione AWS della Regione della chiave primaria.
- La Regione deve essere abilitata — Se una regione è disabilitata per impostazione predefinita, non è possibile creare alcuna risorsa in tale Regione finché non viene abilitata per il tuo Account AWS.

Creazione di chiavi di replica (console)

Nella console AWS KMS, è possibile creare una o più repliche di una chiave primaria multiregione nella stessa operazione.

Questa procedura è simile alla creazione di una chiave KMS standard per singola Regione nella console. Tuttavia, poiché una chiave di replica è basata sulla chiave primaria, non è possibile selezionare i valori per le proprietà condivise, ad esempio la specifica della chiave (simmetrica o asimmetrica), l'utilizzo della chiave o l'origine della chiave.

È possibile specificare proprietà non condivise, tra cui un alias, tag, una descrizione e una policy chiave. Per comodità, la console visualizza i valori delle proprietà correnti della chiave primaria, ma è possibile modificarli. Anche se si mantengono i valori della chiave primaria, AWS KMS non mantiene questi valori sincronizzati.

> **Important**
>
> Non includere informazioni riservate o sensibili nell'alias, nella descrizione o nei tag. Questi campi possono apparire in testo semplice nei CloudTrail log e in altri output.

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.
4. Seleziona l'alias o l'ID chiave di una chiave primaria multiregione. In questo modo si apre la pagina dei dettagli delle chiavi per la chiave KMS.

   Per identificare una chiave primaria multiregione, utilizza l'icona dello strumento nell'angolo in alto a destra per aggiungere la colonna Regionalità nella tabella.
5. Seleziona la tab Regionalità.
6. Nella sezione Chiavi multiregione correlate, scegli Crea nuove chiavi di replica.

   Le chiavi multiregione correlate mostrano la Regione della chiave primaria e le relative chiavi di replica. È possibile utilizzare questa visualizzazione per scegliere la Regione per la nuova chiave di replica.
7. Scegli una o più Regioni AWS. Questa procedura crea una chiave di replica in ciascuna delle Regioni selezionate.

   Il menu include solo le Regioni nella stessa partizione AWS della chiave primaria. Le Regioni che dispongono già di una chiave multiregione correlata vengono visualizzate, ma non sono

selezionabili. È possibile che non si disponga dell'autorizzazione per replicare una chiave in tutte le Regioni del menu.

Quando hai finito di scegliere Regioni, chiudi il menu. Vengono visualizzate le Regioni selezionate. Per annullare la replica in una Regione, scegli la casella di controllo X accanto al nome della Regione.

8. Digita un alias per la chiave di replica.

   La console visualizza uno degli alias correnti della chiave primaria, ma è possibile modificarlo. È possibile assegnare alla chiave primaria multiregione e alle relative repliche gli stessi alias o alias diversi. Gli alias non sono una proprietà condivisa delle chiavi multiregione. AWS KMS non sincronizza gli alias delle chiavi multiegione.

   L'aggiunta, l'eliminazione o l'aggiornamento di un alias può consentire o negare l'autorizzazione alla chiave KMS. Per informazioni dettagliate, consulta ABAC per AWS KMS e Utilizzo degli alias per controllare l'accesso alle chiavi KMS.

9. (Facoltativo) Digita una descrizione della chiave di replica.

   La console visualizza la descrizione corrente della chiave primaria, ma è possibile modificarla. Le descrizioni non sono una proprietà condivisa delle chiavi multiregione. È possibile assegnare alla chiave primaria multiregione e alle relative repliche le stesse descrizioni o descrizioni diverse. AWS KMS non sincronizza le descrizioni delle chiavi multiregione.

10. (Facoltativo) Digitare una tag di chiave e un valore di tag facoltativo. Per assegnare più di un tag alla chiave di replica, scegli Aggiungi tag.

    Nella console vengono visualizzati i tag attualmente collegati alla chiave primaria, ma è possibile modificarli. I tag non sono una proprietà condivisa delle chiavi multiregione. È possibile assegnare alla chiave primaria multiregione e alle relative repliche gli stessi tag o tag diversi. AWS KMS non sincronizza i tag delle chiavi multiregione.

    L'applicazione o l'eliminazione di un tag chiave KMS può consentire o negare l'autorizzazione alla chiave KMS. Per informazioni dettagliate, consulta ABAC per AWS KMS e Utilizzo dei tag per controllare l'accesso alle chiavi KMS.

11. Seleziona i ruoli e gli utenti IAM che possono gestire la chiave di replica.

> **Note**
>
> Le policy IAM possono fornire ad altri ruoli e utenti IAM l'autorizzazione per utilizzare le chiavi di replica.
> Le best practice di IAM disincentivano l'uso di utenti IAM con credenziali a lungo termine. Quando possibile, utilizza i ruoli IAM che forniscono credenziali temporanee. Per i dettagli, consulta la sezione Best practice di sicurezza in IAM nella Guida per l'utente IAM.

Questo passaggio avvia il processo di creazione di una policy chiave per la chiave di replica. Nella console vengono visualizzate le policy chiave correnti della chiave primaria, ma è possibile modificarle. Le policy chiave non sono una proprietà condivisa delle chiavi multiregione.
È possibile assegnare alla chiave primaria multiregione e alle relative repliche le stesse policy chiave o policy chiave diverse. AWS KMS non sincronizza le policy chiave. È possibile modificare la policy chiave delle chiavi KMS in qualsiasi momento.

12. Completa la procedura per la creazione della policy delle chiavi, inclusa la selezione degli utenti della chiave. Dopo aver revisionato la policy chiavi, seleziona Fine per creare la chiave di replica.

Creazione di una chiave di replica (API AWS KMS)

Per creare una chiave di replica multiregionale, utilizzare l'operazione. ReplicateKey Non è possibile utilizzare l'CreateKeyoperazione per creare una chiave di replica. Questa operazione crea una chiave di replica per volta. La regione specificata deve essere conforme ai Requisiti per le Regioni per le chiavi di replica.

Quando si utilizza l'operazione `ReplicateKey`, non specificare valori per le proprietà condivise delle chiavi multiregione. I valori delle proprietà condivise vengono copiati dalla chiave primaria e mantenuti sincronizzati. Tuttavia, è possibile specificare valori per proprietà non condivise. In caso contrario, AWS KMS applica i valori predefiniti standard per le chiavi KMS, non i valori della chiave primaria.

> **Note**
>
> Se non specifichi valori per i parametri `Description`, `KeyPolicy` o `Tags`, AWS KMS crea la chiave di replica senza tag, con una descrizione costituita da una stringa vuota, la policy della chiave predefinita, senza tag.

> Non includere informazioni riservate o sensibili nei campi `Description` o `Tags`. Questi campi possono apparire in testo semplice nei CloudTrail log e in altri output.

Ad esempio, il seguente comando crea una chiave di replica multiregione nella Regione Asia Pacifico (Sydney) (ap-southeast-2). Questa chiave di replica è modellata sulla chiave primaria nella Regione Stati Uniti orientali (Virginia settentrionale) (us-east-1), identificata dal valore del parametro `KeyId`. Questo esempio accetta valori predefiniti per tutte le altre proprietà, inclusa la policy chiave.

La risposta descrive la nuova chiave di replica. Include i campi per le proprietà condivise, ad esempio `KeyId`, `KeySpec`, `KeyUsage` e l'origine del materiale chiave (`Origin`). Include anche proprietà indipendenti dalla chiave primaria, come la `Description`, la policy chiave (`ReplicaKeyPolicy`), e i tag (`ReplicaTags`).

La risposta include anche l'ARN chiave e la Regione della chiave primaria e tutte le relative chiavi di replica, inclusa quella appena creata nella Regione ap-southeast-2. In questo esempio, l'elemento `ReplicaKey` mostra che questa chiave primaria è già stata replicata nella Regione Europa (Irlanda) (eu-west-1).

```
$ aws kms replicate-key \
    --key-id arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab \
    --replica-region ap-southeast-2
{
    "ReplicaKeyMetadata": {
        "MultiRegion": true,
        "MultiRegionConfiguration": {
            "MultiRegionKeyType": "REPLICA",
            "PrimaryKey": {
                "Arn": "arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
                "Region": "us-east-1"
            },
            "ReplicaKeys": [
                {
                    "Arn": "arn:aws:kms:ap-southeast-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
                    "Region": "ap-southeast-2"
                },
                {
```

```
                    "Arn": "arn:aws:kms:eu-west-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
                    "Region": "eu-west-1"
                }
            ]
        },
        "AWSAccountId": "111122223333",
        "Arn": "arn:aws:kms:ap-southeast-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
        "CreationDate": 1607472987.918,
        "Description": "",
        "Enabled": true,
        "KeyId": "mrk-1234abcd12ab34cd56ef1234567890ab",
        "KeyManager": "CUSTOMER",
        "KeySpec": "SYMMETRIC_DEFAULT",
        "KeyState": "Enabled",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "Origin": "AWS_KMS",
        "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "EncryptionAlgorithms": [
            "SYMMETRIC_DEFAULT"
        ]
    },
    "ReplicaKeyPolicy": "{\n  \"Version\" : \"2012-10-17\",\n  \"Id\" : \"key-
default-1\",...,
    "ReplicaTags": []
}
```


Visualizzazione di chiavi multiregione

Puoi visualizzare le chiavi a Regione singola e multiregione nella console AWS KMS e con le operazioni dell'API AWS KMS.

Argomenti

- Visualizzazione di chiavi multiregione nella console
- Visualizzazione di chiavi multiregione nell'API

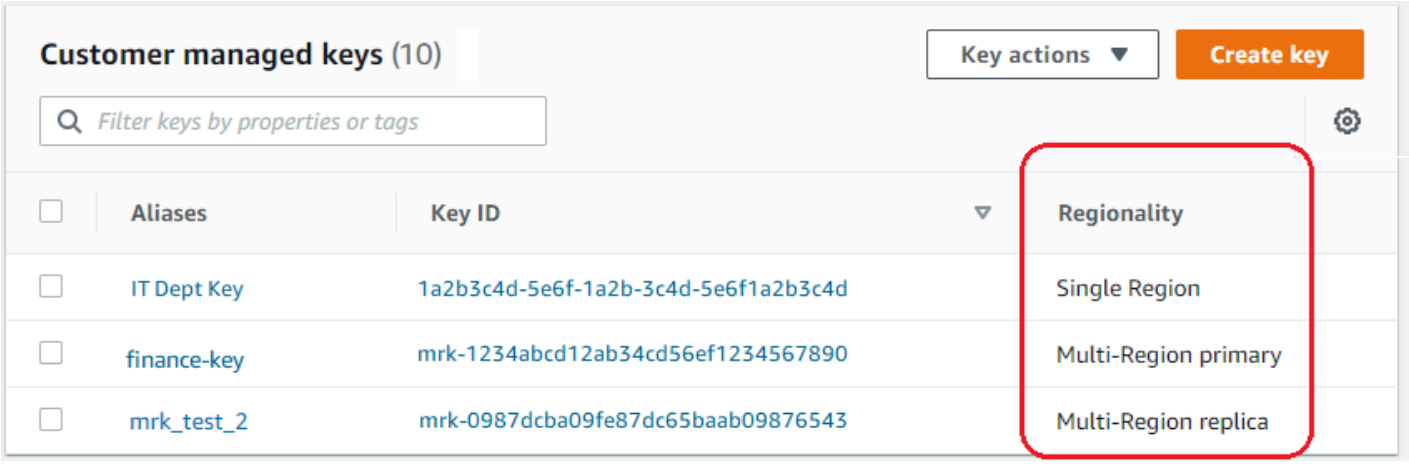
Visualizzazione di chiavi multiregione nella console

Nella console AWS KMS, puoi visualizzare le chiavi KMS nella Regione selezionata. Tuttavia, se disponi di una chiave multiregione, puoi visualizzare le relative chiavi multiregione in altre Regioni AWS.

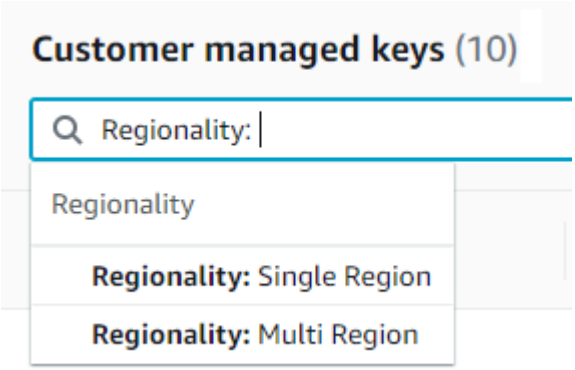
La tabella Chiave gestite dal cliente nella console AWS KMS visualizza solo le chiavi KMS nella Regione selezionata. È possibile visualizzare le chiavi primarie e di replica multiregione nella Regione selezionata. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.

La tabella Chiavi gestite da AWS non ha le funzioni di regionalità perché Chiavi gestite da AWS sono sempre chiavi di Regione singola.

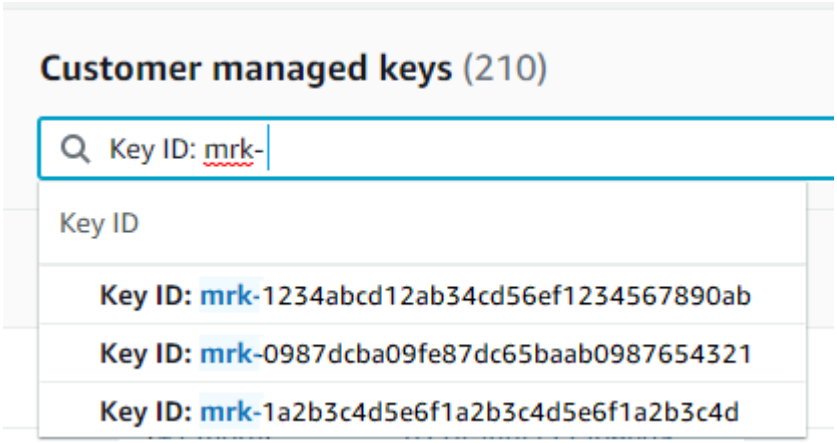
- Per semplificare l'identificazione delle chiavi multiregione, aggiungi la colonna Regionalità nella tabella delle chiavi. Per assistenza, consulta Personalizzazione delle tabelle delle chiavi KMS.



- Per visualizzare solo le chiavi di Regione singola o solo le chiavi multiregione nella tabella chiave, filtra le chiavi in base alla proprietà Regionalità di ogni chiave. Per assistenza, consulta Ordinamento e filtraggio delle tue chiavi KMS.



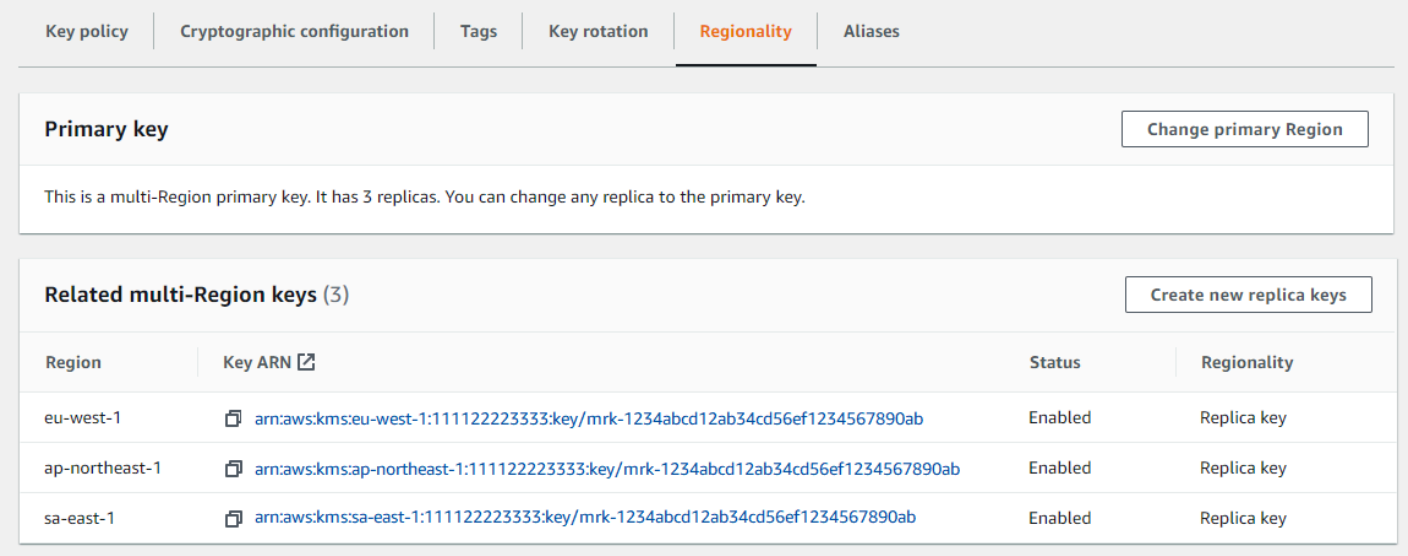
- È inoltre possibile ordinare e filtrare la tabella Chiavi gestite dal cliente per il prefisso distintivo dell'ID chiave Mrk-.



- Per informazioni dettagliate su una chiave primaria o una chiave replica multiregione, vai alla pagina dei dettagli per la chiave e scegli la tab Regionalità.

  La tab Regionalità per una chiave primaria include i pulsanti Modifica Regione primaria e Crea nuove chiavi di replica. (La tab Regionalità per una chiave di replica non dispone di alcun pulsante.) La sezione Chiavi multiregione correlate elenca tutte le chiavi multiregione correlate a quella corrente. Se la chiave corrente è una chiave di replica, l'elenco include la chiave primaria.

  Se si sceglie una chiave multiregione correlata dalla tabella Chiavi multiregione correlate, la console AWS KMS passa alla Regione della chiave selezionata e apre la pagina dei dettagli della chiave. Ad esempio, se scegli la chiave di replica nella Regione `sa-east-1` dalla sezione di esempio Chiavi multiregione correlate qui sotto, la console AWS KMS passa alla Regione `sa-east-1` per mostrare la pagina dei dettagli della chiave di replica. È possibile eseguire questa operazione per visualizzare l'alias o la policy chiave per la chiave di replica. Per modificare di nuovo la Regione, utilizza il selettore Regione nell'angolo in alto a destra della pagina.



Visualizzazione di chiavi multiregione nell'API

Per visualizzare le chiavi multiregionali nell'AWS KMSAPI, utilizza l'DescribeKeyoperazione. Visualizza la chiave specificata e tutte le relative chiavi multiregione.

Come per la console AWS KMS, le operazioni dell'API AWS KMS sono regionali. Ad esempio, quando si chiamano ListAliasesle operazioni ListKeyso, queste restituiscono solo le risorse nella regione corrente o specificata. Ma, quando chiami l'operazione `DescribeKey` su una chiave multiregione, la risposta include tutte le chiavi multiregione correlate in altre Regioni AWS.

Ad esempio, la seguente richiesta `DescribeKey` ottiene dettagli su una chiave replica multiregione nella Regione Asia Pacifico (Tokyo) (`ap-northeast-1`).

```
$ aws kms describe-key \
        --key-id arn:aws:kms:ap-northeast-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab \
        --region ap-northeast-1
```

La maggior parte dei `KeyMetadata` nella risposta descrive la chiave di replica nella Regione Asia Pacifico (Tokyo) oggetto della richiesta. Tuttavia, l'elemento `MultiRegionConfiguration` descrive la chiave primaria nella Regione Stati Uniti occidentali (Oregon) (us-west-2) e le relative chiavi di replica in altre Regioni AWS, inclusa la replica nella Regione Asia Pacifico (Tokyo). `DescribeKey` restituisce lo stesso valore `MultiRegionConfiguration` per tutte le chiavi multiregione correlate.

```
{
    "KeyMetadata": {
        "MultiRegion": true,
        "AWSAccountId": "111122223333",
        "Arn": "arn:aws:kms:ap-northeast-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
        "CreationDate": 1586329200.918,
        "Description": "",
        "Enabled": true,
        "KeyId": "mrk-1234abcd12ab34cd56ef1234567890ab",
        "KeyManager": "CUSTOMER",
        "KeyState": "Enabled",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "Origin": "AWS_KMS",
        "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "EncryptionAlgorithms": [
            "SYMMETRIC_DEFAULT"
        ],
        "MultiRegionConfiguration": {
            "MultiRegionKeyType": "PRIMARY",
            "PrimaryKey": {
                "Arn": "arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
                "Region": "us-west-2"
            },
            "ReplicaKeys": [
                {
                    "Arn": "arn:aws:kms:eu-west-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
                    "Region": "eu-west-1"
                },
                {
                    "Arn": "arn:aws:kms:ap-northeast-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
                    "Region": "ap-northeast-1"
                },
                {
                    "Arn": "arn:aws:kms:sa-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
                    "Region": "sa-east-1"
                }
            ]
        }
```

```
    }
}
```

Gestione delle chiavi multiregione

Per la maggior parte delle azioni, gestisci le chiavi multiregione nello stesso modo in cui utilizzi e gestisci le chiavi in una singola Regione. È possibile abilitare e disabilitare le chiavi, impostare e aggiornare alias, policy chiave, concessioni e tag. Tuttavia, la gestione delle chiavi multiregione differisce nei seguenti modi.

- È possibile aggiornare la Regione principale. In questo modo una delle chiavi di replica viene modificata in una chiave primaria e la chiave primaria corrente in una replica.
- Gestisci la rotazione automatica delle chiavi solo sulla chiave primaria.
- Puoi ottenere la chiave pubblica per una chiave asimmetrica multiregione da una qualsiasi delle chiavi primarie o di replica correlate.

La proprietà multi-Regione impostata al momento della creazione di una chiave KMS è immutabile. Non è possibile convertire una chiave a Regione singola in chiave multi-Regione o convertire una chiave multi-Regione in una chiave a Regione singola.

Aggiornamento della Regione principale

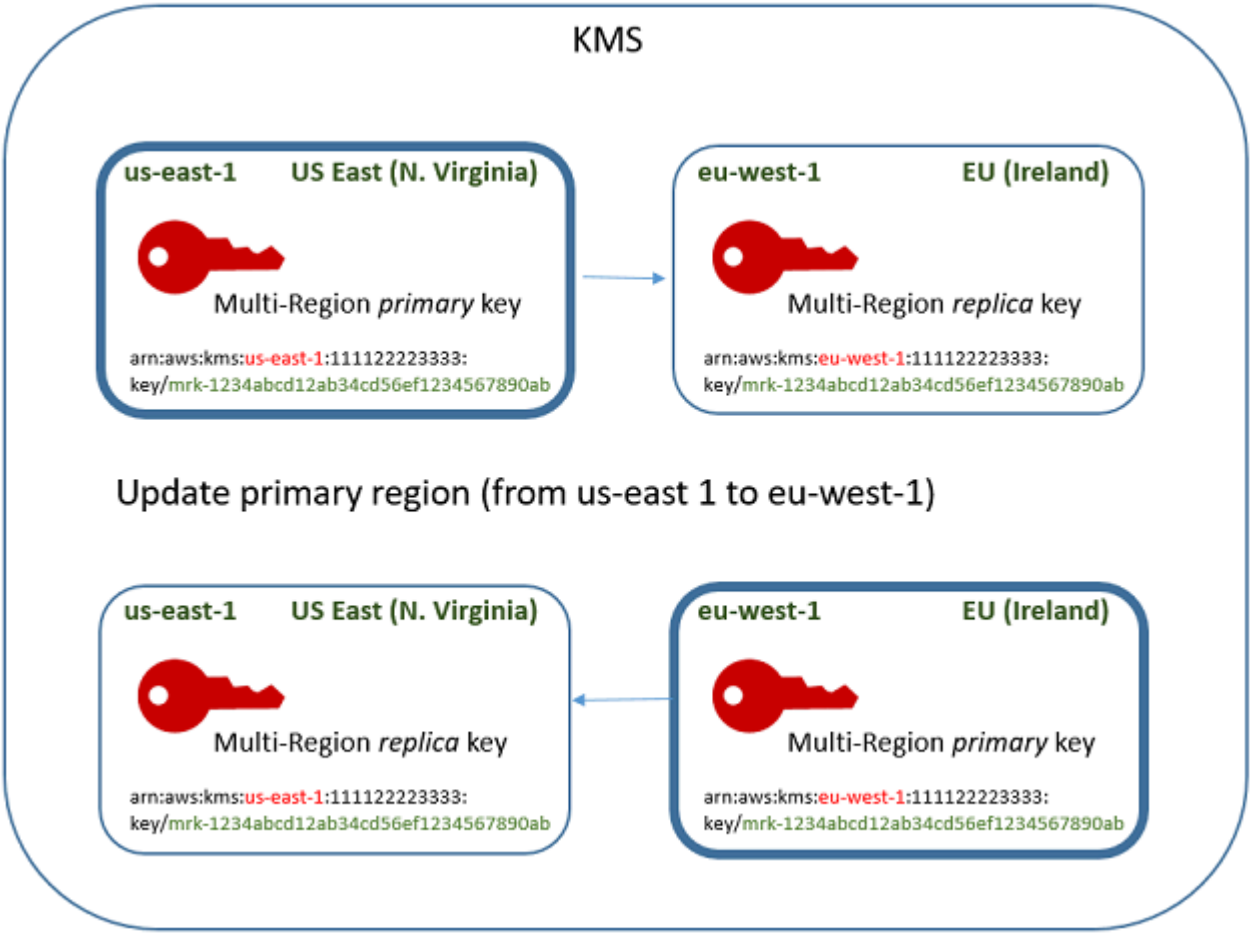
Ogni set di chiavi multiregione correlate deve avere una chiave primaria. Ma puoi cambiare la chiave primaria. Questa azione, nota come aggiornamento della Regione principale, converte la chiave primaria corrente in una chiave di replica e converte una delle chiavi di replica correlate nella chiave primaria. È possibile eseguire questa operazione se è necessario eliminare la chiave primaria corrente mantenendo le chiavi di replica o individuare la chiave primaria nella stessa Regione degli amministratori delle chiavi.

È possibile selezionare qualsiasi chiave di replica correlata come nuova chiave primaria. Sia la chiave primaria che la chiave di replica devono avere come stato della chiave `Enabled` all'avvio dell'operazione.

Anche al termine di questa operazione, il processo di aggiornamento della Regione primaria potrebbe essere ancora in corso per alcuni secondi. Durante questo periodo, le chiavi primarie vecchie e nuove hanno uno stato di chiave transitorio Aggiornamento in corso. Quando lo stato della chiave è `Updating`, è possibile utilizzare le chiavi nelle operazioni di crittografia, ma non è possibile replicare

la nuova chiave primaria o eseguire determinate operazioni di gestione, ad esempio l'attivazione o la disattivazione di queste chiavi. Operazioni come DescribeKeypotrebbero visualizzare sia la vecchia che la nuova chiave primaria come repliche. Lo stato della chiave `Enabled` viene ripristinato al termine dell'aggiornamento.

Supponi di avere una chiave primaria negli Stati Uniti orientali (Virginia settentrionale) (us-east-1) e una chiave replica in Europa (Irlanda) (eu-west-1). È possibile utilizzare la funzionalità di aggiornamento per modificare la chiave primaria negli Stati Uniti orientali (Virginia settentrionale) (us-east-1) in una chiave di replica e modificare la chiave di replica in Europa (Irlanda) (eu-west-1) nella chiave primaria.



Al termine del processo di aggiornamento, la chiave multiregione nella Regione Europa (Irlanda) (eu-west-1) è una chiave primaria multiregione e la chiave nella Regione Stati Uniti orientali (Virginia) (us-est-1) è la chiave di replica. Se sono presenti altre chiavi di replica correlate, queste diventano repliche della nuova chiave primaria. La prossima volta che AWS KMS sincronizza le proprietà condivise delle chiavi multiregione, otterrà le proprietà condivise dalla nuova chiave primaria e le copierà nelle chiavi di replica, inclusa la precedente chiave primaria.

L'operazione di aggiornamento non ha alcun effetto sull'ARN della chiavedi qualsiasi chiave multiregione. Inoltre, non ha alcun effetto sulle proprietà condivise, come il materiale chiave, o sulle proprietà indipendenti, come la policy chiave. Tuttavia, potresti voler aggiornare la policy chiave della nuova chiave primaria. Ad esempio, potresti voler aggiungere kms: ReplicateKey permission for trusted principals alla nuova chiave primaria e rimuoverla dalla nuova chiave di replica.

Stato della chiave **`Updating`**

Il processo di aggiornamento di una Regione primaria richiede un po' più di tempo rispetto al breve ritardo finale di coerenza che riguarda la maggior parte delle operazioni AWS KMS. Il processo potrebbe essere ancora in corso dopo l'operazione `UpdatePrimaryRegion` o dopo che è stata completata la procedura di aggiornamento nella console. Operazioni come DescribeKeypotrebbero visualizzare sia la vecchia che la nuova chiave primaria come repliche fino al completamento del processo.

Durante il processo di aggiornamento della Regione primaria, la vecchia chiave primaria e la nuova chiave primaria hanno come stato della chiave `Updating`. Quando il processo di aggiornamento viene completato correttamente, entrambe le chiavi ritornano allo stato della chiave `Enabled`. Durante lo stato `Updating`, alcune operazioni di gestione, come l'attivazione e la disattivazione delle chiavi, non sono disponibili. È tuttavia possibile continuare a utilizzare entrambe le chiavi nelle operazioni di crittografia senza interruzioni. Per informazioni sull'effetto dello stato della chiave `Updating`, consulta Stati chiave delle chiavi AWS KMS.

Aggiornamento di una Regione primaria (console)

È possibile aggiornare la chiave primaria nella console AWS KMS. Inizia nella pagina dei dettagli delle chiavi per la chiave primaria corrente.

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.
4. Selezionare l'alias o l'ID chiave della chiave primaria multiregione. In questo modo si apre la pagina dei dettagli delle chiavi per la chiave primaria.

   Per identificare una chiave primaria multiregione, utilizza l'icona dello strumento nell'angolo in alto a destra per aggiungere la colonna Regionalità nella tabella.
5. Seleziona la tab Regionalità.

6. Nella sezione Chiave primaria, scegli Modifica Regione primaria.
7. Scegliere la Regione della nuova chiave primaria. È possibile scegliere una sola Regione dal menu.

   Il menu Modifica Regioni principali include solo le Regioni che dispongono di una chiave multiregione correlata. Potresti non avere l'autorizzazione per aggiornare la Regione primaria in tutte le Regioni del menu.
8. Scegli Modifica Regione primaria.

Aggiornamento di una regione primaria (API AWS KMS)

Per modificare la chiave primaria in un set di chiavi multiregionali correlate, utilizzare l'operazione. UpdatePrimaryRegion

Usa il parametro `KeyId` per identificare la chiave primaria corrente. Usa il parametro `PrimaryRegion` per indicare la Regione AWS della nuova chiave primaria. Se la chiave primaria non dispone già di una replica nella nuova Regione primaria, l'operazione ha esito negativo.

Nell'esempio seguente la chiave primaria viene modificata da chiave multiregione nella Regione `us-west-2` a sua replica nella Regione `eu-west-1`. Il parametro `KeyId` identifica la chiave primaria corrente nella Regione `us-west-2`. Il parametro `PrimaryRegion` specifica la Regione AWS della nuova chiave primaria, `eu-west-1`.

```
$ aws kms update-primary-region \
      --key-id arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab \
      --primary-region eu-west-1
```

In caso di esito positivo, questa operazione non restituisce alcun output; solo il codice di stato HTTP. Per vedere l'effetto, chiamate l'DescribeKeyoperazione su uno dei tasti multiregione. Potresti dover attendere fino a quando lo stato della chiave ritorna `Enabled`. Quando lo stato della chiave è Aggiornamento in corso, i valori per la chiave potrebbero essere ancora in flusso.

Ad esempio, la seguente chiamata `DescribeKey` ottiene i dettagli sulla chiave multiregione nella Regione `eu-west-1`. L'output indica che la chiave multiregione nella Regione `eu-west-1` è ora la chiave primaria. La chiave multiregione correlata (stesso ID chiave) nella Regione `us-west-2` è ora una chiave di replica.

```
$ aws kms describe-key \
```

```
      --key-id arn:aws:kms:eu-west-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab \

{
    "KeyMetadata": {
        "AWSAccountId": "111122223333",
        "KeyId": "mrk-1234abcd12ab34cd56ef1234567890ab",
        "Arn": "arn:aws:kms:eu-west-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
        "CreationDate": 1609193147.831,
        "Enabled": true,
        "Description": "multi-region-key",
        "KeySpec": "SYMMETRIC_DEFAULT",
        "KeyState": "Enabled",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "Origin": "AWS_KMS",
        "KeyManager": "CUSTOMER",
        "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "EncryptionAlgorithms": [
            "SYMMETRIC_DEFAULT"
        ],
        "MultiRegion": true,
        "MultiRegionConfiguration": {
           "MultiRegionKeyType": "PRIMARY",
           "PrimaryKey": {
              "Arn": "arn:aws:kms:eu-west-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
              "Region": "eu-west-1"
           },
           "ReplicaKeys": [
              {
                 "Arn": "arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
                 "Region": "us-west-2"
              }
           ]
        }
    }
}
```

Rotazione di chiavi multiregione

Puoi abilitare e disabilitare la rotazione automatica del materiale chiave per le chiavi multiregione. La rotazione automatica delle chiavi è una proprietà condivisa delle chiavi multiregione.

Puoi abilitare e disabilitare la rotazione automatica delle chiavi solo sulla chiave primaria.

- Quando AWS KMS sincronizza le chiavi multiregione, copia l'impostazione della proprietà di rotazione della chiave dalla chiave primaria alle chiavi di replica.
- Quando AWS KMS ruota il materiale chiave, crea nuovo materiale chiave per la chiave primaria e quindi copia il nuovo materiale chiave attraverso i limiti della Regione in tutte le chiavi di replica correlate. Il materiale chiave mantiene AWS KMS crittografato. Questo passaggio viene controllato con attenzione per garantire che il materiale chiave sia completamente sincronizzato prima che qualsiasi chiave venga utilizzata in un'operazione di crittografia.
- AWS KMS non crittografa i dati con il nuovo materiale chiave fino a quando tale materiale chiave non è disponibile nella chiave primaria e in tutte le relative chiavi di replica.
- Quando si replica una chiave primaria che è stata ruotata, la nuova chiave di replica contiene il materiale chiave corrente e tutte le versioni precedenti del materiale chiave per le relative chiavi multiregione.

Questo modello assicura che le chiavi multiregione correlate siano completamente interoperabili. Qualsiasi chiave multiregione può decrittare qualsiasi testo cifrato crittografato da una chiave multiregione correlata, anche se il testo cifrato è stato crittografato prima della creazione della chiave.

La rotazione automatica delle chiavi non è supportata per le chiavi asimmetriche o le chiavi KMS con materiale chiave importato. Per informazioni sulla rotazione automatica delle chiavi e sulle istruzioni per abilitarla e disabilitarla, consulta Rotazione delle AWS KMS keys.

Download delle chiavi pubbliche

Quando si crea una chiave KMS asimmetrica multiregione, AWS KMS crea una coppia di chiavi RSA o basate su curva ellittica (ECC) per la chiave primaria. Quindi copia quella coppia di chiavi in ogni replica della chiave primaria. Di conseguenza, è possibile scaricare la chiave pubblica dalla chiave primaria o da una qualsiasi delle relative chiavi di replica. Otterrai sempre lo stesso materiale chiave.

Per informazioni su come scaricare e utilizzare le chiavi pubbliche al di fuori di AWS KMS, consulta Considerazioni speciali per il download delle chiavi pubbliche. Per istruzioni, consultare Download delle chiavi pubbliche.

Importazione di materiale chiave in chiavi multiregione

Puoi importare il tuo materiale della chiave in una chiave KMS multi-regione. Le chiavi multiregione create con il tuo materiale chiave sono interoperabili. È possibile crittografare i dati in una Regione e decrittarli in una Regione diversa con una chiave multiregione correlata.

Tuttavia, è necessario gestire il materiale chiave.

- AWS KMS non copia o sincronizza il materiale della chiave da una chiave primaria con il materiale chiave importato nelle relative chiavi di replica. È necessario importare lo stesso materiale chiave nelle chiavi primarie e di replica correlate.
- È possibile impostare il modello di scadenza e le date di scadenza per ogni chiave in modo indipendente quando si importa il materiale chiave. È possibile configurare lo stesso modello di scadenza o uno stesso modello di scadenza e le date di scadenza per le chiavi multiregione correlate. Se il materiale chiave si avvicina alla data di scadenza, è necessario reimportare il materiale chiave nella chiave multiregione interessata.

  Gli stati delle chiavi multiregione correlate sono indipendenti l'una dall'altra. Ad esempio, se il materiale chiave nella chiave primaria scade, le relative chiavi di replica non vengono influenzate.

Gli stessi requisiti per le chiavi di replica si applicano alle chiavi multiregione con materiale chiave importato. Se si importa lo stesso materiale chiave in chiavi di Regioni singole o chiavi multiregione non correlate, queste chiavi KMS sono non interoperabili.

Puoi creare chiavi multi-regione con materiale di chiavi simmetriche, asimmetriche o HMAC. AWS KMS non supporta materiale della chiave importato in archivi di chiavi personalizzate. Inoltre, non puoi abilitare la rotazione automatica delle chiavi di chiavi KMS con materiale chiave importato.

A parte le funzioni multiregione, le chiavi multiregione con materiale chiave importato sono uguali alle altre chiavi KMS con materiale chiave importato. Per ulteriori informazioni sulla creazione e la configurazione di chiavi per singola Regione con materiale chiave importato, consulta Informazioni sul materiale della chiave importato.

Argomenti

- Perché tutte le chiavi KMS con materiale importato non sono interoperabili?
- Creazione di una chiave primaria con materiale chiave importato
- Creazione di una chiave di replica con materiale chiave importato

Perché tutte le chiavi KMS con materiale importato non sono interoperabili?

Le chiavi KMS con materiale importato non sono interoperabili, anche se hanno lo stesso materiale chiave. Quando AWS KMS utilizza una chiave KMS per crittografare i dati, associa crittograficamente alcuni dei metadati chiave al testo cifrato. Questo protegge il testo cifrato in modo che solo la chiave KMS che ha crittografato i dati possa decrittarli.

Le chiavi multiregione sono progettate per essere interoperabili. Oltre ad avere lo stesso materiale chiave, hanno gli stessi ID chiave e altri metadati. Pertanto, i testi cifrati che generano possono essere decrittografati da qualsiasi chiave multiregione correlata. Di conseguenza, le proprietà di trust delle chiavi multiregione sono diverse da quelle delle chiavi della singola Regione. Tuttavia, per alcuni clienti, il vantaggio della decrittografia multiregione supera il valore di sicurezza di un testo cifrato basato su una singola chiave KMS in una singola Regione AWS.

Creazione di una chiave primaria con materiale chiave importato

Per creare una chiave primaria con materiale della chiave importato, inizia creando una chiave KMS senza materiale della chiave. Quando crei la chiave primaria senza materiale della chiave, devi indicare le specifiche della chiave che riflettono il tipo di materiale della chiave da importare. Importa, quindi, il materiale della chiave nella chiave primaria.

La procedura per la creazione di una chiave primaria multiregione senza materiale chiave è quasi la stessa della creazione di una chiave in una singola regione senza materiale chiave. L'unica differenza è che specifichi che la chiave è una chiave multi-regione.

Le autorizzazioni per la creazione di una chiave primaria multiregione con materiale chiave importato sono le stesse richieste per creare una chiave primaria multiregione con materiale AWS KMS chiave, incluse le CreateServiceLinkedRole autorizzazioni kms: CreateKey e iam: in una policy IAM. Puoi utilizzare le chiavi condizionali kms: MultiRegionKeyType e kms: KeyOrigin per consentire o negare l'autorizzazione alla creazione di chiavi primarie multiregionali con materiale chiave importato.

Quando crei una chiave primaria con materiale della chiave importato nella console AWS KMS, utilizza le impostazioni nella sezione Opzioni avanzate. Una volta creata la chiave KMS, non è più possibile modificare queste proprietà.

- Imposta Key material origin (Origine del materiale della chiave) su External (Import key material) (Esterna (Importa materiale della chiave)).
- Imposta Replica multiregione per consentire la replica di questa chiave in altre Regioni.

Quando si utilizza l'CreateKeyoperazione per creare una chiave primaria con materiale chiave importato, utilizzare i `MultiRegion` parametri `Origin` and e specificare e. `KeySpec` `KeyUsage` L'esempio seguente crea una chiave KMS `EXTERNAL` che può importare materiale della chiave `ECC_NIST_P384`.

```
$ aws kms create-key --origin EXTERNAL --key-spec ECC_NIST_P384 --key-usage SIGN_VERIFY
 --multi-region
```

Il risultato è una chiave primaria multiregione senza materiale chiave e uno stato della chiave `PendingImport`.

Per abilitare questa chiave KMS, è necessario scaricare una chiave pubblica e importare il token, utilizzare la chiave pubblica per crittografare il materiale chiave e quindi importare il materiale chiave. Per istruzioni, consulta Importazione di materiale chiave per le AWS KMS chiavi.

Creazione di una chiave di replica con materiale chiave importato

È possibile creare una AWS KMSchiave di replica multiregione nella console o utilizzando l'operazione API AWS KMS. Per replicare una chiave primaria multiregione con materiale chiave importato, utilizzare la stessa procedura utilizzata per la creazione di una chiave di replica con materiale chiave AWS KMS Tuttavia, il risultato è diverso. Anziché restituire una chiave di replica con lo stesso materiale chiave della chiave primaria, il processo di replica restituisce una chiave di replica senza materiale chiave e uno stato della chiave `PendingImport`. Per abilitare la chiave di replica, è necessario importare lo stesso materiale chiave nella chiave di replica importata nella chiave primaria.

Anche se non replica il materiale della chiave, AWS KMS crea la chiave di replica con lo stesso ID chiave, la stessa specifica della chiave, lo stesso utilizzo della chiave e la stessa origine del materiale della chiave della chiave primaria. Garantisce inoltre che il materiale chiave importato nella chiave di replica sia identico a quello importato nella chiave primaria.

Per creare una chiave di replica con materiale chiave importato:

1. Crea una chiave primaria multiregione con materiale chiave importato.
2. Scegli una delle seguenti operazioni.

   Nella console AWS KMS scegli una chiave primaria multiregione con materiale chiave importato. Quindi, sulla tab Regionalità, scegli Crea nuove chiavi di replica. Per istruzioni, consulta Creazione di chiavi di replica (console).

Oppure utilizzate l'ReplicateKeyoperazione. Per il parametro `KeyId`, immetti l'ID chiave o l'ARN della chiave di una chiave primaria multiregione con materiale chiave importato. Per istruzioni, consulta Creazione di una chiave di replica (API AWS KMS).

3. Per ogni nuova chiave di replica, attieniti alla procedura per scaricare una chiave pubblica e importare il token. Utilizza la chiave pubblica per crittografare il materiale della chiave primaria e quindi importare il materiale della chiave primaria nella chiave di replica. Per ciascuna chiave di replica è necessario disporre di una chiave pubblica e di un token di importazione diverso.

   Se il materiale chiave che tenti di importare nella chiave di replica non è lo stesso materiale chiave della chiave primaria, l'operazione ha esito negativo. AWS KMS non richiede che il modello di scadenza e le date di scadenza siano coordinate, ma è possibile stabilire regole business per le chiavi multiregione. Per istruzioni, consulta Importazione di materiale chiave per le AWS KMS chiavi.

Autorizzazioni per replicare chiavi con materiali chiave importati

Per creare una chiave di replica con materiale chiave importato, è necessario disporre delle autorizzazioni seguenti.

Nella Regione della chiave primaria:

- kms: ReplicateKey sulla chiave primaria (nella regione della chiave primaria). Includi questa autorizzazione nelle policy chiave della chiave primaria o in una policy IAM.

Nella Regione della chiave di replica:

- kms: CreateKey in una politica IAM.
- km:. GetParametersForImport È possibile includere questa autorizzazione nelle policy chiave della chiave di replica o in una policy IAM.
- km:. ImportKeyMaterial È possibile includere questa autorizzazione nelle policy chiave della chiave di replica o in una policy IAM.
- kms: TagResource è necessario per assegnare tag durante la replica. Includi questa autorizzazione in una policy IAM nella Regione di replica.
- kms: CreateAlias è necessario per replicare una chiave nella console. AWS KMS Per informazioni dettagliate, vedi Controllo dell'accesso agli alias.

Eliminazione di chiavi multiregione

Quando non si utilizza più una chiave primaria o una chiave di replica multiregione, è possibile programmarne l'eliminazione.

Sebbene l'eliminazione delle chiavi del servizio di gestione delle chiavi debba sempre essere eseguita con cautela, l'eliminazione di una replica di una chiave multiregione è meno rischiosa, a condizione che la chiave primaria esista ancora in AWS KMS. Se si elimina una chiave di replica dalla relativa Regione, ma si rileva il testo cifrato crittografato sotto la chiave eliminata, è possibile decrittare tale testo cifrato con qualsiasi chiave multiregione correlata. È inoltre possibile ricreare la chiave di replica replicando nuovamente la chiave primaria nella Regione della chiave di replica.

Tuttavia, l'eliminazione di una chiave primaria e della relativa chiave di replica è un'operazione molto pericolosa, equivalente all'eliminazione di una chiave in una singola Regione.

> **Warning**
>
> L'eliminazione di una chiave KMS è un'operazione distruttiva e potenzialmente pericolosa. Dovresti procedere solo quando hai la certezza di non dover più utilizzare la chiave KMS e che non ne avrai bisogno in futuro. In caso di dubbio, dovresti disabilitare la chiave KMS invece di eliminarla.

Per eliminare una chiave primaria, devi prima eliminare tutte le chiavi di replica. Se è necessario eliminare una chiave primaria da una determinata Regione senza eliminarne le chiavi di replica, modificare la chiave primaria in una chiave di replica aggiornando la Regione principale.

Prima di pianificare l'eliminazione di qualsiasi chiave KMS, consulta le avvertenze nell'Eliminazione di AWS KMS keysargomento e gli argomenti che spiegano come determinare l'uso passato di una chiave KMS e come impostare un CloudWatch allarme che ti avvisi dell'utilizzo della chiave KMS durante il periodo di attesa. Prima di eliminare la chiave primaria di una chiave asimmetrica multiregione, controlla l'argomento Eliminazione di chiavi asimmetriche.

Argomenti

- Autorizzazioni per l'eliminazione di chiavi multiregione
- Eliminazione di una chiave di replica
- Come eliminare una chiave primaria

Autorizzazioni per l'eliminazione di chiavi multiregione

Per pianificare l'eliminazione di una chiave multiregione, è necessaria solo la seguente autorizzazione.

- kms: ScheduleKeyDeletion — per pianificare l'eliminazione della chiave multiregionale e impostarne il periodo di attesa.

Si consiglia inoltre di disporre delle seguenti autorizzazioni correlate.

- kms: CancelKeyDeletion — per annullare l'eliminazione pianificata della chiave multiregionale.
- kms: DescribeKey — per visualizzare lo stato chiave della chiave multiregione e l'elenco delle chiavi multiregione correlate.
- kms: DisableKey — per darti la possibilità di disabilitare una chiave multiregionale invece di eliminarla.
- kms: EnableKey — per ripristinare la funzionalità di una chiave multiregionale dopo averne annullato l'eliminazione.

È inoltre possibile includere l'autorizzazione per replicare la chiave primaria e modificare la chiave primaria.

- km: ReplicateKey
- km: UpdateReplicaRegion

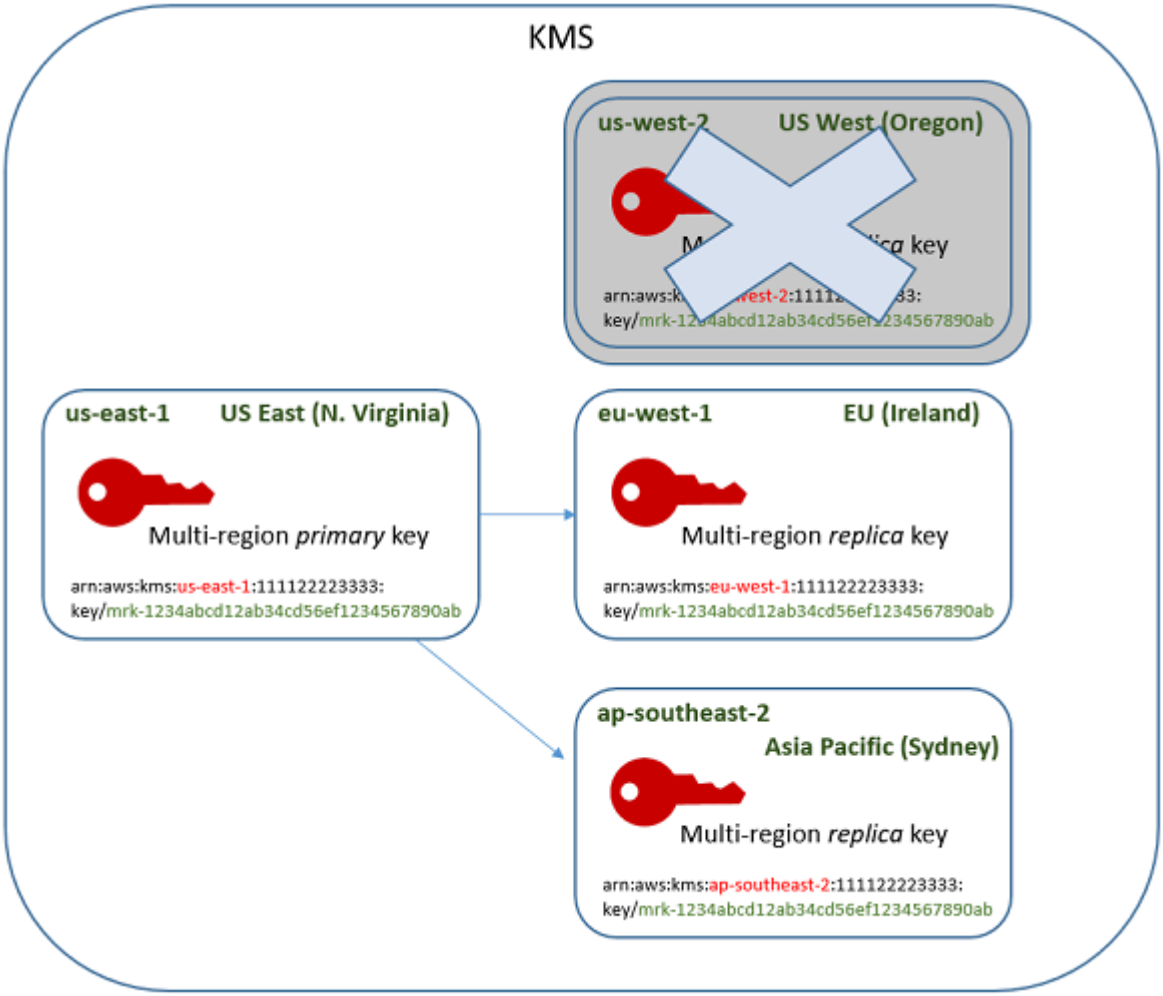
È possibile includere queste autorizzazioni in una policy IAM, ma come best practice è consigliabile inserirle in una policy chiave in cui si applicano solo alla chiave KMS da gestire.

Eliminazione di una chiave di replica

Per eliminare una chiave di replica, puoi utilizzare la console AWS KMS o l'API AWS KMS . Puoi eliminare una chiave di replica in qualsiasi momento. Non dipende dallo stato della chiave di qualsiasi altra chiave KMS.

Se si elimina accidentalmente una chiave di replica, è possibile ricrearla replicando la stessa chiave primaria nella stessa regione. La nuova chiave di replica creata avrà le stesse proprietà condivise della chiave di replica originale.

La procedura per l'eliminazione di una chiave di replica multiregione equivale all'eliminazione di una chiave in una singola Regione.



1. Pianificare l'eliminazione della chiave di replica. Selezionare un periodo di attesa di 7-30 giorni. Il periodo di attesa predefinito è di 30 giorni.
2. Durante il periodo di attesa, lo stato della chiave di replica diventa `Pending deletion` (`PendingDeletion`) e non è possibile utilizzare la chiave nelle operazioni di crittografia.
3. È possibile annullare l'eliminazione pianificata della chiave di replica in qualsiasi momento nel periodo di attesa. Lo stato della chiave diventa `Disabled`, ma puoi riabilitare la chiave KMS.
4. Alla scadenza del periodo di attesa, AWS KMS elimina la chiave di replica.

Puoi visualizzare un registro delle tue azioni nel tuo log AWS CloudTrail. AWS KMS registra le operazioni che pianificano l'eliminazione della chiave KMS e l'azione che elimina la chiave KMS.

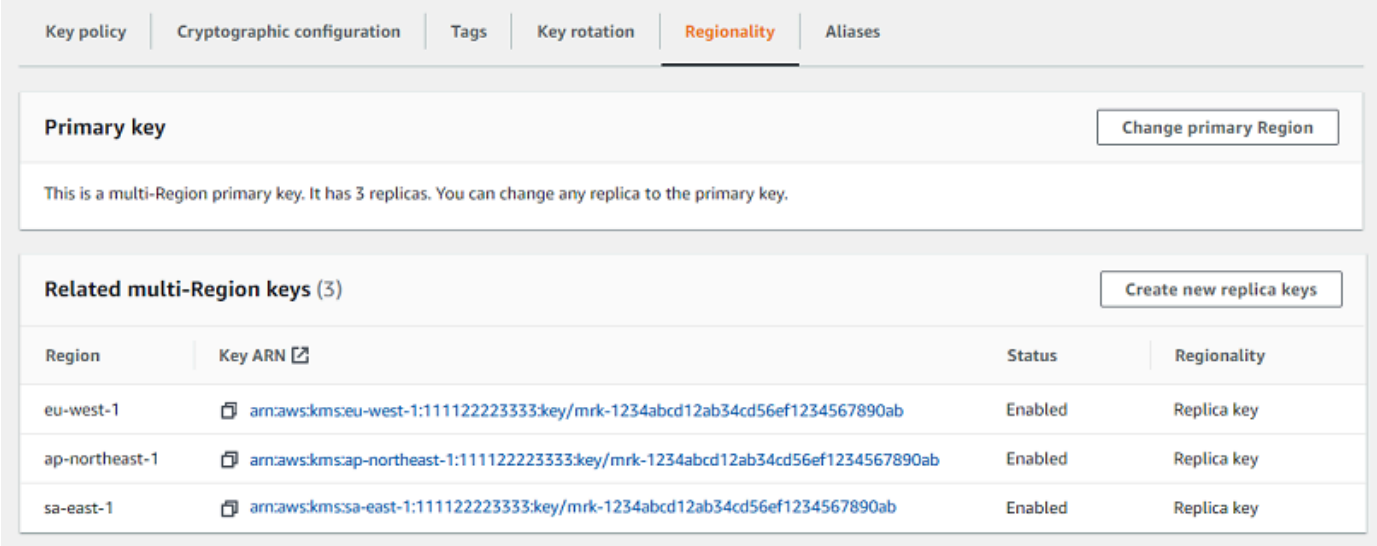
Eliminazione di una chiave di replica (console)

Per pianificare l'eliminazione di una chiave di replica multiregione, utilizza la stessa procedura che utilizzi per pianificare l'eliminazione di una chiave in una singola Regione.

Poiché le chiavi di replica correlate sono in diverse Regioni AWS, non è possibile pianificare l'eliminazione di più di una chiave di replica alla volta. Per eliminare tutte le chiavi di replica correlate, utilizza un modello come quello seguente.

Per pianificare l'eliminazione di tutte le chiavi di replica correlate

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.
3. Usa il selettore Regione nell'angolo in alto a destra per scegliere la Regione della chiave primaria multiregione.
4. Scegli l'alias o l'ID chiave della chiave primaria.
5. Seleziona la tab Regionalità.



6. Nella sezione Chiavi multiregione correlate, scegli l'ARN della chiave di replica.

   Questa azione apre la pagina dei dettagli della chiave di replica in una nuova tab del browser. La console è impostata sulla Regione della chiave di replica.
7. Scegli Azioni sulle chiavi, Pianifica eliminazione chiave.

Questa azione avvia il processo di pianificazione dell'eliminazione della chiave. Completare il processo di eliminazione della chiave di pianificazione. Per informazioni dettagliate, vedi Pianificazione e annullamento dell'eliminazione di chiavi (console).

8. Torna alla scheda del browser che mostra la tab Regionalità della chiave primaria. (Potrebbe essere necessario aggiornare la pagina per visualizzare lo stato aggiornato delle chiavi di replica). Scegliere l'ARN chiave di un'altra chiave di replica e ripetere il processo di pianificazione dell'eliminazione della chiave di replica.

Eliminazione di una chiave di replica (API AWS KMS)

Per pianificare l'eliminazione di una chiave di replica multiregionale, utilizzare l'operazione. ScheduleKeyDeletion Per specificare la chiave KMS, utilizzare il relativo ID chiave o l'ARN chiave. Quando si lavora con chiavi multiregione, è possibile ridurre l'incidenza di errori utilizzando la chiave ARN con il suo valore Regione esplicito.

Ad esempio, questo comando elimina una chiave di replica dalla Regione us-west-2 (Stati Uniti occidentali (Oregon)). Poiché il comando non specifica un periodo di attesa, il periodo di attesa è impostato sul valore predefinito di 30 giorni.

```
$ aws kms schedule-key-deletion \
    --region us-west-2 \
    --key-id arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab
```

Quando il comando viene completato, restituisce l'ARN chiave (`KeyId`), il periodo di attesa (`PendingWindowInDays`), la data di cancellazione (`DeletionDate`) e lo stato della chiave corrente (`KeyState`), che dovrebbe essere `PendingDeletion`.

Quando si elimina una chiave di replica multiregione, assicurarsi di verificare che i valori ID chiave e Regione nell'ARN chiave siano quelli previsti.

```
{
    "KeyId": "arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
    "DeletionDate": 1599523200.0,
    "KeyState": "PendingDeletion",
    "PendingWindowInDays": 30
}
```

Per eliminare tutte le repliche di una chiave primaria multiregione a livello di programmazione, creare un elenco delle Regioni che contengono chiavi di replica. Quindi, per ogni Regione nell'elenco, chiama l'operazione `ScheduleKeyDeletion`, come mostrato sopra.

A differenza di una chiave in una singola Regione eliminata in modo permanente, è possibile ripristinare una chiave di replica replicando la chiave primaria nella Regione in cui si trovava la chiave di replica eliminata.

Per verificare lo stato della chiave di replica e visualizzare la chiave primaria e le chiavi di replica di una chiave multiregionale, utilizzare l'operazione. DescribeKey

Come eliminare una chiave primaria

È possibile pianificare l'eliminazione di una chiave primaria multiregione in qualsiasi momento. Tuttavia, AWS KMS non eliminerà una chiave primaria multiregione che ha una chiave di replica, anche se è stata pianificata l'eliminazione.

Per eliminare una chiave primaria, è necessario pianificare l'eliminazione di tutte le chiavi di replica e quindi attendere l'eliminazione delle chiavi di replica. Il periodo di attesa richiesto per l'eliminazione di una chiave primaria inizia quando viene eliminata l'ultima delle relative chiavi di replica. Se è necessario eliminare una chiave primaria da una determinata Regione senza eliminarne le chiavi di replica, modificare la chiave primaria in una chiave di replica aggiornando la Regione principale.

Se una chiave primaria non dispone di chiavi di replica, il processo è identico a quello di eliminazione di una chiave di replica o di eliminazione di qualsiasi chiave KMS regionale.

Se è stata pianificata l'eliminazione di una chiave primaria, non è possibile utilizzarla nelle operazioni di crittografia e non è possibile replicarla. Tuttavia, a meno che non siano pianificate anche per l'eliminazione, le relative chiavi di replica non vengono influenzate.

Puoi utilizzare la console AWS KMSo l'API AWS KMS per pianificare l'eliminazione delle chiavi primarie e di replica. È possibile pianificare l'eliminazione della chiave primaria prima, dopo o nello stesso momento in cui si pianifichi l'eliminazione delle chiavi di replica. Il processo deve essere simile al seguente:

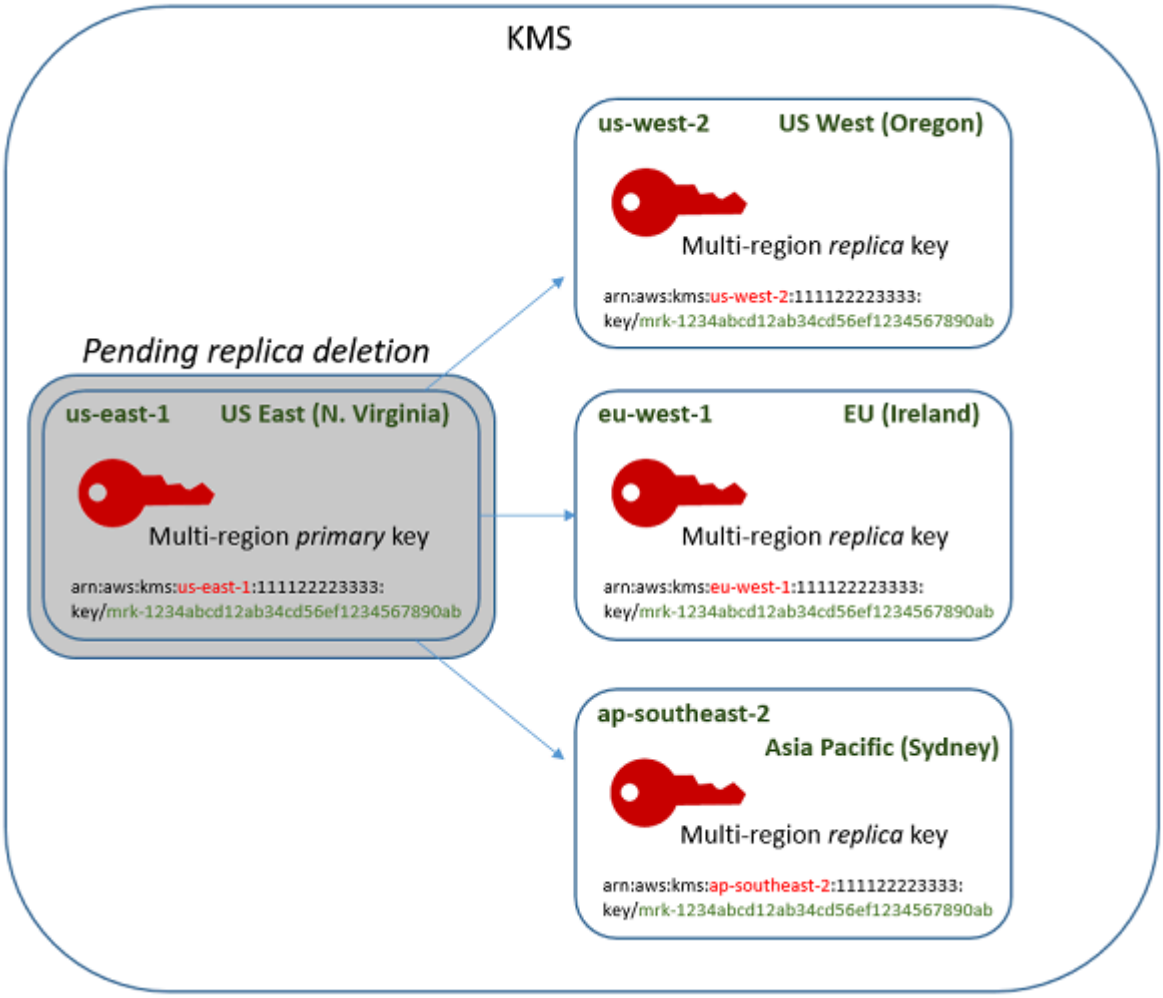
1. Pianificare l'eliminazione della chiave primaria. Selezionare un periodo di attesa di 7-30 giorni. Il periodo di attesa predefinito è di 30 giorni. Tuttavia, il periodo di attesa per la chiave primaria non inizia finché non vengono eliminate tutte le chiavi di replica.

   Se esistono ancora chiavi di replica, lo stato della chiave primaria diventa `Pending replica deletion` (`PendingReplicaDeletion`). In caso contrario, diventa `Pending deletion`

(`PendingDeletion`). In entrambi i casi, non è possibile utilizzare la chiave primaria nelle operazioni di crittografia e non è possibile replicarla.

La pianificazione dell'eliminazione di una chiave primaria non influisce sulle chiavi di replica. Lo stato di chiave rimane abilitato e puoi utilizzarle nelle operazioni di crittografia. Se le chiavi di replica non vengono eliminate, lo stato `Pending replica deletion` della chiave primaria può persistere a tempo indeterminato.

```
KMS key:                    Key state:
Primary (us-east-1)           Pending replica deletion (waiting period 30 days -- not
 started)
Replica (us-west-2)           Enabled
Replica (eu-west-1)           Enabled
Replica (ap-southeast-2)      Enabled
```



2. Pianificare l'eliminazione di ogni chiave di replica. Selezionare un periodo di attesa di 7-30 giorni. Il periodo di attesa predefinito è di 30 giorni. È possibile eliminare più chiavi di replica contemporaneamente. I loro periodi di attesa vengono eseguiti contemporaneamente. Durante il periodo di attesa, lo stato della chiave delle chiavi di replica diventa `Pending deletion` (`PendingDeletion`) e non è possibile utilizzare le chiavi KMS nelle operazioni di crittografia.

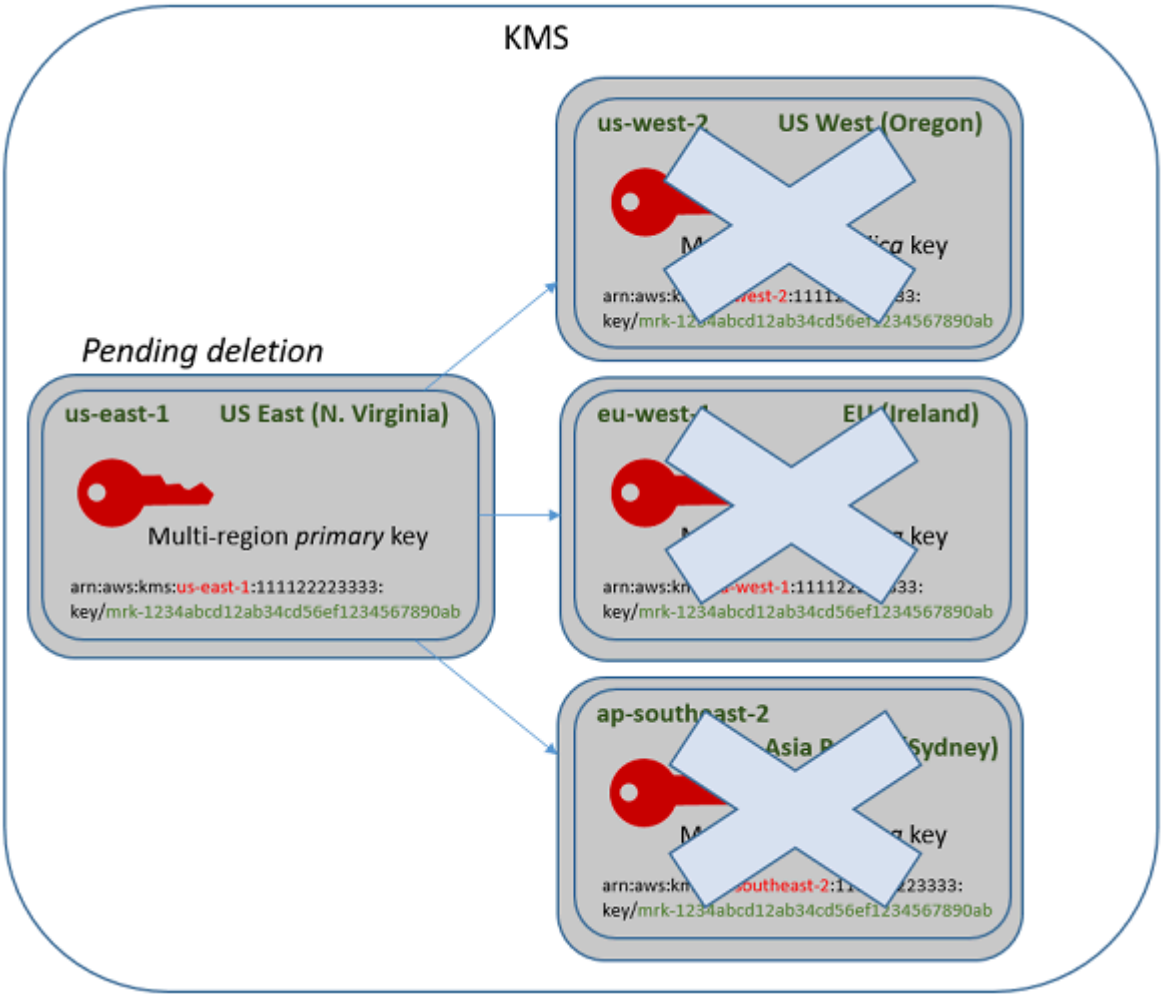
   Ad esempio, se si dispone di tre chiavi di replica, è possibile pianificare l'eliminazione di tutte e tre contemporaneamente. Possono avere periodi di attesa uguali o diversi. Si noti che il periodo di attesa sulla chiave primaria non è ancora iniziato. Il suo stato della chiave è `PendingReplicaDeletion` perché dispone di chiavi di replica esistenti.

   ```
   KMS key:                    Key state:
   Primary key (us-east-1)       Pending replica deletion (waiting period 30 days -- not
    started)
   Replica (us-west-2)           Pending deletion (7 days)
   Replica (eu-west-1)           Pending deletion (7 days)
   Replica (ap-southeast-2)      Pending deletion (30 days)
   ```

3. È possibile annullare l'eliminazione pianificata della chiave primaria o di qualsiasi chiave di replica finché non viene eliminata. Lo stato della chiave diventa `Disabled`, ma puoi riabilitare la chiave KMS.

4. Alla scadenza del periodo di attesa dell'ultima chiave di replica, AWS KMS elimina l'ultima chiave di replica. Lo stato della chiave primaria passa da `Pending replica deletion` (`PendingReplicaDeletion`) a `Pending deletion` (`PendingDeletion`) e inizia il periodo di attesa di 7-30 giorni per la chiave primaria.

   ```
   KMS key:                    Key state:
   Primary key (us-east-1)       Pending deletion (waiting period 30 days)
   ```



5. Alla scadenza del periodo di attesa, AWS KMS elimina la chiave primaria.

Il tempo minimo per eliminare una chiave primaria con repliche è di 14 giorni.

Se pianifichi l'eliminazione della chiave primaria e di tutte le chiavi di replica con un periodo di attesa di 7 giorni, le chiavi di replica vengono eliminate dopo 7 giorni. La chiave primaria viene eliminata il 14° giorno.

- Giorno 1: pianificare l'eliminazione delle chiavi primarie e di replica con il periodo di attesa minimo di 7 giorni. Iniziano i periodi di attesa di eliminazione di 7 giorni per le chiavi di replica. Il periodo di attesa di eliminazione per la chiave primaria non viene ancora avviato.
- Giorno 7: terminano i periodi di attesa di eliminazione per le chiavi di replica. AWS KMS elimina tutte le chiavi di replica. Quando viene eliminata l'ultima chiave di replica, viene avviato il periodo di attesa di eliminazione di 7 giorni per la chiave primaria.

- Giorno 14: termina il periodo di attesa per l'eliminazione della chiave primaria. AWS KMS elimina la chiave primaria.

Puoi visualizzare un registro delle tue azioni nel tuo log AWS CloudTrail. AWS KMS registra le operazioni che pianificano l'eliminazione di ciascuna chiave KMS e l'azione che elimina la chiave KMS.

Eliminazione di una chiave primaria (console)

Per eliminare una chiave primaria multiregione, attenersi alla procedura descritta di seguito.

Per pianificare l'eliminazione di chiavi

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.
4. Seleziona la casella di controllo accanto alla chiave KMS da eliminare. È inoltre possibile selezionare una o più chiavi KMS, incluse le repliche di questa chiave primaria.
5. Scegliere Key actions (Operazioni sulle chiavi), Schedule key deletion (Pianifica eliminazione chiave).
6. Leggere l'avviso e le informazioni sull'annullamento dell'eliminazione durante il periodo di attesa. Se si decide di annullare l'eliminazione, scegliere Cancel (Annulla).
7. Per Waiting period (in days) (Periodo di attesa (in giorni)), immettere un numero di giorni compreso tra 7 e 30. Se sono state selezionate più chiavi KMS, il periodo di attesa scelto si applica a tutte le chiavi KMS selezionate. Il periodo di attesa per le chiavi di replica viene eseguito contemporaneamente, ma il periodo di attesa per la chiave primaria non inizia fino a quando AWS KMS non elimina l'ultima delle chiavi di replica.
8. Seleziona la casella di controllo accanto a Conferma di voler eliminare della chiave tra ***<number of days>*** giorni..
9. Scegliere Schedule deletion (Pianifica eliminazione).

Per verificare lo stato di eliminazione delle chiavi KMS, nella tab Pagina dei dettagli per la chiave primaria, consulta la sezione Configurazione generale. Lo stato della chiave viene mostrato nel

campo Stato. Quando lo stato della chiave primaria diventa `Pending deletion`, viene mostrata la data di eliminazione pianificata.

È inoltre possibile controllare lo stato della chiave (Stato) di tutte le chiavi primarie e di replica nella tab Regionalità della pagina dei dettagli per ciascuna chiave multiregione. Per informazioni dettagliate, vedi Visualizzazione di chiavi multiregione.

Eliminazione di una chiave primaria (API AWS KMS)

Per eliminare una chiave di replica multiregionale, utilizzare l'operazione. ScheduleKeyDeletion Per specificare la chiave KMS, utilizzare il relativo ID chiave o l'ARN chiave. Quando si lavora con chiavi multiregione, è possibile ridurre l'incidenza di errori utilizzando la chiave ARN con il suo valore Regione esplicito.

Ad esempio, questo comando elimina una chiave primaria dalla Regione us-east-1 (Stati Uniti orientali (Virginia settentrionale)). Poiché il comando non specifica un periodo di attesa, il periodo di attesa è impostato sul valore predefinito di 30 giorni.

```
$ aws kms schedule-key-deletion \
    --key-id arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab
```

Quando il comando viene completato, restituisce l'ARN chiave, lo stato della chiave risultante e il periodo di attesa (`PendingWindowInDays`).

Se la chiave primaria non dispone di repliche, lo stato della chiave primaria è`PendingDeletion` e l'output include il campo `DeletionDate`. Se rimangono chiavi di replica, lo stato della chiave primaria è `PendingReplicaDeletion` e `DeletionDate` viene omesso perché è incerto. Anche se le chiavi di replica sono pianificate per l'eliminazione, è possibile annullare l'eliminazione pianificata.

Quando si elimina una chiave primaria multiregione, assicurarsi di verificare che i valori ID chiave e Regione nell'ARN chiave siano quelli previsti.

```
{
    "KeyId": "arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
    "KeyState": "PendingReplicaDeletion",
    "PendingWindowInDays": 30
}
```

Per verificare lo stato di eliminazione delle chiavi KMS, utilizza l'DescribeKeyoperazione sulla chiave primaria o sulle eventuali chiavi di replica rimanenti. L'orologio del periodo di attesa per la chiave primaria non viene avviato fino a quando l'ultima replica viene eliminata e lo stato della chiave diventa `PendingDeletion`.

Per calcolare la data di eliminazione prevista della chiave primaria, scorri gli ARN della chiave di replica nella risposta, eseguire `DescribeKey` su ognuno di essi, ottieni l'ultimo valore `DeletionDate` e quindi aggiungi il valore `PendingDeletionWindowInDays` per la chiave primaria. I periodi di attesa per le chiavi di replica vengono eseguiti contemporaneamente.

Nell'esempio seguente, la chiave KMS è una chiave primaria multiregione con chiavi di replica esistenti. Perché lo stato della chiave è `PendingReplicaDeletion`, la risposta include il periodo di attesa (`PendingWindowInDays`), ma non la `DeletionDate`. La data di eliminazione effettiva della chiave primaria dipende da quando vengono eliminate le chiavi di replica.

```
$ aws kms describe-key \
    --key-id arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab

{
    "KeyMetadata": {
        "AWSAccountId": "111122223333",
        "KeyId": "mrk-1234abcd12ab34cd56ef1234567890ab",
        "Arn": "arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
        "CreationDate": 1597902361.481,
        "Enabled": false,
        "Description": "",
        "KeySpec": "SYMMETRIC_DEFAULT",
        "KeyState": "PendingReplicaDeletion",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "Origin": "AWS_KMS",
        "KeyManager": "CUSTOMER",
        "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "EncryptionAlgorithms": [
            "SYMMETRIC_DEFAULT"
        ],
        "MultiRegion": true,
        "MultiRegionConfiguration": {
            "MultiRegionKeyType": "PRIMARY",
            "PrimaryKey": {
```

```
                "Arn": "arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
                "Region": "us-east-1"
            },
            "ReplicaKeys": [
                {
                    "Arn": "arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
                    "Region": "us-west-2"
                },
{
                    "Arn": "arn:aws:kms:eu-west-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
                    "Region": "eu-west-1"
                },
                {
                    "Arn": "arn:aws:kms:ap-southeast-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
                    "Region": "ap-southeast-2"
                }
            ]
        },
        "PendingDeletionWindowInDays": 30
    }
}
```

Quando tutte le repliche vengono eliminate, l'output `DescribeKey` mostra la chiave primaria rimanente con uno stato della chiave `PendingDeletion`. Mentre lo stato della chiave è `PendingDeletion`, il campo `DeletionDate` viene visualizzato al posto del campo `PendingWindowInDays`.

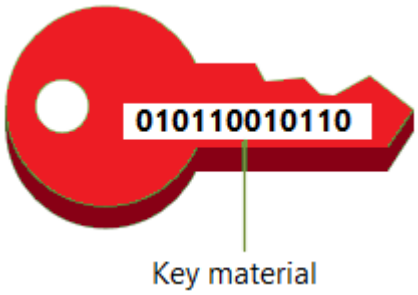
```
$ aws kms describe-key \
    --key-id arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab

{
    "KeyMetadata": {
        "AWSAccountId": "111122223333",
        "KeyId": "mrk-1234abcd12ab34cd56ef1234567890ab",
        "Arn": "",
        "CreationDate": 1597902361.481,
        "Enabled": false,
        "Description": "",
```

```
        "KeySpec": "SYMMETRIC_DEFAULT",
        "KeyState": "PendingDeletion",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "DeletionDate": 1597968000.0,
        "Origin": "AWS_KMS",
        "KeyManager": "CUSTOMER",
        "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "EncryptionAlgorithms": [
            "SYMMETRIC_DEFAULT"
        ],
        "MultiRegion": true,
        "MultiRegionConfiguration": {
            "MultiRegionKeyType": "PRIMARY",
            "PrimaryKey": {
                "Arn": "arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
                "Region": "us-east-1"
            },
            "ReplicaKeys": []
        }
    }
}
```

Importazione di materiale chiave per le AWS KMS chiavi

Puoi creare una AWS KMS keys (chiave KMS) con il materiale della chiave fornito da te.

Una chiave KMS è la rappresentazione logica di una chiave crittografica. I metadati per una chiave KMS includono l'ID del materiale della chiave utilizzato per crittografare e decrittografare i dati. Quando crei una chiave KMS, per impostazione predefinita, AWS KMS genera il materiale della chiave per quella chiave KMS. Tuttavia è possibile creare una chiave KMS senza materiale della chiave e importare il proprio materiale in quella chiave KMS. Questa caratteristica è definita "bring your own key" (BYOK).



> **Note**
>
> AWS KMS non supporta la decrittografia di alcun testo AWS KMS cifrato esterno a AWS KMS, anche se il testo cifrato è stato crittografato con una chiave KMS con materiale chiave importato. AWS KMS non pubblica il formato di testo cifrato richiesto da questa attività e il formato potrebbe cambiare senza preavviso.

Il materiale della chiave importato è supportato su tutti i tipi di chiavi KMS ad eccezione delle chiavi KMS in archivi di chiavi personalizzate. Nelle regioni cinesi, tuttavia, puoi importare il materiale della chiave di crittografia simmetrica solo in chiavi KMS.

Quando si utilizza materiale chiave importato, l'utente rimane responsabile del materiale chiave, consentendone AWS KMS al contempo l'utilizzo di una copia. Potresti scegliere di farlo per uno o più dei seguenti motivi:

- Per dimostrare che il materiale della chiave è stato generato utilizzando una sorgente di entropia che soddisfa i tuoi requisiti.
- Utilizzare materiale chiave proveniente dalla propria infrastruttura con AWS servizi e utilizzarlo per AWS KMS gestire il ciclo di vita di tale materiale chiave all'interno. AWS
- Utilizzare chiavi esistenti e consolidate, ad esempio le chiavi per la firma del codice AWS KMS, la firma dei certificati PKI e le applicazioni con certificato bloccato
- Per impostare una scadenza per il materiale chiave AWS e per eliminarlo manualmente, ma anche per renderlo nuovamente disponibile in futuro. La pianificazione, dell'eliminazione di una chiave, invece, richiede un periodo di attesa compreso tra 7 e 30 giorni, trascorso il quale non puoi più recuperare la chiave KMS eliminata.
- Possedere la copia originale del materiale chiave e conservarla all'esterno AWS per una maggiore durabilità e ripristino di emergenza durante l'intero ciclo di vita del materiale chiave.
- Per le chiavi asimmetriche e le chiavi HMAC, l'importazione crea chiavi compatibili e interoperabili che funzionano all'interno e all'esterno di. AWS

È possibile controllare e monitorare l'uso e la gestione di una chiave KMS con materiale chiave importato. AWS KMS registra un evento nel AWS CloudTrail registro quando crei la chiave KMS, scarichi la chiave pubblica di wrapping e importi il token e importi il materiale chiave. AWS KMS registra anche un evento quando si elimina manualmente il materiale chiave importato o quando si AWS KMS elimina il materiale chiave scaduto.

Per informazioni sulle differenze importanti tra le chiavi KMS con materiale chiave importato e quelle con materiale chiave generato da AWS KMS, vedere. Informazioni sul materiale della chiave importato

Chiavi KMS supportate

AWS KMS supporta materiale chiave importato per i seguenti tipi di chiavi KMS. Non puoi importare il materiale della chiave in chiavi KMS in archivi di chiavi personalizzate. Nelle regioni cinesi, tuttavia, puoi importare materiale della chiave solo in chiavi di crittografia simmetrica.

- Chiavi KMS di crittografia simmetrica
- Chiavi KMS RSA asimmetriche (per la crittografia o la firma, ma non entrambe)
- Chiavi KMS a curva ellittica asimmetrica (ECC) (solo per la firma)
- Chiavi KMS HMAC
- Chiavi multi-regione di tutti i tipi supportati.

Regioni

Il materiale chiave importato è supportato in tutti i Regioni AWS AWS KMS supporti.

Nelle regioni cinesi puoi importare materiale della chiave solo in chiavi KMS di crittografia simmetrica. I requisiti del materiali della chiave, inoltre, differiscono da quelli di altre regioni. Per informazioni dettagliate, vedi Importazione del materiale delle chiavi Fase 3: crittografare il materiale delle chiavi.

Argomenti

- Pianificazione dell'importazione del materiale della chiave
- Gestione del materiale della chiave importato
- Importazione del materiale della chiave - Fase 1: creare una AWS KMS key senza materiale chiave
- Fase 2 dell'importazione del materiale della chiave: scaricare la chiave pubblica di wrapping e il token di importazione
- Importazione del materiale delle chiavi Fase 3: crittografare il materiale delle chiavi
- Importazione del materiale delle chiavi Fase 4: importare il materiale delle chiavi

Pianificazione dell'importazione del materiale della chiave

Il materiale chiave importato consente di proteggere le AWS risorse con le chiavi crittografiche generate dall'utente. Il materiale della chiave che importi è associato a una chiave KMS particolare. Puoi reimportare lo stesso materiale chiave nella stessa chiave KMS, ma non puoi importare materiale chiave diverso nella chiave KMS e non puoi convertire una chiave KMS progettata per il materiale chiave importato in una chiave KMS con materiale chiave. AWS KMS

Ulteriori informazioni:

- the section called “Selezione di una specifica della chiave pubblica di wrapping”
- the section called “Selezione di un algoritmo di wrapping”

Argomenti

Informazioni sul materiale della chiave importato

Prima di decidere di importare materiale chiave in AWS KMS, è necessario comprendere le seguenti caratteristiche del materiale chiave importato.

Generare il materiale della chiave

Sei responsabile della generazione del materiale della chiave utilizzando una fonte di casualità che soddisfa i tuoi requisiti di sicurezza.

Puoi eliminare il materiale chiave

Puoi eliminare il materiale della chiave importato da una chiave KMS, rendendo immediatamente inutilizzabile la chiave KMS. Quando importi il materiale della chiave in una chiave KMS, puoi determinare se la chiave scade e impostare la data di scadenza. Quando arriva la data di scadenza, AWS KMS elimina il materiale chiave. Senza materiale chiave, la chiave KMS non può essere utilizzata in nessuna operazione di crittografia. Per ripristinare la chiave, è necessario importare nuovamente lo stesso materiale chiave nella chiave.

Non puoi modificare il materiale della chiave

Quando importi materiale della chiave in una chiave KMS, la chiave KMS viene associata in modo permanente a quel materiale della chiave. Puoi importare nuovamente lo stesso materiale della chiave, ma non puoi importare materiale della chiave diverso in quella chiave KMS. Inoltre, non puoi abilitare la rotazione automatica delle chiavi per una chiave KMS con materiale della chiave importato. Tuttavia, puoi ruotare manualmente una chiave KMS con materiale della chiave importato.

Non puoi modificare l'origine del materiale della chiave

Le chiavi KMS progettate per il materiale chiave importato ha un valore di origine di `EXTERNAL` che non può essere modificato. Non è possibile convertire una chiave KMS per materiale chiave importato in modo da utilizzare materiale chiave proveniente da altre fonti, tra cui. AWS KMSAllo stesso modo, non è possibile convertire una chiave KMS con materiale AWS KMS chiave in una chiave progettata per il materiale chiave importato.

Non puoi esportare il materiale della chiave

Non è possibile esportare alcun materiale chiave importato. AWS KMS non può restituirti il materiale chiave importato in nessuna forma. È necessario conservare una copia del materiale chiave importato all'esterno AWS, preferibilmente in un gestore di chiavi, come un modulo di sicurezza hardware (HSM), in modo da poter reimportare il materiale chiave in caso di eliminazione o scadenza.

Puoi creare chiavi multi-regione con materiale della chiave importato

Le chiavi multi-regione con il materiale della chiave importato includono le funzionalità delle chiavi KMS con il materiale della chiave importato e possono interoperare tra Regioni AWS. Per creare una chiave multi-regione con il materiale della chiave importato, devi importare lo stesso materiale della chiave nella chiave KMS primaria e in ogni chiave di replica. Per informazioni dettagliate, vedi Importazione di materiale chiave in chiavi multiregione.

Le chiavi asimmetriche e le chiavi HMAC sono portatili e interoperabili

È possibile utilizzare il materiale chiave asimmetrico e il materiale chiave HMAC all'esterno AWS per interagire con chiavi con AWS KMS lo stesso materiale chiave importato.

A differenza del testo cifrato AWS KMS simmetrico, che è indissolubilmente legato alla chiave KMS utilizzata nell'algoritmo, AWS KMS utilizza formati HMAC standard e asimmetrici per la crittografia, la firma e la generazione MAC. Di conseguenza, le chiavi sono portatili e supportano gli scenari di chiavi di deposito tradizionali.

Quando la chiave KMS ha importato materiale chiave, puoi utilizzare il materiale chiave importato all'esterno per eseguire le seguenti operazioni. AWS

- Chiavi HMAC: puoi verificare un tag HMAC generato dalla chiave KMS HMAC con il materiale della chiave importato. Puoi anche utilizzare la chiave KMS HMAC con il materiale chiave importato per verificare un tag HMAC generato dal materiale chiave all'esterno di. AWS
- Chiavi di crittografia asimmetriche: puoi utilizzare la tua chiave di crittografia asimmetrica privata all'esterno di AWS per decrittografare un testo cifrato crittografato dalla chiave KMS con la chiave pubblica corrispondente. Puoi anche utilizzare la tua chiave KMS asimmetrica per decrittografare un testo cifrato asimmetrico generato all'esterno di. AWS
- Chiavi di firma asimmetriche: puoi utilizzare la tua chiave KMS di firma asimmetrica con materiale chiave importato per verificare le firme digitali generate dalla tua chiave di firma privata all'esterno di. AWSPuoi anche utilizzare la tua chiave di firma pubblica asimmetrica all'esterno di per verificare le firme generate dalla tua chiave KMS asimmetrica. AWS

Se importi lo stesso materiale della chiave in chiavi KMS diverse nella stessa Regione AWS, anche queste chiavi sono interoperabili. Per creare chiavi KMS interoperabili in diversi formati, crea una chiave multiregionale con materiale chiave importato. Regioni AWS

Le chiavi di crittografia simmetriche non sono portatili né interoperabili

I testi cifrati simmetrici che produce non sono portatili o interoperabili. AWS KMS AWS KMS non pubblica il formato di testo cifrato simmetrico richiesto dalla portabilità e il formato potrebbe cambiare senza preavviso.

- AWS KMS non è in grado di decrittografare testi cifrati simmetrici crittografati all'esterno, anche se si utilizza materiale chiave importato. AWS
- AWS KMS non supporta la decrittografia di alcun testo cifrato AWS KMS simmetrico al di fuori di, anche se il testo cifrato è stato crittografato con una chiave KMS con AWS KMSmateriale chiave importato.
- Le chiavi KMS con lo stesso materiale della chiave importato non sono interoperabili. Il testo cifrato simmetrico che genera testo cifrato specifico per ogni chiave KMS. AWS KMS Questo formato di testo criptato garantisce che solo la chiave KMS che ha crittografato i dati possa decrittografarli.

Inoltre, non è possibile utilizzare AWS strumenti, come la crittografia lato client di Amazon S3 AWS Encryption SDKo Amazon S3, per decrittografare testi cifrati simmetrici. AWS KMS

Di conseguenza, non è possibile utilizzare chiavi con materiale chiave importato per supportare accordi di deposito di chiavi in cui una terza parte autorizzata con accesso condizionato

al materiale chiave possa decrittografare determinati testi cifrati all'esterno. AWS KMSPer supportare il deposito delle chiavi, utilizza il AWS Encryption SDK per crittografare il messaggio in una chiave indipendente da AWS KMS.

Sei responsabile della disponibilità e della durata

AWS KMS è progettato per garantire un'elevata disponibilità del materiale chiave importato. Tuttavia, AWS KMS non mantiene la durabilità del materiale chiave importato allo stesso livello del materiale chiave che AWS KMS genera. Per informazioni dettagliate, vedi Protezione del materiale della chiave importato.

Protezione del materiale della chiave importato

Il materiale della chiave importato è protetto durante il transito e a riposo. Prima di importare il materiale chiave, si crittografa (o «avvolge») il materiale chiave con la chiave pubblica di una coppia di chiavi RSA generata in moduli di sicurezza AWS KMS hardware (HSM) convalidati nell'ambito del programma di convalida dei moduli crittografici FIPS 140-2. Puoi crittografare il materiale della chiave direttamente con la chiave pubblica di wrapping oppure crittografare il materiale della chiave con una chiave simmetrica AES e quindi crittografare la chiave simmetrica AES con la chiave pubblica RSA.

Alla ricezione, AWS KMS decripta il materiale chiave con la chiave privata corrispondente in un AWS KMS HSM e lo cripta nuovamente con una chiave simmetrica AES che esiste solo nella memoria volatile dell'HSM. Il materiale della chiave non esce mai in testo normale dal modulo HSM. Viene decrittografato solo mentre è in uso e solo all'interno degli HSM. AWS KMS

L'uso della chiave KMS con il materiale della chiave importato è determinato esclusivamente dalle policy di controllo degli accessi che hai impostato sulla chiave KMS. Inoltre, puoi utilizzare alias e tag per identificare e controllare l'accesso alla chiave KMS. Puoi abilitare e disabilitare la chiave, visualizzare e modificare le sue proprietà e monitorarla utilizzando servizi come AWS CloudTrail.

Ciononostante, conserva solo la copia sicura del materiale della chiave. In cambio di questa ulteriore misura di controllo, l'utente è responsabile della durabilità e della disponibilità complessiva del materiale chiave importato. AWS KMS è progettato per garantire un'elevata disponibilità del materiale chiave importato. Tuttavia, AWS KMS non mantiene la durabilità del materiale chiave importato allo stesso livello del materiale chiave che AWS KMS genera.

Questa differenza di durabilità è significativa nei seguenti casi:

- Quando impostate una scadenza per il materiale chiave importato, AWS KMS elimina il materiale chiave dopo la sua scadenza. AWS KMS non elimina la chiave KMS o i relativi metadati. Puoi

creare un CloudWatch allarme Amazon che ti avvisa quando il materiale chiave importato si avvicina alla data di scadenza.

Non puoi eliminare il materiale chiave AWS KMS generato per una chiave KMS e non puoi impostare la scadenza del materiale AWS KMS chiave, sebbene sia possibile ruotarlo.

- Quando elimini manualmente il materiale chiave importato, AWS KMS elimina il materiale chiave ma non elimina la chiave KMS o i relativi metadati. La pianificazione dell'eliminazione di una chiave, invece, richiede un periodo di attesa compreso tra 7 e 30 giorni, trascorso il quale AWS KMS elimina permanentemente la chiave KMS, i relativi metadati e il materiale della chiave.
- Nell'improbabile eventualità che si verifichino determinati guasti a livello regionale AWS KMS (come una perdita totale di alimentazione), AWS KMS non è possibile ripristinare automaticamente il materiale chiave importato. Tuttavia, AWS KMS può ripristinare la chiave KMS e i relativi metadati.

È necessario conservare una copia del materiale chiave importato all'esterno di AWS un sistema controllato dall'utente. Ti consigliamo di archiviare una copia esportabile del materiale della chiave importato in un sistema di gestione delle chiavi, ad esempio un modulo HSM. Se il materiale della chiave importato viene eliminato o scade, la chiave KMS associata diventa inutilizzabile fino a quando non importi nuovamente lo stesso materiale della chiave. Se il materiale della chiave importato viene perso definitivamente, qualunque testo criptato crittografato con la chiave KMS è irrecuperabile.

Autorizzazioni per l'importazione del materiale della chiave

Per creare e gestire le chiave KMS con materiale della chiave importato, l'utente deve avere l'autorizzazione per le operazioni di questo processo. Puoi fornire le autorizzazioni `kms:GetParametersForImport`, `kms:ImportKeyMaterial`, e `kms:DeleteImportedKeyMaterial` nella policy delle chiavi quando crei la chiave KMS. Nella AWS KMS console, queste autorizzazioni vengono aggiunte automaticamente per gli amministratori chiave quando si crea una chiave con un'origine materiale esterna.

Per creare chiavi KMS con materiale della chiave importato, il principale richiede le seguenti autorizzazioni.

- kms: CreateKey (politica IAM)
  - Per limitare questa autorizzazione alle chiavi KMS con materiale chiave importato, utilizza la condizione kms: KeyOrigin policy con un valore di. `EXTERNAL`

```
{
```

```
  "Sid": "CreateKMSKeysWithoutKeyMaterial",
  "Effect": "Allow",
  "Resource": "*",
  "Action": "kms:CreateKey",
  "Condition": {
    "StringEquals": {
      "kms:KeyOrigin": "EXTERNAL"
    }
  }
}
```

- kms: GetParametersForImport (Politica chiave o politica IAM)
  - Per limitare questa autorizzazione alle richieste che utilizzano un particolare algoritmo di wrapping e una specifica chiave di wrapping, utilizza le condizioni delle policy kms: WrappingAlgorithm e kms:. WrappingKeySpec
- kms: ImportKeyMaterial (Politica chiave o politica IAM)
  - Per consentire o vietare la scadenza del materiale chiave e controllare la data di scadenza, utilizza le condizioni delle politiche kms: ExpirationModel e kms:. ValidTo

Per reimportare il materiale chiave importato, il principale necessita delle autorizzazioni kms: e kms:. GetParametersForImport ImportKeyMaterial

Per eliminare il materiale chiave importato, il principale necessita dell'autorizzazione kms:. DeleteImportedKeyMaterial

Ad esempio, per dare a `KMSAdminRole` di esempio l'autorizzazione per gestire tutti gli aspetti di una chiave KMS con materiale chiave importato, includi una dichiarazione di policy delle chiavi come la seguente nella policy della chiave KMS.

```
{
  "Sid": "Manage KMS keys with imported key material",
  "Effect": "Allow",
  "Resource": "*",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/KMSAdminRole"
  },
  "Action": [
    "kms:GetParametersForImport",
    "kms:ImportKeyMaterial",
    "kms:DeleteImportedKeyMaterial"
  ]
```

```
}
```

Requisiti per il materiale della chiave importato

Il materiale della chiave importato deve essere compatibile con le specifiche chiave della chiave KMS associata. Per le coppie di chiavi asimmetriche, importa solo la chiave privata della coppia. AWS KMS ricava la chiave pubblica dalla chiave privata.

AWS KMS supporta le seguenti specifiche chiave per le chiavi KMS con materiale chiave importato. Nelle regioni cinesi, il materiale della chiave importato è supportato solo per le specifiche della chiave SYMMETRIC_DEFAULT.

Specifiche della chiave KMS	Requisiti del materiale della chiave
Chiavi di crittografia simmetrica SYMMETRIC_DEFAULT	256 bit (32 byte) di dati binari Nelle regioni cinesi, devono essere dati binari a 128 bit (16 byte).
Chiavi HMAC HMAC_224 HMAC_256 HMAC_384 HMAC_512	Il materiale della chiave HMAC deve essere conforme alla RFC 2104. La lunghezza della chiave deve corrispondere alla lunghezza specificata dalle specifiche della chiave.
Chiave privata asimmetrica RSA RSA_2048 RSA_3072 RSA_4096	La chiave privata asimmetrica RSA importata deve far parte di una coppia di chiavi conforme alla RFC 3447. Modulo: 2048 bit, 3072 bit o 4096 bit Numero di numeri primi: 2 (le chiavi RSA con più numeri primi non sono supportate) Il materiale della chiave asimmetrica deve essere codificato BER o DER nel formato

Specifiche della chiave KMS	Requisiti del materiale della chiave
	Public-Key Cryptography Standards (PKCS) #8 conforme allaRFC 5208.
Chiave privata asimmetrica a curva ellittica ECC_NIST_P256 (secp256r1) ECC_NIST_P384 (secp384r1) ECC_NIST_P521 (secp521r1) ECC_SECG_P256K1 (secp256k1)	La chiave privata asimmetrica RSA importata deve far parte di una coppia di chiavi conforme alla RFC 5915. Curva: NIST P-256, NIST P-384, NIST P-521 o Secp256k1 Parametri: solo curve denominate (le chiavi ECC con parametri espliciti vengono rifiutate) Coordinate pubbliche dei punti: possono essere compresse, non compresse o proiettive Il materiale della chiave asimmetrica deve essere codificato BER o DER nel formato Public-Key Cryptography Standards (PKCS) #8 conforme allaRFC 5208.

Gestione del materiale della chiave importato

Questi argomenti spiegano come importare e reimportare il materiale della chiave in una chiave KMS e come creare materiale della chiave importato che scade automaticamente.

Argomenti

- Panoramica dell'importazione del materiale della chiave
- Reimportazione del materiale della chiave
- Identificazione delle chiavi KMS con il materiale della chiave importato
- Creazione di un CloudWatch avviso di scadenza del materiale chiave importato
- Eliminazione del materiale della chiave importato
- Eliminazione di una chiave KMS con il materiale della chiave importato

Panoramica dell'importazione del materiale della chiave

La seguente panoramica illustra come importare il materiale della chiave in AWS KMS. Per ulteriori dettagli su ogni fase del processo, consulta l'argomento corrispondente.

1. Crea una chiave KMS senza materiale della chiave: l'origine deve essere `EXTERNAL`. Un'origine chiave di `EXTERNAL` indica che la chiave è progettata per il materiale chiave importato e AWS KMS impedisce la generazione di materiale chiave per la chiave KMS. In una fase successiva importerai il tuo materiale della chiave in questa chiave KMS.

   Il materiale chiave che importate deve essere compatibile con le specifiche chiave della chiave associata. AWS KMS Per ulteriori informazioni sulla compatibilità, consulta the section called “Requisiti per il materiale della chiave importato”.

2. Scarica la chiave pubblica di wrapping e il token di importazione: dopo aver completato la fase 1, scarica una chiave pubblica di wrapping e un token di importazione. Questi articoli proteggono il materiale chiave durante l'importazione. AWS KMS

   In questa fase, scegli il tipo ("specifica chiave") della chiave di wrapping RSA e l'algoritmo di wrapping che utilizzerai per la crittografia dei dati in transito in AWS KMS. Puoi scegliere una specifica della chiave di wrapping e un algoritmo della chiave di wrapping diversi ogni volta che importi o reimporti lo stesso materiale della chiave.

3. Decripta il materiale della chiave: usa la chiave pubblica di wrapping che hai scaricato nella fase 2 per crittografare il materiale della chiave che hai creato sul tuo sistema.

4. Importa il materiale chiave – Carica il materiale della chiave crittografato che hai creato nella fase 3 e il token di importazione che hai scaricato nella fase 2.

   In questa fase, puoi impostare una scadenza facoltativa. Quando il materiale chiave importato scade, lo AWS KMS elimina e la chiave KMS diventa inutilizzabile. Per continuare a utilizzare la chiave KMS, devi importare nuovamente lo stesso materiale della chiave.

   Quando l'operazione di importazione viene completata correttamente, lo stato della chiave della chiave KMS cambia da `PendingImport` a `Enabled`. ora, puoi utilizzare la chiave KMS nelle operazioni di crittografia.

AWS KMS registra una voce nel AWS CloudTrail registro quando si crea la chiave KMS, si scarica la chiavepubblica di wrapping e si importa il token e si importa il materiale chiave. AWS KMS registra

anche una voce quando si elimina materiale chiave importato o quando si AWS KMS elimina materiale chiave scaduto.

Reimportazione del materiale della chiave

Se gestisci una chiave KMS con materiale chiave importato, potresti dover reimportare il materiale della chiave. Puoi reimportare il materiale della chiave per sostituire il materiale della chiave in scadenza o eliminato oppure per modificare il modello di scadenza o la data di scadenza del materiale.

Quando importi materiale della chiave in una chiave KMS, la chiave KMS viene associata in modo permanente a quel materiale della chiave. Puoi importare nuovamente lo stesso materiale della chiave, ma non puoi importare materiale della chiave diverso in quella chiave KMS. Non puoi ruotare il materiale della chiave e AWS KMS non può creare il materiale della chiave per una chiave KMS con materiale della chiave importato.

Puoi reimportare il materiale della chiave in qualsiasi momento e secondo qualsiasi pianificazione che soddisfi i requisiti di sicurezza. Non è necessario attendere che il materiale della chiave sia scaduto o prossimo alla scadenza.

Per reimportare il materiale della chiave, attieniti alla stessa procedura utilizzata per importare il materiale della chiave la prima volta, con le seguenti eccezioni.

- Utilizzare una chiave KMS del servizio di gestione delle chiavi esistenti anziché creare una nuova chiave KMS del servizio di gestione delle chiavi. Puoi saltare la fase 1 della procedura di importazione.
- Quando si reimporta il materiale della chiave, è possibile modificare il modello di scadenza e la data di scadenza.

Ogni volta che importi materiale della chiave in una chiave KMS, devi scaricare e utilizzare una nuova chiave di wrapping e un nuovo token di importazione per la chiave KMS. La procedura di wrapping non influisce sul contenuto del materiale della chiave, per cui puoi utilizzare chiavi pubbliche di wrapping diverse e algoritmi di wrapping diversi per importare lo stesso materiale della chiave.

Identificazione delle chiavi KMS con il materiale della chiave importato

Quando crei una chiave KMS senza materiale della chiave, il valore della proprietà `Origin` della chiave KMS è `EXTERNAL` e non può essere modificato. A differenza dello stato della chiave, il valore `Origin` non dipende dalla presenza o dall'assenza di materiale chiave.

Puoi utilizzare il valore di origine `EXTERNAL` per identificare le chiavi KMS progettate per il materiale chiave importato. È possibile trovare l'origine della chiave nella AWS KMS console o utilizzando l'DescribeKeyoperazione. È inoltre possibile visualizzare le proprietà del materiale della chiave, ad esempio se e quando scade utilizzando la console o le API.

Per identificare le chiavi KMS del Servizio di gestione delle chiavi con il materiale chiave importato (console)

1. Apri la AWS KMS console all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, usa il selettore della regione nell'angolo in alto a destra della pagina.
3. Utilizza una delle seguenti tecniche per visualizzare la proprietà `Origin` delle chiavi KMS.
   - Per aggiungere una colonna Origin (Origine) alla tabella delle chiavi KMS, nell'angolo in alto a destra, scegliere l'icona delle impostazioni. Scegliere Origin (Origine) e quindi Confirm (Conferma). La colonna Origine semplifica l'identificazione delle chiavi KMS il cui valore della proprietà dell'origine è Esterna (Importa il materiale della chiave).
   - Per trovare il valore della proprietà `Origin` di una determinata chiave KMS, scegli l'alias o l'ID chiave della chiave KMS. Quindi seleziona la scheda Cryptographic configuration (Configurazione crittografica). Le schede sono sotto la sezione Configurazione generale.
4. Per visualizzare le informazioni dettagliate sul materiale chiave, scegli la scheda Materiale della chiave. Questa scheda viene visualizzata nella pagina prodotto solo per le chiavi KMS del Servizio di gestione delle chiavi con materiale importato.

Per identificare le chiavi KMS con materiale chiave importato (API)AWS KMS

Usa l'DescribeKeyoperazione. La risposta include l'`Origin` della chiave KMS, del modello di scadenza e della data di scadenza, come illustrato nell'esempio seguente.

```
$  aws kms describe-key --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
{
    "KeyMetadata": {
        "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "Origin": "EXTERNAL",
        "ExpirationModel": "KEY_MATERIAL_EXPIRES"
        "ValidTo": 2023-06-05T12:00:00+00:00,
        "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
```

```
        "AWSAccountId": "111122223333",
        "CreationDate": 2018-06-09T00:06:50.831000+00:00,
        "Enabled": false,
        "MultiRegion": false,
        "Description": "",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "KeyState": "PendingImport",
        "KeyManager": "CUSTOMER",
        "KeySpec": "SYMMETRIC_DEFAULT",
        "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "EncryptionAlgorithms": [
            "SYMMETRIC_DEFAULT"
        ]
    }
}
```

Creazione di un CloudWatch avviso di scadenza del materiale chiave importato

Puoi creare un CloudWatch avviso che ti avvisi quando il materiale chiave importato in una chiave KMS si avvicina alla scadenza. Ad esempio, l'allarme può avvisarti quando mancano meno di 30 giorni alla scadenza.

Quando importi il materiale della chiave in una chiave KMS, puoi specificare una data e un'ora in cui tale materiale scade. Quando il materiale chiave scade, AWS KMS elimina il materiale chiave e la chiave KMS diventa inutilizzabile. Per utilizzare di nuovo la chiave KMS, devi importare nuovamente lo stesso materiale della chiave. Tuttavia, se reimporti il materiale chiave prima della scadenza, è possibile evitare di interrompere i processi che utilizzano quella chiave KMS.

Questo allarme utilizza la `SecondsUntilKeyMaterialExpires`metrica AWS KMS pubblicata su CloudWatch per le chiavi KMS con materiale chiave importato che scade. Ogni allarme utilizza questo parametro per monitorare il materiale chiave importato per una determinata chiave KMS. Non puoi creare un singolo allarme per tutte le chiavi KMS con materiale chiave in scadenza o un allarme per le chiavi KMS che potresti creare in futuro.

Requisiti

Le seguenti risorse sono necessarie per un CloudWatch allarme che monitora la scadenza del materiale chiave importato.

- Una chiave KMS con materiale della chiave importato. Per assistenza, consulta Identificazione delle chiavi KMS con il materiale della chiave importato.

- Argomento Amazon SNS Per maggiori dettagli, consulta l'argomento Creating an Amazon SNS nella Amazon CloudWatch User Guide.

Creazione dell'allarme

Segui le istruzioni riportate in Creare un CloudWatch allarme basato su una soglia statica utilizzando i seguenti valori obbligatori. Per gli altri campi, accetta i valori predefiniti e immetti i nomi come richiesto.

Campo	Valore
Seleziona parametro	Scegli KMS, quindi scegli Per-Key Metrics (Parametri per chiave). Scegli la riga con la chiave KMS e il parametro `SecondsUntilKeyMaterialExpires` . Quindi, scegli Seleziona parametro. L'elenco Metrics (Parametri) visualizza il parametro `SecondsUntilKeyMaterialExpires` solo per le chiavi KMS con materiale della chiave importato. Se non disponi di chiavi KMS con queste proprietà nell'account e nella regione, questo elenco è vuoto.
Statistic	Minimo
Periodo	1 minuto
Tipo di soglia	Statico
Quando...	Ogni volta che *`nome della metrica`* è maggiore di 1

Eliminazione del materiale della chiave importato

È possibile eliminare il materiale chiave importato da una chiave KMS in qualsiasi momento. Inoltre, quando il materiale chiave importato con una data di scadenza scade, AWS KMS elimina il materiale chiave. In entrambi i casi, quando il materiale della chiave viene eliminato, lo stato chiave della chiave KMS diventa Importazione in attesa e la chiave KMS non può essere utilizzata in operazioni crittografiche fino a quando non importi nuovamente lo stesso materiale della chiave. (Non puoi importare altro materiale della chiave nella chiave KMS.)

Oltre alla disabilitazione della chiave KMS e alla revoca delle autorizzazioni, l'eliminazione del materiale della chiave può essere utilizzata come strategia per interrompere rapidamente, ma temporaneamente, l'uso della chiave KMS. Al contrario, la pianificazione dell'eliminazione di una chiave KMS con il materiale della chiave importato interrompe rapidamente anche l'uso della chiave KMS. Tuttavia, se l'eliminazione non viene annullata durante il periodo di attesa, la chiave KMS, il materiale della chiave e tutti i metadati della chiave vengono eliminati definitivamente. Per informazioni dettagliate, vedi the section called “Eliminazione di una chiave KMS con il materiale della chiave importato”.

Per eliminare il materiale chiave, puoi utilizzare la AWS KMS console o il funzionamento dell'DeleteImportedKeyMaterialAPI. AWS KMS registra una voce nel AWS CloudTrail registro quando si elimina materiale chiave importato e quando siAWS KMS elimina materiale chiave scaduto.

Argomenti

- In che modo l'eliminazione di materiale chiave influisce sui servizi AWS
- Eliminare il materiale della chiave (console)
- Elimina il materiale chiave (API)AWS KMS

In che modo l'eliminazione di materiale chiave influisce sui servizi AWS

Quando elimini il materiale della chiave, la chiave KMS diventa immediatamente inutilizzabile (in base alla coerenza finale). Tuttavia, le risorse crittografate con chiavi di dati protette dalla chiave KMS non sono interessate fino a quando la chiave KMS non viene nuovamente utilizzata, ad esempio per decrittografare la chiave dati. Questo problema riguarda Servizi AWS, molti dei quali utilizzano chiavi di dati per proteggere le risorse. Per informazioni dettagliate, vedi In che modo le chiavi KMS inutilizzabili influiscono sulle chiavi dati.

Eliminare il materiale della chiave (console)

È possibile utilizzare il AWS Management Console per eliminare il materiale chiave.

1. Accedi AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare il Regione AWS, usa il selettore della regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.
4. Esegui una di queste operazioni:

- Seleziona la casella di controllo di una chiave KMS con materiale chiave importato. Scegliere Key actions (Operazioni della chiave), Delete key material (Elimina materiale della chiave).
- Scegli l'alias o l'ID chiave di una chiave KMS con materiale chiave importato. Scegli la tab Materiale chiave e quindi scegli Elimina materiale chiave.

5. Confermare che si intende eliminare il materiale della chiave, quindi selezionare Delete key material (Elimina materiale chiave). Lo stato della chiave KMS, che corrisponde al relativo stato di chiave, diventa In attesa di importazione.

Elimina il materiale chiave (API)AWS KMS

Per utilizzare l'AWS KMS API per eliminare il materiale chiave, invia una DeleteImportedKeyMaterialrichiesta. L'esempio seguente mostra come eseguire questa operazione con l'AWS CLI.

Sostituisci *1234abcd-12ab-34cd-56ef-1234567890ab* con l'ID chiave della chiave KMS il cui materiale desideri eliminare. Puoi utilizzare l'ID chiave o l'ARN della chiave KMS, mentre non puoi utilizzare un alias per questa operazione.

```
$ aws kms delete-imported-key-material --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

Eliminazione di una chiave KMS con il materiale della chiave importato

L'eliminazione del materiale della chiave di una chiave KMS con il materiale della chiave importato è temporanea e reversibile. Per ripristinare la chiave, reimporta il materiale della chiave.

Al contrario, l'eliminazione di una chiave KMS è irreversibile. Se pianifichi l'eliminazione delle chiavi e il periodo di attesa richiesto scade, elimina AWS KMS in modo permanente e irreversibile la chiave KMS, il relativo materiale chiave e tutti i metadati associati alla chiave KMS.

Tuttavia, il rischio e le conseguenze dell'eliminazione di una chiave KMS con materiale della chiave importato dipendono dal tipo ("specifica chiave") di chiave KMS.

- Chiavi di crittografia simmetrica: se elimini una chiave KMS di crittografia simmetrica, tutto il testo criptato rimanente crittografati da tale chiave sarà irrecuperabile. Non puoi creare una nuova chiave KMS di crittografia simmetrica in grado di decrittografare i testi criptati di una chiave KMS di crittografia simmetrica eliminata, neppure se disponi dello stesso materiale della chiave. I metadati univoci di ogni chiave KMS sono associati crittograficamente a ogni testo criptato simmetrico.

Questa funzionalità di sicurezza garantisce che solo la chiave KMS che ha crittografato il testo criptato simmetrico possa decrittografarlo, ma impedisce di ricreare una chiave KMS equivalente.

- Chiavi asimmetriche e HMAC: se disponi del materiale chiave originale, puoi creare una nuova chiave KMS con le stesse proprietà crittografiche di una chiave KMS asimmetrica o HMAC che è stata eliminata. AWS KMS genera firme e testi cifrati RSA standard, firme ECC e tag HMAC, che non includono funzionalità di sicurezza esclusive. Inoltre, puoi utilizzare una chiave HMAC o la chiave privata di una coppia di chiavi asimmetrica esternamente a AWS.

  Una nuova chiave KMS creata con lo stesso materiale della chiave asimmetrica o HMAC avrà un identificatore della chiave diverso. Dovrai creare una nuova policy della chiave, creare nuovamente eventuali alias e aggiornare le concessioni e le policy IAM esistenti in modo che facciano riferimento alla nuova chiave.

Importazione del materiale della chiave - Fase 1: creare una AWS KMS key senza materiale chiave

Per impostazione predefinita, quando crei una chiave KMS, AWS KMS crea automaticamente il materiale della chiave. Per importare invece il materiale della propria chiave, avvia creando una chiave KMS senza materiale chiave. Quindi, importare il materiale chiave. Per creare una chiave KMS senza materiale chiave, usa la AWS KMS console o l'CreateKeyoperazione.

Per creare una chiave senza materiale della chiave, specifica un'origine `EXTERNAL`. La proprietà dell'origine di una chiave KMS è immutabile. Una volta creato, non è possibile convertire una chiave KMS progettata per il materiale chiave importato in una chiave KMS con materiale chiave da AWS KMS o da qualsiasi altra fonte.

Lo stato della chiave di una chiave KMS con un origine `EXTERNAL` e nessun materiale chiave è `PendingImport`. Una chiave KMS può rimanere in uno stato `PendingImport` indefinitamente. Tuttavia, non puoi utilizzare una chiave KMS in stato `PendingImport` in operazioni crittografiche. Quando importi il materiale della chiave, lo stato della chiave KMS diventa `Enabled` e puoi utilizzarla in operazioni crittografiche.

AWS KMSregistra un evento nel AWS CloudTrail registro quando si crea la chiave KMS, si scarica la chiave pubblica, si importa il token e si importa il materiale chiave. AWS KMSregistra anche un CloudTrail evento quando si elimina materiale chiave importato o quando si AWS KMS elimina materiale chiave scaduto.

Per ulteriori informazioni sulla creazione di chiavi multiregione con materiale della chiave importato, consulta Importazione di materiale chiave in chiavi multiregione.

Argomenti

- Creazione di una chiave KMS senza materiale della chiave (console)
- Creazione di una chiave KMS senza materiale chiave (API AWS KMS)

Creazione di una chiave KMS senza materiale della chiave (console)

Devi solo creare una sola volta una chiave KMS per il materiale della chiave importato. Puoi importare e reimportare quando vuoi lo stesso materiale della chiave nella chiave KMS, ma non puoi importare materiale della chiave diverso in una chiave KMS. Per informazioni dettagliate, vedi Fase 2: download della chiave pubblica di wrapping e del token di importazione.

Per trovare le chiavi KMS esistenti con materiale della chiave importato nella tabella Customer managed keys (Chiavi gestite dal cliente), utilizza l'icona a forma di ingranaggio nell'angolo in alto a destra per mostrare la colonna Origin (Origine) nell'elenco delle chiavi KMS. Il valore di Origine per le chiavi importate è Esterna (Importa il materiale della chiave).

Per creare una chiave KMS con il materiale della chiave importato, inizia seguendo le istruzioni basilari per creare una chiave KMS del tipo preferito, con l'eccezione indicata di seguito.

Una volta scelto l'utilizzo della chiave, effettua le seguenti operazioni:

1. Espandere Advanced options (Opzioni avanzate).
2. In Key material origin (Origine del materiale della chiave), seleziona External (Import key material) (Esterna (Importa materiale della chiave)).
3. Scegli la casella di controllo accanto a Comprendo le implicazioni in termini di sicurezza e durabilità derivanti dall'utilizzo di una chiave importata) per confermare di aver compreso le implicazioni dell'utilizzo del materiale della chiave importato. Per leggere queste implicazioni, consulta Protezione del materiale della chiave importato.
4. Torna alle istruzioni basilari. Le fasi rimanenti della procedura basilare sono identici per tutte le chiavi KMS di tale tipo.

Quando scegli Fine, hai creato una chiave KMS senza materiale della chiave con lo stato (stato chiave) Importazione in attesa.

Tuttavia, invece di tornare alla tabella delle Chiavi gestite dal cliente, la console visualizza una pagina in cui puoi scaricare la chiave pubblica e importare il token necessario per l'importazione del materiale della chiave. A questo punto, puoi continuare con la fase di download o scegliere Annulla per fermarti a questo punto. Puoi tornare a questa fase di download in qualunque momento.

Successivo: Fase 2: download della chiave pubblica di wrapping e del token di importazione.

Creazione di una chiave KMS senza materiale chiave (API AWS KMS)

Per utilizzare l'AWS KMSAPI per creare una chiave KMS di crittografia simmetrica senza materiale chiave, invia una CreateKeyrichiesta con il parametro impostato su. `Origin` `EXTERNAL` L'esempio seguente mostra come eseguire questa operazione con l'AWS Command Line Interface (AWS CLI).

```
$ aws kms create-key --origin EXTERNAL
```

Se il comando viene eseguito correttamente, verrà visualizzato un output simile al seguente. L'`Origin` della chiave AWS KMS è `EXTERNAL` e il suo `KeyState` è `PendingImport`.

> **Tip**
>
> Se l'esito del comando non è positivo, potresti visualizzare un'`KMSInvalidStateException` o un'`NotFoundException`. Puoi ritentare la richiesta.


```
{
    "KeyMetadata": {
        "Origin": "EXTERNAL",
        "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "Description": "",
        "Enabled": false,
        "MultiRegion": false,
        "KeyUsage": "ENCRYPT_DECRYPT",
        "KeyState": "PendingImport",
        "CreationDate": 1568289600.0,
        "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "AWSAccountId": "111122223333",
        "KeyManager": "CUSTOMER",
        "KeySpec": "SYMMETRIC_DEFAULT",
        "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
```

```
        "EncryptionAlgorithms": [
            "SYMMETRIC_DEFAULT"
        ]
    }
}
```

Copia il valore `KeyId` dall'output del comando per utilizzarlo in un secondo momento, quindi passa a Fase 2: download della chiave pubblica di wrapping e del token di importazione.

> **Note**
>
> Questo comando crea una chiave KMS di crittografia simmetrica con `KeySpec` `SYMMETRIC_DEFAULT` e `KeyUsage` `ENCRYPT_DECRYPT`. Puoi utilizzare i parametri opzionali `--key-spec` e `--key-usage` per creare una chiave KMS HMAC o asimmetrica. Per maggiori informazioni, vedi l'operazione CreateKey.

Fase 2 dell'importazione del materiale della chiave: scaricare la chiave pubblica di wrapping e il token di importazione

Dopo aver creato un materiale AWS KMS key senza chiave, scarica una chiave pubblica di wrapping RSA e un token di importazione per quella chiave KMS utilizzando la AWS KMS console o l'API. GetParametersForImport La chiave pubblica di wrapping e il token di importazione costituiscono due elementi di un set indivisibile che devono essere usati assieme.

Utilizzerai la chiave pubblica di wrapping per crittografare il materiale della chiave per il trasporto. Prima del download, seleziona la lunghezza (specifica chiave) della coppia di chiavi di wrapping RSA e l'algoritmo di wrapping che utilizzerai per crittografare il materiale della chiave importato per il trasporto nella fase 3.

Ogni set di chiave pubblica di wrapping e token di importazione è valido per 24 ore. Se non lo utilizzi per importare il materiale della chiave entro 24 ore dal download, devi scaricare un nuovo set. Puoi scaricare set con una nuova chiave pubblica di wrapping e token di importazione in qualunque momento. Ciò consente di modificare la lunghezza della chiave di wrapping RSA ("specifica chiave") o di sostituire un set perso.

Puoi importare un set con chiave pubblica di wrapping e token di importazione anche per importare nuovamente lo stesso materiale della chiave in una chiave KMS. Puoi eseguire questa operazione

per importare o modificare la data di scadenza del materiale della chiave o per ripristinare materiale della chiave scaduto o eliminato. Devi scaricare e crittografare nuovamente il materiale della chiave ogni volta che lo importi in AWS KMS.

Utilizzo della chiave pubblica di wrapping

Il download include una chiave pubblica univoca per il tuo Account AWS, denominata anche chiave pubblica di wrapping.

Prima di importare il materiale della chiave, esegui la crittografia del materiale della chiave con la chiave pubblica di wrapping e carica il materiale della chiave crittografata in AWS KMS. Quando AWS KMS riceve il materiale della chiave crittografata, lo decripta con la chiave privata corrispondente, quindi esegue nuovamente la crittografia del materiale della chiave con una chiave simmetrica AES, tutto in un modulo di sicurezza hardware (HSM) AWS KMS.

Utilizzo dei token di importazione

Il download include un token di importazione con i metadati che assicura che il materiale della chiave sia stato importato correttamente. Quando carichi il materiale della chiave crittografata in AWS KMS, devi caricare lo stesso token di importazione scaricato in questa fase.

Selezione di una specifica della chiave pubblica di wrapping

Per proteggere il materiale della chiave durante l'importazione, devi crittografarlo utilizzando la chiave pubblica di wrapping scaricata da AWS KMS e un algoritmo di wrapping supportato. Seleziona una specifica chiave prima di scaricare la chiave pubblica di wrapping e il token di importazione. Tutte le coppie di chiavi di wrapping vengono generate in moduli di sicurezza hardware (HSM) AWS KMS. La chiave non esce mai dal modulo HSM in testo semplice.

Le specifiche chiave della chiave pubblica di wrapping determinano la lunghezza delle chiavi nella coppia di chiavi RSA che protegge il materiale della chiave durante il trasporto in AWS KMS. In generale, consigliamo di utilizzare la chiave pubblica di wrapping più lunga possibile tale che sia pratica. Offriamo diverse specifiche della chiave pubblica di wrapping, per supportare svariati moduli HSM e gestori di chiavi.

AWS KMS supporta le seguenti specifiche della chiave per le chiavi di wrapping RSA utilizzate per importare materiale della chiave di tutti i tipi, ad eccezione di quanto indicato.

- RSA_4096 (preferito)

- RSA_3072
- RSA_2048

> **Note**
>
> La seguente combinazione NON è supportata: materiale della chiave ECC_NIST_P521, specifica della chiave di wrapping pubblica RSA_2048 e algoritmo di wrapping RSAES_OAEP_SHA_*.
> Non puoi eseguire il wrapping del materiale della chiave ECC_NIST_P521 direttamente con una chiave di wrapping pubblica RSA_2048. Usa una chiave di wrapping più grande o un algoritmo di wrapping RSA_AES_KEY_WRAP_SHA_*.

Selezione di un algoritmo di wrapping

Per proteggere il materiale della chiave durante l'importazione, crittografalo utilizzando la chiave pubblica di wrapping scaricata e un algoritmo di wrapping supportato.

AWS KMS supporta diversi algoritmi di wrapping RSA standard e un algoritmo di wrapping ibrido in due fasi. In generale, consigliamo di utilizzare l'algoritmo di wrapping più sicuro che sia compatibile con il materiale della chiave importato e con le specifiche della chiave di wrapping. Di solito, puoi scegliere un algoritmo che è supportato del modulo di sicurezza hardware (HSM) o del sistema di gestione delle chiavi che protegge il materiale della chiave.

La tabella seguente mostra gli algoritmi di wrapping supportati per ogni tipo di chiave KMS e materiale della chiave. Gli algoritmi sono elencati in ordine di preferenza.

Materiale chiave	Specifiche e algoritmo di wrapping supportati
Chiave di crittografia simmetrica Chiave AES a 256-bit Chiave SM4 a 128 bit (solo regioni cinesi)	Algoritmi di wrapping: RSAES_OAEP_SHA_256 RSAES_OAEP_SHA_1 Algoritmi di wrapping obsoleti: RASES_PKCS1_V1

Materiale chiave	Specifiche e algoritmo di wrapping supportati
	Note A partire dal 10 ottobre 2023, non AWS KMS supporta l'algoritmo di wrapping RSAES_PKCS1_V1_5. Specifiche della chiave di wrapping: RSA_2048 RSA_3072 RSA_4096
Chiave privata RSA asimmetrica	Algoritmi di wrapping: RSA_AES_KEY_WRAP_SHA_256 RSA_AES_KEY_WRAP_SHA_1 Specifiche della chiave di wrapping: RSA_2048 RSA_3072 RSA_4096

Materiale chiave	Specifiche e algoritmo di wrapping supportati
Chiave privata a curva ellittica asimmetrica (ECC) Non puoi utilizzare gli algoritmi di wrapping RSAES_OAEP_SHA_* con la specifica della chiave di wrapping RSA_2048 per eseguire il wrapping del materiale della chiave ECC_NIST_P521.	Algoritmi di wrapping: RSA_AES_KEY_WRAP_SHA_256 RSA_AES_KEY_WRAP_SHA_1 RSAES_OAEP_SHA_256 RSAES_OAEP_SHA_1 Specifiche della chiave di wrapping: RSA_2048 RSA_3072 RSA_4096
Chiave HMAC	Algoritmi di wrapping: RSAES_OAEP_SHA_256 RSAES_OAEP_SHA_1 Specifiche della chiave di wrapping: RSA_2048 RSA_3072 RSA_4096

- `RSA_AES_KEY_WRAP_SHA_256`: algoritmo di wrapping ibrido in due fasi che combina la crittografia del materiale della chiave con una chiave simmetrica AES generata da te, quindi la crittografia della chiave simmetrica AES con la chiave di wrapping pubblica RSA scaricata e l'algoritmo di wrapping RSAES_OAEP_SHA_256.

  Per il wrapping del materiale della chiave privata RSA di wrapping è necessario un algoritmo di wrapping RSA_AES_KEY_WRAP_SHA_*.

- `RSA_AES_KEY_WRAP_SHA_1`: algoritmo di wrapping ibrido in due fasi che combina la crittografia del materiale della chiave con una chiave simmetrica AES generata da te, quindi la crittografia della chiave simmetrica AES con la chiave pubblica di wrapping RSA scaricata e l'algoritmo di wrapping RSAES_OAEP_SHA_1.

  Per il wrapping del materiale della chiave privata RSA di wrapping è necessario un algoritmo di wrapping `RSA_AES_KEY_WRAP_SHA_*`.
- `RSAES_OAEP_SHA_256`: l'algoritmo di crittografia RSA con Optimal Asymmetric Encryption Padding (OAEP) con la funzione hash SHA-256.
- `RSAES_OAEP_SHA_1`: l'algoritmo di crittografia RSA con Optimal Asymmetric Encryption Padding (OAEP) con la funzione hash SHA-1.
- `RSAES_PKCS1_V1_5` (obsoleto; dal 10 ottobre 2023; AWS KMS non supporta l'algoritmo di wrapping RSAES_PKCS1_V1_5): algoritmo di crittografia RSA con il formato di riempimento definito in PKCS #1 versione 1.5.

Argomenti

Download della chiave pubblica di wrapping e del token di importazione (console)

Puoi utilizzare la console AWS KMS, per scaricare la chiave pubblica di wrapping e il token di importazione.

1. Se hai appena completato la procedura per creare una chiave KMS senza materiale chiave e ti trovi sulla pagina Scarica la chiave di wrapping e il token di importazione, passa a Step 9.
2. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
3. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
4. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.

> **Tip**
>
> Puoi importare il materiale della chiave solo in una chiave KMS con Origine Esterna (Importa il materiale della chiave). Ciò indica che la chiave KMS è stata

creata senza materiale chiave. Per aggiungere una colonna Origin (Origine) alla tabella, nell'angolo in alto a destra della pagina scegliere l'icona delle impostazioni (). Attivare l'origine in Origine (Origine), quindi scegliere Confirm (Conferma).

5. Scegli l'alias o l'ID chiave della chiave KMS che è in attesa di importazione.
6. Scegli la tab Configurazione crittografica e visualizzane i valori. Le tab si trovano nella sezione Configurazione generale.

   Puoi importare il materiale della chiave solo in chiavi KMS con Origine Esterna (Importa il materiale della chiave). Per ulteriori informazioni sulla creazione di chiavi KMS con materiale chiave importato, consulta Importazione di materiale chiave per le AWS KMS chiavi.
7. Scegli la scheda Materiale della chiave, quindi scegli Importa il materiale della chiave.

   La scheda Materiale della chiave viene visualizzata solo per le chiavi KMS simmetriche il cui valore Origine è Esterna (Importa il materiale della chiave).
8. Per Seleziona le specifiche della chiave di wrapping, scegli la configurazione per la tua chiave KMS. Dopo aver creato questa chiave, non puoi modificare le specifiche della chiave.
9. In Select wrapping algorithm (Seleziona algoritmo di wrapping), scegliere l'opzione da utilizzare per crittografare il materiale della chiave. Per ulteriori informazioni sulle opzioni, consulta Selezione di un algoritmo di wrapping.
10. Scegli Scarica la chiave pubblica di wrapping e il token di importazione), quindi salva il file.

    Se è presente un'opzione Next (Successivo), per continuare il processo ora scegliere Next (Successivo). Per continuare in un secondo momento, scegliere Cancel (Annulla).
11. Decomprimere il file `.zip` salvato nella fase precedente (`Import_Parameters_<key_id>_<timestamp>`).

    La cartella contiene i file seguenti:

    - Una chiave pubblica di wrapping RSA in un file denominato `WrappingPublicKey.bin`.
    - Un token di importazione in un file denominato `ImportToken.bin`.
    - Un file di testo denominato README.txt. Questo file contiene informazioni sulla chiave pubblica di wrapping, l'algoritmo di wrapping da utilizzare per crittografare il materiale della chiave e la data e l'ora in cui di scadenza della chiave pubblica di wrapping e del token di importazione.

12. Per continuare il processo, crittografare il materiale della chiave.

Download della chiave pubblica di wrapping e del token di importazione (API AWS KMS)

Per scaricare la chiave pubblica e importare il token, utilizza l'API. GetParametersForImport Specifica la chiave KMS che verrà associata al materiale della chiave importato. Questa chiave KMS deve avere un valore di origine pari a `EXTERNAL`.

Questo esempio specifica l'algoritmo di wrapping `RSA_AES_KEY_WRAP_SHA_256`, la specifica della chiave pubblica di wrapping RSA_3072 e un esempio di ID chiave. Sostituisci questi valori di esempio con valori validi per il download. Per l'ID della chiave puoi utilizzare l'ID della chiave o l'ARN della chiave, ma non puoi utilizzare un nome alias o l'ARN alias in questa operazione.

```
$ aws kms get-parameters-for-import \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --wrapping-algorithm RSA_AES_KEY_WRAP_SHA_256 \
    --wrapping-key-spec RSA_3072
```

Se il comando viene eseguito correttamente, verrà visualizzato un output simile al seguente:

```
{
    "ParametersValidTo": 1568290320.0,
    "PublicKey": "public key (base64 encoded)",
    "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "ImportToken": "import token (base64 encoded)"
}
```

Per preparare i dati per il passaggio successivo, base64 decodifica la chiave pubblica e il token di importazione e salva i valori decodificati nei file.

Perché base64 decodifichi la chiave pubblica e importi il token:

1. Copia la chiave pubblica codificata in base64 (rappresentata dalla *chiave pubblica (codificata in base64* nell'output di esempio), incollala in un nuovo file, quindi salva il file. Assegna al file un nome descrittivo, ad esempio `PublicKey.b64`.

2. Utilizza OpenSSL per decodificare su base64 il contenuto del file e salvare i dati decodificati in un nuovo file. L'esempio seguente decodifica i dati nel file salvato nel passaggio precedente (`PublicKey.b64`) e salva l'output in un nuovo file con nome `WrappingPublicKey.bin`.

```
$ openssl enc -d -base64 -A -in PublicKey.b64 -out WrappingPublicKey.bin
```

3. Copia il token di importazione codificato in base64 (rappresentato dal *`token di importazione (codificato in base64)`* nell'output di esempio), incollalo in un nuovo file, quindi salva il file. Assegna al file un nome descrittivo, ad esempio `importtoken.b64`.
4. Utilizza OpenSSL per decodificare su base64 il contenuto del file e salvare i dati decodificati in un nuovo file. L'esempio seguente decodifica i dati nel file salvato nel passaggio precedente (`ImportToken.b64`) e salva l'output in un nuovo file con nome `ImportToken.bin`.

```
$ openssl enc -d -base64 -A -in importtoken.b64 -out ImportToken.bin
```

Passa a Fase 3: crittografare il materiale delle chiavi.

Importazione del materiale delle chiavi Fase 3: crittografare il materiale delle chiavi

Dopo aver scaricato la chiave pubblica e il token di importazione, esegue la crittografia del materiale della chiave utilizzando la chiave pubblica scaricata e l'algoritmo di wrapping specificato. Se devi sostituire la chiave pubblica o il token di importazione oppure modificare l'algoritmo di wrapping, devi scaricare una nuova chiave pubblica e un nuovo token di importazione. Per informazioni sulle chiavi pubbliche e gli algoritmi di wrapping supportati da AWS KMS, consulta Selezione di una specifica della chiave pubblica di wrapping e Selezione di un algoritmo di wrapping.

Il materiale delle chiavi deve essere in formato binario. Per informazioni dettagliate, consulta Requisiti per il materiale della chiave importato.

> **Note**
>
> Per le coppie di chiavi asimmetriche, esegue la crittografia e importa solo la chiave privata: AWS KMS ricava la chiave pubblica dalla chiave privata.
> La seguente combinazione NON è supportata: materiale della chiave ECC_NIST_P521, specifica della chiave di wrapping pubblica RSA_2048 e algoritmo di wrapping RSAES_OAEP_SHA_*.

Non puoi eseguire il wrapping del materiale della chiave ECC_NIST_P521 direttamente con una chiave di wrapping pubblica RSA_2048. Usa una chiave di wrapping più grande o un algoritmo di wrapping RSA_AES_KEY_WRAP_SHA_*.

Di solito, è possibile crittografare il materiale delle chiavi quando viene esportato dal modulo di sicurezza hardware (HSM) o dal sistema di gestione delle chiavi. Per informazioni su come esportare il materiale delle chiavi in formato binario, consulta la documentazione per il tuo HSM o per il sistema di gestione delle chiavi. È anche possibile consultare la sezione seguente che fornisce un proof of concept sull'utilizzo di OpenSSL.

Quando crittografi il materiale della chiave, usa lo stesso algoritmo di wrapping specificato quando hai scaricato la chiave pubblica e il token di importazione. Per trovare l'algoritmo di wrapping che hai specificato, vedi l'evento di CloudTrail registro per la GetParametersForImportrichiesta associata.

Genera il materiale della chiave per i test

I comandi OpenSSL indicati di seguito generano il materiale della chiave di ogni tipo supportato per i test. Questi esempi vengono forniti solo a scopo di test e proof-of-concept dimostrazioni. Per i sistemi di produzione, usa un metodo più sicuro per generare e memorizzare il materiale della chiave, ad esempio un modulo di sicurezza hardware o un sistema di gestione delle chiavi.

Per convertire le chiavi private delle coppie di chiavi asimmetriche in formato con codifica DER, reindirizza il comando di generazione del materiale della chiave sul comando `openssl pkcs8` seguente. Il parametro `topk8` indica a OpenSSL di accettare una chiave privata come input e restituire una chiave in formato PKCS #8. (Il comportamento predefinito è l'opposto.)

```
openssl pkcs8 -topk8 -outform der -nocrypt
```

I comandi indicati di seguito generano il materiale della chiave per ogni tipo di chiave supportato.

- Chiavi di crittografia simmetrica (32 byte)

  Questo comando genera una chiave simmetrica a 256 bit (stringa casuale di 32 byte) e la salva nel file `PlaintextKeyMaterial.bin`. Non è necessario codificare questo materiale della chiave.

  ```
  openssl rand -out PlaintextKeyMaterial.bin 32
  ```

Solo nelle regioni cinesi, devi generare una chiave simmetrica a 128 bit (stringa casuale di 16 byte).

```
openssl rand -out PlaintextKeyMaterial.bin 16
```

- Chiavi HMAC

  Questo comando genera una stringa di byte casuale della dimensione specificata. Non è necessario codificare questo materiale della chiave.

  La lunghezza della chiave HMAC deve corrispondere alla lunghezza definita dalle specifiche della chiave KMS. Ad esempio, se la chiave KMS è HMAC_384, devi importare una chiave a 384 bit (48 byte).

```
openssl rand -out HMAC_224_PlaintextKey.bin 28

openssl rand -out HMAC_256_PlaintextKey.bin 32

openssl rand -out HMAC_384_PlaintextKey.bin 48

openssl rand -out HMAC_512_PlaintextKey.bin 64
```

- Chiavi private RSA

```
openssl genpkey -algorithm rsa -pkeyopt rsa_keygen_bits:2048 | openssl pkcs8 -topk8 -
outform der -nocrypt > RSA_2048_PrivateKey.der

openssl genpkey -algorithm rsa -pkeyopt rsa_keygen_bits:3072 | openssl pkcs8 -topk8 -
outform der -nocrypt > RSA_3072_PrivateKey.der

openssl genpkey -algorithm rsa -pkeyopt rsa_keygen_bits:4096 | openssl pkcs8 -topk8 -
outform der -nocrypt > RSA_4096_PrivateKey.der
```

- Chiavi private EEC

```
openssl genpkey -algorithm ec -pkeyopt ec_paramgen_curve:P-256 | openssl pkcs8 -topk8
 -outform der -nocrypt > ECC_NIST_P256_PrivateKey.der

openssl genpkey -algorithm ec -pkeyopt ec_paramgen_curve:P-384 | openssl pkcs8 -topk8
 -outform der -nocrypt > ECC_NIST_P384_PrivateKey.der
```

```
openssl genpkey -algorithm ec -pkeyopt ec_paramgen_curve:P-521 | openssl pkcs8 -topk8
 -outform der -nocrypt > ECC_NIST_P521_PrivateKey.der

openssl genpkey -algorithm ec -pkeyopt ec_paramgen_curve:secp256k1 | openssl pkcs8 -
topk8 -outform der -nocrypt > ECC_SECG_P256K1_PrivateKey.der
```

Esempio di crittografia del materiale della chiave con OpenSSL

Gli esempi seguenti descrivono l'utilizzo di OpenSSL per crittografare il materiale della chiave con la chiave pubblica scaricata.

> **Important**
>
> Questo esempio è solo una dimostrazione di proof of concept. Per i sistemi di produzione, utilizzare un metodo più sicuro (ad esempio un sistema di gestione delle chiavi commerciale o HSM) per generare e memorizzare il materiale delle chiavi.
> La seguente combinazione NON è supportata: materiale della chiave ECC_NIST_P521, specifica della chiave di wrapping pubblica RSA_2048 e algoritmo di wrapping RSAES_OAEP_SHA_*.
> Non puoi eseguire il wrapping del materiale della chiave ECC_NIST_P521 direttamente con una chiave di wrapping pubblica RSA_2048. Usa una chiave di wrapping più grande o un algoritmo di wrapping RSA_AES_KEY_WRAP_SHA_*.

RSAES_OAEP_SHA_1

AWS KMS supporta RSAES_OAEP_SHA_1 per chiavi di crittografia simmetriche (SYMMETRIC_DEFAULT), chiavi private a curva ellittica (ECC) e chiavi HMAC.

RSAES_OAEP_SHA_1 non è supportato per le chiavi private RSA. Inoltre, non puoi utilizzare una chiave di wrapping pubblica RSA_2048 con un algoritmo di wrapping RSAES_OAEP_SHA_* per eseguire il wrapping di una chiave privata ECC_NIST_P521 (secp521r1). Devi utilizzare una chiave di wrapping più grande o un algoritmo di wrapping RSA_AES_KEY_WRAP.

Nell'esempio seguente il materiale della chiave viene criptato con la chiave pubblica scaricata e l'algoritmo di wrapping RSAES_OAEP_SHA_1, quindi viene salvato nel file `EncryptedKeyMaterial.bin`.

In questo esempio:

- *WrappingPublicKey.bin* è il file che contiene la chiave pubblica di wrapping scaricata.
- *PlaintextKeyMaterial.bin* è il file che contiene il materiale della chiave da crittografare, ad esempio `PlaintextKeyMaterial.bin`, `HMAC_384_PlaintextKey.bin` o `ECC_NIST_P521_PrivateKey.der`.

```
$ openssl pkeyutl \
    -encrypt \
    -in PlaintextKeyMaterial.bin \
    -out EncryptedKeyMaterial.bin \
    -inkey WrappingPublicKey.bin \
    -keyform DER \
    -pubin \
    -pkeyopt rsa_padding_mode:oaep \
    -pkeyopt rsa_oaep_md:sha1
```

RSAES_OAEP_SHA_256

AWS KMS supporta RSAES_OAEP_SHA_256 per chiavi di crittografia simmetriche (SYMMETRIC_DEFAULT), chiavi private a curva ellittica (ECC) e chiavi HMAC.

RSAES_OAEP_SHA_256 non è supportato per le chiavi private RSA. Inoltre, non puoi utilizzare una chiave di wrapping pubblica RSA_2048 con un algoritmo di wrapping RSAES_OAEP_SHA_* per eseguire il wrapping di una chiave privata ECC_NIST_P521 (secp521r1). Devi utilizzare una chiave pubblica più grande o un algoritmo di wrapping RSA_AES_KEY_WRAP.

Nell'esempio seguente, il materiale della chiave viene criptato con la chiave pubblica scaricata e l'algoritmo di wrapping RSAES_OAEP_SHA_256, quindi viene salvato nel file `EncryptedKeyMaterial.bin`.

In questo esempio:

- *WrappingPublicKey.bin* è il file che contiene la chiave di wrapping pubblica scaricata. Se hai scaricato la chiave pubblica dalla console, questo file è denominato `wrappingKey_`*KMS key_key_ID_timestamp* (ad esempio `wrappingKey_f44c4e20-f83c-48f4-adc6-a1ef38829760_0809092909`).
- *PlaintextKeyMaterial.bin* è il file che contiene il materiale della chiave da crittografare, ad esempio `PlaintextKeyMaterial.bin`, `HMAC_384_PlaintextKey.bin` o `ECC_NIST_P521_PrivateKey.der`.

```
$ openssl pkeyutl \
    -encrypt \
    -in PlaintextKeyMaterial.bin \
    -out EncryptedKeyMaterial.bin \
    -inkey WrappingPublicKey.bin \
    -keyform DER \
    -pubin \
    -pkeyopt rsa_padding_mode:oaep \
    -pkeyopt rsa_oaep_md:sha256 \
    -pkeyopt rsa_mgf1_md:sha256
```

RSA_AES_KEY_WRAP_SHA_1

L'algoritmo di wrapping RSA_AES_KEY_WRAP_SHA_1 prevede due operazioni di crittografia.

1. Esegui la crittografia del materiale della chiave con una chiave simmetrica AES generata da te e un algoritmo di crittografia simmetrica AES.
2. Esegui la crittografia della chiave simmetrica AES che hai usato con la chiave pubblica che hai scaricato e l'algoritmo di wrapping RSAES_OAEP_SHA_1.

AWS KMS supporta algoritmi di wrapping RSA_AES_KEY_WRAP_SHA_* per tutti i tipi supportati di materiale della chiave importato e tutte le specifiche della chiave pubblica supportate. Gli algoritmi RSA_AES_KEY_WRAP_SHA_* sono gli unici algoritmi di wrapping supportati per il wrapping del materiale della chiave RSA.

L'algoritmo di wrapping RSA_AES_KEY_WRAP_SHA_1 richiede OpenSSL versione 3.x o versione successiva.

1. Genera una chiave di crittografia simmetrica AES a 256-bit

   Questo comando genera una chiave di crittografia simmetrica AES composta da 256 bit casuali e la salva nel file `aes-key.bin`

   ```
   # Generate a 32-byte AES symmetric encryption key
   $ openssl rand -out aes-key.bin 32
   ```

2. Esegui la crittografia del materiale della chiave con la chiave di crittografia simmetrica AES

   Questo comando esegue la crittografia del materiale chiave con la chiave di crittografia simmetrica AES e salva il materiale della chiave crittografato nel file `key-material-wrapped.bin`.

   In questo esempio di comando:

   - *`PlaintextKeyMaterial.bin`* è il file che contiene il materiale della chiave da importare, ad esempio `PlaintextKeyMaterial.bin`, `HMAC_384_PlaintextKey.bin`, `RSA_3072_PrivateKey.der` o `ECC_NIST_P521_PrivateKey.der`.
   - *`aes-key.bin`* è il file che contiene la chiave di crittografia simmetrica AES a 256 bit generata nel comando precedente.

   ```
   # Encrypt your key material with the AES symmetric encryption key
   $ openssl enc -id-aes256-wrap-pad \
           -K "$(xxd -p < aes-key.bin | tr -d '\n')" \
           -iv A65959A6 \
           -in PlaintextKeyMaterial.bin\
           -out key-material-wrapped.bin
   ```

3. Esegui la crittografia della chiave di crittografia simmetrica AES con la chiave pubblica

   Questo comando esegue la crittografia della chiave di crittografia simmetrica AES con la chiave pubblica scaricata e l'algoritmo di wrapping RSAES_OAEP_SHA_1, applica la codifica DER e la salva nel file `aes-key-wrapped.bin`.

   In questo esempio di comando:

   - *`WrappingPublicKey.bin`* è il file che contiene la chiave di wrapping pubblica scaricata. Se hai scaricato la chiave pubblica dalla console, questo file è denominato `wrappingKey_`*`KMS key_key_ID_timestamp`* (ad esempio `wrappingKey_f44c4e20-f83c-48f4-adc6-a1ef38829760_0809092909`).
   - *`aes-key.bin`* è il file che contiene la chiave di crittografia simmetrica AES a 256 bit generata nel primo comando in questa sequenza di esempi.

   ```
   # Encrypt your AES symmetric encryption key with the downloaded public key
   $ openssl pkeyutl \
   ```

```
    -encrypt \
    -in aes-key.bin \
    -out aes-key-wrapped.bin \
    -inkey WrappingPublicKey.bin \
    -keyform DER \
    -pubin \
    -pkeyopt rsa_padding_mode:oaep \
    -pkeyopt rsa_oaep_md:sha1 \
    -pkeyopt rsa_mgf1_md:sha1
```

4. Generare il file da importare

   Concatena il file con il materiale della chiave crittografato e il file con la chiave AES crittografata. Salvali nel file `EncryptedKeyMaterial.bin`, che è il file che importerai in Fase 4: importare il materiale delle chiavi.

   In questo esempio di comando:

   - *key-material-wrapped.bin* è il file che contiene il materiale della chiave crittografato.
   - *aes-key-wrapped.bin* è il file che contiene la chiave di crittografia AES crittografata.

```
# Combine the encrypted AES key and encrypted key material in a file
$ cat aes-key-wrapped.bin key-material-wrapped.bin > EncryptedKeyMaterial.bin
```

RSA_AES_KEY_WRAP_SHA_256

L'algoritmo di wrapping RSA_AES_KEY_WRAP_SHA_256 prevede due operazioni di crittografia.

1. Esegui la crittografia del materiale della chiave con una chiave simmetrica AES generata da te e un algoritmo di crittografia simmetrica AES.
2. Esegui la crittografia della chiave simmetrica AES che hai usato con la chiave pubblica che hai scaricato e l'algoritmo di wrapping RSAES_OAEP_SHA_256.

AWS KMS supporta algoritmi di wrapping RSA_AES_KEY_WRAP_SHA_* per tutti i tipi supportati di materiale della chiave importato e tutte le specifiche della chiave pubblica supportate. Gli algoritmi RSA_AES_KEY_WRAP_SHA_* sono gli unici algoritmi di wrapping supportati per il wrapping del materiale della chiave RSA.

L'algoritmo di wrapping RSA_AES_KEY_WRAP_SHA_256 richiede OpenSSL versione 3.x o versione successiva.

1. Genera una chiave di crittografia simmetrica AES a 256-bit

   Questo comando genera una chiave di crittografia simmetrica AES composta da 256 bit casuali e la salva nel file `aes-key.bin`

   ```
   # Generate a 32-byte AES symmetric encryption key
   $ openssl rand -out aes-key.bin 32
   ```

2. Esegui la crittografia del materiale della chiave con la chiave di crittografia simmetrica AES

   Questo comando esegue la crittografia del materiale chiave con la chiave di crittografia simmetrica AES e salva il materiale della chiave crittografato nel file `key-material-wrapped.bin`.

   In questo esempio di comando:

   - *`PlaintextKeyMaterial.bin`* è il file che contiene il materiale della chiave da importare, ad esempio `PlaintextKeyMaterial.bin`, `HMAC_384_PlaintextKey.bin`, `RSA_3072_PrivateKey.der` o `ECC_NIST_P521_PrivateKey.der`.
   - *`aes-key.bin`* è il file che contiene la chiave di crittografia simmetrica AES a 256 bit generata nel comando precedente.

   ```
   # Encrypt your key material with the AES symmetric encryption key
   $ openssl enc -id-aes256-wrap-pad \
           -K "$(xxd -p < aes-key.bin | tr -d '\n')" \
           -iv A65959A6 \
           -in PlaintextKeyMaterial.bin\
           -out key-material-wrapped.bin
   ```

3. Esegui la crittografia della chiave di crittografia simmetrica AES con la chiave pubblica

   Questo comando esegue la crittografia della chiave di crittografia simmetrica AES con la chiave pubblica scaricata e l'algoritmo di wrapping RSAES_OAEP_SHA_256, applica la codifica DER e la salva nel file `aes-key-wrapped.bin`.

   In questo esempio di comando:

- *WrappingPublicKey.bin* è il file che contiene la chiave di wrapping pubblica scaricata. Se hai scaricato la chiave pubblica dalla console, questo file è denominato `wrappingKey_`*KMS key_key_ID_timestamp* (ad esempio `wrappingKey_f44c4e20-f83c-48f4-adc6-a1ef38829760_0809092909`).
- *aes-key.bin* è il file che contiene la chiave di crittografia simmetrica AES a 256 bit generata nel primo comando in questa sequenza di esempi.

```
# Encrypt your AES symmetric encryption key with the downloaded public key
$ openssl pkeyutl \
    -encrypt \
    -in aes-key.bin \
    -out aes-key-wrapped.bin \
    -inkey WrappingPublicKey.bin \
    -keyform DER \
    -pubin \
    -pkeyopt rsa_padding_mode:oaep \
    -pkeyopt rsa_oaep_md:sha256 \
    -pkeyopt rsa_mgf1_md:sha256
```

4. Generare il file da importare

   Concatena il file con il materiale della chiave crittografato e il file con la chiave AES crittografata. Salvali nel file `EncryptedKeyMaterial.bin`, che è il file che importerai in Fase 4: importare il materiale delle chiavi.

   In questo esempio di comando:

   - *key-material-wrapped.bin* è il file che contiene il materiale della chiave crittografato.
   - *aes-key-wrapped.bin* è il file che contiene la chiave di crittografia AES crittografata.

```
# Combine the encrypted AES key and encrypted key material in a file
$ cat aes-key-wrapped.bin key-material-wrapped.bin > EncryptedKeyMaterial.bin
```

Passa a Fase 4: importare il materiale delle chiavi.

Importazione del materiale delle chiavi Fase 4: importare il materiale delle chiavi

Dopo aver crittografato il materiale della chiave, puoi importarlo per utilizzarlo con una AWS KMS key. Per importare il materiale della chiave, è possibile caricare il materiale della chiave crittografato da Fase 3: crittografare il materiale delle chiavi e il token di importazione scaricato in Fase 2: download della chiave pubblica di wrapping e del token di importazione. È necessario importare il materiale nella stessa chiave KMS che hai specificato quando hai scaricato la chiave pubblica e il token di importazione. Quando il materiale della chiave viene importato correttamente, lo stato chiave della chiave KMS diventa `Enabled`, per cui puoi utilizzare la chiave KMS in operazioni crittografiche.

Quando importi il materiale della chiave, puoi impostare un'ora di scadenza facoltativa per il materiale della chiave. Quando il materiale della chiave scade, AWS KMS elimina tale materiale e la chiave KMS diventa inutilizzabile. Per utilizzare la chiave KMS nelle operazioni di crittografia, devi importare nuovamente lo stesso materiale della chiave. Dopo aver importato il materiale della chiave, non potrai impostare, modificare o annullare la data di scadenza dell'importazione corrente. Per modificare questi valori, dovrai eliminare e reimportare lo stesso materiale della chiave.

Per importare materiale chiave, puoi utilizzare la AWS KMS console o l'ImportKeyMaterialAPI. Puoi utilizzare l'API direttamente facendo richieste HTTP oppure usando SDK AWS, AWS Command Line Interface o AWS Tools for PowerShell.

Quando si importa il materiale chiave, viene aggiunta una ImportKeyMaterialvoce al AWS CloudTrail registro per registrare l'`ImportKeyMaterial`operazione. La CloudTrail voce è la stessa sia che si utilizzi la AWS KMS console che l'AWS KMSAPI.

Impostazione di una data di scadenza (facoltativo)

Quando importi il materiale della chiave per la chiave KMS, puoi impostare facoltativamente una data e un'ora di scadenza per il materiale della chiave fino a 365 giorni dalla data di importazione. Quando il materiale della chiave importato scade, AWS KMS lo elimina. Questa azione modifica lo stato chiave della chiave KMS in `PendingImport`, impedendone l'utilizzo in qualsiasi operazione di crittografia. Per utilizzare la chiave KMS, devi reimportare una copia del materiale della chiave originale.

Garantire che il materiale della chiave importato scada frequentemente può aiutarti a soddisfare i requisiti normativi, ma comporta un ulteriore rischio per i dati crittografati con la chiave KMS. Fino a quando non reimporti una copia del materiale della chiave originale, la chiave KMS con il materiale della chiave scaduto è inutilizzabile e tutti i dati crittografati con essa sono inaccessibili.

Se per qualsiasi motivo non riesci a reimportare il materiale della chiave o se perdi il materiale della chiave originale, la chiave KMS è definitivamente inutilizzabile e i dati crittografati con essa non sono recuperabili.

Per ridurre questo rischio, assicurati che la copia del materiale della chiave importato sia accessibile e progetta un sistema per eliminare e reimportare il materiale della chiave prima che scada e interrompa il carico di lavoro AWS. Ti consigliamo di configurare un allarme per la scadenza del materiale della chiave importato, in modo da avere tutto il tempo necessario per reimportarlo prima che scada. È inoltre possibile utilizzare CloudTrail i registri per controllare le operazioni di importazione (e reimportazione) del materiale chiave e l'eliminazione del materiale chiave importato, nonché l'AWS KMSoperazione per eliminare il materiale chiave scaduto.

Non puoi importare un materiale della chiave diverso nella chiave KMS e AWS KMS non è in grado di ripristinare, recuperare o riprodurre il materiale della chiave eliminato. Invece di impostare una scadenza, puoi periodicamente eliminare e reimportare a livello di programmazione il materiale della chiave importato, tuttavia i requisiti per conservare una copia del materiale della chiave originale sono gli stessi.

Puoi determinare l'eventuale scadenza del materiale della chiave importato durante la sua importazione. Tuttavia, puoi attivare e disattivare la scadenza o impostare una nuova data di scadenza eliminando e reimportando il materiale della chiave. Utilizzate il `ExpirationModel` parametro di ImportKeyMaterialper attivare () e disattivare (`KEY_MATERIAL_EXPIRES`) la scadenza e il `ValidTo` parametro per impostare l'ora di scadenza. `KEY_MATERIAL_DOES_NOT_EXPIRE` Il tempo massimo è di 365 giorni dall'importazione dei dati. Sebbene non sia prevista una data minima, l'ora di scadenza deve essere successiva alla data corrente.

Importazione del materiale della chiave (console)

Per importare il materiale della chiave è possibile utilizzare la AWS Management Console.

1. Se ti trovi nella pagina Carica il materiale della chiave di wrapping, passa a Step 8.
2. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
3. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
4. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.
5. Scegli l'alias o l'ID chiave della chiave KMS per la quale hai scaricato il token di importazione e la chiave pubblica.

6. Scegli la tab Configurazione crittografica e visualizzane i valori. Le tab si trovano nella pagina dei dettagli di una chiave KMS sotto la sezione Configurazione generale.

   Puoi importare il materiale della chiave solo in chiavi KMS con Origine Esterna (Importa materiale chiave). Per ulteriori informazioni sulla creazione di chiavi KMS con materiale della chiave importato, consulta Importazione di materiale chiave per le AWS KMS chiavi.

7. Scegli la scheda Materiale della chiave, quindi scegli Importa il materiale della chiave. La scheda Materiale della chiave viene visualizzata solo per chiavi KMS il cui valore Origine è Esterna (Importa materiale chiave).

   Se hai scaricato il materiale della chiave, il token di importazione e hai crittografato il materiale della chiave, scegli Avanti.

8. Nella sezione Materiale della chiave crittografato e token di importazione, effettua le operazioni seguenti.

   a. In Materiale della chiave di wrapping, scegli Scegli file. Quindi caricare il file contenente il materiale delle chiave (crittografato) sottoposto a wrapping.

   b. In Token di importazione, sceglie Scegli file. Caricare il file contenente il token di importazione scaricato.

9. Nella sezione Choose an expiration option (Scegli un'opzione di scadenza) stabilire se il materiale della chiave scade. Per impostare una data e un'ora di scadenza, scegliere Key material expires (Il materiale chiave scade) e utilizzare il calendario per selezionare una data e un'ora. Puoi specificare una data fino a 365 giorni dalla data e dall'ora corrente.

10. Scegliere Upload key material (Carica materiale chiave).

Importazione del materiale chiave (API AWS KMS)

Per importare materiale chiave, utilizzate l'ImportKeyMaterialoperazione. Gli esempi seguenti utilizzano la AWS CLI, ma puoi usare anche qualsiasi linguaggio di programmazione supportato.

Per utilizzare questo esempio:

1. Sostituisci *1234abcd-12ab-34cd-56ef-1234567890ab* con l'ID chiave della chiave KMS specificata per il download della chiave pubblica e del token di importazione. Per identificare la chiave KMS utilizza l'ID chiave o l'ARN di chiave. Per questa operazione, non puoi utilizzare un nome alias o un ARN alias.

2. Sostituire *EncryptedKeyMaterial.bin* con il nome del file che contiene il materiale della chiave crittografato.
3. Sostituire *ImportToken.bin* con il nome del file che contiene il token di importazione.
4. Se desideri che il materiale della chiave importato abbia una scadenza, imposta il valore del parametro `expiration-model` sul valore predefinito, `KEY_MATERIAL_EXPIRES`, oppure ometti il parametro `expiration-model`. Quindi, sostituisci il valore del parametro `valid-to` con la data e l'ora in cui desideri che il materiale della chiave scada. La data e l'ora possono arrivare fino a 365 giorni dal momento della richiesta.

```
$ aws kms import-key-material --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --encrypted-key-material fileb://EncryptedKeyMaterial.bin \
    --import-token fileb://ImportToken.bin \
    --expiration-model KEY_MATERIAL_EXPIRES \
    --valid-to 2023-06-17T12:00:00-08:00
```

Se desideri che il materiale della chiave importato abbia una scadenza, imposta il valore del parametro `expiration-model` su `KEY_MATERIAL_DOES_NOT_EXPIRE` e ometti il parametro `valid-to` dal comando.

```
$ aws kms import-key-material --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --encrypted-key-material fileb://EncryptedKeyMaterial.bin \
    --import-token fileb://ImportToken.bin \
    --expiration-model KEY_MATERIAL_DOES_NOT_EXPIRE
```

> **Tip**
>
> Se l'esito del comando non è positivo, potresti visualizzare un'`KMSInvalidStateException` o un'`NotFoundException`. Puoi ritentare la richiesta.

store delle chiavi personalizzate

Un archivio delle chiavi è una posizione sicura in cui archiviare chiavi crittografiche. L'archivio chiavi predefinito in AWS KMS supporta inoltre metodi per la generazione e la gestione delle chiavi che contiene. Per impostazione predefinita, il materiale della chiave crittografica per le AWS KMS keys che crei in AWS KMS viene generato e protetto da moduli di sicurezza hardware (HSM), ovvero

moduli di crittografia convalidati con certificazione FIPS 140-2. Il materiale della chiave per le chiavi KMS esegue sempre la crittografia di HSM.

Tuttavia, se è necessario un controllo ancora maggiore dei moduli di protezione hardware, puoi creare un archivio delle chiavi personalizzate.

Un archivio delle chiavi personalizzate è un archivio delle chiavi logico all'interno di AWS KMS supportato da un gestore delle chiavi esterne al di fuori di AWS KMS di tua proprietà e gestione. Gli archivi delle chiavi personalizzate combinano l'interfaccia di gestione delle chiavi pratica e completa di AWS KMS con la capacità di possedere e controllare il materiale della chiave e le operazioni di crittografia. Quando utilizzi una chiave KMS in un archivio delle chiavi personalizzate, le operazioni di crittografia vengono eseguite dal gestore delle chiavi tramite le chiavi crittografiche. Di conseguenza, ti assumi una maggiore responsabilità per la disponibilità e la durata delle chiavi crittografiche e per il funzionamento degli HSM.

AWS KMS supporta due tipi di archivi delle chiavi personalizzate.

- Un archivio delle chiavi di AWS CloudHSM è un archivio delle chiavi personalizzate di AWS KMS supportato da un cluster AWS CloudHSM. Quando crei una chiave KMS nell'archivio delle chiavi di AWS CloudHSM, AWS KMS genera una chiave simmetrica AES (Advanced Encryption Standard) a 256 bit non estraibile e persistente nel cluster AWS CloudHSM associato. Questo materiale della chiave esegue sempre la crittografia dei cluster AWS CloudHSM. Quando utilizzi una chiave KMS in un archivio delle chiavi di AWS CloudHSM, le operazioni di crittografia vengono eseguite negli HSM del cluster. I cluster AWS CloudHSM sono supportati da moduli di sicurezza hardware (HSM) con certificazione FIPS 140-2 di livello 3.
- Un archivio delle chiavi esterne è un archivio delle chiavi personalizzate di AWS KMS supportato da un gestore delle chiavi esterne al di fuori di AWS di tua proprietà e gestione. Quando utilizzi una chiave KMS nell'archivio delle chiavi esterne, tutte le operazioni di crittografia e decrittografia vengono eseguite dal gestore delle chiavi esterne tramite le chiavi crittografiche. Gli archivi delle chiavi esterne sono progettati per supportare una varietà di gestori di diversi fornitori.

  AWS KMS non visualizza, accede o interagisce mai direttamente con il gestore delle chiavi esterne o con le chiavi crittografiche. Quando esegui la crittografia o la decrittografia con una chiave KMS in un archivio delle chiavi esterne, l'operazione viene eseguita dal gestore utilizzando le chiavi esterne. Mantieni il pieno controllo delle chiavi crittografiche, inclusa la possibilità di rifiutare o interrompere un'operazione di crittografia senza interagire con AWS. Tuttavia, a causa della distanza e dell'elaborazione aggiuntiva, le chiavi KMS in un archivio delle chiavi esterne potrebbero avere latenza e prestazioni inferiori, oltre a caratteristiche di disponibilità diverse rispetto alle

chiavi KMS con materiale della chiave in AWS KMS. Per ulteriori informazioni sui gestori di chiavi compatibili con la funzionalità di archivio chiavi esterno AWS KMS, consulta Quali fornitori esterni supportano la specifica proxy XKS? nelle Domande frequenti di AWS Key Management Service.

Questi due tipi di archivi delle chiavi personalizzate sono molto diversi tra loro e rispetto all'archivio delle chiavi di AWS KMS standard. Anche i loro modelli di sicurezza, la responsabilità, le prestazioni, il prezzo e i casi d'uso sono molto diversi. Prima di scegliere un archivio delle chiavi personalizzate, leggi la documentazione correlata e verifica che la responsabilità di configurazione e manutenzione aggiuntiva sia un saggio compromesso per il maggiore controllo. Tuttavia, se le norme e i regolamenti in base ai quali operi richiedono il controllo diretto del materiale della chiave, un archivio delle chiavi personalizzate potrebbe essere la scelta ideale per te.

Caratteristiche non supportate

AWS KMS non supporta le seguenti funzioni negli archivi delle chiavi personalizzate.

- Chiavi KMS asimmetriche
- Coppie di chiavi di dati asimmetriche
- Chiavi KMS HMAC
- Chiavi KMS con materiale della chiave importato
- Rotazione automatica delle chiavi
- Chiavi multi-regione

Argomenti

- AWS CloudHSM negozi chiave
- Archivi delle chiavi esterne

AWS CloudHSM negozi chiave

Un AWS CloudHSM key store è un archivio di chiavi personalizzato supportato da un AWS CloudHSM cluster. Quando ne crei uno AWS KMS keyin un archivio di chiavi personalizzato, AWS KMS genera e archivia materiale chiave non estraibile per la chiave KMS in un AWS CloudHSM cluster di tua proprietà e gestione. Quando utilizzi una chiave KMS in un archivio delle chiavi personalizzate, le operazioni di crittografia vengono eseguite negli HSM nel cluster. Questa

funzionalità combina la praticità e l'ampia integrazione di AWS KMS con il controllo aggiuntivo di un AWS CloudHSM cluster nel tuo. Account AWS

AWS KMS fornisce supporto completo per console e API per la creazione, l'utilizzo e la gestione degli archivi di chiavi personalizzati. È possibile utilizzare le chiavi KMS nell'archivio delle chiavi personalizzate nello stesso modo in cui si utilizza qualsiasi chiave KMS. Ad esempio, puoi utilizzare le chiavi KMS per generare chiavi di dati ed effettuare la crittografia dei dati. Puoi anche utilizzare le chiavi KMS nel tuo archivio chiavi personalizzato con AWS servizi che supportano le chiavi gestite dai clienti.

È necessario uno store di chiavi personalizzato?

Per la maggior parte degli utenti, l'archivio AWS KMS chiavi predefinito, protetto da moduli crittografici convalidati FIPS 140-2, soddisfa i requisiti di sicurezza. Non è richiesto un livello supplementare di responsabilità per la manutenzione o la dipendenza da un ulteriore servizio.

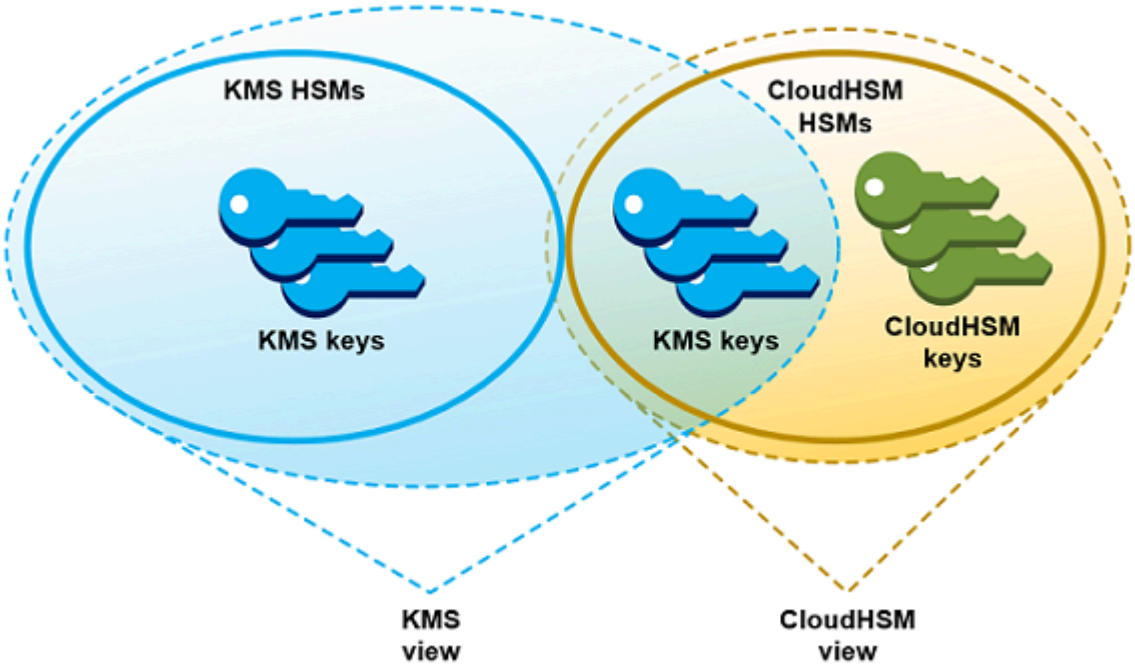
Tuttavia, è possibile prendere in considerazione la creazione di uno store di chiavi personalizzato qualora l'organizzazione possieda i seguenti requisiti:

- Hai chiavi che devono essere protette esplicitamente in un modulo HSM a tenant singolo o in un modulo HSM su cui hai il controllo diretto.
- È necessaria la possibilità di rimuovere immediatamente il materiale chiave da. AWS KMS
- Devi essere in grado di controllare tutti gli usi delle tue chiavi indipendentemente da AWS KMS o AWS CloudTrail.

Come funzionano gli store di chiavi personalizzati?

Ogni archivio di chiavi personalizzato è associato a un AWS CloudHSM cluster del tuo Account AWS. Quando connetti l'archivio di chiavi personalizzato al relativo cluster, AWS KMS crea l'infrastruttura di rete per supportare la connessione. Quindi accede al AWS CloudHSM client chiave del cluster utilizzando le credenziali di un utente crittografico dedicato nel cluster.

Crei e gestisci i tuoi archivi di chiavi personalizzati AWS KMS e crei e gestisci i tuoi cluster HSM in. AWS CloudHSM Quando crei AWS KMS keys in un archivio di chiavi AWS KMS personalizzato, visualizzi e gestisci le chiavi KMS in. AWS KMS Ma puoi anche visualizzare e gestire il loro materiale chiave in AWS CloudHSM, proprio come faresti per le altre chiavi del cluster.



Puoi creare chiavi KMS con crittografia simmetrica con materiale chiave generato dal tuo archivio AWS KMS di chiavi personalizzato. Utilizza quindi le stesse tecniche per visualizzare e gestire le chiavi KMS nell'archivio chiavi personalizzato utilizzate per le chiavi KMS nell'archivio chiavi. AWS KMS Puoi controllare l'accesso con e le policy IAM e delle chiavi, creare tag e alias, abilitare e disabilitare chiavi KMS e pianificare l'eliminazione della chiave. Puoi utilizzare le chiavi KMS per operazioni crittografiche e utilizzarle con AWS servizi che si integrano con. AWS KMS

Inoltre, hai il pieno controllo sul AWS CloudHSM cluster, inclusa la creazione e l'eliminazione degli HSM e la gestione dei backup. Puoi utilizzare il AWS CloudHSM client e le librerie software supportate per visualizzare, controllare e gestire il materiale chiave per le tue chiavi KMS. Sebbene l'archivio chiavi personalizzato sia disconnesso, AWS KMS non possono accedervi e gli utenti non possono utilizzare le chiavi KMS nell'archivio chiavi personalizzato per operazioni crittografiche. Questo ulteriore livello di controllo rende gli store di chiavi personalizzati una soluzione potente per le aziende che lo richiedono.

Da dove iniziare?

Per creare e gestire un archivio di AWS CloudHSM chiavi, si utilizzano le funzionalità di e. AWS KMS AWS CloudHSM

1. Inizia in AWS CloudHSM. Creare un cluster AWS CloudHSM attivo oppure selezionare un cluster esistente. Il cluster deve avere almeno due moduli HSM attivi in diverse zone di disponibilità.

Creare poi un account utente di crittografia dedicato (CU, crypto user) in quel cluster per AWS KMS.

2. In AWS KMS, crea un archivio di chiavi personalizzato associato al AWS CloudHSM cluster selezionato. AWS KMS fornisce un'interfaccia di gestione completa che consente di creare, visualizzare, modificare ed eliminare gli archivi di chiavi personalizzati.
3. Quando sei pronto per utilizzare il tuo archivio di chiavi personalizzato, collegalo al AWS CloudHSM cluster associato. AWS KMS crea l'infrastruttura di rete necessaria per supportare la connessione. Effettua poi l'accesso al cluster tramite le credenziali dell'account crypto user (CU) dedicato, in modo da poter generare e gestire il materiale chiave nel cluster.
4. Ora puoi creare chiavi KMS di crittografia simmetrica nel tuo archivio delle chiavi personalizzate. Basta specificare l'archivio delle chiavi personalizzate in fase di creazione della chiave KMS.

Qualora durante questa procedura non si riesca a procedere, cercare assistenza nell'argomento Risoluzione di problemi relativi a store delle chiavi personalizzate. Se non si trova risposta, utilizzare il collegamento di feedback nella parte inferiore di ogni pagina della guida o pubblicare una domanda nel Forum di discussione AWS Key Management Service.

Quote

AWS KMS consente fino a 10 archivi di chiavi personalizzati in ciascuna Account AWS regione, inclusi archivi AWS CloudHSM chiavi e archivi chiavi esterni, indipendentemente dallo stato della connessione. Inoltre, sono previste quote di AWS KMS richiesta per l'uso delle chiavi KMS in un AWS CloudHSM archivio di chiavi.

Prezzi

Per informazioni sul costo degli archivi di chiavi AWS KMS personalizzati e delle chiavi gestite dai clienti in un archivio di chiavi personalizzato, consulta AWS Key Management Service i prezzi. Per informazioni sul costo dei AWS CloudHSM cluster e degli HSM, vedi AWS CloudHSM Prezzi.

Regioni

AWS KMS supporta i AWS CloudHSM principali store in tutti i paesi in Regioni AWS cui AWS KMS è supportato, ad eccezione di Asia Pacifico (Melbourne), Cina (Pechino), Cina (Ningxia) ed Europa (Spagna).

Caratteristiche non supportate

AWS KMS non supporta le seguenti funzionalità negli archivi di chiavi personalizzati.

- Chiavi KMS asimmetriche
- Coppie di chiavi di dati asimmetriche
- Chiavi KMS HMAC
- Chiavi KMS con materiale della chiave importato
- Rotazione automatica delle chiavi
- Chiavi multi-regione

Argomenti

- Concetti fondamentali sull'archivio delle chiavi di AWS CloudHSM
- Controllo dell'accesso all'archivio delle chiavi di AWS CloudHSM
- Gestione di un archivio delle chiavi personalizzate di CloudHSM
- Gestione di chiavi KMS in un archivio delle chiavi di CloudHSM
- Risoluzione di problemi relativi a store delle chiavi personalizzate

Concetti fondamentali sull'archivio delle chiavi di AWS CloudHSM

Questo argomento descrive alcuni dei concetti utilizzati in relazione agli archivi delle chiavi di AWS CloudHSM.

Archivio delle chiavi di AWS CloudHSM

Un archivio delle chiavi di AWS CloudHSM è un archivio delle chiavi personalizzate associato a un cluster AWS CloudHSM di tua proprietà e gestione. I cluster AWS CloudHSM sono supportati da moduli di sicurezza hardware (HSM) con certificazione FIPS 140-2 di livello 3.

Quando crei una chiave KMS nell'archivio delle chiavi di AWS CloudHSM, AWS KMS genera una chiave simmetrica AES (Advanced Encryption Standard) a 256 bit non estraibile e persistente nel cluster AWS CloudHSM associato. Questo materiale chiave è sempre crittografato. Quando utilizzi una chiave KMS in un archivio delle chiavi di AWS CloudHSM, le operazioni di crittografia vengono eseguite negli HSM nel cluster.

Gli archivi delle chiavi di AWS CloudHSM combinano l'interfaccia di gestione delle chiavi pratica e completa di AWS KMS con i controlli supplementari forniti da un cluster AWS CloudHSM del tuo Account AWS. Questa funzionalità integrata consente di creare, gestire e utilizzare chiavi KMS

in AWS KMS mantenendo nel contempo il controllo completo degli HSM che archiviano il relativo materiale della chiave, tra cui la gestione di cluster, HSM e backup. Puoi utilizzare le API e la console AWS KMS per gestire l'archivio delle chiavi di AWS CloudHSM e le relative chiavi KMS. È inoltre possibile utilizzare la console AWS CloudHSM, le API, il software client e le librerie software correlate per gestire il cluster associato.

Puoi visualizzare e gestire l'archivio delle chiavi di AWS CloudHSM, modificarne le proprietà e connetterlo e disconnetterlo dal cluster AWS CloudHSM associato. Se intendi eliminare un archivio delle chiavi di AWS CloudHSM, devi innanzitutto eliminare le chiavi KMS presenti nello stesso archivio delle chiavi AWS CloudHSM pianificandone l'eliminazione e attendendo la scadenza del periodo di grazia. L'eliminazione dell'archivio delle chiavi di AWS CloudHSM rimuove la risorsa da AWS KMS, ma non influisce sul cluster AWS CloudHSM.

AWS CloudHSM cluster

Ogni archivio delle chiavi di AWS CloudHSM è associato a un cluster AWS CloudHSM. Quando crei AWS KMS key nell'archivio delle chiavi di AWS CloudHSM, AWS KMS crea il relativo materiale della chiave nel cluster associato. Quando utilizzi una chiave KMS nell'archivio delle chiavi di AWS CloudHSM, l'operazione di crittografia viene eseguita nel cluster associato.

Ogni cluster AWS CloudHSM può essere associato a un unico archivio delle chiavi di AWS CloudHSM. Il cluster che scegli non può essere associato a un altro archivio delle chiavi di AWS CloudHSM o condividere una cronologia dei backup con un cluster associato a un altro archivio delle chiavi di AWS CloudHSM. Il cluster deve essere inizializzato e attivo e deve trovarsi nella stessa regione e nello stesso Account AWS dell'archivio delle chiavi di AWS CloudHSM. Puoi creare un nuovo cluster o utilizzarne uno esistente. AWS KMS non richiede l'uso esclusivo del cluster. Per creare chiavi KMS nell'archivio delle chiavi di AWS CloudHSM, il relativo cluster associato deve contenere almeno due HSM attivi. Per tutte le altre operazioni è richiesto un solo HSM.

Il cluster AWS CloudHSM viene specificato durante la creazione dell'archivio delle chiavi di AWS CloudHSM e non può essere modificato. Puoi tuttavia sostituire qualsiasi cluster che condivide una cronologia dei backup con il cluster originale. Ciò ti consente di eliminare il cluster, se necessario, e sostituirlo con un cluster creato a partire da uno dei relativi backup. Mantieni quindi il controllo completo del cluster AWS CloudHSM associato in modo da poter gestire utenti e chiavi, creare ed eliminare HSM, e utilizzare e gestire backup.

Quando sei pronto a utilizzare l'archivio delle chiavi di AWS CloudHSM, connettilo al cluster AWS CloudHSM associato. Puoi connettere e disconnettere lo store delle chiavi personalizzate in qualsiasi momento. Quando un archivio delle chiavi personalizzate è connesso, puoi creare chiavi KMS e

utilizzare quelle che contiene. Quando è disconnesso, puoi visualizzare e gestire l'archivio delle chiavi di AWS CloudHSM e le relative chiavi KMS. Tuttavia, non puoi creare nuove chiavi KMS o utilizzare le chiavi KMS che contiene l'archivio delle chiavi di AWS CloudHSM per operazioni di crittografia.

Crypto user (CU) **`kmsuser`**

Per creare e gestire il materiale chiave nel cluster AWS CloudHSM per tuo conto, AWS KMS utilizza un crypto user (CU) AWS CloudHSM dedicato nel cluster denominato `kmsuser`. L'utente di crittografia `kmsuser` è un account utente di crittografia standard che viene automaticamente sincronizzato con tutti gli HSM nel cluster e viene salvato nei backup del cluster.

Prima di creare l'archivio delle chiavi di AWS CloudHSM, devi creare un account CU `kmsuser` nel cluster AWS CloudHSM utilizzando il comando createUser in cloudhsm_mgmt_util. Durante la creazione dell'archivio delle chiavi di AWS CloudHSM, fornisci la password dell'account `kmsuser` a AWS KMS. Quando si connette l'archivio delle chiavi personalizzate, AWS KMS accede al cluster come utente di crittografia `kmsuser` e ruota la password. AWS KMS esegue la crittografia della password `kmsuser` prima di archiviarla in modo sicuro. Quando la password viene ruotata, la nuova password viene crittografata e archiviata in modo analogo.

AWS KMS rimane collegato come `kmsuser` fino a che l'archivio delle chiavi di AWS CloudHSM è connesso. Non devi utilizzare questo account utente di crittografia per altri scopi. Mantieni tuttavia il controllo finale dell'account utente di crittografia `kmsuser`. In qualsiasi momento, puoi trovare l'handle di chiave delle chiavi di cui `kmsuser` è proprietario. Se necessario, è possibile disconnettere l'archivio delle chiavi personalizzate, modificare la password di `kmsuser`, accedere al cluster come `kmsuser` e visualizzare e gestire le chiavi di cui l'`kmsuser` è proprietario.

Per istruzioni sulla creazione dell'account utente di crittografia `kmsuser`, consulta Creazione del crypto user (CU)`kmsuser`.

Chiavi KMS in un archivio delle chiavi di AWS CloudHSM

Puoi utilizzare la AWS KMS o l'API AWS KMS per creare una AWS KMS keys in un archivio delle chiavi di AWS CloudHSM. A questo proposito, utilizzi la stessa tecnica che utilizzeresti per qualsiasi chiave KMS. La sola differenza è che devi identificare l'archivio delle chiavi di AWS CloudHSM e specificare che l'origine del materiale della chiave è il cluster AWS CloudHSM.

Quando crei una chiave KMS in un archivio delle chiavi di AWS CloudHSM, AWS KMS crea la chiave KMS in AWS KMS e genera un materiale della chiave simmetrica AES (Advanced Encryption

Standard) a 256 bit non esportabile e persistente nel relativo cluster associato. Quando utilizzi la chiave AWS KMS in un'operazione di crittografia, quest'ultima viene eseguita nel cluster AWS CloudHSM utilizzando la chiave AES basata sul cluster. Anche se AWS CloudHSM supporta chiavi simmetriche e asimmetriche di diversi tipi, gli archivi delle chiavi di AWS CloudHSM supportano solo chiavi crittografiche simmetrica AES.

Puoi visualizzare le chiavi KMS in un archivio delle chiavi di AWS CloudHSM nella console AWS KMS e utilizzare le opzioni della console per visualizzare l'ID dell'archivio delle chiavi personalizzate. È inoltre possibile utilizzare l'DescribeKeyoperazione per trovare l'ID dell'archivio AWS CloudHSM chiavi e l'ID AWS CloudHSM del cluster.

Le chiavi KMS in un archivio delle chiavi di AWS CloudHSM funzionano esattamente come le chiavi KMS in AWS KMS. Gli utenti autorizzati devono disporre delle stesse autorizzazioni per utilizzare e gestire le chiavi KMS. Usa le stesse procedure della console e le stesse operazioni dell'API per visualizzare e gestire le chiavi KMS in un archivio delle chiavi di AWS CloudHSM. Queste includono l'abilitazione e la disabilitazione di chiavi KMS, la creazione e l'utilizzo di tag e alias e l'impostazione e la modifica di policy IAM e di policy chiave. Puoi utilizzare le chiavi KMS in un archivio delle chiavi di AWS CloudHSM per operazioni di crittografia e con servizi AWS integrati che supportano l'uso di chiavi gestite dal cliente. Tuttavia, non puoi abilitare la rotazione automatica delle chiavi o importare il materiale della chiave in una chiave KMS di un archivio delle chiavi di AWS CloudHSM.

Utilizza inoltre lo stesso processo per pianificare l'eliminazione di una chiave KMS in un archivio delle chiavi di AWS CloudHSM. Dopo la scadenza del periodo di attesa, AWS KMS elimina la chiave KMS da KMS. Tenta quindi di eliminare il materiale della chiave per la chiave KMS dal cluster AWS CloudHSM associato. È tuttavia possibile che sia necessario eliminare manualmente il materiale della chiave orfano dal cluster e dai relativi backup.

Controllo dell'accesso all'archivio delle chiavi di AWS CloudHSM

Le policy IAM ti consentono di controllare l'accesso all'archivio delle chiavi di AWS CloudHSM e al cluster AWS CloudHSM. Puoi utilizzare le policy chiave, le policy IAM e le concessioni per controllare l'accesso alle AWS KMS keys nell'archivio delle chiavi di AWS CloudHSM. Ti consigliamo di concedere a utenti, gruppi e ruoli soltanto le autorizzazioni necessarie per le attività che sono supposti eseguire.

Argomenti

- Autorizzazione di gestori e utenti dell'archivio delle chiavi di AWS CloudHSM
- Autorizzazione di AWS KMS per gestire risorse AWS CloudHSM e Amazon EC2

Autorizzazione di gestori e utenti dell'archivio delle chiavi di AWS CloudHSM

Durante la progettazione dell'archivio delle chiavi di AWS CloudHSM, assicurati che i principali che lo utilizzano e gestiscono dispongano soltanto delle autorizzazioni necessarie. L'elenco seguente descrive le autorizzazioni minime necessarie per i gestori e gli utenti dell'archivio delle chiavi di AWS CloudHSM.

- I principali che creano e gestiscono l'archivio delle chiavi di AWS CloudHSM necessitano della seguente autorizzazione per utilizzare le operazioni API relative all'archivio di AWS CloudHSM.
  - `cloudhsm:DescribeClusters`
  - `kms:CreateCustomKeyStore`
  - `kms:ConnectCustomKeyStore`
  - `kms:DeleteCustomKeyStore`
  - `kms:DescribeCustomKeyStores`
  - `kms:DisconnectCustomKeyStore`
  - `kms:UpdateCustomKeyStore`
  - `iam:CreateServiceLinkedRole`
- I principali che creano e gestiscono il cluster AWS CloudHSM associato all'archivio delle chiavi di AWS CloudHSM devono disporre dell'autorizzazione per creare e inizializzare un cluster AWS CloudHSM. Ciò include l'autorizzazione a creare o utilizzare un cloud privato virtuale (VPC) di Amazon, creare sottoreti e un'istanza Amazon EC2. Potrebbero inoltre aver bisogno di creare ed eliminare HSM e gestire backup. Per un elenco delle autorizzazioni necessarie, consulta Identity and access management per AWS CloudHSM nella Guida per l'utente di AWS CloudHSM.
- I principali che creano e gestiscono le AWS KMS keys nell'archivio delle chiavi di AWS CloudHSM devono disporre delle stesse autorizzazioni degli utenti che creano e gestiscono le chiavi KMS in AWS KMS. La policy chiave predefinita per le chiavi KMS in un archivio delle chiavi di AWS CloudHSM è identica alla policy chiave predefinita per le chiavi KMS in AWS KMS. Il controllo degli accessi basato su attributi (ABAC), che utilizza tag e alias per controllare l'accesso alle chiavi KMS, è efficace anche per le chiavi KMS negli archivi delle chiavi di AWS CloudHSM.
- I principali che utilizzano le chiavi KMS nell'archivio delle chiavi di AWS CloudHSM per operazioni di crittografia devono essere autorizzati a eseguire l'operazione di crittografia con la chiave KMS, ad esempio kms:Decrypt. Puoi fornire queste autorizzazioni in una policy delle chiavi, una policy IAM. I principali non hanno tuttavia bisogno di autorizzazioni supplementari per utilizzare una chiave KMS in un archivio delle chiavi di AWS CloudHSM.

Autorizzazione di AWS KMS per gestire risorse AWS CloudHSM e Amazon EC2

Per supportare gli archivi delle chiavi di AWS CloudHSM, AWS KMS deve disporre dell'autorizzazione per ottenere informazioni sui cluster AWS CloudHSM. Ha inoltre bisogno dell'autorizzazione per creare l'infrastruttura di rete che connette l'archivio delle chiavi di AWS CloudHSM al relativo cluster AWS CloudHSM. Per ottenere queste autorizzazioni, AWS KMS crea il ruolo AWSServiceRoleForKeyManagementServiceCustomKeyStorescollegato al servizio nel tuo. Account AWS Gli utenti che creano archivi delle chiavi di AWS CloudHSM devono disporre dell'autorizzazione `iam:CreateServiceLinkedRole` che consente loro di creare ruoli collegati ai servizi.

Argomenti

- Informazioni sul ruolo collegato ai servizi AWS KMS
- Creazione del ruolo collegato ai servizi
- Modifica della descrizione di un ruolo collegato ai servizi
- Eliminazione del ruolo collegato ai servizi

Informazioni sul ruolo collegato ai servizi AWS KMS

Un ruolo collegato ai servizi è un ruolo IAM che concede a un servizio AWS l'autorizzazione per chiamare altri servizi AWS a tuo nome. È concepito per facilitare l'utilizzo delle funzionalità di molteplici servizi AWS integrati senza la necessità di creare e gestire policy IAM complesse. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per AWS KMS.

Per gli archivi AWS CloudHSM chiave, AWS KMS crea il ruolo AWSServiceRoleForKeyManagementServiceCustomKeyStorescollegato al servizio con la policy. AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy Questa policy concede al ruolo le seguenti autorizzazioni:

- CloudHSM:Describe* — rileva le modifiche nel AWS CloudHSM cluster collegato al tuo archivio di chiavi personalizzato.
- ec2: CreateSecurityGroup — utilizzato quando connetti un archivio di AWS CloudHSM chiavi per creare il gruppo di sicurezza che abilita il flusso del traffico di rete tra e il cluster. AWS KMS AWS CloudHSM
- ec2: AuthorizeSecurityGroupIngress — utilizzato quando si connette un AWS CloudHSM key store per consentire l'accesso alla rete dal AWS KMS VPC che contiene AWS CloudHSM il cluster.

- ec2: CreateNetworkInterface — utilizzato quando si connette un AWS CloudHSM key store per creare l'interfaccia di rete utilizzata per la comunicazione tra AWS KMS e il cluster. AWS CloudHSM
- ec2: RevokeSecurityGroupEgress — utilizzato quando si connette un archivio di AWS CloudHSM chiavi per rimuovere tutte le regole in uscita dal gruppo di sicurezza creato. AWS KMS
- ec2: DeleteSecurityGroup — utilizzato quando si disconnette un archivio di AWS CloudHSM chiavi per eliminare i gruppi di sicurezza creati quando si è connesso l'archivio chiavi. AWS CloudHSM
- ec2: DescribeSecurityGroups — utilizzato per monitorare le modifiche nel gruppo di sicurezza AWS KMS creato nel VPC che contiene AWS CloudHSM il cluster in modo AWS KMS che possa fornire messaggi di errore chiari in caso di guasti.
- ec2: DescribeVpcs — utilizzato per monitorare le modifiche nel VPC che contiene AWS CloudHSM il cluster in modo da AWS KMS fornire messaggi di errore chiari in caso di guasti.
- ec2: DescribeNetworkAcls — utilizzato per monitorare le modifiche negli ACL di rete per il VPC che contiene il AWS CloudHSM cluster in modo da AWS KMS fornire messaggi di errore chiari in caso di guasti.
- ec2: DescribeNetworkInterfaces — utilizzato per monitorare le modifiche nelle interfacce di rete AWS KMS create nel VPC che contiene il AWS CloudHSM cluster in modo da AWS KMS fornire messaggi di errore chiari in caso di guasti.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudhsm:Describe*",
        "ec2:CreateNetworkInterface",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource": "*"
    }
```

```
  ]
}
```

Poiché solo il ruolo AWSServiceRoleForKeyManagementServiceCustomKeyStorescollegato al servizio è affidabile`cks.kms.amazonaws.com`, solo può assumere questo ruolo collegato al servizio. AWS KMS Questo ruolo è limitato alle operazioni di cui AWS KMS necessita per visualizzare i cluster AWS CloudHSM e connettere un archivio delle chiavi di AWS CloudHSM al relativo cluster AWS CloudHSM. Non fornisce a AWS KMS autorizzazioni aggiuntive. Ad esempio, AWS KMS non dispone dell'autorizzazione per creare, gestire o eliminare cluster AWS CloudHSM, HSM o backup.

Regioni

Come la funzionalità degli archivi AWS CloudHSM chiave, il AWSServiceRoleForKeyManagementServiceCustomKeyStoresruolo è supportato ovunque e è disponibile. Regioni AWS AWS KMS AWS CloudHSM Per un elenco di Regioni AWS supportate da ogni servizio, consulta Endpoint e quote AWS Key Management Service ed Endpoint e quote AWS CloudHSM nella Riferimenti generali di Amazon Web Services.

Per ulteriori informazioni su come i servizi AWS utilizzano i ruoli collegati ai servizi, consulta la pagina Uso di ruoli collegati ai servizi nella Guida per l'utente di IAM.

Creazione del ruolo collegato ai servizi

AWS KMScrea automaticamente il ruolo AWSServiceRoleForKeyManagementServiceCustomKeyStorescollegato al servizio Account AWS quando crei un archivio di AWS CloudHSM chiavi, se il ruolo non esiste già. Non è possibile creare o ricreare direttamente questo ruolo collegato ai servizi.

Modifica della descrizione di un ruolo collegato ai servizi

Non puoi modificare il nome del ruolo o le istruzioni di policy nel ruolo collegato ai servizi AWSServiceRoleForKeyManagementServiceCustomKeyStores, ma puoi modificare la descrizione del ruolo. Per istruzioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione del ruolo collegato ai servizi

AWS KMSnon elimina il ruolo AWSServiceRoleForKeyManagementServiceCustomKeyStorescollegato al servizio

dal tuo Account AWS anche se hai eliminato tutti i tuoi archivi di chiavi. AWS CloudHSM Sebbene al momento non esista una procedura per eliminare il ruolo AWSServiceRoleForKeyManagementServiceCustomKeyStorescollegato al servizio, non assume questo ruolo né ne utilizza le autorizzazioni a meno che AWS KMS non disponga di archivi di chiavi attivi. AWS CloudHSM

Gestione di un archivio delle chiavi personalizzate di CloudHSM

Puoi gestire uno store delle chiavi personalizzate utilizzando la AWS Management Console e l'API AWS KMS. Ad esempio, puoi visualizzare uno store delle chiavi personalizzate, modificarne le proprietà, connetterlo e disconnetterlo dal cluster AWS CloudHSM associato ed eliminarlo.

Argomenti

- Creazione di un archivio delle chiavi di AWS CloudHSM
- Visualizzazione di un archivio delle chiavi di AWS CloudHSM
- Modifica delle impostazioni di un archivio delle chiavi di AWS CloudHSM
- Connessione e disconnessione di un archivio delle chiavi di AWS CloudHSM
- Eliminazione di un archivio delle chiavi di AWS CloudHSM

Creazione di un archivio delle chiavi di AWS CloudHSM

Puoi creare uno o più archivi delle chiavi di AWS CloudHSM nel tuo account. Ogni archivio delle chiavi di AWS CloudHSM è associato a un cluster AWS CloudHSM nella stessa regione e Account AWS. Prima di creare l'archivio delle chiavi di AWS CloudHSM, devi assemblare i prerequisiti. Quindi, prima di poter utilizzare l'archivio delle chiavi di AWS CloudHSM, devi connetterlo al relativo cluster AWS CloudHSM.

> **Note**
>
> Se tenti di creare un archivio delle chiavi di AWS CloudHSM con tutti gli stessi valori di proprietà di un archivio delle chiavi di AWS CloudHSM disconnesso esistente, AWS KMS non crea un nuovo archivio delle chiavi di AWS CloudHSM e non genera un'eccezione né visualizza un errore. Al contrario, AWS KMS riconosce il duplicato come probabile conseguenza di un nuovo tentativo e restituisce l'ID dell'archivio delle chiavi di AWS CloudHSM esistente.

> **Tip**
>
> Non devi connettere l'archivio delle chiavi di AWS CloudHSM immediatamente. Puoi lasciarlo disconnesso fino a che non sei pronto a utilizzarlo. Tuttavia, per verificare che sia configurato correttamente, puoi connetterlo, visualizzarne lo stato di connessione e quindi disconnetterlo.

Argomenti

- Assemblare i prerequisiti
- Creazione di un archivio delle chiavi di AWS CloudHSM (console)
- Creazione di un archivio delle chiavi di AWS CloudHSM (API)

Assemblare i prerequisiti

Ogni archivio delle chiavi di AWS CloudHSM è supportato da un cluster AWS CloudHSM. Per creare un archivio delle chiavi di AWS CloudHSM, devi specificare un cluster AWS CloudHSM attivo e non associato a un altro archivio delle chiavi. Devi inoltre creare un crypto user (CU) dedicato negli HSM del cluster che AWS KMS può utilizzare per creare e gestire chiavi a tuo nome.

Prima di creare un archivio delle chiavi di AWS CloudHSM, esegui le operazioni descritte di seguito:

Selezione di un cluster AWS CloudHSM

Ogni archivio delle chiavi di AWS CloudHSM è associato a un solo cluster AWS CloudHSM. Quando crei una AWS KMS keys nell'archivio delle chiavi di AWS CloudHSM, AWS KMS crea i metadati della chiave KMS, ad esempio un ID e un nome della risorsa Amazon (ARN) in AWS KMS. Successivamente crea il materiale della chiave negli HSM del cluster associato. Puoi creare un nuovo cluster AWS CloudHSM o utilizzarne uno esistente. AWS KMS non richiede l'accesso esclusivo al cluster.

Il cluster AWS CloudHSM che selezioni viene associato in modo permanente all'archivio delle chiavi di AWS CloudHSM. Dopo la creazione dell'archivio delle chiavi di AWS CloudHSM, puoi modificare l'ID cluster del cluster associato, tuttavia il cluster specificato deve condividere una cronologia dei backup con il cluster originale. Per utilizzare un cluster non correlato, devi creare un nuovo archivio delle chiavi di AWS CloudHSM.

Il cluster AWS CloudHSM che selezioni deve avere le seguenti caratteristiche:

- Il cluster deve essere attivo.

  Devi creare il cluster, inizializzarlo, installare il software client AWS CloudHSM per la piattaforma in uso e quindi attivare il cluster. Per istruzioni dettagliate, consulta la sezione Nozioni di base su AWS CloudHSM della Guida per l'utente di AWS CloudHSM.
- Il cluster deve trovarsi nello stesso account e nella stessa regione dell'archivio delle chiavi di AWS CloudHSM. Non puoi associare un archivio delle chiavi di AWS CloudHSM presente in una regione a un cluster in una regione diversa. Per creare un'infrastruttura della chiave in più regioni, devi creare gli archivi delle chiavi di AWS CloudHSM e i cluster in ciascuna regione.
- Il cluster non può essere associato a un altro archivio chiavi personalizzate nello stesso account e nella stessa regione. Ogni archivio delle chiavi di AWS CloudHSM nell'account e nella regione deve essere associato a un cluster AWS CloudHSM differente. Non puoi specificare un cluster che è già associato a uno store delle chiavi personalizzate o un cluster che condivide una cronologia dei backup con un cluster associato. I cluster che condividono una cronologia dei backup hanno lo stesso certificato di cluster. Per visualizzare il certificato del cluster di un cluster, utilizzare la AWS CloudHSM console o l'DescribeClustersoperazione.

  Se effettui il backup in un cluster AWS CloudHSM in una regione differente, tale cluster viene considerato diverso e puoi associare il backup a un archivio chiavi personalizzate nella relativa regione. Tuttavia, le chiavi KMS nei due archivi delle chiavi personalizzate non sono interoperabili, neppure se hanno lo stesso materiale. AWS KMS associa i metadati al testo criptato in modo da poterli decrittografare solo tramite la chiave KMS che li ha crittografati.
- Il cluster deve essere configurato con sottoreti private in almeno due zone di disponibilità nella regione. Poiché AWS CloudHSM non è supportato in tutte le zone di disponibilità, ti consigliamo di creare sottoreti private in tutte le zone di disponibilità della regione. Non puoi riconfigurare le sottoreti di un cluster esistente, ma puoi creare un cluster a partire da un backup con varie sottoreti nella configurazione del cluster.

  > **Important**
  >
  > Dopo aver creato l'archivio delle chiavi di AWS CloudHSM, non eliminare nessuna delle sottoreti private configurate per il relativo cluster AWS CloudHSM. Se AWS KMS non riesce a trovare tutte le sottoreti nella configurazione del cluster, i tentativi di connettersi allo store delle chiavi personalizzate non riescono con uno stato di errore di connessione `SUBNET_NOT_FOUND`. Per informazioni dettagliate, vedi Come correggere un errore di connessione.

- Il gruppo di sicurezza per il cluster (`cloudhsm-cluster-<cluster-id>-sg`) deve includere regole in entrata e regole in uscita che consentono il traffico TCP sulle porte 2223-2225. La Source (Origine) nelle regole in entrata e la Destination (Destinazione) nelle regole in uscita devono corrispondere all'ID del gruppo di sicurezza. Tali regole sono configurate per impostazione predefinita quando si crea il cluster. Non eliminarle o modificarle.
- Il cluster deve contenere almeno due HSM attivi in differenti zone di disponibilità. Per verificare il numero di moduli di protezione hardware, utilizzare la AWS CloudHSM console o l'DescribeClustersoperazione. Se necessario, puoi aggiungere un HSM.

Ricerca del certificato trust anchor

Quando crei un archivio delle chiavi personalizzate, devi caricare il certificato di ancora di fiducia per il cluster AWS CloudHSM in AWS KMS. AWS KMS necessita di questo certificato per connettere l'archivio delle chiavi di AWS CloudHSM al cluster AWS CloudHSM associato.

Ogni cluster AWS CloudHSM attivo ha un certificato trust anchor. Quando inizializzi il cluster, genera questo certificato, salvalo nel file `customerCA.crt` e copialo negli host che si connettono al cluster.

Creazione del crypto user (CU) **`kmsuser`** per AWS KMS

Per amministrare l'archivio delle chiavi di AWS CloudHSM, AWS KMS accede all'account crypto user (CU) `kmsuser` nel cluster selezionato. Prima di creare l'archivio delle chiavi di AWS CloudHSM, devi creare il crypto user (CU) `kmsuser`. Durante la creazione dell'archivio delle chiavi di AWS CloudHSM, indica la password per `kmsuser` in AWS KMS. Ogni volta che connetti l'archivio delle chiavi di AWS CloudHSM al cluster AWS CloudHSM associato, AWS KMS accede come `kmsuser` ed esegue la rotazione della password `kmsuser`.

> **Important**
>
> Non specificare l'opzione `2FA` quando crei l'utente di crittografia `kmsuser`. In caso contrario, AWS KMS non può effettuare l'accesso e l'archivio delle chiavi di AWS CloudHSM non può essere connesso a questo cluster AWS CloudHSM. Una volta specificata, l'opzione 2FA non può essere annullata. Dovrai invece eliminare l'utente di crittografia e ricrearlo.

Per creare l'utente di crittografia `kmsuser`, utilizza la procedura seguente.

1. Avvia cloudhsm_mgmt_util come descritto nell'argomento Getting started with CloudHSM Management Utility (CMU) (Nozioni di base su CloudHSM Management Utility (CMU)) della Guida per l'utente di AWS CloudHSM.
2. Utilizzare il comando createUser in cloudhsm_mgmt_util per creare un utente di crittografia denominato `kmsuser`. La password deve contenere da 7 a 32 caratteri alfanumerici, rispettare la distinzione tra maiuscole e minuscole e non includere caratteri speciali.

   Ad esempio, il comando di esempio seguente crea un utente di crittografia `kmsuser` con la password `kmsPswd`.

   ```
   aws-cloudhsm> createUser CU kmsuser kmsPswd
   ```

Creazione di un archivio delle chiavi di AWS CloudHSM (console)

Quando crei un archivio delle chiavi di AWS CloudHSM nella AWS Management Console, puoi aggiungere e creare i prerequisiti come parte del flusso di lavoro. Tuttavia, il processo risulta più rapido se li hai assemblati in precedenza.

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Archivi di chiavi personalizzate, Archivi di chiavi AWS CloudHSM.
4. Scegli Crea un archivio di chiavi.
5. Immettere un nome descrittivo per lo store delle chiavi personalizzate. Il nome deve essere univoco per tutti gli archivi delle chiavi personalizzate presenti nell'account.

   > **Important**
   >
   > Non includere informazioni riservate o sensibili in questo campo. Questo campo può essere visualizzato in testo semplice nei CloudTrail log e in altri output.

6. Seleziona un cluster AWS CloudHSM per l'archivio delle chiavi di AWS CloudHSM. In alternativa, per creare un nuovo cluster AWS CloudHSM, scegli il link Crea un cluster AWS CloudHSM.

Il menu visualizza i cluster AWS CloudHSM dell'account e della regione che non sono già associati a un archivio delle chiavi di AWS CloudHSM. Il cluster deve soddisfare i requisiti per l'associazione con uno store delle chiavi personalizzate.

7. Scegli Choose file (Scegli file), quindi carica il certificato dell'ancora di fiducia per il cluster AWS CloudHSM scelto. Si tratta del file `customerCA.crt` creato all'inizializzazione del cluster.
8. Immettere la password del crypto user (CU) `kmsuser` creato nel cluster selezionato.
9. Scegliere Create (Crea) .

Se la procedura riesce, il nuovo archivio delle chiavi di AWS CloudHSM viene visualizzato nell'elenco degli archivi delle chiavi di AWS CloudHSM dell'account e della regione. Se ha esito negativo, viene visualizzato un messaggio di errore che descrive il problema e fornisce istruzioni su come risolverlo. Per ulteriori informazioni, consulta Risoluzione di problemi relativi a store delle chiavi personalizzate.

Se tenti di creare un archivio delle chiavi di AWS CloudHSM con tutti gli stessi valori di proprietà di un archivio delle chiavi di AWS CloudHSM disconnesso esistente, AWS KMS non crea un nuovo archivio delle chiavi di AWS CloudHSM e non genera un'eccezione né visualizza un errore. Al contrario, AWS KMS riconosce il duplicato come probabile conseguenza di un nuovo tentativo e restituisce l'ID dell'archivio delle chiavi di AWS CloudHSM esistente.

Successivo: i nuovi archivi delle chiavi di AWS CloudHSM non sono connessi automaticamente. Prima di creare AWS KMS keys nell'archivio delle chiavi di AWS CloudHSM, devi connettere l'archivio delle chiavi personalizzate al cluster AWS CloudHSM associato.

Creazione di un archivio delle chiavi di AWS CloudHSM (API)

È possibile utilizzare l'CreateCustomKeyStoreoperazione per creare un nuovo archivio di AWS CloudHSM chiavi associato a un AWS CloudHSM cluster nell'account e nella regione. Questi esempi utilizzano l'AWS Command Line Interface (AWS CLI), ma puoi anche utilizzare qualsiasi linguaggio di programmazione supportato.

L'operazione `CreateCustomKeyStore` richiede i valori di parametro seguenti.

- CustomKeyStoreName — Un nome descrittivo per l'archivio di chiavi personalizzato che è unico nell'account.

> **Important**
>
> Non includere informazioni riservate o sensibili in questo campo. Questo campo può essere visualizzato in testo semplice nei CloudTrail registri e in altri output.

- CloudHsmClusterId — L'ID del cluster di un AWS CloudHSM cluster che soddisfa i requisiti per un archivio di chiavi. AWS CloudHSM
- KeyStorePassword — La password dell'account `kmsuser` CU nel cluster specificato.
- TrustAnchorCertificate — Il contenuto del `customerCA.crt` file creato durante l'inizializzazione del cluster.

L'esempio seguente utilizza un ID cluster fittizio. Prima di eseguire il comando, sostituiscilo con un ID cluster valido

```
$ aws kms create-custom-key-store
        --custom-key-store-name ExampleCloudHSMKeyStore \
        --cloud-hsm-cluster-id cluster-1a23b4cdefg \
        --key-store-password kmsPswd \
        --trust-anchor-certificate <certificate-goes-here>
```

Se utilizzi l'AWS CLI, puoi specificare il file del certificato trust anchor anziché il relativo contenuto. Nell'esempio seguente, il file `customerCA.crt` si trova nella directory principale:

```
$ aws kms create-custom-key-store
        --custom-key-store-name ExampleCloudHSMKeyStore \
        --cloud-hsm-cluster-id cluster-1a23b4cdefg \
        --key-store-password kmsPswd \
        --trust-anchor-certificate file://customerCA.crt
```

Se l'operazione riesce, `CreateCustomKeyStore` restituisce l'ID store chiavi personalizzate, come illustrato nel seguente esempio di risposta.

```
{
    "CustomKeyStoreId": cks-1234567890abcdef0
}
```

Se l'operazione ha esito negativo, correggi l'errore indicato dall'eccezione e riprova. Per ulteriori informazioni, consulta Risoluzione di problemi relativi a store delle chiavi personalizzate.

Se tenti di creare un archivio delle chiavi di AWS CloudHSM con tutti gli stessi valori di proprietà di un archivio delle chiavi di AWS CloudHSM disconnesso esistente, AWS KMS non crea un nuovo archivio delle chiavi di AWS CloudHSM e non genera un'eccezione né visualizza un errore. Al contrario, AWS KMS riconosce il duplicato come probabile conseguenza di un nuovo tentativo e restituisce l'ID dell'archivio delle chiavi di AWS CloudHSM esistente.

Successivo: per utilizzare l'archivio delle chiavi di AWS CloudHSM, connettilo al relativo cluster AWS CloudHSM.

Visualizzazione di un archivio delle chiavi di AWS CloudHSM

È possibile visualizzare gli archivi delle AWS CloudHSM chiavi in ogni account e regione utilizzando la AWS KMS console o l'DescribeCustomKeyStoresoperazione.

Consulta anche:

- Visualizzazione di un archivio delle chiavi esterne
- Visualizzazione delle chiavi KMS in un archivio delle chiavi di AWS CloudHSM
- Registrazione delle chiamate API AWS KMS con AWS CloudTrail

Argomenti

- Visualizzazione di un archivio delle chiavi di AWS CloudHSM (console)
- Visualizzazione di un archivio delle chiavi di AWS CloudHSM (API)

Visualizzazione di un archivio delle chiavi di AWS CloudHSM (console)

Quando visualizzi gli archivi delle chiavi di AWS CloudHSM nella AWS Management Console, hai accesso alle seguenti informazioni:

- Il nome e l'ID dell'archivio delle chiavi personalizzate
- L'ID del cluster AWS CloudHSM associato.
- Il numero di HSM nel cluster
- Lo stato di connessione corrente

Il valore Disconnected (Disconnesso) dello stato di connessione Status (Stato), indica che l'archivio delle chiavi personalizzate è nuovo e non è mai stato connesso o che è stato intenzionalmente

disconnesso dal relativo cluster AWS CloudHSM. Se tuttavia i tentativi di utilizzare una chiave KMS in un archivio delle chiavi personalizzate connesso non riescono, è possibile che vi sia un problema con l'archivio o con il cluster AWS CloudHSM. Per assistenza, consulta Come correggere una chiave KMS non funzionante.

Per visualizzare gli archivi delle chiavi di AWS CloudHSM in determinati account e regioni, utilizza la procedura seguente.

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Archivi di chiavi personalizzate, Archivi di chiavi AWS CloudHSM.

Per personalizzare la visualizzazione, fai clic sull'icona che raffigura un ingranaggio visualizzata sotto il pulsante Create key store (Crea store delle chiavi).

Visualizzazione di un archivio delle chiavi di AWS CloudHSM (API)

Per visualizzare gli archivi delle AWS CloudHSM chiavi, utilizza l'DescribeCustomKeyStoresoperazione. Per impostazione predefinita, questa operazione restituisce tutti gli store delle chiavi personalizzate presenti nell'account e nella regione. Puoi tuttavia utilizzare il parametro `CustomKeyStoreName` o `CustomKeyStoreId` (ma non entrambi) per limitare l'output a un determinato store delle chiavi personalizzate. Per quanto riguarda gli archivi delle chiavi di AWS CloudHSM, l'output include l'ID e il nome dell'archivio delle chiavi personalizzate, l'ID del cluster AWS CloudHSM associato e lo stato della connessione. Se lo stato della connessione indica un errore, l'output include un codice di errore che descrive il motivo del problema.

Gli esempi in questa sezione utilizzano AWS Command Line Interface (AWS CLI), ma puoi usare anche qualsiasi linguaggio di programmazione supportato.

Ad esempio, il comando seguente restituisce tutti gli store delle chiavi personalizzate presenti nell'account e nella regione. Per scorrere gli store delle chiavi personalizzate nell'output puoi utilizzare i parametri `Limit` e `Marker`.

```
$ aws kms describe-custom-key-stores
```

Il comando di esempio seguente utilizza il parametro `CustomKeyStoreName` per ottenere solo lo store delle chiavi personalizzate con il nome descrittivo `ExampleCloudHSMKeyStore`. Puoi utilizzare il parametro `CustomKeyStoreName` o `CustomKeyStoreId` (ma non entrambi) in ogni comando.

L'output di esempio seguente rappresenta un archivio delle chiavi di AWS CloudHSM connesso al relativo cluster AWS CloudHSM.

> **Note**
>
> Il campo `CustomKeyStoreType` è stato aggiunto alla risposta `DescribeCustomKeyStores` per distinguere gli archivi delle chiavi di AWS CloudHSM da quelli esterni.

```
$ aws kms describe-custom-key-stores --custom-key-store-name ExampleCloudHSMKeyStore
{
   "CustomKeyStores": [
      {
         "CloudHsmClusterId": "cluster-1a23b4cdefg",
         "ConnectionState": "CONNECTED",
         "CreationDate": "1.499288695918E9",
         "CustomKeyStoreId": "cks-1234567890abcdef0",
         "CustomKeyStoreName": "ExampleCloudHSMKeyStore",
         "CustomKeyStoreType": "AWS_CLOUDHSM",
         "TrustAnchorCertificate": "<certificate appears here>"
      }
   ]
}
```

Se `ConnectionState` è `Disconnected`, indica che uno store delle chiavi personalizzate non è mai stato connesso oppure è stato intenzionalmente disconnesso dal relativo cluster AWS CloudHSM. Se tuttavia i tentativi di utilizzare una chiave KMS in un archivio delle chiavi di AWS CloudHSM connesso non riescono, è possibile che vi sia un problema con l'archivio AWS CloudHSM o con il cluster AWS CloudHSM. Per assistenza, consulta Come correggere una chiave KMS non funzionante.

Se il campo `ConnectionState` dello store delle chiavi personalizzate è `FAILED`, la risposta `DescribeCustomKeyStores` include un elemento `ConnectionErrorCode` che descrive il motivo dell'errore.

Ad esempio, nell'output seguente, il valore `INVALID_CREDENTIALS` indica che la connessione dello store delle chiavi di connessione non è riuscita in quanto la password `kmsuser` non è valida. Per informazioni su questo e altri errori di connessione, consulta Risoluzione di problemi relativi a store delle chiavi personalizzate.

```
$ aws kms describe-custom-key-stores --custom-key-store-id cks-1234567890abcdef0
{
   "CustomKeyStores": [
      {
         "CloudHsmClusterId": "cluster-1a23b4cdefg",
         "ConnectionErrorCode": "INVALID_CREDENTIALS",
         "ConnectionState": "FAILED",
         "CustomKeyStoreId": "cks-1234567890abcdef0",
         "CustomKeyStoreName": "ExampleCloudHSMKeyStore",
         "CustomKeyStoreType": "AWS_CLOUDHSM",
         "CreationDate": "1.499288695918E9",
         "TrustAnchorCertificate": "<certificate appears here>"
      }
   ]
}
```

Modifica delle impostazioni di un archivio delle chiavi di AWS CloudHSM

Puoi modificare le impostazioni di un archivio delle chiavi di AWS CloudHSM esistente. L'archivio delle chiavi personalizzate deve essere disconnesso dal relativo cluster AWS CloudHSM.

Per modificare le impostazioni di un archivio delle chiavi di AWS CloudHSM:

1. Disconnettere lo store delle chiavi personalizzate dal relativo cluster AWS CloudHSM. Quando l'archivio delle chiavi personalizzate è disconnesso, non è possibile creare AWS KMS keys (chiavi KMS) nell'archivio né utilizzare le chiavi KMS che contiene per le operazioni di crittografia.
2. Modifica una o più impostazioni relative all'archivio delle chiavi di AWS CloudHSM.
3. Riconnettere lo store delle chiavi personalizzate al relativo cluster AWS CloudHSM.

Puoi modificare le impostazioni seguenti in uno store delle chiavi personalizzate:

Il nome descrittivo dello store delle chiavi personalizzate

Immetti un nuovo nome descrittivo. Il nuovo nome deve essere univoco per tutti gli archivi delle chiavi personalizzate presenti nel tuo Account AWS.

> **Important**
>
> Non includere informazioni riservate o sensibili in questo campo. Questo campo può essere visualizzato in testo semplice nei CloudTrail log e in altri output.

L'ID cluster del cluster AWS CloudHSM associato

Modifica questo valore per sostituire il cluster originale con un cluster AWS CloudHSM correlato. Puoi utilizzare questa funzionalità per riparare uno store delle chiavi personalizzate se il relativo cluster AWS CloudHSM è danneggiato o è stato eliminato.

Specifica un cluster AWS CloudHSM che condivide una cronologia dei backup con il cluster originale e soddisfa i requisiti per l'associazione con uno store delle chiavi personalizzate, tra cui due HSM attivi in zone di disponibilità differenti. I cluster che condividono una cronologia dei backup hanno lo stesso certificato di cluster. Per visualizzare il certificato del cluster di un cluster, utilizzare l'operazione. DescribeClusters Non puoi utilizzare la funzionalità di modifica per associare lo store delle chiavi personalizzate a un cluster AWS CloudHSM non correlato.

La password corrente del crypto user (CU) **`kmsuser`**

Segnala a AWS KMS la password corrente dell'utente di crittografia `kmsuser` nel cluster AWS CloudHSM. Questa operazione non modifica la password dell'utente di crittografia `kmsuser` nel cluster AWS CloudHSM.

Se modifichi la password dell'utente di crittografia `kmsuser` nel cluster AWS CloudHSM, utilizza questa funzionalità per segnalare a AWS KMS la nuova password `kmsuser`. In caso contrario, AWS KMS non può accedere al cluster e tutti i tentativi di connessione dello store delle chiavi personalizzate al cluster hanno esito negativo.

Argomenti

Modifica di un archivio delle chiavi di AWS CloudHSM (console)

Quando modifichi un archivio delle chiavi di AWS CloudHSM, puoi modificare qualsiasi valore configurabile.

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Archivi di chiavi personalizzate, Archivi di chiavi AWS CloudHSM.
4. Scegli la riga relativa all'archivio delle chiavi di AWS CloudHSM che vuoi modificare.

   Se il valore nella colonna Stato connessione non è Disconnesso, devi scollegare l'archivio di chiavi personalizzate per poterlo modificare. Dal menu Key store actions (Operazioni per l'archivio delle chiavi), scegli Disconnect (Disconnetti).

   Quando un archivio delle chiavi di AWS CloudHSM è disconnesso, puoi gestire l'archivio delle chiavi di AWS CloudHSM e le relative chiavi KMS, ma non puoi creare o utilizzare le chiavi KMS nell'archivio delle chiavi di AWS CloudHSM.
5. Dal menu Key store actions (Operazioni per l'archivio delle chiavi), scegli Edit (Modifica).
6. Effettuare una o più delle operazioni seguenti.

   - Digitare un nuovo nome descrittivo per lo store delle chiavi personalizzate.
   - Digitare l'ID cluster di un cluster AWS CloudHSM correlato.
   - Digitare la password corrente del crypto user (CU) `kmsuser` nel cluster AWS CloudHSM associato.
7. Selezionare Salva.

   Se la procedura ha esito positivo, un messaggio descrive le impostazioni modificate. Se ha esito negativo, viene visualizzato un messaggio di errore che descrive il problema e fornisce istruzioni su come risolverlo. Per ulteriori informazioni, consulta Risoluzione di problemi relativi a store delle chiavi personalizzate.
8. Riconnettere lo store delle chiavi personalizzate.

   Per utilizzare l'archivio delle chiavi di AWS CloudHSM, devi riconnetterlo dopo la modifica. Puoi lasciare disconnesso l'archivio delle chiavi di AWS CloudHSM, tuttavia, durante la disconnessione, non puoi creare chiavi KMS nell'archivio delle chiavi di AWS CloudHSM o utilizzare le chiavi KMS nell'archivio delle chiavi di AWS CloudHSM per operazioni di crittografia.

Modifica di un archivio delle chiavi di AWS CloudHSM (API)

Per modificare le proprietà di un archivio di AWS CloudHSM chiavi, utilizzare l'UpdateCustomKeyStoreoperazione. Puoi modificare più proprietà di un store delle chiavi personalizzate nello stesso comando. Se l'operazione ha esito positivo, AWS KMS restituisce una risposta HTTP 200 e un oggetto JSON senza proprietà. Per verificare che le modifiche siano effettive, utilizzate l'DescribeCustomKeyStoresoperazione.

Gli esempi in questa sezione utilizzano AWS Command Line Interface (AWS CLI), ma puoi usare anche qualsiasi linguaggio di programmazione supportato.

Inizia a utilizzare DisconnectCustomKeyStoreper disconnettere l'archivio di chiavi personalizzato dal relativo AWS CloudHSM cluster. Sostituisci l'ID archivio chiavi personalizzate di esempio, cks-1234567890abcdef0, con un ID effettivo.

```
$ aws kms disconnect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

Il primo esempio utilizza UpdateCustomKeyStoreper modificare il nome descrittivo del AWS CloudHSM key store in`DevelopmentKeys`. Il comando utilizza il parametro `CustomKeyStoreId` per identificare l'archivio delle chiavi di AWS CloudHSM e `CustomKeyStoreName` per specificarne il nuovo nome.

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 --new-
custom-key-store-name DevelopmentKeys
```

L'esempio seguente modifica il cluster associato a un archivio delle chiavi di AWS CloudHSM in un altro backup dello stesso cluster. Il comando utilizza il parametro `CustomKeyStoreId` per identificare l'archivio delle chiavi di AWS CloudHSM e il parametro `CloudHsmClusterId` per specificarne il nuovo ID cluster.

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 --cloud-
hsm-cluster-id cluster-1a23b4cdefg
```

L'esempio seguente segnala a AWS KMS che la password `kmsuser` corrente è `ExamplePassword`. Il comando utilizza il parametro `CustomKeyStoreId` per identificare l'archivio delle chiavi di AWS CloudHSM e il parametro `KeyStorePassword` per specificare la password corrente.

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 --key-
store-password ExamplePassword
```

Il comando finale riconnette l'archivio delle chiavi di AWS CloudHSM al relativo cluster AWS CloudHSM. Puoi lasciare l'archivio delle chiavi personalizzate disconnesso, ma devi connetterlo per poter creare nuove chiavi KMS o utilizzare le chiavi KMS esistenti per operazioni di crittografia. Sostituisci l'ID store chiavi personalizzate di esempio con un ID effettivo.

```
$ aws kms connect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

Connessione e disconnessione di un archivio delle chiavi di AWS CloudHSM

I nuovi archivi delle chiavi di AWS CloudHSM non sono connessi. Prima di creare e utilizzare AWS KMS keys nel tuo archivio delle chiavi di AWS CloudHSM, devi connettere tale archivio al cluster AWS CloudHSM associato. Puoi connettere e disconnettere l'archivio delle chiavi di AWS CloudHSM in qualsiasi momento e visualizzare il relativo stato di connessione.

Non sei obbligato a connettere l'archivio delle chiavi di AWS CloudHSM. Puoi lasciare l'archivio delle chiavi di AWS CloudHSM disconnesso indefinitamente e connetterlo solo quando devi utilizzarlo. Puoi tuttavia testare la connessione periodicamente per verificare che le impostazioni sono corrette e che non vi sono problemi di connessione dello store.

> **Note**
>
> Gli archivi delle chiavi di AWS CloudHSM presentano uno stato di connessione `DISCONNECTED` solo quando l'archivio non è mai stato connesso o se lo si disconnette esplicitamente. Se lo stato di connessione dell'archivio delle chiavi di AWS CloudHSM è `CONNECTED` ma hai problemi ad usarlo, assicurati che il cluster AWS CloudHSM associato sia attivo e contenga almeno un HSM attivo. Per informazioni sugli errori di connessione, consulta the section called “Risoluzione di problemi relativi a store delle chiavi personalizzate”.

Argomenti

- Collegamento di un archivio delle chiavi di AWS CloudHSM
- Disconnessione di un archivio delle chiavi di AWS CloudHSM
- Connessione di un archivio delle chiavi di AWS CloudHSM (console)
- Connessione di uno store delle chiavi personalizzate (API)
- Disconnessione di un archivio delle chiavi di AWS CloudHSM (console)
- Disconnessione di un archivio delle chiavi di AWS CloudHSM (API)

Collegamento di un archivio delle chiavi di AWS CloudHSM

Quando connetti un archivio delle chiavi di AWS CloudHSM, AWS KMS individua il cluster AWS CloudHSM associato, vi si connette, accede al client AWS CloudHSM come crypto user (CU) `kmsuser` e quindi esegue la rotazione della password `kmsuser`. AWS KMS rimane collegato al client AWS CloudHSM fino a che l'archivio delle chiavi di AWS CloudHSM rimane connesso.

Per stabilire la connessione, AWS KMS crea un gruppo di sicurezza denominato `kms-<custom key store ID>` nel cloud privato virtuale (VPC) del cluster. Il gruppo di sicurezza include una singola regola che consente il traffico in entrata dal gruppo di sicurezza del cluster. Inoltre, AWS KMS crea un'interfaccia di rete elastica (ENI) in ogni zona di disponibilità della sottorete privata per il cluster. AWS KMS aggiunge le ENI al gruppo di sicurezza `kms-<cluster ID>` e al gruppo di sicurezza per il cluster. La descrizione di ogni ENI è `KMS managed ENI for cluster <cluster-ID>`.

Il completamento del processo di connessione può richiedere fino a 20 minuti.

Prima di connettere l'archivio delle chiavi di AWS CloudHSM, verifica che soddisfi i seguenti requisiti.

- Il cluster AWS CloudHSM associato deve contenere almeno un HSM attivo. Per trovare il numero di HSM nel cluster, visualizza il cluster nella AWS CloudHSM console o usa l'DescribeClustersoperazione. Se necessario, puoi aggiungere un HSM.
- Il cluster deve disporre di un account crypto user (CU) `kmsuser`, ma tale utente non può essere registrato nel cluster quando si connette l'archivio delle chiavi di AWS CloudHSM. Per informazioni su come effettuare la disconnessione, consulta Come scollegarsi e riconnettersi.
- Lo stato di connessione dell'archivio delle chiavi di AWS CloudHSM non può essere `DISCONNECTING` o `FAILED`. Per visualizzare lo stato della connessione, usa la AWS KMS console o la DescribeCustomKeyStoresrisposta. Se lo stato della connessione è `FAILED`, disconnetti l'archivio delle chiavi personalizzate, correggi il problema e riconnettilo.

Per informazioni sugli errori di connessione, consulta Come correggere un errore di connessione.

Quando l'archivio delle chiavi di AWS CloudHSM è connesso, puoi creare chiavi KMS nello stesso e utilizzare le chiavi KMS esistenti in operazioni di crittografia.

Disconnessione di un archivio delle chiavi di AWS CloudHSM

Quando disconnetti un archivio delle chiavi di AWS CloudHSM, AWS KMS si scollega dal client AWS CloudHSM, si disconnette dal cluster AWS CloudHSM associato e rimuove l'infrastruttura di rete creata per supportare la connessione.

Quando un archivio delle chiavi di AWS CloudHSM è disconnesso, puoi gestire l'archivio delle chiavi di AWS CloudHSM e le relative chiavi KMS, ma non puoi creare o utilizzare le chiavi KMS nell'archivio delle chiavi di AWS CloudHSM. Lo stato di connessione dell'archivio delle chiavi è `DISCONNECTED` e lo stato della chiave delle chiavi KMS nell'archivio delle chiavi personalizzate è `Unavailable`, a meno che non siano `PendingDeletion`. La riconnessione dell'archivio delle chiavi di AWS CloudHSM può avvenire in qualsiasi momento.

Quando disconnetti un archivio delle chiavi personalizzate, le chiavi KMS nell'archivio diventano immediatamente inutilizzabili (in base alla coerenza finale). Tuttavia, le risorse crittografate con chiavi di dati protette dalla chiave KMS non sono interessate fino a quando la chiave KMS non viene nuovamente utilizzata, ad esempio per decrittografare la chiave dati. Questo problema riguarda i Servizi AWS, molti dei quali proteggono le risorse tramite le chiavi dati. Per informazioni dettagliate, vedi In che modo le chiavi KMS inutilizzabili influiscono sulle chiavi dati.

> **Note**
>
> Quando un archivio delle chiavi personalizzate è disconnesso, tutti i tentativi di creare chiavi KMS nell'archivio delle chiavi personalizzate o di utilizzare le chiavi KMS in operazioni di crittografia avrà esito negativo. Questa azione può impedire agli utenti di archiviare e accedere ai dati sensibili.

Per valutare meglio l'effetto della disconnessione dell'archivio delle chiavi personalizzate, identifica le chiavi KMS nell'archivio delle chiavi personalizzate e determinane l'utilizzo precedente.

Puoi disconnettere un archivio delle chiavi di AWS CloudHSM per i seguenti motivi:

- Per effettuare una rotazione della password **`kmsuser`**. AWS KMS modifica la password `kmsuser` ogni volta che si connette al cluster AWS CloudHSM. Per forzare una rotazione della password, esegui la disconnessione e quindi una nuova connessione.
- Per verificare il materiale chiave per le chiavi KMS nel cluster AWS CloudHSM. Quando disconnetti lo store delle chiavi personalizzate, AWS KMS si scollega dall'account del crypto user (CU) `kmsuser` nel client AWS CloudHSM. Ciò ti consente di accedere al cluster come utente di crittografia `kmsuser` e di verificare e gestire il materiale chiave per la chiave KMS.
- Per disabilitare immediatamente tutte le chiavi KMS nell'archivio delle chiavi di AWS CloudHSM. È possibile disabilitare e riattivare le chiavi KMS in un archivio di AWS CloudHSM chiavi utilizzando l'operazione AWS Management Console o. DisableKey Queste operazioni vengono completate rapidamente, ma agiscono su una sola chiave KMS alla volta. Una disconnessione immediata

dell'archivio delle chiavi di AWS CloudHSM modifica lo stato di tutte le chiavi KMS nell'archivio delle chiavi di AWS CloudHSM in `Unavailable`, che ne impedisce l'utilizzo in qualsiasi operazione di crittografia.

- Per riparare un tentativo di connessione non riuscito. Se un tentativo di connessione di un archivio delle chiavi di AWS CloudHSM ha esito negativo (il relativo stato di connessione è `FAILED`), devi disconnettere l'archivio delle chiavi di AWS CloudHSM prima di eseguire un nuovo tentativo di connessione.

Connessione di un archivio delle chiavi di AWS CloudHSM (console)

Per connettere un archivio delle chiavi di AWS CloudHSM nella AWS Management Console, comincia col selezionare l'archivio delle chiavi di AWS CloudHSM nella pagina Custom key stores (Archivi delle chiavi personalizzate). Il completamento del processo di connessione può richiedere fino a 20 minuti.

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Archivi di chiavi personalizzate, Archivi di chiavi AWS CloudHSM.
4. Scegli la riga relativa all'archivio delle chiavi di AWS CloudHSM che vuoi connettere.

   Se lo stato di connessione dell'archivio di chiavi AWS CloudHSM è Non riuscito, devi scollegare l'archivio di chiavi personalizzate prima della connessione.
5. Dal menu Key store actions (Operazioni per l'archivio delle chiavi), scegli Connect (Connetti).

AWS KMS inizia il processo di connessione dello store delle chiavi personalizzate. Trova il cluster AWS CloudHSM associato, crea l'infrastruttura di rete necessaria, si connette alla stessa, accede al cluster AWS CloudHSM come utente di crittografia `kmsuser` ed esegue la rotazione della password `kmsuser`. Al termine dell'operazione, lo stato della connessione diventa Connesso.

Se l'operazione ha esito negativo, viene visualizzato un messaggio di errore che descrive il motivo del problema. Prima di effettuare un nuovo tentativo di connessione, visualizza lo stato della connessione dell'archivio delle chiavi di AWS CloudHSM. Se è Non riuscito, devi scollegare l'archivio

di chiavi personalizzate prima di ricollegarlo. Per assistenza, consulta Risoluzione di problemi relativi a store delle chiavi personalizzate.

Successivo: the section called “Creazione di chiavi KMS in un archivio delle chiavi di AWS CloudHSM”.

Connessione di uno store delle chiavi personalizzate (API)

Per connettere un archivio di AWS CloudHSM chiavi disconnesso, usa l'operazione. ConnectCustomKeyStore Il cluster AWS CloudHSM associato deve contenere almeno un HSM attivo e lo stato della connessione non può essere `FAILED`.

Il completamento del processo di connessione può richiedere fino a 20 minuti. Se l'operazione non genera rapidamente un errore, l'operazione restituisce una risposta HTTP 200 e un oggetto JSON senza proprietà. Questa risposta iniziale non indica tuttavia che la connessione è riuscita. Per determinare lo stato di connessione dell'archivio chiavi personalizzato, consulta la DescribeCustomKeyStoresrisposta.

Gli esempi in questa sezione utilizzano AWS Command Line Interface (AWS CLI), ma puoi usare anche qualsiasi linguaggio di programmazione supportato.

Per identificare l'archivio delle chiavi di AWS CloudHSM, utilizza l'ID archivio delle chiavi personalizzate. È possibile trovare l'ID nella pagina Custom key stores della console o utilizzando l'DescribeCustomKeyStoresoperazione senza parametri. Prima di eseguire questo esempio, sostituisci l'ID di esempio con uno valido.

```
$ aws kms connect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

Per verificare che l'archivio AWS CloudHSM chiavi sia connesso, usa l'DescribeCustomKeyStoresoperazione. Per impostazione predefinita, questa operazione restituisce tutti gli store delle chiavi personalizzate presenti nel tuo account e nella regione. Puoi tuttavia utilizzare il parametro `CustomKeyStoreName` o `CustomKeyStoreId` (ma non entrambi) per limitare la risposta a determinati store delle chiavi personalizzate. Se il valore di `ConnectionState` è `CONNECTED`, indica che lo store delle chiavi personalizzate è connesso al relativo cluster AWS CloudHSM.

> **Note**
>
> Il campo `CustomKeyStoreType` è stato aggiunto alla risposta `DescribeCustomKeyStores` per distinguere gli archivi delle chiavi di AWS CloudHSM da quelli esterni.

```
$ aws kms describe-custom-key-stores --custom-key-store-id cks-1234567890abcdef0
{
   "CustomKeyStores": [
      "CustomKeyStoreId": "cks-1234567890abcdef0",
      "CustomKeyStoreName": "ExampleCloudHSMKeyStore",
      "CloudHsmClusterId": "cluster-1a23b4cdefg",
      "CustomKeyStoreType": "AWS_CLOUDHSM",
      "TrustAnchorCertificate": "<certificate string appears here>",
      "CreationDate": "1.499288695918E9",
      "ConnectionState": "CONNECTED"
   ],
}
```

Se il valore di `ConnectionState` è Failed (Non riuscito), l'elemento `ConnectionErrorCode` indica il motivo dell'errore. In questo caso, AWS KMS non ha trovato un cluster AWS CloudHSM nel tuo account con l'ID cluster `cluster-1a23b4cdefg`. Se hai eliminato il cluster, puoi ripristinarlo a partire da un backup del cluster originale e quindi modificare l'ID cluster per lo store delle chiavi personalizzate. Per informazioni sulla risposta a un codice di errore di connessione, consulta Come correggere un errore di connessione.

```
$ aws kms describe-custom-key-stores --custom-key-store-id cks-1234567890abcdef0
{
   "CustomKeyStores": [
      "CustomKeyStoreId": "cks-1234567890abcdef0",
      "CustomKeyStoreName": "ExampleKeyStore",
      "CloudHsmClusterId": "cluster-1a23b4cdefg",
      "CustomKeyStoreType": "AWS_CLOUDHSM",
      "TrustAnchorCertificate": "<certificate string appears here>",
      "CreationDate": "1.499288695918E9",
      "ConnectionState": "FAILED"
      "ConnectionErrorCode": "CLUSTER_NOT_FOUND"
   ],
}
```

Successivo: Creazione di chiavi KMS in un archivio delle chiavi di AWS CloudHSM.

Disconnessione di un archivio delle chiavi di AWS CloudHSM (console)

Per disconnettere un archivio delle chiavi di AWS CloudHSM nella AWS Management Console, seleziona innanzitutto l'archivio delle chiavi di AWS CloudHSM nella pagina Custom Key Stores (Archivi delle chiavi personalizzate).

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Archivi di chiavi personalizzate, Archivi di chiavi AWS CloudHSM.
4. Scegli la riga relativa all'archivio delle chiavi esterne che vuoi disconnettere.
5. Dal menu Key store actions (Operazioni per l'archivio delle chiavi), scegli Disconnect (Disconnetti).

Al termine dell'operazione, lo stato della connessione da Disconnessione in corso diventa Disconnesso. Se l'operazione ha esito negativo, viene visualizzato un messaggio di errore che descrive il problema e fornisce istruzioni su come risolverlo. Per ulteriori informazioni, consulta Risoluzione di problemi relativi a store delle chiavi personalizzate.

Disconnessione di un archivio delle chiavi di AWS CloudHSM (API)

Per disconnettere un archivio di AWS CloudHSM chiavi connesso, utilizzare l'DisconnectCustomKeyStoreoperazione. Se l'operazione ha esito positivo, AWS KMS restituisce una risposta HTTP 200 e un oggetto JSON senza proprietà.

Gli esempi in questa sezione utilizzano AWS Command Line Interface (AWS CLI), ma puoi usare anche qualsiasi linguaggio di programmazione supportato.

Questo esempio mostra come disconnettere un archivio delle chiavi di AWS CloudHSM. Prima di eseguire questo esempio, sostituisci l'ID di esempio con uno valido.

```
$ aws kms disconnect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

Per verificare che l'archivio AWS CloudHSM chiavi sia disconnesso, utilizzare l'DescribeCustomKeyStoresoperazione. Per impostazione predefinita, questa operazione restituisce

tutti gli store delle chiavi personalizzate presenti nel tuo account e nella regione. Puoi tuttavia utilizzare il parametro `CustomKeyStoreName` o `CustomKeyStoreId` (ma non entrambi) per limitare la risposta a determinati store delle chiavi personalizzate. Se il valore di `ConnectionState` è `DISCONNECTED`, indica che questo archivio delle chiavi di AWS CloudHSM di esempio non è connesso al relativo cluster AWS CloudHSM.

```
$ aws kms describe-custom-key-stores --custom-key-store-id cks-1234567890abcdef0
{
   "CustomKeyStores": [
      "CloudHsmClusterId": "cluster-1a23b4cdefg",
      "ConnectionState": "DISCONNECTED",
      "CreationDate": "1.499288695918E9",
      "CustomKeyStoreId": "cks-1234567890abcdef0",
      "CustomKeyStoreName": "ExampleKeyStore",
      "CustomKeyStoreType": "AWS_CLOUDHSM",
      "TrustAnchorCertificate": "<certificate string appears here>"
   ],
}
```

Eliminazione di un archivio delle chiavi di AWS CloudHSM

Quando elimini un archivio delle chiavi di AWS CloudHSM, AWS KMS elimina tutti i metadati relativi a tale archivio AWS CloudHSM da KMS, incluse informazioni sull'associazione con un cluster AWS CloudHSM. Questa operazione non influisce sul cluster AWS CloudHSM, i relativi HSM o utenti. Puoi creare un nuovo archivio delle chiavi di AWS CloudHSM associato allo stesso cluster AWS CloudHSM associato, ma non puoi annullare l'operazione di eliminazione.

Solo un archivio delle chiavi di AWS CloudHSM disconnesso dal relativo cluster AWS CloudHSM e non contenente AWS KMS keys può essere eliminato. Prima di eliminare uno store delle chiavi personalizzate, esegui le operazioni descritte di seguito.

- Verifica che non avrai la necessità di utilizzare alcuna chiave KMS presente nell'archivio delle chiavi per qualsiasi operazione di crittografia. Quindi pianifica l'eliminazione di tutte le chiavi KMS dall'archivio delle chiavi. Per informazioni su come identificare le chiavi KMS in un archivio delle chiavi di AWS CloudHSM, consulta Ricerca delle chiavi KMS in un archivio delle chiavi di AWS CloudHSM.
- Verifica che tutte le chiavi KMS siano state eliminate. Per visualizzare le chiavi KMS in un archivio delle chiavi di AWS CloudHSM, consulta Visualizzazione delle chiavi KMS in un archivio delle chiavi di AWS CloudHSM.

- Disconnetti l'archivio delle chiavi di AWS CloudHSM dal relativo cluster AWS CloudHSM.

Anziché eliminare l'archivio delle chiavi di AWS CloudHSM, puoi disconnetterlo dal cluster AWS CloudHSM associato. Quando un AWS CloudHSM archivio delle chiavi di AWS CloudHSM è disconnesso, puoi gestirlo insieme alle relative AWS KMS keys. Tuttavia, non puoi creare o utilizzare le chiavi KMS nell'archivio delle chiavi di AWS CloudHSM. La riconnessione dell'archivio delle chiavi di AWS CloudHSM può avvenire in qualsiasi momento.

Argomenti

- Eliminazione di un archivio delle chiavi di AWS CloudHSM (console)
- Eliminazione di un archivio delle chiavi di AWS CloudHSM (API)

Eliminazione di un archivio delle chiavi di AWS CloudHSM (console)

Per eliminare un archivio delle chiavi di AWS CloudHSM nella AWS Management Console, comincia col selezionare l'archivio AWS CloudHSM nella pagina Custom key stores (Archivi delle chiavi personalizzate).

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Archivi di chiavi personalizzate, Archivi di chiavi AWS CloudHSM.
4. Trova la riga che rappresenta l'archivio delle chiavi di AWS CloudHSM da rimuovere. Se lo Stato connessione dell'archivio di chiavi AWS CloudHSM non è Disconnesso, devi scollegare l'archivio di chiavi AWS CloudHSM prima di eliminarlo.
5. Dal menu Key store actions (Operazioni per l'archivio delle chiavi), scegli Delete (Elimina).

Al termine dell'operazione, viene visualizzato un messaggio di conferma e l'archivio delle chiavi di AWS CloudHSM non viene più visualizzato nel relativo elenco. Se l'operazione ha esito negativo, viene visualizzato un messaggio di errore che descrive il problema e fornisce istruzioni su come risolverlo. Per ulteriori informazioni, consulta Risoluzione di problemi relativi a store delle chiavi personalizzate.

Eliminazione di un archivio delle chiavi di AWS CloudHSM (API)

Per eliminare un archivio di AWS CloudHSM chiavi, utilizzare l'DeleteCustomKeyStoreoperazione. Se l'operazione ha esito positivo, AWS KMS restituisce una risposta HTTP 200 e un oggetto JSON senza proprietà.

Per iniziare, verifica che l'archivio delle chiavi di AWS CloudHSM non contenga alcuna AWS KMS keys. Non puoi eliminare un archivio delle chiavi personalizzate che contiene chiavi KMS. Il primo comando di esempio utilizza ListKeyse DescribeKeycerca AWS KMS keys nell'archivio AWS CloudHSM chiavi con l'esempio *cks-1234567890abcdef0* ID di archiviazione chiavi personalizzato. In questo caso, il comando non restituisce alcuna chiave KMS. In caso affermativo, utilizza l'ScheduleKeyDeletionoperazione per pianificare l'eliminazione di ciascuna chiave KMS.

Bash

```
for key in $(aws kms list-keys --query 'Keys[*].KeyId' --output text) ;
do aws kms describe-key --key-id $key |
grep '"CustomKeyStoreId": "cks-1234567890abcdef0"' --context 100; done
```

PowerShell

```
PS C:\> Get-KMSKeyList | Get-KMSKey | where CustomKeyStoreId -eq
 'cks-1234567890abcdef0'
```

Successivamente, disconnetti l'archivio delle chiavi di AWS CloudHSM. Questo comando di esempio utilizza l'DisconnectCustomKeyStoreoperazione per disconnettere un archivio di AWS CloudHSM chiavi dal relativo AWS CloudHSM cluster. Prima di eseguire questo comando, sostituisci l'ID store chiavi personalizzate di esempio con uno valido.

Bash

```
$ aws kms disconnect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

PowerShell

```
PS C:\> Disconnect-KMSCustomKeyStore -CustomKeyStoreId cks-1234567890abcdef0
```

Dopo la disconnessione dell'archivio chiavi personalizzato, è possibile utilizzare l'DeleteCustomKeyStoreoperazione per eliminarlo.

Bash

```
$ aws kms delete-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

PowerShell

```
PS C:\> Remove-KMSCustomKeyStore -CustomKeyStoreId cks-1234567890abcdef0
```

Gestione di chiavi KMS in un archivio delle chiavi di CloudHSM

Puoi creare, visualizzare, gestire, utilizzare e pianificare l'eliminazione della AWS KMS keys in un archivio delle chiavi di AWS CloudHSM. Le procedure utilizzate sono molto simili a quelle impiegate per le altre chiavi KMS. L'unica differenza è che specifichi un archivio delle chiavi di AWS CloudHSM quando crei la chiave KMS. Successivamente, AWS KMS crea il materiale della chiave non estraibile per la chiave KMS nel cluster AWS CloudHSM associato all'archivio delle chiavi di AWS CloudHSM. Quando utilizzi una chiave KMS in un archivio delle chiavi di AWS CloudHSM, le operazioni di crittografia vengono eseguite negli HSM nel cluster.

Funzionalità supportate

Oltre alle procedure discusse in questa sezione, puoi eseguire le seguenti operazioni con le chiavi KMS in un archivio delle chiavi di AWS CloudHSM:

- Utilizzare le policy delle chiavi, le policy IAM e le concessioni per autorizzare l'accesso alle chiavi KMS.
- Abilitare e disabilitare le chiavi KMS.
- Assegnare tag, creare alias e utilizzare il controllo degli accessi basato su attributi (ABAC) per autorizzare l'accesso alle chiavi KMS.
- Utilizza le chiavi KMS per operazioni di crittografia, ad esempio crittografia, decrittazione, ricrittografia e generazione di chiavi di dati.
- Utilizzare le chiavi KMS con servizi AWS che si integrano con AWS KMS e supportano le chiavi gestite dal cliente.
- Tieni traccia dell'uso delle tue chiavi KMS nei AWS CloudTraillog e negli strumenti di CloudWatch monitoraggio di Amazon.

Caratteristiche non supportate

- Gli archivi delle chiavi di AWS CloudHSM supportano solo chiavi KMS di crittografia simmetrica. Non puoi creare chiavi KMS HMAC, chiavi KMS asimmetriche o coppie di chiavi di dati asimmetriche in un archivio delle chiavi di AWS CloudHSM.
- Non puoi importare il materiale della chiave in una chiave KMS in un archivio delle chiavi di AWS CloudHSM. AWS KMS genera il materiale della chiave per la chiave KMS nel cluster AWS CloudHSM.
- Non puoi abilitare o disabilitare la rotazione automatica del materiale della chiave per una chiave KMS in un archivio delle chiavi di AWS CloudHSM.

Argomenti

Creazione di chiavi KMS in un archivio delle chiavi di AWS CloudHSM

Dopo aver creato un archivio delle chiavi di AWS CloudHSM, puoi creare AWS KMS keys nell'archivio delle chiavi. Devono essere chiavi KMS di crittografia simmetrica con materiale della chiave generato da AWS KMS. Non è possibile creare chiavi KMS asimmetriche, chiavi KMS HMAC o chiavi KMS con materiale della chiave importato in un archivio delle chiavi personalizzate. Inoltre, non è possibile utilizzare chiavi KMS di crittografia simmetrica in un archivio delle chiavi personalizzate per generare coppie di chiavi di dati asimmetriche.

Per creare una chiave KMS in un archivio delle chiavi di AWS CloudHSM, l'archivio delle chiavi di AWS CloudHSM deve essere connesso al cluster AWS CloudHSM associato e il cluster deve contenere almeno due HSM attivi in zone di disponibilità differenti. Per trovare lo stato di connessione e il numero di HSM, visualizza la pagina degli archivi delle chiavi di AWS CloudHSM nella AWS Management Console. Quando si utilizzano le operazioni API, utilizzare l'DescribeCustomKeyStoresoperazione per verificare che l'archivio delle AWS CloudHSM chiavi sia connesso. Per verificare il numero di HSM attivi nel cluster e le relative zone di disponibilità, utilizza l'AWS CloudHSMDescribeClustersoperazione.

Quando crei una chiave KMS nell'archivio delle chiavi di AWS CloudHSM, AWS KMS genera la chiave KMS in AWS KMS. Il materiale della chiave viene creato per la chiave KMS nel cluster AWS CloudHSM associato. Più precisamente, AWS KMS accede al cluster come il CU `kmsuser` che hai creato. Crea quindi una chiave simmetrica AES (Advanced Encryption Standard) a 256 bit non estraibile e persistente nel cluster. AWS KMS imposta il valore dell'attributo dell'etichetta di chiave, visibile solo nel cluster, sull'Amazon Resource Name (ARN) della chiave KMS.

Quando il comando riesce, lo stato di chiave della nuova chiave KMS è `Enabled` e la relativa origine è `AWS_CLOUDHSM`. Non puoi modificare l'origine di una chiave KMS dopo averla creata. Quando si visualizza una chiave KMS in un archivio AWS CloudHSM chiavi della AWS KMS console o utilizzando l'DescribeKeyoperazione, è possibile visualizzare le proprietà tipiche, come l'ID della chiave, lo stato della chiave e la data di creazione. Ma puoi anche visualizzare l'ID store chiavi personalizzate ed eventualmente l'ID del cluster AWS CloudHSM. Per informazioni dettagliate, vedi Visualizzazione delle chiavi KMS in un archivio delle chiavi di AWS CloudHSM.

Se il tentativo di creare una chiave KMS nell'archivio delle chiavi di AWS CloudHSM ha esito negativo, utilizza il messaggio di errore per determinarne la causa. Questo messaggio potrebbe indicare che l'archivio delle chiavi di AWS CloudHSM non è connesso (`CustomKeyStoreInvalidStateException`) o che il cluster AWS CloudHSM associato non dispone dei due HSM attivi necessari per questa operazione (`CloudHsmClusterInvalidConfigurationException`). Per assistenza, consulta Risoluzione di problemi relativi a store delle chiavi personalizzate.

Per un esempio del log AWS CloudTrail relativo all'operazione in grado di creare una chiave KMS in un archivio delle chiavi di AWS CloudHSM, consulta CreateKey.

Argomenti

- Creazione di una chiave KMS in un archivio delle chiavi di AWS CloudHSM (console)
- Creazione di una chiave KMS in un archivio delle chiavi di AWS CloudHSM (API)

Creazione di una chiave KMS in un archivio delle chiavi di AWS CloudHSM (console)

Utilizza la procedura seguente per creare una chiave KMS di crittografia simmetrica in un archivio delle chiavi di AWS CloudHSM.

> **Note**
>
> Non includere informazioni riservate o sensibili nell'alias, nella descrizione o nei tag. Questi campi possono apparire in testo semplice nei CloudTrail log e in altri output.

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.
4. Scegliere Create key (Crea chiave).
5. Scegliere Symmetric (Simmetrica).
6. In Key usage (Utilizzo della chiave), l'opzione Encrypt and decrypt (Crittografa e decrittografa) è selezionata per default. Non modificarla.
7. Scegliere Advanced options (Opzioni avanzate).
8. Per Origine del materiale della chiave, scegli Archivio di chiavi AWS CloudHSM.

   Non è possibile creare una chiave multi-regione in un archivio delle chiavi di AWS CloudHSM.
9. Seleziona Avanti.
10. Seleziona un archivio delle chiavi di AWS CloudHSM per la nuova chiave KMS. Per creare un nuovo archivio delle chiavi di AWS CloudHSM, scegli Create custom key store (Crea un archivio delle chiavi personalizzate).

    Lo stato dell'archivio di chiavi AWS CloudHSM selezionato deve essere Connesso. Il cluster AWS CloudHSM associato deve essere attivo e contenere almeno due HSM attivi in zone di disponibilità differenti.

    Per informazioni sulla connessione di un archivio delle chiavi di AWS CloudHSM, consulta Connessione e disconnessione di un archivio delle chiavi di AWS CloudHSM. Per informazioni sull'aggiunta di HSM, consulta Aggiunta di un HSM nella Guida per l'utente di AWS CloudHSM.
11. Seleziona Avanti.
12. Digita un alias ed eventualmente una descrizione per la chiave KMS.
13. (Facoltativo). Nella pagina Add Tags (Aggiungi tag), aggiungi i tag che identificano o categorizzano la chiave KMS.

Quando aggiungi i tag alle risorse AWS, AWS genera un report di allocazione dei costi in cui l'utilizzo e i costi sono aggregati in base ai tag. I tag possono essere utilizzati anche per controllare l'accesso a una chiave KMS. Per informazioni sull'assegnazione di tag delle chiavi KMS, consulta Chiavi di tagging e ABAC per AWS KMS.

14. Seleziona Next (Successivo).
15. Nella sezione amministratori delle chiavi, seleziona utenti IAM e ruoli IAM che possono gestire la chiave KMS. Per ulteriori informazioni, consulta Consente agli amministratori delle chiavi di amministrare la chiave KMS.

> **Note**
>
> Le policy IAM possono fornire ad altri ruoli e utenti IAM l'autorizzazione per utilizzare la chiave KMS.
> Le best practice di IAM disincentivano l'uso di utenti IAM con credenziali a lungo termine. Quando possibile, utilizza i ruoli IAM che forniscono credenziali temporanee. Per i dettagli, consulta la sezione Best practice di sicurezza in IAM nella Guida per l'utente IAM.

16. (Facoltativo) Per impedire a questi amministratori delle chiavi di eliminare questa chiave KMS, nella parte inferiore della pagina deseleziona Allow key administrators to delete this key. (Consenti agli amministratori delle chiavi di eliminare questa chiave).
17. Seleziona Avanti.
18. Nella sezione Questo account, seleziona i ruoli e gli utenti IAM in questo Account AWS che possono utilizzare la chiave KMS nelle operazioni di crittografia. Per ulteriori informazioni, consulta Consente agli utenti della chiave di utilizzare la chiave KMS.

> **Note**
>
> Le policy IAM possono fornire ad altri ruoli e utenti IAM l'autorizzazione per utilizzare la chiave KMS.
> Le best practice di IAM disincentivano l'uso di utenti IAM con credenziali a lungo termine. Quando possibile, utilizza i ruoli IAM che forniscono credenziali temporanee. Per i dettagli, consulta la sezione Best practice di sicurezza in IAM nella Guida per l'utente IAM.

19. (Facoltativo) È possibile consentire ad altri Account AWS di utilizzare questa chiave KMS per operazioni di crittografia. A questo proposito, nella sezione Altri Account AWS, nella parte inferiore della pagina, scegli Aggiungi un altro Account AWS e inserisci l'ID Account AWS di un account esterno. Per aggiungere più account esterni, ripetere questo passaggio.

    > **Note**
    >
    > Anche gli amministratori degli altri Account AWS devono consentire l'accesso alla chiave KMS creando policy IAM per i propri utenti. Per ulteriori informazioni, consulta la pagina Autorizzazione per gli utenti in altri account di utilizzare una chiave KMS.

20. Seleziona Next (Successivo).
21. Esaminare le principali impostazioni scelte. È comunque possibile tornare indietro e modificare tutte le impostazioni.
22. Al termine, scegli Crea filtro.

Quando la procedura riesce, la visualizzazione mostra la nuova chiave KMS nell'archivio delle chiavi di AWS CloudHSM scelto. Quando scegli il nome o l'alias della nuova chiave KMS, la scheda Cryptographic configuration (Configurazione crittografica) nella pagina dei dettagli visualizza l'origine della chiave KMS (AWS CloudHSM), nonché il nome, l'ID e il tipo di archivio delle chiavi personalizzate e l'ID del cluster AWS CloudHSM. Se la procedura ha esito negativo, viene visualizzato un messaggio di errore che descrive l'errore.

> **Tip**
>
> Per agevolare l'identificazione delle chiavi KMS in uno store delle chiavi personalizzate, nella pagina Chiavi gestite cliente, aggiungi la colonna ID dell'archivio delle chiavi personalizzate alla visualizzazione. Fai clic sull'icona che raffigura un ingranaggio in alto a destra e seleziona Custom key store ID (ID store chiavi personalizzate). Per informazioni dettagliate, vedi Personalizzazione delle tabelle delle chiavi KMS.

Creazione di una chiave KMS in un archivio delle chiavi di AWS CloudHSM (API)

Per creare una nuova AWS KMS key(chiave KMS) nel tuo archivio AWS CloudHSM chiavi, usa l'CreateKeyoperazione. Utilizza il parametro `CustomKeyStoreId` per identificare lo store e specifica `AWS_CLOUDHSM` per `Origin`.

Potresti anche voler utilizzare il parametro `Policy` per specificare una policy delle chiavi. Puoi modificare la politica chiave (PutKeyPolicy) e aggiungere elementi opzionali, come una descrizione e dei tag in qualsiasi momento.

Gli esempi in questa sezione utilizzano AWS Command Line Interface (AWS CLI), ma puoi usare anche qualsiasi linguaggio di programmazione supportato.

L'esempio seguente inizia con una chiamata all'DescribeCustomKeyStoresoperazione per verificare che l'archivio AWS CloudHSM chiavi sia connesso al AWS CloudHSM cluster associato. Per impostazione predefinita, questa operazione restituisce tutti gli store delle chiavi personalizzate presenti nel tuo account e nella regione. Per descrivere solo un determinato archivio delle chiavi di AWS CloudHSM, utilizza il parametro `CustomKeyStoreId` o `CustomKeyStoreName`, ma non entrambi.

Prima di eseguire questo comando, sostituisci l'ID store chiavi personalizzate di esempio con un ID valido.

> **Note**
>
> Non includere informazioni riservate o sensibili nei campi `Description` o `Tags`. Questi campi possono apparire in testo semplice nei CloudTrail log e in altri output.

```
$ aws kms describe-custom-key-stores --custom-key-store-id cks-1234567890abcdef0
{
   "CustomKeyStores": [
      "CustomKeyStoreId": "cks-1234567890abcdef0",
      "CustomKeyStoreName": "ExampleKeyStore",
      "CustomKeyStoreType": "AWS CloudHSM key store",
      "CloudHsmClusterId": "cluster-1a23b4cdefg",
      "TrustAnchorCertificate": "<certificate string appears here>",
      "CreationDate": "1.499288695918E9",
      "ConnectionState": "CONNECTED"
   ],
}
```

Il comando di esempio successivo utilizza l'DescribeClustersoperazione per verificare che il AWS CloudHSM cluster associato a `ExampleKeyStore` (cluster-1a23b4cdefg) abbia almeno due moduli di protezione hardware attivi. Se il cluster ha meno di due HSM, l'operazione `CreateKey` ha esito negativo.

```
$ aws cloudhsmv2 describe-clusters
{
    "Clusters": [
        {
            "SubnetMapping": {
               ...
            },
            "CreateTimestamp": 1507133412.351,
            "ClusterId": "cluster-1a23b4cdefg",
            "SecurityGroup": "sg-865af2fb",
            "HsmType": "hsm1.medium",
            "VpcId": "vpc-1a2b3c4d",
            "BackupPolicy": "DEFAULT",
            "Certificates": {
                "ClusterCertificate": "-----BEGIN CERTIFICATE-----\...\n-----END
 CERTIFICATE-----\n"
            },
            "Hsms": [
                {
                    "AvailabilityZone": "us-west-2a",
                    "EniIp": "10.0.1.11",
                    "ClusterId": "cluster-1a23b4cdefg",
                    "EniId": "eni-ea8647e1",
                    "StateMessage": "HSM created.",
                    "SubnetId": "subnet-a6b10bd1",
                    "HsmId": "hsm-abcdefghijk",
                    "State": "ACTIVE"
                },
                {
                    "AvailabilityZone": "us-west-2b",
                    "EniIp": "10.0.0.2",
                    "ClusterId": "cluster-1a23b4cdefg",
                    "EniId": "eni-ea8647e1",
                    "StateMessage": "HSM created.",
                    "SubnetId": "subnet-b6b10bd2",
                    "HsmId": "hsm-zyxwvutsrqp",
                    "State": "ACTIVE"
                },
            ],
            "State": "ACTIVE"
        }
    ]
}
```

Questo comando di esempio utilizza l'CreateKeyoperazione per creare una chiave KMS in un archivio di chiavi. AWS CloudHSM Per creare una chiave KMS in un archivio delle chiavi di AWS CloudHSM, devi fornire l'ID archivio delle chiavi personalizzate dell'archivio delle chiavi di AWS CloudHSM e specificare un valore `Origin` per `AWS_CLOUDHSM`.

La risposta include gli ID dello store delle chiavi personalizzate e del cluster AWS CloudHSM.

Prima di eseguire questo comando, sostituisci l'ID store chiavi personalizzate di esempio con un ID valido.

```
$ aws kms create-key --origin AWS_CLOUDHSM --custom-key-store-id cks-1234567890abcdef0
{
  "KeyMetadata": {
    "AWSAccountId": "111122223333",
    "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "CreationDate": 1.499288695918E9,
    "Description": "Example key",
    "Enabled": true,
    "MultiRegion": false,
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "KeyManager": "CUSTOMER",
    "KeyState": "Enabled",
    "KeyUsage": "ENCRYPT_DECRYPT",
    "Origin": "AWS_CLOUDHSM"
    "CloudHsmClusterId": "cluster-1a23b4cdefg",
    "CustomKeyStoreId": "cks-1234567890abcdef0"
    "KeySpec": "SYMMETRIC_DEFAULT",
    "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
    "EncryptionAlgorithms": [
        "SYMMETRIC_DEFAULT"
    ]
  }
}
```

Visualizzazione delle chiavi KMS in un archivio delle chiavi di AWS CloudHSM

Per visualizzare AWS KMS keys in un archivio delle chiavi di AWS CloudHSM, utilizza le stesse tecniche che useresti per visualizzare qualsiasi chiave gestita dal cliente AWS KMS. Per le nozioni di base sulla visualizzazione di chiavi, consulta Visualizzazione di chiavi. Per identificare nel cluster AWS CloudHSM le chiavi che fungono da materiale della chiave per la chiave KMS, consulta Ricerca di chiavi KMS e di materiale della chiave. Per informazioni sulla visualizzazione dei registri AWS

CloudTrail che registrano tutte le operazioni delle API in un archivio delle chiavi personalizzate, consultare Registrazione delle chiamate API AWS KMS con AWS CloudTrail.

Nella console AWS KMS, le chiavi KMS nell'archivio delle chiavi personalizzate vengono visualizzate nella pagina delle chiavi gestite dal cliente, insieme a tutte le altre chiavi gestite dal cliente presenti in un Account AWS e nella regione.

Tuttavia, i valori seguenti sono specifici delle chiavi KMS in un archivio delle chiavi di AWS CloudHSM.

- Il nome e l'ID dell'archivio delle chiavi di AWS CloudHSM in cui si trova la chiave KMS.
- L'ID cluster del cluster AWS CloudHSM associato che contiene il relativo materiale della chiave.
- Il campo `Origin` con valore `AWS CloudHSM` nella console AWS KMS o `AWS_CLOUDHSM` nelle risposte API.
- Il valore dello stato di chiave può essere `Unavailable`. Per informazioni sulla risoluzione dello stato, consulta Come correggere chiavi KMS non disponibili.

Per visualizzare le chiavi KMS in un archivio delle chiavi di AWS CloudHSM (console)

1. Aprire la console AWS KMS all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.
4. Nell'angolo in alto a destra, scegliere l'icona che raffigura un ingranaggio, scegliere Custom key store ID (ID store chiavi personalizzate) e Origin (Origine), quindi Confirm (Conferma).
5. Per identificare le chiavi KMS in qualsiasi archivio delle chiavi di AWS CloudHSM, cerca le chiavi KMS il cui campo Origin (Origine) ha valore AWS CloudHSM. Per identificare le chiavi KMS in un determinato archivio delle chiavi di AWS CloudHSM, visualizza i valori nella colonna Custom key store ID (ID dell'archivio chiavi personalizzate).
6. Scegli l'alias o l'ID chiave di una chiave KMS in un archivio delle chiavi di AWS CloudHSM.

   In questa pagina vengono visualizzate informazioni dettagliate sulla chiave KMS, inclusi l'Amazon Resource Name (ARN), la policy delle chiavi e i tag.
7. Scegli la tab Configurazione crittografica. Le schede si trovano al di sotto della sezione Configurazione generale.

Questa sezione contiene informazioni sull'archivio delle chiavi di AWS CloudHSM e sul cluster AWS CloudHSM associato alla chiave KMS.

Per visualizzare le chiavi KMS in un archivio delle chiavi personalizzate (API)

Utilizzi le stesse operazioni AWS KMS API per visualizzare le chiavi KMS in un archivio di AWS CloudHSM chiavi che utilizzeresti per qualsiasi chiave KMS, tra cui ListKeysDescribeKey, e. GetKeyPolicy Ad esempio, l'operazione `describe-key` seguente in AWS CLI mostra i campi speciali per una chiave KMS in un archivio delle chiavi di AWS CloudHSM. Prima di eseguire un comando come questo, sostituisci l'ID della chiave KMS di esempio con un valore valido.

```
$ aws kms describe-key --key-id 1234abcd-12ab-34cd-56ef-1234567890ab

{
   "KeyMetadata": {
      "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "AWSAccountId": "111122223333",
      "CloudHsmClusterId": "cluster-1a23b4cdefg",
      "CreationDate": 1537582718.431,
      "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
      "CustomKeyStoreId": "cks-1234567890abcdef0",
      "Description": "Key in custom key store",
      "Enabled": true,
      "EncryptionAlgorithms": [
         "SYMMETRIC_DEFAULT"
      ],
      "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
      "KeyManager": "CUSTOMER",
      "KeySpec": "SYMMETRIC_DEFAULT",
      "KeyState": "Enabled",
      "KeyUsage": "ENCRYPT_DECRYPT",
      "MultiRegion": false,
      "Origin": "AWS_CLOUDHSM"
   }
}
```

Per informazioni sulla ricerca di chiavi KMS in un archivio delle chiavi di AWS CloudHSM o sull'identificazione delle chiavi nel cluster AWS CloudHSM che funge da materiale della chiave per la chiave KMS, consulta Ricerca di chiavi KMS e di materiale della chiave.

Uso delle chiavi KMS in un archivio delle chiavi di AWS CloudHSM

Dopo aver creato una chiave KMS di crittografia simmetrica in un archivio delle chiavi di AWS CloudHSM, puoi utilizzarla per le seguenti operazioni di crittografia:

- Encrypt
- Decrypt
- GenerateDataKey
- GenerateDataKeyWithoutPlaintext
- ReEncrypt

Le operazioni che generano coppie di chiavi di dati asimmetriche GenerateDataKeyPaire GenerateDataKeyPairWithoutPlaintext, non sono supportate negli archivi di chiavi personalizzati.

Quando utilizzi la chiave KMS in una richiesta, identificando la chiave KMS tramite il relativo ID o alias; non devi specificare l'archivio delle chiavi di AWS CloudHSM o il cluster AWS CloudHSM. La risposta include gli stessi campi che vengono restituiti per qualsiasi chiave KMS di crittografia simmetrica.

Tuttavia, quando utilizzi una chiave KMS in un archivio delle chiavi di AWS CloudHSM, l'operazione di crittografia viene eseguita interamente all'interno del cluster AWS CloudHSM associato all'archivio delle chiavi di AWS CloudHSM. L'operazione utilizza il materiale della chiave nel cluster associato alla chiave KMS scelta.

Perché ciò avvenga, devono essere soddisfatte le seguenti condizioni.

- Lo stato di chiave della chiave KMS deve essere `Enabled`. Per trovare lo stato della chiave, utilizza il campo Status nella AWS KMSconsole o il `KeyState` campo nella risposta. DescribeKey
- L'archivio delle chiavi di AWS CloudHSM deve essere connesso al relativo cluster AWS CloudHSM. Il relativo stato nella AWS KMSconsole o `ConnectionState` nella DescribeCustomKeyStoresrisposta deve essere`CONNECTED`.
- Il cluster AWS CloudHSM associato allo store delle chiavi personalizzate deve contenere almeno un HSM attivo. Per trovare il numero di moduli di protezione hardware attivi nel cluster, usa la AWS KMSconsole, la AWS CloudHSM console o l'DescribeClustersoperazione.
- Il cluster AWS CloudHSM deve contenere il materiale della chiave per la chiave KMS. Se questo materiale è stato eliminato dal cluster oppure un HSM è stato creato a partire da un backup che non includeva quel materiale, l'operazione di crittografia non riuscirà.

Se queste condizioni non sono soddisfatte, l'operazione di crittografia non riesce e AWS KMS restituisce un'eccezione `KMSInvalidStateException`. In genere, è sufficiente riconnettere l'archivio delle chiavi di AWS CloudHSM. Per ulteriori informazioni, consulta Come correggere una chiave KMS non funzionante.

Quando utilizzi le chiavi KMS in un archivio delle chiavi di AWS CloudHSM, tieni presente che le chiavi KMS in ogni archivio delle chiavi di AWS CloudHSM condividono una quota di richiesta dell'archivio delle chiavi personalizzate per le operazioni di crittografia. Se superi la quota, AWS KMS restituisce una `ThrottlingException`. Se il cluster AWS CloudHSM associato all'archivio delle chiavi di AWS CloudHSM elabora numerosi comandi, inclusi quelli non collegati all'archivio delle chiavi di AWS CloudHSM, è possibile che venga generato `ThrottlingException` a una frequenza ancora inferiore. Se viene generata un'eccezione `ThrottlingException` per una qualsiasi richiesta, riduci la frequenza delle richieste e riesegui i comandi. Per informazioni dettagliate sulle quote di richiesta dell'archivio delle chiavi personalizzate, consulta Quote di richiesta per l'archivio delle chiavi personalizzate.

Ricerca di chiavi KMS e di materiale della chiave

Se gestisci un archivio delle chiavi di AWS CloudHSM, potresti dover identificare le chiavi KMS in ogni archivio delle chiavi di AWS CloudHSM. Ad esempio, potresti aver bisogno di eseguire alcune delle operazioni seguenti.

- Monitorare le chiavi KMS presenti nell'archivio delle chiavi di AWS CloudHSM nei log AWS CloudTrail.
- Prevedere l'effetto sulle chiavi KMS della disconnessione di un archivio delle chiavi di AWS CloudHSM.
- Pianifica l'eliminazione di chiavi KMS prima di eliminare un archivio delle chiavi di AWS CloudHSM.

Inoltre, potresti voler identificare nel cluster AWS CloudHSM le chiavi che fungono da materiale della chiave per le chiavi KMS. Sebbene AWS KMS gestisca le chiavi KMS e il relativo materiale della chiave, hai sempre il controllo e la responsabilità della gestione del cluster AWS CloudHSM, dei relativi HSM e backup nonché delle chiavi negli HSM. È possibile che sia necessario identificare le chiavi per controllare il materiale della chiave, proteggerlo da un'eliminazione accidentale o eliminarlo dagli HSM e dai backup del cluster dopo l'eliminazione della chiave KMS.

Tutto il materiale per le chiavi KMS nel tuo archivio delle chiavi di AWS CloudHSM è di proprietà del crypto user (CU) `kmsuser`. AWS KMS imposta l'attributo dell'etichetta di chiave, visualizzabile solo in AWS CloudHSM, nel nome della risorsa Amazon (ARN) della chiave KMS.

Per trovare le chiavi KMS e il materiale della chiave, utilizza una delle tecniche seguenti.

- Ricerca delle chiavi KMS in un archivio delle chiavi di AWS CloudHSM: come identificare le chiavi KMS in uno o in tutti gli archivi delle chiavi di AWS CloudHSM.
- Ricerca di tutte le chiavi per un archivio delle chiavi di AWS CloudHSM: come trovare nel cluster tutte le chiavi che fungono da materiale della chiave per le chiavi KMS nell'archivio delle chiavi di AWS CloudHSM.
- Ricerca della chiave di AWS CloudHSM per una chiave KMS: come trovare nel cluster la chiave che funge da materiale della chiave per una particolare chiave KMS nell'archivio delle chiavi di AWS CloudHSM.
- Ricerca della chiave KMS per una chiave di AWS CloudHSM — Come trovare la chiave KMS per un determinata chiave nel cluster.

Ricerca delle chiavi KMS in un archivio delle chiavi di AWS CloudHSM

Se gestisci un archivio delle chiavi di AWS CloudHSM, potresti dover identificare le chiavi KMS in ogni archivio delle chiavi di AWS CloudHSM. Puoi utilizzare queste informazioni per monitorare le operazioni della chiave KMS nei log AWS CloudTrail, prevedere l'effetto sulle chiavi KMS della disconnessione di un archivio delle chiavi personalizzate o pianificare l'eliminazione di chiavi KMS prima di eliminare un archivio delle chiavi di AWS CloudHSM.

Per trovare le chiavi KMS in un archivio delle chiavi di AWS CloudHSM (console)

Per trovare le chiavi KMS in un determinato archivio delle chiavi di AWS CloudHSM, nella pagina Customer managed keys (Chiavi gestite dal cliente), visualizza i valori dei campi Custom Key Store Name (Nome dell'archivio delle chiavi personalizzate) o Custom Key Store ID (ID dell'archivio chiavi personalizzate). Per identificare le chiavi KMS in qualsiasi archivio delle chiavi di AWS CloudHSM, cerca le chiavi KMS il cui campo Origin (Origine) ha valore AWS CloudHSM. Per aggiungere colonne facoltative alla visualizzazione, scegli l'icona che raffigura un ingranaggio nell'angolo in alto a destra della pagina.

Per trovare le chiavi KMS in un archivio delle chiavi di AWS CloudHSM (API)

Per trovare le chiavi KMS in un archivio AWS CloudHSM chiavi, usa le DescribeKeyoperazioni ListKeysand, quindi filtra per `CustomKeyStoreId` valore. Prima di eseguire gli esempi, sostituisci i valori dell'ID store chiavi personalizzate fittizio con una valore valido.

Bash

Per trovare le chiavi KMS in un determinato archivio delle chiavi di AWS CloudHSM, ottieni tutte le chiavi KMS dell'account e della regione. Quindi filtra in base all'ID dell'archivio delle chiavi personalizzate.

```
for key in $(aws kms list-keys --query 'Keys[*].KeyId' --output text) ;
do aws kms describe-key --key-id $key |
grep '"CustomKeyStoreId": "cks-1234567890abcdef0"' --context 100; done
```

Per ottenere le chiavi KMS di qualsiasi archivio delle chiavi di AWS CloudHSM nell'account e nella regione, cerca `CustomKeyStoreType` con il valore `AWS_CloudHSM`.

```
for key in $(aws kms list-keys --query 'Keys[*].KeyId' --output text) ;
do aws kms describe-key --key-id $key |
grep '"CustomKeyStoreType": "AWS_CloudHSM"' --context 100; done
```

PowerShell

Per trovare le chiavi KMS in un particolare archivio AWS CloudHSM chiavi, utilizza i KmsKey cmdlet Get- KmsKeyList e Get- per ottenere tutte le chiavi KMS nell'account e nella regione. Quindi filtra in base all'ID dell'archivio delle chiavi personalizzate.

```
PS C:\> Get-KMSKeyList | Get-KMSKey | where CustomKeyStoreId -eq
 'cks-1234567890abcdef0'
```

Per ottenere le chiavi KMS in qualsiasi AWS CloudHSM archivio di chiavi dell'account e della regione, filtra in base al valore di. CustomKeyStoreType `AWS_CLOUDHSM`

```
PS C:\> Get-KMSKeyList | Get-KMSKey | where CustomKeyStoreType -eq 'AWS_CLOUDHSM'
```

Ricerca di tutte le chiavi per un archivio delle chiavi di AWS CloudHSM

Nel cluster AWS CloudHSM puoi identificare le chiavi che fungono da materiale della chiave per il tuo archivio delle chiavi di AWS CloudHSM. Per farlo, usa il findAllKeyscomando in cloudhsm_mgmt_util per trovare gli handle delle chiavi di tutte le chiavi che possiede o condivide. `kmsuser` Se non hai eseguito l'accesso come `kmsuser` e creato chiavi al di fuori di AWS KMS, tutte le chiavi di cui `kmsuser` è proprietario rappresentano il materiale della chiave per le chiavi KMS .

Qualsiasi crypto officer nel cluster può eseguire questo comando senza disconnettere l'archivio delle chiavi di AWS CloudHSM.

1. Avvia cloudhsm_mgmt_util utilizzando la procedura descritta nell'argomento Getting started with CloudHSM Management Utility (CMU) (Nozioni di base su CloudHSM Management Utility [CMU]).
2. Accedere a cloudhsm_mgmt_util utilizzando un account di crypto officer (CO).
3. Utilizzare il comando listUsers per trovare l'ID utente del crypto user (CU) `kmsuser`.

   In questo esempio, l'ID utente di `kmsuser` è 3.

```
aws-cloudhsm> listUsers
Users on server 0(10.0.0.1):
Number of users found:3

    User Id             User Type       User Name            MofnPubKey
 LoginFailureCnt         2FA
         1              PCO             admin                    NO
 0               NO
         2              AU              app_user                 NO
 0               NO
         3              CU              kmsuser                  NO
 0               NO
```

4. Usa il findAllKeyscomando per trovare gli handle dei tasti di tutte le chiavi che possiedono o condividono. `kmsuser` Sostituisci l'ID utente di esempio (3) con l'ID utente effettivo di `kmsuser` nel cluster.

   L'output di esempio mostra che `kmsuser` possiede chiavi con gli handle di chiave 8, 9 e 262162 su entrambi gli HSM nel cluster.

```
aws-cloudhsm> findAllKeys 3 0
Keys on server 0(10.0.0.1):
Number of keys found 3
number of keys matched from start index 0::6
8,9,262162
findAllKeys success on server 0(10.0.0.1)

Keys on server 1(10.0.0.2):
Number of keys found 6
number of keys matched from start index 0::6
```

```
8,9,262162
findAllKeys success on server 1(10.0.0.2)
```

Ricerca della chiave KMS per una chiave di AWS CloudHSM

Se conosci l'handle della chiave di cui `kmsuser` è proprietario nel cluster, puoi utilizzare l'etichetta di chiave per identificare la chiave KMS associata nell'archivio delle chiavi di AWS CloudHSM.

Quando AWS KMS crea il materiale della chiave per una chiave KMS nel cluster AWS CloudHSM, scrive l'Amazon Resource Name (ARN) della chiave KMS nell'etichetta di chiave. Se non hai modificato il valore dell'etichetta, puoi utilizzare il comando getAttribute in key_mgmt_util o cloudhsm_mgmt_util per associare la chiave alla relativa chiave KMS.

Per eseguire questa procedura, devi disconnettere temporaneamente l'archivio delle chiavi di AWS CloudHSM, in modo da poter accedere come CU `kmsuser`.

> **Note**
>
> Quando un archivio delle chiavi personalizzate è disconnesso, tutti i tentativi di creare chiavi KMS nell'archivio delle chiavi personalizzate o di utilizzare le chiavi KMS in operazioni di crittografia avrà esito negativo. Questa azione può impedire agli utenti di archiviare e accedere ai dati sensibili.

1. Se non è già disconnesso, disconnetti l'archivio delle chiavi di AWS CloudHSM, quindi accedi a key_mgmt_util come `kmsuser`, come descritto in Come disconnettersi ed eseguire l'accesso.
2. Utilizzare il comando `getAttribute` in key_mgmt_util o cloudhsm_mgmt_util per ottenere l'attributo dell'etichetta (`OBJ_ATTR_LABEL`, attributo `3`) per un determinato handle di chiave.

   Ad esempio, questo comando utilizza `getAttribute` in cloudhsm_mgmt_util per ottenere l'attributo dell'etichetta (attributo `3`) della chiave con l'handle di chiave `262162`. L'output indica che la chiave `262162` funge da materiale della chiave per la chiave KMS con l'ARN `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`. Prima di eseguire questo comando, sostituire l'handle di chiave di esempio con uno valido.

Per un elenco di attributi delle chiavi, utilizza il comando listAttributes o consulta Documentazione di riferimento per l'attributo della chiave nella Guida per l'utente di AWS CloudHSM.

```
aws-cloudhsm> getAttribute 262162 3

Attribute Value on server 0(10.0.1.10):
OBJ_ATTR_LABEL
arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

3. Disconnettiti da key_mgmt_util o cloudhsm_mgmt_util e connettiti nuovamente all'archivio delle chiavi di AWS CloudHSM, come descritto in Come scollegarsi e riconnettersi.

Ricerca della chiave di AWS CloudHSM per una chiave KMS

Puoi utilizzare l'ID di una chiave KMS in un archivio delle chiavi di AWS CloudHSM per identificare nel cluster AWS CloudHSM la chiave che funge da materiale della chiave. Puoi quindi utilizzare il relativo handle di chiave per identificare la chiave nei comandi del client AWS CloudHSM.

Quando AWS KMS crea il materiale della chiave per una chiave KMS nel cluster AWS CloudHSM, scrive l'Amazon Resource Name (ARN) della chiave KMS nell'etichetta di chiave. Se non hai modificato il valore dell'etichetta, puoi utilizzare il comando findKey in key_mgmt_util per ottenere l'handle di chiave del materiale della chiave per la chiave KMS. Per eseguire questa procedura, devi disconnettere temporaneamente l'archivio delle chiavi di AWS CloudHSM, in modo da poter accedere come CU `kmsuser`.

> **Note**
>
> Quando un archivio delle chiavi personalizzate è disconnesso, tutti i tentativi di creare chiavi KMS nell'archivio delle chiavi personalizzate o di utilizzare le chiavi KMS in operazioni di crittografia avrà esito negativo. Questa azione può impedire agli utenti di archiviare e accedere ai dati sensibili.

1. Se non è già disconnesso, disconnetti l'archivio delle chiavi di AWS CloudHSM, quindi accedi a key_mgmt_util come `kmsuser`, come descritto in Come disconnettersi ed eseguire l'accesso.
2. Utilizza il comando findKey in key_mgmt_util per cercare una chiave con un'etichetta corrispondente all'ARN di una chiave KMS nell'archivio delle chiavi di AWS CloudHSM.

Sostituire l'ARN della chiave KMS di esempio nel valore del parametro `-l` (L minuscola per "label" (etichetta)) con un ARN della chiave KMS valido.

Ad esempio, questo comando trova la chiave con un'etichetta che corrisponde all'ARN della chiave KMS di esempio, ovvero `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`. L'output di esempio mostra che la chiave con l'handle di chiave 262162 include l'ARN della chiave KMS specificato nella relativa etichetta. A questo punto è possibile utilizzare questo handle di chiave in altri comandi key_mgmt_util.

```
Command: findKey -l arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
Total number of keys present 1

 number of keys matched from start index 0::1
262162

        Cluster Error Status
        Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
        Node id 0 and err state 0x00000000 : HSM Return: SUCCESS

        Cfm3FindKey returned: 0x00 : HSM Return: SUCCESS
```

3. Scollegarsi da key_mgmt_util e riconnettere lo store delle chiavi personalizzate come descritto in Come scollegarsi e riconnettersi.

Pianificazione dell'eliminazione di chiavi KMS da un archivio delle chiavi di AWS CloudHSM

Quando si ha la certezza che non si avrà più bisogno di utilizzare una determinata AWS KMS key per le operazioni di crittografia, è possibile pianificare l'eliminazione della chiave KMS. Per farlo, utilizza la stessa procedura che utilizzeresti per programmare l'eliminazione di qualsiasi chiave KMS da AWS KMS. Mantieni inoltre connesso l'archivio delle chiavi di AWS CloudHSM in modo che AWS KMS possa eliminare il materiale della chiave corrispondente dal cluster AWS CloudHSM associato alla scadenza del periodo di attesa.

Puoi monitorare la pianificazione, la cancellazione e l'eliminazione della chiave KMS nei log di AWS CloudTrail.

> **Warning**
>
> L'eliminazione di una chiave KMS è un'operazione distruttiva e potenzialmente pericolosa che impedisce il recupero di tutti i dati crittografati con la chiave KMS. Prima di pianificare l'eliminazione della chiave KMS, esamina l'utilizzo passato della chiave KMS e crea un CloudWatch allarme Amazon che ti avvisi quando qualcuno tenta di utilizzare la chiave KMS mentre è in attesa di eliminazione. Quando possibile, disabilita la chiave KMS anziché eliminarla.

Se pianifichi l'eliminazione di una chiave KMS da un archivio delle chiavi di AWS CloudHSM, il relativo stato chiave viene impostato su Pending deletion (Eliminazione in attesa). La chiave KMS rimane nello stato In attesa di eliminazione durante l'intero periodo di attesa, anche se la chiave KMS diventa indisponibile a seguito della disconnessione dell'archivio delle chiavi personalizzate. Ciò consente di annullare l'eliminazione della chiave KMS in qualsiasi momento durante il periodo di attesa.

Alla scadenza del periodo di attesa, AWS KMS elimina la chiave KMS da AWS KMS. AWS KMS tenta quindi di eliminare il materiale della chiave dal cluster AWS CloudHSM associato. Se AWS KMS non riesce a eliminare tale materiale, ad esempio quando lo store delle chiavi personalizzate è disconnesso da AWS KMS, è possibile che tu debba eliminare manualmente il materiale della chiave orfano dal cluster.

AWS KMS non elimina il materiale della chiave dai backup del cluster. Anche se elimini la chiave KMS da AWS KMS e il relativo materiale della chiave dal cluster AWS CloudHSM, i cluster creati a partire dai backup potrebbero contenere quel materiale eliminato. Per eliminare definitivamente il materiale della chiave visualizza la data di creazione della chiave KMS. Quindi elimina tutti i backup del cluster che potrebbero contenere quel materiale.

Quando pianifichi l'eliminazione di una chiave KMS da un archivio delle chiavi di AWS CloudHSM, la chiave KMS diventa immediatamente inutilizzabile (in base alla coerenza finale). Tuttavia, le risorse crittografate con chiavi dati protette dalla chiave KMS non sono interessate fino a quando la chiave KMS non viene nuovamente usata, ad esempio per decrittografare la chiave dati. Questo problema riguarda i Servizi AWS, molti dei quali proteggono le risorse tramite le chiavi dati. Per informazioni dettagliate, vedi In che modo le chiavi KMS inutilizzabili influiscono sulle chiavi dati.

Risoluzione di problemi relativi a store delle chiavi personalizzate

Gli archivi delle chiavi di AWS CloudHSM sono progettati per essere disponibili e resilienti. Sono tuttavia presenti alcune condizioni di errore che potresti dover correggere per garantire il corretto funzionamento dell'archivio delle chiavi di AWS CloudHSM.

Argomenti

Come correggere chiavi KMS non disponibili

Lo stato della chiave di AWS KMS keys in un archivio delle chiavi di AWS CloudHSM è in genere `Enabled`. Come con tutte le chiavi KMS, anche per le chiavi KMS in un archivio delle chiavi di AWS CloudHSM lo stato della chiave cambia se queste vengono disabilitate o se ne pianifica l'eliminazione. Tuttavia, a differenza delle altre chiavi KMS, le chiavi KMS in un archivio delle chiavi personalizzate possono anche avere lo stato di chiave `Unavailable`.

Lo stato di chiave `Unavailable` indica che la chiave KMS si trova in un archivio delle chiavi personalizzate che è stato intenzionalmente disconnesso e che gli eventuali tentativi di riconnetterlo non sono riusciti. Quando una chiave KMS non è disponibile, puoi visualizzare e gestire la chiave KMS, ma non utilizzarla per operazioni di crittografia.

Per trovare lo stato di chiave di una chiave KMS, nella pagina Chiavi gestite cliente, visualizza il campo Stato della chiave KMS. In alternativa, utilizzate l'DescribeKeyoperazione e visualizzate l'`KeyState`elemento nella risposta. Per informazioni dettagliate, vedi Visualizzazione di chiavi.

Le chiavi KMS in uno store delle chiavi personalizzate disconnesso avranno lo stato di chiave `Unavailable` o `PendingDeletion`. Le chiavi KMS per le quali è stata pianificata l'eliminazione da un archivio delle chiavi personalizzate hanno lo stato della chiave `Pending Deletion`, anche

quando tale archivio è disconnesso. Ciò ti consente di annullare l'eliminazione pianificata delle chiavi senza riconnettere lo store delle chiavi personalizzate.

Per correggere una chiave KMS non disponibile, riconnetti l'archivio delle chiavi personalizzate. Dopo la riconnessione, per le chiavi KMS nello store delle chiavi personalizzate viene ripristinato lo stato di chiave precedente, ovvero `Enabled` o `Disabled`. Lo stato delle chiavi KMS in attesa di eliminazione rimane `PendingDeletion`. Tuttavia, se il problema persiste, l'abilitazione e la disabilitazione di una chiave KMS non disponibile non ne modifica lo stato. L'abilitazione o la disabilitazione ha effetto solo quando la chiave diventa disponibile.

Per informazioni sulle connessioni non riuscite, consulta Come correggere un errore di connessione.

Come correggere una chiave KMS non funzionante

I problemi relativi alla creazione e all'utilizzo di chiavi KMS negli archivi delle chiavi di AWS CloudHSM possono essere causati da un errore nell'archivio delle chiavi di AWS CloudHSM, nel cluster AWS CloudHSM associato, nella chiave KMS o nel materiale della chiave.

Quando un archivio delle chiavi di AWS CloudHSM viene disconnesso dal relativo cluster AWS CloudHSM, lo stato delle chiavi KMS nell'archivio delle chiavi personalizzate è `Unavailable`. Tutte le richieste per creare chiavi KMS in un archivio delle chiavi di AWS CloudHSM disconnesso restituiscono l'eccezione `CustomKeyStoreInvalidStateException`. Tutte le richieste di crittografare, decrittografare, ricrittografare o generare chiavi di dati restituiscono un'eccezione `KMSInvalidStateException`. Per risolvere il problema, riconnetti l'archivio delle chiavi di AWS CloudHSM.

I tentativi di utilizzare una chiave KMS in un archivio delle chiavi di AWS CloudHSM per operazioni di crittografia potrebbero tuttavia non riuscire anche quando lo stato è `Enabled` e lo stato di connessione dell'archivio delle chiavi di AWS CloudHSM è `Connected`. Ciò può essere dovuto a una qualsiasi delle condizioni seguenti.

- Il materiale della chiave per la chiave KMS potrebbe essere stato eliminato dal cluster AWS CloudHSM associato. A questo proposito, trova l'handle di chiave del materiale chiave di una chiave KMS e, se necessario, prova a recuperare tale materiale.
- Tutti gli HSM sono stati eliminati dal cluster AWS CloudHSM associato all'archivio delle chiavi di AWS CloudHSM. Per utilizzare una chiave KMS di un archivio delle chiavi di AWS CloudHSM in un'operazione di crittografia, il relativo cluster AWS CloudHSM deve contenere almeno un HSM attivo. Per verificare il numero e lo stato degli HSM in un AWS CloudHSM cluster, usa la AWS

CloudHSM console o l'DescribeClustersoperazione. Per aggiungere un HSM al cluster, usa la AWS CloudHSM console o l'CreateHsmoperazione.

- Il cluster AWS CloudHSM associato all'archivio delle chiavi di AWS CloudHSM è stato eliminato. Per risolvere il problema, crea un cluster da un backup che è correlato al cluster originale, ad esempio un backup del cluster originale o un backup utilizzato per creare il cluster originale. Quindi, modifica l'ID cluster nelle impostazioni relative allo store delle chiavi personalizzate. Per istruzioni, consulta Come recuperare il materiale chiave eliminato per una chiave KMS.
- Il cluster AWS CloudHSM associato all'archivio delle chiavi personalizzate non disponeva di sessioni PKCS #11. Ciò si verifica in genere durante i periodi di traffico di espansione elevato, ovvero quando sono necessarie sessioni aggiuntive per gestire il traffico. Per rispondere a un'eccezione `KMSInternalException` con un messaggio di errore relativo alle sessioni PKCS #11, torna indietro e riprova a eseguire la richiesta.

Come correggere un errore di connessione

Se tenti di connettere un archivio delle chiavi di AWS CloudHSM al relativo cluster AWS CloudHSM, ma l'operazione ha esito negativo, lo stato di connessione dell'archivio delle chiavi di AWS CloudHSM diventa `FAILED`. Per trovare lo stato di connessione di un AWS CloudHSM key store, usa la AWS KMS console o l'DescribeCustomKeyStoresoperazione.

In alternativa, alcuni tentativi di connessione si interrompono rapidamente a causa di errori di configurazione del cluster facilmente rilevati. In questo caso, lo stato della connessione è ancora `DISCONNECTED`. Questi errori restituiranno un messaggio di errore o un'eccezione che spiega perché il tentativo non è riuscito. Esamina la descrizione dell'eccezione e i requisiti del cluster, risolvi il problema, aggiorna l'archivio delle chiavi di AWS CloudHSM, se necessario, e riprova a connetterti.

Quando lo stato della connessione è `FAILED` impostato, esegui l'DescribeCustomKeyStoresoperazione e visualizza l'`ConnectionErrorCode`elemento nella risposta.

> **Note**
>
> Quando lo stato di connessione di un archivio delle chiavi di AWS CloudHSM è `FAILED`, devi disconnettere l'archivio delle chiavi di AWS CloudHSM prima di tentare di riconnetterlo. Non puoi connettere un archivio delle chiavi di AWS CloudHSM il cui stato di connessione è `FAILED`.

- `CLUSTER_NOT_FOUND` indica che AWS KMS non trova un cluster AWS CloudHSM con l'ID cluster specificato. Il problema potrebbe essere dovuto a un ID cluster errato fornito a un'operazione API oppure all'eliminazione e alla mancata sostituzione del cluster. Per correggere questo errore, verifica l'ID del cluster, ad esempio utilizzando la AWS CloudHSM console o l'DescribeClustersoperazione. Se il cluster è stato eliminato, crea un cluster a partire da un backup recente dell'originale. Successivamente, disconnetti l'archivio delle chiavi di AWS CloudHSM, modifica l'impostazione dell'ID cluster dell'archivio delle chiavi di AWS CloudHSM e riconnetti l'archivio AWS CloudHSM al cluster.
- `INSUFFICIENT_CLOUDHSM_HSMS` indica che il cluster AWS CloudHSM associato non contiene alcun HSM. Per eseguire la connessione, il cluster deve avere almeno un HSM. Per trovare il numero di moduli di protezione hardware nel cluster, utilizzate l'DescribeClustersoperazione. Per correggere questo errore, aggiungi almeno un HSM al cluster. Se aggiungi più HSM, è meglio crearli in zone di disponibilità differenti.
- `INSUFFICIENT_FREE_ADDRESSES_IN_SUBNET` indica che AWS KMS non può connettere l'archivio delle chiavi di AWS CloudHSM al relativo cluster AWS CloudHSM perché almeno una sottorete privata associata al cluster non dispone di indirizzi IP disponibili. Una connessione all'archivio delle chiavi di AWS CloudHSM richiede almeno un indirizzo IP libero in ciascuna delle sottoreti private associate, preferibilmente due.

  Non puoi aggiungere indirizzi IP (blocchi CIDR) a una sottorete esistente. Se possibile, sposta o elimina altre risorse che utilizzano gli indirizzi IP nella sottorete, ad esempio istanze EC2 inutilizzate o interfacce di rete elastiche. In caso contrario, puoi creare un cluster da un backup recente del cluster AWS CloudHSM con sottoreti private nuove o esistenti che hanno più spazio di indirizzi libero. Quindi, per associare il nuovo cluster all'archivio delle chiavi di AWS CloudHSM, disconnetti l'archivio delle chiavi personalizzate, modifica l'ID cluster dell'archivio delle chiavi di AWS CloudHSM con l'ID del nuovo cluster e prova a connetterti nuovamente.

  > **Tip**
  >
  > Per evitare di reimpostare la password `kmsuser`, utilizzare il backup più recente del cluster AWS CloudHSM.

- `INTERNAL_ERROR` indica che AWS KMS non è stato in grado di completare la richiesta a causa di un errore interno. Riprova la richiesta . Per le richieste `ConnectCustomKeyStore`, scollega l'archivio delle chiavi di AWS CloudHSM prima di provare a connetterti di nuovo.

- `INVALID_CREDENTIALS` indica che AWS KMS non può accedere al cluster AWS CloudHSM associato in quanto non dispone della password corretta per l'account `kmsuser`. Per informazioni su questo errore, consulta Come correggere credenziali `kmsuser` non valide.
- `NETWORK_ERRORS` indica in genere problemi di rete temporanei. Disconnetti l'archivio delle chiavi di AWS CloudHSM, attendi alcuni minuti ed effettua un nuovo tentativo di connessione.
- `SUBNET_NOT_FOUND` indica che almeno una sottorete nella configurazione del cluster AWS CloudHSM è stata eliminata. Se AWS KMS non riesce a trovare tutte le sottoreti nella configurazione del cluster, i tentativi di connettere l'archivio delle chiavi di AWS CloudHSM al cluster AWS CloudHSM hanno esito negativo.

  Per correggere questo errore, creare un cluster da un backup recente dello stesso cluster AWS CloudHSM. Questo processo crea una nuova configurazione del cluster con un VPC e sottoreti private. Verificare che il nuovo cluster soddisfi i requisiti per uno store delle chiavi personalizzate e prendere nota del nuovo ID cluster. Quindi, per associare il nuovo cluster all'archivio delle chiavi di AWS CloudHSM, disconnetti l'archivio delle chiavi personalizzate, modifica l'ID cluster dell'archivio delle chiavi di AWS CloudHSM con l'ID del nuovo cluster e prova a connetterti nuovamente.

  > **Tip**
  >
  > Per evitare di reimpostare la password `kmsuser`, utilizzare il backup più recente del cluster AWS CloudHSM.

- `USER_LOCKED_OUT` indica che l'account crypto user (CU) `kmsuser` è bloccato per il cluster AWS CloudHSM a causa di troppi tentativi con password errate. Per informazioni su questo errore, consulta Come correggere credenziali `kmsuser` non valide.

  Per correggere questo errore, disconnetti l'archivio delle chiavi di AWS CloudHSM e utilizza il comando changePswd in cloudhsm_mgmt_util per modificare la password dell'account `kmsuser`. Quindi, modifica l'impostazione della password `kmsuser` per lo store delle chiavi personalizzate ed esegui un nuovo tentativo di connessione. Per assistenza, utilizza la procedura descritta nell'argomento Come correggere credenziali `kmsuser` non valide.

- `USER_LOGGED_IN` indica che l'account utente di crittografia `kmsuser` è registrato nel cluster AWS CloudHSM associato. Ciò impedisce a AWS KMS di ruotare la password dell'account `kmsuser` e di accedere al cluster. Per correggere questo errore, registra l'utente di crittografia `kmsuser` fuori dal cluster. Se hai modificato la password `kmsuser` per accedere al cluster, devi aggiornare anche il valore della password dell'archivio delle chiavi per l'archivio delle chiavi di AWS CloudHSM. Per assistenza, consulta Come scollegarsi e riconnettersi.

- `USER_NOT_FOUND` indica che AWS KMS non è in grado di trovare un account utente di crittografia `kmsuser` nel cluster AWS CloudHSM associato. Per correggere questo errore, crea un account CU `kmsuser` nel cluster, quindi aggiorna il valore della password dell'archivio delle chiavi per l'archivio delle chiavi di AWS CloudHSM. Per assistenza, consulta Come correggere credenziali `kmsuser` non valide.

Come rispondere a un errore di un'operazione di crittografia

L'esito di un'operazione di crittografia che utilizza una chiave KMS in un archivio di chiavi personalizzate potrebbe essere negativo con un'`KMSInvalidStateException`. L'eccezione `KMSInvalidStateException` può essere accompagnata dai seguenti messaggi di errore.

KMS non può comunicare con il tuo cluster CloudHSM. Potrebbe trattarsi di un problema di rete temporaneo. Se visualizzi ripetutamente questo errore, controlla se gli ACL di rete e le regole del gruppo di sicurezza per il VPC del tuo cluster AWS CloudHSM sono corretti.

- Sebbene si tratti di un errore HTTPS 400, potrebbe derivare da problemi di rete transitori. Per rispondere, prova a riformulare la richiesta. Tuttavia, se il problema persiste, esamina la configurazione dei componenti di rete. Questo errore è probabilmente causato dall'errata configurazione di un componente di rete, ad esempio una regola firewall o una regola di gruppo di protezione VPC che blocca il traffico in uscita.

KMS non può comunicare con il tuo cluster AWS CloudHSM perché kmsuser è bloccato. Se visualizzi questo errore ripetutamente, scollega l'archivio di chiavi AWS CloudHSM e reimposta la password dell'account kmsuser. Aggiorna la password kmsuser per l'archivio di chiavi personali zzate e ritenta la richiesta.

- Questo messaggio di errore indica che l'account crypto user (CU) `kmsuser` è bloccato per il cluster AWS CloudHSM associato a causa del numero eccessivo di tentativi con password errate. Per informazioni su questo errore, consulta Come disconnettersi ed eseguire l'accesso.

Come correggere credenziali **kmsuser** non valide

Quando connetti un archivio delle chiavi di AWS CloudHSM, AWS KMS accede al cluster AWS CloudHSM associato come crypto user (CU) `kmsuser`. Rimane collegato fino a che l'archivio delle chiavi di AWS CloudHSM non viene disconnesso. La risposta DescribeCustomKeyStores mostra un `ConnectionState` di `FAILED` e il valore `ConnectionErrorCode` di `INVALID_CREDENTIALS`, come mostrato nell'esempio seguente.

Se disconnetti l'archivio delle chiavi di AWS CloudHSM e modifichi la password `kmsuser`, AWS KMS non può accedere al cluster AWS CloudHSM con le credenziali dell'account CU `kmsuser`. Di conseguenza, tutti i tentativi di connessione all'archivio delle chiavi di AWS CloudHSM hanno esito negativo. La risposta `DescribeCustomKeyStores` mostra un `ConnectionState` di `FAILED` e il valore `ConnectionErrorCode` di `INVALID_CREDENTIALS`, come mostrato nell'esempio seguente.

```
$ aws kms describe-custom-key-stores --custom-key-store-name ExampleKeyStore
{
   "CustomKeyStores": [
      "CloudHsmClusterId": "cluster-1a23b4cdefg",
      "ConnectionErrorCode": "INVALID_CREDENTIALS"
      "CustomKeyStoreId": "cks-1234567890abcdef0",
      "CustomKeyStoreName": "ExampleKeyStore",
      "TrustAnchorCertificate": "<certificate string appears here>",
      "CreationDate": "1.499288695918E9",
      "ConnectionState": "FAILED"
   ],
}
```

Inoltre, dopo cinque tentativi di accesso al cluster non riusciti a causa di una password errata, AWS CloudHSM blocca l'account utente. Per accedere al cluster, devi modificare la password dell'account.

Se AWS KMS riceve una risposta di blocco quando tenta di accedere al cluster come utente CU `kmsuser`, la richiesta di connessione all'archivio delle chiavi di AWS CloudHSM ha esito negativo. La DescribeCustomKeyStoresrisposta include un `ConnectionState` of `FAILED` e un `ConnectionErrorCode` valore di`USER_LOCKED_OUT`, come illustrato nell'esempio seguente.

```
$ aws kms describe-custom-key-stores --custom-key-store-name ExampleKeyStore
{
   "CustomKeyStores": [
      "CloudHsmClusterId": "cluster-1a23b4cdefg",
      "ConnectionErrorCode": "USER_LOCKED_OUT"
```

```
      "CustomKeyStoreId": "cks-1234567890abcdef0",
      "CustomKeyStoreName": "ExampleKeyStore",
      "TrustAnchorCertificate": "<certificate string appears here>",
      "CreationDate": "1.499288695918E9",
      "ConnectionState": "FAILED"
   ],
}
```

Per correggere queste condizioni, utilizza la procedura seguente.

1. Disconnetti l'archivio delle chiavi di AWS CloudHSM.
2. Eseguite l'DescribeCustomKeyStoresoperazione e visualizzate il valore dell'`ConnectionErrorCode`elemento nella risposta.
   - Se `ConnectionErrorCode` è `INVALID_CREDENTIALS`, determinare la password corrente per l'account `kmsuser`. Se necessario, utilizzare il comando changePswd in cloudhsm_mgmt_util per impostare una nuova password.
   - Se `ConnectionErrorCode` è `USER_LOCKED_OUT`, è necessario utilizzare il comando changePswd in cloudhsm_mgmt_util per modificare la password `kmsuser`.
3. Modificare l'impostazione della password `kmsuser` di modo che corrisponda alla password `kmsuser` corrente nel cluster. Questa operazione indica a AWS KMS quale password utilizzare per accedere al cluster. Non modifica la password `kmsuser` nel cluster.
4. Connettere lo store delle chiavi personalizzate.

Come eliminare materiale della chiave orfano

Dopo la pianificazione dell'eliminazione di una chiave KMS da un archivio delle chiavi di AWS CloudHSM, è possibile che sia necessario eliminare manualmente il materiale della chiave corrispondente dal cluster AWS CloudHSM associato.

Quando crei una chiave KMS in un archivio delle chiavi di AWS CloudHSM, AWS KMS genera i metadati della chiave KMS in AWS KMS e il materiale della chiave nel cluster AWS CloudHSM associato. Quando pianifichi l'eliminazione di una chiave KMS in un archivio delle chiavi di AWS CloudHSM, al termine del periodo di attesa, AWS KMS elimina i metadati della chiave KMS. AWS KMS prova quindi a eliminare il materiale chiave corrispondente dal cluster AWS CloudHSM. Il tentativo potrebbe avere esito negativo se AWS KMS non riesce ad accedere al cluster, ad esempio quando è disconnesso dall'archivio delle chiavi di AWS CloudHSM o se la password `kmsuser` cambia. AWS KMS non prova a eliminare il materiale chiave dai backup del cluster.

AWS KMS riporta i risultati del tentativo di eliminazione del materiale chiave dal cluster nella voce dell'evento `DeleteKey`dei registri di AWS CloudTrail. Appare nell'elemento `backingKeysDeletionStatus` dell'elemento `additionalEventData`, come mostrato nella seguente voce di esempio. Questa voce include l'ARN della chiave KMS, l'ID cluster AWS CloudHSM e l'handle di chiave del materiale chiave (`backing-key-id`).

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "111122223333",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2021-12-10T14:23:51Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DeleteKey",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "customKeyStoreId": "cks-1234567890abcdef0",
        "clusterId": "cluster-1a23b4cdefg",
        "backingKeys": "[{\"keyHandle\":\"01\",\"backingKeyId\":\"backing-key-id\"}]",
        "backingKeysDeletionStatus": "[{\"keyHandle\":\"16\",\"backingKeyId\":
\"backing-key-id\",\"deletionStatus\":\"FAILURE\"}]"
    },
    "eventID": "c21f1f47-f52b-4ffe-bff0-6d994403cf40",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "111122223333",
    "managementEvent": true,
    "eventCategory": "Management"
}
```

Per eliminare il materiale della chiave dal cluster AWS CloudHSM associato, utilizza una procedura simile alla seguente. In questo esempio vengono utilizzati la AWS CLI e gli strumenti a riga di comando AWS CloudHSM, ma è possibile utilizzare la AWS Management Console anziché la CLI.

1. Se non è già disconnesso, disconnetti l'archivio delle chiavi di AWS CloudHSM, quindi accedi a key_mgmt_util come descritto in Come disconnettersi ed eseguire l'accesso.
2. Utilizzare il comando deleteKey in key_mgmt_util per eliminare la chiave dagli HSM nel cluster.

   Ad esempio, questo comando elimina la chiave 262162 dagli HSM nel cluster. L'handle della chiave è elencato nella voce di CloudTrail registro.

   ```
   Command: deleteKey -k 262162

           Cfm3DeleteKey returned: 0x00 : HSM Return: SUCCESS

           Cluster Error Status
           Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
           Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
           Node id 2 and err state 0x00000000 : HSM Return: SUCCESS
   ```
3. Disconnettiti da key_mgmt_util e connettiti nuovamente all'archivio delle chiavi di AWS CloudHSM, come descritto in Come scollegarsi e riconnettersi.

Come recuperare il materiale chiave eliminato per una chiave KMS

Se il materiale chiave di una AWS KMS key viene eliminato, la chiave KMS è inutilizzabile e tutto il testo cifrato che è stato crittografato sotto la chiave KMS non può essere decrittato. Ciò può verificarsi se il materiale della chiave per una chiave KMS in un archivio delle chiavi di AWS CloudHSM viene eliminato dal cluster AWS CloudHSM associato. Potrebbe tuttavia essere possibile recuperare questo materiale.

Quando crei una AWS KMS key (chiave KMS) in un archivio delle chiavi di AWS CloudHSM, AWS KMS accede al cluster AWS CloudHSM associato e crea il materiale della chiave per la chiave KMS. Imposta inoltre una nuova password che è il solo a conoscere e rimane collegato fino a che l'archivio delle chiavi di AWS CloudHSM non viene disconnesso. Poiché solo il proprietario della chiave, ovvero l'utente di crittografia che l'ha creata, può eliminarla, è improbabile che venga eliminata accidentalmente dagli HSM.

Tuttavia, se il materiale chiave per una chiave KMS viene eliminato dagli HSM in un cluster, lo stato della chiave KMS eventualmente diventa `UNAVAILABLE`. Se tenti di utilizzare la

chiave KMS per un'operazione di crittografia, questa ha esito negativo con un'eccezione `KMSInvalidStateException`. Cosa più importante, tutti i dati crittografati con la chiave KMS non possono essere decrittati.

In alcuni casi, è possibile recuperare il materiale della chiave creando un cluster a partire da un backup contenente tale materiale. Questa strategia funziona solo se almeno un backup è stato creato quando la chiave esisteva e prima di essere eliminata.

Utilizza la procedura seguente per recuperare il materiale della chiave.

1. Trovare un backup del cluster che contiene il materiale della chiave. Il backup deve contenere almeno tutti gli utenti e le chiavi necessari per supportare il cluster e i relativi dati crittografati.

   Utilizzate l'DescribeBackupsoperazione per elencare i backup per un cluster. Utilizzare quindi il timestamp del backup per la selezione di un backup. Per limitare l'output al cluster associato all'archivio delle chiavi di AWS CloudHSM, utilizza il parametro `Filters`, come mostrato nell'esempio seguente.

   ```
   $ aws cloudhsmv2 describe-backups --filters clusterIds=<cluster ID>
   {
       "Backups": [
           {
               "ClusterId": "cluster-1a23b4cdefg",
               "BackupId": "backup-9g87f6edcba",
               "CreateTimestamp": 1536667238.328,
               "BackupState": "READY"
           },
                ...
       ]
   }
   ```

2. Creare un cluster a partire dal backup selezionato. Verificare che il backup contenga la chiave eliminata e altri utenti e chiavi che il cluster richiede.
3. Disconnetti l'archivio delle chiavi di AWS CloudHSM affinché sia possibile modificarne le proprietà.
4. Modifica l'ID cluster dell'archivio delle chiavi di AWS CloudHSM. Immettere l'ID cluster del cluster creato a partire dal backup. Poiché il cluster condivide una cronologia dei backup con il cluster originale, il nuovo ID cluster deve essere valido.
5. Connetti nuovamente l'archivio delle chiavi di AWS CloudHSM.

Come accedere come **kmsuser**

Per creare e gestire il materiale della chiave nel cluster AWS CloudHSM per l'archivio delle chiavi di AWS CloudHSM, AWS KMS utilizza l'account crypto user (CU) `kmsuser`. Crea l'account CU `kmsuser` nel cluster e fornisci la relativa password a AWS KMS durante la creazione dell'archivio delle chiavi di AWS CloudHSM.

In genere, l'account `kmsuser` è gestito da AWS KMS. Tuttavia, per alcune attività, devi disconnettere l'archivio delle chiavi di AWS CloudHSM, accedere al cluster come utente CU `kmsuser` e utilizzare gli strumenti a riga di comando cloudhsm_mgmt_util e key_mgmt_util.

> **Note**
>
> Quando un archivio delle chiavi personalizzate è disconnesso, tutti i tentativi di creare chiavi KMS nell'archivio delle chiavi personalizzate o di utilizzare le chiavi KMS in operazioni di crittografia avrà esito negativo. Questa azione può impedire agli utenti di archiviare e accedere ai dati sensibili.

Questo argomento descrive come disconnettere l'archivio delle chiavi di AWS CloudHSM e accedere come `kmsuser`, eseguire lo strumento a riga di comando AWS CloudHSM e quindi scollegarsi e riconnettere l'archivio delle chiavi di AWS CloudHSM.

Argomenti

- Come disconnettersi ed eseguire l'accesso
- Come scollegarsi e riconnettersi

Come disconnettersi ed eseguire l'accesso

Utilizza la procedura seguente ogni volta che devi accedere a un cluster associato come utente di crittografia `kmsuser`.

1. Se non è già disconnesso, disconnetti l'archivio delle chiavi di AWS CloudHSM. Puoi usare la console AWS KMS o l'API AWS KMS.

   Quando l'archivio delle chiavi di AWS CloudHSM è disconnesso, AWS KMS è collegato come `kmsuser`. Ciò impedisce l'accesso come `kmsuser` o la modifica della password `kmsuser`.

Ad esempio, questo comando utilizza DisconnectCustomKeyStoreper disconnettere un archivio di chiavi di esempio. Sostituisci l'ID dell'archivio delle chiavi di AWS CloudHSM di esempio con uno valido.

```
$ aws kms disconnect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

2. Avviare cloudhsm_mgmt_util. Utilizzare la procedura descritta nella sezione Preparazione per l'esecuzione di cloudhsm_mgmt_util della Guida per l'utente di AWS CloudHSM.
3. Accedere a cloudhsm_mgmt_util sul cluster AWS CloudHSM come crypto officer (CO).

   Ad esempio, questo comando esegue l'accesso come responsabile della crittografia denominato admin. Sostituire la password e il nome dell'utente responsabile delle crittografia di esempio con valori validi.

```
aws-cloudhsm>loginHSM CO admin <password>
loginHSM success on server 0(10.0.2.9)
loginHSM success on server 1(10.0.3.11)
loginHSM success on server 2(10.0.1.12)
```

4. Utilizza il comando changePswd per modificare la password dell'account `kmsuser` con una nota (AWS KMS esegue la rotazione della password alla connessione dell'archivio delle chiavi di AWS CloudHSM). La password deve contenere da 7 a 32 caratteri alfanumerici, rispettare la distinzione tra maiuscole e minuscole e non includere caratteri speciali.

   Ad esempio, questo comando modifica la password da `kmsuser` a `tempPassword`.

```
aws-cloudhsm>changePswd CU kmsuser tempPassword

************************CAUTION*******************************
This is a CRITICAL operation, should be done on all nodes in the
cluster. Cav server does NOT synchronize these changes with the
nodes on which this operation is not executed or failed, please
ensure this operation is executed on all nodes in the cluster.
**************************************************************

Do you want to continue(y/n)?y
Changing password for kmsuser(CU) on 3 nodes
```

5. Accedere a key_mgmt_util o cloudhsm_mgmt_util come `kmsuser` utilizzando la password impostata. Per istruzioni dettagliate, consulta la pagina relativa alle nozioni di base su

cloudhsm_mgmt_util e quella relativa alle nozioni di base su key_mgmt_util. Lo strumento utilizzato dipende dall'attività.

Ad esempio, questo comando esegue l'accesso a key_mgmt_util.

```
Command: loginHSM -u CU -s kmsuser -p tempPassword
Cfm3LoginHSM returned: 0x00 : HSM Return: SUCCESS

Cluster Error Status
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
Node id 2 and err state 0x00000000 : HSM Return: SUCCESS
```

Come scollegarsi e riconnettersi

1. Eseguire l'attività, quindi scollegarsi dallo strumento a riga di comando. Se non effettui la disconnessione, i tentativi di riconnessione dell'archivio delle chiavi di AWS CloudHSM avranno esito negativo.

```
Command:  logoutHSM
Cfm3LogoutHSM returned: 0x00 : HSM Return: SUCCESS

Cluster Error Status
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
```

2. Modificare la password `kmsuser` per lo store delle chiavi personalizzate.

   In questo modo si indica a AWS KMS la password corrente per `kmsuser` nel cluster. Se si omette questo passaggio, AWS KMS non potrà accedere al cluster `kmsuser` e tutti i tentativi di riconnettere lo store delle chiavi personalizzate non riusciranno. È possibile utilizzare la AWS KMS console o il `KeyStorePassword` parametro dell'UpdateCustomKeyStoreoperazione.

   Ad esempio, questo comando indica a AWS KMS che la password corrente è `tempPassword`. Sostituire la password di esempio con una effettiva.

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 --
key-store-password tempPassword
```

3. Riconnetti l'archivio delle chiavi di AWS KMS al relativo cluster AWS CloudHSM. Sostituisci l'ID dell'archivio delle chiavi di AWS CloudHSM di esempio con uno valido. Durante il processo di connessione, AWS KMS imposta una nuova password `kmsuser` che è il solo a conoscere.

   L'ConnectCustomKeyStoreoperazione viene ripristinata rapidamente, ma il processo di connessione può richiedere un periodo di tempo prolungato. La risposta iniziale non indica se il processo di connessione è riuscito.

   ```
   $ aws kms connect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
   ```

4. Utilizzare l'DescribeCustomKeyStoresoperazione per verificare che l'archivio delle AWS CloudHSM chiavi sia connesso. Sostituisci l'ID dell'archivio delle chiavi di AWS CloudHSM di esempio con uno valido.

   In questo esempio, il campo dello stato della connessione mostra che l'archivio delle chiavi di AWS CloudHSM è ora connesso.

   ```
   $ aws kms describe-custom-key-stores --custom-key-store-
   id cks-1234567890abcdef0
   {
      "CustomKeyStores": [
         "CustomKeyStoreId": "cks-1234567890abcdef0",
         "CustomKeyStoreName": "ExampleKeyStore",
         "CloudHsmClusterId": "cluster-1a23b4cdefg",
         "TrustAnchorCertificate": "<certificate string appears here>",
         "CreationDate": "1.499288695918E9",
         "ConnectionState": "CONNECTED"
      ],
   }
   ```

Archivi delle chiavi esterne

Gli archivi delle chiavi esterne consentono di proteggere le risorseAWS utilizzando chiavi crittografiche al di fuori di AWS. Questa funzionalità avanzata è progettata per carichi di lavoro regolamentati che è necessario proteggere con chiavi crittografiche archiviate in un sistema di gestione delle chiavi esterno da te controllato. Gli archivi delle chiavi esterne supportano l'impegno per la sovranità digitale di AWS per conferirti il pieno controllo dei dati in AWS, inclusa la possibilità di crittografarli con un materiale della chiave al di fuori di AWS di tua proprietà e gestione.

Un archivio delle chiavi esterne è un archivio delle chiavi personalizzate supportato da un gestore delle chiavi esterne che possiedi e gestisci al di fuori di AWS. Il gestore delle chiavi esterne può essere un modulo di sicurezza hardware (HSM) fisico o virtuale o qualsiasi sistema basato su hardware o software in grado di generare e utilizzare chiavi crittografiche. Le operazioni di crittografia e decrittografia che utilizzano una chiave KMS in un archivio delle chiavi esterne vengono eseguite dal gestore delle chiavi esterne utilizzando il materiale della chiave crittografica, una funzionalità nota come HYOK (Hold Your Own Keys).

AWS KMS non interagisce mai direttamente con il gestore delle chiavi esterne e non può creare, visualizzare, gestire o eliminare le chiavi. AWS KMS interagisce soltanto con il software del proxy dell'archivio delle chiavi esterne (proxy XKS) fornito dall'utente. Il proxy dell'archivio delle chiavi esterne media tutte le comunicazioni tra AWS KMS e il tuo gestore delle chiavi esterne. Trasmette tutte le richieste da AWS KMS al gestore delle chiavi esterne e inoltra le risposte in senso inverso, fino ad arrivare a AWS KMS. Il proxy dell'archivio delle chiavi esterne traduce inoltre le richieste generiche provenienti da AWS KMS in un formato specifico del fornitore che il gestore delle chiavi esterne è in grado di comprendere, consentendoti di utilizzare gli archivi delle chiavi esterne con gestori di diversi fornitori.

Puoi utilizzare le chiavi KMS in un archivio delle chiavi esterne per la crittografia lato client, tra cui AWS Encryption SDK. Tuttavia, gli archivi delle chiavi esterni sono una risorsa importante per la crittografia lato server, poiché consentono di proteggere le risorse AWS in più Servizi AWS con le chiavi crittografiche esterne ad AWS. Servizi AWSche supportano le chiavi gestite dal cliente per la crittografia simmetrica supportano anche le chiavi KMS in un archivio delle chiavi esterno. Per i dettagli sul supporto del servizio, consulta la sezione Integrazione del servizio AWS.

Gli archivi delle chiavi esterne ti consentono di utilizzare AWS KMS per carichi di lavoro regolamentati in cui le chiavi crittografiche devono essere archiviate e utilizzate al di fuori di AWS. Tuttavia, si discostano notevolmente dal modello standard di responsabilità condivisa e richiedono oneri operativi aggiuntivi. Il rischio maggiore in termini di disponibilità e latenza supererà, per la maggior parte dei clienti, i vantaggi di sicurezza percepiti per gli archivi delle chiavi esterne.

Gli archivi delle chiavi esterne ti consentono di controllare la radice di attendibilità. I dati crittografati con le chiavi KMS dell'archivio delle chiavi esterne possono essere decrittografati solo utilizzando il gestore delle chiavi esterne che è sotto tuo controllo. Se revochi temporaneamente l'accesso al gestore delle chiavi esterne, ad esempio disconnettendo l'archivio delle chiavi esterne o il relativo gestore dal proxy, AWS perde l'accesso alle chiavi crittografiche fino al ripristino. Durante tale intervallo di tempo, il testo criptato con le chiavi KMS non può essere decifrato. Se revochi definitivamente l'accesso al gestore delle chiavi esterne, tutto il testo criptato con una chiave KMS

nell'archivio delle chiavi esterne diventa irrecuperabile. Le uniche eccezioni sono i servizi AWS che memorizzano brevemente nella cache le chiavi dati protette dalle chiavi KMS. Queste chiavi dati continuano a funzionare fino alla disattivazione della risorsa o alla scadenza della cache. Per informazioni dettagliate, vedi In che modo le chiavi KMS inutilizzabili influiscono sulle chiavi dati.

Gli archivi delle chiavi esterne sbloccano i pochi casi d'uso dei carichi di lavoro regolamentati in cui le chiavi crittografiche devono rimanere esclusivamente sotto il tuo controllo e inaccessibili ad AWS. Ciò rappresenta un cambiamento importante nel modo in cui gestisci l'infrastruttura basata sul cloud e una modifica sostanziale nel modello di responsabilità condivisa. Per la maggior parte dei carichi di lavoro, gli oneri operativi aggiuntivi e i maggiori rischi associati alla disponibilità e alle prestazioni superano i vantaggi di sicurezza percepiti per gli archivi delle chiavi esterne.

Ulteriori informazioni:

- Annuncio degli archivi delle chiavi esterne di AWS KMS nel Blog AWS News.

È necessario un archivio delle chiavi esterne?

Per la maggior parte degli utenti, l'archivio di chiavi AWS KMS predefinito, protetto da moduli di crittografia hardware con convalida del livello di sicurezza 3 FIPS 140-2, soddisfa i requisiti correlati a normative, controllo e sicurezza. Gli utenti dell'archivio delle chiavi esterne devono sostenere costi elevati, oneri di manutenzione e risoluzione dei problemi, nonché rischi per latenza, disponibilità e affidabilità.

Quando prendi in considerazione un archivio delle chiavi esterne, assicurati di comprendere bene le alternative. Queste includono, ad esempio, un archivio delle chiavi di AWS CloudHSM supportato da un cluster AWS CloudHSM che possiedi e gestisci e chiavi KMS con materiale della chiave importato che puoi generare nei moduli di sicurezza hardware ed eliminare dalle chiavi KMS su richiesta. In particolare, l'importazione del materiale della chiave con un intervallo di scadenza molto breve potrebbe fornire un livello di controllo simile senza comportare rischi in termini di prestazioni o disponibilità.

Un archivio delle chiavi esterne potrebbe essere la soluzione ideale per la tua organizzazione se disponi dei requisiti seguenti:

- Devi utilizzare le chiavi crittografiche nel gestore delle chiavi on-premise o in un gestore delle chiavi esterne al di fuori di AWS che è sotto il tuo controllo.

- Devi dimostrare che le chiavi crittografiche vengono conservate esclusivamente sotto il tuo controllo al di fuori del cloud.
- Devi crittografare e decrittografare tramite chiavi crittografiche con autorizzazione indipendente.
- Il materiale chiave deve essere sottoposto a un percorso di audit secondario e indipendente.

Se scegli un archivio delle chiavi esterne, limita il suo utilizzo ai carichi di lavoro che richiedono protezione con chiavi crittografiche al di fuori di AWS.

Modello di responsabilità condivisa

Le chiavi KMS standard utilizzano il materiale della chiave generato e utilizzato nei moduli di sicurezza hardware di proprietà e gestiti da AWS KMS. Sei tu a stabilire le policy di controllo degli accessi sulle chiavi KMS e a configurare i Servizi AWS che utilizzano le chiavi KMS per proteggere le tue risorse. AWS KMS si assume la responsabilità della sicurezza, della disponibilità, della latenza e della durata del materiale della chiave nelle chiavi KMS.

Le chiavi KMS negli archivi delle chiavi esterne si basano sul materiale della chiave e sulle operazioni del gestore delle chiavi esterne. Pertanto, l'equilibrio delle responsabilità si sposta a tuo carico. Sei responsabile della sicurezza, dell'affidabilità, della durata e delle prestazioni delle chiavi crittografiche nel gestore delle chiavi esterne. AWS KMS è responsabile della risposta tempestiva alle richieste e della comunicazione con il proxy dell'archivio delle chiavi esterne, nonché del mantenimento dei nostri standard di sicurezza. Per garantire che ogni testo criptato dell'archivio delle chiavi esterne sia almeno altrettanto robusto del testo criptato AWS KMS standard, AWS KMS crittografa innanzitutto il testo in chiaro con il materiale della chiave AWS KMS specifico per la tua chiave KMS e poi lo invia al gestore delle chiavi esterne per la crittografia con la chiave esterna, una procedura nota come doppia crittografia. Di conseguenza, né AWS KMS né il proprietario del materiale della chiave esterna possono decrittografare da soli il testo criptato con doppia crittografia.

Sei responsabile del mantenimento di un gestore di chiavi esterno che soddisfi i tuoi standard normativi e prestazionali, della fornitura e della manutenzione di un proxy dell'archivio di chiavi esterno che sia conforme alla specifica API del proxy dell'archivio di chiavi esterno AWS KMS e della garanzia di durabilità e disponibilità del materiale della tua chiave. Devi inoltre creare, configurare e gestire un archivio delle chiavi esterne. Quando si verificano errori causati dai componenti da te gestiti, devi essere pronto a identificarli e risolverli in modo che i servizi AWS possano accedere alle risorse senza interruzioni indebite. AWS KMS fornisce una guida alla risoluzione dei problemi per aiutarti a determinare la causa dei problemi e le soluzioni più probabili.

Esamina le CloudWatch metriche e le dimensioni di Amazon registrate per gli AWS KMS archivi di chiavi esterni. AWS KMSconsiglia vivamente di creare CloudWatch allarmi per monitorare l'archivio di chiavi esterno in modo da poter rilevare i primi segnali di problemi prestazionali e operativi prima che si verifichino.

Cosa sta cambiando?

Gli archivi delle chiavi esterne supportano solo chiavi KMS di crittografia simmetrica. All'interno di AWS KMS, utilizzi e gestisci le chiavi KMS in un archivio delle chiavi esterne più o meno allo stesso modo in cui gestisci le altre chiavi gestite dal cliente, inclusa l'impostazione delle policy di controllo degli accessi e il monitoraggio dell'uso delle chiavi. Utilizzi le stesse API e gli stessi parametri per richiedere un'operazione di crittografia con una chiave KMS in un archivio delle chiavi esterne che usi per qualsiasi chiave KMS. Anche i prezzi sono gli stessi delle chiavi KMS standard. Per i dettagli, consulta le sezioni Gestione di chiavi KMS in un archivio delle chiavi esterne, Utilizzo delle chiavi KMS in un archivio delle chiavi esterne e Prezzi di AWS Key Management Service.

Tuttavia, con gli archivi delle chiavi esterne cambiano i seguenti principi:

- Sei responsabile della disponibilità, della durata e della latenza delle operazioni con le chiavi.
- Sei responsabile di tutti i costi per lo sviluppo, l'acquisto, il funzionamento e la concessione di licenze per il sistema di gestione delle chiavi esterne.
- Puoi implementare l'autorizzazione indipendente di tutte le richieste da AWS KMS al proxy dell'archivio delle chiavi esterne.
- Puoi monitorare, controllare e registrare tutte le operazioni del proxy dell'archivio delle chiavi esterne e tutte le operazioni del gestore delle chiavi esterne relative alle richieste AWS KMS.

Da dove iniziare?

Per creare e gestire un archivio delle chiavi esterne, è necessario scegliere l'opzione di connettività proxy dell'archivio delle chiavi esterne, assemblare i prerequisiti e infine creare e configurare l'archivio delle chiavi esterne. Per iniziare, consulta Pianificazione di un archivio delle chiavi esterne.

Quote

AWS KMS consente la creazione di un massimo di 10 archivi delle chiavi personalizzate in ciascuna regione e Account AWS, inclusi gli archivi delle chiavi di AWS CloudHSM e gli archivi delle chiavi esterne, indipendentemente dallo stato della connessione. Inoltre, sono previste quote di richieste AWS KMS sull'uso delle chiavi KMS in un archivio delle chiavi esterno.

Se scegli la connettività proxy VPC per il proxy dell'archivio delle chiavi esterne, potrebbero esserci anche quote sui componenti richiesti, come VPC, sottoreti e Network Load Balancer. Per ulteriori informazioni su queste quote, utilizza la console Service Quotas.

Regioni

Per ridurre al minimo la latenza di rete, crea i componenti dell'archivio delle chiavi esterne nella Regione AWS più vicina al gestore delle chiavi esterne. Se possibile, scegli una regione con un tempo di andata e ritorno (RTT) della rete di 35 millisecondi o meno.

Gli archivi di chiavi esterni sono supportati in tutte le Regioni AWS che supportano AWS KMS, ad eccezione di Cina (Pechino) e Cina (Ningxia).

Caratteristiche non supportate

AWS KMS non supporta le seguenti funzioni negli archivi delle chiavi personalizzate.

- Chiavi KMS asimmetriche
- Coppie di chiavi di dati asimmetriche
- Chiavi KMS HMAC
- Chiavi KMS con materiale della chiave importato
- Rotazione automatica delle chiavi
- Chiavi multi-regione

Argomenti

- Concetti fondamentali sull'archivio delle chiavi esterne
- Funzionamento degli archivi delle chiavi esterne
- Controllo dell'accesso all'archivio delle chiavi esterne
- Pianificazione di un archivio delle chiavi esterne
- Gestione di un archivio delle chiavi esterne
- Gestione di chiavi KMS in un archivio delle chiavi esterne
- Risoluzione dei problemi relativi all'archivio delle chiavi esterne

Concetti fondamentali sull'archivio delle chiavi esterne

Questo argomento descrive alcuni dei concetti utilizzati in relazione agli archivi delle chiavi esterne.

Argomenti

Archivio delle chiavi esterne

Un archivio delle chiavi esterne è un archivio delle chiavi personalizzate di AWS KMS supportato da un gestore delle chiavi esterne che possiedi e gestisci al di fuori di AWS. Ogni chiave KMS in un archivio delle chiavi esterne è associata a una chiave esterna nel gestore delle chiavi esterne. Quando utilizzi una chiave KMS in un archivio delle chiavi esterne per la crittografia o la decrittografia, l'operazione viene eseguita nel gestore delle chiavi esterne utilizzando la chiave esterna, una funzionalità nota come HYOK (Hold Your Own Keys). Questa funzionalità è progettata per le organizzazioni che devono mantenere le chiavi crittografiche nel proprio gestore delle chiavi esterne.

Gli archivi delle chiavi esterne assicurano che le chiavi e le operazioni di crittografia che proteggono le risorse AWS rimangano nel gestore delle chiavi esterne sotto il tuo controllo. AWS KMS invia le richieste al gestore delle chiavi esterne per crittografare e decrittografare i dati, ma AWS KMS non può creare, eliminare o gestire le chiavi esterne. Tutte le richieste inviate da AWS KMS al gestore delle chiavi esterne sono mediate da un componente software del proxy dell'archivio delle chiavi esterne che fornisci, possiedi e gestisci.

I servizi AWS che supportano le chiavi gestite dal cliente di AWS KMS possono utilizzare le chiavi KMS all'interno dell'archivio delle chiavi esterne al fine di proteggere i dati. Di conseguenza, i tuoi dati sono infine protetti dalle chiavi utilizzando le operazioni di crittografia nel gestore delle chiavi esterne.

Le chiavi KMS in un archivio delle chiavi esterne presentano modelli di attendibilità, accordi di responsabilità condivisa e aspettative prestazionali fondamentalmente diversi rispetto alle chiavi KMS standard. Con gli archivi delle chiavi esterne, sei responsabile della sicurezza e dell'integrità del materiale della chiave e delle operazioni di crittografia. La disponibilità e la latenza delle chiavi KMS in un archivio delle chiavi esterne sono influenzate dall'hardware, dal software, dai componenti di rete e dalla distanza tra AWS KMS e il gestore delle chiavi esterne. È inoltre probabile che vengano addebitati costi aggiuntivi per il gestore delle chiavi esterne e per l'infrastruttura di rete e il sistema di bilanciamento del carico necessari per la comunicazione tra il gestore e AWS KMS.

Puoi utilizzare l'archivio delle chiavi esterne come parte di una strategia di protezione dei dati più ampia. Per ogni risorsa AWS protetta, puoi decidere quali richiedono una chiave KMS in un archivio delle chiavi esterne e quali possono essere protette da una chiave KMS standard. Ciò ti offre la flessibilità di scegliere le chiavi KMS per classificazioni di dati, applicazioni o progetti specifici.

Gestore delle chiavi esterne

Un gestore delle chiavi esterne è un componente al di fuori di AWS che può generare chiavi simmetriche AES a 256 bit ed eseguire operazioni di crittografia e decrittografia simmetriche. Il gestore delle chiavi esterne per un relativo archivio può essere costituito da un modulo di sicurezza hardware (HSM) fisico, un HSM virtuale o un gestore delle chiavi software con o senza un componente HSM. Può trovarsi ovunque al di fuori di AWS, anche in un sistema on-premise, in un data center locale o remoto o in qualsiasi cloud. L'archivio delle chiavi esterne può essere supportato da un singolo gestore delle chiavi esterne o da più istanze di gestione delle chiavi correlate che condividono chiavi crittografiche, ad esempio un cluster HSM. Gli archivi delle chiavi esterne sono progettati per supportare una varietà di gestori esterni di diversi fornitori. Per informazioni dettagliate sui requisiti del gestore delle chiavi esterne, consulta Pianificazione di un archivio delle chiavi esterne.

Chiave esterna

Ogni chiave KMS in un archivio delle chiavi esterne è associata a una chiave crittografica, nota come chiave esterna, nel gestore delle chiavi esterne. Quando si esegue la crittografia o la decrittografia con una chiave KMS nell'archivio delle chiavi esterne, l'operazione di crittografia viene eseguita nel gestore delle chiavi esterne tramite la chiave esterna.

> **Warning**
>
> La chiave esterna è essenziale per il funzionamento della chiave KMS. Se la chiave esterna viene persa o eliminata, il testo criptato che è stato crittografato con la chiave KMS associata non è recuperabile.

Per gli archivi delle chiavi esterne, una chiave esterna deve essere una chiave AES a 256 bit abilitata per e in grado di eseguire le operazioni di crittografia e decrittografia. Per maggiori dettagli sui requisiti della chiave esterna, consulta Requisiti per una chiave KMS in un archivio delle chiavi esterne.

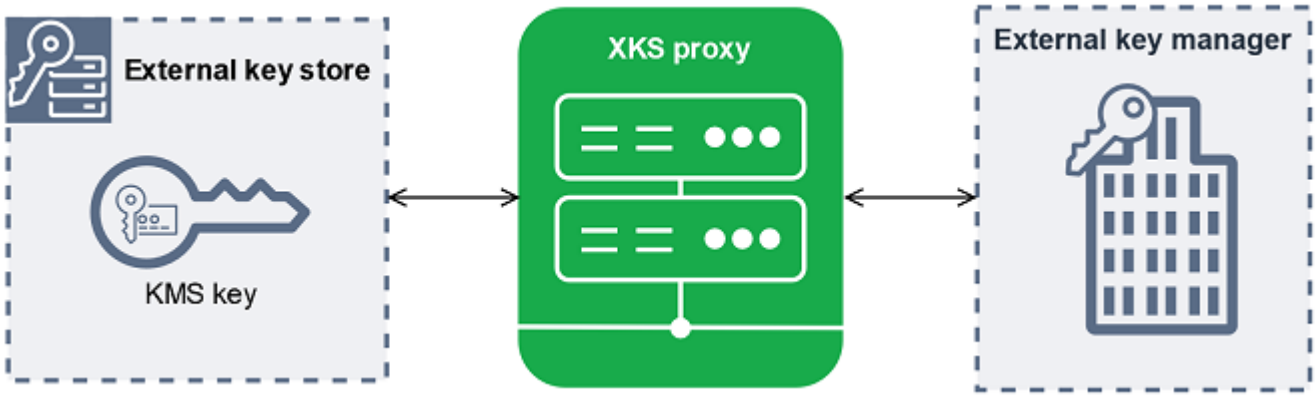
AWS KMS non può creare, eliminare o gestire chiavi esterne. Il materiale della chiave crittografica resta sempre all'interno del gestore delle chiavi esterne. Quando crei una chiave KMS in un archivio delle chiavi esterne, sei tu a fornire l'ID di una chiave esterna (`XksKeyId`). Non puoi modificare l'ID della chiave esterna associato a una chiave KMS, sebbene il gestore delle chiavi esterne possa ruotare il materiale della chiave associato a tale ID.

Oltre alla chiave esterna, una chiave KMS in un archivio delle chiavi esterne contiene anche il materiale della chiave AWS KMS. I dati protetti dalla chiave KMS vengono crittografati innanzitutto da AWS KMS utilizzando il materiale della chiave AWS KMS e quindi dal gestore delle chiavi esterne tramite la chiave esterna. Questo processo di doppia crittografia garantisce che il testo criptato protetto dalla chiave KMS sia sempre perlomeno altrettanto sicuro che il testo criptato protetto solo da AWS KMS.

Molte chiavi crittografiche presentano diversi tipi di identificatori. Quando crei una chiave KMS in un archivio delle chiavi esterne, fornisci l'ID della chiave esterna che il proxy dell'archivio delle chiavi esterne utilizza per fare riferimento alla chiave esterna. Se utilizzi l'identificatore sbagliato, il tentativo di creare una chiave KMS nell'archivio delle chiavi esterne ha esito negativo.

Proxy dell'archivio delle chiavi esterne

Il proxy dell'archivio delle chiavi esterne ("proxy XKS") è un'applicazione software di proprietà e gestione del cliente che media tutte le comunicazioni tra AWS KMS e il gestore delle chiavi esterne. Inoltre, traduce le richieste generiche di AWS KMS in un formato comprensibile al gestore delle chiavi esterne specifico del fornitore. Per un archivio delle chiavi esterne è necessario un relativo proxy. Ogni archivio delle chiavi esterne è associato a un relativo proxy.



AWS KMS non può creare, eliminare o gestire chiavi esterne. Il materiale delle chiavi crittografiche resta sempre all'interno del gestore delle chiavi. Tutte le comunicazioni tra AWS KMS e il gestore delle chiavi esterne sono mediate dal proxy dell'archivio delle chiavi esterne. AWS KMS invia le richieste al proxy dell'archivio delle chiavi esterne e riceve da esso le relative risposte. Il proxy dell'archivio delle chiavi esterne è responsabile della trasmissione delle richieste da AWS KMS al gestore delle chiavi esterne e della trasmissione delle risposte dal gestore a AWS KMS.

Tieni presente che, in quanto proprietario e gestore del proxy dell'archivio delle chiavi esterne, sei responsabile della manutenzione e del funzionamento. Puoi sviluppare il proxy dell'archivio delle chiavi esterne in base alla specifica API relativa al proxy dell'archivio delle chiavi esterne che AWS KMS pubblica oppure puoi acquistare un'applicazione proxy da un fornitore. Il proxy dell'archivio delle chiavi esterne potrebbe essere incluso nel gestore delle chiavi esterne. Per supportare lo sviluppo del proxy, fornisce AWS KMS anche un esempio di key store proxy esterno (aws-kms-xks-proxy) e un client di test (xks-kms-xksproxy-test-client) che verifica che il proxy dell'archivio chiavi esterno sia conforme alle specifiche.

Per l'autenticazione in AWS KMS, il proxy utilizza certificati TLS lato server. Per eseguire l'autenticazione al proxy, AWS KMS firma tutte le richieste per il proxy dell'archivio delle chiavi esterne con credenziali di autenticazione proxy SigV4. Facoltativamente, il proxy può abilitare l'autenticazione TLS reciproca (mTLS) per assicurarsi che accetti solo le richieste provenienti da AWS KMS.

Il proxy dell'archivio di chiavi esterno deve supportare HTTP/1.1 o versione successiva e TLS 1.2 o versione successiva con almeno una delle seguenti suite di crittografia:

- TLS_AES_256_GCM_SHA384 (TLS 1.3)
- TLS_CHACHA20_POLY1305_SHA256 (TLS 1.3)

> **Note**
>
> AWS GovCloud (US) Region non supporta TLS_CHACHA20_POLY1305_SHA256.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (TLS 1.2)
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (TLS 1.2)

Per creare e utilizzare le chiavi KMS nell'archivio delle chiavi esterne, devi innanzitutto connettere l'archivio delle chiavi esterne al relativo proxy. Puoi anche disconnettere l'archivio delle chiavi esterne dal relativo proxy su richiesta. Quando esegui questa operazione, tutte le chiavi KMS nell'archivio delle chiavi esterne diventano non disponibili, di conseguenza non possono essere utilizzate in alcuna operazione di crittografia.

Connettività proxy dell'archivio delle chiavi esterne

La connettività proxy dell'archivio delle chiavi esterne ("connettività proxy XKS") descrive il metodo utilizzato da AWS KMS per comunicare con il proxy dell'archivio delle chiavi esterne.

Puoi specificare l'opzione di connettività proxy durante la creazione dell'archivio delle chiavi esterne, rendendola così una proprietà di tale archivio. Puoi modificare l'opzione di connettività proxy aggiornando la proprietà dell'archivio delle chiavi personalizzate, tuttavia devi accertarti che il proxy dell'archivio delle chiavi esterne possa comunque accedere alle stesse chiavi esterne.

AWS KMS supporta le opzioni di connettività seguenti:

- Connettività dell'endpoint pubblico: AWS KMS invia richieste per il proxy dell'archivio delle chiavi esterne tramite Internet a un endpoint pubblico sotto il tuo controllo. Questa opzione è semplice da creare e gestire, ma potrebbe non soddisfare i requisiti di sicurezza per ogni installazione.
- Connettività del servizio endpoint VPC: AWS KMS invia richieste a un servizio endpoint Amazon Virtual Private Cloud (Amazon VPC) che crei e gestisci tu. Puoi ospitare il proxy dell'archivio delle chiavi esterne all'interno di Amazon VPC oppure al di fuori di AWS, utilizzando Amazon VPC solo per la comunicazione.

Per informazioni dettagliate sulle opzioni di connettività proxy dell'archivio delle chiavi esterne, consulta Scelta di un'opzione di connettività proxy.

Credenziali di autenticazione al proxy dell'archivio delle chiavi esterne

Per eseguire l'autenticazione al proxy dell'archivio delle chiavi esterne, AWS KMS firma tutte le richieste al proxy dell'archivio delle chiavi esterne con credenziali di autenticazione Signature V4 (SigV4). Sei tu a stabilire e gestire le credenziali di autenticazione sul proxy, quindi a fornire tali credenziali a AWS KMS durante la creazione dell'archivio delle chiavi esterne.

> **Note**
>
> Le credenziali SigV4 utilizzate da AWS KMS per firmare le richieste al proxy XKS non sono correlate alle credenziali SigV4 associate ai principali AWS Identity and Access Management nei tuoi Account AWS. Non riutilizzare le credenziali SigV4 IAM per il proxy dell'archivio delle chiavi esterne.

Ogni credenziale di autenticazione proxy è costituita da due parti. Devi fornire entrambe le parti durante la creazione di un archivio delle chiavi esterne o l'aggiornamento delle credenziali di autenticazione per l'archivio delle chiavi esterne.

- ID chiave di accesso: identifica la chiave di accesso segreta. Puoi fornire questo ID come un testo non crittografato.
- Chiave di accesso segreta: la parte segreta delle credenziali. AWS KMS crittografa la chiave di accesso segreta nelle credenziali prima di archiviarla.

Puoi modificare l'impostazione delle credenziali in qualsiasi momento, ad esempio quando inserisci valori errati, quando modifichi le credenziali nel proxy o quando il proxy esegue la rotazione delle credenziali. Per dettagli tecnici sull'autenticazione di AWS KMS al proxy dell'archivio delle chiavi esterne, consulta Autenticazione nella Specifica API relativa al proxy dell'archivio delle chiavi esterne di AWS KMS.

Per ruotare le credenziali senza interrompere i Servizi AWS che utilizzano le chiavi KMS nell'archivio delle chiavi esterne, assicurati che il proxy dell'archivio delle chiavi esterne supporti almeno due credenziali di autenticazione valide per AWS KMS. Ciò garantisce che le credenziali precedenti continuino a funzionare mentre fornisci le nuove credenziali a AWS KMS.

Per aiutarti a tenere traccia dell'età delle tue credenziali di autenticazione proxy, AWS KMS definisce una CloudWatch metrica Amazon,. XksProxyCredentialAge Puoi utilizzare questa metrica per creare

un CloudWatch allarme che ti avvisa quando l'età delle tue credenziali raggiunge una soglia da te stabilita.

Per garantire inoltre che il proxy dell'archivio delle chiavi esterne risponda solo a AWS KMS, alcuni proxy supportano l'autenticazione TLS reciproca. Per informazioni dettagliate, vedi Autenticazione TLS reciproca (facoltativa).

API proxy

Per supportare un archivio delle chiavi esterne di AWS KMS, un proxy dell'archivio delle chiavi esterne deve implementare le API proxy richieste come descritto nella Specifica API relativa al proxy dell'archivio delle chiavi esterne di AWS KMS. Queste richieste API proxy sono le uniche richieste inviate da AWS KMS al proxy. Sebbene non si inviino mai direttamente queste richieste, conoscerle potrebbe aiutarti a risolvere eventuali problemi che potrebbero verificarsi con l'archivio delle chiavi esterne o il relativo proxy. Ad esempio, AWS KMS include informazioni sulla latenza e le percentuali di successo di queste chiamate API nelle CloudWatch metriche Amazon per gli archivi di chiavi esterni. Per informazioni dettagliate, vedi Monitoraggio di un archivio delle chiavi esterne.

Nella tabella seguente sono elencate e descritte tutte le API proxy. Include anche le operazioni AWS KMS che attivano una chiamata all'API proxy e tutte le eccezioni operative di AWS KMS relative all'API proxy.

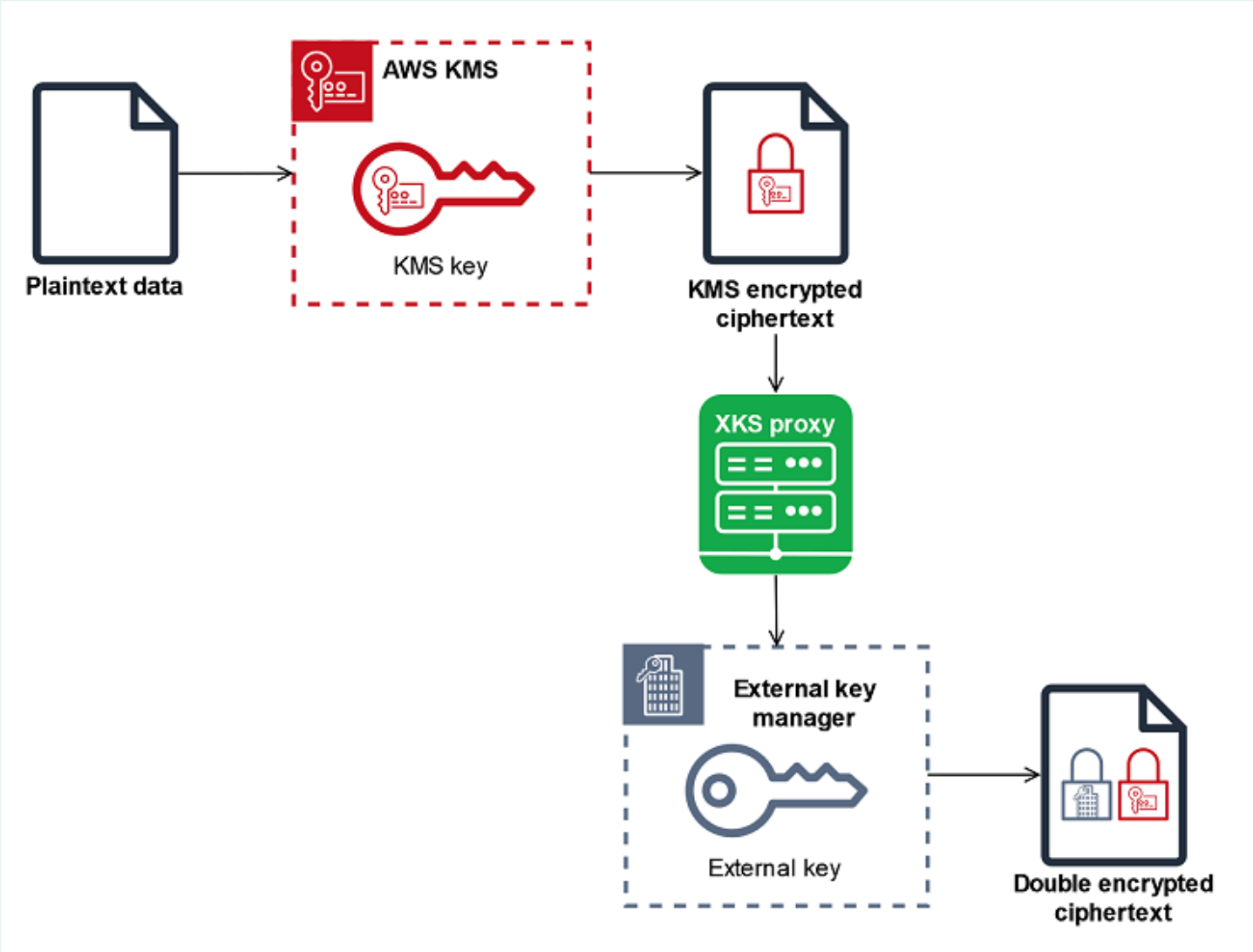
API proxy	Descrizione	Operazioni AWS KMS correlate
Decrypt	AWS KMS invia il testo criptato da decifrare e l'ID della chiave esterna da utilizzare. L'algoritmo di crittografia richiesto è AES_GCM.	Decrittografa, ReEncrypt
Crittografa	AWS KMS invia i dati da crittografare e l'ID della chiave esterna da utilizzare. L'algoritmo di crittografia richiesto è AES_GCM.	Crittografa,, GenerateDataKeyGenerateDataKeyWithoutPlaintextReEncrypt
GetHealthStatus	AWS KMS richiede informazioni sullo stato del proxy e del gestore delle chiavi esterne.	CreateCustomKeyStore(per la connettività degli endpoint pubblici), ConnectCustomKeyStore(per la connettività del servizio endpoint VPC)

API proxy	Descrizione	Operazioni AWS KMS correlate
	Lo stato di ogni gestore delle chiavi esterne può essere uno dei seguenti. • `Active`: integro, può servire il traffico • `Degraded`: non integro, ma può servire il traffico • `Unavailable` : non integro, non può servire il traffico	Se tutte le istanze del gestore delle chiavi esterne sono `Unavailable` , i tentativi di creare o connettere l'archivio delle chiavi hanno esito negativo con l'eccezione `XksProxyUriUnreachableException` .
GetKeyMetadata	AWS KMS richiede informazioni sulla chiave esterna associata a una chiave KMS nell'archivio delle chiavi esterne. La risposta include le specifiche della chiave (`AES_256`), il suo utilizzo (`[ENCRYPT, DECRYPT]`) e se la chiave esterna è `ENABLED` o `DISABLED`.	CreateKey Se la specifica della chiave non è `AES_256`, se l'utilizzo della chiave non è `[ENCRYPT, DECRYPT]` o lo stato è `DISABLED`, l'operazione `CreateKey` ha esito negativo con l'eccezione `XksKeyInvalidConfigurationException` .

Doppia crittografia

I dati crittografati con una chiave KMS in un archivio delle chiavi esterne vengono crittografati due volte. Innanzitutto ,AWS KMS esegue la crittografia dei dati con il materiale della chiave di AWS KMS specifico per la chiave KMS. Quindi, il testo criptato con AWS KMS viene crittografato dal gestore delle chiavi esterne utilizzando la chiave esterna. Questo processo è noto come doppia crittografia.

La doppia crittografia garantisce che i dati crittografati da una chiave KMS in un archivio delle chiavi esterne siano almeno altrettanto sicuri del testo criptato crittografato da una chiave KMS standard. Protegge inoltre il testo non crittografato in transito da AWS KMS al proxy dell'archivio delle chiavi esterne. Con la doppia crittografia, mantieni il pieno controllo dei tuoi testi criptati. Se revochi definitivamente l'accesso AWS alla chiave esterna tramite il proxy esterno, qualsiasi testo criptato rimasto in AWS viene effettivamente eliminato in modo crittografato.



Per abilitare la doppia crittografia, ogni chiave KMS in un archivio delle chiavi esterne dispone di due materiali della chiave crittografica:

- Un materiale della chiave di AWS KMS univoco per la chiave KMS. Questo materiale della chiave viene generato e utilizzato solo in moduli di sicurezza hardware (HSM) con certificazione del livello di sicurezza 3 FIPS 140-2 AWS KMS.
- Una chiave esterna nel gestore delle chiavi esterne.

La doppia crittografia ha i seguenti effetti:

- AWS KMS non è in grado di decrittografare alcun testo criptato crittografato da una chiave KMS in un archivio delle chiavi esterne senza accedere alle chiavi esterne tramite il proxy dell'archivio delle chiavi esterne.

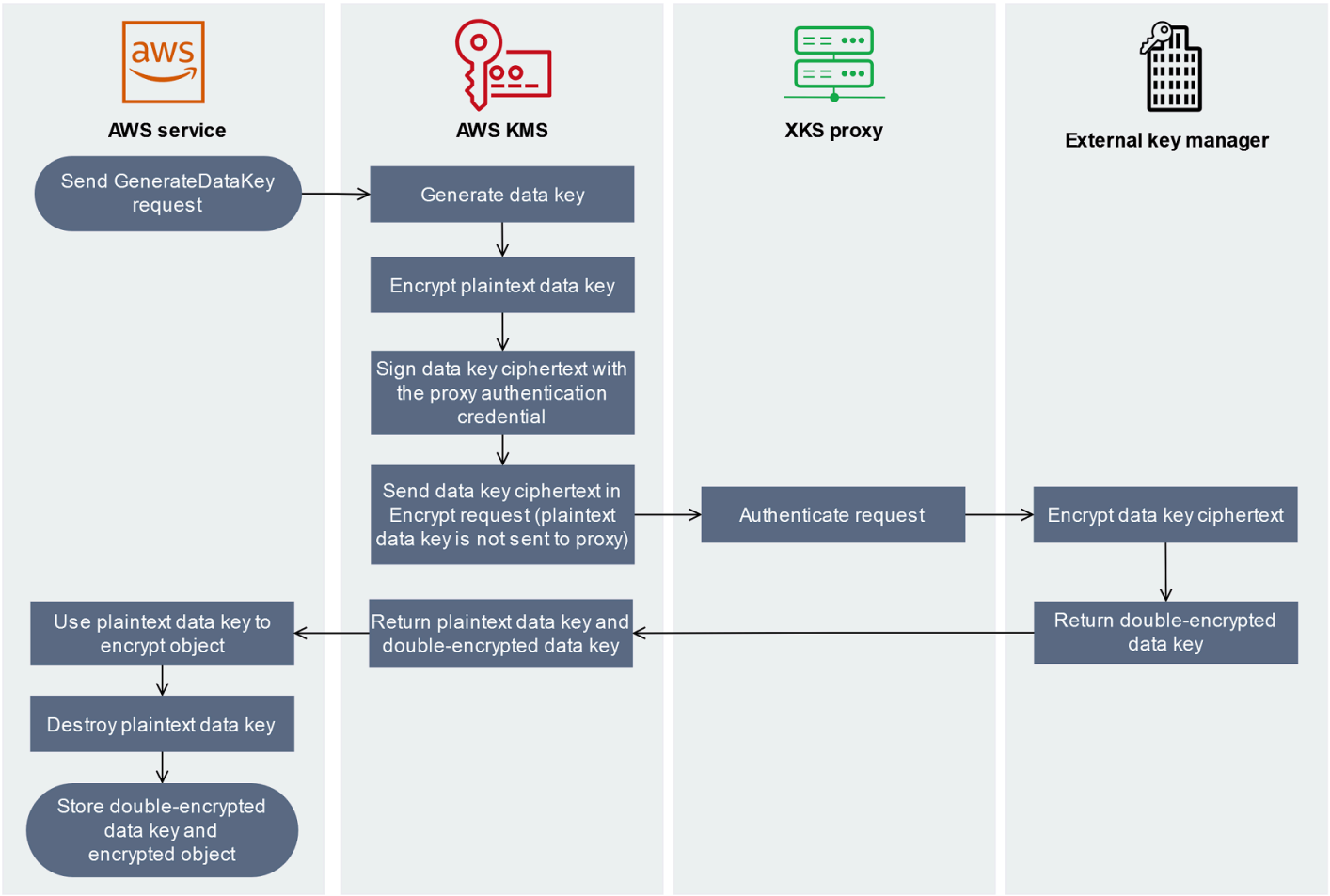
- Non puoi decrittografare alcun testo criptato crittografato da una chiave KMS in un archivio delle chiavi esterne al di fuori di AWS, anche se disponi del relativo materiale della chiave.
- Non puoi ricreare una chiave KMS eliminata da un archivio delle chiavi esterne, anche se disponi del relativo materiale della chiave. Ogni chiave KMS presenta metadati univoci inclusi nel testo criptato simmetrico. Una nuova chiave KMS non sarebbe in grado di decrittografare il testo criptato con la chiave originale, anche se utilizza lo stesso materiale della chiave esterna.

Per un esempio pratico di doppia crittografia, consulta Funzionamento degli archivi delle chiavi esterne.

Funzionamento degli archivi delle chiavi esterne

L'archivio delle chiavi esterne, il proxy dell'archivio delle chiavi esterne e il gestore delle chiavi esterne collaborano insieme per proteggere le tue risorse AWS. La procedura seguente descrive il flusso di lavoro di crittografia di un tipico Servizio AWS che esegue la crittografia di ogni oggetto con una chiave dati univoca protetta da una chiave KMS. In questo caso, hai scelto una chiave KMS in un archivio delle chiavi esterne per proteggere l'oggetto. L'esempio mostra il modo in cui AWS KMS utilizza la doppia crittografia per proteggere la chiave dati in transito e garantire che il testo criptato generato da una chiave KMS in un archivio delle chiavi esterne sia sempre altrettanto sicuro del testo crittografato da una chiave KMS simmetrica standard con il materiale della chiave in AWS KMS.

I metodi di crittografia utilizzati da ogni Servizio AWS effettivo che si integra con AWS KMS variano. Per maggiori dettagli, consulta l'argomento "Protezione dei dati" nel capitolo Sicurezza della documentazione di Servizio AWS.



1. Aggiungi un nuovo oggetto alla risorsa Servizio AWS. Per crittografare l'oggetto, Servizio AWS invia una GenerateDataKeyrichiesta all'AWS KMSutilizzo di una chiave KMS nell'archivio di chiavi esterno.
2. AWS KMS genera una chiave dati simmetrica a 256 bit e si prepara a inviare una copia non crittografata di essa al gestore delle chiavi esterne tramite il proxy dell'archivio delle chiavi esterne. AWS KMS inizia il processo di doppia crittografia crittografando la chiave dati con il materiale della chiave di AWS KMS associato alla chiave KMS nell'archivio delle chiavi esterne.
3. AWS KMS invia una richiesta encrypt al proxy associato all'archivio delle chiavi esterne. La richiesta include il testo criptato della chiave dati da crittografare e l'ID della chiave esterna associata alla chiave KMS. AWS KMS firma la richiesta utilizzando le credenziali di autenticazione proxy per il proxy dell'archivio delle chiavi esterne.

   La copia non crittografata della chiave dati non viene inviata al proxy dell'archivio delle chiavi esterno.

4. Il proxy dell'archivio delle chiavi esterne autentica la richiesta di crittografia e quindi la trasmette al gestore delle chiavi esterne.

   Alcuni proxy dell'archivio delle chiavi esterne implementano anche una policy di autorizzazione facoltativa che consente solo ai principali selezionati di eseguire operazioni in condizioni specifiche.
5. Il gestore delle chiavi esterne esegue la crittografia del testo criptato della chiave dati utilizzando la chiave esterna specificata e restituisce la chiave dati con doppia crittografia al proxy dell'archivio delle chiavi esterne che a sua volta la restituisce a AWS KMS.
6. AWS KMS restituisce la chiave dati non crittografata e la copia della chiave dati con doppia crittografia a Servizio AWS.
7. Servizio AWS utilizza la chiave dati non crittografata per crittografare l'oggetto della risorsa prima di distruggerla e archivia la chiave dati crittografata con l'oggetto crittografato.

   Alcuni Servizi AWS potrebbero memorizzare nella cache la chiave dati non crittografata per utilizzarla con più oggetti o mentre la risorsa è in uso. Per informazioni dettagliate, vedi In che modo le chiavi KMS inutilizzabili influiscono sulle chiavi dati.

Per decrittografare l'oggetto crittografato, il Servizio AWS deve inviare nuovamente la chiave dati a AWS KMS in una richiesta Decrypt. Per decrittografare la chiave di dati crittografata, AWS KMS deve inviare la chiave dati crittografata al proxy dell'archivio delle chiavi esterne con l'ID della chiave esterna. Se per qualsiasi motivo la richiesta di decrittografia al proxy dell'archivio delle chiavi esterne ha esito negativo, AWS KMS non può decrittografare la chiave dati crittografata e Servizio AWS non può decrittografare l'oggetto crittografato.

Controllo dell'accesso all'archivio delle chiavi esterne

Tutte le funzionalità di controllo degli accessi AWS KMS, vale a dire le policy delle chiavi, le policy IAM e le autorizzazioni, utilizzate con le chiavi KMS standard funzionano allo stesso modo per le chiavi KMS in un archivio delle chiavi esterne. Puoi utilizzare le policy IAM per controllare l'accesso alle operazioni API che creano e gestiscono archivi delle chiavi esterne. Puoi utilizzare le policy IAM e le policy delle chiavi per controllare l'accesso alle AWS KMS keys nell'archivio delle chiavi esterne. Puoi anche utilizzare le policy di controllo dei servizi per la tua organizzazione AWS e le policy degli endpoint VPC per controllare l'accesso alle chiavi KMS nell'archivio delle chiavi esterne.

Ti consigliamo di concedere a utenti e ruoli soltanto le autorizzazioni necessarie per le attività che sono supposti eseguire.

Argomenti

Autorizzazione dei gestori dell'archivio delle chiavi esterne

I principali che creano e gestiscono un archivio delle chiavi esterne necessitano di autorizzazioni per eseguire le operazioni dell'archivio delle chiavi personalizzate. L'elenco seguente descrive le autorizzazioni minime necessarie per i gestori dell'archivio delle chiavi esterne. Dal momento che l'archivio delle chiavi personalizzate non è una risorsa AWS, non è possibile fornire autorizzazioni a un archivio delle chiavi esterne per i principali di altri Account AWS.

- `kms:CreateCustomKeyStore`
- `kms:DescribeCustomKeyStores`
- `kms:ConnectCustomKeyStore`
- `kms:DisconnectCustomKeyStore`
- `kms:UpdateCustomKeyStore`
- `kms:DeleteCustomKeyStore`

I principali che creano un archivio delle chiavi esterne devono disporre dell'autorizzazione per creare e configurare i componenti di tale archivio. I principali possono creare archivi delle chiavi esterne solo nei propri account. Per creare un archivio delle chiavi esterne con connettività del servizio endpoint VPC, i principali devono disporre dell'autorizzazione per creare i seguenti componenti:

- Un Amazon VPC
- Sottoreti pubbliche e private
- Un Network Load Balancer e un gruppo di destinazione
- Un servizio endpoint Amazon VPC

Per maggiori dettagli, consulta le sezioni Identity and access management per Amazon VPC, Identity and Access Management per endpoint VPC e servizi endpoint VPC e Autorizzazioni API di Elastic Load Balancing.

Autorizzazione degli utenti delle chiavi KMS in archivi delle chiavi esterne

I principali che creano e gestiscono le AWS KMS keys nell'archivio delle chiavi esterne devono disporre delle stesse autorizzazioni di chi crea e gestisce le chiavi KMS in AWS KMS. La policy chiave predefinita per le chiavi KMS in un archivio delle chiavi esterne è identica alla policy chiave predefinita per le chiavi KMS in AWS KMS. Il controllo degli accessi basato su attributi (ABAC), che utilizza tag e alias per controllare l'accesso alle chiavi KMS, sono efficaci anche nelle chiavi KMS negli archivi delle chiavi esterne.

I principali che utilizzano le chiavi KMS nell'archivio delle chiavi personalizzate per operazioni di crittografia devono disporre dell'autorizzazione per eseguire l'operazione di crittografia con la chiave KMS, ad esempio kms:Decrypt. Puoi fornire queste autorizzazioni in una policy IAM o in una policy delle chiavi. I principali non hanno tuttavia bisogno di autorizzazioni supplementari per utilizzare una chiave KMS in un archivio delle chiavi personalizzate.

Per impostare un'autorizzazione che si applica solo alle chiavi KMS in un archivio delle chiavi esterne, utilizza la condizione della policy `kms:KeyOrigin` con un valore di `EXTERNAL_KEY_STORE`. Puoi utilizzare questa condizione per limitare l'CreateKeyautorizzazione kms: o qualsiasi autorizzazione specifica per una risorsa chiave KMS. Ad esempio, la policy IAM seguente consente all'identità a cui è associata di chiamare le operazioni specificate in tutte le chiavi KMS, a condizione che le chiavi KMS si trovino in un archivio delle chiavi esterne. Tieni presente che puoi limitare l'autorizzazione alle chiavi KMS in un archivio delle chiavi esterne e in un Account AWS, ma non a un particolare archivio delle chiavi esterne nell'account.

```
{
  "Sid": "AllowKeysInExternalKeyStores",
  "Effect": "Allow",
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "arn:aws:kms:us-west-2:111122223333:key/*",
  "Condition": {
```

```
    "StringEquals": {
      "kms:KeyOrigin": "EXTERNAL_KEY_STORE"
    }
  }
}
```

Autorizzazione di AWS KMS per comunicare con il proxy dell'archivio delle chiavi esterne

AWS KMS comunica con il gestore delle chiavi esterne solo tramite il proxy dell'archivio delle chiavi esterne che fornisci. AWS KMS esegue l'autenticazione sul proxy firmando le relative richieste tramite il processo Signature Version 4 (SigV4) con le credenziali di autenticazione per il proxy dell'archivio delle chiavi esterne specificate. Se utilizzi la connettività dell'endpoint pubblico per il proxy dell'archivio delle chiavi esterne, AWS KMS non richiede autorizzazioni aggiuntive.

Tuttavia, se utilizzi la connettività del servizio endpoint VPC, devi concedere ad AWS KMS l'autorizzazione per creare un endpoint di interfaccia per il servizio endpoint Amazon VPC. Questa autorizzazione è necessaria, indipendentemente dal fatto che il proxy dell'archivio delle chiavi esterne si trovi nel VPC o altrove, ma utilizza il servizio endpoint VPC per comunicare con AWS KMS.

AWS KMSPer consentire la creazione di un endpoint di interfaccia, utilizza la console Amazon VPC o ModifyVpcEndpointServicePermissionsl'operazione. Consenti le autorizzazioni per il seguente principale: `cks.kms.<region>.amazonaws.com`.

Ad esempio, il comando AWS CLI consente ad AWS KMS di connettersi al servizio endpoint VPC specificato nella regione Stati Uniti occidentali (Oregon) (us-west-2). Prima di eseguire questo comando, sostituisci l'ID del servizio Amazon VPC e la Regione AWS con valori validi per la tua configurazione.

```
modify-vpc-endpoint-service-permissions
--service-id vpce-svc-12abc34567def0987
--add-allowed-principals '["cks.kms.us-west-2.amazonaws.com"]'
```

Per rimuovere questa autorizzazione, usa la console Amazon VPC o ModifyVpcEndpointServicePermissionscon il `RemoveAllowedPrincipals` parametro.

Autorizzazione proxy dell'archivio delle chiavi esterne (facoltativo)

Alcuni proxy degli archivi delle chiavi esterne implementano i requisiti di autorizzazione per l'uso delle relative chiavi esterne. Un proxy dell'archivio delle chiavi esterne è consentito, ma non obbligatorio, per progettare e implementare uno schema di autorizzazione che consenta a determinati utenti di

richiedere determinate operazioni solo in base ad alcune condizioni. Ad esempio, un proxy potrebbe essere configurato per consentire all'utente A di eseguire la crittografia con una particolare chiave esterna, ma non di effettuare l'operazione inversa.

L'autorizzazione proxy è indipendente dall'autenticazione proxy basata su SigV4 richiesta da AWS KMS per tutti i proxy degli archivi delle chiavi esterne. È inoltre indipendente dalle policy delle chiavi, dalle policy IAM e dalle concessioni che autorizzano l'accesso alle operazioni che riguardano l'archivio delle chiavi esterne o le relative chiavi KMS.

Per abilitare l'autorizzazione da parte del proxy dell'archivio delle chiavi esterne, AWS KMS include i metadati in ogni richiesta API proxy, tra cui il chiamante, la chiave KMS, l'operazione AWS KMS e il Servizio AWS (se presente). I metadati della richiesta per la versione 1 (v1) dell'API proxy dell'archivio delle chiavi esterne sono i seguenti.

```
"requestMetadata": {
    "awsPrincipalArn": string,
    "awsSourceVpc": string, // optional
    "awsSourceVpce": string, // optional
    "kmsKeyArn": string,
    "kmsOperation": string,
    "kmsRequestId": string,
    "kmsViaService": string // optional
}
```

Ad esempio, potresti configurare il proxy in modo da consentire le richieste provenienti da un determinato principale (`awsPrincipalArn`), ma solo quando tale richiesta viene effettuata da uno specifico Servizio AWS (`kmsViaService`) per conto del principale.

Se l'autorizzazione proxy fallisce, anche la relativa l'operazione AWS KMS ha esito negativo e viene visualizzato un messaggio che spiega l'errore. Per maggiori dettagli, consulta Problemi relativi all'autorizzazione proxy.

Autenticazione TLS reciproca (facoltativa)

Per consentire al proxy dell'archivio delle chiavi esterne di autenticare le richieste provenienti da AWS KMS, AWS KMS firma tutte le richieste che arrivano al proxy con le credenziali di autenticazione proxy Signature V4 (SigV4) per l'archivio delle chiavi esterne.

Per garantire inoltre che il proxy dell'archivio delle chiavi esterne risponda solo alle richieste di AWS KMS, alcuni proxy supportano l'autenticazione TLS reciproca, in cui le parti che partecipano a una

transazione utilizzano certificati per autenticarsi reciprocamente. L'autenticazione TLS reciproca aggiunge l'autenticazione lato client, in cui il server proxy dell'archivio delle chiavi esterne autentica il client AWS KMS, all'autenticazione lato server fornita dall'autenticazione TLS standard. Nel raro caso in cui le credenziali di autenticazione proxy siano compromesse, l'autenticazione TLS reciproca impedisce a terzi di effettuare richieste API al proxy dell'archivio delle chiavi esterne.

Per implementare l'autenticazione TLS reciproca, configura il proxy dell'archivio delle chiavi esterne in modo che accetti solo certificati TLS lato client con le seguenti proprietà:

- Il nome comune dell'oggetto sul certificato TLS deve essere `cks.kms.<Region>.amazonaws.com`, ad esempio `cks.kms.eu-west-3.amazonaws.com`.
- Il certificato deve essere concatenato a un'autorità di certificazione associata ai servizi di trust di Amazon.

Pianificazione di un archivio delle chiavi esterne

Prima di creare l'archivio delle chiavi esterne, scegli l'opzione di connettività che determina il modo in cui AWS KMS comunica con i componenti dell'archivio. L'opzione di connettività scelta determina il resto del processo di pianificazione.

Ulteriori informazioni:

- Rivedi il processo di creazione di un archivio delle chiavi esterne, incluso l'assemblaggio dei prerequisiti. Ti aiuterà a verificare di disporre di tutti i componenti necessari per la creazione dell'archivio delle chiavi esterne.
- Scopri come controllare l'accesso all'archivio delle chiavi esterne, comprese le autorizzazioni richieste dagli amministratori e dagli utenti dell'archivio.
- Scopri le CloudWatch metriche e le dimensioni di Amazon registrate per gli AWS KMS archivi di chiavi esterni. Ti consigliamo di creare allarmi per monitorare l'archivio delle chiavi esterne, in modo da poter rilevare fin dal principio eventuali segnali relativi a problemi operativi e prestazionali.

Scelta di un'opzione di connettività proxy

Se stai creando un archivio delle chiavi esterne, devi innanzitutto determinare in che modo AWS KMS comunica con il proxy dell'archivio delle chiavi esterne. Questa scelta determinerà i componenti sono necessari e la modalità di configurazione. AWS KMS supporta le seguenti opzioni di connettività. Scegli l'opzione che soddisfa gli obiettivi di prestazioni e sicurezza.

Prima di iniziare, verifica che sia necessario un archivio delle chiavi esterne. La maggior parte dei clienti può utilizzare le chiavi KMS supportate da un materiale della chiave di AWS KMS.

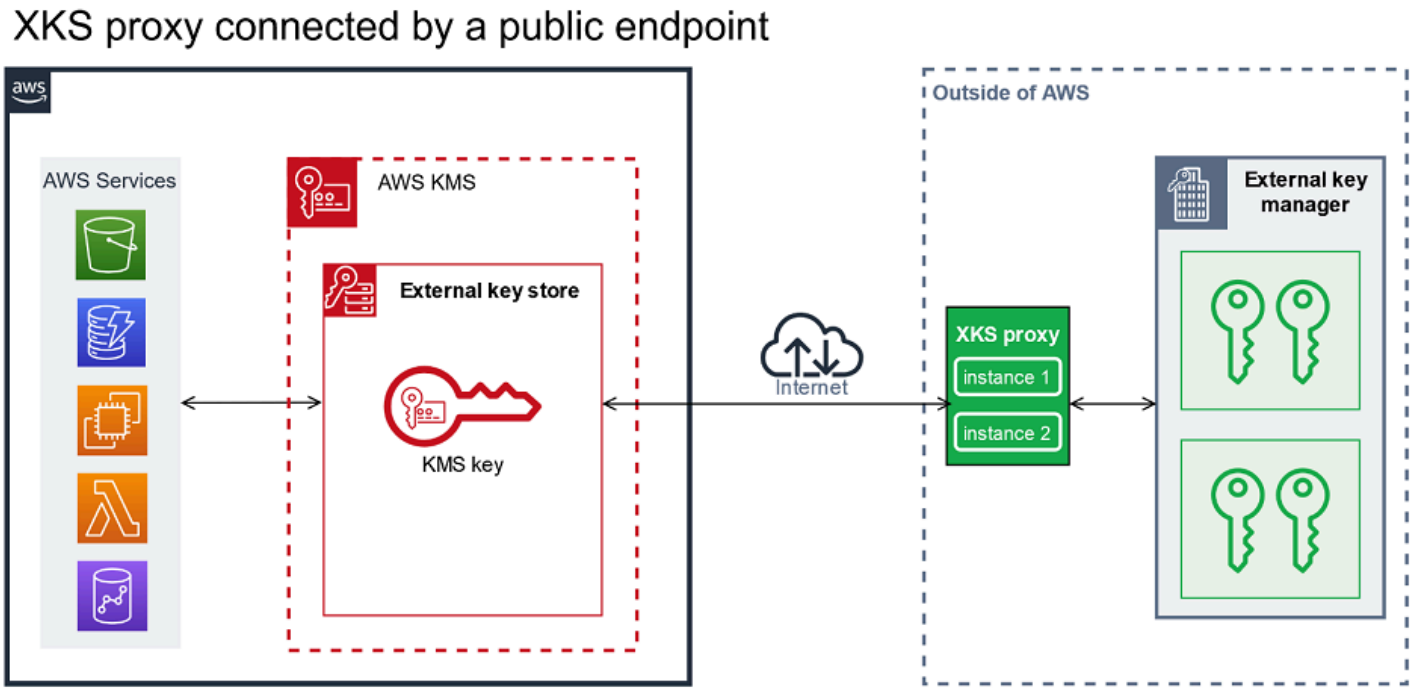
> **Note**
>
> Se il proxy dell'archivio delle chiavi esterne è integrato nel gestore delle chiavi esterne, la connettività potrebbe essere predeterminata. Per informazioni, consulta la documentazione del gestore delle chiavi esterne o del proxy dell'archivio delle chiavi esterne.

Puoi modificare l'opzione di connettività proxy dell'archivio delle chiavi esterne anche su un archivio delle chiavi esterne operativo. Tuttavia, il processo deve essere pianificato ed eseguito con cura per ridurre al minimo le interruzioni, evitare errori e garantire l'accesso continuo alle chiavi crittografiche che crittografano i dati.

Connettività dell'endpoint pubblico

AWS KMS si connette al proxy dell'archivio delle chiavi esterne (proxy XKS) su Internet utilizzando un endpoint pubblico.

Questa opzione di connettività è molto semplice da configurare e gestire e si allinea bene con alcuni modelli di gestione delle chiavi. Tuttavia, potrebbe non soddisfare i requisiti di sicurezza di alcune organizzazioni.



Requisiti

Se scegli la connettività all'endpoint pubblico, è necessario quanto segue.

- Il proxy dell'archivio delle chiavi esterne deve essere raggiungibile da un endpoint indirizzabile pubblicamente.
- Puoi utilizzare lo stesso endpoint pubblico per più archivi delle chiavi esterne, a condizione che utilizzino valori diversi per il percorso URI proxy.
- Non puoi utilizzare lo stesso endpoint per un archivio delle chiavi esterne con connettività all'endpoint pubblico e qualsiasi archivio delle chiavi esterne con connettività del servizio endpoint VPC nella stessa Regione AWS, anche se gli archivi delle chiavi si trovano in diversi Account AWS.
- Devi ottenere un certificato TLS emesso da un'autorità di certificazione pubblica supportata per gli archivi delle chiavi esterne. Per un elenco, consulta Autorità di certificazione attendibili.

  Il nome comune del soggetto (CN) sul certificato TLS deve corrispondere al nome di dominio nell'endpoint URI proxy del proxy dell'archivio delle chiavi esterne. Ad esempio, se l'endpoint pubblico è `https://myproxy.xks.example.com` il TLS, il CN sul certificato TLS deve essere `myproxy.xks.example.com` o `*.xks.example.com`.
- Assicurati che tutti i firewall tra AWS KMS e il proxy dell'archivio delle chiavi esterne consentano il traffico da e verso la porta 443 del proxy. AWS KMS comunica sulla porta 443. Questo valore non è configurabile.

Per informazioni su tutti i requisiti di un archivio delle chiavi esterne, consulta Assemblare i prerequisiti.

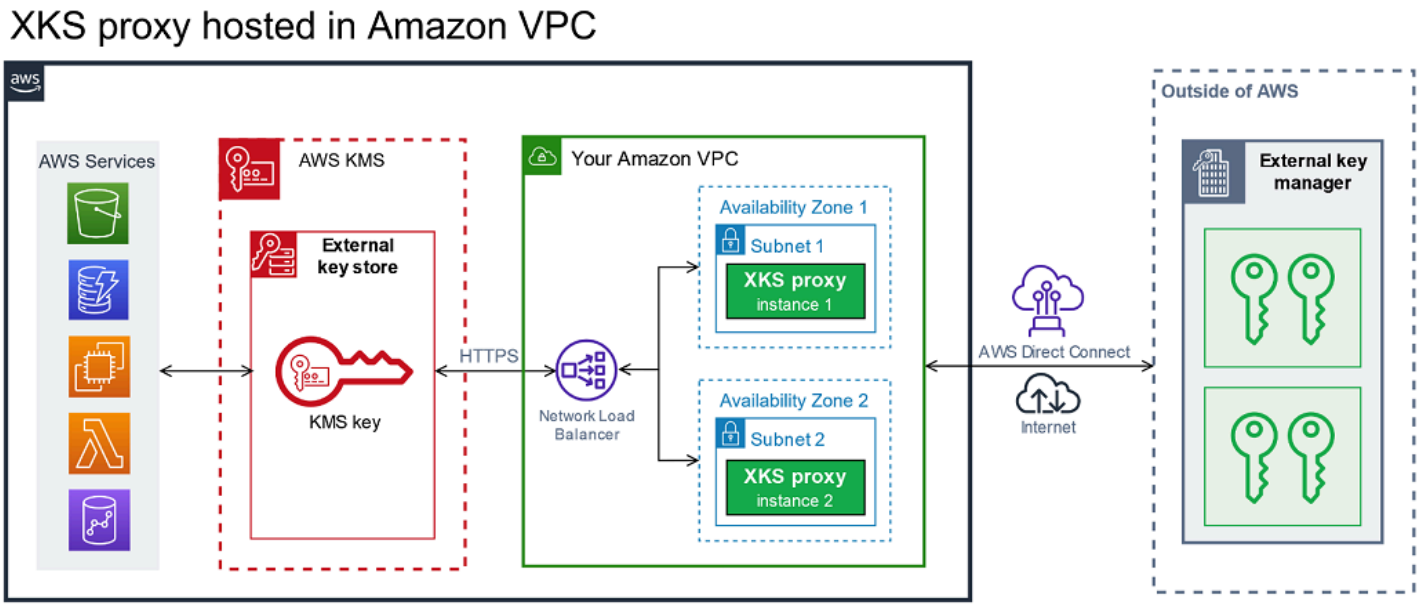
Connettività del servizio endpoint VPC

AWS KMS si connette al proxy dell'archivio delle chiavi esterne (proxy XKS) creando un endpoint di interfaccia a un servizio endpoint Amazon VPC creato e configurato dall'utente. Sei responsabile della creazione del servizio endpoint VPC e della connessione del VPC al gestore delle chiavi esterne.

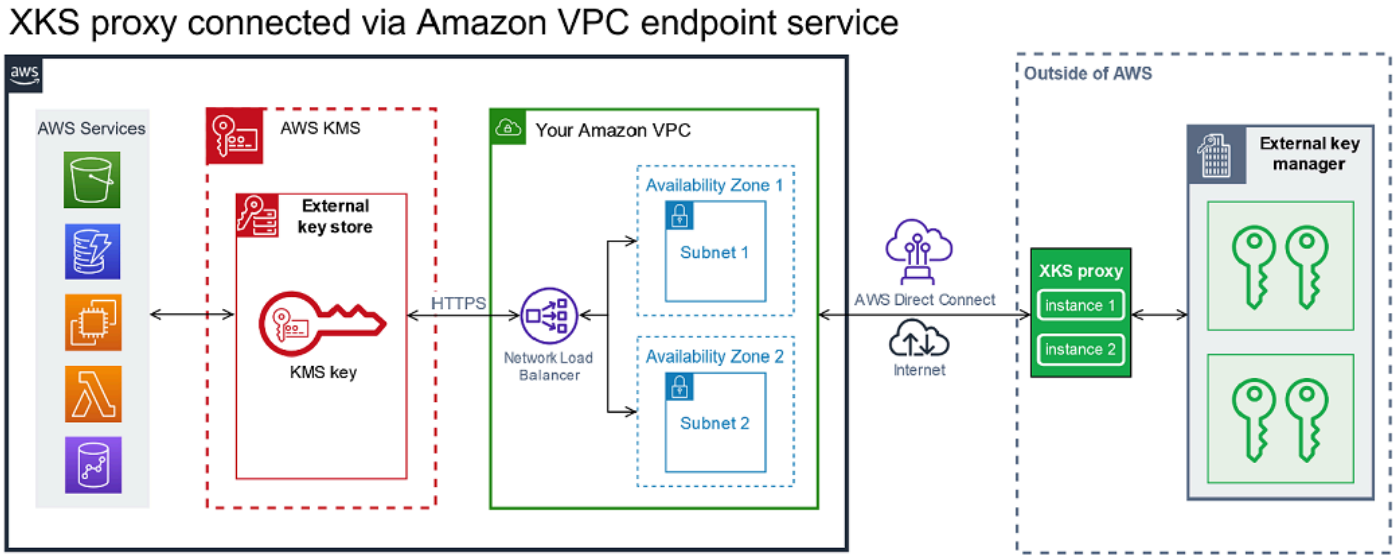
Il servizio endpoint può utilizzare qualsiasi opzione da rete ad Amazon VPC supportata per le comunicazioni, tra cui AWS Direct Connect.

Questa opzione di connettività è più complessa da configurare e gestire. Tuttavia, l'utilizzo di AWS PrivateLink consente ad AWS KMS di connettersi privatamente ad Amazon VPC e al proxy dell'archivio delle chiavi esterne senza utilizzare la rete Internet pubblica.

Puoi posizionare il proxy dell'archivio delle chiavi esterne in Amazon VPC.



Oppure, posiziona il proxy dell'archivio delle chiavi esterne al di fuori di AWS e utilizza il servizio endpoint Amazon VPC esclusivamente per le comunicazioni sicure con AWS KMS.



Configurazione della connettività del servizio endpoint VPC

Utilizza le linee guida in questa sezione per creare e configurare le risorse AWS e i componenti correlati necessari per un archivio delle chiavi esterne che utilizza la connettività del servizio endpoint VPC. Le risorse elencate per questa opzione di connettività sono un supplemento alle risorse necessarie per tutti gli archivi delle chiavi esterne. Dopo aver creato e configurato le risorse necessarie, puoi creare l'archivio delle chiavi esterne.

Puoi posizionare il proxy dell'archivio delle chiavi esterne in Amazon VPC o al di fuori di AWS e utilizzare il servizio endpoint VPC per la comunicazione.

Prima di iniziare, verifica che sia necessario un archivio delle chiavi esterne. La maggior parte dei clienti può utilizzare le chiavi KMS supportate da un materiale della chiave di AWS KMS.

> **Note**
>
> Alcuni degli elementi necessari per la connettività del servizio endpoint VPC potrebbero essere inclusi nel gestore delle chiavi esterne. Inoltre, il software potrebbe avere requisiti di configurazione aggiuntivi. Prima di creare e configurare le risorse AWS presenti in questa sezione, consulta la documentazione del proxy e del gestore delle chiavi.

Argomenti

Requisiti per la connettività del servizio endpoint VPC

Se scegli la connettività del servizio endpoint VPC per l'archivio delle chiavi esterne, sono necessarie le seguenti risorse.

Per ridurre al minimo la latenza di rete, crea i componenti AWS nella Regione AWS supportata più vicina al gestore delle chiavi esterne. Se possibile, scegli una regione con un tempo di andata e ritorno (RTT) della rete di 35 millisecondi o meno.

- Un Amazon VPC collegato al gestore delle chiavi esterne. Deve avere almeno due sottoreti private in due zone di disponibilità diverse.

Puoi utilizzare un Amazon VPC esistente, a condizione che soddisfi i requisiti per l'utilizzo con un archivio delle chiavi esterne. Più archivi delle chiavi esterne possono condividere un Amazon VPC, ma ogni archivio deve avere il proprio servizio endpoint VPC e il proprio nome DNS privato.

- Un servizio endpoint Amazon VPC basato su un AWS PrivateLink con un Network Load Balancer e un gruppo di destinazione.

  Il servizio endpoint non può richiedere l'accettazione. Inoltre, devi aggiungere AWS KMS come principale consentito. In questo modo, AWS KMS è in grado di creare endpoint di interfaccia che gli consentono di comunicare con il proxy dell'archivio delle chiavi esterne.
- Un nome DNS privato per il servizio endpoint VPC univoco nella Regione AWS.

  Il nome DNS privato deve essere un sottodominio di un dominio pubblico di livello superiore. Ad esempio, se il nome DNS privato è `myproxy-private.xks.example.com`, deve essere un sottodominio di un dominio pubblico come `xks.example.com` o `example.com`.

  Devi verificare la proprietà del dominio DNS per il nome DNS privato.
- Un certificato TLS emesso da un'autorità di certificazione pubblica supportata per il proxy dell'archivio delle chiavi esterne.

  Il nome comune del soggetto (CN) sul certificato TLS deve corrispondere al nome DNS privato. Ad esempio, se il nome DNS privato è `myproxy-private.xks.example.com`, il CN sul certificato TLS deve essere `myproxy-private.xks.example.com` o `*.xks.example.com`.

Per informazioni su tutti i requisiti di un archivio delle chiavi esterne, consulta Assemblare i prerequisiti.

Creazione di un Amazon VPC e delle sottoreti

La connettività del servizio endpoint VPC richiede un Amazon VPC connesso al gestore delle chiavi esterne con almeno due sottoreti private. Puoi creare un Amazon VPC o utilizzarne uno esistente che soddisfi i requisiti per gli archivi delle chiavi esterne. Per informazioni sulla creazione di un nuovo Amazon VPC, consulta Creazione di un VPC nella Guida per l'utente di Amazon Virtual Private Cloud.

Requisiti per Amazon VPC

Per lavorare con gli archivi delle chiavi esterne tramite la connettività del servizio endpoint VPC, Amazon VPC deve avere le seguenti proprietà:

- Deve trovarsi nello stesso Account AWS e nella stessa regione supportata dell'archivio delle chiavi esterne.
- Richiede almeno due sottoreti private, ognuna in una zona di disponibilità diversa.
- L'intervallo di indirizzi IP privati di Amazon VPC non deve sovrapporsi all'intervallo di indirizzi IP privati del data center che ospita il gestore delle chiavi esterne.
- Tutti i componenti devono utilizzare IPv4.

Le opzioni per connettere Amazon VPC al proxy dell'archivio delle chiavi esterne sono molteplici. Scegli un'opzione che soddisfi le tue esigenze di prestazioni e sicurezza. Per un elenco, consulta Connetti il tuo VPC ad altre reti e Opzioni di connettività da rete ad Amazon VPC. Per ulteriori dettagli, consulta AWS Direct Connect e la Guida per l'utente di AWS Site-to-Site VPN.

Creazione di un Amazon VPC per l'archivio delle chiavi esterne

Utilizza le istruzioni seguenti per creare un Amazon VPC per l'archivio delle chiavi esterne. Un Amazon VPC è necessario solo se scegli l'opzione di connettività del servizio endpoint VPC. Puoi utilizzare un Amazon VPC esistente, a condizione che soddisfi i requisiti di un archivio delle chiavi esterne.

Segui le istruzioni nell'argomento Creazione di VPC, sottoreti e altre risorse VPC utilizzando i seguenti valori obbligatori. Per gli altri campi, accetta i valori predefiniti e immetti i nomi come richiesto.

Campo	Valore
IPv4 CIDR block (Blocco CIDR IPv4)	Inserisci gli indirizzi IP per il VPC. L'intervallo di indirizzi IP privati di Amazon VPC non deve sovrapporsi all'intervallo di indirizzi IP privati del data center che ospita il gestore delle chiavi esterne.
Numero di zone di disponibilità (AZ)	2 o più
Numero di sottoreti pubbliche	Non è necessario indicare alcun valore (0)

Campo	Valore
Numero di sottoreti private	Una per ogni zona di disponibilità
Gateway NAT	Non è necessario indicare alcun valore.
Endpoint VPC	Non è necessario indicare alcun valore.
Enable DNS hostnames (Abilita hostname DNS)	Sì
Abilita risoluzione DNS	Sì

Assicurati di testare la comunicazione VPC. Ad esempio, se il proxy dell'archivio delle chiavi esterne non si trova nel tuo Amazon VPC, crea un'istanza Amazon EC2 in Amazon VPC e verifica che Amazon VPC sia in grado di comunicare con il proxy dell'archivio delle chiavi esterne.

Connessione del VPC al gestore delle chiavi esterne

Connetti il VPC al data center che ospita il gestore delle chiavi esterne utilizzando una delle opzioni di connettività di rete supportate da Amazon VPC. Assicurati che l'istanza Amazon EC2 nel VPC (o il proxy dell'archivio delle chiavi esterne nel caso in cui si trovi nel VPC) sia in grado di comunicare con il data center e il gestore delle chiavi esterne.

Creazione di un gruppo di destinazione

Prima di creare il servizio endpoint VPC richiesto, crea i componenti necessari, vale a dire un Network Load Balancer e un gruppo di destinazione. Il Network Load Balancer distribuisce le richieste tra più destinazioni integre, ognuna delle quali può soddisfare la richiesta. In questo passaggio, crea un gruppo di destinazione con almeno due host per il proxy dell'archivio delle chiavi esterne e registra gli indirizzi IP con il gruppo di destinazione.

Segui le istruzioni nell'argomento Configurazione di un gruppo di destinazione utilizzando i seguenti valori obbligatori. Per gli altri campi, accetta i valori predefiniti e immetti i nomi come richiesto.

Campo	Valore
Target type (Tipo di destinazione)	Indirizzi IP
Protocollo	TCP
Porta	443
Tipo di indirizzo IP	IPv4
VPC	Scegli il VPC in cui creare il servizio endpoint VPC per l'archivio delle chiavi esterne.
Protocollo e percorso di controllo dell'integrità	Il protocollo e il percorso di controllo dell'integrità saranno diversi a seconda della configurazione del proxy dell'archivio delle chiavi esterne. Consulta la documentazione del gestore delle chiavi esterne o del proxy dell'archivio delle chiavi esterne. Per informazioni generali sulla configurazione dei controlli dell'integrità per i gruppi di destinazione, consulta Controlli dell'integrità per i gruppi di destinazione nella Guida per l'utente di Elastic Load Balancing per Network Load Balancer.
Rete	Altro indirizzo IP privato
Indirizzo IPv4	Gli indirizzi privati del proxy dell'archivio delle chiavi esterne
Porte	443

Creazione di un Network Load Balancer

Il Network Load Balancer distribuisce il traffico di rete, comprese le richieste provenienti da AWS KMS al proxy dell'archivio delle chiavi esterne, fino alle destinazioni configurate.

Segui le istruzioni nell'argomento Configurare un sistema di bilanciamento del carico e un ascoltatore per configurare e aggiungere un ascoltatore e creare un sistema di bilanciamento del carico

utilizzando i seguenti valori obbligatori. Per gli altri campi, accetta i valori predefiniti e immetti i nomi come richiesto.

Campo	Valore
Schema	Interno
Tipo di indirizzo IP	IPv4
Mappatura della rete	Scegli il VPC in cui creare il servizio endpoint VPC per l'archivio delle chiavi esterne.
Mapping	Scegli entrambe le zone di disponibilità (almeno due) configurate per le sottoreti VPC. Verifica i nomi delle sottoreti e l'indirizzo IP privato.
Protocollo	TCP
Porta	443
Azione predefinita: Inoltra a	Scegli il gruppo di destinazione per il Network Load Balancer.

Creazione di un servizio endpoint VPC

In genere, la creazione di un endpoint è destinata a un servizio. Tuttavia, quando crei un servizio endpoint VPC, il fornitore set e di conseguenza AWS KMS crea un endpoint per il tuo servizio. Per un archivio delle chiavi esterne, crea un servizio endpoint VPC con il Network Load Balancer creato nel passaggio precedente. Il servizio endpoint VPC deve trovarsi nello stesso Account AWS e nella stessa regione supportata dell'archivio delle chiavi esterne.

Più archivi delle chiavi esterne possono condividere un Amazon VPC, ma ogni archivio deve avere il proprio servizio endpoint VPC e il proprio nome DNS privato.

Segui le istruzioni nell'argomento Creazione di un servizio endpoint per creare il servizio endpoint VPC con i seguenti valori obbligatori. Per gli altri campi, accetta i valori predefiniti e immetti i nomi come richiesto.

Campo	Valore
Nuovo tipo di load balancer	Rete
Sistemi di bilanciamento del carico disponibili	Scegli il Network Load Balancer creato nella fase precedente. Se il nuovo sistema di bilanciamento del carico non compare nell'elenco, verifica che il suo stato sia attivo. Potrebbero essere necessari alcuni minuti prima che lo stato del sistema di bilanciamento del carico passi dal provisioning ad attivo.
Accettazione richiesta	Falso. Deseleziona la casella di controllo. L'accettazione non è obbligatoria. AWS KMS non può connettersi al servizio endpoint VPC senza un'accettazione manuale. Se è richiesta l'accettazione, i tentativi di creare l'archivio delle chiavi esterne falliscono con un'eccezione `XksProxyInvalidConfigurationException` .
Abilita nome DNS privato	Associa un nome DNS privato al servizio
Nome DNS privato	Inserisci un nome DNS privato che sia univoco nella Regione AWS. Il nome DNS privato deve essere un sottodominio di un dominio pubblico di livello superiore. Ad esempio, se il nome DNS privato è `myproxy-private.xks.example.com` , deve essere un sottodominio di un dominio pubblico come `xks.example.com` o `example.com` . Questo nome DNS privato deve corrispondere al nome comune del soggetto (CN) nel certificato TLS configurato sul proxy dell'archivio delle chiavi esterne. Ad esempio, se il nome DNS privato è `myproxy-private.xks.example.com` , il CN sul certificato TLS deve essere `myproxy-private.xks.example.com` o `*.xks.example.com` . Se il certificato e il nome DNS privato non corrispondono, i tentativi di connettere un archivio delle chiavi esterne al relativo proxy hanno esito negativo con un codice di errore di connessione di `XKS_PROXY_INVALID_TLS_CONFI`

Campo	Valore
	`GURATION` . Per informazioni dettagliate, vedi Errori di configurazione generale.
Tipi di indirizzo IP supportati	IPv4

Verifica del dominio del nome DNS privato

Quando crei il servizio endpoint VPC, lo stato di verifica del dominio è `pendingVerification`. Prima di creare un archivio delle chiavi esterne con il servizio endpoint VPC, tale stato deve essere `verified`. Per verificare di essere il proprietario del dominio associato al nome DNS privato, devi creare un record TXT in un server DNS pubblico.

Ad esempio, se il nome DNS privato per il servizio endpoint VPC è `myproxy-private.xks.example.com`, devi creare un record TXT in un dominio pubblico, ad esempio `xks.example.com` o `example.com`, a seconda di quale sia pubblico. AWS PrivateLink cerca il record TXT prima su `xks.example.com` e poi su `example.com`.

> **Tip**
>
> Dopo aver aggiunto un record TXT, potrebbero essere necessari alcuni minuti prima che il valore di Domain verification status (Stato di verifica del dominio) passi da `pendingVerification` a `verify`.

Per iniziare, individua lo stato di verifica del dominio utilizzando uno dei metodi seguenti. I valori validi sono `verified`, `pendingVerification` e `failed`.

- Nella console Amazon VPC, scegli Endpoint services (Servizi endpoint), quindi seleziona il servizio endpoint. Nel riquadro dei dettagli, vedi Domain verification status (Stato di verifica del dominio).
- Usa l'DescribeVpcEndpointServiceConfigurationsoperazione. Il valore `State` si trova nel campo `ServiceConfigurations.PrivateDnsNameConfiguration.State`.

Se lo stato della verifica non è `verified`, segui le istruzioni nell'argomento Verifica della proprietà del dominio per aggiungere un record TXT al server DNS del dominio e verificare che il record TXT sia pubblicato. Quindi controlla nuovamente lo stato della verifica.

Non è necessario creare un record A per il nome del dominio DNS privato. Quando AWS KMS crea un endpoint di interfaccia per il servizio endpoint VPC, AWS PrivateLink crea automaticamente una zona ospitata con il record A richiesto per il nome del dominio privato nel VPC AWS KMS. Per gli archivi delle chiavi esterne con connettività del servizio endpoint VPC, ciò accade quando colleghi l'archivio delle chiavi esterne al relativo proxy.

Autorizzazione di AWS KMS alla connessione al servizio endpoint VPC

Aggiungi AWS KMS all'elenco Allow principals (Consenti entità principali) per il servizio endpoint VPC. Ciò consente ad AWS KMS di creare endpoint di interfaccia per il servizio endpoint VPC. Se AWS KMS non rappresenta un principale consentito, i tentativi di creare un archivio delle chiavi esterne avranno esito negativo con un'eccezione `XksProxyVpcEndpointServiceNotFoundException`.

Segui le istruzioni nell'argomento Gestione delle autorizzazioni della Guida di AWS PrivateLink. Utilizza il seguente valore obbligatorio.

Campo	Valore
ARN	`cks.kms.<region>.amazonaws.com` Ad esempio, `cks.kms.us-east-1.amazonaws.com`

Successivo: Creazione di un archivio delle chiavi esterne

Gestione di un archivio delle chiavi esterne

Puoi gestire un archivio delle chiavi esterne utilizzando la console AWS KMS o l'API AWS KMS. Puoi creare un archivio delle chiavi esterne, visualizzarne e modificarne le proprietà, connetterlo e disconnetterlo dal proxy dell'archivio delle chiavi esterne ed eliminarlo.

Argomenti

- Creazione di un archivio delle chiavi esterne
- Modifica delle proprietà dell'archivio delle chiavi esterne
- Visualizzazione di un archivio delle chiavi esterne
- Monitoraggio di un archivio delle chiavi esterne
- Connessione e disconnessione di un archivio delle chiavi esterne

- Eliminazione di un archivio delle chiavi esterne

Creazione di un archivio delle chiavi esterne

Puoi creare uno o più archivi delle chiavi esterne in ogni Account AWS e regione. Ogni archivio delle chiavi esterne deve essere associato a un gestore delle chiavi esterne al di fuori di AWS e a un proxy dell'archivio delle chiavi esterne (proxy XKS) che media la comunicazione tra AWS KMS e il gestore. Per informazioni dettagliate, vedi Pianificazione di un archivio delle chiavi esterne. Prima di iniziare, verifica che sia necessario un archivio delle chiavi esterne. La maggior parte dei clienti può utilizzare le chiavi KMS supportate da un materiale della chiave di AWS KMS.

> **Tip**
>
> Alcuni gestori delle chiavi esterne offrono un metodo più semplice per creare un relativo archivio. Per ulteriori informazioni, consulta la documentazione del gestore delle chiavi esterne.

Prima di creare l'archivio delle chiavi esterne, devi assemblare i prerequisiti. Durante il processo di creazione, specifica le proprietà dell'archivio delle chiavi esterne. Indica in particolare se l'archivio delle chiavi esterne in AWS KMS utilizza un endpoint pubblico o un servizio endpoint VPC per connettersi al relativo proxy. Specifica inoltre i dettagli della connessione, tra cui l'endpoint URI del proxy e il percorso all'interno di tale endpoint proxy in cui AWS KMS invia le richieste API al proxy.

- Se utilizzi la connettività dell'endpoint pubblico, assicurati che AWS KMS sia in grado di comunicare con il proxy su Internet utilizzando una connessione HTTPS. Ciò include la configurazione dell'autenticazione TLS sul proxy dell'archivio delle chiavi esterne e la garanzia che tutti i firewall tra AWS KMS e il proxy consentano il traffico da e verso la porta 443 del proxy. Durante la creazione di un archivio delle chiavi esterne con connettività dell'endpoint pubblico, AWS KMS verifica la connessione inviando una richiesta di stato al proxy dell'archivio delle chiavi esterne. Questo test verifica che l'endpoint sia raggiungibile e che il proxy accetti una richiesta firmata con le credenziali di autenticazione proxy dell'archivio delle chiavi esterne. Se tale richiesta di test fallisce, l'operazione di creazione dell'archivio delle chiavi esterne ha esito negativo.
- Se utilizzi la connettività del servizio endpoint VPC, assicurati che il Network Load Balancer, il nome DNS privato e il servizio endpoint VPC siano operativi e configurati correttamente. Se il proxy dell'archivio delle chiavi esterne non si trova nel VPC, assicurati che il servizio endpoint VPC possa

comunicare con il proxy dell'archivio delle chiavi esterne. AWS KMS verifica la connettività del servizio endpoint VPC quando si collega l'archivio delle chiavi esterne al relativo proxy.

Ulteriori considerazioni:

- AWS KMSregistra i CloudWatch parametri e le dimensioni di Amazon, in particolare per gli archivi di chiavi esterni. I grafici di monitoraggio basati su alcuni di questi parametri vengono visualizzati nella console AWS KMS per ogni archivio delle chiavi esterne. Ti consigliamo di utilizzare questi parametri per creare allarmi in grado di monitorare tale archivio, in modo da poter rilevare eventuali segnali relativi a problemi operativi e prestazionali prima che si verifichino. Per istruzioni, consulta Monitoraggio di un archivio delle chiavi esterne.
- Gli archivi delle chiavi esterne sono soggetti a quote di risorse. L'uso delle chiavi KMS in un archivio delle chiavi esterne è soggetto a quote di richieste. Esamina queste quote prima di progettare l'implementazione dell'archivio delle chiavi esterne.

> **Note**
>
> Rivedi la tua configurazione per verificare eventuali dipendenze circolari che potrebbero impedirne il funzionamento.
> Ad esempio, se crei il proxy dell'archivio di chiavi esterno utilizzando risorse AWS, accertati che il funzionamento del proxy non richieda la disponibilità di una chiave KMS in un archivio di chiavi esterno a cui si accede tramite tale proxy.

Tutti i nuovi archivi delle chiavi esterne vengono creati in uno stato disconnesso. Prima di poter creare chiavi KMS nell'archivio delle chiavi esterne, devi collegarlo al relativo proxy. Per modificare le proprietà dell'archivio delle chiavi esterne, modifica le impostazioni.

Argomenti

- Assemblare i prerequisiti
- File di configurazione proxy
- Creazione di un archivio delle chiavi esterne (console)
- Creazione di un archivio delle chiavi esterne (API)

Assemblare i prerequisiti

Prima di creare un archivio delle chiavi esterne, devi assemblare i componenti necessari, tra cui il gestore delle chiavi esterne che verrà utilizzato per supportare l'archivio e il proxy dell'archivio delle chiavi esterne che traduce le richieste di AWS KMS in un formato comprensibile dal gestore.

I seguenti componenti sono necessari per tutti gli archivi delle chiavi esterne. Oltre a questi elementi, devi fornire anche i componenti necessari per supportare l'opzione di connettività proxy dell'archivio delle chiavi esterne scelta.

> **Tip**
>
> Il gestore delle chiavi esterne potrebbe includere alcuni di questi componenti oppure potrebbero essere configurati automaticamente. Per ulteriori informazioni, consulta la documentazione del gestore delle chiavi esterne.
> Se stai creando l'archivio delle chiavi esterne nella console AWS KMS, puoi scegliere di caricare un file di configurazione proxy basato su JSON che specifica il percorso URI proxy e le credenziali di autenticazione proxy. Alcuni proxy dell'archivio delle chiavi esterne generano automaticamente questo file. Per maggiori dettagli, consulta la documentazione relativa al proxy dell'archivio delle chiavi esterne o al gestore delle chiavi esterne.

Gestore delle chiavi esterne

Ogni archivio delle chiavi esterne richiede almeno un'istanza del gestore delle chiavi esterne. Può trattarsi di un modulo di sicurezza hardware (HSM) fisico o virtuale o di un software di gestione delle chiavi.

Sebbene sia possibile utilizzare un unico gestore delle chiavi, ti consigliamo di impiegare almeno due istanze correlate che condividono chiavi crittografiche per motivi di ridondanza. L'archivio delle chiavi esterne non richiede l'uso esclusivo del gestore delle chiavi esterne. Tuttavia, il gestore deve essere in grado di gestire la frequenza prevista delle richieste di crittografia e decrittografia provenienti dai servizi AWS che utilizzano le chiavi KMS nell'archivio delle chiavi esterne per proteggere le risorse. Il gestore delle chiavi esterne deve essere configurato per gestire fino a 1.800 richieste al secondo e per rispondere a ciascuna richiesta entro il timeout di 250 millisecondi. Ti consigliamo di posizionare il gestore delle chiavi esterne vicino a una Regione AWS, in modo che il tempo di andata e ritorno (RTT) della rete sia pari o inferiore a 35 millisecondi.

Se il proxy dell'archivio delle chiavi esterne lo consente, puoi modificare il gestore delle chiavi esterne associato al proxy, tuttavia il nuovo gestore deve essere un backup o uno snapshot con lo stesso materiale della chiave. Se la chiave esterna associata a una chiave KMS non è più disponibile per il proxy dell'archivio delle chiavi esterne, AWS KMS non è in grado di decrittografare il testo criptato con la chiave KMS.

Il gestore delle chiavi esterne deve essere accessibile al proxy dell'archivio delle chiavi esterne. Se la GetHealthStatusrisposta del proxy riporta che tutte le istanze esterne del gestore di chiavi lo sonoUnavailable, tutti i tentativi di creare un archivio di chiavi esterno falliscono con un. XksProxyUriUnreachableException

Proxy dell'archivio delle chiavi esterne

Devi specificare un proxy dell'archivio delle chiavi esterne (proxy XKS) conforme ai requisiti di progettazione della Specifica API relativa al proxy dell'archivio delle chiavi esterne di AWS KMS. Il proxy dell'archivio delle chiavi esterne può essere sviluppato o acquistato. In alternativa, puoi utilizzare il proxy fornito con il gestore delle chiavi esterne o integrato in esso. AWS KMS consiglia di configurare il proxy dell'archivio delle chiavi esterne in modo da gestire fino a 1.800 richieste al secondo e rispondere a ciascuna richiesta entro il timeout di 250 millisecondi. Ti consigliamo di posizionare il gestore delle chiavi esterne vicino a una Regione AWS, in modo che il tempo di andata e ritorno (RTT) della rete sia pari o inferiore a 35 millisecondi.

Puoi utilizzare un proxy dell'archivio delle chiavi esterne per più archivi, ma ogni archivio deve disporre di un endpoint URI univoco e di un percorso all'interno del proxy dell'archivio delle chiavi esterne per le relative richieste.

Se utilizzi la connettività del servizio endpoint VPC, puoi collocare il proxy dell'archivio delle chiavi esterne in Amazon VPC, ma ciò non è necessario. Il proxy può trovarsi anche al di fuori di AWS, ad esempio nel data center privato, e utilizzare il servizio endpoint VPC solo per comunicare con il proxy.

Credenziali di autenticazione proxy

Per creare un archivio delle chiavi esterne, devi specificare le credenziali di autenticazione proxy dell'archivio (XksProxyAuthenticationCredential).

Devi stabilire le credenziali di autenticazione (XksProxyAuthenticationCredential) per AWS KMS nel proxy dell'archivio delle chiavi esterne. AWS KMS esegue l'autenticazione al proxy firmando le relative richieste tramite il processo Signature Version 4 (SIGv4) con le credenziali di autenticazione proxy dell'archivio delle chiavi esterne. Puoi specificare le credenziali di autenticazione

durante la creazione dell'archivio delle chiavi esterne e modificarle in qualsiasi momento. Se il proxy effettua la rotazione delle credenziali, assicurati di aggiornare i valori delle credenziali per l'archivio delle chiavi esterne.

Le credenziali di autenticazione proxy sono composte da due parti. Per l'archivio delle chiavi esterne, devi fornire entrambe.

- ID chiave di accesso: identifica la chiave di accesso segreta. Puoi fornire questo ID come testo non crittografato.
- Chiave di accesso segreta: la parte segreta delle credenziali. AWS KMS crittografa la chiave di accesso segreta nelle credenziali prima di archiviarla.

Le credenziali SigV4 utilizzate da AWS KMS per firmare le richieste al proxy dell'archivio delle chiavi esterne non sono correlate alle credenziali SIGv4 associate ai principali AWS Identity and Access Management negli account AWS. Non riutilizzare le credenziali SigV4 IAM per il proxy dell'archivio delle chiavi esterne.

Connettività proxy

Per creare un archivio delle chiavi esterne, devi specificare l'opzione di connettività proxy (`XksProxyConnectivity`).

AWS KMS può comunicare con il proxy dell'archivio delle chiavi esterne utilizzando un endpoint pubblico o un servizio endpoint Amazon Virtual Private Cloud (Amazon VPC). Sebbene un endpoint pubblico sia più semplice da configurare e gestire, potrebbe non soddisfare i requisiti di sicurezza per ogni installazione. Se scegli l'opzione di connettività del servizio endpoint Amazon VPC, devi creare e gestire i componenti richiesti, tra cui un Amazon VPC con almeno due sottoreti in due diverse zone di disponibilità, un servizio endpoint VPC con un Network Load Balancer e un gruppo di destinazione e un nome DNS privato per il servizio endpoint VPC.

Puoi modificare l'opzione di connettività proxy dell'archivio delle chiavi esterne. Tuttavia, devi assicurarti che il materiale della chiave associato alle chiavi KMS sia sempre disponibile nell'archivio. In caso contrario, AWS KMS non è in grado di decrittografare il testo criptato crittografato con tali chiavi KMS.

Per informazioni relative all'opzione di connettività proxy migliore per l'archivio delle chiavi esterne, consulta Scelta di un'opzione di connettività proxy. Per informazioni sulla creazione e sulla configurazione della connettività del servizio endpoint VPC, consulta Configurazione della connettività del servizio endpoint VPC.

Endpoint dell'URI proxy

Per creare un archivio delle chiavi esterne, devi specificare l'endpoint (`XksProxyUriEndpoint`) utilizzato da AWS KMS per inviare richieste al proxy dell'archivio delle chiavi esterne.

Il protocollo deve essere HTTPS. AWS KMS comunica sulla porta 443. Non specificare la porta nel valore dell'endpoint URI proxy.

- Connettività dell'endpoint pubblico: specifica l'endpoint disponibile per il proxy dell'archivio delle chiavi esterne. Tale endpoint deve essere raggiungibile prima di creare l'archivio delle chiavi esterne.
- Connettività del servizio endpoint VPC: specifica `https://` seguito dal nome DNS privato del servizio endpoint VPC.

Il certificato del server TLS configurato sul proxy dell'archivio delle chiavi esterne deve corrispondere al nome di dominio nell'endpoint URI proxy ed essere emesso da un'autorità di certificazione supportata per gli archivi delle chiavi esterne. Per un elenco, consulta Autorità di certificazione attendibili. L'autorità di certificazione richiederà una prova della proprietà del dominio prima di emettere il certificato TLS.

Il nome comune del soggetto (CN) sul certificato TLS deve corrispondere al nome DNS privato. Ad esempio, se il nome DNS privato è `myproxy-private.xks.example.com`, il CN sul certificato TLS deve essere `myproxy-private.xks.example.com` o `*.xks.example.com`.

Puoi modificare l'endpoint dell'URI proxy, tuttavia devi assicurarti che il proxy dell'archivio delle chiavi esterne abbia accesso al materiale della chiave associato alle chiavi KMS nell'archivio. In caso contrario, AWS KMS non è in grado di decrittografare il testo criptato crittografato con tali chiavi KMS.

Requisiti di unicità

- Il valore combinato di endpoint dell'URI proxy (`XksProxyUriEndpoint`) e percorso URI proxy (`XksProxyUriPath`) deve essere univoco nel tuo Account AWS e nella regione.
- Gli archivi delle chiavi esterne con connettività dell'endpoint pubblico possono condividere lo stesso endpoint URI proxy, a condizione che abbiano valori diversi per il percorso URI proxy.
- Un archivio delle chiavi esterne con connettività dell'endpoint pubblico non può utilizzare lo stesso valore dell'endpoint URI proxy di qualsiasi dell'endpoint pubblico con connettività del servizio endpoint VPC nella stessa Regione AWS, anche se gli archivi delle chiavi di trovano in diversi Account AWS.

- Ogni archivio delle chiavi esterne con connettività all'endpoint VPC deve avere il proprio nome DNS privato. L'endpoint URI proxy (nome DNS privato) deve essere univoco nella regione e nell'Account AWS.

Percorso URI proxy

Per creare un archivio delle chiavi esterne, devi specificare il percorso di base nel proxy dell'archivio verso le API proxy necessarie. Il valore deve iniziare con `/` e terminare con /kms/xks/v1, dove `v1` rappresenta la versione dell'API AWS KMS per il proxy dell'archivio delle chiavi esterne. Questo percorso può includere un prefisso facoltativo tra gli elementi richiesti, ad esempio `/example-prefix/kms/xks/v1`. Per trovare questo valore, consulta la documentazione del proxy dell'archivio delle chiavi esterne.

AWS KMS invia richieste proxy all'indirizzo specificato dalla concatenazione dell'endpoint URI proxy e del percorso URI proxy. Ad esempio, se l'endpoint dell'URI proxy è `https://myproxy.xks.example.com` e il percorso URI proxy è `/kms/xks/v1`, AWS KMS invia le relative richieste API proxy a `https://myproxy.xks.example.com/kms/xks/v1`.

Puoi modificare il percorso URI proxy, tuttavia devi assicurarti che il proxy dell'archivio delle chiavi esterne abbia accesso al materiale della chiave associato alle chiavi KMS nell'archivio. In caso contrario, AWS KMS non è in grado di decrittografare il testo criptato crittografato con tali chiavi KMS.

Requisiti di unicità

- Il valore combinato di endpoint dell'URI proxy (`XksProxyUriEndpoint`) e percorso URI proxy (`XksProxyUriPath`) deve essere univoco nel tuo Account AWS e nella regione.

Servizio endpoint VPC

Specifica il nome del servizio endpoint Amazon VPC utilizzato per comunicare con il proxy dell'archivio delle chiavi esterne. Questo componente è richiesto solo per gli archivi delle chiavi esterne che utilizzano la connettività del servizio endpoint VPC. Per informazioni sull'impostazione e sulla configurazione del servizio endpoint VPC per un archivio delle chiavi esterne, consulta Configurazione della connettività del servizio endpoint VPC.

Il servizio endpoint VPC deve avere le seguenti proprietà:

- Il servizio endpoint VPC deve trovarsi nello stesso Account AWS e nella stessa regione dell'archivio delle chiavi esterne.

- Deve avere un Network Load Balancer (NLB) connesso ad almeno due sottoreti, ognuna in una zona di disponibilità diversa.
- L'elenco dei principali consentiti per il servizio endpoint VPC deve includere il principale del servizio AWS KMS per la regione `cks.kms.<region>.amazonaws.com`, ad esempio `cks.kms.us-east-1.amazonaws.com`.
- Non deve richiedere l'accettazione delle richieste di connessione.
- Deve avere un nome DNS privato all'interno di un dominio pubblico di livello superiore. Ad esempio, potresti avere un nome DNS privato myproxy-private.xks.example.com nel dominio `xks.example.com` pubblico.

  Il nome DNS privato per un archivio delle chiavi esterne con connettività del servizio endpoint VPC deve essere univoco nella Regione AWS.
- Lo stato di verifica del dominio per il dominio del nome DNS privato deve essere `verified`.
- Il certificato del server TLS configurato sul proxy dell'archivio delle chiavi esterne deve indicare il nome host DNS privato in cui l'endpoint è raggiungibile.

Requisiti di unicità

- Gli archivi delle chiavi esterne con connettività all'endpoint VPC possono condividere un `Amazon VPC`, ma ogni archivio deve avere il proprio servizio endpoint VPC e il proprio nome DNS privato.

File di configurazione proxy

Un file di configurazione proxy è un file facoltativo basato su JSON che contiene valori per le proprietà del percorso URI proxy e delle credenziali di autenticazione proxy dell'archivio delle chiavi esterne. Quando crei o modifichi un archivio delle chiavi esterne nella console AWS KMS, puoi caricare un file di configurazione proxy per fornire i valori di configurazione dell'archivio. L'utilizzo di questo file consente di evitare errori correlati alle operazioni di digitazione e di copia e incolla, garantendo che i valori nell'archivio delle chiavi esterne corrispondano ai valori del relativo proxy.

I file di configurazione proxy vengono generati dal proxy dell'archivio delle chiavi esterne. Per scoprire se il proxy dell'archivio delle chiavi esterne offre un file di configurazione proxy, consulta la relativa documentazione.

Di seguito è riportato un esempio di un file di configurazione proxy ben formato con valori fittizi.

```
{
```

```
  "XksProxyUriPath": "/example-prefix/kms/xks/v1",
  "XksProxyAuthenticationCredential": {
    "AccessKeyId": "ABCDE12345670EXAMPLE",
    "RawSecretAccessKey": "0000EXAMPLEFA5FT0mCc3DrGUe2sti527BitkQ0Zr9MO9+vE="
  }
}
```

Puoi caricare un file di configurazione proxy solo durante la creazione o la modifica di un archivio delle chiavi esterne nella console AWS KMS. Non è possibile utilizzarlo con le UpdateCustomKeyStoreoperazioni CreateCustomKeyStoreo, ma è possibile utilizzare i valori nel file di configurazione del proxy per garantire che i valori dei parametri siano corretti.

Creazione di un archivio delle chiavi esterne (console)

Prima di creare un archivio delle chiavi esterne, rivedi la sezione Pianificazione di un archivio delle chiavi esterne, scegli il tipo di connettività proxy e assicurati di aver creato e configurato tutti i componenti richiesti. Se hai bisogno di aiuto per trovare uno dei valori richiesti, consulta la documentazione del proxy dell'archivio delle chiavi esterne o del software di gestione delle chiavi.

> **Note**
>
> Quando crei un archivio delle chiavi esterne nella AWS Management Console, puoi caricare un file di configurazione proxy basato su JSON con i valori per il percorso URI proxy e le credenziali di autenticazione proxy. Alcuni proxy generano automaticamente questo file, ma non è obbligatorio.

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel pannello di navigazione, scegli Custom key stores (Archivi delle chiavi personalizzate), External key stores (Archivi delle chiavi esterne).
4. Scegli Create external key store (Crea archivio delle chiavi esterne).
5. Immetti un nome descrittivo per l'archivio delle chiavi esterne. Il nome deve essere univoco tra tutti gli archivi delle chiavi esterne nel tuo account.

> **Important**
>
> Non includere informazioni riservate o sensibili in questo campo. Questo campo può essere visualizzato in testo semplice nei CloudTrail log e in altri output.

6. Scegli il tipo di connettività proxy.

   La scelta della connettività proxy determina i componenti necessari per il proxy dell'archivio delle chiavi esterne. Per assistenza durante la scelta, consulta Scelta di un'opzione di connettività proxy.

7. Scegli o inserisci il nome del servizio endpoint VPC per questo archivio delle chiavi esterne. Questo passaggio viene visualizzato solo quando il tipo di connettività proxy è servizio endpoint VPC.

   Il servizio endpoint VPC e i relativi VPC devono soddisfare i requisiti per un archivio delle chiavi esterne. Per informazioni dettagliate, vedi the section called “Assemblare i prerequisiti”.

8. Inserisci l'endpoint URI proxy. Il protocollo deve essere HTTPS. AWS KMS comunica sulla porta 443. Non specificare la porta nel valore dell'endpoint URI proxy.

   Se AWS KMS riconosce il servizio endpoint VPC specificato nel passaggio precedente, completa automaticamente questo campo.

   Per la connettività dell'endpoint pubblico, inserisci un URI endpoint disponibile pubblicamente. Per la connettività dell'endpoint VPC, inserisci `https://` seguito dal nome DNS privato del servizio endpoint VPC.

9. Per inserire i valori relativi al prefisso del percorso URI proxy e le credenziali di autenticazione proxy, carica un file di configurazione proxy o inserisci i valori manualmente.

   - Se disponi di un file di configurazione proxy facoltativo che contiene i valori del percorso URI proxy e delle credenziali di autenticazione proxy, scegli Upload configuration file (Carica file di configurazione). Segui le istruzioni per caricare il file.

     Quando il file viene caricato, la console visualizza i valori del file in campi modificabili. Puoi modificare i valori in questo momento o modificarli dopo la creazione dell'archivio delle chiavi esterne.

     Per visualizzare il valore della chiave di accesso segreta, scegli Show secret access key (Mostra chiave di accesso segreta).

- Se non hai a disposizione un file di configurazione proxy, puoi inserire manualmente i valori del percorso URI proxy e delle credenziali di autenticazione proxy.

  a. Se non disponi di un file di configurazione proxy, puoi inserire l'URI proxy manualmente. La console fornisce il valore /kms/xks/v1 richiesto.

     Se il percorso URI proxy comprende un prefisso facoltativo, ad esempio `example-prefix` in `/example-prefix/kms/xks/v1`, inseriscilo nel campo Proxy URI path prefix (Prefisso del percorso URI proxy). In caso contrario, lascia vuoto il campo.

  b. Se non disponi di un file di configurazione proxy, puoi inserire le credenziali di autenticazione proxy manualmente. Sono necessari sia l'ID chiave di accesso che la chiave di accesso segreta.

     - In Proxy credential: Access key ID (Credenziali proxy: ID chiave di accesso), inserisci l'ID chiave di accesso delle credenziali di autenticazione proxy. L'ID della chiave di accesso identifica la chiave di accesso segreta.
     - In Proxy credential: Secret access key (Credenziali proxy: chiave di accesso segreta), inserisci la chiave di accesso segreta delle credenziali di autenticazione proxy.

     Per visualizzare il valore della chiave di accesso segreta, scegli Show secret access key (Mostra chiave di accesso segreta).

     Questa procedura non imposta o modifica le credenziali di autenticazione stabilite sul proxy dell'archivio delle chiavi esterne, ma associa semplicemente tali valori all'archivio. Per informazioni sull'impostazione, la modifica e la rotazione delle credenziali di autenticazione proxy, consulta la documentazione del proxy dell'archivio delle chiavi esterne o del software di gestione delle chiavi.

     Se le credenziali di autenticazione proxy cambiano, modifica l'impostazione delle credenziali per l'archivio delle chiavi esterne.

10. Scegli Create external key store (Crea archivio delle chiavi esterne).

Quando la procedura ha esito positivo, il nuovo archivio delle chiavi esterne viene visualizzato nell'elenco degli archivi delle chiavi esterne dell'account e della regione. Se ha esito negativo, viene visualizzato un messaggio di errore che descrive il problema e fornisce istruzioni su come risolverlo. Per ulteriori informazioni, consulta CreateKey errori per la chiave esterna.

Successivo: i nuovi archivi delle chiavi esterne non sono connessi automaticamente. Prima di poter creare le AWS KMS keys nell'archivio delle chiavi esterne, devi connettere l'archivio delle chiavi esterne al relativo proxy.

Creazione di un archivio delle chiavi esterne (API)

È possibile utilizzare l'CreateCustomKeyStoreoperazione per creare un nuovo archivio di chiavi esterno. Per assistenza nell'individuazione dei valori per i parametri richiesti, consulta la documentazione del proxy dell'archivio delle chiavi esterne o del software di gestione delle chiavi.

> **Tip**
>
> Non puoi caricare un file di configurazione proxy quando utilizzi l'operazione `CreateCustomKeyStore`. Tuttavia, puoi utilizzare i valori presenti nel file di configurazione proxy per assicurarti che i valori dei parametri siano corretti.

Per creare un archivio delle chiavi esterne, l'operazione `CreateCustomKeyStore` richiede i valori di parametro seguenti.

- `CustomKeyStoreName`: un nome descrittivo per l'archivio delle chiavi esterne univoco nell'account.

  > **Important**
  >
  > Non includere informazioni riservate o sensibili in questo campo. Questo campo può essere visualizzato in testo semplice nei CloudTrail log e in altri output.

- `CustomKeyStoreType`: specifica `EXTERNAL_KEY_STORE`.
- `XksProxyConnectivity`: specifica `PUBLIC_ENDPOINT` o `VPC_ENDPOINT_SERVICE`.
- `XksProxyAuthenticationCredential`: specifica sia l'ID chiave di accesso che la chiave di accesso segreta.
- `XksProxyUriEndpoint`: l'endpoint utilizzato da AWS KMS per comunicare con il proxy dell'archivio delle chiavi esterne.
- `XksProxyUriPath`: il percorso all'interno del proxy verso le API proxy.
- `XksProxyVpcEndpointServiceName`: obbligatorio solo quando il valore di `XksProxyConnectivity` è `VPC_ENDPOINT_SERVICE`.

> **Note**
>
> Se utilizzi AWS CLI versione 1.0, esegui il comando seguente prima di specificare un parametro con un valore HTTP o HTTPS, ad esempio il parametro `XksProxyUriEndpoint`.
>
> ```
> aws configure set cli_follow_urlparam false
> ```
>
> In caso contrario, AWS CLI versione 1.0 sostituisce il valore del parametro con il contenuto trovato in tale indirizzo URI, causando il seguente errore:
>
> ```
> Error parsing parameter '--xks-proxy-uri-endpoint': Unable to retrieve
> https:// : received non 200 status code of 404
> ```

Gli esempi seguenti utilizzano valori fittizi. Prima di eseguire il comando, sostituiscili con valori validi per l'archivio delle chiavi esterne.

Crea un archivio delle chiavi esterne con connettività dell'endpoint pubblico.

```
$ aws kms create-custom-key-store
        --custom-key-store-name ExampleExternalKeyStorePublic \
        --custom-key-store-type EXTERNAL_KEY_STORE \
        --xks-proxy-connectivity PUBLIC_ENDPOINT \
        --xks-proxy-uri-endpoint https://myproxy.xks.example.com \
        --xks-proxy-uri-path /kms/xks/v1 \
        --xks-proxy-authentication-credential
 AccessKeyId=<value>,RawSecretAccessKey=<value>
```

Crea un archivio delle chiavi esterne con connettività del servizio endpoint VPC.

```
$ aws kms create-custom-key-store
        --custom-key-store-name ExampleExternalKeyStoreVPC \
        --custom-key-store-type EXTERNAL_KEY_STORE \
        --xks-proxy-connectivity VPC_ENDPOINT_SERVICE \
        --xks-proxy-vpc-endpoint-service-name com.amazonaws.vpce.us-east-1.vpce-svc-
example \
        --xks-proxy-uri-endpoint https://myproxy-private.xks.example.com \
        --xks-proxy-uri-path /kms/xks/v1 \
        --xks-proxy-authentication-credential
 AccessKeyId=<value>,RawSecretAccessKey=<value>
```

Se l'operazione riesce, `CreateCustomKeyStore` restituisce l'ID store chiavi personalizzate, come illustrato nel seguente esempio di risposta.

```
{
    "CustomKeyStoreId": cks-1234567890abcdef0
}
```

Se l'operazione ha esito negativo, correggi l'errore indicato dall'eccezione e riprova. Per ulteriori informazioni, consulta Risoluzione dei problemi relativi all'archivio delle chiavi esterne.

Successivo: Per utilizzare l'archivio delle chiavi esterne, connettilo al relativo proxy dell'archivio delle chiavi esterne.

Modifica delle proprietà dell'archivio delle chiavi esterne

Puoi modificare le proprietà selezionate di un archivio delle chiavi esterne esistente.

Quando l'archivio delle chiavi esterne è connesso o disconnesso, puoi modificare solo alcune proprietà. Per modificare le altre proprietà, disconnetti l'archivio delle chiavi esterne dal relativo proxy. Lo stato di connessione dell'archivio delle chiavi esterne deve essere `DISCONNECTED`. Quando un archivio delle chiavi esterne è disconnesso, puoi gestire l'archivio e le relative chiavi KMS, ma non puoi creare o utilizzare le chiavi KMS nell'archivio delle chiavi esterne. Per trovare lo stato di connessione del tuo archivio chiavi esterno, usa l'DescribeCustomKeyStoresoperazione o consulta la sezione Configurazione generale nella pagina dei dettagli dell'archivio chiavi esterno.

Prima di aggiornare le proprietà dell'archivio di chiavi esterno, AWS KMS invia una GetHealthStatusrichiesta al proxy dell'archivio chiavi esterno utilizzando i nuovi valori. Se la richiesta ha esito positivo, indica che è possibile connettersi e autenticarsi a un proxy dell'archivio delle chiavi esterne con i valori delle proprietà aggiornati. Se la richiesta non riesce, l'operazione di modifica ha esito negativo con un'eccezione che identifica l'errore.

Al termine dell'operazione di modifica, i valori aggiornati delle proprietà per l'archivio delle chiavi esterne vengono visualizzati nella console AWS KMS e nella risposta `DescribeCustomKeyStores`. Tuttavia, possono essere necessari fino a cinque minuti affinché le modifiche diventino effettive.

Se modifichi l'archivio delle chiavi esterne nella console AWS KMS, hai la possibilità di caricare un file di configurazione proxy basato su JSON che specifica il percorso URI proxy e le credenziali di autenticazione proxy. Alcuni proxy dell'archivio delle chiavi esterne generano automaticamente

questo file. Per maggiori dettagli, consulta la documentazione relativa al proxy dell'archivio delle chiavi esterne o al gestore delle chiavi esterne.

> **Warning**
>
> I valori delle proprietà aggiornati devono connettere l'archivio delle chiavi esterne a un proxy per lo stesso gestore delle chiavi esterne dei valori precedenti o per un backup o uno snapshot del gestore con le stesse chiavi crittografiche. Se l'archivio delle chiavi esterne perde definitivamente l'accesso alle chiavi esterne associate alle relative chiavi KMS, il testo criptato crittografato con tali chiavi esterne è irrecuperabile. In particolare, la modifica della connettività proxy di un archivio delle chiavi esterne può impedire ad AWS KMS di accedere alle chiavi esterne.

> **Tip**
>
> Alcuni gestori delle chiavi esterne offrono un metodo più semplice per modificare le proprietà dell'archivio delle chiavi esterne. Per ulteriori informazioni, consulta la documentazione del gestore delle chiavi esterne.

Puoi modificare le seguenti proprietà di un archivio delle chiavi esterne.

Proprietà modificabili dell'archivio delle chiavi esterne	Qualsiasi stato di connessione	Richiede lo stato Disconnesso
Il nome dello store delle chiavi personalizzate Un nome descrittivo per l'archivio delle chiavi personalizzate. **Important** Non includere informazioni riservate o sensibili in questo campo. Questo campo può essere visualizzato in testo semplice nei CloudTrail log e in altri output.	✓	

Proprietà modificabili dell'archivio delle chiavi esterne	Qualsiasi stato di connessione	Richiede lo stato Disconnesso
Credenziali di autenticazione proxy () XksProxyAuthenticationCredential Devi specificare sia l'ID chiave di accesso che la chiave di accesso segreta, anche se modifichi un solo elemento.	✓	
Percorso URI del proxy () XksProxyUriPath	✓	
Connettività proxy (XksProxyConnectivity) Devi inoltre aggiornare l'endpoint URI proxy. Se stai passando alla connettività del servizio endpoint VPC, devi specificare un nome del servizio endpoint VPC del proxy.		✓
Endpoint URI proxy () XksProxyUriEndpoint Se modifichi l'URI endpoint proxy, potrebbe anche essere necessario modificare il certificato TLS associato.		✓
Nome del servizio endpoint VPC proxy () XksProxyVpcEndpointServiceName Questo campo è obbligatorio per la connettività del servizio endpoint VPC		✓

Argomenti

- Modifica di un archivio delle chiavi esterne (console)
- Modifica di un archivio delle chiavi esterne (API)

Modifica di un archivio delle chiavi esterne (console)

Quando modifichi un archivio delle chiavi esterne, puoi modificare qualsiasi valore configurabile. Alcune modifiche richiedono la disconnessione dell'archivio delle chiavi esterne dal relativo proxy.

Se stai modificando il percorso URI proxy o le credenziali di autenticazione proxy, puoi inserire i nuovi valori o caricare un file di configurazione proxy dell'archivio delle chiavi esterne che includa i nuovi valori.

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel pannello di navigazione, scegli Custom key stores (Archivi delle chiavi personalizzate), External key stores (Archivi delle chiavi esterne).
4. Scegli la riga relativa all'archivio delle chiavi esterne che vuoi modificare.
5. Se necessario, disconnetti l'archivio delle chiavi esterne dal relativo proxy. Dal menu Key store actions (Operazioni per l'archivio delle chiavi), scegli Disconnect (Disconnetti).
6. Dal menu Key store actions (Operazioni per l'archivio delle chiavi), scegli Edit (Modifica).
7. Modifica una o più proprietà configurabili dell'archivio delle chiavi esterne. Puoi inoltre caricare un file di configurazione proxy dell'archivio delle chiavi esterne con i valori per il percorso URI proxy e le credenziali di autenticazione proxy. Puoi utilizzare tale file di configurazione proxy anche se alcuni valori specificati nel file non sono stati modificati.
8. Scegli Update external key store (Aggiornamento dell'archivio delle chiavi esterne).
9. Esamina l'avviso e, se decidi di continuare, confermalo, quindi scegli Update external key store (Aggiornamento dell'archivio delle chiavi esterne).

   Se la procedura ha esito positivo, un messaggio descrive le proprietà modificate. Se ha esito negativo, viene visualizzato un messaggio di errore che descrive il problema e fornisce istruzioni su come risolverlo.
10. Se necessario, connetti nuovamente l'archivio delle chiavi esterne. Dal menu Key store actions (Operazioni per l'archivio delle chiavi), scegli Connect (Connetti).

    Puoi lasciarlo disconnesso, ma in questo stato, non puoi creare o utilizzare le chiavi KMS nell'archivio delle chiavi esterne per operazioni di crittografia.

Modifica di un archivio delle chiavi esterne (API)

Per modificare le proprietà di un archivio di chiavi esterno, utilizzare l'UpdateCustomKeyStoreoperazione. Puoi modificare più proprietà di un archivio delle chiavi esterne con la stessa operazione. Se l'operazione ha esito positivo, AWS KMS restituisce una risposta HTTP 200 e un oggetto JSON senza proprietà.

Utilizza il parametro `CustomKeyStoreId` per identificare l'archivio delle chiavi esterne. Utilizza gli altri parametri per modificare le proprietà. Non puoi utilizzare un file di configurazione proxy con l'operazione `UpdateCustomKeyStore`, poiché tale file è supportato solo dalla console AWS KMS. Tuttavia, puoi utilizzare il file di configurazione proxy per determinare i valori dei parametri corretti per il proxy dell'archivio delle chiavi esterne.

Gli esempi in questa sezione utilizzano AWS Command Line Interface (AWS CLI), ma puoi usare anche qualsiasi linguaggio di programmazione supportato.

Prima di iniziare, se necessario, disconnetti l'archivio delle chiavi esterne dal relativo proxy. Dopo l'aggiornamento, se necessario, connetti nuovamente l'archivio al proxy dell'archivio delle chiavi esterne. Puoi lasciare l'archivio delle chiavi esterne disconnesso, ma devi connetterlo per poter creare nuove chiavi KMS o utilizzare le chiavi KMS esistenti nell'archivio delle chiavi per operazioni di crittografia.

> **Note**
>
> Se utilizzi AWS CLI versione 1.0, esegui il comando seguente prima di specificare un parametro con un valore HTTP o HTTPS, ad esempio il parametro `XksProxyUriEndpoint`.
>
> ```
> aws configure set cli_follow_urlparam false
> ```
>
> In caso contrario, AWS CLI versione 1.0 sostituisce il valore del parametro con il contenuto trovato in tale indirizzo URI, causando il seguente errore:
>
> ```
> Error parsing parameter '--xks-proxy-uri-endpoint': Unable to retrieve
> https:// : received non 200 status code of 404
> ```

Modifica del nome dell'archivio delle chiavi esterne

Il primo esempio utilizza l'UpdateCustomKeyStoreoperazione per modificare il nome descrittivo dell'archivio chiavi esterno in`XksKeyStore`. Il comando utilizza il parametro `CustomKeyStoreId` per identificare lo store delle chiavi personalizzate e `CustomKeyStoreName` per specificarne il nuovo nome. Sostituisci tutti i valori di esempio con i valori effettivi per l'archivio delle chiavi esterne.

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 --new-
custom-key-store-name XksKeyStore
```

Modifica delle credenziali di autenticazione proxy

L'esempio seguente aggiorna le credenziali di autenticazione proxy utilizzate daAWS KMS per l'autenticazione nel proxy dell'archivio delle chiavi esterne. Puoi utilizzare un comando simile a questo per aggiornare le credenziali se vengono ruotate sul proxy.

Aggiorna prima le credenziali nel proxy dell'archivio delle chiavi esterne. Quindi, utilizza questa funzione per segnalare la modifica ad AWS KMS. Il proxy supporterà per un breve periodo tempo sia le credenziali vecchie che quelle nuove, per consentirti di aggiornarle in AWS KMS.

Nelle credenziali devi specificare sia l'ID chiave di accesso che la chiave di accesso segreta, anche se viene modificato un solo valore.

I primi due comandi impostano le variabili per contenere i valori delle credenziali. Le operazioni `UpdateCustomKeyStore` utilizzano il parametro `CustomKeyStoreId` per identificare l'archivio delle chiavi esterne. Utilizza il parametro `XksProxyAuthenticationCredential` con i relativi campi `AccessKeyId` e `RawSecretAccessKey` per specificare le nuove credenziali. Sostituisci tutti i valori di esempio con i valori effettivi per l'archivio delle chiavi esterne.

```
$ accessKeyID=access key id
$ secretAccessKey=secret access key

$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 \
       --xks-proxy-authentication-credential \
           AccessKeyId=$accessKeyId,RawSecretAccessKey=$secretAccessKey
```

Modifica del percorso URI proxy

L'esempio seguente aggiorna il percorso URI proxy (`XksProxyUriPath`). La combinazione di endpoint URI proxy e percorso URI proxy deve essere univoca per Account AWS e regione. Sostituisci tutti i valori di esempio con i valori effettivi per l'archivio delle chiavi esterne.

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 \
            --xks-proxy-uri-path /kms/xks/v1
```

Passaggio alla connettività del servizio endpoint VPC

L'esempio seguente utilizza l'UpdateCustomKeyStoreoperazione per modificare il tipo di connettività proxy dell'archivio chiavi esterno in`VPC_ENDPOINT_SERVICE`. Per apportare questa modifica, devi specificare i valori richiesti per la connettività del servizio endpoint VPC, incluso il nome del servizio endpoint VPC (`XksProxyVpcEndpointServiceName`) e un valore dell'endpoint URI proxy (`XksProxyUriEndpoint`) che includa il nome DNS privato per il servizio endpoint VPC. Sostituisci tutti i valori di esempio con i valori effettivi per l'archivio delle chiavi esterne.

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 \
            --xks-proxy-connectivity "VPC_ENDPOINT_SERVICE" \
            --xks-proxy-uri-endpoint https://myproxy-private.xks.example.com \
            --xks-proxy-vpc-endpoint-service-name com.amazonaws.vpce.us-east-1.vpce-
svc-example
```

Passaggio alla connettività dell'endpoint pubblico

L'esempio seguente modifica il tipo di connettività del proxy dell'archivio delle chiavi esterne in `PUBLIC_ENDPOINT`. Quando apporti questa modifica, devi aggiornare il valore dell'endpoint URI proxy (`XksProxyUriEndpoint`). Sostituisci tutti i valori di esempio con i valori effettivi per l'archivio delle chiavi esterne.

> **Note**
>
> La connettività dell'endpoint VPC offre una maggiore sicurezza rispetto alla connettività dell'endpoint pubblico. Prima di passare alla connettività dell'endpoint pubblico, prendi in considerazione altre opzioni, tra cui il posizionamento del proxy dell'archivio delle chiavi esterne on-premise e l'utilizzo del VPC solo per la comunicazione.

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 \
            --xks-proxy-connectivity "PUBLIC_ENDPOINT" \
            --xks-proxy-uri-endpoint https://myproxy.xks.example.com
```

Visualizzazione di un archivio delle chiavi esterne

È possibile visualizzare gli archivi di chiavi esterni in ogni account e regione utilizzando la AWS KMS console o utilizzando l'DescribeCustomKeyStoresoperazione.

Quando visualizzi un archivio delle chiavi esterne, hai accesso alle seguenti informazioni:

- Informazioni di base sull'archivio delle chiavi, tra cui nome descrittivo, ID, tipo di archivio e data di creazione.
- Informazioni di configurazione per il proxy dell'archivio delle chiavi esterne, tra cui tipo di connettività, endpoint URI proxy, percorso URI proxy e ID della chiave di accesso delle credenziali di autenticazione proxy correnti.
- Se il proxy dell'archivio delle chiavi esterne utilizza la connettività del servizio endpoint VPC, la console visualizza il nome del servizio endpoint VPC.
- Lo stato di connessione corrente.

> **Note**
>
> Il valore Disconnected (Disconnesso) dello stato di connessione indica che l'archivio delle chiavi esterne non è mai stato connesso oppure che è stato intenzionalmente disconnesso dal relativo proxy. Se tuttavia i tentativi di utilizzare una chiave KMS in un archivio delle chiavi esterne connesso non riescono, è possibile che vi sia un problema con l'archivio o con il cluster . Per assistenza, consulta Errori di connessione all'archivio delle chiavi esterne.

- Una sezione di monitoraggio con grafici delle CloudWatch metriche di Amazon progettati per aiutarti a rilevare e risolvere problemi con il tuo archivio di chiavi esterno. Per informazioni sull'interpretazione dei grafici, sul loro utilizzo nella pianificazione e risoluzione dei problemi e sulla creazione di CloudWatch allarmi in base alle metriche dei grafici, consulta. Monitoraggio di un archivio delle chiavi esterne

Consulta anche:

- Visualizzazione delle chiavi KMS in un archivio delle chiavi esterne
- Registrazione delle chiamate API AWS KMS con AWS CloudTrail

Argomenti

Proprietà dell'archivio delle chiavi esterne

Le seguenti proprietà di un archivio di chiavi esterno sono visibili nella console e nella AWS KMS risposta. DescribeCustomKeyStores

Proprietà dell'archivio delle chiavi personalizzate

I valori seguenti vengono visualizzati nella sezione General configuration (Configurazione generale) della pagina dei dettagli di ogni archivio delle chiavi personalizzate. Queste proprietà si applicano a tutti gli archivi delle chiavi personalizzate, inclusi gli archivi delle chiavi di AWS CloudHSM e gli archivi delle chiavi esterne.

ID dello store delle chiavi personalizzate

: Un ID univoco che AWS KMS assegna all'archivio delle chiavi personalizzate.

Il nome dello store delle chiavi personalizzate

: Nome descrittivo assegnato all'archivio delle chiavi personalizzate durante la sua creazione. Puoi modificare questo valore in qualsiasi momento.

Tipo di archivio delle chiavi personalizzate

: Il tipo di archivio delle chiavi personalizzate. I valori validi sono AWS CloudHSM (`AWS_CLOUDHSM`) o External key store (Archivio delle chiavi esterne) (`EXTERNAL_KEY_STORE`). Il tipo di archivio non può essere modificato dopo la creazione.

Data di creazione

: La data in cui è stato creato l'archivio delle chiavi personalizzate. Questa data viene visualizzata nell'ora locale per la Regione AWS.

Stato connessione

: Indica se l'archivio delle chiavi personalizzate è connesso al relativo archivio del materiale della chiave. Lo stato della connessione è `DISCONNECTED` solo se l'archivio delle chiavi personalizzate non è mai stato collegato al relativo archivio del materiale della chiave o se è stato disconnesso intenzionalmente. Per informazioni dettagliate, vedi the section called “Stato connessione”.

Proprietà di configurazione dell'archivio delle chiavi esterne

I seguenti valori vengono visualizzati nella sezione Configurazione proxy dell'archivio chiavi esterno della pagina di dettaglio per ogni archivio di chiavi esterno e nell'`XksProxyConfiguration`elemento della DescribeCustomKeyStoresrisposta. Per una descrizione dettagliata di ogni campo, inclusi i requisiti di unicità e le informazioni utili per determinare il valore corretto per ogni campo, consulta the section called “Assemblare i prerequisiti” nell'argomento Creazione di un archivio delle chiavi esterne.

Connettività proxy

Indica se l'archivio delle chiavi esterne utilizza la connettività dell'endpoint pubblico o la connettività del servizio endpoint VPC.

Endpoint dell'URI proxy

L'endpoint utilizzato da AWS KMS per connettersi al proxy dell'archivio delle chiavi esterne.

Percorso URI proxy

Il percorso dall'endpoint URI proxy a cui AWS KMS invia le richieste API del proxy.

Credenziali proxy: ID chiave di accesso

Parte delle credenziali di autenticazione proxy che stabilisci nel proxy dell'archivio delle chiavi esterne. L'ID della chiave di accesso identifica la chiave di accesso segreta nelle credenziali.

AWS KMS utilizza il processo di firma SigV4 e le credenziali di autenticazione proxy per firmare le richieste indirizzate al proxy dell'archivio delle chiavi esterne. Le credenziali della firma consentono al proxy di autenticare le richieste per tuo conto da AWS KMS.

Nome del servizio endpoint VPC

Il nome del servizio endpoint Amazon VPC che supporta l'archivio delle chiavi esterne. Questo valore viene visualizzato solo quando l'archivio delle chiavi esterne utilizza la connettività del servizio endpoint VPC. Puoi individuare il proxy dell'archivio delle chiavi esterne nel VPC oppure puoi utilizzare il servizio endpoint VPC per comunicare in modo sicuro con il proxy.

Visualizzazione di un archivio delle chiavi esterne (console)

Per visualizzare gli archivi delle chiavi esterne in determinati account e regioni, utilizza la procedura seguente.

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel pannello di navigazione, scegli Custom key stores (Archivi delle chiavi personalizzate), External key stores (Archivi delle chiavi esterne).
4. Per visualizzare le informazioni dettagliate su un archivio delle chiavi esterne, scegli il nome dell'archivio delle chiavi.

Visualizzazione di un archivio delle chiavi esterne (API)

Per visualizzare gli archivi di chiavi esterni, utilizza l'DescribeCustomKeyStoresoperazione. Per impostazione predefinita, questa operazione restituisce tutti gli store delle chiavi personalizzate presenti nell'account e nella regione. Puoi tuttavia utilizzare il parametro `CustomKeyStoreName` o `CustomKeyStoreId` (ma non entrambi) per limitare l'output a un determinato store delle chiavi personalizzate.

Per quanto riguarda gli archivi delle chiavi personalizzate, l'output include l'ID, il nome e il tipo dell'archivio delle chiavi personalizzate, oltre allo lo stato di connessione dell'archivio delle chiavi. Se lo stato della connessione è `FAILED`, l'output include un `ConnectionErrorCode` che descrive il motivo dell'errore. Per informazioni sull'interpretazione di `ConnectionErrorCode` per un archivio delle chiavi esterne, consulta Codici di errore di connessione per archivi delle chiavi esterne.

Per gli archivi delle chiavi esterne, l'output include anche l'elemento `XksProxyConfiguration`. Questo elemento comprende il tipo di connettività, l'endpoint URI proxy, il percorso URI proxy e l'ID della chiave di accesso delle credenziali di autenticazione proxy.

Gli esempi in questa sezione utilizzano AWS Command Line Interface (AWS CLI), ma puoi usare anche qualsiasi linguaggio di programmazione supportato.

Ad esempio, il comando seguente restituisce tutti gli store delle chiavi personalizzate presenti nell'account e nella regione. Per scorrere gli store delle chiavi personalizzate nell'output puoi utilizzare i parametri `Limit` e `Marker`.

```
$ aws kms describe-custom-key-stores
```

Il comando seguente utilizza il parametro `CustomKeyStoreName` per ottenere solo l'archivio delle chiavi esterne di esempio con il nome descrittivo `ExampleXksPublic`. Tale archivio delle chiavi

utilizza la connettività dell'endpoint pubblico ed è collegato al relativo proxy dell'archivio delle chiavi esterne.

```
$ aws kms describe-custom-key-stores --custom-key-store-name ExampleXksPublic
{
    "CustomKeyStores": [
    {
      "CustomKeyStoreId": "cks-1234567890abcdef0",
      "CustomKeyStoreName": "ExampleXksPublic",
      "ConnectionState": "CONNECTED",
      "CreationDate": "2022-12-14T20:17:36.419000+00:00",
      "CustomKeyStoreType": "EXTERNAL_KEY_STORE",
      "XksProxyConfiguration": {
        "AccessKeyId": "ABCDE12345670EXAMPLE",
        "Connectivity": "PUBLIC_ENDPOINT",
        "UriEndpoint": "https://xks.example.com:6443",
        "UriPath": "/example/prefix/kms/xks/v1"
      }
    }
  ]
}
```

Tramite il comando seguente si ottiene un archivio delle chiavi esterne di esempio con connettività del servizio endpoint VPC. In questo esempio, l'archivio delle chiavi esterne è connesso al relativo proxy.

```
$ aws kms describe-custom-key-stores --custom-key-store-name ExampleXksVpc
{
    "CustomKeyStores": [
    {
      "CustomKeyStoreId": "cks-9876543210fedcba9",
      "CustomKeyStoreName": "ExampleXksVpc",
      "ConnectionState": "CONNECTED",
      "CreationDate": "2022-12-13T18:34:10.675000+00:00",
      "CustomKeyStoreType": "EXTERNAL_KEY_STORE",
      "XksProxyConfiguration": {
        "AccessKeyId": "ABCDE98765432EXAMPLE",
        "Connectivity": "VPC_ENDPOINT_SERVICE",
        "UriEndpoint": "https://example-proxy-uri-endpoint-vpc",
        "UriPath": "/example/prefix/kms/xks/v1",
        "VpcEndpointServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-example"
      }
    }
```

```
  ]
}
```

Se `ConnectionState` è `Disconnected`, indica che un archivio delle chiavi esterne non è mai stato connesso oppure è stato intenzionalmente disconnesso dal relativo proxy. Se tuttavia i tentativi di utilizzare una chiave KMS in un archivio delle chiavi esterne connesso non riescono, è possibile che vi sia un problema con il proxy o altri componenti esterni.

Se il campo `ConnectionState` dell'archivio delle chiavi esterne è `FAILED`, la risposta `DescribeCustomKeyStores` include un elemento `ConnectionErrorCode` che descrive il motivo dell'errore.

Ad esempio, nell'output seguente, il valore `XKS_PROXY_TIMED_OUT` indica che AWS KMS può connettersi al proxy dell'archivio delle chiavi esterne, ma la connessione ha avuto esito negativo in quanto il proxy non ha risposto ad AWS KMS nel tempo assegnato. Se visualizzi ripetutamente questo codice di errore di connessione, informa il fornitore del proxy dell'archivio delle chiavi esterne. Per informazioni su questo e altri errori di connessione, consulta Risoluzione dei problemi relativi all'archivio delle chiavi esterne.

```
$ aws kms describe-custom-key-stores --custom-key-store-name ExampleXksVpc
{
    "CustomKeyStores": [
    {
      "CustomKeyStoreId": "cks-9876543210fedcba9",
      "CustomKeyStoreName": "ExampleXksVpc",
      "ConnectionState": "FAILED",
      "ConnectionErrorCode": "XKS_PROXY_TIMED_OUT",
      "CreationDate": "2022-12-13T18:34:10.675000+00:00",
      "CustomKeyStoreType": "EXTERNAL_KEY_STORE",
      "XksProxyConfiguration": {
        "AccessKeyId": "ABCDE98765432EXAMPLE",
        "Connectivity": "VPC_ENDPOINT_SERVICE",
        "UriEndpoint": "https://example-proxy-uri-endpoint-vpc",
        "UriPath": "/example/prefix/kms/xks/v1",
        "VpcEndpointServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-example"
      }
    }
  ]
}
```

Monitoraggio di un archivio delle chiavi esterne

AWS KMSraccoglie le metriche per ogni interazione con un archivio di chiavi esterno e le pubblica nel tuo account. CloudWatch Questi parametri vengono utilizzati per generare i grafici nella sezione di monitoraggio della pagina dei dettagli relativa a ogni archivio delle chiavi esterne. L'argomento seguente descrive in dettaglio come utilizzare i grafici per identificare e risolvere i problemi operativi e di configurazione che influiscono sull'archivio delle chiavi esterne. Ti consigliamo di utilizzare le CloudWatch metriche per impostare allarmi che ti avvisino quando l'archivio chiavi esterno non funziona come previsto. Per ulteriori informazioni, consulta Monitoraggio con Amazon CloudWatch.

Argomenti

- Visualizzazione dei grafici
- Interpretazione dei grafici
- Impostazione degli allarmi

Visualizzazione dei grafici

Puoi visualizzare i grafici a diversi livelli di dettaglio. Per impostazione predefinita, ogni grafico utilizza un intervallo di tempo di tre ore e un periodo di aggregazione di cinque minuti. Puoi regolare la visualizzazione del grafico all'interno della console, ma le modifiche verranno ripristinate alle impostazioni predefinite quando la pagina dei dettagli dell'archivio delle chiavi esterne viene chiusa o quando il browser viene aggiornato. Per assistenza sulla CloudWatch terminologia di Amazon, consulta Amazon CloudWatch concepts.

Visualizzazione dei dettagli di punti dati

I dati in ogni grafico vengono raccolti in base ai parametri di AWS KMS. Per visualizzare ulteriori informazioni su un punto dati specifico, posiziona il puntatore del mouse sul punto dati del grafico a linee. Verrà visualizzato un popup con ulteriori informazioni sul parametro da cui è stato derivato il grafico. Ogni elemento dell'elenco visualizza il valore della dimensione registrato in quel punto dati. Il popup visualizza un valore nullo (—) se non sono disponibili dati di parametro per il valore della dimensione in quel punto dati. Alcuni grafici registrano più dimensioni e valori per un singolo punto dati. Altri grafici, come il grafico di affidabilità, utilizzano i dati raccolti dal parametro per calcolare un valore univoco. Ogni elemento dell'elenco è associato a un colore diverso del grafico a linee.

Modifica dell'intervallo di tempo

Per modificare l'intervallo temporale, seleziona uno degli intervalli di tempo predefiniti nell'angolo in alto a destra della sezione di monitoraggio. Questi intervalli predefiniti vanno da 1 ora a 1 settimana

(1h [1 ora], 3h [3 ore], 12h [12 ore], 1d [1 giorno], 3d [3 giorni] oppure 1w [1 settimana]). In questo modo si regola l'intervallo di tempo per tutti i grafici. Se desideri visualizzare un grafico specifico in un intervallo di tempo diverso o se desideri impostare un intervallo di tempo personalizzato, ingrandisci il grafico o visualizzalo nella CloudWatch console Amazon.

Ingrandimento dei grafici

Puoi utilizzare la funzione di ingrandimento mini-mappa per concentrarti su sezioni di grafici a linee e porzioni impilate dei grafici senza passare tra la visualizzazione ingrandita e ridimensionata. Ad esempio, puoi utilizzare la funzione di ingrandimento mini-mappa per concentrarti su un picco di un grafico a linee, in modo da poter confrontare il picco con altri grafici nella sezione di monitoraggio dalla stessa sequenza temporale.

1. Seleziona e trascina l'area del grafico che desideri ingrandire, quindi rilasciala.
2. Per ripristinare lo zoom, seleziona l'icona Reset zoom, a forma di lente d'ingrandimento con un simbolo meno (-) all'interno.

Ingrandimento di un grafico

Per ingrandire un grafico, seleziona l'icona del menu nell'angolo in alto a destra di un singolo grafico e scegli Enlarge (Ingrandisci). Puoi anche selezionare l'icona di ingrandimento che appare accanto all'icona del menu quando passi il mouse su un grafico.

L'ingrandimento di un grafico consente di modificare ulteriormente la visualizzazione di un grafico specificando un periodo diverso, un intervallo di tempo personalizzato o un intervallo di aggiornamento. Queste modifiche verranno ripristinate alle impostazioni predefinite quando si chiude la vista ingrandita.

Modifica del periodo

1. Scegli il menu Period options (Opzioni periodo). Per impostazione predefinita, questo menu visualizza il valore 5 minuti.
2. Scegli un periodo; i periodi predefiniti vanno da 1 secondo a 30 giorni.

   Ad esempio, puoi scegliere la visualizzazione di un minuto, che può essere utile durante la risoluzione dei problemi. In alternativa, scegli la visualizzazione meno dettagliata di un'ora. Può essere utile quando si visualizza un intervallo di tempo più ampio (ad esempio 3 giorni) in modo da poter vedere le tendenze nel tempo. Per ulteriori informazioni, consulta Periodi nella Amazon CloudWatch User Guide.

Modifica dell'intervallo di tempo o del fuso orario

1. Seleziona uno degli intervalli di tempo predefiniti, che partono da 1 ora fino a 1 settimana: 1h (1 ora), 3h (3 ore), 12h (12 ore), 1d (1 giorno), 3d (3 giorni) oppure 1w (1 settimana). In alternativa, è possibile scegliere Personalizza per impostare il tuo intervallo di tempo.
2. Scegli Custom (Personalizzato)

    a. Intervallo di tempo: seleziona la scheda Absolute (Assoluto) nell'angolo in alto a sinistra della casella. Utilizza la selezione calendario o i campi di testo per specificare l'intervallo di tempo.

    b. Fuso orario: scegli il menu a discesa nell'angolo in alto a destra della casella. È possibile modificare il fuso orario in UTC o Fuso orario locale.
3. Dopo aver specificato un intervallo di tempo, scegli Applica.

Modifica la frequenza di aggiornamento dei dati nel grafico

1. Scegli il menu Refresh options (Aggiorna opzioni) nell'angolo in alto a destra.
2. Scegli un intervallo di aggiornamento: Off (Disattivato), 10 Seconds (10 secondi), 1 Minute (1 minuto), 2 Minutes (2 minuti), 5 Minutes (5 minuti) o 15 Minutes (15 minuti).

Visualizza i grafici nella console Amazon CloudWatch

I grafici nella sezione di monitoraggio derivano da metriche predefinite pubblicate su AmazonAWS KMS. CloudWatch Puoi aprirli all'interno della CloudWatch console e salvarli nelle dashboard. CloudWatch Se disponi di più archivi di chiavi esterni, puoi aprire i rispettivi grafici CloudWatch e salvarli in un'unica dashboard per confrontarne lo stato e l'utilizzo.

Aggiungi alla dashboard CloudWatch

Seleziona Aggiungi alla dashboard nell'angolo in alto a destra per aggiungere tutti i grafici a una CloudWatch dashboard di Amazon. Puoi selezionare un pannello di controllo esistente o crearne uno nuovo. Per informazioni sull'utilizzo di questa dashboard per creare visualizzazioni personalizzate dei grafici e degli allarmi, consulta Using Amazon CloudWatch dashboard nella Amazon CloudWatch User Guide.

Visualizza nelle metriche CloudWatch

Seleziona l'icona del menu nell'angolo in alto a destra di un singolo grafico e scegli Visualizza nelle metriche per visualizzare questo grafico nella CloudWatch console Amazon. Dalla CloudWatch

console, puoi aggiungere questo grafico singolo a una dashboard e modificare intervalli di tempo, periodi e intervalli di aggiornamento. Per ulteriori informazioni, consulta la sezione Grafica delle metriche nella Amazon CloudWatch User Guide.

Interpretazione dei grafici

AWS KMS offre diversi grafici per monitorare l'integrità dell'archivio delle chiavi esterne all'interno della console AWS KMS. Questi grafici vengono configurati automaticamente e derivati dai parametri di AWS KMS.

I dati del grafico vengono raccolti come parte delle chiamate effettuate all'archivio delle chiavi esterne e alle chiavi esterne. È possibile che i grafici vengano popolati dai dati durante un intervallo di tempo in cui non è stata effettuata alcuna chiamata, Questi dati provengono dalle chiamate `GetHealthStatus`periodiche effettuate da AWS KMS per tuo conto al fine di verificare lo stato del proxy e del gestore delle chiavi esterne. Se nei grafici viene visualizzato il messaggio No data available (Nessun dato disponibile), significa che non sono state registrate chiamate durante tale intervallo di tempo o che l'archivio delle chiavi esterne si trova in uno stato `DISCONNECTED`. Potresti riuscire a identificare l'ora in cui l'archivio delle chiavi esterne è stato disconnesso regolando la visualizzazione su un intervallo di tempo più ampio.

Argomenti

- Total Requests (Richieste totali)
- Affidabilità
- Latenza
- Le 5 eccezioni principali
- Giorni alla scadenza del certificato

Total Requests (Richieste totali)

Il numero totale di richieste AWS KMS ricevute per uno specifico archivio delle chiavi esterne in un determinato intervallo di tempo. Usa questo grafico per determinare se sei a rischio di limitazione (della larghezza di banda della rete).

AWS KMS consiglia la gestione di 1.800 richieste di operazioni di crittografia al secondo per il gestore delle chiavi esterne. Se ti avvicini a 540.000 chiamate in un periodo di cinque minuti, sei a rischio di limitazione (della larghezza di banda della rete).

Puoi monitorare il numero di richieste di operazioni crittografiche sulle chiavi KMS nell'archivio delle chiavi esterne che AWS KMS limita con il parametro ExternalKeyStoreThrottle.

Se ricevi errori `KMSInvalidStateException` molto frequenti con un messaggio che spiega che la richiesta è stata rifiutata "a causa di un tasso di richieste molto elevato", ciò potrebbe indicare che il gestore delle chiavi esterne o il proxy dell'archivio delle chiavi esterne non è in grado di tenere il passo con il tasso di richieste corrente. Se possibile, riduci il tasso di richiesta. Potresti anche prendere in considerazione la possibilità di richiedere una riduzione del valore della quota di richiesta dell'archivio delle chiavi personalizzate. La riduzione di questo valore potrebbe aumentare la limitazione (della larghezza di banda della rete), ma indica che AWS KMS rifiuta rapidamente le richieste in eccesso prima che vengano inviate al proxy dell'archivio delle chiavi esterne o al gestore delle chiavi esterne. Per richiedere una riduzione della quota, consulta la sezione Centro AWS Support e crea un caso.

Il grafico delle richieste totali deriva dal parametro XksProxyErrors, che raccoglie dati sulle risposte riuscite e non riuscite che AWS KMS riceve dal proxy dell'archivio delle chiavi esterne. Quando visualizzi un punto dati specifico, il popup mostra il valore della dimensione `CustomKeyStoreId` insieme al numero totale di richieste AWS KMS registrate in quel punto dati. Il valore di `CustomKeyStoreId` sarà sempre lo stesso.

Affidabilità

La percentuale di richieste AWS KMS per le quali il proxy dell'archivio delle chiavi esterne ha restituito una risposta corretta o un errore non irreversibile. Utilizza questo grafico per valutare lo stato operativo del proxy dell'archivio delle chiavi esterne.

Quando il grafico mostra un valore inferiore al 100%, indica i casi in cui il proxy non ha risposto o ha risposto con un errore non irreversibile. Ciò può indicare problemi con la rete, lentezza del proxy o del gestore delle chiavi esterne o bug di implementazione.

Se la richiesta include credenziali non valide e il proxy risponde con un'eccezione `AuthenticationFailedException`, il grafico indicherà comunque un'affidabilità del 100% perché il proxy ha identificato un valore errato nella richiesta dell'API proxy dell'archivio delle chiavi esterne e quindi l'errore è previsto. Se la percentuale del grafico di affidabilità è del 100%, il proxy dell'archivio delle chiavi esterne risponde come previsto. Se il grafico mostra un valore inferiore al 100%, il proxy ha risposto con un errore non irreversibile o è scaduto. Ad esempio, se il proxy risponde con un'eccezione `ThrottlingException` a causa di un tasso di richiesta molto elevato, mostrerà una percentuale di affidabilità inferiore perché il proxy non è stato in grado di identificare un problema

specifico nella richiesta che ne ha causato l'errore. Questo perché gli errori non irreversibili sono probabilmente problemi temporanei che possono essere risolti ripetendo la richiesta.

Le seguenti risposte di errore ridurranno la percentuale di affidabilità. Puoi utilizzare il grafico Le 5 eccezioni principali e il parametro XksProxyErrors per monitorare ulteriormente la frequenza con cui il proxy restituisce ogni errore non irreversibile.

- `InternalException`
- `DependencyTimeoutException`
- `ThrottlingException`
- `XksProxyUnreachableException`

Il grafico di affidabilità deriva dal parametro XksProxyErrors, che raccoglie dati sulle risposte riuscite e non riuscite che AWS KMS riceve dal proxy dell'archivio delle chiavi esterne. La percentuale di affidabilità diminuirà solo se la risposta ha un valore `ErrorType` di `Retryable`. Quando visualizzi un punto dati specifico, il popup mostra il valore della dimensione `CustomKeyStoreId` insieme alla percentuale di affidabilità per le richieste AWS KMS registrate in quel punto dati. Il valore di `CustomKeyStoreId` sarà sempre lo stesso.

Ti consigliamo di utilizzare la XksProxyErrors metrica per creare un CloudWatch allarme che ti avvisi di potenziali problemi di rete avvisandoti quando vengono registrati più di cinque errori ripetibili in un minuto. Per ulteriori informazioni, consulta Creazione di un CloudWatch allarme Amazon per errori ripetibili.

Latenza

Il numero di millisecondi necessari a un proxy dell'archivio delle chiavi esterne per rispondere a una richiesta AWS KMS. Utilizza questo grafico per valutare le prestazioni del proxy dell'archivio delle chiavi esterne e del gestore delle chiavi esterne.

AWS KMS prevede che il proxy dell'archivio delle chiavi esterne risponda a ogni richiesta entro 250 millisecondi. In caso di timeout di rete, AWS KMS eseguirà un altro tentativo con la richiesta. Se il proxy restituisce ancora una volta un errore, la latenza registrata è il limite di timeout combinato per entrambi i tentativi di richiesta e il grafico mostrerà circa 500 millisecondi. In tutti gli altri casi in cui il proxy non risponde entro il limite di timeout di 250 millisecondi, la latenza registrata è di 250 millisecondi. Se il proxy è spesso in timeout durante le operazioni di crittografia e decrittografia, rivolgiti all'amministratore del proxy esterno. Per informazioni sulla risoluzione dei problemi di latenza, consulta Errori di latenza e timeout.

Le risposte lente potrebbero anche indicare che il gestore delle chiavi esterne non è in grado di gestire il traffico delle richieste corrente. AWS KMS consiglia la gestione di 1.800 richieste di operazioni di crittografia al secondo per il gestore delle chiavi esterne. Se il gestore delle chiavi esterne non è in grado di gestire 1.800 richieste al secondo, prendi in considerazione la possibilità di richiedere una riduzione della quota di richieste per le chiavi KMS in un archivio delle chiavi personalizzate. Le richieste relative alle operazioni di crittografia che utilizzano le chiavi KMS nell'archivio delle chiavi esterne anticiperanno rapidamente l'errore (fail fast) con un'eccezione di limitazione (della larghezza di banda della rete), anziché essere elaborate e successivamente rifiutate dal proxy o dal gestore delle chiavi esterne.

Il grafico della latenza è derivato dal parametro XksProxyLatency. Quando visualizzi un punto dati specifico, il popup mostra i valori delle dimensioni `KmsOperation` e `XksOperation` corrispondenti, oltre alla latenza media registrata per le operazioni in quel punto dati. Gli elementi dell'elenco sono ordinati dalla latenza più alta a quella più bassa.

Ti consigliamo di utilizzare la XksProxyLatency metrica per creare un CloudWatch allarme che ti avvisi quando la latenza si avvicina al limite di timeout. Per ulteriori informazioni, consulta Creazione di un CloudWatch allarme Amazon per il timeout di risposta.

Le 5 eccezioni principali

Le cinque eccezioni principali per le operazioni di crittografia e di gestione non riuscite in un determinato intervallo di tempo. Usa questo grafico per tenere traccia degli errori più frequenti, in modo da poter assegnare priorità diverse agli interventi tecnici.

Questo conteggio include le eccezioni che AWS KMS ha ricevuto dal proxy dell'archivio delle chiavi esterne e l'eccezione `XksProxyUnreachableException` che AWS KMS restituisce internamente quando non è in grado di stabilire una comunicazione con il proxy.

Tassi elevati di errori non irreversibili potrebbero indicare errori di rete, mentre un'elevata percentuale di errori irreversibili potrebbe indicare un problema con la configurazione dell'archivio delle chiavi esterne. Ad esempio, un picco in `AuthenticationFailedExceptions` indica una discrepanza tra le credenziali di autenticazione configurate in AWS KMS e il proxy dell'archivio delle chiavi esterne. Per visualizzare la configurazione dell'archivio delle chiavi esterne, consulta Visualizzazione di un archivio delle chiavi esterne. Per modificare le impostazioni dell'archivio delle chiavi esterne, consulta Modifica delle proprietà dell'archivio delle chiavi esterne.

Le eccezioni che AWS KMS riceve dal proxy dell'archivio delle chiavi esterno sono diverse dalle eccezioni che AWS KMS restituisce quando un'operazione non va a buon fine. Le operazioni di crittografia AWS KMS restituiscono un'eccezione `KMSInvalidStateException` per tutti gli errori

relativi alla configurazione esterna o allo stato di connessione dell'archivio delle chiavi esterno. Per identificare il problema, utilizza il testo del messaggio di errore allegato.

La tabella seguente mostra le eccezioni che possono essere visualizzate nel grafico delle 5 eccezioni principali e le eccezioni corrispondenti restituite da AWS KMS.

Tipi di errore	Eccezione visualizzata nel grafico	Eccezione restituita da AWS KMS
Irreversibile	**`AccessDeniedException`** Per la risoluzione dei problemi, consultare Problemi relativi all'autorizzazione proxy.	**`CustomKeyStoreInvalidStateException`** in risposta alle operazioni `CreateKey` . **`KMSInvalidStateException`** in risposta alle operazioni di crittografia.
Irreversibile	**`AuthenticationFailedException`** Per la risoluzione dei problemi, consultare Errori delle credenziali di autenticazione.	**`XksProxyIncorrectAuthenticationCredentialException`** in risposta alle operazioni `CreateCustomKeyStore` e `UpdateCustomKeyStore` . **`CustomKeyStoreInvalidStateException`** in risposta alle operazioni `CreateKey` . **`KMSInvalidStateException`** in risposta alle operazioni di crittografia.
Non irreversibile	**`DependencyTimeoutException`**	**`XksProxyUriUnreachableException`** in risposta alle operazioni `CreateCustomKeyStore`

Tipi di errore	Eccezione visualizzata nel grafico	Eccezione restituita da AWS KMS
	Per la risoluzione dei problemi, consultare Errori di latenza e timeout.	e `UpdateCustomKeyStore` . **`CustomKeyStoreInvalidStateException`** in risposta alle operazioni `CreateKey` . **`KMSInvalidStateException`** in risposta alle operazioni di crittografia.
Non irreversibile	**`InternalException`** Il proxy dell'archivio delle chiavi esterne ha rifiutato la richiesta perché non è in grado di comunicare con il gestore delle chiavi esterne. Verifica che la configurazione del proxy dell'archivio delle chiavi esterne sia corretta e che il gestore delle chiavi esterne sia disponibile.	**`XksProxyInvalidResponseException`** in risposta alle operazioni `CreateCustomKeyStore` e `UpdateCustomKeyStore` . **`CustomKeyStoreInvalidStateException`** in risposta alle operazioni `CreateKey` . **`KMSInvalidStateException`** in risposta alle operazioni di crittografia.
Irreversibile	**`InvalidCiphertextException`** Per la risoluzione dei problemi, consultare Errori di decrittografia.	**`KMSInvalidStateException`** in risposta alle operazioni di crittografia.

Tipi di errore	Eccezione visualizzata nel grafico	Eccezione restituita da AWS KMS
Irreversibile	**`InvalidKeyUsageException`** Per la risoluzione dei problemi, consultare Errori relativi alle operazioni di crittografia per la chiave esterna.	**`XksKeyInvalidConfigurationException`** in risposta alle operazioni `CreateKey` . **`KMSInvalidStateException`** in risposta alle operazioni di crittografia.
Irreversibile	**`InvalidStateException`** Per la risoluzione dei problemi, consultare Errori relativi alle operazioni di crittografia per la chiave esterna.	**`XksKeyInvalidConfigurationException`** in risposta alle operazioni `CreateKey` . **`KMSInvalidStateException`** in risposta alle operazioni di crittografia.
Irreversibile	**`InvalidUriPathException`** Per la risoluzione dei problemi, consultare Errori di configurazione generale.	**`XksProxyInvalidConfigurationException`** in risposta alle operazioni `CreateCustomKeyStore` e `UpdateCustomKeyStore` . **`CustomKeyStoreInvalidStateException`** in risposta alle operazioni `CreateKey` . **`KMSInvalidStateException`** in risposta alle operazioni di crittografia.

Tipi di errore	Eccezione visualizzata nel grafico	Eccezione restituita da AWS KMS
Irreversibile	**`KeyNotFoundException`** Per la risoluzione dei problemi, consultare Errori relativi alla chiave esterna.	**`XksKeyNotFoundException`** in risposta alle operazioni `CreateKey` . **`KMSInvalidStateException`** in risposta alle operazioni di crittografia.
Non irreversibile	**`ThrottlingException`** Il proxy dell'archivio delle chiavi esterne ha rifiutato la richiesta a causa di un tasso di richieste molto elevato. Riduci la frequenza delle chiamate utilizzando le chiavi KMS in questo archivio delle chiavi esterne.	**`XksProxyUriUnreachableException`** in risposta alle operazioni `CreateCustomKeyStore` e `UpdateCustomKeyStore` . **`CustomKeyStoreInvalidStateException`** in risposta alle operazioni `CreateKey` . **`KMSInvalidStateException`** in risposta alle operazioni di crittografia.
Irreversibile	**`UnsupportedOperationException`** Per la risoluzione dei problemi, consultare Errori relativi alle operazioni di crittografia per la chiave esterna.	**`XksKeyInvalidResponseException`** in risposta alle operazioni `CreateKey` . **`KMSInvalidStateException`** in risposta alle operazioni di crittografia.

Tipi di errore	Eccezione visualizzata nel grafico	Eccezione restituita da AWS KMS
Irreversibile	**`ValidationException`** Per la risoluzione dei problemi, consultare Problemi relativi al proxy.	**`XksProxyInvalidResponseException`** in risposta alle operazioni `CreateCustomKeyStore` e `UpdateCustomKeyStore` . **`CustomKeyStoreInvalidStateException`** in risposta alle operazioni `CreateKey` . **`KMSInvalidStateException`** in risposta alle operazioni di crittografia.
Non irreversibile	**`XksProxyUnreachableException`** Se riscontri ripetutamente questo errore, verifica che il proxy dell'archivio delle chiavi esterne sia attivo e connesso alla rete. Verifica inoltre che il percorso URI e l'URI endpoint o il nome del servizio VPC all'interno dell'archivio delle chiavi esterne siano corretti.	**`XksProxyUriUnreachableException`** in risposta alle operazioni `CreateCustomKeyStore` e `UpdateCustomKeyStore` . **`CustomKeyStoreInvalidStateException`** in risposta alle operazioni `CreateKey` . **`KMSInvalidStateException`** in risposta alle operazioni di crittografia.

Il grafico delle 5 eccezioni principali deriva dal parametro XksProxyErrors. Quando visualizzi un punto dati specifico, il popup mostra il valore della dimensione `ExceptionName`, insieme al numero di

volte in cui l'eccezione è stata registrata in quel punto dati. Le cinque voci dell'elenco sono ordinate dall'eccezione più frequente alla meno frequente.

Ti consigliamo di utilizzare la XksProxyErrors metrica per creare un CloudWatch allarme che ti avvisi di potenziali problemi di configurazione avvisandoti quando vengono registrati più di cinque errori non ripetibili in un periodo di un minuto. Per ulteriori informazioni, consulta Creazione di un CloudWatch allarme Amazon per errori irreparabili.

Giorni alla scadenza del certificato

Il numero di giorni che mancano alla scadenza del certificato TLS per l'endpoint proxy dell'archivio delle chiavi esterne (`XksProxyUriEndpoint`). Utilizza questo grafico per monitorare la scadenza imminente del certificato TLS.

Alla scadenza del certificato, AWS KMS non è in grado di comunicare con il proxy dell'archivio delle chiavi esterne. Tutti i dati protetti dalle chiavi KMS nell'archivio delle chiavi esterne diventano inaccessibili fino al rinnovo del certificato.

Il grafico dei giorni di scadenza del certificato deriva dal parametro XksProxyCertificateDaysToExpire. Ti consigliamo vivamente di utilizzare questa metrica per creare un CloudWatch allarme che ti avvisi della scadenza imminente. La scadenza del certificato potrebbe impedirti di accedere alle risorse crittografate. Configura l'allarme in modo che l'organizzazione abbia la possibilità di rinnovare il certificato prima della sua scadenza. Per ulteriori informazioni, consulta Creazione di un CloudWatch allarme Amazon per la scadenza dei certificati.

Impostazione degli allarmi

I grafici nella sezione di monitoraggio offrono una panoramica dell'integrità degli archivi delle chiavi esterne e delle relative chiavi KMS per un determinato periodo di tempo. Tuttavia, puoi creare CloudWatch allarmi Amazon basati su parametri di archiviazione di chiavi esterne per avvisarti quando il valore di una metrica supera una soglia specificata. L'allarme può inviare un messaggio a un argomento Servizio di notifica semplice Amazon (Amazon Simple Notification Service (Amazon SNS)) o alla policy di Dimensionamento automatico Amazon EC2. Per informazioni dettagliate sugli CloudWatch allarmi, consulta Using Amazon CloudWatch alarms nella Amazon CloudWatch User Guide.

Prima di creare un CloudWatch allarme Amazon, è necessario un argomento su Amazon SNS. Per maggiori dettagli, consulta l'argomento Creating an Amazon SNS nella Amazon CloudWatch User Guide.

Argomenti

Creazione di un CloudWatch allarme Amazon per la scadenza dei certificati

Questo allarme utilizza la XksProxyCertificateDaysToExpire metrica AWS KMS pubblicata su per CloudWatch registrare la scadenza prevista del certificato TLS associato all'endpoint proxy di archiviazione delle chiavi esterno. Non puoi creare un singolo allarme per tutti gli archivi delle chiavi esterne dell'account o un allarme per gli archivi delle chiavi esterne che è possibile creare in futuro.

Ti consigliamo di impostare l'allarme in modo che ti avvisi 10 giorni prima della scadenza del certificato, ma dovresti impostare la soglia più adatta alle tue esigenze.

Creazione dell'allarme

Segui le istruzioni riportate in Creare un CloudWatch allarme basato su una soglia statica utilizzando i seguenti valori obbligatori. Per gli altri campi, accetta i valori predefiniti e immetti i nomi come richiesto.

Campo	Valore
Seleziona parametro	Scegli KMS, quindi XKS Proxy Certificate Metrics (Parametri del certificato proxy XKS). Seleziona la casella di controllo accanto al valore `XksProxyCertificateName` da monitorare. Quindi, scegli Seleziona parametro.
Statistic	Minimo
Periodo	5 minuti
Tipo di soglia	Statico
Quando...	Ogni volta `Lower` che XksProxyCertificateDaysToExpireè così`10`.

Creazione di un CloudWatch allarme Amazon per il timeout di risposta

Questo allarme utilizza la XksProxyLatency metrica AWS KMS pubblicata su per registrare il numero di millisecondi necessari CloudWatch a un proxy di archiviazione di chiavi esterno per rispondere a una richiesta. AWS KMS Non puoi creare un singolo allarme per tutti gli archivi delle chiavi esterne dell'account o un allarme per gli archivi delle chiavi esterne che è possibile creare in futuro.

AWS KMS prevede che il proxy dell'archivio delle chiavi esterne risponda a ogni richiesta entro 250 millisecondi. Ti consigliamo di impostare un allarme per avvisarti quando il proxy dell'archivio delle chiavi esterne impiega più di 200 millisecondi per rispondere, ma dovresti impostare la soglia più adatta alle tue esigenze.

Creazione dell'allarme

Segui le istruzioni riportate in Creare un CloudWatch allarme basato su una soglia statica utilizzando i seguenti valori obbligatori. Per gli altri campi, accetta i valori predefiniti e immetti i nomi come richiesto.

Campo	Valore
Seleziona parametro	Scegli KMS, quindi XKS Proxy Latency Metrics (Parametri di latenza del proxy XKS). Seleziona la casella di controllo accanto al valore `KmsOperation` da monitorare. Quindi, scegli Seleziona parametro.
Statistic	Media
Periodo	5 minuti
Tipo di soglia	Statico
Quando...	Ogni volta `Greater` che XksProxyLatencyè così`200`.

Creazione di un CloudWatch allarme Amazon per errori ripetibili

Questo allarme utilizza la XksProxyErrors metrica AWS KMS pubblicata su per CloudWatch registrare il numero di eccezioni relative AWS KMS alle richieste al proxy esterno dell'archivio di

chiavi. Non puoi creare un singolo allarme per tutti gli archivi delle chiavi esterne dell'account o un allarme per gli archivi delle chiavi esterne che è possibile creare in futuro.

Gli errori non irreversibili riducono la percentuale di affidabilità e possono indicare errori di rete. Ti consigliamo di impostare un allarme per avvisarti quando vengono registrati più di cinque errori non irreversibili in un minuto, ma dovresti impostare la soglia più adatta alle tue esigenze.

Segui le istruzioni riportate in Creare un CloudWatch allarme basato su una soglia statica utilizzando i seguenti valori obbligatori. Per gli altri campi, accetta i valori predefiniti e immetti i nomi come richiesto.

Campo	Valore
Seleziona parametro	Scegli la scheda Queries (Query). Scegli `AWS/KMS` per Namespace. Inserisci `SUM(XksProxyErrors)` in Metric name (Nome parametro). Inserisci `ErrorType = Retryable` in Filter by (Filtra per). Scegli Esegui. Quindi, scegli Seleziona parametro.
Etichetta	*Errori non irreversibili*
Periodo	1 minuto
Tipo di soglia	Statico
Quando...	Ogni volta che q1 è `Greater` di `5`.

Creazione di un CloudWatch allarme Amazon per errori irreparabili

Questo allarme utilizza la XksProxyErrors metrica AWS KMS pubblicata su per registrare il numero di eccezioni relative CloudWatch alle AWS KMS richieste al proxy di archiviazione delle chiavi esterno. Non puoi creare un singolo allarme per tutti gli archivi delle chiavi esterne dell'account o un allarme per gli archivi delle chiavi esterne che è possibile creare in futuro.

Gli errori irreversibili possono indicare un problema con la configurazione dell'archivio delle chiavi esterne. Ti consigliamo di impostare un allarme per avvisarti quando vengono registrati più di cinque errori irreversibili in un minuto, ma dovresti impostare la soglia più adatta alle tue esigenze.

Segui le istruzioni riportate in Creare un CloudWatch allarme basato su una soglia statica utilizzando i seguenti valori obbligatori. Per gli altri campi, accetta i valori predefiniti e immetti i nomi come richiesto.

Campo	Valore
Seleziona parametro	Scegli la scheda Queries (Query). Scegli `AWS/KMS` per Namespace. Inserisci `SUM(XksProxyErrors)` in Metric name (Nome parametro). Inserisci `ErrorType = Non-retryable` in Filter by (Filtra per). Scegli Esegui. Quindi, scegli Seleziona parametro.
Etichetta	*Errori irreversibili*
Periodo	1 minuto
Tipo di soglia	Statico
Quando...	Ogni volta che q1 è `Greater` di `5`.

Connessione e disconnessione di un archivio delle chiavi esterne

I nuovi archivi delle chiavi esterne non sono connessi. Per creare e utilizzare AWS KMS keys nell'archivio delle chiavi esterne, devi connettere tale archivio al relativo proxy. Puoi connettere e disconnettere l'archivio delle chiavi esterne in qualsiasi momento e visualizzare il relativo stato di connessione.

Quando l'archivio delle chiavi esterne è disconnesso, AWS KMS non è in grado di comunicare con il proxy dell'archivio delle chiavi esterne. Di conseguenza, puoi visualizzare e gestire l'archivio delle chiavi esterne e le relative chiavi KMS, ma non puoi creare chiavi KMS nell'archivio delle chiavi esterne o utilizzare le relative chiavi KMS in operazioni di crittografia. In alcuni casi, ad esempio si modificano le proprietà, potresti dover disconnettere l'archivio delle chiavi esterne, per cui ti

consigliamo di pianificare le operazioni di conseguenza. La disconnessione dell'archivio delle chiavi potrebbe interrompere il funzionamento dei servizi AWS che utilizzano le relative chiavi KMS.

Non sei obbligato a connettere l'archivio delle chiavi esterne. Puoi lasciarlo disconnesso indefinitamente e connetterlo solo quando devi utilizzarlo. Puoi tuttavia testare la connessione periodicamente per verificare che le impostazioni sono corrette e che non vi sono problemi di connessione dello store.

Quando disconnetti un archivio delle chiavi personalizzate, le chiavi KMS nell'archivio diventano immediatamente inutilizzabili (in base alla coerenza finale). Tuttavia, le risorse crittografate con chiavi di dati protette dalla chiave KMS non sono interessate fino a quando la chiave KMS non viene nuovamente utilizzata, ad esempio per decrittografare la chiave dati. Questo problema riguarda i Servizi AWS, molti dei quali proteggono le risorse tramite le chiavi dati. Per informazioni dettagliate, vedi In che modo le chiavi KMS inutilizzabili influiscono sulle chiavi dati.

> **Note**
>
> Gli archivi delle chiavi esterne presentano lo stato `DISCONNECTED` solo quando l'archivio non è mai stato connesso o se lo si disconnette esplicitamente. Lo stato `CONNECTED` non indica che l'archivio delle chiavi esterne o i relativi componenti di supporto funzionino in modo efficiente. Per informazioni relative alle prestazioni dei componenti dell'archivio delle chiavi esterne, consulta i grafici nella sezione Monitoraggio della pagina dei dettagli di ogni archivio delle chiavi esterne. Per informazioni dettagliate, vedi Monitoraggio di un archivio delle chiavi esterne.
>
> Il gestore delle chiavi esterne potrebbe fornire metodi aggiuntivi per interrompere e riavviare la comunicazione tra AWS KMS e il proxy dell'archivio delle chiavi esterne o tra il proxy e il gestore. Per ulteriori informazioni, consulta la documentazione del gestore delle chiavi esterne.

Argomenti

- Connessione di un archivio delle chiavi esterne
- Disconnessione di un archivio delle chiavi esterne
- Stato connessione
- Connessione di un archivio delle chiavi esterne (console)
- Connessione di un archivio delle chiavi esterne (API)
- Disconnessione di un archivio delle chiavi esterne (console)

- Disconnessione di un archivio delle chiavi esterne (API)

Connessione di un archivio delle chiavi esterne

Quando l'archivio delle chiavi esterne è connesso al relativo proxy, puoi creare chiavi KMS nello stesso archivio delle chiavi esterne e utilizzare le chiavi KMS esistenti in operazioni di crittografia.

Il processo che collega un archivio delle chiavi esterne al relativo proxy varia in base alla connettività dell'archivio.

- Quando si connette un archivio di chiavi esterno con connettività endpoint pubblica, AWS KMS invia una GetHealthStatus richiesta al proxy dell'archivio chiavi esterno per convalidare l'endpoint URI del proxy, il percorso URI del proxy e le credenziali di autenticazione del proxy. Una risposta positiva da parte del proxy conferma che l'endpoint dell'URI proxy e il percorso URI proxy sono corretti e accessibili e che il proxy ha autenticato la richiesta firmata con le credenziali di autenticazione proxy per l'archivio delle chiavi esterne.
- Quando connetti un archivio delle chiavi esterne con connettività del servizio endpoint VPC al relativo proxy, AWS KMS esegue le seguenti operazioni:
  - Conferma che il dominio per il nome DNS privato specificato nell'endpoint URI proxy è verificato.
  - Crea un endpoint di interfaccia da un VPC AWS KMS al servizio endpoint VPC.
  - Crea una zona ospitata privata per il nome DNS privato specificato nell'endpoint URI proxy
  - Invia una GetHealthStatusrichiesta al proxy dell'archivio chiavi esterno. Una risposta positiva da parte del proxy conferma che l'endpoint dell'URI proxy e il percorso URI proxy sono corretti e accessibili e che il proxy ha autenticato la richiesta firmata con le credenziali di autenticazione proxy per l'archivio delle chiavi esterne.

L'operazione di connessione avvia il processo di connessione dell'archivio delle chiavi personalizzate, ma il collegamento di un archivio delle chiavi esterne al relativo proxy esterno richiede circa cinque minuti. Una risposta positiva dell'operazione di connessione non indica che l'archivio delle chiavi esterne sia connesso. Per confermare che la connessione è avvenuta correttamente, utilizza la AWS KMS console o l'DescribeCustomKeyStoresoperazione per visualizzare lo stato della connessione del tuo key store esterno.

Quando lo stato della connessione è `FAILED`, nella console AWS KMS viene visualizzato un codice di errore di connessione che viene aggiunto alla risposta `DescribeCustomKeyStore`. Per informazioni sull'interpretazione dei codici di errore di connessione, consulta Codici di errore di connessione per archivi delle chiavi esterne.

Disconnessione di un archivio delle chiavi esterne

Quando disconnetti un archivio delle chiavi esterne con connettività del servizio endpoint VPC dal relativo proxy dell'archivio delle chiavi esterne, AWS KMS elimina l'endpoint di interfaccia per il servizio endpoint VPC e rimuove l'infrastruttura di rete che ha creato per supportare la connessione. Non è richiesto alcun processo equivalente per gli archivi delle chiavi esterne con connettività dell'endpoint pubblico. Questa operazione non influisce sul servizio endpoint VPC o sui suoi componenti di supporto. Inoltre, non ha alcun impatto sul proxy dell'archivio delle chiavi esterne o su eventuali componenti esterni.

Quando l'archivio delle chiavi esterne è disconnesso, AWS KMS non invia alcuna richiesta al proxy dell'archivio delle chiavi esterne. Lo stato di connessione dell'archivio delle chiavi esterne è `DISCONNECTED`. Le chiavi KMS nell'archivio delle chiavi esterne disconnesso presentano uno stato `UNAVAILABLE` (a meno che non siano in attesa di eliminazione), pertanto non possono essere utilizzate nelle operazioni di crittografia. Tuttavia, puoi comunque visualizzare e gestire l'archivio delle chiavi esterne e le relative chiavi KMS esistenti.

Lo stato disconnesso è progettato per essere temporaneo e reversibile. La riconnessione dell'archivio delle chiavi esterne può avvenire in qualsiasi momento. In genere, non è necessaria alcuna riconfigurazione. Tuttavia, se alcune proprietà del proxy dell'archivio delle chiavi esterne associato sono state modificate durante la disconnessione, ad esempio la rotazione delle credenziali di autenticazione proxy, è necessario modificare le impostazioni dell'archivio delle chiavi esterne prima di riconnetterlo.

> **Note**
>
> Quando un archivio delle chiavi personalizzate è disconnesso, tutti i tentativi di creare chiavi KMS nell'archivio delle chiavi personalizzate o di utilizzare le chiavi KMS in operazioni di crittografia avrà esito negativo. Questa azione può impedire agli utenti di archiviare e accedere ai dati sensibili.

Per valutare meglio l'effetto della disconnessione dell'archivio delle chiavi esterne, identifica le chiavi KMS e determinane l'utilizzo precedente.

Puoi disconnettere un archivio delle chiavi esterne per i seguenti motivi:

- Per modificarne le proprietà. Puoi modificare il nome dell'archivio delle chiavi personalizzate, il percorso URI proxy e le credenziali di autenticazione proxy mentre l'archivio delle chiavi esterne è

connesso. Tuttavia, per modificare il tipo di connettività proxy, l'endpoint dell'URI proxy o il nome del servizio endpoint VPC, devi prima disconnettere l'archivio delle chiavi esterne. Per informazioni dettagliate, vedi Modifica delle proprietà dell'archivio delle chiavi esterne.

- Per interrompere tutte le comunicazioni tra AWS KMS e il proxy dell'archivio delle chiavi esterne. Puoi anche interrompere la comunicazione tra AWS KMS e il proxy disabilitando l'endpoint o il servizio endpoint VPC. Inoltre, il proxy dell'archivio delle chiavi esterne o il software di gestione delle chiavi potrebbe fornire meccanismi aggiuntivi per impedire ad AWS KMS di comunicare con il proxy o per impedire al proxy di accedere al gestore delle chiavi esterne.
- Per disabilitare tutte le chiavi KMS nell'archivio delle chiavi esterne. È possibile disabilitare e riattivare le chiavi KMS in un archivio di chiavi esterno utilizzando la AWS KMS console o l'DisableKeyoperazione. Queste operazioni vengono completate rapidamente (in base alla coerenza finale), ma agiscono su una sola chiave KMS alla volta. La disconnessione modifica lo stato di chiave di tutte le chiavi KMS nell'archivio delle chiavi esterne in `Unavailable`, che ne impedisce l'utilizzo in qualsiasi operazione di crittografia.
- Per riparare un tentativo di connessione non riuscito. Se un tentativo di connessione di un archivio delle chiavi esterne ha esito negativo (il relativo stato di connessione è `FAILED`), devi disconnettere l'archivio prima di eseguire un nuovo tentativo di connessione.

Stato connessione

La connessione e la disconnessione modificano lo stato di connessione dell'archivio delle chiavi personalizzate. I valori dello stato di connessione per gli archivi delle chiavi di AWS CloudHSM e gli archivi delle chiavi esterne sono gli stessi.

Per visualizzare lo stato di connessione del tuo archivio di chiavi personalizzato, utilizza l'DescribeCustomKeyStoresoperazione o AWS KMS la console. Il campo Connection state (Stato connessione) viene visualizzato in ogni tabella dell'archivio delle chiavi personalizzate, nella sezione General configuration (Configurazione generale) della pagina dei dettagli di ogni archivio e nella scheda Cryptographic configuration (Configurazione crittografica) delle chiavi KMS. Per informazioni dettagliate, consulta Visualizzazione di un archivio delle chiavi di AWS CloudHSM e Visualizzazione di un archivio delle chiavi esterne.

Un archivio delle chiavi personalizzate può avere uno dei seguenti stati di connessione:

- `CONNECTED`: l'archivio delle chiavi personalizzate è connesso al relativo archivio del materiale della chiave. Puoi creare o utilizzare le chiavi KMS nell'archivio delle chiavi personalizzate.

L'archivio del materiale della chiave per un archivio delle chiavi di AWS CloudHSM è il cluster AWS CloudHSM associato. L'archivio del materiale della chiave per un archivio delle chiavi esterne è rappresentato da un proxy dell'archivio delle chiavi esterne e dal gestore delle chiavi esterne che supporta.

Uno stato CONNECTED (CONNESSO) indica che la connessione è riuscita e che l'archivio delle chiavi personalizzate non è stato disconnesso intenzionalmente. Non indica che la connessione sta funzionando correttamente. Per informazioni sullo stato del AWS CloudHSM cluster associato all'archivio delle AWS CloudHSM chiavi, consulta Ottenere le CloudWatch metriche AWS CloudHSM nella Guida per l'AWS CloudHSMutente. Per informazioni sullo stato e sul funzionamento dell'archivio delle chiavi esterne, consulta i grafici nella sezione Monitoring (Monitoraggio) della pagina dei dettagli di ogni archivio. Per informazioni dettagliate, vedi Monitoraggio di un archivio delle chiavi esterne.

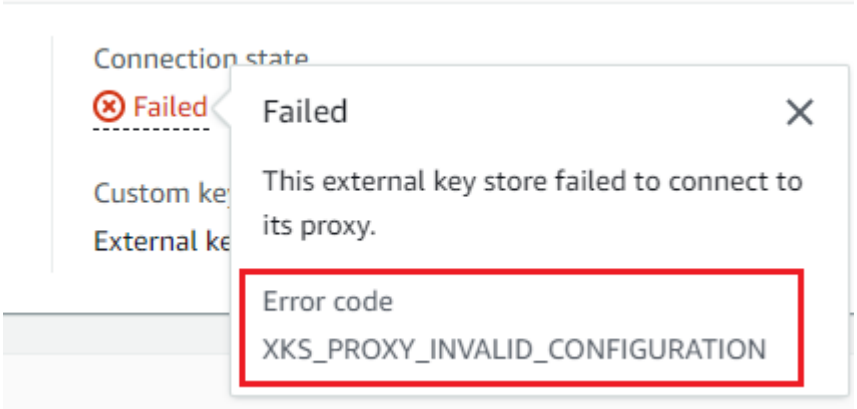
- `CONNECTING`: il processo di connessione di un archivio delle chiavi personalizzate è in corso. Si tratta di uno stato transitorio.
- `DISCONNECTED`: L'archivio chiavi personalizzato non è mai stato collegato al relativo supporto oppure è stato disconnesso intenzionalmente utilizzando la AWS KMS console o l'operazione. DisconnectCustomKeyStore
- `DISCONNECTING`: il processo di disconnessione di un archivio delle chiavi personalizzate è in corso. Si tratta di uno stato transitorio.
- `FAILED`: tentativo di connessione dell'archivio delle chiavi personalizzate non riuscito. `ConnectionErrorCode`Nella DescribeCustomKeyStoresrisposta indica il problema.

Per connettere un archivio delle chiavi personalizzate, il relativo stato di connessione deve essere `DISCONNECTED`. Se lo stato della connessione è `FAILED`, utilizza `ConnectionErrorCode` per identificare e risolvere il problema. Disconnetti quindi l'archivio delle chiavi personalizzate prima di provare a connetterlo di nuovo. Per informazioni sugli errori di connessione, consulta Errori di connessione all'archivio delle chiavi esterne. Per informazioni sulla risposta a un codice di errore di connessione, consulta Codici di errore di connessione per archivi delle chiavi esterne.

Per visualizzare il codice di errore della connessione:

- Nella DescribeCustomKeyStoresrisposta, visualizza il valore dell'`ConnectionErrorCode`elemento. Tale elemento appare nella risposta `DescribeCustomKeyStores` solo quando `ConnectionState` è nello stato `FAILED`.

- Per visualizzare il codice di errore della connessione nella console AWS KMS, accedi alla pagina dei dettagli dell'archivio delle chiavi esterne e passa il puntatore del mouse sul valore Failed (Non riuscito).



Connessione di un archivio delle chiavi esterne (console)

Puoi utilizzare la console AWS KMS per connettere un archivio delle chiavi esterne al relativo proxy.

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel pannello di navigazione, scegli Custom key stores (Archivi delle chiavi personalizzate), External key stores (Archivi delle chiavi esterne).
4. Scegli la riga relativa all'archivio delle chiavi esterne che vuoi connettere.

   Se la voce Connection state (Stato connessione) dell'archivio delle chiavi esterne è FAILED (NON RIUSCITO), devi disconnettere l'archivio prima di connetterlo.
5. Dal menu Key store actions (Operazioni per l'archivio delle chiavi), scegli Connect (Connetti).

Il completamento del processo di connessione richiede in genere circa cinque minuti. Al termine dell'operazione, lo stato di connessione cambia in CONNECTED (CONNESSO).

Se lo stato della connessione è Failed (Non riuscito), passa il mouse sullo stato per visualizzare il codice di errore di connessione e la causa dell'errore. Per informazioni sulla risposta a un codice di errore di connessione, consulta Codici di errore di connessione per archivi delle chiavi esterne. Per connettere un archivio delle chiavi esterne con uno stato di connessione Failed (Non riuscito), devi innanzitutto disconnettere l'archivio delle chiavi personalizzate.

Connessione di un archivio delle chiavi esterne (API)

Per connettere un archivio di chiavi esterno disconnesso, utilizzare l'ConnectCustomKeyStoreoperazione.

Prima della connessione, lo stato dell'archivio delle chiavi esterne deve essere `DISCONNECTED`. Se lo stato di connessione corrente è `FAILED`, disconnetti l'archivio delle chiavi esterne e riconnettilo.

Il completamento del processo di connessione può richiedere fino a cinque minuti. Se l'operazione non genera rapidamente un errore, `ConnectCustomKeyStore` restituisce una risposta HTTP 200 e un oggetto JSON senza proprietà. Questa risposta iniziale non indica tuttavia che la connessione è riuscita. Per determinare se l'archivio chiavi esterno è connesso, vedi lo stato della connessione nella DescribeCustomKeyStoresrisposta.

Gli esempi in questa sezione utilizzano AWS Command Line Interface (AWS CLI), ma puoi usare anche qualsiasi linguaggio di programmazione supportato.

Per identificare l'archivio delle chiavi esterne, utilizza l'ID dell'archivio delle chiavi personalizzate. È possibile trovare l'ID nella pagina Custom key stores della console o utilizzando l'DescribeCustomKeyStoresoperazione. Prima di eseguire questo esempio, sostituisci l'ID di esempio con uno valido.

```
$ aws kms connect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

L'operazione `ConnectCustomKeyStore` non restituisce alcun `ConnectionState` nella risposta. Per verificare che l'archivio chiavi esterno sia connesso, utilizzare l'DescribeCustomKeyStoresoperazione. Per impostazione predefinita, questa operazione restituisce tutti gli store delle chiavi personalizzate presenti nel tuo account e nella regione. Puoi tuttavia utilizzare il parametro `CustomKeyStoreName` o `CustomKeyStoreId` (ma non entrambi) per limitare la risposta a determinati store delle chiavi personalizzate. Un `ConnectionState` con valore `CONNECTED` indica che l'archivio delle chiavi esterne è connesso al relativo proxy.

```
$ aws kms describe-custom-key-stores --custom-key-store-name ExampleXksVpc
{
    "CustomKeyStores": [
    {
      "CustomKeyStoreId": "cks-9876543210fedcba9",
      "CustomKeyStoreName": "ExampleXksVpc",
      "ConnectionState": "CONNECTED",
      "CreationDate": "2022-12-13T18:34:10.675000+00:00",
      "CustomKeyStoreType": "EXTERNAL_KEY_STORE",
```

```
      "XksProxyConfiguration": {
        "AccessKeyId": "ABCDE98765432EXAMPLE",
        "Connectivity": "VPC_ENDPOINT_SERVICE",
        "UriEndpoint": "https://example-proxy-uri-endpoint-vpc",
        "UriPath": "/example/prefix/kms/xks/v1",
        "VpcEndpointServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-example"
      }
    }
  ]
}
```

Se il valore `ConnectionState` nella risposta `DescribeCustomKeyStores` è `FAILED`, l'elemento `ConnectionErrorCode` indica il motivo dell'errore.

Nell'esempio seguente, il valore `XKS_VPC_ENDPOINT_SERVICE_NOT_FOUND` di `ConnectionErrorCode` indica che AWS KMS non riesce a trovare il servizio endpoint VPC utilizzato per comunicare con il proxy dell'archivio delle chiavi esterne. Verifica che `XksProxyVpcEndpointServiceName` sia corretto, che il principale del servizio AWS KMS sia consentito nel servizio endpoint Amazon VPC e che il servizio endpoint VPC non richieda l'accettazione delle richieste di connessione. Per informazioni sulla risposta a un codice di errore di connessione, consulta Codici di errore di connessione per archivi delle chiavi esterne.

```
$ aws kms describe-custom-key-stores --custom-key-store-name ExampleXksVpc
{
    "CustomKeyStores": [
    {
      "CustomKeyStoreId": "cks-9876543210fedcba9",
      "CustomKeyStoreName": "ExampleXksVpc",
      "ConnectionState": "FAILED",
      "ConnectionErrorCode": "XKS_VPC_ENDPOINT_SERVICE_NOT_FOUND",
      "CreationDate": "2022-12-13T18:34:10.675000+00:00",
      "CustomKeyStoreType": "EXTERNAL_KEY_STORE",
      "XksProxyConfiguration": {
        "AccessKeyId": "ABCDE98765432EXAMPLE",
        "Connectivity": "VPC_ENDPOINT_SERVICE",
        "UriEndpoint": "https://example-proxy-uri-endpoint-vpc",
        "UriPath": "/example/prefix/kms/xks/v1",
        "VpcEndpointServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-example"
      }
    }
  ]
}
```

Disconnessione di un archivio delle chiavi esterne (console)

Puoi utilizzare la console AWS KMS per connettere un archivio delle chiavi esterne al relativo proxy. Questo processo dura circa 5 minuti.

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel pannello di navigazione, scegli Custom key stores (Archivi delle chiavi personalizzate), External key stores (Archivi delle chiavi esterne).
4. Scegli la riga relativa all'archivio delle chiavi esterne che vuoi disconnettere.
5. Dal menu Key store actions (Operazioni per l'archivio delle chiavi), scegli Disconnect (Disconnetti).

Al completamento dell'operazione, lo stato della connessione cambia da CONNECTED (CONNESSO) a DISCONNECTED (DISCONNESSO). Se l'operazione ha esito negativo, viene visualizzato un messaggio di errore che descrive il problema e fornisce istruzioni su come risolverlo. Per ulteriori informazioni, consulta Errori di connessione all'archivio delle chiavi esterne.

Disconnessione di un archivio delle chiavi esterne (API)

Per disconnettere un archivio di chiavi esterno connesso, utilizzare l'DisconnectCustomKeyStoreoperazione. Se l'operazione ha esito positivo, AWS KMS restituisce una risposta HTTP 200 e un oggetto JSON senza proprietà. Il completamento del processo può richiedere fino a cinque minuti. Per trovare lo stato di connessione dell'archivio chiavi esterno, utilizzare l'DescribeCustomKeyStoresoperazione.

Gli esempi in questa sezione utilizzano AWS Command Line Interface (AWS CLI), ma puoi usare anche qualsiasi linguaggio di programmazione supportato.

Questo esempio disconnette un archivio delle chiavi esterne con connettività del servizio endpoint VPC. Prima di eseguire questo comando, sostituisci l'ID dell'archivio delle chiavi personalizzate di esempio con uno valido.

```
$ aws kms disconnect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

Per verificare che l'archivio chiavi esterno sia disconnesso, utilizzare l'DescribeCustomKeyStoresoperazione. Per impostazione predefinita, questa operazione restituisce tutti gli store delle chiavi personalizzate presenti nel tuo account e nella regione. Puoi tuttavia utilizzare il parametro `CustomKeyStoreName` o `CustomKeyStoreId` (ma non entrambi) per limitare la risposta a determinati store delle chiavi personalizzate. Il `ConnectionState` con valore `DISCONNECTED` indica che questo archivio delle chiavi esterne di esempio non è più connesso al relativo proxy.

```
$ aws kms describe-custom-key-stores --custom-key-store-name ExampleXksVpc
{
    "CustomKeyStores": [
    {
      "CustomKeyStoreId": "cks-9876543210fedcba9",
      "CustomKeyStoreName": "ExampleXksVpc",
      "ConnectionState": "DISCONNECTED",
      "CreationDate": "2022-12-13T18:34:10.675000+00:00",
      "CustomKeyStoreType": "EXTERNAL_KEY_STORE",
      "XksProxyConfiguration": {
        "AccessKeyId": "ABCDE98765432EXAMPLE",
        "Connectivity": "VPC_ENDPOINT_SERVICE",
        "UriEndpoint": "https://example-proxy-uri-endpoint-vpc",
        "UriPath": "/example/prefix/kms/xks/v1",
        "VpcEndpointServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-example"
      }
    }
  ]
}
```

Eliminazione di un archivio delle chiavi esterne

Quando elimini un archivio delle chiavi esterne, AWS KMS rimuove tutti i metadati relativi a tale archivio da AWS KMS, incluse le informazioni relative al proxy dell'archivio delle chiavi esterne. Questa operazione non influisce sul proxy dell'archivio delle chiavi esterne, sul gestore delle chiavi esterne, sulle chiavi esterne o sulle risorse AWS create per supportare l'archivio, come Amazon VPC o un servizio endpoint VPC.

Prima di eliminare un archivio delle chiavi esterne, devi eliminare tutte le chiavi KMS dall'archivio delle chiavi e disconnettere l'archivio dal relativo proxy. In caso contrario, i tentativi di eliminare l'archivio delle chiavi hanno esito negativo.

L'operazione di eliminazione di un archivio delle chiavi esterne è irreversibile, tuttavia puoi creare un nuovo archivio e associarlo allo stesso proxy dell'archivio delle chiavi esterne e allo stesso gestore delle chiavi esterne. Non puoi tuttavia ricreare le chiavi KMS di crittografia simmetrica nell'archivio delle chiavi esterne, anche se hai accesso allo stesso materiale delle chiavi esterne. AWS KMS include i metadati nel testo criptato simmetrico univoco per ogni chiave KMS. Questa funzionalità di sicurezza garantisce che solo la chiave KMS che ha crittografato i dati possa decrittografarli.

Anziché eliminare l'archivio delle chiavi esterne, puoi disconnetterlo. Quando un archivio delle chiavi esterne è disconnesso, puoi gestire l'archivio e le relative AWS KMS keys, ma non puoi creare o utilizzare le chiavi KMS nell'archivio delle chiavi esterne. Puoi ricollegare l'archivio delle chiavi esterne in qualsiasi momento e utilizzare le chiavi KMS per crittografare e decrittografare i dati. Non è previsto alcun costo per un proxy dell'archivio delle chiavi esterne disconnesso o per le relative chiavi KMS non disponibili.

Argomenti

- Eliminazione di un archivio delle chiavi esterne (console)
- Eliminazione di un archivio delle chiavi esterne (API)

Eliminazione di un archivio delle chiavi esterne (console)

Puoi utilizzare la console AWS KMS per eliminare un archivio delle chiavi esterne.

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel pannello di navigazione, scegli Custom key stores (Archivi delle chiavi personalizzate), External key stores (Archivi delle chiavi esterne).
4. Trova la riga che rappresenta l'archivio delle chiavi esterne da rimuovere. Se la voce Connection state (Stato connessione) dell'archivio delle chiavi esterne non è DISCONNECTED (DISCONNESSO), devi disconnettere l'archivio delle chiavi esterne prima di eliminarlo.
5. Dal menu Key store actions (Operazioni per l'archivio delle chiavi), scegli Delete (Elimina).

Se l'operazione riesce, viene visualizzato un messaggio di conferma e l'archivio delle chiavi esterne non è più visualizzato nel relativo elenco. Se l'operazione ha esito negativo, viene visualizzato un

messaggio di errore che descrive il problema e fornisce istruzioni su come risolverlo. Per ulteriori informazioni, consulta Risoluzione dei problemi relativi all'archivio delle chiavi esterne.

Eliminazione di un archivio delle chiavi esterne (API)

Per eliminare un archivio di chiavi esterno, utilizzare l'DeleteCustomKeyStoreoperazione. Se l'operazione ha esito positivo, AWS KMS restituisce una risposta HTTP 200 e un oggetto JSON senza proprietà.

Per iniziare, disconnetti l'archivio delle chiavi esterne. Prima di eseguire questo comando, sostituisci l'ID store chiavi personalizzate di esempio con uno valido.

```
$ aws kms disconnect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

Dopo aver disconnesso l'archivio chiavi esterno, è possibile utilizzare l'DeleteCustomKeyStoreoperazione per eliminarlo.

```
$ aws kms delete-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

Per confermare che l'archivio chiavi esterno è stato eliminato, utilizzare l'DescribeCustomKeyStoresoperazione.

```
$ aws kms describe-custom-key-stores

{
    "CustomKeyStores": []
}
```

Se specifichi un nome o ID che non esiste più, AWS KMS restituisce un'eccezione `CustomKeyStoreNotFoundException`.

```
$ aws kms describe-custom-key-stores --custom-key-store-id cks-1234567890abcdef0

An error occurred (CustomKeyStoreNotFoundException) when calling the
 DescribeCustomKeyStore operation:
```

Gestione di chiavi KMS in un archivio delle chiavi esterne

Per creare, visualizzare, gestire, utilizzare e pianificare l'eliminazione delle chiavi KMS in un archivio delle chiavi esterne, puoi utilizzare procedure molto simili a quelle impiegate per altre chiavi KMS.

Tuttavia, durante la creazione di una chiave KMS in un archivio delle chiavi esterne, specifica un archivio delle chiavi esterne e una chiave esterna. Quando utilizzi una chiave KMS in un archivio delle chiavi esterne, le operazioni di crittografia e decrittografia vengono eseguite dal gestore delle chiavi esterne utilizzando la chiave esterna specificata.

AWS KMS non è in grado di creare, visualizzare, aggiornare o eliminare le chiavi crittografiche nel gestore delle chiavi esterne. AWS KMS non accede mai direttamente al gestore delle chiavi esterne o a qualsiasi chiave esterna. Tutte le richieste relative alle operazioni di crittografia sono mediate dal proxy dell'archivio delle chiavi esterne. Per utilizzare una chiave KMS in un archivio delle chiavi esterne, l'archivio che ospita la chiave KMS deve essere connesso al relativo proxy dell'archivio delle chiavi esterne.

Funzionalità supportate

Oltre alle procedure discusse in questa sezione, puoi eseguire le seguenti operazioni con le chiavi KMS in un archivio delle chiavi esterne:

- Utilizzare le policy delle chiavi, le policy IAM e le concessioni per autorizzare l'accesso alle chiavi KMS.
- Abilitare e disabilitare le chiavi KMS. Queste azioni non influiscono sulla chiave esterna nel gestore delle chiavi esterne.
- Assegnare tag, creare alias e utilizzare il controllo degli accessi basato su attributi (ABAC) per autorizzare l'accesso alle chiavi KMS.
- Utilizzare le chiavi KMS con Servizi AWS che si integrano con AWS KMS e supportano le chiavi gestite dal cliente.

Caratteristiche non supportate

- Gli archivi delle chiavi esterne supportano solo chiavi KMS di crittografia simmetrica. Non puoi creare chiavi KMS HMAC o chiavi KMS asimmetriche in un archivio delle chiavi esterne.
- GenerateDataKeyPaire non GenerateDataKeyPairWithoutPlaintextsono supportati sulle chiavi KMS in un archivio chiavi esterno.
- Non puoi utilizzare un modello AWS CloudFormation per creare un archivio delle chiavi esterne o una chiave KMS all'interno di esso.
- Le chiavi multi-regione non sono supportate in un archivio delle chiavi esterne.
- Le chiavi KMS con materiale della chiave importato non sono supportate in un archivio delle chiavi esterne.

- La rotazione automatica delle chiavi non è supportata per le chiavi KMS in un archivio delle chiavi esterne.

Argomenti

- Creazione di chiavi KMS in un archivio delle chiavi esterne
- Visualizzazione delle chiavi KMS in un archivio delle chiavi esterne
- Utilizzo delle chiavi KMS in un archivio delle chiavi esterne
- Pianificazione dell'eliminazione di chiavi KMS da un archivio delle chiavi esterne

Creazione di chiavi KMS in un archivio delle chiavi esterne

Dopo aver creato e collegato l'archivio delle chiavi esterne, puoi creare le AWS KMS keys. Devono essere chiavi KMS con crittografia simmetrica con un valore di origine impostato su External key store (Archivio delle chiavi esterne) (`EXTERNAL_KEY_STORE`). Non è possibile creare chiavi KMS asimmetriche, chiavi KMS HMAC o chiavi KMS con materiale della chiave importato in un archivio delle chiavi personalizzate. Inoltre, non è possibile utilizzare chiavi KMS di crittografia simmetrica in un archivio delle chiavi personalizzate per generare coppie di chiavi di dati asimmetriche.

Una chiave KMS in un archivio delle chiavi esterne potrebbe avere una latenza, una durata e una disponibilità inferiori rispetto a una chiave KMS standard, perché dipende da componenti situati al di fuori di AWS. Prima di creare o utilizzare una chiave KMS in un archivio delle chiavi esterne, verifica che sia necessaria una chiave con proprietà di archivio delle chiavi esterne.

> **Note**
>
> Alcuni gestori delle chiavi esterne offrono un metodo più semplice per creare chiavi KMS in un archivio delle chiavi esterne. Per ulteriori informazioni, consulta la documentazione del gestore delle chiavi esterne.

Per creare una chiave KMS nell'archivio delle chiavi esterne, devi specificare quanto segue:

- L'ID dell'archivio delle chiavi esterne.
- Un'origine del materiale della chiave con valore External key store (Archivio delle chiavi esterne) (`EXTERNAL_KEY_STORE`).

- L'ID di una chiave esterna esistente nel gestore delle chiavi esterne associato all'archivio delle chiavi esterne. Questa chiave esterna funge da materiale della chiave per la chiave KMS. Non puoi modificare l'ID della chiave esterna dopo aver creato la chiave KMS.

  AWS KMS fornisce l'ID della chiave esterna al proxy dell'archivio delle chiavi esterne nelle richieste di operazioni di crittografia e decrittografia. AWS KMS non può accedere direttamente al gestore delle chiavi esterne o alle relative chiavi crittografiche.

Oltre alla chiave esterna, una chiave KMS in un archivio delle chiavi esterne contiene anche il materiale della chiave di AWS KMS. Tutti i dati crittografati con la chiave KMS vengono prima crittografati in AWS KMS utilizzando il materiale della chiave di AWS KMS e quindi dal gestore delle chiavi esterne tramite la chiave esterna. Questo processo di doppia crittografia garantisce che il testo criptato protetto da una chiave KMS in un archivio delle chiavi esterne sia almeno altrettanto sicuro del testo criptato protetto solo da AWS KMS. Per informazioni dettagliate, vedi Funzionamento degli archivi delle chiavi esterne.

Quando l'operazione `CreateKey` ha esito positivo, lo stato chiave della nuova chiave KMS è `Enabled`. Quando visualizzi una chiave KMS in un archivio delle chiavi esterne puoi vedere proprietà tipiche, come l'ID, le specifiche della chiave, nonché l'utilizzo della chiave, lo stato della chiave e la data di creazione. Puoi inoltre visualizzare l'ID e lo stato di connessione dell'archivio delle chiavi esterne e l'ID della chiave esterna.

Se il tentativo di creare una chiave KMS nell'archivio delle chiavi esterne ha esito negativo, utilizza il messaggio di errore per determinarne la causa. Potrebbe indicare che l'archivio delle chiavi esterne non è connesso (`CustomKeyStoreInvalidStateException`), che il proxy dell'archivio delle chiavi esterne non è in grado di trovare una chiave esterna con l'ID della chiave esterna specificato (`XksKeyNotFoundException`) o che la chiave esterna è già associata a una chiave KMS nello stesso archivio con l'eccezione `XksKeyAlreadyInUseException`.

.

Per un esempio del log AWS CloudTrail dell'operazione che crea una chiave KMS in un archivio delle chiavi esterne, consulta CreateKey.

Argomenti

- Requisiti per una chiave KMS in un archivio delle chiavi esterne
- Creazione di una chiave KMS in un archivio delle chiavi esterne (console)
- Creazione di una chiave KMS in un archivio delle chiavi esterne (API AWS KMS)

Requisiti per una chiave KMS in un archivio delle chiavi esterne

Per creare una chiave KMS in un archivio delle chiavi esterne, sono necessarie le seguenti proprietà dell'archivio delle chiavi esterne, della chiave KMS e della chiave esterna che funge da materiale della chiave crittografica esterna per la chiave KMS.

Requisiti dell'archivio delle chiavi esterne

- Deve essere collegato al relativo proxy dell'archivio delle chiavi esterne.

  Per visualizzare lo stato di connessione dell'archivio delle chiavi esterne, consulta Visualizzazione di un archivio delle chiavi esterne. Per connettere l'archivio delle chiavi esterne, consulta Connessione e disconnessione di un archivio delle chiavi esterne.

Requisiti della chiave KMS

Dopo aver creato la chiave KMS, non puoi più modificare queste proprietà.

- Specifica della chiave SYMMETRIC_DEFAULT
- Utilizzo della chiave: ENCRYPT_DECRYPT
- Origine del materiale della chiave: EXTERNAL_KEY_STORE
- Multi regione: FALSE

Requisiti della chiave esterna

- Chiave crittografica AES a 256 bit (256 bit casuali). Il valore di `KeySpec` per la chiave esterna deve essere `AES_256`.
- Attivata e disponibile per l'uso. Il valore di `Status` per la chiave esterna deve essere `ENABLED`.
- Configurata per la crittografia e la decrittografia. Il valore di `KeyUsage` per la chiave esterna deve includere `ENCRYPT` e `DECRYPT`.
- Utilizzata solo con questa chiave KMS. Ciascuna `KMS key` in un archivio delle chiavi esterne deve essere associata a una chiave esterna diversa.

  AWS KMS consiglia inoltre di utilizzare la chiave esterna esclusivamente per l'archivio delle chiavi esterne. Questa restrizione semplifica l'identificazione e la risoluzione dei problemi relativi alla chiave.
- Accessibile dal proxy dell'archivio delle chiavi esterne per l'archivio delle chiavi esterne.

Se il proxy dell'archivio delle chiavi esterne non riesce a trovare la chiave utilizzando l'ID della chiave esterna specificato, l'operazione `CreateKey` ha esito negativo.

- È in grado di gestire il traffico previsto generato dall'utilizzo degli Servizi AWS. AWS KMS consiglia di preparare le chiavi esterne per gestire fino a 1.800 richieste al secondo.

Creazione di una chiave KMS in un archivio delle chiavi esterne (console)

Esistono due modi per creare una chiave KMS in un archivio delle chiavi esterne.

- Metodo 1 (consigliato): scegli un archivio di chiavi esterno e crea una chiave KMS all'interno dell'archivio di chiavi esterno.
- Metodo 2: crea una chiave KMS e indica che si trova in un archivio di chiavi esterno.

Se utilizzi il metodo 1, con cui scegli l'archivio di chiavi esterno prima di creare la chiave, AWS KMS seleziona automaticamente tutte le proprietà della chiave KMS richieste e inserisce l'ID dell'archivio di chiavi esterno. Questo metodo evita errori che potrebbero verificarsi durante la creazione della chiave KMS.

> **Note**
>
> Non includere informazioni riservate o sensibili nell'alias, nella descrizione o nei tag. Questi campi possono apparire in testo semplice nei CloudTrail log e in altri output.

Metodo 1 (consigliato): inizia dall'archivio di chiavi esterno

Per utilizzare questo metodo, scegli l'archivio delle chiavi esterne, quindi crea una chiave KMS. La console AWS KMS sceglie automaticamente tutte le proprietà richieste e inserisce l'ID dell'archivio delle chiavi esterne. Questo metodo evita molti errori che potrebbero verificarsi durante la creazione della chiave KMS.

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel pannello di navigazione, scegli Custom key stores (Archivi delle chiavi personalizzate), External key stores (Archivi delle chiavi esterne).

4. Scegli il nome dell'archivio delle chiavi esterne.
5. Nell'angolo in alto a destra, scegli Create a KMS key in this key store (Crea una chiave KMS in questo archivio delle chiavi).

   Se l'archivio delle chiavi esterne non è connesso, ti verrà richiesto di collegarlo. Se il tentativo di connessione fallisce, è necessario risolvere il problema e connettere l'archivio delle chiavi esterne prima di poter creare una nuova chiave KMS al suo interno.

   Se l'archivio delle chiavi esterne è connesso, verrai reindirizzato alla pagina Customer managed keys (Chiavi gestite dal cliente) per creare una chiave. I valori di Key configuration (Configurazione della chiave) richiesti sono già stati selezionati automaticamente. Inoltre, è già stato inserito l'ID dell'archivio delle chiavi personalizzate per l'archivio delle chiavi esterne, sebbene sia possibile modificarlo.
6. Inserisci l'ID chiave di una chiave esterna nel gestore delle chiavi esterne. Questa chiave esterna deve soddisfare i requisiti per l'uso con una chiave KMS. Non puoi modificare questo valore dopo la creazione della chiave.

   Se la chiave esterna presenta più ID, inserisci l'ID chiave utilizzato dal proxy dell'archivio delle chiavi esterne per identificare la chiave esterna.
7. Conferma che intendi creare una chiave KMS nell'archivio delle chiavi esterne specificato.
8. Seleziona Avanti.

   Il resto di questa procedura è uguale alla creazione di una chiave KMS standard.
9. Digita un alias (obbligatorio) e, facoltativamente, una descrizione della chiave KMS.
10. (Facoltativo). Nella pagina Add Tags (Aggiungi tag), aggiungi i tag che identificano o categorizzano la chiave KMS.

    Quando aggiungi i tag alle risorse AWS, AWS genera un report di allocazione dei costi in cui l'utilizzo e i costi sono aggregati in base ai tag. I tag possono essere utilizzati anche per controllare l'accesso a una chiave KMS. Per informazioni sull'assegnazione di tag delle chiavi KMS, consulta Chiavi di tagging e ABAC per AWS KMS.
11. Seleziona Next (Successivo).
12. Nella sezione amministratori delle chiavi, seleziona utenti IAM e ruoli IAM che possono gestire la chiave KMS. Per ulteriori informazioni, consulta Consente agli amministratori delle chiavi di amministrare la chiave KMS.

> **Note**
>
> Le policy IAM possono fornire ad altri ruoli e utenti IAM l'autorizzazione per utilizzare la chiave KMS.
> Le best practice di IAM disincentivano l'uso di utenti IAM con credenziali a lungo termine. Quando possibile, utilizza i ruoli IAM che forniscono credenziali temporanee. Per i dettagli, consulta la sezione Best practice di sicurezza in IAM nella Guida per l'utente IAM.

13. (Facoltativo) Per impedire a questi amministratori delle chiavi di eliminare tale chiave KMS, deseleziona la casella di controllo Allow key administrators to delete this key. (Consenti agli amministratori delle chiavi di eliminare questa chiave).

    L'eliminazione di una chiave KMS è un'operazione distruttiva e irreversibile che può rendere il testo criptato irrecuperabile. Non puoi ricreare una chiave KMS simmetrica in un archivio delle chiavi esterne, anche se disponi del materiale della chiave. L'eliminazione di una chiave KMS non ha alcun effetto sulla chiave esterna associata. Per informazioni sull'eliminazione di una chiave KMS da un archivio delle chiavi esterne, consulta Pianificazione dell'eliminazione di chiavi KMS da un archivio delle chiavi esterne.
14. Seleziona Avanti.
15. Nella sezione Questo account, seleziona i ruoli e gli utenti IAM in questo Account AWS che possono utilizzare la chiave KMS nelle operazioni di crittografia. Per ulteriori informazioni, consulta Consente agli utenti della chiave di utilizzare la chiave KMS.

    > **Note**
    >
    > Le policy IAM possono fornire ad altri ruoli e utenti IAM l'autorizzazione per utilizzare la chiave KMS.
    > Le best practice di IAM disincentivano l'uso di utenti IAM con credenziali a lungo termine. Quando possibile, utilizza i ruoli IAM che forniscono credenziali temporanee. Per i dettagli, consulta la sezione Best practice di sicurezza in IAM nella Guida per l'utente IAM.
16. (Facoltativo) È possibile consentire ad altri Account AWS di utilizzare questa chiave KMS per operazioni di crittografia. A questo proposito, nella sezione Altri Account AWS, nella parte

inferiore della pagina, scegli Aggiungi un altro Account AWS e inserisci l'ID Account AWS di un account esterno. Per aggiungere più account esterni, ripetere questo passaggio.

> **Note**
>
> Anche gli amministratori degli altri Account AWS devono consentire l'accesso alla chiave KMS creando policy IAM per i propri utenti. Per ulteriori informazioni, consulta la pagina Autorizzazione per gli utenti in altri account di utilizzare una chiave KMS.

17. Seleziona Next (Successivo).
18. Esaminare le principali impostazioni scelte. È comunque possibile tornare indietro e modificare tutte le impostazioni.
19. Al termine, scegli Crea filtro.

Metodo 2: inizia dalle chiavi gestite dal cliente

Questa procedura è identica alla procedura per creare una chiave crittografica simmetrica con il materiale della chiave di AWS KMS. Tuttavia, in questa procedura puoi specificare l'ID dell'archivio delle chiavi personalizzate dell'archivio delle chiavi esterne e l'ID chiave della chiave esterna. Puoi inoltre specificare i valori delle proprietà richiesti per una chiave KMS in un archivio delle chiavi esterne, come le specifiche e l'utilizzo della chiave.

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.
4. Scegliere Create key (Crea chiave).
5. Scegliere Symmetric (Simmetrica).
6. In Key usage (Utilizzo della chiave), l'opzione Encrypt and decrypt (Crittografa e decrittografa) è selezionata per default. Non modificarla.
7. Scegliere Advanced options (Opzioni avanzate).
8. In Key material origin (Origine del materiale della chiave), scegli External key store (Archivio delle chiavi esterne).
9. Conferma che intendi creare una chiave KMS nell'archivio delle chiavi esterne specificato.

10. Seleziona Avanti.
11. Scegli la riga che rappresenta l'archivio delle chiavi esterne per la nuova chiave KMS.

    Non puoi scegliere un archivio delle chiavi esterne disconnesso. Per connettere un archivio delle chiavi disconnesso, scegli il nome dell'archivio, quindi in Key store actions (Operazioni per l'archivio delle chiavi), scegli Connect (Connetti). Per informazioni dettagliate, vedi Connessione di un archivio delle chiavi esterne (console).
12. Inserisci l'ID chiave di una chiave esterna nel gestore delle chiavi esterne. Questa chiave esterna deve soddisfare i requisiti per l'uso con una chiave KMS. Non puoi modificare questo valore dopo la creazione della chiave.

    Se la chiave esterna presenta più ID, inserisci l'ID chiave utilizzato dal proxy dell'archivio delle chiavi esterne per identificare la chiave esterna.
13. Seleziona Avanti.

    Il resto di questa procedura è uguale alla creazione di una chiave KMS standard.
14. Digita un alias ed eventualmente una descrizione per la chiave KMS.
15. (Facoltativo). Nella pagina Add Tags (Aggiungi tag), aggiungi i tag che identificano o categorizzano la chiave KMS.

    Quando aggiungi i tag alle risorse AWS, AWS genera un report di allocazione dei costi in cui l'utilizzo e i costi sono aggregati in base ai tag. I tag possono essere utilizzati anche per controllare l'accesso a una chiave KMS. Per informazioni sull'assegnazione di tag delle chiavi KMS, consulta Chiavi di tagging e ABAC per AWS KMS.
16. Seleziona Next (Successivo).
17. Nella sezione amministratori delle chiavi, seleziona utenti IAM e ruoli IAM che possono gestire la chiave KMS. Per ulteriori informazioni, consulta Consente agli amministratori delle chiavi di amministrare la chiave KMS.

    > **Note**
    >
    > Le policy IAM possono fornire ad altri ruoli e utenti IAM l'autorizzazione per utilizzare la chiave KMS.
18. (Facoltativo) Per impedire a questi amministratori delle chiavi di eliminare tale chiave KMS, deseleziona la casella di controllo Allow key administrators to delete this key. (Consenti agli amministratori delle chiavi di eliminare questa chiave).

L'eliminazione di una chiave KMS è un'operazione distruttiva e irreversibile che può rendere il testo criptato irrecuperabile. Non puoi ricreare una chiave KMS simmetrica in un archivio delle chiavi esterne, anche se disponi del materiale della chiave. L'eliminazione di una chiave KMS non ha alcun effetto sulla chiave esterna associata. Per informazioni sull'eliminazione di una chiave KMS da un archivio delle chiavi esterne, consulta Pianificazione dell'eliminazione di chiavi KMS da un archivio delle chiavi esterne.

19. Seleziona Avanti.
20. Nella sezione Questo account, seleziona i ruoli e gli utenti IAM in questo Account AWS che possono utilizzare la chiave KMS nelle operazioni di crittografia. Per ulteriori informazioni, consulta Consente agli utenti della chiave di utilizzare la chiave KMS.

> **Note**
>
> Le policy IAM possono fornire ad altri ruoli e utenti IAM l'autorizzazione per utilizzare la chiave KMS.

21. (Facoltativo) È possibile consentire ad altri Account AWS di utilizzare questa chiave KMS per operazioni di crittografia. A questo proposito, nella sezione Altri Account AWS, nella parte inferiore della pagina, scegli Aggiungi un altro Account AWS e inserisci l'ID Account AWS di un account esterno. Per aggiungere più account esterni, ripetere questo passaggio.

> **Note**
>
> Anche gli amministratori degli altri Account AWS devono consentire l'accesso alla chiave KMS creando policy IAM per i propri utenti. Per ulteriori informazioni, consulta la pagina Autorizzazione per gli utenti in altri account di utilizzare una chiave KMS.

22. Seleziona Next (Successivo).
23. Esaminare le principali impostazioni scelte. È comunque possibile tornare indietro e modificare tutte le impostazioni.
24. Al termine, scegli Crea filtro.

Quando la procedura riesce, la visualizzazione mostra la nuova chiave KMS nell'archivio delle chiavi esterne che hai scelto. Quando scegli il nome o l'alias della nuova chiave KMS, la scheda Cryptographic configuration (Configurazione crittografica) nella relativa pagina dei dettagli visualizza l'origine della chiave KMS (External key store [Archivio delle chiavi esterne]), il nome, l'ID e il tipo

dell'archivio delle chiavi personalizzate, nonché l'ID, l'utilizzo della chiave e lo stato della chiave esterna. Se la procedura ha esito negativo, viene visualizzato un messaggio di errore che descrive l'errore. Per , consulta Risoluzione dei problemi relativi all'archivio delle chiavi esterne.

> **Tip**
>
> Per agevolare l'identificazione delle chiavi KMS in un archivio delle chiavi personalizzate, nella pagina Customer managed keys (Chiavi gestite dal cliente), aggiungi il campo Origin (Origine) e la colonna Custom key store ID (ID dell'archivio chiavi personalizzate) alla visualizzazione. Per modificare i campi della tabella, scegli l'icona a forma di ingranaggio nell'angolo in alto a destra della pagina. Per informazioni dettagliate, vedi Personalizzazione delle tabelle delle chiavi KMS.

Creazione di una chiave KMS in un archivio delle chiavi esterne (API AWS KMS)

Per creare una nuova chiave KMS in un archivio di chiavi esterno, usa l'CreateKeyoperazione. I parametri seguenti sono obbligatori:

- Il valore `Origin` deve essere `EXTERNAL_KEY_STORE`.
- Il parametro `CustomKeyStoreId` identifica l'archivio delle chiavi esterne. Il valore di `ConnectionState` per l'archivio delle chiavi esterne specificato deve essere `CONNECTED`. Per trovare `CustomKeyStoreId` e `ConnectionState`, usa l'operazione `DescribeCustomKeyStores`.
- Il parametro `XksKeyId` identifica la chiave esterna. Tale chiave deve soddisfare i requisiti per l'associazione a una chiave KMS.

Puoi inoltre utilizzare uno qualsiasi dei parametri facoltativi dell'operazione `CreateKey`, ad esempio `Policy` o i parametri Tags (Tag).

> **Note**
>
> Non includere informazioni riservate o sensibili nei campi `Description` o `Tags`. Questi campi possono apparire in testo semplice nei CloudTrail log e in altri output.

Gli esempi in questa sezione utilizzano AWS Command Line Interface (AWS CLI), ma puoi usare anche qualsiasi linguaggio di programmazione supportato.

Questo comando di esempio utilizza l'CreateKeyoperazione per creare una chiave KMS in un archivio di chiavi esterno. La risposta include le proprietà delle chiavi KMS, l'ID dell'archivio delle chiavi esterne e l'ID, l'utilizzo e lo stato della chiave esterna. Per informazioni dettagliate su questi campi, consulta Visualizzazione delle chiavi KMS in un archivio delle chiavi esterne.

Prima di eseguire questo comando, sostituisci l'ID store chiavi personalizzate di esempio con un ID valido.

```
$ aws kms create-key --origin EXTERNAL_KEY_STORE --custom-key-store-
id cks-1234567890abcdef0 --xks-key-id bb8562717f809024
{
  "KeyMetadata": {
    "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "AWSAccountId": "111122223333",
    "CreationDate": "2022-12-02T07:48:55-07:00",
    "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
    "CustomKeyStoreId": "cks-1234567890abcdef0",
    "Description": "",
    "Enabled": true,
    "EncryptionAlgorithms": [
      "SYMMETRIC_DEFAULT"
    ],
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "KeyManager": "CUSTOMER",
    "KeySpec": "SYMMETRIC_DEFAULT",
    "KeyState": "Enabled",
    "KeyUsage": "ENCRYPT_DECRYPT",
    "MultiRegion": false,
    "Origin": "EXTERNAL_KEY_STORE",
    "XksKeyConfiguration": {
      "Id": "bb8562717f809024"
    }
  }
}
```

Visualizzazione delle chiavi KMS in un archivio delle chiavi esterne

Per visualizzare le chiavi KMS in un archivio chiavi esterno, usa la AWS KMS console o l'DescribeKeyoperazione. Puoi utilizzare le stesse tecniche impiegate per visualizzare le chiavi gestite dal cliente di AWS KMS. Per le nozioni di base sulla visualizzazione di chiavi, consulta Visualizzazione di chiavi.

Nella console AWS KMS, le chiavi KMS nell'archivio delle chiavi esterne vengono visualizzate nella pagina Customer managed keys (Chiavi gestite dal cliente), insieme a tutte le altre chiavi gestite dal cliente presenti in un Account AWS e nella regione. Per identificare le chiavi KMS in un archivio delle chiavi esterne, filtra in base al valore di origine distintivo, all'archivio delle chiavi esterne e all'ID dell'archivio delle chiavi personalizzate.

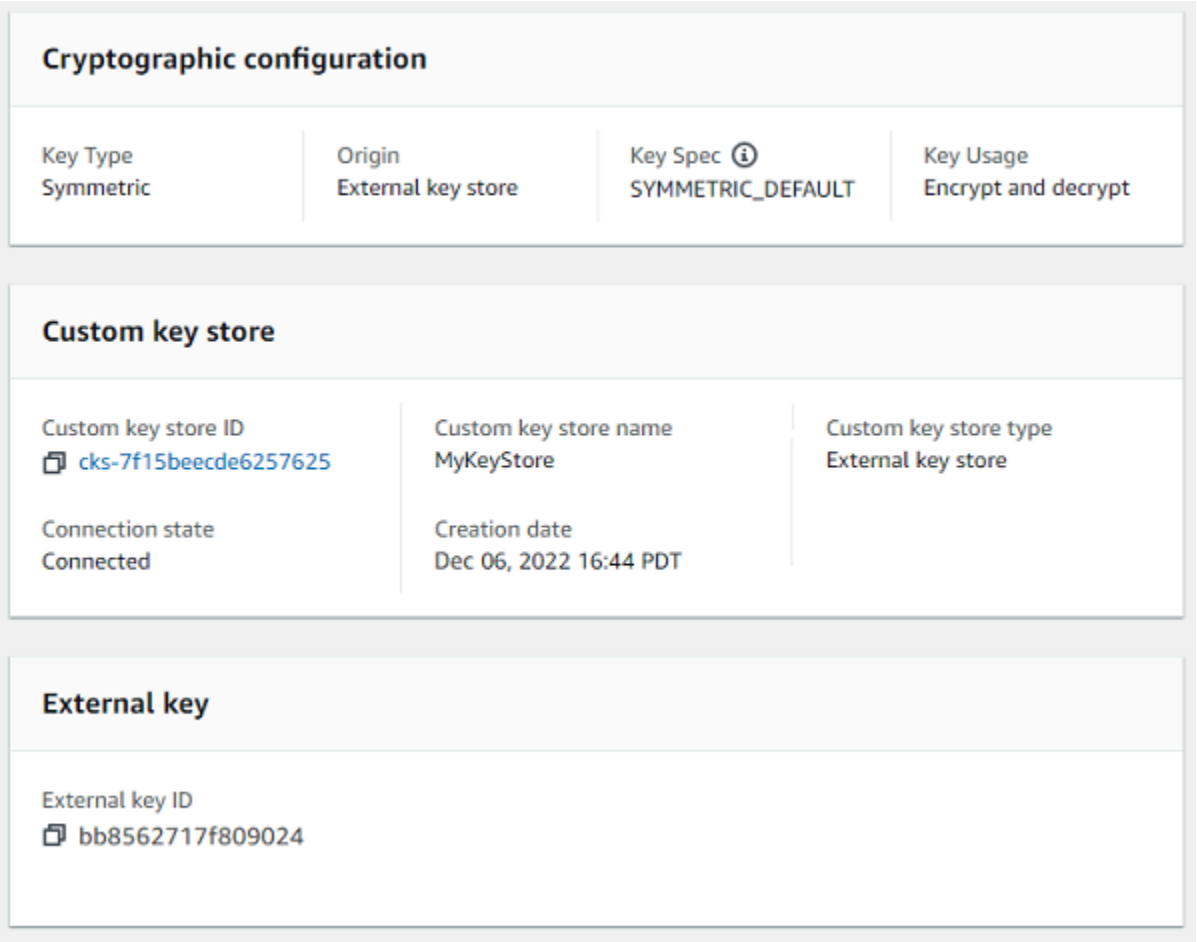
Per ulteriori informazioni, consulta Visualizzazione di un archivio delle chiavi esterne, Monitoraggio di un archivio delle chiavi esterne e Registrazione delle chiamate API AWS KMS con AWS CloudTrail.

Argomenti

Proprietà delle chiavi KMS in un archivio delle chiavi esterne

Come tutte le chiavi KMS, le chiavi KMS in un archivio delle chiavi esterne presentano un ARN chiave, una specifica della chiave e valori di utilizzo della chiave, ma hanno anche proprietà e valori di proprietà specifici per le chiavi KMS. Ad esempio, il valore Origin (Origine) per tutte le chiavi KMS negli archivi delle chiavi esterne è External key store (Archivio delle chiavi esterne).

Per una chiave KMS in un archivio delle chiavi esterne, la scheda Cryptographic configuration (Configurazione crittografica) della console AWS KMS include due sezioni aggiuntive: Custom key store (Archivio delle chiavi personalizzate) e External key (Chiave esterna).



Proprietà dell'archivio delle chiavi personalizzate

I seguenti valori vengono visualizzati nella sezione Archivio chiavi personalizzate della scheda Configurazione crittografica e nella DescribeKeyrisposta. Queste proprietà si applicano a tutti gli archivi delle chiavi personalizzate, inclusi gli archivi delle chiavi di AWS CloudHSM e gli archivi delle chiavi esterne.

ID dello store delle chiavi personalizzate

Un ID univoco che AWS KMS assegna all'archivio delle chiavi personalizzate.

Il nome dello store delle chiavi personalizzate

Nome descrittivo assegnato all'archivio delle chiavi personalizzate durante la sua creazione. Puoi modificare questo valore in qualsiasi momento.

Tipo di archivio delle chiavi personalizzate

Il tipo di archivio delle chiavi personalizzate. I valori validi sono AWS CloudHSM (`AWS_CLOUDHSM`) o External key store (Archivio delle chiavi esterne) (`EXTERNAL_KEY_STORE`). Il tipo di archivio non può essere modificato dopo la creazione.

Data di creazione

La data in cui è stato creato l'archivio delle chiavi personalizzate. Questa data viene visualizzata nell'ora locale per la Regione AWS.

Stato connessione

Indica se l'archivio delle chiavi personalizzate è connesso al relativo archivio del materiale della chiave. Lo stato della connessione è `DISCONNECTED` solo se l'archivio delle chiavi personalizzate non è mai stato collegato al relativo archivio del materiale della chiave o se è stato disconnesso intenzionalmente. Per informazioni dettagliate, vedi the section called “Stato connessione”.

Proprietà della chiave esterna

Le proprietà della chiave esterna vengono visualizzate nella sezione Chiave esterna della scheda Configurazione crittografica e nell'`XksKeyConfiguration`elemento della DescribeKeyrisposta.

La sezione External key (Chiave esterna) viene visualizzata nella console AWS KMS solo per le chiavi KMS negli archivi delle chiavi esterne. Fornisce informazioni sulla chiave esterna associata alla chiave KMS. La chiave esterna è una chiave crittografica al di fuori di AWS che funge da materiale della chiave per la chiave KMS nell'archivio delle chiavi esterne. Quando si crittografa o si decrittografa con la chiave KMS, l'operazione viene eseguita dal gestore delle chiavi esterne utilizzando la chiave esterna specificata.

I seguenti valori vengono visualizzati nella sezione External key (Chiave esterna).

ID chiave esterna

L'identificatore della chiave esterna nel relativo gestore delle chiavi esterne. Si tratta del valore utilizzato dal proxy dell'archivio delle chiavi esterne per identificare la chiave esterna. Puoi specificare l'ID della chiave esterna in fase di creazione della chiave KMS e non puoi modificarla in seguito. Se il valore dell'ID della chiave esterna utilizzato per creare la chiave KMS cambia o diventa non valido, è necessario pianificare l'eliminazione della chiave KMS e creare una nuova chiave KMS con il valore ID della chiave esterna corretto.

Visualizzazione delle chiavi KMS in un archivio delle chiavi esterne (console)

Per visualizzare le chiavi KMS in un archivio delle chiavi esterne (console)

1. Aprire la console AWS KMS all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.
4. Per identificare le chiavi KMS nell'archivio delle chiavi esterne, aggiungi i campi Origin (Origine) e Custom key store ID (ID dell'archivio chiavi personalizzate) alla tabella delle chiavi. Le chiavi KMS in un archivio delle chiavi esterne hanno un valore Origin (Origine) impostato su External key store (Archivio delle chiavi esterne).

   Nell'angolo in alto a destra, scegli l'icona a forma di ingranaggio, seleziona Origin (Origine) e Custom key store ID (ID dell'archivio chiavi personalizzate), quindi scegli Confirm (Conferma).
5. Scegli l'alias o l'ID chiave di una chiave KMS in un archivio delle chiavi esterne.
6. Per visualizzare le proprietà specifiche delle chiavi KMS in un archivio delle chiavi esterne, scegli la scheda Cryptographic configuration (Configurazione crittografica). I valori speciali per le chiavi KMS in un archivio delle chiavi esterne vengono visualizzati nelle sezioni Custom key store (Archivio delle chiavi personalizzate) e External key (Chiave esterna).

Visualizzazione delle chiavi KMS in un archivio delle chiavi esterne (API AWS KMS)

Per visualizzare le chiavi KMS in un archivio delle chiavi esterne (API)

Utilizzi le stesse operazioni AWS KMS API per visualizzare le chiavi KMS in un archivio di chiavi esterno che utilizzeresti per qualsiasi chiave KMS, tra cui ListKeys, DescribeKeye. GetKeyPolicy Ad esempio, l'operazione `describe-key` seguente nella AWS CLI mostra i campi speciali per una chiave KMS in un archivio delle chiavi esterne. Prima di eseguire un comando come questo, sostituisci l'ID della chiave KMS di esempio con un valore valido.

```
$ aws kms describe-key --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
{
  "KeyMetadata": {
    "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "AWSAccountId": "111122223333",
    "CreationDate": "2022-12-02T07:48:55-07:00",
    "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
```

```
    "CustomKeyStoreId": "cks-1234567890abcdef0",
    "Description": "",
    "Enabled": true,
    "EncryptionAlgorithms": [
      "SYMMETRIC_DEFAULT"
    ],
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "KeyManager": "CUSTOMER",
    "KeySpec": "SYMMETRIC_DEFAULT",
    "KeyState": "Enabled",
    "KeyUsage": "ENCRYPT_DECRYPT",
    "MultiRegion": false,
    "Origin": "EXTERNAL_KEY_STORE",
    "XksKeyConfiguration": {
      "Id": "bb8562717f809024"
    }
  }
}
```


Utilizzo delle chiavi KMS in un archivio delle chiavi esterne

Dopo aver creato una chiave KMS di crittografia simmetrica in un archivio delle chiavi esterne, puoi utilizzarla per le seguenti operazioni di crittografia:

- Encrypt
- Decrypt
- GenerateDataKey
- GenerateDataKeyWithoutPlaintext
- ReEncrypt

Le operazioni di crittografia simmetrica che generano coppie di chiavi di dati asimmetriche GenerateDataKeyPaire non sono supportate negli GenerateDataKeyPairWithoutPlaintextarchivi di chiavi personalizzati.

Un contesto di crittografia è supportato per tutte le operazioni di crittografia con chiavi KMS in un archivio delle chiavi esterne. Come sempre, l'utilizzo di un contesto di crittografia rappresenta una best practice di sicurezza consigliata da AWS KMS.

Quando utilizzi la chiave KMS in una richiesta, identifica la chiave KMS in base a ID chiave, ARN chiave, alias o ARN alias. Non è necessario specificare l'archivio delle chiavi esterne. La risposta

include gli stessi campi che vengono restituiti per qualsiasi chiave KMS di crittografia simmetrica. Tuttavia, quando utilizzi una chiave KMS in un archivio delle chiavi esterne, le operazioni di crittografia e decrittografia vengono eseguite dal gestore delle chiavi esterne utilizzando la chiave esterna associata alla chiave KMS.

Per garantire che il testo criptato da una chiave KMS in un archivio delle chiavi esterne sia sicuro almeno quanto un testo criptato da una chiave KMS standard, AWS KMS utilizza la doppia crittografia. I dati vengono prima crittografati in AWS KMS utilizzando il materiale chiave di AWS KMS. Quindi, viene crittografato dal gestore delle chiavi esterne utilizzando la chiave esterna per la chiave KMS. Per decrittografare il testo criptato con doppia crittografia, il testo viene innanzitutto decodificato dal gestore delle chiavi esterno utilizzando la chiave esterna per la chiave KMS. Quindi, viene decodificato in AWS KMS utilizzando il materiale della chiave di AWS KMS per la chiave KMS.

Perché ciò avvenga, devono essere soddisfatte le seguenti condizioni.

- Lo stato di chiave della chiave KMS deve essere `Enabled`. Per trovare lo stato della chiave, consulta il campo Stato per le chiavi gestite dal cliente, la AWS KMSconsole o il `KeyState` campo nella risposta. DescribeKey
- L'archivio delle chiavi esterne che ospita la chiave KMS deve essere connesso al relativo proxy dell'archivio delle chiavi esterne, ovvero lo stato di connessione dell'archivio delle chiavi esterne deve essere `CONNECTED`.

  È possibile visualizzare lo stato della connessione nella pagina Archivi di chiavi esterni della AWS KMS console o nella DescribeCustomKeyStoresrisposta. Lo stato di connessione dell'archivio delle chiavi esterne viene visualizzato anche nella pagina dei dettagli della chiave KMS nella console AWS KMS. Nella pagina dei dettagli, scegli la scheda Cryptographic configuration (Configurazione crittografica) e visualizza il campo Connection state (Stato connessione) nella sezione Custom key store (Archivio delle chiavi personalizzate).

  Se lo stato della connessione è `DISCONNECTED`, devi prima connetterlo. Se lo stato della connessione è `FAILED`, devi risolvere il problema, disconnettere l'archivio delle chiavi esterne e riconnetterlo. Per istruzioni, consulta Connessione e disconnessione di un archivio delle chiavi esterne.
- Il proxy dell'archivio delle chiavi personalizzate deve essere in grado di trovare la chiave esterna.
- La chiave esterna deve essere abilitata e deve eseguire le operazioni di crittografia e decrittografia.

  Lo stato della chiave esterna è indipendente e non influisce sulle modifiche apportate allo stato chiave della chiave KMS, inclusa l'attivazione e la disabilitazione della chiave stessa. Allo stesso

modo, la disabilitazione o l'eliminazione della chiave esterna non modifica lo stato chiave della chiave KMS, ma le operazioni di crittografia che utilizzano la chiave KMS associata avranno esito negativo.

Se queste condizioni non sono soddisfatte, l'operazione di crittografia non riesce e AWS KMS restituisce un'eccezione `KMSInvalidStateException`. Potrebbe essere necessario ricollegare l'archivio delle chiavi esterne o utilizzare gli strumenti di gestione delle chiavi esterne per riconfigurare o riparare la chiave esterna. Per ulteriori informazioni, consulta the section called “Risoluzione dei problemi relativi all'archivio delle chiavi esterne”.

Quando utilizzi le chiavi KMS in un archivio delle chiavi esterne, tieni presente che le chiavi KMS in ogni archivio delle chiavi esterne condividono una quota di richiesta dell'archivio delle chiavi personalizzate per le operazioni di crittografia. Se superi la quota, AWS KMS restituisce una `ThrottlingException`. Per informazioni dettagliate sulle quote di richiesta dell'archivio delle chiavi personalizzate, consulta Quote di richiesta per l'archivio delle chiavi personalizzate.

Pianificazione dell'eliminazione di chiavi KMS da un archivio delle chiavi esterne

Quando si ha la certezza che non si avrà più bisogno di utilizzare una determinata AWS KMS key per le operazioni di crittografia, è possibile pianificare l'eliminazione della chiave KMS. Per farlo, utilizza la stessa procedura che utilizzeresti per programmare l'eliminazione di qualsiasi chiave KMS da AWS KMS. L'eliminazione di una chiave KMS da un archivio delle chiavi esterne non ha alcun effetto sulla chiave esterna utilizzata come materiale della chiave.

Puoi annullare l'eliminazione pianificata di una chiave KMS durante il periodo di attesa obbligatorio, tuttavia una chiave KMS eliminata non è più recuperabile. Non puoi ricreare una chiave KMS di crittografia simmetrica in un archivio delle chiavi esterne, anche se utilizzi la stessa chiave esterna. Poiché ogni chiave KMS simmetrica in un archivio delle chiavi esterne presenta materiali della chiave di AWS KMS e metadati univoci, solo la chiave di AWS KMS che ha crittografato un testo criptato simmetrico può decrittografarlo.

> **Warning**
>
> L'eliminazione di una chiave KMS è un'operazione distruttiva e potenzialmente pericolosa che impedisce il recupero di tutti i dati crittografati con la chiave KMS. Prima di pianificare l'eliminazione della chiave KMS, esamina l'utilizzo passato della chiave KMS e crea un CloudWatch allarme Amazon che ti avvisi quando qualcuno tenta di utilizzare la chiave

KMS mentre è in attesa di eliminazione. Quando possibile, disabilita la chiave KMS anziché eliminarla.

Se pianifichi l'eliminazione di una chiave KMS da un archivio delle chiavi esterne, il relativo stato chiave diventa Pending deletion (Eliminazione in attesa). La chiave KMS rimane nello stato Pending deletion (Eliminazione in attesa) durante l'intero periodo di attesa, anche se la chiave KMS non è più disponibile dopo la disconnessione dell'archivio delle chiavi esterne. Ciò consente di annullare l'eliminazione della chiave KMS in qualsiasi momento durante il periodo di attesa. Alla scadenza del periodo di attesa, AWS KMS elimina la chiave KMS da AWS KMS.

Quando pianifichi l'eliminazione di una chiave KMS da un archivio delle chiavi esterne, la chiave KMS diventa immediatamente inutilizzabile (in base alla coerenza finale). Tuttavia, le risorse crittografate con chiavi di dati protette dalla chiave KMS non sono interessate fino a quando la chiave KMS non viene nuovamente utilizzata, ad esempio per decrittografare la chiave dati. Questo problema riguarda i Servizi AWS, molti dei quali proteggono le risorse tramite le chiavi dati. Per informazioni dettagliate, vedi In che modo le chiavi KMS inutilizzabili influiscono sulle chiavi dati.

Puoi monitorare la pianificazione, la cancellazione e l'eliminazione della chiave KMS nei log di AWS CloudTrail.

Risoluzione dei problemi relativi all'archivio delle chiavi esterne

La risoluzione della maggior parte dei problemi relativi agli archivi delle chiavi esterne è indicata dal messaggio di errore visualizzato da AWS KMS con ogni eccezione o dal codice di errore di connessione restituito da AWS KMS quando un tentativo di connettere l'archivio delle chiavi esterne al relativo proxy ha esito negativo. Tuttavia, alcune questioni sono un po' più complesse.

Durante la diagnosi di un problema con un archivio delle chiavi esterne, individua innanzitutto la causa. Questa operazione consente di restringere la gamma di rimedi e rendere più efficiente la risoluzione dei problemi.

- AWS KMS: il problema potrebbe riguardare AWS KMS, ad esempio un valore errato nella configurazione dell'archivio delle chiavi esterne.
- Esterno: il problema potrebbe avere origine al di fuori di AWS KMS. Sono inclusi i problemi relativi alla configurazione o al funzionamento del proxy dell'archivio delle chiavi esterne, del gestore delle chiavi esterne, delle chiavi esterne o del servizio endpoint VPC.
- Rete: potrebbe trattarsi di un problema di connettività o di rete, ad esempio un problema con l'endpoint proxy, la porta o il nome/dominio DNS privato.

> **Note**
>
> Quando le operazioni di gestione negli archivi delle chiavi esterne hanno esito negativo, generano diverse eccezioni. Tuttavia, le operazioni di crittografia AWS KMS restituiscono l'eccezione `KMSInvalidStateException` per tutti gli errori relativi alla configurazione esterna o allo stato di connessione dell'archivio delle chiavi esterno. Per identificare il problema, utilizza il testo del messaggio di errore allegato.
> L'ConnectCustomKeyStoreoperazione viene completata rapidamente prima del completamento del processo di connessione. Per determinare se il processo di connessione ha esito positivo, visualizza lo stato della connessione dell'archivio delle chiavi esterne. Se il processo di connessione fallisce, AWS KMS restituisce un codice di errore di connessione che spiega la causa e suggerisce una soluzione.

Argomenti

Strumenti per la risoluzione dei problemi degli archivi delle chiavi esterne

AWS KMS offre diversi strumenti per aiutarti a identificare e risolvere i problemi relativi all'archivio delle chiavi esterne e alle relative chiavi. Utilizza questi strumenti insieme alle funzioni fornite con il proxy dell'archivio delle chiavi esterne e il gestore delle chiavi esterne.

> **Note**
>
> Il proxy dell'archivio delle chiavi esterne e il gestore delle chiavi esterne potrebbero fornire metodi più semplici per creare e gestire l'archivio delle chiavi esterne e le relative chiavi KMS. Per ulteriori informazioni, consulta la documentazione degli strumenti esterni.

Eccezioni e messaggi di errore di AWS KMS

AWS KMS fornisce un messaggio di errore dettagliato per qualsiasi problema riscontrato. Puoi trovare ulteriori informazioni sulle eccezioni AWS KMS nei Riferimenti delle API AWS Key Management Service e negli SDK AWS. Tali riferimenti potrebbero rivelarsi utili anche se utilizzi la console AWS KMS. Ad esempio, consulta l'elenco Errori per l'operazione `CreateCustomKeyStores`.

Se il problema si verifica in un servizio AWS diverso, ad esempio quando utilizzi una chiave KMS nell'archivio delle chiavi esterne per proteggere una risorsa in un altro servizio AWS, il servizio AWS potrebbe fornire informazioni aggiuntive per aiutarti a identificare il problema. Se il AWS servizio non fornisce il messaggio, puoi visualizzare il messaggio di errore nei CloudTrail registri che registrano l'uso della tua chiave KMS.

CloudTrail registri

Ogni operazione API AWS KMS, tra cui le azioni nella console AWS KMS, viene registrata nei log di AWS CloudTrail. AWS KMS registra una voce di log per le operazioni con esito positivo e negativo. Per le operazioni con esito negativo, la voce di log include il nome dell'eccezione AWS KMS (`errorCode`) e il messaggio di errore (`errorMessage`). Puoi utilizzare queste informazioni per identificare e risolvere l'errore. Per vedere un esempio, consulta Errore di decrittografia con una chiave KMS in un archivio delle chiavi esterne.

La voce di log include anche l'ID della richiesta. Se la richiesta ha raggiunto il proxy dell'archivio delle chiavi esterne, puoi utilizzare l'ID della richiesta nella voce di log per trovare la richiesta corrispondente nei log del proxy, se disponibili.

CloudWatch metriche

AWS KMSregistra CloudWatch metriche Amazon dettagliate sul funzionamento e le prestazioni del tuo archivio di chiavi esterno, tra cui latenza, throttling, errori proxy, stato di gestore di chiavi esterno, il numero di giorni che mancano alla scadenza del certificato TLS e l'età riportata delle credenziali di autenticazione proxy. Puoi utilizzare queste metriche per sviluppare modelli di dati

per il funzionamento del tuo archivio di chiavi esterno e CloudWatch allarmi che ti avvisano di problemi imminenti prima che si verifichino.

> **Important**
>
> AWS KMSconsiglia di creare CloudWatch allarmi per monitorare le metriche dell'archivio di chiavi esterne. Questi allarmi ti avvisano dei primi segnali di problemi prima che si verifichino.

Grafici di monitoraggio

AWS KMSvisualizza i grafici delle CloudWatch metriche dell'archivio chiavi esterno nella pagina di dettaglio di ogni archivio di chiavi esterno nella console. AWS KMS È possibile utilizzare i dati nei grafici per individuare l'origine degli errori, rilevare problemi imminenti, stabilire linee di base e perfezionare le soglie di allarme. CloudWatch Per informazioni dettagliate sull'interpretazione dei grafici di monitoraggio e sull'utilizzo dei relativi dati, consulta Monitoraggio di un archivio delle chiavi esterne.

Visualizzazione di archivi delle chiavi esterne e chiavi KMS

AWS KMSvisualizza informazioni dettagliate sugli archivi di chiavi esterni e sulle chiavi KMS nell'archivio chiavi esterno della AWS KMS console e nella risposta alle operazioni and. DescribeCustomKeyStoresDescribeKey Queste visualizzazioni includono campi speciali per gli archivi delle chiavi esterne e le chiavi KMS con informazioni che è possibile utilizzare per la risoluzione dei problemi, come lo stato di connessione dell'archivio delle chiavi esterne e l'ID della chiave esterna associata alla chiave KMS. Per informazioni dettagliate, consulta Visualizzazione di un archivio delle chiavi esterne e Visualizzazione delle chiavi KMS in un archivio delle chiavi esterne.

Client di test proxy XKS

AWS KMS fornisce un client di test open source che verifica la conformità del proxy dell'archivio delle chiavi esterne alla Specifica API relativa al proxy dell'archivio delle chiavi esterne di AWS KMS. Puoi utilizzare tale client di test per identificare e risolvere i problemi relativi al proxy dell'archivio delle chiavi esterne.

Errori di configurazione

Durante la creazione di un archivio delle chiavi esterne, puoi specificare i valori delle proprietà che comprendono la configurazione dell'archivio, come le credenziali di autenticazione proxy, l'endpoint URI proxy, il percorso URI proxy e il nome del servizio dell'endpoint VPC. Quando AWS KMS rileva un errore nel valore di una proprietà, l'operazione fallisce e restituisce un errore che indica il valore errato.

Molti problemi di configurazione possono essere risolti correggendo il valore errato. Puoi correggere un percorso URI proxy o le credenziali di autenticazione proxy non valide senza disconnettere l'archivio delle chiavi esterne. Per le definizioni di questi valori, inclusi i requisiti di unicità, consulta Assemblare i prerequisiti. Per istruzioni sull'aggiornamento di tali valori, consulta Modifica delle proprietà dell'archivio delle chiavi esterne.

Per evitare errori con il percorso URI proxy e i valori delle credenziali di autenticazione proxy, quando crei o aggiorni l'archivio delle chiavi esterne, carica un file di configurazione proxy nella console AWS KMS. Si tratta di un file basato su JSON con il percorso URI proxy e i valori delle credenziali di autenticazione proxy forniti dal proxy o dal gestore delle chiavi esterne. Non puoi utilizzare un file di configurazione proxy con le operazioni API AWS KMS, ma puoi impiegare i valori nel file per ottenere valori di parametro per le richieste API che corrispondono ai valori del proxy.

Errori di configurazione generale

Eccezioni: `CustomKeyStoreInvalidStateException` (`CreateKey`), `KMSInvalidStateException` (operazioni di crittografia), `XksProxyInvalidConfigurationException` (operazioni di gestione, ad eccezione di `CreateKey`)

Codici di errore di connessione: `XKS_PROXY_INVALID_CONFIGURATION`, `XKS_PROXY_INVALID_TLS_CONFIGURATION`

Per gli archivi delle chiavi esterne con connettività dell'endpoint pubblico, AWS KMS testa i valori delle proprietà durante la creazione e l'aggiornamento dell'archivio delle chiavi esterne. Per gli archivi delle chiavi esterne con connettività del servizio endpoint VPC, AWS KMS testa i valori delle proprietà durante la connessione e l'aggiornamento dell'archivio delle chiavi esterne.

> **Note**
>
> L'operazione `ConnectCustomKeyStore`, che è asincrona, potrebbe avere esito positivo anche se il tentativo di connettere l'archivio delle chiavi esterne al relativo proxy fallisce. In tal

caso non vi è alcuna eccezione, ma lo stato di connessione dell'archivio delle chiavi esterne è Failed (Non riuscito) e viene visualizzato un codice di errore di connessione che spiega il messaggio di errore. Per ulteriori informazioni, consulta Errori di connessione all'archivio delle chiavi esterne.

Se AWS KMS rileva un errore nel valore di una proprietà, l'operazione ha esito negativo e restituisce l'eccezione `XksProxyInvalidConfigurationException` con uno dei seguenti messaggi di errore.

Il proxy dell'archivio delle chiavi esterne ha rifiutato la richiesta a causa di un percorso URI non valido. Verifica il percorso URI dell'archivio delle chiavi esterne e aggiornalo, se necessario.

- Il percorso URI proxy è il percorso di base per le richieste AWS KMS alle API del proxy. Se questo percorso non è corretto, tutte le richieste al proxy hanno esito negativo. Per visualizzare il percorso URI proxy corrente dell'archivio delle chiavi esterne, usa la console AWS KMS o l'operazione `DescribeCustomKeyStores`. Per trovare il percorso URI proxy corretto, consulta la documentazione del proxy dell'archivio delle chiavi esterne. Per informazioni sulla correzione del valore relativo al percorso URI proxy, consulta Modifica delle proprietà dell'archivio delle chiavi esterne.
- Il percorso URI proxy per il proxy dell'archivio delle chiavi esterne può cambiare con gli aggiornamenti del proxy o del gestore delle chiavi esterne. Per informazioni relative a queste modifiche, consulta la documentazione del proxy o del gestore delle chiavi esterne.

`XKS_PROXY_INVALID_TLS_CONFIGURATION`
AWS KMS non è in grado di stabilire una connessione TLS al proxy dell'archivio delle chiavi esterne. Verifica la configurazione TLS e il relativo certificato.

- Tutti i proxy dell'archivio delle chiavi esterne richiedono un certificato TLS. Il certificato TLS deve essere emesso da un'autorità di certificazione (CA) pubblica supportata per gli archivi delle chiavi esterne. Per un elenco delle autorità di certificazione supportate, consulta Autorità di certificazione attendibili nella Specifica API relativa al proxy dell'archivio delle chiavi esterne di AWS KMS.
- Per quanto riguarda la connettività dell'endpoint pubblico, il nome comune del soggetto (CN) sul certificato TLS deve corrispondere al nome di dominio nell'endpoint URI proxy

per il proxy dell'archivio delle chiavi esterne. Ad esempio, se l'endpoint pubblico è https://myproxy.xks.example.com, il CN sul certificato TLS deve essere `myproxy.xks.example.com` o `*.xks.example.com`.

- Per la connettività del servizio endpoint VPC, il nome comune del soggetto (CN) sul certificato TLS deve corrispondere al nome DNS privato del servizio endpoint VPC. Ad esempio, se il nome DNS privato è myproxy-private.xks.example.com, il CN sul certificato TLS deve essere `myproxy-private.xks.example.com` o `*.xks.example.com`.
- Il certificato TLS non deve essere scaduto. Per ottenere la data di scadenza di un certificato TLS, utilizza gli strumenti SSL, come OpenSSL. Per monitorare la data di scadenza di un certificato TLS associato a un archivio di chiavi esterno, utilizza la XksProxyCertificateDaysToExpire CloudWatch metrica. Il numero di giorni che mancano alla data di scadenza della certificazione TLS viene visualizzato anche nella sezione Monitoring (Monitoraggio) della console AWS KMS.
- Se utilizzi la connettività dell'endpoint pubblico, testa la configurazione SSL tramite gli strumenti di test SSL. Gli errori di connessione TLS possono derivare da un concatenamento errato dei certificati.

Errori di configurazione per la connettività del servizio endpoint VPC

Eccezioni: `XksProxyVpcEndpointServiceNotFoundException`, `XksProxyVpcEndpointServiceInvalidConfigurationException`

Oltre ai problemi di connettività generali, potresti riscontrare i seguenti problemi durante la creazione, la connessione o l'aggiornamento di un archivio delle chiavi esterne con connettività del servizio endpoint VPC. AWS KMS testa i valori delle proprietà di un archivio delle chiavi esterne con la connettività del servizio endpoint VPC durante la creazione, la connessione e l'aggiornamento dell'archivio delle chiavi esterne. Quando le operazioni di gestione falliscono a causa di errori di configurazione, generano le seguenti eccezioni:

```
XksProxyVpcEndpointServiceNotFoundEccezione
```

Di seguito è riportata la possibile causa:

- Un nome del servizio endpoint VPC errato. Verifica che il nome del servizio endpoint VPC per l'archivio delle chiavi esterne sia corretto e corrisponda al valore dell'endpoint URI proxy per l'archivio delle chiavi esterne. Per trovare il nome del servizio endpoint VPC, usa la console Amazon VPC o l'operazione. DescribeVpcEndpointServices Per trovare il nome del servizio

endpoint VPC e l'endpoint URI proxy di un key store esterno esistente, usa la AWS KMS console o l'operazione. DescribeCustomKeyStores Per informazioni dettagliate, vedi Visualizzazione di un archivio delle chiavi esterne.

- Il servizio endpoint VPC potrebbe trovarsi in una Regione AWS diversa rispetto all'archivio delle chiavi esterne. Verifica che il servizio endpoint VPC e l'archivio delle chiavi esterne si trovino nella stessa regione. (Il nome esterno del nome della regione, ad esempio, fa parte del nome del servizio endpoint VPC`us-east-1`, ad esempio com.amazonaws.vpce.us-east-1. vpce-svc-example.) Per un elenco dei requisiti per il servizio endpoint VPC di un archivio delle chiavi esterne, consulta Servizio endpoint VPC. Non puoi spostare un servizio endpoint VPC o un archivio delle chiavi esterne in una regione diversa, tuttavia puoi creare un nuovo archivio delle chiavi esterne nella stessa regione del servizio endpoint VPC. Per informazioni dettagliate, consulta Configurazione della connettività del servizio endpoint VPC e Creazione di un archivio delle chiavi esterne.
- AWS KMS non è un principale consentito per il servizio endpoint VPC. L'elenco Allow principals (Consenti entità principali) per il servizio endpoint VPC deve includere il valore `cks.kms.<region>.amazonaws.com`, ad esempio `cks.kms.eu-west-3.amazonaws.com`. Per istruzioni sull'aggiunta di questo valore, consulta Gestione delle autorizzazioni nella Guida di AWS PrivateLink.

XksProxyVpcEndpointServiceInvalidConfigurationEccezione

Questo errore si verifica quando il servizio endpoint VPC non soddisfa uno dei seguenti requisiti:

- Il VPC richiede almeno due sottoreti private, ognuna in una zona di disponibilità diversa. Per assistenza sull'aggiunta di una sottorete al VPC, consulta Creazione di una sottorete nel VPC nella Guida per l'utente di Amazon VPC.
- Il tipo di servizio endpoint VPC deve utilizzare un Network Load Balancer, non un sistema di bilanciamento del carico gateway.
- L'accettazione non deve essere richiesta per il servizio endpoint VPC (Acceptance required [Accettazione richiesta] deve essere false). Se è necessaria l'accettazione manuale di ogni richiesta di connessione, AWS KMS non è in grado di utilizzare il servizio endpoint VPC per connettersi al proxy dell'archivio delle chiavi esterne. Per maggiori dettagli, consulta Accettare o rifiutare le richieste di connessione nella Guida di AWS PrivateLink.
- Il servizio endpoint VPC deve avere un nome DNS privato che è un sottodominio di un dominio pubblico. Ad esempio, se il nome DNS privato è `https://myproxy-`

`private.xks.example.com`, i domini `xks.example.com` o `example.com` devono disporre di un server DNS pubblico. Per visualizzare o modificare il nome DNS privato per il servizio endpoint VPC, consulta Gestione dei nomi DNS per i servizi endpoint VPC nella Guida di AWS PrivateLink.

- Il valore di Domain verification status (Stato di verifica del dominio) per il nome DNS privato deve essere `verified`. Per visualizzare e aggiornare lo stato di verifica del dominio del nome DNS privato, consulta Verifica del dominio del nome DNS privato. Potrebbero essere necessari alcuni minuti prima che venga visualizzato lo stato di verifica aggiornato dopo aver aggiunto il record di testo richiesto.

  > **Note**
  >
  > Un dominio DNS privato può essere verificato solo se è il sottodominio di un dominio pubblico. In caso contrario, lo stato di verifica del dominio DNS privato non cambia, anche dopo aver aggiunto il record TXT richiesto.

- Il nome DNS privato del servizio endpoint VPC deve corrispondere al valore dell'endpoint URI proxy per l'archivio delle chiavi esterne. Per un archivio delle chiavi esterne con connettività del servizio endpoint VPC, l'endpoint URI proxy deve essere `https://` seguito dal nome DNS privato del servizio endpoint VPC. Per visualizzare il valore dell'endpoint URI proxy, consulta Visualizzazione di un archivio delle chiavi esterne. Per modificare il valore dell'endpoint URI proxy, consulta Modifica delle proprietà dell'archivio delle chiavi esterne.

Errori di connessione all'archivio delle chiavi esterne

Il processo di connessione di un archivio delle chiavi esterne al relativo proxy richiede circa cinque minuti. Se l'operazione non genera rapidamente un errore, l'operazione `ConnectCustomKeyStore` restituisce una risposta HTTP 200 e un oggetto JSON senza proprietà. Questa risposta iniziale non indica tuttavia che la connessione è riuscita. Per determinare se l'archivio delle chiavi esterne è connesso, visualizza lo stato della connessione. Se la connessione ha esito negativo, lo stato della connessione dell'archivio delle chiavi esterne cambia in `FAILED` e AWS KMS restituisce un codice di errore di connessione che spiega la causa dell'errore.

> **Note**
>
> Quando lo stato di connessione di un archivio delle chiavi personalizzate è `FAILED`, devi disconnettere l'archivio prima di tentare di riconnetterlo. Non puoi connettere uno store delle chiavi personalizzate il cui stato di connessione è `FAILED`.

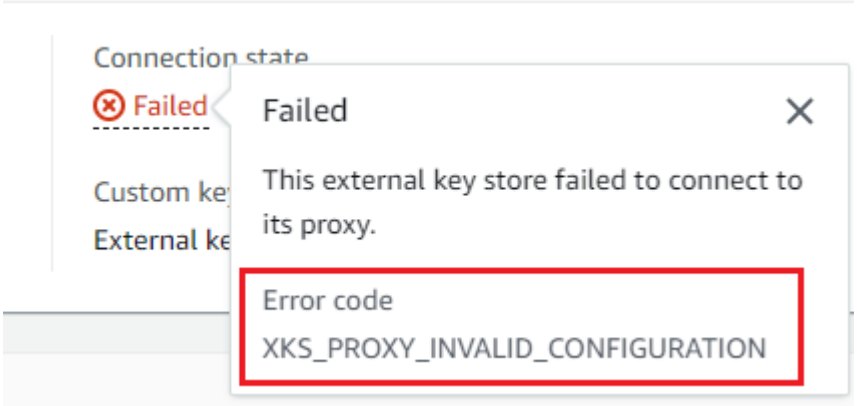
Per visualizzare lo stato di connessione di un archivio delle chiavi esterne:

- Nella DescribeCustomKeyStoresrisposta, visualizza il valore dell'`ConnectionState`elemento.
- Nella console AWS KMS, il campo Connection state (Stato connessione) viene visualizzato nella tabella dell'archivio delle chiavi esterne. Inoltre, nella pagina dei dettagli di ogni archivio delle chiavi esterne, il campo Connection state (Stato connessione) viene visualizzato nella sezione General configuration (Configurazione generale).

Quando lo stato della connessione è `FAILED`, il codice di errore di connessione indica l'errore.

Per visualizzare il codice di errore della connessione:

- Nella DescribeCustomKeyStoresrisposta, visualizza il valore dell'`ConnectionErrorCode`elemento. Tale elemento appare nella risposta `DescribeCustomKeyStores` solo quando `ConnectionState` è nello stato `FAILED`.
- Per visualizzare il codice di errore della connessione nella console AWS KMS, accedi alla pagina dei dettagli dell'archivio delle chiavi esterne e passa il puntatore del mouse sul valore Failed (Non riuscito).



Codici di errore di connessione per archivi delle chiavi esterne

I seguenti codici di errore di connessione si applicano agli archivi delle chiavi esterne

`INTERNAL_ERROR`

AWS KMS non è stato in grado di completare la richiesta a causa di un errore interno. Riprova la richiesta . Per le richieste `ConnectCustomKeyStore`, scollega lo store delle chiavi personalizzate prima di provare a connetterti di nuovo.

`INVALID_CREDENTIALS`

Uno o entrambi i valori `XksProxyAuthenticationCredential` non sono validi nel proxy dell'archivio delle chiavi esterne specificato.

`NETWORK_ERRORS`

Gli errori di rete impediscono ad AWS KMS di connettere l'archivio delle chiavi personalizzate al relativo archivio del materiale della chiave.

`XKS_PROXY_ACCESS_DENIED`

Alle richieste AWS KMS viene negato l'accesso al proxy dell'archivio delle chiavi esterne. Se tale proxy dispone di regole di autorizzazione, verifica che consentano ad AWS KMS di comunicare con il proxy per tuo conto.

`XKS_PROXY_INVALID_CONFIGURATION`

Un errore di configurazione impedisce all'archivio delle chiavi esterne di connettersi al relativo proxy. Verifica il valore di `XksProxyUriPath`.

`XKS_PROXY_INVALID_RESPONSE`

AWS KMS non è in grado di interpretare la risposta proveniente dal proxy dell'archivio delle chiavi esterne. Se visualizzi ripetutamente questo codice di errore di connessione, informa il fornitore del proxy dell'archivio delle chiavi esterne.

`XKS_PROXY_INVALID_TLS_CONFIGURATION`

AWS KMS non è in grado di connettersi al proxy dell'archivio delle chiavi esterne perché la configurazione TLS non è valida. Verifica che il proxy dell'archivio delle chiavi esterne supporti TLS 1.2 o 1.3. Inoltre, verifica che il certificato TLS sia ancora valido, che corrisponda al nome host nel valore `XksProxyUriEndpoint` e che sia firmato da un'autorità di certificazione affidabile inclusa nell'elenco delle autorità di certificazione attendibili.

`XKS_PROXY_NOT_REACHABLE`

AWS KMS non è in grado di comunicare con il proxy dell'archivio delle chiavi esterne. Verifica che `XksProxyUriEndpoint` e `XksProxyUriPath` siano corretti. Utilizza gli strumenti del proxy dell'archivio delle chiavi esterne per verificare che il proxy sia attivo e disponibile sulla rete. Inoltre, verifica che le istanze del gestore delle chiavi esterne funzionino correttamente. I tentativi di connessione hanno esito negativo e restituiscono questo codice di errore di connessione se il proxy segnala che tutte le istanze del gestore delle chiavi esterne non sono disponibili.

`XKS_PROXY_TIMED_OUT`

AWS KMS può connettersi al proxy dell'archivio delle chiavi esterne, ma il proxy non risponde ad AWS KMS nel tempo assegnato. Se visualizzi ripetutamente questo codice di errore di connessione, informa il fornitore del proxy dell'archivio delle chiavi esterne.

`XKS_VPC_ENDPOINT_SERVICE_INVALID_CONFIGURATION`

La configurazione del servizio endpoint Amazon VPC non è conforme ai requisiti per un archivio delle chiavi esterne di AWS KMS.

- Il servizio endpoint VPC deve essere un servizio endpoint per gli endpoint di interfaccia nell'Account AWS del chiamante.
- Deve avere un Network Load Balancer (NLB) connesso ad almeno due sottoreti, ognuna in una zona di disponibilità diversa.
- L'elenco `Allow principals` deve includere il principale del servizio AWS KMS per la regione `cks.kms.<region>.amazonaws.com`, ad esempio `cks.kms.us-east-1.amazonaws.com`.
- Non deve richiedere l'accettazione delle richieste di connessione.
- Deve avere un nome DNS privato. Il nome DNS privato per un archivio delle chiavi esterne con connettività `VPC_ENDPOINT_SERVICE` deve essere univoco nella Regione AWS.
- Lo stato di verifica per il dominio del nome DNS privato deve essere `verified`.
- Il certificato TLS specifica il nome host DNS privato in cui è raggiungibile l'endpoint.

`XKS_VPC_ENDPOINT_SERVICE_NOT_FOUND`

AWS KMS non riesce a trovare il servizio endpoint VPC utilizzato per comunicare con il proxy dell'archivio delle chiavi esterne. Verifica che `XksProxyVpcEndpointServiceName` sia corretto e che il principale del servizio AWS KMS disponga delle autorizzazioni consumer per il servizio endpoint Amazon VPC.

Errori di latenza e timeout

Eccezioni: `CustomKeyStoreInvalidStateException` (`CreateKey`), `KMSInvalidStateException` (operazioni di crittografia), `XksProxyUriUnreachableException` (operazioni di gestione)

Codici di errore di connessione: `XKS_PROXY_NOT_REACHABLE`, `XKS_PROXY_TIMED_OUT`

Quando AWS KMS non riesce a contattare il proxy entro l'intervallo di timeout di 250 millisecondi, restituisce un'eccezione. `CreateCustomKeyStore` e `UpdateCustomKeyStore` restituiscono un'eccezione `XksProxyUriUnreachableException`. Le operazioni di crittografia restituiscono l'eccezione `KMSInvalidStateException` standard con un messaggio di errore che descrive il problema. Se `ConnectCustomKeyStore` ha esito negativo, AWS KMS restituisce un codice di errore di connessione che descrive il problema.

Gli errori di timeout possono essere problemi temporanei che possono essere risolti ripetendo la richiesta. Se il problema persiste, verifica che il proxy dell'archivio delle chiavi esterne sia attivo e connesso alla rete e che l'endpoint URI proxy, il percorso URI proxy e il nome del servizio endpoint VPC (se presente) siano corretti. Inoltre, verifica che il gestore delle chiavi esterne sia vicino alla Regione AWS dell'archivio delle chiavi esterne. Se è necessario aggiornare uno di questi valori, consulta Modifica delle proprietà dell'archivio delle chiavi esterne.

Per tenere traccia dei modelli di latenza, utilizza la `XksProxyLatency` CloudWatch metrica e il grafico della latenza media (basato su tale metrica) nella sezione Monitoraggio della console. AWS KMS Il proxy dell'archivio delle chiavi esterne potrebbe anche generare log e parametri in grado di tracciare la latenza e i timeout.

`XksProxyUriUnreachableException`
AWS KMS non è in grado di comunicare con il proxy dell'archivio delle chiavi esterne. Potrebbe trattarsi di un problema di rete temporaneo. Se visualizzi questo errore ripetutamente, verifica che il proxy dell'archivio delle chiavi esterne sia attivo e connesso alla rete e che l'URI endpoint sia corretto.

- Il proxy dell'archivio delle chiavi esterne non ha risposto a una richiesta API proxy AWS KMS entro l'intervallo di timeout di 250 millisecondi. Ciò potrebbe indicare un problema di rete temporaneo o un problema operativo o di prestazioni con il proxy. Se un nuovo tentativo non risolve il problema, informa l'amministratore del proxy dell'archivio delle chiavi esterne.

Gli errori di latenza e timeout si manifestano spesso come errori di connessione. Quando l'ConnectCustomKeyStoreoperazione fallisce, lo stato di connessione dell'archivio chiavi esterno cambia `FAILED` e AWS KMS restituisce un codice di errore di connessione che spiega l'errore. Per un elenco di codici di errore di connessione e suggerimenti per la relativa risoluzione, consulta Codici di errore di connessione per archivi delle chiavi esterne. Gli elenchi dei codici di connessione per All custom key stores (Tutti gli archivi delle chiavi personalizzate) e External key stores (Archivi delle

chiavi esterne) si applicano agli archivi delle chiavi esterne. I seguenti errori di connessione sono correlati alla latenza e ai timeout.

`XKS_PROXY_NOT_REACHABLE`

oppure

`CustomKeyStoreInvalidStateException` , `KMSInvalidStateException` , `XksProxyUriUnreachableException`
AWS KMS non è in grado di comunicare con il proxy dell'archivio delle chiavi esterne. Verifica che il proxy dell'archivio delle chiavi esterne sia attivo e connesso alla rete e che il percorso URI e l'URI endpoint o il nome del servizio VPC siano corretti nell'archivio delle chiavi esterne.

Questo errore può verificarsi per i seguenti motivi:

- Il proxy dell'archivio delle chiavi esterne non è attivo o non è connesso alla rete.
- Si è verificato un errore nei valori endpoint URI proxy, percorso URI proxy o del nome del servizio endpoint VPC (se applicabile) nella configurazione dell'archivio delle chiavi esterne. Per visualizzare la configurazione dell'archivio chiavi esterno, utilizza l'DescribeCustomKeyStoresoperazione o visualizza la pagina di dettaglio dell'archivio chiavi esterno nella AWS KMS console.
- Potrebbe essersi verificato un errore di configurazione della rete, ad esempio un errore di porta, nel percorso di rete tra AWS KMS e il proxy dell'archivio delle chiavi esterne. AWS KMS comunica con il proxy dell'archivio delle chiavi esterne sulla porta 443. Questo valore non è configurabile.
- Quando il proxy dell'archivio di chiavi esterno segnala (in GetHealthStatusrisposta) che tutte le istanze del gestore di chiavi esterno lo sonoUNAVAILABLE, l'ConnectCustomKeyStoreoperazione fallisce e restituisce un valore `ConnectionErrorCode` di`XKS_PROXY_NOT_REACHABLE`. Per assistenza, consulta la documentazione del gestore delle chiavi esterne.
- Questo errore può essere causato da una grande distanza fisica tra il gestore delle chiavi esterne e la Regione AWS con l'archivio delle chiavi esterne. La latenza del ping, ossia il tempo di andata e ritorno (RTT) della rete, tra Regione AWS e il gestore delle chiavi esterne non deve superare i 35 millisecondi. Potrebbe essere necessario creare un archivio delle chiavi esterne in una Regione AWS più vicina al gestore delle chiavi esterne o spostare il gestore in un data center più vicino alla Regione AWS.

`XKS_PROXY_TIMED_OUT`

oppure

`CustomKeyStoreInvalidStateException` , `KMSInvalidStateException` , `XksProxyUriUnreachableException`
AWS KMS ha rifiutato la richiesta perché il proxy dell'archivio delle chiavi esterne non ha risposto in tempo. Riprova la richiesta . Se visualizzi questo errore ripetutamente, segnalalo all'ammin istratore del proxy dell'archivio delle chiavi esterne.

Questo errore può verificarsi per i seguenti motivi:

- Questo errore può essere causato da una grande distanza fisica tra il gestore delle chiavi esterne e il proxy dell'archivio delle chiavi esterne. Se possibile, avvicina il proxy al gestore delle chiavi esterne.
- Gli errori di timeout possono verificarsi quando il proxy non è progettato per gestire il volume e la frequenza delle richieste provenienti da AWS KMS. Se le CloudWatch metriche indicano un problema persistente, informate l'amministratore proxy dell'archivio chiavi esterno.
- Gli errori di timeout possono verificarsi quando la connessione tra il gestore delle chiavi esterne e Amazon VPC per l'archivio delle chiavi esterne non funziona correttamente. Se utilizzi AWS Direct Connect, verifica che il VPC e il gestore delle chiavi esterne siano in grado di comunicare in modo efficace. Per assistenza nella risoluzione di eventuali problemi, consulta Risoluzione dei problemi di AWS Direct Connect nella Guida per l'utente di AWS Direct Connect.

`XKS_PROXY_TIMED_OUT`

oppure

`CustomKeyStoreInvalidStateException` , `KMSInvalidStateException` , `XksProxyUriUnreachableException`
Il proxy dell'archivio delle chiavi esterne non ha risposto alla richiesta nel tempo assegnato. Riprova la richiesta . Se visualizzi questo errore ripetutamente, segnalalo all'amministratore del proxy dell'archivio delle chiavi esterne.

- Questo errore può essere causato da una grande distanza fisica tra il gestore delle chiavi esterne e il proxy dell'archivio delle chiavi esterne. Se possibile, avvicina il proxy al gestore delle chiavi esterne.

Errori delle credenziali di autenticazione

Eccezioni: `CustomKeyStoreInvalidStateException` (`CreateKey`), `KMSInvalidStateException` (operazioni di crittografia), `XksProxyIncorrectAuthenticationCredentialException` (operazioni di gestione diverse da `CreateKey`)

Sei tu a stabilire e gestire le credenziali di autenticazione per AWS KMS nel proxy dell'archivio delle chiavi esterne. Comunica quindi ad AWS KMS i valori delle credenziali durante la creazione dell'archivio delle chiavi esterne. Per modificare le credenziali di autenticazione, esegui questa operazione nel proxy dell'archivio delle chiavi esterne. Quindi aggiorna le credenziali per l'archivio delle chiavi esterne. Se il proxy effettua la rotazione delle credenziali, devi aggiornarle.

Se il proxy dell'archivio delle chiavi esterne non autentica una richiesta firmata con le credenziali di autenticazione proxy per l'archivio delle chiavi esterne, l'effetto dipende dalla richiesta:

- `CreateCustomKeyStore` e `UpdateCustomKeyStore` hanno esito negativo con un'eccezione `XksProxyIncorrectAuthenticationCredentialException`.
- `ConnectCustomKeyStore` ha esito positivo, ma la connessione fallisce. Lo stato della connessione è `FAILED` e il codice di errore è `INVALID_CREDENTIALS`. Per informazioni dettagliate, vedi Errori di connessione all'archivio delle chiavi esterne.
- Le operazioni di crittografia restituiscono `KMSInvalidStateException` per tutti gli errori di configurazione esterna e gli errori dello stato di connessione in un archivio delle chiavi esterno. Il messaggio di errore allegato descrive il problema.

Il proxy dell'archivio delle chiavi esterne ha rifiutato la richiesta perché non era in grado di autenticare AWS KMS. Verifica le credenziali dell'archivio delle chiavi esterne e aggiornale se necessario.

Questo errore può verificarsi per i seguenti motivi:

- L'ID della chiave di accesso o la chiave di accesso segreta per l'archivio delle chiavi esterne non corrisponde ai valori stabiliti nel proxy.

  Per correggere questo errore, aggiorna le credenziali di autenticazione proxy per l'archivio delle chiavi esterne. Puoi apportare questa modifica senza disconnettere l'archivio delle chiavi esterne.
- Un proxy inverso tra AWS KMS e il proxy dell'archivio delle chiavi esterne potrebbe manipolare le intestazioni HTTP in modo da invalidare le firme SigV4. Per correggere questo errore, informa l'amministratore del proxy.

Errori relativi allo stato delle chiavi

Eccezioni: `KMSInvalidStateException`

`KMSInvalidStateException` viene utilizzato per due scopi distinti per le chiavi KMS negli archivi delle chiavi personalizzate.

- Quando un'operazione di gestione, ad esempio `CancelKeyDeletion`, ha esito negativo e restituisce questa eccezione, indica che lo stato della chiave KMS non è compatibile con l'operazione.
- Quando un'operazione di crittografia su una chiave KMS in un archivio delle chiavi personalizzate ha esito negativo e restituisce un'eccezione `KMSInvalidStateException`, può indicare un problema con lo stato della chiave KMS. Tuttavia, le operazioni di crittografia AWS KMS restituiscono l'eccezione `KMSInvalidStateException` per tutti gli errori di configurazione esterna e gli errori dello stato di connessione in un archivio delle chiavi esterno. Per identificare il problema, utilizza il messaggio di errore che accompagna l'eccezione.

Per trovare lo stato della chiave richiesto per le operazioni API AWS KMS, consulta Stati chiave delle chiavi AWS KMS. Per trovare lo stato di chiave di una chiave KMS, nella pagina Chiavi gestite cliente, visualizza il campo Stato della chiave KMS. Oppure, utilizzate l'DescribeKeyoperazione e visualizzate l'`KeyState`elemento nella risposta. Per informazioni dettagliate, vedi Visualizzazione di chiavi.

> **Note**
>
> Lo stato di una chiave KMS in un archivio delle chiavi esterne non indica lo stato della chiave esterna associata. Per informazioni sullo stato della chiave esterna, usa il gestore delle chiavi esterne e gli strumenti del proxy dell'archivio delle chiavi esterne.

`CustomKeyStoreInvalidStateException` si riferisce allo stato di connessione dell'archivio delle chiavi esterne, non allo stato chiave di una chiave KMS.

Un'operazione di crittografia su una chiave KMS in un archivio personalizzato potrebbe non riuscire perché lo stato della chiave KMS è `Unavailable` o `PendingDeletion`. (I tasti disattivati restituiscono `DisabledException`).

- Una chiave KMS ha uno stato `Disabled` chiave solo quando la disabiliti intenzionalmente nella AWS KMS console o utilizzando l'operazione. DisableKey Quando una chiave KMS è disabilitata, puoi visualizzare e gestire la chiave, ma non utilizzarla per operazioni di crittografia. Per risolvere il problema, abilita la chiave. Per informazioni dettagliate, vedi Abilitazione e disabilitazione delle chiavi.
- Una chiave KMS ha uno stato chiave `Unavailable` quando l'archivio delle chiavi esterne viene disconnesso dal relativo proxy. Per correggere una chiave KMS non disponibile, riconnetti l'archivio delle chiavi esterne. Dopo la riconnessione, per le chiavi KMS nell'archivio delle chiavi esterne viene ripristinato lo stato di chiave precedente, ovvero `Enabled` o `Disabled`.

  Una chiave KMS ha uno stato di chiave `PendingDeletion` quando ne è stata programmata l'eliminazione e si trova nel periodo di attesa. Un errore di stato della chiave su una chiave KMS in attesa di eliminazione indica che la chiave non deve essere eliminata, perché viene utilizzata per la crittografia o è necessaria per la decrittografia. Per riattivare la chiave KMS, annulla l'eliminazione pianificata e abilita la chiave. Per informazioni dettagliate, vedi Pianificazione e annullamento dell'eliminazione di chiavi.

Errori di decrittografia

Eccezioni: `KMSInvalidStateException`

Quando un'operazione Decrypt (Decrittografa) con una chiave KMS in un archivio delle chiavi esterno non va a buon fine, AWS KMS restituisce l'eccezione `KMSInvalidStateException` standard utilizzata dalle operazioni di crittografia per tutti gli errori di configurazione esterni e gli errori dello stato di connessione su un archivio di chiavi esterno. Il messaggio di errore indica il problema.

Per decrittografare un testo criptato con doppia crittografia, il gestore delle chiavi esterne utilizza prima la chiave esterna per decrittografare il livello esterno. AWS KMS utilizza quindi il materiale della chiave di AWS KMS nella chiave KMS per decrittografare il livello interno del testo criptato. Un

testo criptato non valido o danneggiato può essere rifiutato dal gestore delle chiavi esterne o da AWS KMS.

I seguenti messaggi di errore accompagnano `KMSInvalidStateException` quando la decrittografia ha esito negativo. Indica un problema con il testo criptato o il contesto di crittografia opzionale nella richiesta.

Il proxy dell'archivio delle chiavi esterne ha rifiutato la richiesta perché il testo criptato specificato o i dati autenticati aggiuntivi sono danneggiati, mancanti o non validi.

- Quando il proxy dell'archivio delle chiavi esterne o il gestore delle chiavi esterne segnala che il testo criptato o il relativo contesto di crittografia non è valido, in genere indica questi problemi nella richiesta `Decrypt` inviata a AWS KMS. Per le operazioni `Decrypt`, AWS KMS invia al proxy lo stesso testo criptato e il relativo contesto di crittografia ricevuti nella richiesta `Decrypt`.

  Questo errore potrebbe essere causato da un problema di rete in transito, ad esempio un bit capovolto. Riprova la richiesta `Decrypt`. Se il problema persiste, verifica che il testo criptato non sia stato alterato o danneggiato. Inoltre, verifica che il contesto di crittografia nella richiesta `Decrypt` inviata ad AWS KMS corrisponda al contesto presente nella richiesta che ha crittografato i dati.

Il testo criptato o il contesto di crittografia inviato dal proxy dell'archivio delle chiavi esterne per la decrittografia è danneggiato, mancante o non valido.

- Quando AWS KMS rifiuta il testo criptato ricevuto dal proxy, indica che il gestore delle chiavi esterne o il proxy ha restituito ad AWS KMS un testo criptato non valido o danneggiato.

  Questo errore potrebbe essere causato da un problema di rete in transito, ad esempio un bit capovolto. Riprova la richiesta `Decrypt`. Se il problema persiste, verifica che il gestore delle chiavi esterne funzioni correttamente e che il proxy non alteri il testo criptato ricevuto dal gestore prima di restituirlo ad AWS KMS.

Errori relativi alla chiave esterna

Una chiave esterna è una chiave crittografica nel gestore delle chiavi esterne che funge da materiale della chiave per una chiave KMS. AWS KMS non è in grado di accedere direttamente alla chiave esterna, ma deve chiedere al gestore delle chiavi esterne (tramite il proxy dell'archivio delle chiavi esterne) di utilizzare la chiave esterna per crittografare i dati o decrittografare un testo criptato.

L'ID della chiave esterna viene specificato nel relativo gestore durante la creazione di una chiave KMS nell'archivio delle chiavi esterne. Non puoi modificare l'ID della chiave esterna dopo la creazione della chiave KMS. Per evitare problemi con la chiave KMS, puoi utilizzare l'operazione `CreateKey` per chiedere al proxy dell'archivio delle chiavi esterne di verificare l'ID e la configurazione della chiave esterna. Se la chiave esterna non soddisfa i requisiti per l'uso con una chiave KMS, l'operazione `CreateKey` ha esito negativo con un'eccezione e un messaggio di errore che identifica il problema.

Tuttavia, possono verificarsi problemi dopo la creazione della chiave KMS. Se un'operazione di crittografia fallisce a causa di un problema con la chiave esterna, l'operazione ha esito negativo e restituisce un'eccezione `KMSInvalidStateException` con un messaggio di errore che indica il problema.

CreateKey errori per la chiave esterna

Eccezioni: `XksKeyAlreadyInUseException`, `XksKeyNotFoundException`, `XksKeyInvalidConfigurationException`

L'CreateKeyoperazione tenta di verificare l'ID e le proprietà della chiave esterna fornita nel parametro External key ID (console) o `XksKeyId` (API). Questa procedura è progettata per rilevare gli errori in anticipo prima di provare a utilizzare la chiave esterna con la chiave KMS.

Chiave esterna in uso

Ogni chiave KMS in un archivio delle chiavi esterne deve utilizzare una chiave esterna diversa. Quando `CreateKey` riconosce che l'ID della chiave esterna (XksKeyId) per una chiave KMS non è univoco nell'archivio delle chiavi esterne, fallisce e restituisce un. `XksKeyAlreadyInUseException`

Se utilizzi più ID per la stessa chiave esterna, `CreateKey` non riconosce il duplicato. Tuttavia, le chiavi KMS con la stessa chiave esterna non sono interoperabili perché hanno diversi metadati e materiali delle chiavi di AWS KMS.

Chiave esterna non trovata

Quando il proxy dell'archivio chiavi esterno segnala di non riuscire a trovare la chiave esterna utilizzando l'ID della chiave esterna (XksKeyId) per la chiave KMS, l'`CreateKey`operazione fallisce e restituisce il seguente `XksKeyNotFoundException` messaggio di errore.

> Il proxy dell'archivio delle chiavi esterne ha rifiutato la richiesta perché non riusciva a trovare la chiave esterna.

Questo errore può verificarsi per i seguenti motivi:

- L'ID della chiave esterna (`XksKeyId`) per la chiave KMS potrebbe non essere valido. Per individuare l'ID utilizzato dal proxy dell'archivio delle chiavi esterne per identificare la chiave esterna, consulta la documentazione del proxy o del gestore delle chiavi esterne.
- La chiave esterna potrebbe essere stata eliminata dal gestore delle chiavi esterne. Per verificare, utilizza gli strumenti del gestore delle chiavi esterne. Se la chiave esterna viene eliminata definitivamente, usa una chiave esterna diversa con la chiave KMS. Per un elenco dei requisiti per la chiave esterna, consulta Requisiti per una chiave KMS in un archivio delle chiavi esterne.

Requisiti della chiave esterna non soddisfatti

Quando il proxy dell'archivio delle chiavi esterne segnala che la chiave esterna non soddisfa i requisiti per l'uso con una chiave KMS, l'operazione `CreateKey` ha esito negativo e restituisce l'eccezione `XksKeyInvalidConfigurationException` con uno dei seguenti messaggi di errore.

> La specifica della chiave per la chiave esterna deve essere AES_256. La specifica della chiave per la chiave esterna specificata è *<key-spec>* .

- La chiave esterna deve essere una chiave crittografica simmetrica a 256 bit con una specifica della chiave AES_256. Se la chiave esterna specificata è di tipo diverso, specifica l'ID di una chiave esterna che soddisfi questo requisito.

> Lo stato della chiave esterna deve essere ENABLED (ABILITATO). Lo stato della chiave esterna specificata è *<status>*.

- La chiave esterna deve essere abilitata nel gestore delle chiavi esterne. Se la chiave esterna specificata non è abilitata, utilizza gli strumenti del gestore delle chiavi esterne per abilitarla o specifica una chiave esterna abilitata.

L'utilizzo della chiave per la chiave esterna deve includere ENCRYPT e DECRYPT. L'utilizzo della chiave per la chiave esterna specificata è <*key-usage* >.

- La chiave esterna deve essere configurata per la crittografia e la decrittografia nel gestore delle chiavi esterne. Se la chiave esterna specificata non include queste operazioni, utilizza gli strumenti del gestore delle chiavi esterne per modificare le operazioni o specifica una chiave esterna diversa.

Errori relativi alle operazioni di crittografia per la chiave esterna

Eccezioni: `KMSInvalidStateException`

Quando il proxy dell'archivio delle chiavi esterne non riesce a trovare la chiave esterna associata alla chiave KMS o la chiave esterna non soddisfa i requisiti per l'uso con una chiave KMS, l'operazione di crittografia ha esito negativo.

I problemi relativi alla chiave esterna rilevati durante un'operazione di crittografia sono più difficili da risolvere rispetto ai problemi rilevati prima della creazione della chiave KMS. Non puoi modificare l'ID della chiave esterna dopo la creazione della chiave KMS. Se la chiave KMS non ha ancora crittografato alcun dato, puoi eliminare la chiave KMS e crearne una nuova con un ID diverso. Tuttavia, il testo criptato generato con la chiave KMS non può essere decifrato da nessun'altra chiave KMS, nemmeno da una con la stessa chiave esterna, perché le chiavi avranno diversi metadati e materiali delle chiavi di AWS KMS. Al contrario, utilizza per quanto possibile gli strumenti del gestore delle chiavi esterne per risolvere il problema con la chiave esterna.

Quando il proxy dell'archivio delle chiavi esterne segnala un problema con la chiave esterna, le operazioni di crittografia restituiscono l'eccezione `KMSInvalidStateException` con un messaggio di errore che identifica il problema.

Chiave esterna non trovata

Quando il proxy dell'archivio chiavi esterno segnala di non riuscire a trovare la chiave esterna utilizzando l'ID della chiave esterna (XksKeyId) per la chiave KMS, le operazioni crittografiche restituiscono un `KMSInvalidStateException` con il seguente messaggio di errore.

Il proxy dell'archivio delle chiavi esterne ha rifiutato la richiesta perché non riusciva a trovare la chiave esterna.

Questo errore può verificarsi per i seguenti motivi:

- L'ID della chiave esterna (`XksKeyId`) per la chiave KMS non è più valido.

  Per trovare l'ID della chiave esterna associato alla chiave KMS, visualizza i dettagli della chiave KMS. Per individuare l'ID utilizzato dal proxy dell'archivio delle chiavi esterne per identificare la chiave esterna, consulta la documentazione del proxy o del gestore delle chiavi esterne.

  AWS KMS verifica l'ID della chiave esterna durante la creazione di una chiave KMS in un archivio delle chiavi esterne. Tuttavia, l'ID potrebbe non essere valido, soprattutto se il valore dell'ID della chiave esterna è un alias o un nome modificabile. Non puoi modificare l'ID della chiave esterna associato a una chiave KMS esistente. Per decrittografare un testo criptato generato con la chiave KMS, devi associare nuovamente la chiave esterna all'ID della chiave esterna esistente.

  Se non hai ancora utilizzato la chiave KMS per crittografare i dati, puoi creare una nuova chiave KMS con un ID della chiave esterna valido. Tuttavia, se hai generato un testo criptato con la chiave KMS, non puoi usare nessun'altra chiave KMS per decrittografarlo, anche se utilizza la stessa chiave esterna.
- La chiave esterna potrebbe essere stata eliminata dal gestore delle chiavi esterne. Per verificare, utilizza gli strumenti del gestore delle chiavi esterne. Se possibile, prova a recuperare il materiale della chiave da una copia o da un backup del gestore delle chiavi esterne. Se la chiave esterna viene eliminata definitivamente, qualsiasi testo criptato generato con la chiave KMS associata è irrecuperabile.

Errori di configurazione della chiave esterna

Quando il proxy dell'archivio delle chiavi esterne segnala che la chiave esterna non soddisfa i requisiti per l'uso con una chiave KMS, l'operazione di crittografia genera l'eccezione `KMSInvalidStateException` con uno dei seguenti messaggi di errore.

Il proxy dell'archivio delle chiavi esterne ha rifiutato la richiesta perché la chiave esterna non supporta l'operazione richiesta.

- La chiave esterna deve supportare sia la crittografia che la decrittografia. Se l'utilizzo della chiave non include queste due operazioni, utilizza gli strumenti del gestore delle chiavi esterne per modificarlo.

Il proxy dell'archivio delle chiavi esterne ha rifiutato la richiesta perché la chiave esterna non è abilitata nel gestore delle chiavi esterne.

- La chiave esterna deve essere abilitata e disponibile per l'uso nel gestore delle chiavi esterne. Se lo stato della chiave esterna non è `Enabled`, utilizza gli strumenti del gestore delle chiavi esterne per abilitarlo.

Problemi relativi al proxy

Eccezioni:

`CustomKeyStoreInvalidStateException` (`CreateKey`), `KMSInvalidStateException` (operazioni di crittografia), `UnsupportedOperationException`, `XksProxyUriUnreachableException`, `XksProxyInvalidResponseException` (operazioni di gestione diverse da `CreateKey`)

Il proxy dell'archivio delle chiavi esterne media tutte le comunicazioni tra AWS KMS e il gestore delle chiavi esterne, traducendo le richieste AWS KMS generiche in un formato comprensibile dal gestore. Se il proxy dell'archivio delle chiavi esterne non è conforme alla Specifica API relativa al proxy dell'archivio delle chiavi esterne di AWS KMS oppure non funziona correttamente o non è in grado di comunicare con AWS KMS, non potrai creare o utilizzare le chiavi KMS nell'archivio delle chiavi esterne.

Sebbene molti errori menzionino il proxy dell'archivio delle chiavi esterne a causa del suo ruolo fondamentale nell'architettura dell'archivio, tali problemi potrebbero avere origine nel gestore delle chiavi esterne o nella chiave esterna.

I problemi descritti in questa sezione riguardano errori relativi alla progettazione o al funzionamento del proxy dell'archivio delle chiavi esterne. La risoluzione di questi problemi potrebbe richiedere una modifica al software proxy. Rivolgiti al tuo amministratore proxy. Per aiutarti nell'eseguire la diagnostica dei problemi relativi al proxy, AWS KMS mette a disposizione un client di test XKS Proxy, un client open source che verifica la conformità del proxy dell'archivio delle chiavi esterne alla Specifica API relativa al proxy dell'archivio delle chiavi esterne di AWS KMS.

`CustomKeyStoreInvalidStateException` , `KMSInvalidStateException` o `XksProxyUriUnreachableException`
Il proxy dell'archivio delle chiavi esterne è in uno stato non integro. Se visualizzi questo messaggio ripetutamente, informa l'amministratore del proxy dell'archivio delle chiavi esterne.

- Questo errore può indicare un problema operativo o un errore software nel proxy dell'archivio delle chiavi esterne. È possibile trovare le voci di CloudTrail registro relative all'operazione AWS KMS API che ha generato ogni errore. Questo errore può essere risolto riprovando a eseguire l'operazione. Se persiste, contatta l'amministratore del proxy dell'archivio delle chiavi esterne.
- Quando il proxy dell'archivio di chiavi esterno segnala (in una GetHealthStatusrisposta) che tutte le istanze del gestore di chiavi esterno lo sono`UNAVAILABLE`, i tentativi di creare o aggiornare un archivio di chiavi esterno falliscono con questa eccezione. Se l'errore persiste, consulta la documentazione del gestore delle chiavi esterne.

`CustomKeyStoreInvalidStateException` , `KMSInvalidStateException` o `XksProxyInvalidResponseException`
AWS KMS non è in grado di interpretare la risposta proveniente dal proxy dell'archivio delle chiavi esterne. Se visualizzi questo errore ripetutamente, rivolgiti all'amministratore del proxy dell'archivio delle chiavi esterne.

- Le operazioni AWS KMS generano questa eccezione quando il proxy restituisce una risposta non definita che AWS KMS non è in grado di analizzare o interpretare. Questo errore può verificarsi occasionalmente a causa di problemi esterni temporanei o errori di rete sporadici. Se l'errore persiste, potrebbe indicare che il proxy dell'archivio delle chiavi esterne non è conforme alla Specifica API relativa al proxy dell'archivio delle chiavi esterne di AWS KMS. Informa l'amministratore o il fornitore dell'archivio delle chiavi esterne.

`CustomKeyStoreInvalidStateException` , `KMSInvalidStateException` o `UnsupportedOperationException`

Il proxy dell'archivio delle chiavi esterne ha rifiutato la richiesta in quanto non supporta l'operazione di crittografia richiesta.

- Il proxy dell'archivio delle chiavi esterne deve supportare tutte le API proxy definite nella Specifica API relativa al proxy dell'archivio delle chiavi esterne di AWS KMS. Questo errore indica che il proxy non supporta l'operazione correlata alla richiesta. Informa l'amministratore o il fornitore dell'archivio delle chiavi esterne.

Problemi relativi all'autorizzazione proxy

Eccezioni: `CustomKeyStoreInvalidStateException`, `KMSInvalidStateException`

Alcuni proxy degli archivi delle chiavi esterne implementano i requisiti di autorizzazione per l'uso delle relative chiavi esterne. Un proxy dell'archivio delle chiavi esterne è consentito, ma non obbligatorio, per progettare e implementare uno schema di autorizzazione che consenta a determinati utenti di richiedere operazioni particolari in determinate condizioni. Ad esempio, un proxy potrebbe consentire a un utente di eseguire la crittografia con una particolare chiave esterna, ma non di effettuare l'operazione inversa. Per ulteriori informazioni, consulta Autorizzazione proxy dell'archivio delle chiavi esterne (facoltativo).

L'autorizzazione proxy si basa sui metadati che AWS KMS include nelle richieste al proxy. I campi `awsSourceVpc` e `awsSourceVpce` sono inclusi nei metadati solo quando la richiesta proviene da un endpoint VPC e solo quando il chiamante si trova nello stesso account della chiave KMS.

```
"requestMetadata": {
    "awsPrincipalArn": string,
    "awsSourceVpc": string, // optional
    "awsSourceVpce": string, // optional
    "kmsKeyArn": string,
    "kmsOperation": string,
    "kmsRequestId": string,
    "kmsViaService": string // optional
}
```

Quando il proxy rifiuta una richiesta a causa di un errore di autorizzazione, l'operazione AWS KMS correlata ha esito negativo. `CreateKey` restituisce l'eccezione `CustomKeyStoreInvalidStateException`. Le operazioni di crittografia di AWS KMS generano l'eccezione `KMSInvalidStateException`. Entrambi utilizzano il messaggio di errore seguente:

> Il proxy dell'archivio delle chiavi esterne ha negato l'accesso all'operazione. Verifica che l'utente e la chiave esterna siano autorizzati per questa operazione e riprova a eseguire la richiesta.

- Per risolvere l'errore, utilizza il gestore delle chiavi esterne o gli strumenti del proxy per determinare il motivo per cui l'autorizzazione non è riuscita. Quindi, aggiorna la procedura che ha causato un errore nella richiesta di autorizzazione o utilizza gli strumenti del proxy dell'archivio delle chiavi esterne per aggiornare la policy di autorizzazione. Non puoi risolvere questo errore in AWS KMS.

Documentazione di riferimento dei tipi di chiave

AWS KMS supporta caratteristiche diverse per tipi di chiavi KMS differenti. Ad esempio, puoi utilizzare solo chiavi KMS di crittografia simmetrica per generare chiavi di dati simmetriche e coppie di chiavi di dati asimmetriche. Inoltre, l'importazione del materiale della chiave e la rotazione automatica delle chiavi sono supportate solo per le chiavi KMS di crittografia simmetrica e in un archivio delle chiavi personalizzate è possibile creare solo chiavi KMS di crittografia simmetrica.

Questo riferimento include due tabelle.

- La tabella dei tipi di chiave elenca le operazioni AWS KMS valide per le chiavi KMS di crittografia simmetrica, le chiavi KMS asimmetriche e le chiavi KMS HMAC.
- La tabella delle caratteristiche speciali elenca le operazioni AWS KMS valide per le chiavi KMS multi-regione, le chiavi KMS con materiale della chiave importato e le chiavi KMS negli archivi delle chiavi personalizzate.

Tabella dei tipi di chiave

Potrebbe essere necessario scorrere orizzontalmente o verticalmente per visualizzare tutti i dati di questa tabella.

Operazione API AWS KMS	Chiavi KMS di crittografia simmetrica	Chiavi KMS HMAC	Chiavi KMS asimmetriche (ENCRYPT_DECRYPT)	Chiavi KMS asimmetriche (SIGN_VERIFY)
CancelKeyDeletion	✓	✓	✓	✓

Operazione API AWS KMS	Chiavi KMS di crittografia simmetrica	Chiavi KMS HMAC	Chiavi KMS asimmetriche (ENCRYPT_DECRYPT)	Chiavi KMS asimmetriche (SIGN_VERIFY)
CreateAlias	✓	✓	✓	✓
CreateGrant	✓	✓	✓	✓
CreateKey	✓	✓	✓	✓
Decrypt	✓	⊗	✓	⊗
DeleteAlias	✓	✓	✓	✓
DeleteImportedKeyMaterial Valido solo nelle chiavi KMS con materiale della chiave importato (`Origin` è `EXTERNAL`).	✓	✓	✓	✓
DescribeKey	✓	✓	✓	✓
DisableKey	✓	✓	✓	✓

Operazione API AWS KMS	Chiavi KMS di crittografia simmetrica	Chiavi KMS HMAC	Chiavi KMS asimmetriche (ENCRYPT_DECRYPT)	Chiavi KMS asimmetriche (SIGN_VERIFY)
DisableKeyRotation	✓ Valido solo nelle chiavi KMS con materiale della chiave di AWS KMS (`Origin` is `AWS_KMS`).	⊗	⊗	⊗
EnableKey	✓	✓	✓	✓
EnableKeyRotation	✓ Valido solo nelle chiavi KMS con materiale della chiave di AWS KMS (`Origin` is `AWS_KMS`).	⊗	⊗	⊗
Encrypt	✓	⊗	✓	⊗

Operazione API AWS KMS	Chiavi KMS di crittografia simmetrica	Chiavi KMS HMAC	Chiavi KMS asimmetriche (ENCRYPT_DECRYPT)	Chiavi KMS asimmetriche (SIGN_VERIFY)
GenerateDataKey	✓	⊗	⊗	⊗
GenerateDataKeyPair Genera coppie di chiavi di dati asimmetriche protette da una chiave KMS di crittografia simmetrica.	✓ Non è valido per le chiavi KMS negli archivi delle chiavi personalizzate.	⊗	⊗	⊗
GenerateDataKeyPairWithoutPlaintext Genera coppie di chiavi di dati asimmetriche protette da una chiave KMS di crittografia simmetrica.	✓ Non è valido per le chiavi KMS negli archivi delle chiavi personalizzate.	⊗	⊗	⊗
GenerateDataKeyWithoutPlaintext	✓	⊗	⊗	⊗
GenerateMac	⊗	✓	⊗	⊗

Operazione API AWS KMS	Chiavi KMS di crittografia simmetrica	Chiavi KMS HMAC	Chiavi KMS asimmetriche (ENCRYPT_DECRYPT)	Chiavi KMS asimmetriche (SIGN_VERIFY)
GetKeyPolicy	✓	✓	✓	✓
GetKeyRotationStatus	✓	✓ (`KeyRotationEnabled` sarà sempre `false`).	✓ (`KeyRotationEnabled` sarà sempre `false`).	✓ (`KeyRotationEnabled` sarà sempre `false`).
GetParametersForImport Valido solo nelle chiavi KMS con materiale della chiave importato (`Origin` è `EXTERNAL`).	✓	✓	✓	✓
GetPublicKey	⊗	⊗	✓	✓
ImportKeyMaterial Valido solo nelle chiavi KMS con materiale della chiave importato (`Origin` è `EXTERNAL`).	✓	✓	✓	✓
ListAliases	✓	✓	✓	✓
ListGrants	✓	✓	✓	✓

Operazione API AWS KMS	Chiavi KMS di crittografia simmetrica	Chiavi KMS HMAC	Chiavi KMS asimmetriche (ENCRYPT_DECRYPT)	Chiavi KMS asimmetriche (SIGN_VERIFY)
ListKeyPolicies	✓	✓	✓	✓
ListResourceTags	✓	✓	✓	✓
ListRetirableGrants	✓	✓	✓	✓
PutKeyPolicy	✓	✓	✓	✓
ReEncrypt	✓	⊗	✓	⊗
ReplicateKey - Valido solo su chiavi multi-Regione	✓	✓	✓	✓
RetireGrant	✓	✓	✓	✓
RevokeGrant	✓	✓	✓	✓
ScheduleKeyDeletion	✓	✓	✓	✓
Sign	⊗	⊗	⊗	✓
TagResource	✓	✓	✓	✓
UntagResource	✓	✓	✓	✓

Operazione API AWS KMS	Chiavi KMS di crittografia simmetrica	Chiavi KMS HMAC	Chiavi KMS asimmetriche (ENCRYPT_DECRYPT)	Chiavi KMS asimmetriche (SIGN_VERIFY)
UpdateAlias La chiave KMS corrente e la nuova chiave KMS devono essere dello stesso tipo (entrambe simmetriche, asimmetriche o HMAC) e devono avere lo stesso utilizzo della chiave.	✓	✓	✓	✓
UpdateKeyDescription	✓	✓	✓	✓
UpdateReplicaRegion - Valido solo su chiavi multi-Regione	✓	✓	✓	✓
Verify	⊗	⊗	⊗	✓
VerifyMac	⊗	✓	⊗	⊗

Tabella delle caratteristiche speciali

Questa tabella mostra le operazioni API AWS KMS supportate su ogni tipo di chiave per scopi speciali.

Durante la lettura di questa tabella, tieni a mente le interazioni seguenti:

- Chiavi multi-regione:

  - Le chiavi KMS multi-regione possono essere costituite da chiavi KMS di crittografia simmetrica, chiavi KMS asimmetriche, chiavi KMS HMAC o chiavi KMS con materiale della chiave importato.
  - Non è possibile creare chiavi multi-regione in un archivio delle chiavi personalizzate.
- Materiale della chiave importato
  - Puoi importare il materiale della chiave per chiavi KMS di crittografia simmetrica, KMS asimmetriche e chiavi KMS HMAC.
  - Puoi creare chiavi multi-regione con materiale della chiave importato.
  - Non puoi creare chiavi con materiale della chiave importato in un archivio delle chiavi personalizzate.
  - La rotazione automatica delle chiavi (`EnableKeyRotation`, `DisableKeyRotation`) non è supportata per le chiavi KMS con materiale della chiave importato.
- store delle chiavi personalizzate
  - Gli archivi delle chiavi personalizzate supportano solo chiavi KMS di crittografia simmetrica.
  - Le operazioni di simmetria su coppie di chiavi asimmetriche (`GenerateDataKeyPair`, `GenerateDataKeyPairWithoutPlaintext`) non sono supportate sulle chiavi KMS negli archivi delle chiavi personalizzate.
  - La rotazione automatica delle chiavi (`EnableKeyRotation`, `DisableKeyRotation`) non è supportata sulle chiavi KMS negli archivi di chiavi personalizzate.
  - Non puoi creare chiavi multi-regione negli archivi delle chiavi personalizzate.

Potrebbe essere necessario scorrere orizzontalmente o verticalmente per visualizzare tutti i dati di questa tabella.

Operazione API AWS KMS	Chiavi multi-regione	Materiale della chiave importato	Chiavi KMS in un archivio delle chiavi personalizzate
CancelKeyDeletion	✓	✓	✓
CreateAlias	✓	✓	✓

Operazione API AWS KMS	Chiavi multi-regione	Materiale della chiave importato	Chiavi KMS in un archivio delle chiavi personalizzate
CreateGrant	✓	✓	✓
CreateKey Puoi utilizzare `CreateKey` per creare una chiave primaria multi-regione, una chiave KMS con materiale della chiave importato o una chiave KMS in un archivio delle chiavi personalizzate. Per creare una chiave di replica multi-regione, utilizza `ReplicateKey` .	✓	✓	✓
Decrypt	✓ Valido solo quando `KeyUsage` è `ENCRYPT_DECRYPT`	✓	✓
DeleteAlias	✓	✓	✓
DeleteImportedKeyMaterial	✓ Valido solo per le chiavi con materiale della chiave importato (`Origin` è `EXTERNAL`)	✓	⊗

Operazione API AWS KMS	Chiavi multi-regione	Materiale della chiave importato	Chiavi KMS in un archivio delle chiavi personalizzate
DescribeKey	✓	✓	✓
DisableKey	✓	✓	✓
DisableKeyRotation	✓ Valido solo su chiavi crittografiche simmetriche con materiale della chiave di AWS KMS (`Origin` è `AWS_KMS`).	⊗	⊗
EnableKey	✓ Valido solo su chiavi KMS di crittografia simmetrica	✓	✓

Operazione API AWS KMS	Chiavi multi-regione	Materiale della chiave importato	Chiavi KMS in un archivio delle chiavi personalizzate
EnableKeyRotation	✓ Valido solo su chiavi crittografiche simmetriche con materiale della chiave di AWS KMS (`Origin` è `AWS_KMS`).	⊗	⊗
Encrypt	✓ Valido solo quando `KeyUsage` è `ENCRYPT_DECRYPT`	✓	✓
GenerateDataKey	✓ Valido solo su chiavi KMS di crittografia simmetrica	✓	✓

Operazione API AWS KMS	Chiavi multi-regione	Materiale della chiave importato	Chiavi KMS in un archivio delle chiavi personalizzate
GenerateDataKeyPair	✓ Valido solo su chiavi KMS di crittografia simmetrica	✓	⊗
GenerateDataKeyPairWithoutPlaintext	✓ Valido solo su chiavi KMS di crittografia simmetrica	✓	⊗
GenerateDataKeyWithoutPlaintext	✓ Valido solo su chiavi KMS di crittografia simmetrica	✓	✓
GenerateMac Valido solo per chiavi KMS HMAC	✓	✓	⊗
GetKeyPolicy	✓	✓	✓

Operazione API AWS KMS	Chiavi multi-regione	Materiale della chiave importato	Chiavi KMS in un archivio delle chiavi personalizzate
GetKeyRotationStatus	✓	✓ (`KeyRotationEnabled` sarà sempre `false`).	⊗
GetParametersForImport	✓ Valido solo per le chiavi con materiale della chiave importato (`Origin` è `EXTERNAL`).	✓	⊗
GetPublicKey Valido solo per chiavi KMS asimmetriche.	✓	✓	⊗
ImportKeyMaterial	✓ Valido solo per le chiavi con materiale della chiave importato (`Origin` è `EXTERNAL`).	✓	⊗
ListAliases	✓	✓	✓

Operazione API AWS KMS	Chiavi multi-regione	Materiale della chiave importato	Chiavi KMS in un archivio delle chiavi personalizzate
ListGrants	✓	✓	✓
ListKeyPolicies	✓	✓	✓
ListResourceTags	✓	✓	✓
ListRetirableGrants	✓	✓	✓
PutKeyPolicy	✓	✓	✓
ReEncrypt	✓ Valido solo quando `KeyUsage` è `ENCRYPT_DECRYPT`	✓	✓
ReplicateKey	✓ Valido solo su chiavi primarie multi-regione.	✓ Valido solo su chiavi primarie multi-regione.	⊗
RetireGrant	✓	✓	✓
RevokeGrant	✓	✓	✓

Operazione API AWS KMS	Chiavi multi-regione	Materiale della chiave importato	Chiavi KMS in un archivio delle chiavi personalizzate
ScheduleKeyDeletion	✓	✓	✓
Sign Valido solo quando `KeyUsage` è `SIGN_VERIFY` .	✓	✓	⊗
TagResource	✓	✓	✓
UntagResource	✓	✓	✓
UpdateAlias - La chiave KMS corrente e la nuova chiave KMS devono essere dello stesso tipo (entrambe simmetriche, asimmetriche o HMAC) e devono avere lo stesso utilizzo della chiave.	✓	✓	✓
UpdateKeyDescription	✓	✓	✓
UpdateReplicaRegion	✓	✓ Valido solo su chiavi multi-regione.	⊗
Verify Valido solo quando `KeyUsage` è `SIGN_VERIFY` .	✓	✓	⊗

Operazione API AWS KMS	Chiavi multi-regione	Materiale della chiave importato	Chiavi KMS in un archivio delle chiavi personalizzate
VerifyMac Valido solo per chiavi KMS HMAC	✓	✓	⊗

Sicurezza di AWS Key Management Service

LaPer AWS, la sicurezza del cloud inhalaèmassimaprioritaria.priorità. In quanto cliente AWS, puoi trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle aziende più esigenti a livello di sicurezza.

La sicurezza è una responsabilità condivisa tra AWS e l'utente. Il modello di responsabilità condivisa descrive questo modello come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud – AWS è responsabile della protezione dell'infrastruttura che esegue i servizi AWS in AWS Cloud. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. Revisori di terze parti testano regolarmente e verificano l'efficacia della nostra sicurezza nell'ambito dei Programmi di conformità AWS. Per informazioni sui programmi di conformità applicabili a AWS Key Management Service (AWS KMS), consulta Servizi AWS coperti dal programma di conformità.
- Sicurezza nel cloud – La tua responsabilità è determinata dal servizio AWS che viene utilizzato. In AWS KMS, oltre alla configurazione e all'utilizzo delle AWS KMS keys, l'utente è responsabile di altri fattori, tra cui la sensibilità dei dati, i requisiti aziendali e le leggi e i regolamenti applicabili

Questa documentazione facilitaconsenteladicomprensionecomprenderedell’applicazionecomedelapplicare il modello di responsabilità condivisa quando utilizzisi usaAWS Key Management Service. SpiegaViene illustrato come configurare AWS KMS per soddisfare i tuoigli obiettivi di sicurezza e conformità.

Argomenti

- Protezione dei dati in AWS Key Management Service
- Gestione delle identità e degli accessi per l'AWS Key Management Service
- Registrazione e monitoraggio in AWS Key Management Service
- Convalida della conformità per AWS Key Management Service
- Resilienza nell'AWS Key Management Service
- Sicurezza dell'infrastruttura nell'AWS Key Management Service
- Best practice relative alla sicurezza di AWS Key Management Service

Protezione dei dati in AWS Key Management Service

AWS Key Management Servicememorizzaarchivia e protegge le tue chiavi di crittografia per renderle altamente disponibili, fornendotifornendo al tempo stessocontempo un controllo degli accessi efficace e flessibile.

Argomenti

Protezione del materiale della chiave

Per impostazione predefinita, AWS KMS genera e protegge il materiale delle chiavi crittografiche per le chiavi KMS. AWS KMS, inoltre, offre opzioni per il materiale della chiave creato e protetto all'esterno di AWS KMS. Per i dettagli tecnici sulle chiavi KMS e sul materiale della chiave, consulta Dettagli crittografici di AWS Key Management Service.

Protezione del materiale della chiave generato in AWS KMS

Quando crei una chiave KMS, per impostazione predefinita AWS KMS genera e protegge il materiale crittografico della chiave KMS.

Per proteggere il materiale della chiave per le chiavi KMS, AWS KMS si basa su un parco istanze distribuito di moduli di sicurezza hardware (HSM) con convalida del livello di sicurezza 3 FIPS 140-2. Ogni HSM AWS KMS è un dispositivo hardware crittografico standalone progettato per fornire funzioni crittografiche dedicate per soddisfare i requisiti di sicurezza e scalabilità di AWS KMS. (I moduli HSM utilizzati da AWS KMS nelle regioni della Cina sono dotati di certificazione OSCCA e sono conformi a tutte le normative cinesi pertinenti, ma sono privi di convalida in base al Programma di convalida dei moduli crittografici FIPS 140-2.)

Il materiale della chiave per una chiave KMS è crittografato per impostazione predefinita quando viene generato nel modulo HSM. Il materiale della chiave viene decrittografato solo nella memoria volatile del modulo HSM e solo per i pochi millisecondi necessari per utilizzarlo in un'operazione crittografica. Ogni volta che il materiale della chiave non viene utilizzato attivamente, viene crittografato nel modulo HSM e trasferito su uno storage persistente a bassa latenza e altamente durevole (99,999999999%), dove rimane separato e isolato dai moduli HSM. Il materiale della

chiave in testo normale mantiene sempre i limiti di sicurezza HSM, non viene mai scritto su disco né memorizzato su alcun supporto di memorizzazione. (L'unica eccezione è la chiave pubblica di una coppia di chiavi asimmetriche, che non è segreta.)

AWS attesta come principio di sicurezza fondamentale che in ogni Servizio AWS non avviene alcuna interazione umana (di alcun tipo e in alcun modo) con il materiale della chiave crittografica in testo normale. Non esiste alcun meccanismo che consenta a qualcuno, inclusi gli operatori Servizio AWS, di visualizzare, accedere o esportare il materiale della chiave in testo normale. Questo principio si applica anche in caso di guasti catastrofici ed eventi di ripristino di emergenza. Il materiale della chiave del cliente in testo normale in AWS KMS viene utilizzato per operazioni nei moduli HMS con convalida FIPS AWS KMS solo in risposta a richieste autorizzate inviate al servizio dal cliente o da una persona delegata da questo.

Per le chiavi gestite dal cliente, l'Account AWS che crea la chiave è l'unico proprietario non trasferibile della chiave. L'account proprietario ha il controllo completo ed esclusivo delle policy di autorizzazione che controllano l'accesso alla chiave. Per le Chiavi gestite da AWS, l'Account AWS ha il controllo completo delle policy IAM che autorizzano le richieste al Servizio AWS.

Protezione del materiale della chiave generato esternamente a AWS KMS

AWS KMS fornisce alternative al materiale della chiave generato in AWS KMS.

Gli archivi di chiavi personalizzate, una funzionalità AWS KMS opzionale, consentono la creazione di chiavi KMS supportate dal materiale della chiave generato e utilizzato esternamente a AWS KMS. Le chiavi KMS negli archivi di chiavi AWS CloudHSM sono supportate dalle chiavi in moduli di sicurezza hardware AWS CloudHSM sotto il tuo controllo. Questi moduli HMS sono dotati di certificati del livello di sicurezza 3 FIPS 140-2. Le chiavi KMS negli archivi di chiavi esterni sono supportate dalle chiavi di un gestore di chiavi esterno che puoi controllare e gestire esternamente a AWS, ad esempio un modulo HSM fisico nel tuo data center privato.

Un'altra caratteristica opzionale consente di importare il materiale della chiave per una chiave KMS. Per proteggere il materiale della chiave importato mentre viene trasferito a AWS KMS, puoi crittografare il materiale della chiave utilizzando una chiave pubblica da una coppia di chiavi RSA generata in un modulo HSM AWS KMS. Il materiale della chiave importato viene decrittografato in un modulo HSM AWS KMS e crittografato nuovamente in una chiave simmetrica nel modulo HSM. Come tutto il materiale della chiave AWS KMS, il materiale della chiave importato in testo normale rimane sempre nei moduli HSM crittografati. Tuttavia, il cliente che ha fornito il materiale della chiave è responsabile dell'uso sicuro, della durabilità e della manutenzione del materiale della chiave esternamente a AWS KMS.

Crittografia dei dati

I dati in AWS KMS sono costituiti da AWS KMS keys e dal materiale chiave di crittografia che rappresentano. Questo materiale della chiave è in testo normale solo all'interno dei moduli di sicurezza hardware (HSM) diAWS KMS e solo quando è in uso. In caso contrario, il materiale della chiave viene crittografato e memorizzato in uno storage persistente durevole.

Il materiale della chiave generato da AWS KMS per le chiavi KMS non supera mai il limite dei moduli HMS di AWS KMS non crittografati. Non viene esportato néo trasmesso in alcuna operazione dell'API AWS KMS. L'eccezione è per le chiavi multi-regione, dove AWS KMS utilizza un meccanismo di replica tra regioni per copiare il materiale della chiave per una chiave multi-regione da un HSM in una in una Regione AWS a un HSM in un'altra Regione AWS. Per informazioni dettagliate, consulta Processo di replica per chiavi multi-regione in Dettagli della crittografia di AWS Key Management Service.

Argomenti

- Crittografia a riposo
- Crittografia dei dati in transito

Crittografia a riposo

AWS KMS genera il materiale della chiave per le AWS KMS keys in moduli di sicurezza hardware (HSM) conformi al livello di sicurezza 3 FIPS 140-2. L'unica eccezione è rappresentata dalle regioni della Cina, dove gli HSM utilizzati da AWS KMS per generare chiavi KMS sono conformi a tutte le normative cinesi pertinenti, ma non sono convalidati nell'ambito del programma FIPS 140-2 Cryptographic Module Validation. Quando non in uso, il materiale della chiave viene crittografato da una chiave HSM e scritto in uno storage persistente e durevole. Il materiale della chiave per le chiavi KMS e le chiavi di crittografia che proteggono il materiale della chiave non lasciano mai i moduli di sicurezza hardware in formato di testo normale.

La cifratura e la gestione del materiale della chiave per le chiavi KMS sono eseguite interamente da AWS KMS.

Per ulteriori dettagli, consulta Utilizzo di AWS KMS keys in Dettagli crittografici di AWS Key Management Service.

Crittografia dei dati in transito

Il materiale chiave generato da AWS KMS per le chiavi KMS non viene mai esportato o trasmesso nelle operazioni API AWS KMS. AWS KMS utilizza gli identificatori delle chiavi per rappresentare le chiavi KMS nelle operazioni API. Analogamente, il materiale della chiave per chiavi KMS negli archivi delle chiavi personalizzate di AWS KMS non è esportabile e non viene mai trasmesso nelle operazioni dell'API AWS KMS o AWS CloudHSM.

Tuttavia, alcune operazioni API AWS KMS restituiscono le chiavi dati. Inoltre, i clienti possono utilizzare le operazioni API per importare il materiale chiave per chiavi KMS selezionate.

Tutte le chiamate API AWS KMS devono essere firmate e trasmesse tramite Transport Layer Security (TLS). AWS KMS richiede l'utilizzo di TLS 1.2 e suggerisce l'utilizzo di TLS 1.3 in tutte le regioni. AWS KMS supporta anche TLS post-quantistico ibrido per gli endpoint del servizio AWS KMS in tutte le regioni, ad eccezione delle regioni cinesi. AWS KMS non supporta TLS post-quantistico ibrido per gli endpoint FIPS in AWS GovCloud (US). Le chiamate a AWS KMS richiedono anche una moderna suite di cifratura che supporti la perfect forward secrecy, il che significa che il compromesso di qualsiasi segreto, come una chiave privata, non compromette anche la chiave della sessione.

Se necessiti di moduli crittografici convalidati FIPS 140-2 quando accedi ad AWSattraverso un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per utilizzare endpoint AWS KMS standard o endpoint AWS KMS, i client devono supportare TLS 1.2 o versioni successive. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2. Per un elenco degli endpoint FIPS AWS KMS, consulta Endpoint e quote AWS Key Management Service nella Riferimenti generali di AWS.

Le comunicazioni tra gli host del servizio AWS KMS e i moduli di sicurezza hardware sono protette utilizzando Elliptic Curve Cryptography (ECC) e Advanced Encryption Standard (AES) in uno schema di crittografia autenticato. Per ulteriori dettagli, consulta Sicurezza delle comunicazioni interne in Dettagli crittografici di AWS Key Management Service

Riservatezza del traffico Internet

AWS KMS supporta una AWS Management Console e un set di operazioni API che consentono di creare e gestire le AWS KMS keys e di utilizzarle nelle operazioni di crittografia.

AWS KMS supporta due opzioni di connettività dalla rete privata ad AWS.

- Una connessione VPN IPSec tramite Internet

- AWS Direct Connect, collega la rete interna a una località AWS Direct Connect tramite un cavo Ethernet standard in fibra ottica.

Tutte le chiamate dell'API AWS KMS devono essere firmate e trasmesse utilizzando il Transport Layer Security (TLS). Le chiamate richiedono anche una moderna suite di cifratura che supporta la perfect forward secrecy. Il traffico verso i moduli di sicurezza hardware (HSM) che memorizzano il materiale della chiave per le chiavi KMS è consentito solo da host API AWS KMS noti sulla rete AWS interna.

Per connettersi direttamente a AWS KMS dal cloud privato virtuale (VPC) senza inviare traffico su Internet pubblico, utilizza gli endpoint VPC basati su AWS PrivateLink. Per ulteriori informazioni, consultare Connessione a AWS KMS mediante un endpoint VPC.

AWS KMS supporta anche l'opzione scambio di chiavi post-quantistiche ibride per il protocollo di crittografia di rete Transport Layer Security (TLS). Puoi utilizzare questa opzione con TLS quando ti connetti agli endpoint dell'API AWS KMS.

Gestione delle identità e degli accessi per l'AWS Key Management Service

AWS Identity and Access Management (IAM) aiuta a controllare in modo sicuro l'accesso alle risorse AWS. Gli amministratori controllano chi è autenticato (accesso effettuato) e autorizzato (dispone di autorizzazioni) a utilizzare risorse AWS KMS. Per ulteriori informazioni, consulta Utilizzo delle policy IAM con AWS KMS.

Le policy chiave sono il meccanismo principale per controllare l'accesso alle chiavi KMS in AWS KMS. Ogni chiave KMS deve avere una policy chiave. Puoi inoltre utilizzare le policy IAM e le concessioni, insieme alle policy delle chiavi, per controllare l'accesso alle chiavi KMS. Per ulteriori informazioni, consulta Autenticazione e controllo degli accessi per AWS KMS.

Se utilizzi un Amazon Virtual Private Cloud (Amazon VPC), puoi creare un endpoint VPC dell'interfaccia su AWS KMS con AWS PrivateLink. Inoltre puoi utilizzare le policy di endpoint VPC per determinare quali principali possono accedere all'endpoint AWS KMS, quali chiamate API possono effettuare e a quali chiavi KMS possono accedere. Per informazioni dettagliate, vedi Controllo dell'accesso all'endpoint VPC.

Registrazione e monitoraggio in AWS Key Management Service

Il monitoraggio è una parte importante della comprensione della disponibilità, dello stato e dell'utilizzo delle AWS KMS keys in AWS KMS. Il monitoraggio aiuta a mantenere la sicurezza, l'affidabilità, la disponibilità e le prestazioni delle soluzioni AWS. AWS fornisce diversi strumenti per monitorare le chiavi KMS.

File di log di AWS CloudTrail

Ogni chiamata a un'operazione dell'API AWS KMS viene acquisita come evento in un log di AWS CloudTrail. Questi log registrano tutte le chiamate API dalla console AWS KMS e le chiamate effettuate da AWS KMS e altri servizi AWS. Le chiamate API tra account, ad esempio una chiamata per utilizzare una chiave KMS in un'altraAccount AWS, vengono registrate nei CloudTrail log di entrambi gli account.

Durante la risoluzione dei problemi o il controllo puoi utilizzare il log per ricostruire il ciclo di vita di una chiave KMS. Puoi inoltre visualizzare la gestione e l'utilizzo della chiave KMS nelle operazioni di crittografia. Per ulteriori informazioni, consulta the section called “Registrazione con AWS CloudTrail”.

CloudWatch Registri Amazon

Monitora, archivia e accedi ai file di log da AWS CloudTrail e altre origini. Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.

InfattiAWS KMS, CloudWatch memorizza informazioni utili che ti aiutano a prevenire problemi con le tue chiavi KMS e le risorse che proteggono. Per ulteriori informazioni, consulta the section called “Monitoraggio con CloudWatch”.

Amazon EventBridge

AWS KMSgenera EventBridge eventi quando la chiave KMS viene ruotata o eliminata o il materiale chiave importato nella chiave KMS scade. Cerca gli eventi AWS KMS (operazioni API) e instradali a una o più funzioni o flussi di destinazione per acquisire le informazioni sullo stato. Per ulteriori informazioni, consulta the section called “Monitoraggio con Amazon EventBridge” la Amazon EventBridge User Guide.

CloudWatch Metriche Amazon

Puoi monitorare le tue chiavi KMS utilizzando i CloudWatch parametri, che raccolgono ed elaborano dati grezzi per trasformarli in metriche prestazionali. AWS KMS I dati vengono registrati

a intervalli di due settimane in modo da poter visualizzare le tendenze delle informazioni correnti e cronologiche. Questo ti aiuta a capire come vengono usate le tue chiavi KMS e come il loro utilizzo cambia nel tempo. Per informazioni sull'utilizzo delle CloudWatch metriche per monitorare le chiavi KMS, consulta. Parametri e dimensioni di AWS KMS

CloudWatch Allarmi Amazon

Osserva una singola modifica del parametro in un periodo di tempo specificato. Quindi esegui una o più operazioni basate sul valore del parametro relativo a una soglia per un certo numero di periodi. Ad esempio, puoi creare un CloudWatch allarme che viene attivato quando qualcuno tenta di utilizzare una chiave KMS la cui eliminazione è pianificata in un'operazione crittografica. Ciò indica che la chiave KMS è ancora in uso e probabilmente non dovrebbe essere eliminata. Per ulteriori informazioni, consulta the section called “Creazione di un allarme ”.

AWS Security Hub

Puoi monitorare l'uso di AWS KMS per verificare gli standard del settore della sicurezza e la conformità alle procedure consigliate utilizzando AWS Security Hub. Security Hub utilizza controlli di sicurezza per valutare le configurazioni delle risorse e gli standard di sicurezza per aiutarti a rispettare vari framework di conformità. Per ulteriori informazioni, consulta Controlli di AWS Key Management Service nella Guida per l'utente di AWS Security Hub.

Convalida della conformità per AWS Key Management Service

Revisori di terze parti valutano la sicurezza e la conformità di AWS Key Management Service come parte di più programmi di conformità di AWS. Questi includono SOC, PCI, FedRAMP, HIPAA e altri.

Argomenti

- Documenti di conformità e sicurezza
- Ulteriori informazioni

Documenti di conformità e sicurezza

I seguenti documenti di conformità e sicurezza riguardano AWS KMS. Per visualizzarli, usa AWS Artifact.

- Cloud Computing Compliance Controls Catalogue (C5)
- ISO 27001:2013 Statement of Applicability (SoA)

- Certificazione ISO 27001:2013
- ISO 27017:2015 Statement of Applicability (SoA)
- Certificazione ISO 27017:2015
- ISO 27018:2015 Statement of Applicability (SoA)
- Certificazione ISO 27018:2014
- Certificazione ISO 9001:2015
- Attestazione di conformità allo standard DSS PCI e riepilogo delle responsabilità
- Service Organization Controls (SOC) 1 Report
- Service Organization Controls (SOC) 2 Report
- Service Organization Controls (SOC) 2 Report For Confidentiality
- FedRAMP-High

Per informazioni sull'utilizzo di AWS Artifact, consulta Download di report in AWS Artifact.

Ulteriori informazioni

La tua responsabilità di conformità durante l'utilizzo di AWS KMS è determinata dalla riservatezza dei dati, dagli obiettivi dell'azienda e dalle leggi e normative applicabili. Se l'utilizzo di AWS KMS è soggetto a conformità con uno standard pubblicato, AWS fornisce risorse utili:

- Servizi AWS coperti dal programma di conformità – Questa pagina elenca i servizi AWS che rientrano nell'ambito di programmi di conformità specifici. Per informazioni generali, consulta Programmi di conformità di AWS.
- Guide Quick Start per la sicurezza e conformità: queste guide all'implementazione illustrano considerazioni relative all'architettura e forniscono fasi per l'implementazione di ambienti di base incentrati sulla sicurezza e sulla conformità su AWS.
- Risorse per la conformità di AWS: questa raccolta di workbook e guide potrebbe essere utile al settore e alla posizione.
- AWS Config: questo servizio AWS valuta il livello di conformità delle configurazioni delle risorse con pratiche interne, linee guida e regolamenti di settore.
- AWS Security Hub: questo servizio AWS fornisce una vista completa dello stato di sicurezza in AWS. La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWSe verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi

e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.

Resilienza nell'AWS Key Management Service

L'infrastruttura globale di AWS è progettata attorno a Regioni AWS e zone di disponibilità. Regioni AWS fornisce più zone di disponibilità fisicamente separate e isolate che sono connesse tramite reti altamente ridondanti, a bassa latenza e velocità effettiva elevata. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture tradizionali a data center singolo o multiplo.

Oltre all'infrastruttura globale di AWS, AWS KMS offre numerose funzionalità per supportare la resilienza dei dati e le esigenze di backup. Per ulteriori informazioni sulle Regioni AWS e le zone di disponibilità, consulta Infrastruttura globale di AWS.

Isolamento regionale

AWS Key Management Service (AWS KMS) è un servizio regionale autonomo che è disponibile in tutte le Regioni AWS. Il design isolato a livello di regione di AWS KMS assicura che un problema di disponibilità in una singola Regione AWS non può influire sul funzionamento di AWS KMS in altre regioni. AWS KMS è progettato per garantire l'assenza di tempi inattività pianificati, con tutti gli aggiornamenti software e le operazioni di scalabilità eseguite senza interruzioni e in maniera impercettibile.

L'Accordo sul livello di servizio (SLA) di AWS KMS include un impegno di servizio del 99,999% per tutte le API KMS. Per portare a termine questo impegno, AWS KMS garantisce che tutti i dati e le informazioni di autorizzazione necessarie per eseguire una richiesta API siano disponibili su tutti gli host regionali che ricevono la richiesta.

L'infrastruttura AWS KMS viene replicata in almeno tre zone di disponibilità in ogni regione. Per garantire che più errori host non influiscano sulle prestazioni di AWS KMS, AWS KMS è progettato per gestire il traffico dei clienti da qualsiasi zona di disponibilità in una regione.

Le modifiche apportate alle proprietà o alle autorizzazioni di una chiave KMS vengono replicate in tutti gli host della regione per garantire che la richiesta successiva possa essere elaborata correttamente da qualunque host nella regione. Le richieste di operazioni di crittografia tramite la chiave KMS vengono inoltrate a un parco istanze di moduli di sicurezza hardware (HSM) AWS KMS, ognuno dei quali può eseguire l'operazione con la chiave KMS.

Design multi-tenant

Il design multi-tenant di AWS KMS consente di soddisfare l'SLA di disponibilità al 99,999% e di sostenere elevati tassi di richieste, proteggendo al tempo stesso la riservatezza delle chiavi e dei dati.

Sono implementati più meccanismi di applicazione dell'integrità per garantire che la chiave KMS specificata per l'operazione crittografica sia sempre quella utilizzata.

Il materiale della chiave in testo normale per le chiavi KMS è ampiamente protetto. Il materiale della chiave viene crittografato nel modulo HSM non appena viene creato e quest'ultimo viene spostato immediatamente in uno storage sicuro a bassa latenza. La chiave crittografata viene recuperata e decrittografata all'interno del modulo HSM solo nel momento in cui viene utilizzata. La chiave in testo normale rimane nella memoria HSM solo per il tempo necessario al completamento dell'operazione di crittografia. Dopo di che, viene nuovamente crittografata nel modulo HSM e la chiave crittografata viene restituita allo storage. Il materiale della chiave in testo normale non lascia mai i moduli HSM e non viene mai scritto su storage persistente.

Per ulteriori informazioni sui meccanismi utilizzati da AWS KMS per proteggere le chiavi, consulta Dettagli di crittografia di AWS Key Management Service.

Best practice relative alla resilienza di AWS KMS

Per ottimizzare la resilienza delle tue risorse AWS KMS, valuta le strategie seguenti.

- Per il supporto della strategia di backup e ripristino di emergenza, valuta le chiavi multi-regione, costituite da chiavi KMS create in un'unica Regione AWS e replicate solo nelle regioni che hai specificato. Con le chiavi multi-regione, puoi spostare risorse crittografate tra Regioni AWS (all'interno della stessa partizione) senza mai esporre il testo normale e decrittografare la risorsa, quando necessario, in una delle regioni di destinazione. Le chiavi multi-regione correlate sono interoperabili perché condividono lo stesso materiale e lo stesso ID, ma hanno policy indipendenti per il controllo degli accessi ad alta risoluzione. Per informazioni dettagliate, consulta Chiavi multi-regione in AWS KMS.
- Per proteggere le chiavi in un servizio multi-tenant come AWS KMS, utilizza i controlli degli accessi, incluse policy delle chiavi e policy IAM. Inoltre, puoi inviare le tue richieste a AWS KMS tramite un endpoint dell'interfaccia VPC con tecnologia AWS PrivateLink. In tal modo, tutta la comunicazione tra Amazon VPC e AWS KMS avviene interamente nella rete AWS che utilizza un endpoint AWS KMS dedicato limitato al tuo cloud VPC. Puoi proteggere ulteriormente queste richieste creando un livello di autorizzazione aggiuntivo tramite le policy degli endpoint VPC. Per ulteriori dettagli, consulta Connessione a AWS KMS mediante un endpoint VPC.

Sicurezza dell'infrastruttura nell'AWS Key Management Service

In qualità di servizio gestito, AWS Key Management Service (AWS KMS) è protetto dalle procedure di sicurezza di rete globali di AWS descritte nel whitepaper Panoramica delle procedure di sicurezza di Amazon Web Services.

Per accedere a AWS KMS tramite la rete, puoi richiamare le operazioni dell'API AWS KMS descritte nella Documentazione di riferimento dell'API AWS Key Management Service. AWS KMS richiede l'utilizzo di TLS 1.2 e suggerisce l'utilizzo di TLS 1.3 in tutte le regioni. AWS KMS supporta anche TLS ibrido post-quantistico per gli endpoint del servizio AWS KMS in tutte le regioni, ad eccezione delle regioni cinesi. AWS KMS non supporta il protocollo TLS post-quantistico ibrido per gli endpoint FIPS in AWS GovCloud (US). Per utilizzare endpoint standard AWS KMS o endpoint FIPS AWS KMS, i client devono supportare TLS 1.2 o versioni successive. I client devono, inoltre, supportare le suite di crittografia con PFS (Perfect Forward Secrecy), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un chiave di accesso ID e una chiave di accesso segreta associata a un account principale IAM. O puoi utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Puoi chiamare queste operazioni API da qualsiasi percorso di rete, ma AWS KMS supporta le condizioni delle policy globali che consentono di controllare l'accesso a una chiave KMS in base all'indirizzo IP di origine, al VPC e all'endpoint VPC. È possibile utilizzare le chiavi di condizione globali nelle policy delle chiavi e nelle policy IAM. Tuttavia, queste condizioni possono impedire ad AWS l'utilizzo della chiave KMS per tuo conto. Per informazioni dettagliate, vedi AWS chiavi di condizione globali.

Ad esempio, l'istruzione della policy chiave seguente consente agli utenti che possono assumere il ruolo `KMSTestRole` di utilizzare questa AWS KMS key per le operazioni di crittografia specificate, a meno che l'indirizzo IP di origine non sia uno degli indirizzi IP specificati nella policy.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {"AWS":
    "arn:aws:iam::111122223333:role/KMSTestRole"},
    "Action": [
```

```
      "kms:Encrypt",
      "kms:Decrypt",
      "kms:ReEncrypt*",
      "kms:GenerateDataKey*",
      "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
      "NotIpAddress": {
        "aws:SourceIp": [
          "192.0.2.0/24",
          "203.0.113.0/24"
        ]
      }
    }
  }
}
```

Isolamento di host fisici

La sicurezza dell'infrastruttura fisica utilizzata da AWS KMS è soggetta ai controlli descritti nella sezione Sicurezza fisica e ambientale del whitepaper Panoramica delle procedure di sicurezza di Amazon Web Services. Puoi trovare altri dettagli nei report di conformità e nei risultati degli audit di terze parti elencati nella sezione precedente.

AWS KMS è supportato dai moduli HSM (Hardened Hardware Security Module) dedicati progettati con controlli specifici per resistere agli attacchi fisici. I moduli HSM sono dispositivi fisici che non dispongono di un livello di virtualizzazione, ad esempio un hypervisor, che condivide il dispositivo fisico tra diversi tenant logici. Il materiale chiave per le AWS KMS keys viene archiviato solo nella memoria volatile sui moduli HSM e solo quando la chiave KMS è in uso. Questa memoria viene cancellata quando il modulo HSM non è in stato operativo, inclusi arresti e ripristini previsti e non intenzionali. Per informazioni dettagliate sull'operazione dei moduli HSM AWS KMS, consulta i Dettagli crittografici di AWS Key Management Service..

Best practice relative alla sicurezza di AWS Key Management Service

AWS Key Management Service (AWS KMS) supporta molte caratteristiche di sicurezza che possono essere implementate per migliorare la protezione delle chiavi di crittografia, tra cui policy delle

chiavi e policy IAM, un'opzione del contesto di crittografia per operazioni di crittografia su chiavi di crittografia simmetriche, un ampio set di chiavi di condizione per perfezionare policy delle chiavi e policy IAM e vincoli di concessione per limitare le concessioni.

Queste caratteristiche di sicurezza sono descritte in dettaglio nella sezione Best practice di AWS Key Management Service (PDF). Le linee guida generali in questo documento tecnico non rappresentano una soluzione di sicurezza completa. Poiché non tutte le best practice sono appropriate per tutte le situazioni, non sono prescrittive.

Consulta anche

- Best practice per le policy IAM
- Best practice per le concessioni AWS KMS
- Best practice per la sicurezza in IAM nella Guida per l'utente di IAM

Quote

Per rendere AWS KMS reattivo e performante per tutti gli utenti, AWS KMS applica due tipi di quote: quote di risorse e quote di richieste. Ogni quota viene calcolata in modo indipendente per ogni Regione di ciascun Account AWS.

Tutte le quote AWS KMS sono modificabili, ad eccezione della quota delle risorse delle dimensioni del documento della policy della chiave e della quota delle risorse per archivi di chiavi AWS CloudHSM. Per richiedere un aumento delle quote, consultare Richiesta di aumento delle quote nella Guida dell'utente di Service Quotas. Per richiedere una riduzione della quota, per modificare una quota non elencata in Service Quotas o per modificare una quota in una Regione AWS in cui le Service Quotas per AWS KMS non sono disponibili, visita il Centro AWS Support e crea un caso.

Argomenti

Quote delle risorse

AWS KMS stabilisce delle quote per le risorse al fine di garantire un servizio rapido e resiliente a tutti i nostri clienti. Alcune quote di risorse si applicano solo alle risorse create dall'utente, ma non a quelle create dai servizi AWS. Le risorse che utilizzi, ma che non sono nel tuo account Account AWS, come Chiavi di proprietà di AWS, non vengono considerate nel calcolo di queste quote.

Se viene superato un limite di risorse, le richieste per creare una risorsa aggiuntiva di quel tipo generano il messaggio di errore `LimitExceededException`.

Tutte le quote di risorse AWS KMS sono regolabili, ad eccezione della quota delle dimensioni del documento della policy chiave. Per richiedere un aumento delle quote, consultare Richiesta di aumento delle quote nella Guida dell'utente di Service Quotas. Per richiedere una riduzione della quota, per modificare una quota non elencata in Service Quotas o per modificare una quota in una Regione AWS in cui le Service Quotas per AWS KMS non sono disponibili, visita il Centro AWS Support e crea un caso.

Nella tabella seguente sono elencate e descritte le quote delle risorse AWS KMS in ogni Account AWS e Regione.

Nome quota	Valore predefinito	Si applica a	Regolabile
AWS KMS keys	100.000	Chiavi gestite dal cliente	Sì
Alias per chiave KMS	50	Alias creati dal cliente	Sì
Autorizzazioni per chiave KMS	50.000	Chiavi gestite dal cliente	Sì
Dimensione del documento di policy delle chiavi	32 KB (32.768 byte)	Chiavi gestite dal cliente Chiavi gestite da AWS	No
Quote di risorse per l'archivio delle chiavi personalizzate	10	Account AWS e regione	Sì

Oltre alle quote delle risorse, AWS KMS utilizza per garantire la reattività del servizio. Per informazioni dettagliate, vedi the section called “Quote di richieste”.

AWS KMS keys: 100.000

Puoi avere fino a 100.000 chiavi gestite dal cliente in ciascuna Regione dell'Account AWS. Questa quota si applica a tutte le chiavi gestite dal cliente in tutte le Regioni AWS indipendentemente dalla specifica della chiave o dallo stato della chiave. Ogni chiave KMS è considerata una risorsa. Chiavi gestite da AWS e Chiavi di proprietà di AWS non rientrano nel calcolo di questa quota.

Alias per chiave KMS: 50

Puoi associare fino a 50 alias a ciascuna chiave gestita dal cliente. Gli alias che AWS associa alle Chiavi gestite da AWS non vengono conteggiati in questa quota. Questa quota potrebbe essere interessata quando crei o aggiorni un alias.

> **Note**
>
> La ResourceAliases condizione kms: è efficace solo quando la chiave KMS è conforme a questa quota. Se una chiave KMS supera questa quota, alle entità principali autorizzate a

usare la chiave KMS tramite la condizione `kms:ResourceAliases` viene negato l'accesso alla chiave KMS. Per informazioni dettagliate, vedi Accesso negato a causa di quota alias.

La quota di alias per chiave KMS sostituisce la quota di alias per Regione che ha limitato il numero totale di alias in ogni Regione di un Account AWS. AWS KMS ha eliminato la quota di alias per Regione.

Concessioni per chiave KMS: 50.000

Ogni chiave gestita dal cliente può avere fino a 50.000 concessioni, incluse le concessioni create dai servizi AWS integrati con AWS KMS. Questa quota non si applica alle Chiavi gestite da AWS o alle Chiavi di proprietà di AWS.

Un effetto di questa quota è che non è possibile eseguire più di 50.000 operazioni concesse che utilizzano la stessa chiave KMS contemporaneamente. Una volta raggiunta la quota, puoi creare nuove concessioni sulla chiave KMS solo quando una concessione attiva viene ritirata o revocata.

Ad esempio, quando alleghi un volume Amazon Elastic Block Store (Amazon EBS) a un'istanza Amazon Elastic Compute Cloud (Amazon EC2), il volume viene decrittato in modo che sia leggibile. Per ottenere l'autorizzazione per decrittare i dati, Amazon EBS crea una concessione per ogni volume. Pertanto, se tutti i volumi Amazon EBS utilizzano la stessa chiave KMS, non è possibile collegare più di 50.000 volumi contemporaneamente.

Dimensione del documento di policy delle chiavi: 32 KB

La lunghezza massima di ciascun documento di policy delle chiavi è 32 KB (32.768 byte). Se usi un documento di policy di dimensioni maggiori per creare o aggiornare la policy delle chiavi per una chiave KMS, l'operazione non riesce.

Questa quota non è regolabile. Non è possibile aumentarla utilizzando Service Quotas o creando un ticket in AWS Support. Se la policy delle chiavi si sta avvicinando al limite, ti consigliamo di usare le concessioni invece delle dichiarazioni di policy. Le autorizzazioni sono particolarmente adatte a permessi temporanei o molto specifici.

Si utilizza un documento di politica chiave ogni volta che si crea o si modifica una politica chiave utilizzando la visualizzazione predefinita o la visualizzazione delle politiche nell'operazione AWS Management Console o. PutKeyPolicy Questa quota si applica al documento di policy delle chiavi, anche se si utilizza la visualizzazione predefinita nella console AWS KMS, in cui le istruzioni JSON non vengono modificate direttamente.

Quote di risorse per gli archivi delle chiavi personalizzate: 10

Puoi creare fino a 10 archivi delle chiavi personalizzate in ogni Account AWS e regione. Se si tenta di crearne altri, l'CreateCustomKeyStoreoperazione ha esito negativo.

Questa quota si applica al numero totale di archivi delle chiavi personalizzate in ogni account e regione, inclusi tutti gli archivi delle chiavi di AWS CloudHSM e gli archivi delle chiavi esterne, indipendentemente dallo stato della connessione.

Quote di richieste

AWS KMS stabilisce delle quote per il numero di operazioni API richieste per ogni secondo. Le quote di richieste sono diverse a seconda dell'operazione API, della Regione AWS e di altri fattori, come il tipo di chiave KMS. Quando superi una quota di richieste API, AWS KMS limita la richiesta.

Tutte le quote di richieste AWS KMS sono regolabili, ad eccezione delle quote di richiesta per l'archivio delle chiavi AWS CloudHSM. Per richiedere un aumento delle quote, consultare Richiesta di aumento delle quote nella Guida dell'utente di Service Quotas. Per richiedere una riduzione della quota, per modificare una quota non elencata in Service Quotas o per modificare una quota in una Regione AWS in cui le Service Quotas per AWS KMS non sono disponibili, visita il Centro AWS Support e crea un caso.

Se stai superando la quota di richieste per l'GenerateDataKeyoperazione, prendi in considerazione l'utilizzo della funzionalità di memorizzazione nella cache delle chiavi dati di. AWS Encryption SDK Il riutilizzo delle chiavi dei dati potrebbe ridurre la frequenza delle richieste a AWS KMS.

Oltre alle quote di richieste, AWS KMS utilizza le quote di risorse per garantire la capacità a tutti gli utenti. Per informazioni dettagliate, vedi Quote delle risorse.

Per visualizzare le tendenze nei tassi di richiesta, utilizzare la Console Service Quotas. Puoi anche creare un CloudWatch allarme Amazon che ti avvisi quando la frequenza delle richieste raggiunge una determinata percentuale del valore di quota. Per i dettagli, consulta Gestisci le tariffe di richiesta AWS KMS API utilizzando Service Quotas e Amazon CloudWatch nel blog sulla AWSsicurezza.

Argomenti

- Quote di richieste per ogni operazione API AWS KMS
- Applicazione delle quote di richieste
- Quote condivise per le operazioni di crittografia
- Richieste API eseguite per tuo conto

- Richieste tra account
- Quote di richiesta per l'archivio delle chiavi personalizzate

Quote di richieste per ogni operazione API AWS KMS

Questa tabella elenca il codice delle quote Service Quotas e il valore predefinito per ogni quota di richiesta AWS KMS. Tutte le quote di richieste AWS KMS sono regolabili, ad eccezione delle quote di richiesta per l'archivio delle chiavi AWS CloudHSM.

> **Note**
>
> Potrebbe essere necessario scorrere orizzontalmente o verticalmente per visualizzare tutti i dati di questa tabella.

Nome quota	Valore predefinito (richieste al secondo)

`Cryptographic operations (symmetric) request rate`
 	
Si applica a:
 	
• `Decrypt`
• `Encrypt`
• `GenerateDataKey`
• `GenerateDataKeyWithoutPlaintext`
• `GenerateMac`
• `GenerateRandom`
• `ReEncrypt`
• `VerifyMac`
	Queste quote condivise variano a seconda della Regione AWS e del tipo di chiave KMS utilizzata nella richiesta. Ogni quota è calcolata separatamente.
	
	• 5.500 (condiviso)
	• 10.000 (condiviso) nelle regioni seguenti:
	  • Stati Uniti orientali (Ohio), us-east-2
	  • Asia Pacifico (Singapore), ap-southeast-1
	  • Asia Pacifico (Sydney), ap-southeast-2
	  • Asia Pacifico (Tokyo), ap-northeast-1
	  • Europa (Francoforte), eu-central-1
	  • Europa (Londra), eu-west-2
	• 50.000 (condiviso) nelle Regioni seguenti:
	  • Stati Uniti orientali (Virginia settentrionale), us-east-1
	  • Stati Uniti occidentali (Oregon), us-west-2

Nome quota	Valore predefinito (richieste al secondo)
	• Europa (Irlanda), eu-west-1
`Cryptographic operations (RSA) request rate` Si applica a: • `Decrypt` • `Encrypt` • `ReEncrypt` • `Sign` • `Verify`	500 (condiviso) per chiavi KMS RSA
`Cryptographic operations (ECC) request rate` Si applica a: • `Sign` • `Verify`	300 (condiviso) per chiavi KMS basate su curva ellittica (ECC)
`Cryptographic operations (SM) request rate` Si applica a: • `Decrypt` • `Encrypt` • `ReEncrypt` • `Sign` • `Verify`	300 (condivisa) per chiavi KMS SM2 (solo regioni della Cina)

Nome quota	Valore predefinito (richieste al secondo)
`Custom key store request quotas` Si applica a: • `Decrypt` • `Encrypt` • `GenerateDataKey` • `GenerateDataKeyWithoutPlaintext` • `GenerateRandom` • `ReEncrypt`	Le quote di richiesta per l'archivio delle chiavi personalizzate vengono calcolate separatamente per ogni archivio delle chiavi personalizzate • 1.800 (condiviso) per ogni archivio delle chiavi AWS CloudHSM • 1.800 (condiviso) per ogni archivio delle chiavi esterne
`CancelKeyDeletion request rate`	5
`ConnectCustomKeyStore request rate`	5
`CreateAlias request rate`	5
`CreateCustomKeyStore request rate`	5
`CreateGrant request rate`	50
`CreateKey request rate`	5
`DeleteAlias request rate`	15
`DeleteCustomKeyStore request rate`	5
`DeleteImportedKeyMaterial request rate`	5
`DescribeCustomKeyStores request rate`	5
`DescribeKey request rate`	2000

Nome quota	Valore predefinito (richieste al secondo)
`DisableKey request rate`	5
`DisableKeyRotation request rate`	5
`DisconnectCustomKeyStore request rate`	5
`EnableKey request rate`	5
`EnableKeyRotation request rate`	15
`GenerateDataKeyPair (ECC_NIST_P256) request rate` Si applica a: • `GenerateDataKeyPair` • `GenerateDataKeyPairWithoutPlaintext`	100
`GenerateDataKeyPair (ECC_NIST_P384) request rate` Si applica a: • `GenerateDataKeyPair` • `GenerateDataKeyPairWithoutPlaintext`	100
`GenerateDataKeyPair (ECC_NIST_P521) request rate` Si applica a: • `GenerateDataKeyPair` • `GenerateDataKeyPairWithoutPlaintext`	100

Nome quota	Valore predefinito (richieste al secondo)
`GenerateDataKeyPair (ECC_SECG_P256K1) request rate` Si applica a: • `GenerateDataKeyPair` • `GenerateDataKeyPairWithoutPlaintext`	100
`GenerateDataKeyPair (RSA_2048) request rate` Si applica a: • `GenerateDataKeyPair` • `GenerateDataKeyPairWithoutPlaintext`	1
`GenerateDataKeyPair (RSA_3072) request rate` Si applica a: • `GenerateDataKeyPair` • `GenerateDataKeyPairWithoutPlaintext`	0,5 (1 in ogni intervallo di 2 secondi)
`GenerateDataKeyPair (RSA_4096) request rate` Si applica a: • `GenerateDataKeyPair` • `GenerateDataKeyPairWithoutPlaintext`	0,1 (1 in ogni intervallo di 10 secondi)

Nome quota	Valore predefinito (richieste al secondo)
`GenerateDataKeyPair (SM2 – China Regions only) request rate` Si applica a: • `GenerateDataKeyPair` • `GenerateDataKeyPairWithoutPlaintext`	25
`GetKeyPolicy request rate`	1000
`GetKeyRotationStatus request rate`	1000
`GetParametersForImport request rate`	0,25 (1 in ogni intervallo di 4 secondi)
`GetPublicKey request rate`	2000
`ImportKeyMaterial request rate`	5
`ListAliases request rate`	500
`ListGrants request rate`	100
`ListKeyPolicies request rate`	100
`ListKeys request rate`	500
`ListResourceTags request rate`	2000
`ListRetirableGrants request rate`	100
`PutKeyPolicy request rate`	15

Nome quota	Valore predefinito (richieste al secondo)
`ReplicateKey request rate` Un'operazione `ReplicateKey` conta come una richiesta `ReplicateKey` nella Regione della chiave primaria e due richieste `CreateKey` nella Regione della replica. Una delle richieste `CreateKey` serve per rilevare potenziali problemi prima di creare la chiave.	5
`RetireGrant request rate`	30
`RevokeGrant request rate`	30
`ScheduleKeyDeletion request rate`	15
`TagResource request rate`	10
`UntagResource request rate`	5
`UpdateAlias request rate`	5
`UpdateCustomKeyStore request rate`	5
`UpdateKeyDescription request rate`	5
`UpdatePrimaryRegion request rate` Un'operazione `UpdatePrimaryRegion` conta come due richieste `UpdatePrimaryRegion`; una richiesta in ciascuna delle due Regioni interessate.	5

Applicazione delle quote di richieste

Durante la revisione delle quote di richieste, tieni presente le seguenti informazioni.

- Le quote di richiesta si applicano a entrambe le chiavi gestite dal cliente e le Chiavi gestite da AWS. L'utilizzo delle Chiavi di proprietà di AWS non viene considerato ai fini delle quote di richieste per il tuo Account AWS, anche quando vengono utilizzate per proteggere le risorse dell'account.
- Le quote di richieste si applicano alle richieste inviate agli endpoint FIPS e agli endpoint non FIPS. Per un elenco degli endpoint del servizio AWS KMS, consulta Endpoint e quote AWS Key Management Service nella Riferimenti generali di AWS.
- Il throttling si basa su tutte le richieste per chiavi KMS di tutti i tipi della Regione. Il totale include le richieste di tutte le entità principali nell'Account AWS, incluse le richieste provenienti dai servizi AWS effettuate per tuo conto.
- Ogni quota di richieste è calcolata in modo indipendente. Ad esempio, le richieste per l'CreateKeyoperazione non hanno alcun effetto sulla quota di richiesta per l'CreateAliasoperazione. Se alle richieste `CreateAlias` è applicato il throttling, è comunque possibile completare le richieste `CreateKey`.
- Sebbene le operazioni di crittografia condividano una quota, la quota condivisa viene calcolata indipendentemente dalle quote per altre operazioni. Ad esempio, le chiamate alle operazioni Encrypt e Decrypt condividono una quota di richieste, ma tale quota è indipendente dalla quota per le operazioni di gestione, ad esempio. EnableKey Ad esempio, nella Regione Europa (Londra) è possibile eseguire 10.000 operazioni di crittografia su chiavi KMS simmetriche + 5 operazioni `EnableKey` al secondo senza che venga applicato alcuna limitazione.

Quote condivise per le operazioni di crittografia

Le operazioni di crittografia di AWS KMS condividono quote di richieste. Puoi richiedere qualsiasi combinazione di operazioni di crittografia supportate dalla chiave KMS per fare in modo che il numero totale di operazioni di crittografia non superi la quota di richieste per quel tipo di chiave KMS. Le eccezioni sono GenerateDataKeyPaire GenerateDataKeyPairWithoutPlaintext, che condividono una quota separata.

Le quote per i diversi tipi di chiavi KMS vengono calcolate in modo indipendente. Ogni quota si applica a tutte le richieste per queste operazioni nell'Account AWS e nella Regione con il tipo di chiave specificato in ogni intervallo di un secondo.

- Il tasso di richieste di operazioni di crittografia (simmetriche) è la quota di richiesta condivisa per le operazioni di crittografia che utilizzano le chiavi KMS simmetriche in un account e in una Regione. Questa quota si applica alle operazioni crittografiche con chiavi crittografiche simmetrica e chiavi HMAC, anch'esse simmetriche.

Ad esempio, potresti utilizzare le chiavi KMS simmetriche in una Regione AWS con una quota condivisa di 10.000 richieste al secondo. Quando si effettuano 7.000 GenerateDataKeyrichieste al secondo e 2.000 richieste di decriptazione al secondo, AWS KMS non limita le richieste. Se invece si effettuano 9.500 richieste `GenerateDataKey` e 1.000 richieste Encrypt al secondo, AWS KMS applica il throttling alle richieste perché queste superano la quota condivisa.

Le operazioni di crittografia sulle chiavi KMS di crittografia simmetrica in un archivio di chiavi personalizzate contano sia per la frequenza di richiesta (simmetrica) di operazioni crittografiche per l'account sia per la quota di richiesta dell'archivio di chiavi personalizzate per l'archivio di chiavi personalizzate.

- Il tasso di richieste di operazioni di crittografia (RSA) è la quota di richieste condivisa per le operazioni di crittografia che utilizzano le chiavi KMS RSA asimmetriche.

  Ad esempio, con una quota di richieste per 500 operazioni al secondo, è possibile effettuare 200 richieste di crittografia e 100 richieste di decrittografia con le chiavi KMS RSA in grado di crittografare e decrittografare, più 50 richieste di firma e 150 di verifica con le chiavi KMS RSA che possono firmare e verificare.
- Il tasso di richieste di operazioni di crittografia (ECC) è la quota di richieste condivisa per le operazioni di crittografia che utilizzano le chiavi KMS asimmetriche basate su curva ellittica (ECC).

  Ad esempio, con una quota di richiesta per 300 operazioni al secondo, puoi effettuare 100 richieste Sign e 200 richieste Verify con le chiavi KMS RSA che possono firmare e verificare.
- Il tasso di richieste di operazioni di crittografia (SM - solo regioni della Cina) è la quota di richieste condivisa per le operazioni di crittografia che utilizzano le chiavi KMS SM asimmetriche.

  Ad esempio, con una quota di richieste per 300 operazioni al secondo, è possibile effettuare 100 richieste di Encrypt (crittografia) e 100 richieste di Decrypt (decrittografia) con le chiavi KMS SM2 in grado di crittografare e decrittografare, più 50 richieste di Sign (firma) e 50 di Verify (verifica) con le chiavi KMS SM2 che possono firmare e verificare.
- La quota di richiesta per l'archivio delle chiavi personalizzate è la quota di richiesta condivisa per le operazioni di crittografia sulle chiavi KMS in un archivio delle chiavi personalizzate. Questa quota viene calcolata separatamente per ogni archivio delle chiavi personalizzate.

  Le operazioni di crittografia sulle chiavi KMS di crittografia simmetrica in un archivio di chiavi personalizzate contano sia per la frequenza di richiesta (simmetrica) di operazioni crittografiche per l'account sia per la quota di richiesta dell'archivio di chiavi personalizzate per l'archivio di chiavi personalizzate.

Anche le quote per i diversi tipi di chiave sono calcolate in modo indipendente. Ad esempio, nella regione Asia Pacifico (Singapore), se utilizzi chiavi KMS simmetriche e asimmetriche, puoi effettuare fino a 10.000 chiamate al secondo con le chiavi KMS simmetriche (incluse le chiavi HMAC), più fino a 500 chiamate aggiuntive al secondo con le chiavi KMS asimmetriche RSA, più fino a 300 richieste aggiuntive al secondo con le chiavi KMS basate su ECC.

Richieste API eseguite per tuo conto

È possibile effettuare richieste API direttamente oppure utilizzando un servizio AWS integrato che effettua richieste API a AWS KMS a tuo nome. La quota si applica a entrambi i tipi di richieste.

Ad esempio, è possibile archiviare i dati in Amazon S3 utilizzando la crittografia lato server con una chiave KMS (SSE-KMS). Ogni volta che carichi o scarichi un oggetto S3 codificato con SSE-KMS, Amazon S3 invia una richiesta `GenerateDataKey` (per l'upload) o una richiesta `Decrypt` (per il download) a AWS KMS a tuo nome. Queste richieste vengono calcolate ai fini della quota, pertanto AWS KMS applica una limitazione alle richieste se superi il totale complessivo di 5.500 (oppure 10.000 o 50.000, a seconda della Regione AWS) caricamenti o download al secondo di oggetti S3 crittografati con SSE-KMS.

Richieste tra account

Quando un'applicazione in un Account AWS utilizza una chiave KMS di proprietà di un altro account, si parla di richiesta tra account. Per le richieste tra account, AWS KMS limita l'account che effettua le richieste, non l'account proprietario della chiave KMS. Ad esempio, se un'applicazione nell'account A utilizza una chiave KMS nell'account B, l'uso della chiave KMS viene applicato solo alle quote dell'account A.

Quote di richiesta per l'archivio delle chiavi personalizzate

AWS KMS mantiene le quote di richiesta per le operazioni di crittografia sulle chiavi KMS in un archivio delle chiavi personalizzate. Tali quote di richiesta vengono calcolate separatamente per ogni archivio delle chiavi personalizzate.

Quote di richiesta per l'archivio delle chiavi personalizzate	Valore predefinito (richieste al secondo) per ogni archivio delle chiavi personalizzate	Regolabile
Quota di richiesta per l'archivio delle chiavi AWS CloudHSM	1800	No

Quote di richiesta per l'archivio delle chiavi personalizzate	Valore predefinito (richieste al secondo) per ogni archivio delle chiavi personalizzate	Regolabile
Quota di richiesta per l'archivio delle chiavi esterne	1800	Sì

> **Note**
>
> Le quote di richiesta per l'archivio delle chiavi personalizzate di AWS KMS non vengono visualizzate nella console Service Quotas. Non puoi visualizzare o gestire tali quote utilizzando le operazioni API Service Quotas. Per richiedere una modifica delle quote di richiesta per l'archivio delle chiavi esterne, visita il Centro AWS Support e crea un caso.
> Se il AWS CloudHSM cluster associato a un AWS CloudHSM key store sta elaborando numerosi comandi, inclusi quelli non correlati all'archivio chiavi personalizzato, potresti riceverne uno a pagamento. AWS KMS `ThrottlingException` lower-than-expected In questo caso, riduci la frequenza di richieste ad AWS KMS, riduci il carico non correlato oppure utilizza un cluster AWS CloudHSM dedicato per l'archivio delle chiavi di AWS CloudHSM.
> AWS KMSsegnala la limitazione delle richieste di archiviazione di chiavi esterne nella metrica. `ExternalKeyStoreThrottle` CloudWatch Puoi utilizzare questo parametro per visualizzare gli schemi di limitazione, creare allarmi e modificare la quota di richiesta dell'archivio delle chiavi esterne.

Una richiesta di un'operazione di crittografia su una chiave KMS in un archivio delle chiavi personalizzate viene conteggiata ai fini di due quote:

- Quota di frequenza della richiesta (per account) di operazioni di crittografia (simmetriche)

  Le richieste di operazioni di crittografia sulle chiavi KMS in un archivio delle chiavi personalizzate vengono conteggiate ai fini della quota `Cryptographic operations (symmetric) request rate` per ciascuna regione e Account AWS. Ad esempio, negli Stati Uniti orientali (Virginia settentrionale) (us-east-1), ciascun Account AWS può avere fino a 50.000 richieste al secondo sulle chiavi KMS di crittografia simmetrica, incluse le richieste che utilizzano una chiave KMS in un archivio delle chiavi personalizzate.

- Quota di richiesta dell'archivio di chiavi personalizzate (per archivio delle chiavi personalizzate)

  Le richieste di operazioni di crittografia sulle chiavi KMS in un archivio delle chiavi personalizzate contano anche per una `Custom key store request quota` di 1.800 operazioni al secondo. Tali quote vengono calcolate separatamente per ogni archivio delle chiavi personalizzate. Possono includere le richieste da più Account AWS che utilizzano chiavi KMS nell'archivio delle chiavi personalizzate.

Ad esempio, un'operazione Encrypt (Crittografa) su una chiave KMS in un archivio delle chiavi personalizzate (entrambi i tipi) nella regione Stati Uniti orientali (Virginia settentrionale) (us-east-1) viene conteggiata per la quota a livello di account `Cryptographic operations (symmetric) request rate` (50.000 richieste al secondo) per il rispettivo account e regione e per una `Custom key store request quota` (1.800 richieste al secondo) per il rispettivo archivio delle chiavi personalizzato. Tuttavia, una richiesta per un'operazione di gestione, ad esempio su una chiave KMS in un archivio di chiavi personalizzato PutKeyPolicy, si applica solo alla quota a livello di account (15 richieste al secondo).

Limitazione delle richieste AWS KMS

Affinché AWS KMS possa fornire risposte rapide e affidabili alle richieste API da tutti i clienti, limita le richieste API che superano determinati limiti.

La limitazione si verifica quando AWS KMS rifiuta una richiesta altrimenti valida e restituisce un errore `ThrottlingException` come il seguente.

```
You have exceeded the rate at which you may call KMS. Reduce the frequency of your
 calls.
(Service: AWSKMS; Status Code: 400; Error Code: ThrottlingException; Request ID: <ID>
```

AWS KMS limita le richieste per le seguenti condizioni.

- Il tasso di richieste al secondo supera la quota di richiesta AWS KMS per un account e una Regione.

  Ad esempio, se gli utenti del tuo account inviano 1000 richieste `DescribeKey` in un secondo, AWS KMS limita tutte le successive richieste `DescribeKey` in quel secondo.

  Per rispondere alla limitazione, utilizza una strategia di backoff e riprova. Questa strategia viene implementata automaticamente per gli errori HTTP 400 in alcuni SDK AWS.

- Una frammentazione o una frequenza elevata sostenuta di richieste per modificare lo stato della stessa chiave KMS. Questa condizione è spesso nota come "tasto di scelta rapida".

  Ad esempio, se un'applicazione nel tuo account invia una raffica persistente di richieste `EnableKey` e `DisableKey` per la stessa chiave KMS, AWS KMS limita le richieste. Questa limitazione si verifica anche se le richieste non superano il limite di request-per-second richieste per le operazioni `EnableKey` and`DisableKey`.

  Per rispondere alla limitazione, modifica la logica dell'applicazione in modo che faccia solo richieste richieste richieste o consolidi le richieste di più funzioni.

- Le richieste di operazioni sulle chiavi KMS in un AWS CloudHSMkey store potrebbero essere limitate a una certa lower-than-expected velocità quando il AWS CloudHSM cluster associato all'archivio AWS CloudHSM chiavi elabora numerosi comandi, inclusi quelli non correlati all'archivio chiavi. AWS CloudHSM

  (AWS KMS non limita la larghezza di banda della rete delle richieste di operazioni su chiavi KMS in un archivio di chiavi AWS CloudHSM quando non sono disponibili sessioni PKCS #11 per il cluster AWS CloudHSM, ma genera un'eccezione `KMSInternalException` e consiglia di ritentare la richiesta.)

Per visualizzare le tendenze nei tassi di richiesta, utilizzare la Console Service Quotas. Puoi anche creare un CloudWatch allarme Amazon che ti avvisi quando la frequenza delle richieste raggiunge una determinata percentuale del valore di quota. Per i dettagli, consulta Gestisci le tariffe di richiesta AWS KMS API utilizzando Service Quotas e Amazon CloudWatch nel blog sulla AWSsicurezza.

Tutte le quote AWS KMS sono modificabili, ad eccezione della quota delle risorse delle dimensioni del documento della policy della chiave e della quota delle risorse per archivi di chiavi AWS CloudHSM. Per richiedere un aumento delle quote, consultare Richiesta di aumento delle quote nella Guida dell'utente di Service Quotas. Per richiedere una riduzione della quota, per modificare una quota non elencata in Service Quotas o per modificare una quota in una Regione AWS in cui le Service Quotas per AWS KMS non sono disponibili, visita il Centro AWS Support e crea un caso.

> **Note**
>
> Le quote di richiesta per l'archivio delle chiavi personalizzate di AWS KMS non vengono visualizzate nella console Service Quotas. Non puoi visualizzare o gestire tali quote

utilizzando le operazioni API Service Quotas. Per richiedere una modifica delle quote di richiesta per l'archivio delle chiavi esterne, visita il Centro AWS Support e crea un caso.

In che modo i servizi AWS utilizzano AWS KMS

Molti servizi AWS utilizzano AWS KMS per supportare la crittografia dei dati. Quando un servizio AWS è integrato con AWS KMS, puoi utilizzare la AWS KMS keys nel tuo account per proteggere i dati che il servizio riceve, archivia o gestisce per te. Per un elenco completo dei servizi AWS integrati con AWS KMS, consulta Integrazione dei servizi AWS.

I seguenti argomenti illustrano nel dettaglio in che modo servizi particolari utilizzano AWS KMS, tra cui le chiavi KMS supportate, come gestiscono le chiavi dei dati e le autorizzazioni necessarie e come monitorano l'utilizzo di ciascun servizio delle chiavi KMS nell'account.

> **Important**
>
> I servizi AWS integrati con AWS KMS usano soltanto chiavi KMS di crittografia simmetrica per crittografare i dati. Questi servizi non supportano la crittografia con chiavi KMS asimmetriche. Per informazioni su come determinare se una è simmetrica o asimmetrica, consulta Individuazione di chiavi KMS asimmetriche.

Argomenti

- Come si WorkSpaces usa AWS KMS

Come AWS CloudTrail utilizza AWS KMS

È possibile utilizzare AWS CloudTrail per registrare le chiamate API AWS e altre attività per il tuo Account AWS e per salvare le informazioni registrate nei file di log in un bucket Amazon Simple Storage Service (Amazon S3) da te scelto. Per impostazione predefinita, i file di log CloudTrail inseriti nel bucket S3 sono crittografati utilizzando la crittografia lato server con chiavi di crittografia gestite da Amazon S3 (SSE-S3). Ma è possibile invece decidere di utilizzare la crittografia lato server con una chiave KMS (SSE-KMS). Per informazioni su come crittografare i file di registro con, consulta Encrypting CloudTrail Log Files with AWS KMS (SSE-KMS) nella Guida per l'utente. CloudTrail AWS KMS keys AWS CloudTrail

> **Important**
>
> AWS CloudTrail e Amazon S3 supportano solo AWS KMS keys simmetriche. Non è possibile utilizzare una chiave KMS asimmetrica per crittografare i log. CloudTrail Per informazioni su come determinare se una è simmetrica o asimmetrica, consulta Individuazione di chiavi KMS asimmetriche.

Non si paga alcun costo per l'utilizzo delle chiavi quando si CloudTrail leggono o scrivono file di registro crittografati con una chiave SSE-KMS. Tuttavia, si paga un costo per l'utilizzo delle chiavi quando si accede ai file di CloudTrail registro crittografati con una chiave SSE-KMS. Per informazioni sui prezzi di AWS KMS, consulta la pagina dei prezzi di AWS Key Management Service. Per informazioni sui CloudTrail prezzi, consulta la sezione AWS CloudTrailPrezzi e Gestione dei costi nella Guida per l'AWS CloudTrailutente.

Argomenti

- Capire quando viene utilizzata la chiave KMS

Capire quando viene utilizzata la chiave KMS

La crittografia dei file di CloudTrail registro AWS KMS si basa sulla funzionalità di Amazon S3 denominata crittografia lato server con un (SSE-KMS). AWS KMS key Per maggiori informazioni su SSE-KMS, consultare Come Amazon Simple Storage Service (Amazon S3) usa AWS KMS in

questa guida o Protezione dei dati mediante la crittografia lato server con chiavi KMS (SSE-KMS) nella Guida per l'utente di Amazon Simple Storage Service.

Quando configuri l'uso AWS CloudTrail di SSE-KMS per crittografare i tuoi file di registro e Amazon CloudTrail S3 utilizza il tuo AWS KMS keys quando esegui determinate azioni con tali servizi. Le seguenti sezioni spiegano quando e come tali servizi possono utilizzare la tua chiave KMS e forniscono informazioni aggiuntive da utilizzare per convalidare questa spiegazione.

Azioni che causano CloudTrail l'utilizzo della chiave KMS da parte di Amazon S3

- Ti configuri CloudTrail per crittografare i file di registro con AWS KMS key
- CloudTrail inserisce un file di registro nel tuo bucket S3
- Hai a disposizione un file di log crittografato dal tuo bucket S3

Ti configuri CloudTrail per crittografare i file di registro con AWS KMS key

Quando aggiorni la CloudTrail configurazione per utilizzare la chiave KMS, CloudTrail invia una `GenerateDataKey`richiesta AWS KMS per verificare che la chiave KMS esista e che CloudTrail sia autorizzato a utilizzarla per la crittografia. CloudTrail non utilizza la chiave dati risultante.

La richiesta `GenerateDataKey` include le seguenti informazioni per il contesto di crittografia:

- L'Amazon Resource Name (ARN) del percorso CloudTrail
- L'ARN del bucket S3 e il percorso in cui vengono consegnati i CloudTrail file di registro

La `GenerateDataKey` richiesta genera una voce nei CloudTrail log simile all'esempio seguente. Quando vedete una voce di registro come questa, potete determinare che CloudTrail (1) ha chiamato AWS KMS (2) `GenerateDataKey` operation (3) per uno specifico trail (4). AWS KMSha creato la chiave dati con una chiave KMS specifica (5).

> **Note**
>
> Potrebbe essere necessario scorrere verso destra per visualizzare alcune delle didascalie nella seguente voce di log di esempio.

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::086441151436:user/
AWSCloudTrail",(1)
    "accountId": "086441151436",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "userName": "AWSCloudTrail",
    "sessionContext": {"attributes": {
      "mfaAuthenticated": "false",
      "creationDate": "2015-11-11T21:15:33Z"
    }},
    "invokedBy": "internal.amazonaws.com"
  },
  "eventTime": "2015-11-11T21:15:33Z",
  "eventSource":
 "kms.amazonaws.com",(2)
  "eventName":
 "GenerateDataKey",(3)
  "awsRegion": "us-west-2",
  "sourceIPAddress": "internal.amazonaws.com",
  "userAgent": "internal.amazonaws.com",
  "requestParameters": {
    "keyId": "arn:aws:kms:us-west-2:111122223333:alias/ExampleAliasForCloudTrailKMS
 key",
    "encryptionContext": {
      "aws:cloudtrail:arn": "arn:aws:cloudtrail:us-west-2:111122223333:trail/
Default",(4)
      "aws:s3:arn": "arn:aws:s3:::example-bucket-for-CT-logs/AWSLogs/111122223333/"
    },
    "keySpec": "AES_256"
  },
  "responseElements": null,
```

```
  "requestID": "581f1f11-88b9-11e5-9c9c-595a1fb59ac0",
  "eventID": "3cdb2457-c035-4890-93b6-181832b9e766",
  "readOnly": true,
  "resources": [{
    "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",5
    "accountId": "111122223333"
  }],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333"
}
```

CloudTrail inserisce un file di registro nel tuo bucket S3

Ogni volta che CloudTrail inserisce un file di registro nel tuo bucket S3, Amazon S3 invia `GenerateDataKey`una richiesta AWS KMS a per conto di. CloudTrail In risposta a questa richiesta, AWS KMS genera una chiave di dati univoca e quindi invia ad Amazon S3 due copie della chiave di dati, una in testo in chiaro e una crittografata con la chiave KMS specificata. Amazon S3 utilizza la chiave dati in chiaro per crittografare il file di CloudTrail registro e quindi rimuove la chiave dati in testo semplice dalla memoria il prima possibile dopo l'uso. Amazon S3 archivia la chiave dati crittografata come metadati con il file di registro crittografato CloudTrail .

La richiesta `GenerateDataKey` include le seguenti informazioni per il contesto di crittografia:

- L'Amazon Resource Name (ARN) del percorso CloudTrail
- L'ARN dell'oggetto S3 (il CloudTrail file di registro)

Ogni `GenerateDataKey` richiesta genera una voce nei CloudTrail log simile all'esempio seguente. Quando viene visualizzata una voce di registro come questa, è possibile determinare che CloudTrail
(1)
ha chiamato l'`GenerateDataKey`operazione AWS KMS
(2) 3
per uno specifico trail
(4)
per proteggere un file di registro specifico
(5).
AWS KMSha creato la chiave dati nella chiave KMS specificata

(6),
mostrata due volte nella stessa voce di registro.

> **Note**
>
> Potrebbe essere necessario scorrere verso destra per visualizzare alcune delle didascalie nella seguente voce di log di esempio.

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROACKCEVSQ6C2EXAMPLE:i-34755b85",
    "arn": "arn:aws:sts::086441151436:assumed-role/AWSCloudTrail/
i-34755b85",1
    "accountId": "086441151436",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2015-11-11T20:45:25Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::086441151436:role/AWSCloudTrail",
        "accountId": "086441151436",
        "userName": "AWSCloudTrail"
      }
    },
    "invokedBy": "internal.amazonaws.com"
  },
  "eventTime": "2015-11-11T21:15:58Z",
  "eventSource":
 "kms.amazonaws.com",2
  "eventName":
 "GenerateDataKey",3
  "awsRegion": "us-west-2",
  "sourceIPAddress": "internal.amazonaws.com",
  "userAgent": "internal.amazonaws.com",
```

```
  "requestParameters": {
    "encryptionContext": {
      "aws:cloudtrail:arn": "arn:aws:cloudtrail:us-west-2:111122223333:trail/
Default",4
      "aws:s3:arn": "arn:aws:s3:::example-bucket-for-CT-logs/
AWSLogs/111122223333/CloudTrail/us-west-2/2015/11/11/111122223333_CloudTrail_us-
west-2_20151111T2115Z_7JREEBimdK8d2nC9.json.gz"5
    },
    "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",6
    "keySpec": "AES_256"
  },
  "responseElements": null,
  "requestID": "66f3f74a-88b9-11e5-b7fb-63d925c72ffe",
  "eventID": "7738554f-92ab-4e27-83e3-03354b1aa898",
  "readOnly": true,
  "resources": [{
    "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",6
    "accountId": "111122223333"
  }],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333"
}
```

Hai a disposizione un file di log crittografato dal tuo bucket S3

Ogni volta che ricevi un file di CloudTrail registro crittografato dal tuo bucket S3, Amazon S3 invia `Decrypt`una richiesta AWS KMS a tuo nome per decrittografare la chiave dati crittografata del file di registro. In risposta a questa richiesta, AWS KMS usa la chiave KMS per decrittare la chiave di dati e quindi invia la chiave di dati in testo non crittografato ad Amazon S3. Amazon S3 utilizza la chiave dati in chiaro per decrittografare il file di CloudTrail registro e quindi rimuove la chiave dati in testo semplice dalla memoria il prima possibile dopo l'uso.

La richiesta `Decrypt` include le seguenti informazioni per il contesto di crittografia:

- L'Amazon Resource Name (ARN) del percorso CloudTrail
- L'ARN dell'oggetto S3 (il CloudTrail file di registro)

Ogni `Decrypt` richiesta genera una voce nei CloudTrail log simile all'esempio seguente. Quando visualizzi una voce di log come questa, puoi stabilire che un utente nel tuo Account AWS (1) ha chiamato l'operazione AWS KMS (2) `Decrypt` (3) per un determinato percorso (4) e un file di log specifico (5). AWS KMS ha decrittato la chiave di dati con la chiave KMS specificata (6).

> **Note**
>
> Potrebbe essere necessario scorrere verso destra per visualizzare alcune delle didascalie nella seguente voce di log di esempio.

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::111122223333:role/cloudtrail-
admin",(1)
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "cloudtrail-admin",
    "sessionContext": {"attributes": {
      "mfaAuthenticated": "false",
      "creationDate": "2015-11-11T20:48:04Z"
    }},
    "invokedBy": "signin.amazonaws.com"
  },
  "eventTime": "2015-11-11T21:20:52Z",
```

```
  "eventSource":
 "kms.amazonaws.com",(2)
  "eventName":
 "Decrypt",(3)
  "awsRegion": "us-west-2",
  "sourceIPAddress": "internal.amazonaws.com",
  "userAgent": "internal.amazonaws.com",
  "requestParameters": {
    "encryptionContext": {
      "aws:cloudtrail:arn": "arn:aws:cloudtrail:us-west-2:111122223333:trail/
Default",(4)
      "aws:s3:arn": "arn:aws:s3:::example-bucket-for-CT-logs/
AWSLogs/111122223333/CloudTrail/us-west-2/2015/11/11/111122223333_CloudTrail_us-
west-2_20151111T2115Z_7JREEBimdK8d2nC9.json.gz"(5)
    }
  },
  "responseElements": null,
  "requestID": "16a0590a-88ba-11e5-b406-436f15c3ac01",
  "eventID": "9525bee7-5145-42b0-bed5-ab7196a16daa",
  "readOnly": true,
  "resources": [{
    "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",(6)
    "accountId": "111122223333"
  }],
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}
```

Come Amazon DynamoDB usa AWS KMS

Amazon DynamoDB è un servizio di database NoSQL completamente gestito e scalabile. DynamoDB si integra con AWS Key Management Service (AWS KMS) per supportare la funzione di crittografia lato server Crittografia dei dati inattivi.

Con la crittografia dei dati inattivi, DynamoDB crittografa in modo trasparente tutti i dati dei clienti in una tabella DynamoDB, tra cui la propria chiave primaria e gli indici secondari locali e globali, ogni volta che la tabella viene salvata in modo permanente su disco. Se la tabella dispone di una chiave di ordinamento, alcune di queste chiavi che contrassegnano i limiti dell'intervallo sono archiviate come testo normale nei metadati della tabella. Quando si accede a una tabella, DynamoDB decrittografa

i dati della tabella in modo trasparente. Non è necessario modificare le applicazioni per utilizzare o gestire le tabelle crittografate.

La crittografia dei dati inattivi inoltre protegge i flussi DynamoDB, le tabelle globali e i backup ogni volta che questi oggetti vengono salvati su supporti durevoli. Le istruzioni sulle tabelle contenute in questo argomento si applicano anche a questi oggetti.

Tutte le tabelle DynamoDB sono crittografate. Non è possibile attivare o disattivare la crittografia per tabelle nuove o esistenti. Per impostazione predefinita tutte le tabelle vengono crittografate con una Chiave di proprietà di AWS nell'account del servizio DynamoDB. Tuttavia puoi selezionare un'opzione per crittografare alcune o tutte le tabelle con una chiave gestita dal cliente o la Chiave gestita da AWS per DynamoDB nel tuo account.

Per informazioni sul supporto di Amazon DynamoDB per le chiavi KMS, consulta la sezione Crittografia a riposo per DynamoDB nella Guida per gli sviluppatori di Amazon DynamoDB.

Come Amazon Elastic Block Store (Amazon EBS) usa AWS KMS

Questo argomento illustra in dettaglio come Amazon Elastic Block Store (Amazon EBS) usa AWS KMS per crittografare i volumi e gli snapshot. Per istruzioni di base su come crittografare i volumi Amazon EBS, consulta Crittografia Amazon EBS.

Argomenti

- Crittografia Amazon EBS
- Utilizzo di chiavi KMS e chiavi dati
- Contesto di crittografia di Amazon EBS
- Rilevamento degli errori Amazon EBS
- Utilizzo di AWS CloudFormation per creare volumi crittografati di Amazon EBS

Crittografia Amazon EBS

Quando colleghi un volume Amazon EBS crittografato a un tipo di istanza Amazon Elastic Compute Cloud (Amazon EC2) supportato, i dati archiviati inattivi nel volume, l'I/O su disco e gli snapshot create dai volumi sono tutti crittografati. La crittografia viene implementata a livello di server che ospitano le istanze Amazon EC2.

Questa caratteristica è supportata su tutti i tipi di volume Amazon EBS. Puoi accedere ai volumi crittografati nello stesso modo in cui si accede ad altri volumi; la crittografia e la decrittografia sono

gestite in modo trasparente e non richiedono ulteriore azione da parte dell'utente, dell'istanza EC2 o dell'applicazione. Gli snapshot di volumi crittografati vengono automaticamente crittografati e i volumi creati da snapshot crittografati vengono anch'essi automaticamente crittografati.

Lo stato di crittografia di un volume EBS viene determinato quando si crea il volume. Non è possibile modificare lo stato di crittografia di un volume esistente. Tuttavia, è possibile eseguire la migrazione dei dati tra i volumi crittografati e non crittografati e applicare un nuovo stato di crittografia durante la copia di uno snapshot.

Amazon EBS supporta la crittografia opzionale per impostazione predefinita. Puoi abilitare automaticamente la crittografia su tutti i nuovi volumi EBS e copie snapshot nel tuo Account AWS e nella Regione. Questa impostazione di configurazione non influisce sui volumi o sugli snapshot esistenti. Per informazioni, consulta Crittografia per impostazione predefinita nella Guida per l'utente di Amazon EC2 per le istanze Linux o Guida per l'utente di Amazon EC2 per le istanze Windows.

Utilizzo di chiavi KMS e chiavi dati

Quando crei un volume Amazon EBS crittografato, specifichi una AWS KMS key. Per impostazione predefinita, Amazon EBS utilizza la Chiave gestita da AWS per Amazon EBS nel tuo account (`aws/ebs`). Tuttavia puoi specificare una chiave gestita dal cliente creata e gestita da te.

Per utilizzare una chiave gestita dal cliente, è necessario concedere ad Amazon EBS l'autorizzazione a utilizzare una chiave KMS per conto dell'utente. Per un elenco delle autorizzazioni richieste, consulta Autorizzazioni per gli utenti IAM nella Guida per l'utente di Amazon EC2 per le istanze Linux o Guida per l'utente di Amazon EC2 per le istanze Windows.

> **Important**
>
> Amazon EBS supporta solo chiavi KMS simmetriche. Non è possibile utilizzare una chiave KMS asimmetrica per crittografare il volume Amazon EBS. Per informazioni su come determinare se una chiave KMS è simmetrica o asimmetrica, consulta Individuazione di chiavi KMS asimmetriche.

Per ogni volume, Amazon EBS chiede AWS KMS per generare una chiave di dati univoca crittografata sotto la chiave KMS specificata. Amazon EBS archivia la chiave di dati crittografata con il volume. Quindi, quando colleghi il volume a un'istanza di Amazon EC2, Amazon EBS chiama AWS KMS per decrittare la chiave di dati. Amazon EBS usa la chiave dei dati sotto forma di testo in chiaro

nella memoria dell'hypervisor per crittografare l'I/O su disco verso il volume EBS. Per informazioni, consulta Come funziona la crittografia EBS nella Guida per l'utente di Amazon EC2 per le istanze Linux o la Guida per l'utente di Amazon EC2 per le istanze Windows.

Contesto di crittografia di Amazon EBS

Nelle sue richieste GenerateDataKeyWithoutPlaintexte Decrypt a, AWS KMS Amazon EBS utilizza un contesto di crittografia con una coppia nome-valore che identifica il volume o lo snapshot nella richiesta. Il nome nel contesto di crittografia non varia.

Un contesto di crittografia è un set di coppie chiave-valore che contiene dati arbitrari non segreti. Quando includi un contesto di crittografia in una richiesta di crittografia dei dati, AWS KMS lega il contesto di crittografia ai dati crittografati, in modo che lo stesso contesto di crittografia sia necessario per decrittografare i dati.

Per tutti i volumi e per gli snapshot crittografati creati con l'CreateSnapshotoperazione Amazon EBS, Amazon EBS utilizza l'ID del volume come valore del contesto di crittografia. Nel campo `requestParameters` di una voce di log di CloudTrail, il contesto di crittografia è simile a quanto segue:

```
"encryptionContext": {
  "aws:ebs:id": "vol-0cfb133e847d28be9"
}
```

Per le istantanee crittografate create con l'operazione Amazon CopySnapshotEC2, Amazon EBS utilizza l'ID snapshot come valore del contesto di crittografia. Nel campo `requestParameters` di una voce di log di CloudTrail, il contesto di crittografia è simile a quanto segue:

```
"encryptionContext": {
  "aws:ebs:id": "snap-069a655b568de654f"
}
```

Rilevamento degli errori Amazon EBS

Per creare un volume EBS crittografato o collegare il volume a un'istanza EC2, Amazon EBS e l'infrastruttura Amazon EC2 devono essere in grado di utilizzare la chiave KMS specificata per la crittografia del volume EBS. Quando la chiave KMS non è utilizzabile, ad esempio quando lo stato della chiave non è `Enabled`, la creazione del volume o l'allegato del volume ha esito negativo.

In questo caso, Amazon EBS invia un evento ad Amazon EventBridge (precedentemente CloudWatch Events) per informarti dell'errore. In EventBridge, puoi stabilire regole che attivano azioni automatiche in risposta a questi eventi. Per ulteriori informazioni, consulta Amazon CloudWatch Events for Amazon EBS nella Guida per l'utente di Amazon EC2 per le istanze Linux, in particolare le seguenti sezioni:

- Chiave di crittografia non valida per il collegamento il ricollegamento del volume
- Chiave di crittografia non valida su Crea volume

Per risolvere questi problemi, assicurati che la chiave KMS specificata per la crittografia del volume EBS sia abilitata. Per eseguire questa operazione, visualizza per prima cosa la chiave KMS per stabilirne lo stato di chiave corrente (colonna Stato nella AWS Management Console). Quindi, consulta le informazioni contenute in uno dei seguenti collegamenti:

- Se lo stato di chiave KMS è disabilitato, abilitalo.
- Se lo stato di chiave KMS è in importazione in sospeso, importa il materiale chiave.
- Se lo stato di chiave KMS è in eliminazione in sospeso, annulla l'eliminazione della chiave.

Utilizzo di AWS CloudFormation per creare volumi crittografati di Amazon EBS

È possibile utilizzare AWS CloudFormation per creare volumi di Amazon EBS crittografati. Per ulteriori informazioni, consulta AWS::EC2::Volume nella Guida per l'utente di AWS CloudFormation.

Come Amazon Elastic Transcoder utilizza AWS KMS

È possibile utilizzare Amazon Elastic Transcoder per la conversione di file multimediali archiviati in un bucket Amazon S3 in formati richiesti dai dispositivi di riproduzione dei consumatori. Entrambi i file di input e output possono essere crittografati e decrittografati. Le seguenti sezioni illustrano il modo in cui AWS KMS viene utilizzato per entrambi i processi.

Argomenti

- Crittografia del file di input
- Decrittografia del file di input
- Crittografia del file di output

- Protezione dei contenuti per il protocollo HLS
- Contesto di crittografia di Elastic Transcoder

Crittografia del file di input

Prima di poter utilizzare Elastic Transcoder, è necessario creare un bucket Amazon S3 e caricarvi il file multimediale. È possibile crittografare il file prima di caricarlo utilizzando la crittografia AES lato client o dopo il caricamento utilizzando la crittografia Amazon S3 lato server.

Se scegli la crittografia lato client utilizzando AES, sei responsabile della crittografia del file prima di caricarlo su Amazon S3 e devi fornire a Elastic Transcoder l'accesso alla chiave di crittografia. A questo scopo, utilizza una AWS KMS key AWS KMS simmetrica per proteggere la chiave di crittografia AES che hai utilizzato per crittografare il file multimediale.

Se scegli la crittografia lato server, permetti ad Amazon S3 di crittografare e decrittare tutti i file per tuo conto. È possibile configurare Amazon S3 per l'utilizzo di uno delle tre diverse chiavi di crittografia per proteggere la chiave di dati univoca che crittografa il tuo file:

- Una chiave Amazon S3, una chiave di crittografia che Amazon S3 possiede e gestisce. Non fa parte del tuo Account AWS.
- La Chiave gestita da AWS per Amazon S3, una chiave KMS che fa parte del tuo account, ma è creata e gestita da AWS
- Qualsiasi chiave gestita dal cliente simmetrica che crei utilizzando AWS KMS

> **Important**
>
> Per la crittografia lato client e lato server, Elastic Transcoder supporta solo le chiavi KMS simmetriche. Non puoi utilizzare una chiave KMS asimmetrica per crittografare i file Elastic Transcoder. Per informazioni su come determinare se una chiave KMS è simmetrica o asimmetrica, consulta Individuazione di chiavi KMS asimmetriche.

Puoi abilitare la crittografia e specificare una chiave utilizzando la console Amazon S3 o le API Amazon S3 appropriate. Per ulteriori informazioni su come Amazon S3 esegue la crittografia, consultare Protezione dei dati mediante la crittografia lato server con chiavi KMS (SSE-KMS) nella Guida per l'utente di Amazon Simple Storage Service.

Quando proteggi i file di input utilizzando la Chiave gestita da AWS per Amazon S3 nel tuo account o una chiave gestita dal cliente, Amazon S3 e AWS KMS interagiscono nel modo seguente:

1. Amazon S3 richiede una chiave di dati in testo in chiaro e una copia della chiave dati crittografata con la chiave KMS specificata.
2. AWS KMS crea una chiave di dati, esegue la crittografia utilizzando la chiave KMS specificata e la chiave di dati in testo normale e la chiave di dati crittografata ad Amazon S3.
3. Amazon S3 usa la chiave di dati di testo normale per crittografare il file multimediale, quindi archivia il file nel bucket Amazon S3 specificato.
4. Amazon S3 archivia la chiave di dati crittografata insieme al file multimediale crittografato.

Decrittografia del file di input

Se scegli la crittografia Amazon S3 lato server per crittografare il file di input, Elastic Transcoder non decrittografa il file. Al contrario, Elastic Transcoder si basa su Amazon S3 per eseguire la decrittografia a seconda delle impostazioni specificate al momento della creazione di un processo e di una pipeline.

Sono disponibili le seguenti combinazioni di impostazioni.

Modalità crittografia	Chiave AWS KMS	Significato
`S3`	Predefinita	Amazon S3 crea e gestisce le chiavi utilizzate per crittografare e decrittografare il file multimediale. Il processo non è visibile all'utente.
`S3-AWS-KMS`	Predefinita	Amazon S3 utilizza una chiave di dati crittografata dalla Chiave gestita da AWS per impostazione predefinita per Amazon S3 nel tuo account per crittografare il file multimediale.

Modalità crittografia	Chiave AWS KMS	Significato
S3-AWS-KMS	Personalizzata (con ARN)	Amazon S3 utilizza una chiave di dati crittografati dalla chiave gestita dal cliente per crittografare il file multimediale.

Quando viene specificato S3-AWS-KMS, Amazon S3 e AWS KMS collaborano nel modo seguente per eseguire la decrittografia.

1. Amazon S3 invia la chiave di dati crittografati a AWS KMS.
2. AWS KMS decritta la chiave di dati utilizzando la chiave KMS appropriata, quindi invia la chiave di dati in testo in chiaro nuovamente ad Amazon S3.
3. Amazon S3 utilizza la chiave di dati in testo normale per decrittare il testo cifrato.

Se scegli la crittografia lato client utilizzando una chiave di crittografia AES, Elastic Transcoder recupera il file crittografato dal bucket Amazon S3 e lo decrittografa. Elastic Transcoder utilizza la chiave di crittografia da te indicata al momento della creazione della pipeline per decrittare la chiave AES, quindi utilizza la chiave AES per decrittare il file multimediale.

Crittografia del file di output

Elastic Transcoder crittografa il file di output in base alla modalità di specificare le impostazioni di crittografia al momento della creazione di un processo e di una pipeline. Sono disponibili le seguenti opzioni.

Modalità crittografia	Chiave AWS KMS	Significato
S3	Predefinita	Amazon S3 crea e gestisce le chiavi utilizzate per crittografare il file di output.
S3-AWS-KMS	Predefinita	Amazon S3 utilizza una chiave dati creata da AWS KMS e crittografata dalla Chiave

Modalità crittografia	Chiave AWS KMS	Significato
		gestita da AWS per Amazon S3 nel tuo account.
S3-AWS-KMS	Personalizzata (con ARN)	Amazon S3 utilizza una chiave di dati crittografati tramite la chiave gestita dal cliente specificata dall'ARN per crittografare il file multimedi ale.
AES-	Predefinita	Elastic Transcoder usa la Chiave gestita da AWS per Amazon S3 nel tuo account per decrittare la chiave AES specificata che fornisci e utilizza tale chiave per crittografare il file di output.
AES-	Personalizzata (con ARN)	Elastic Transcoder usa la chiave gestita dal cliente specificata dall'ARN per decrittare la chiave AES specificata che fornisci e utilizza tale chiave per crittografare il file di output.

Quando specifichi che una Chiave gestita da AWS per Amazon S3 nel tuo account o una chiave gestita dal cliente viene utilizzata per crittografare il file di output, Amazon S3 e AWS KMS interagiscono nel modo seguente:

1. Amazon S3 richiede una chiave di dati in testo in chiaro e una copia della chiave dati crittografata con la chiave KMS specificata.
2. AWS KMS crea una chiave di dati, esegue la crittografia utilizzando la chiave KMS, quindi invia la chiave di dati in testo normale e la chiave di dati crittografata ad Amazon S3.

3. Amazon S3 crittografa i contenuti multimediali utilizzando la chiave di dati e li archivia nel bucket Amazon S3 specificato.
4. Amazon S3 archivia la chiave di dati crittografata insieme al file multimediale crittografato.

Quando specifichi che la chiave AES fornita deve essere utilizzata per crittografare il file di output, la chiave AES deve essere crittografata utilizzando una chiave KMS in AWS KMS. Elastic Transcoder, AWS KMS e tu interagite nel modo seguente:

1. Puoi crittografare la chiave AES chiamando l'operazione Encrypt nell'API AWS KMS. AWS KMS crittografa la chiave utilizzando la chiave KMS specificata. Puoi specificare quale chiave KMS utilizzare quando crei la pipeline.
2. Puoi specificare il file contenente la chiave AES crittografata al momento della creazione del processo Elastic Transcoder.
3. Elastic Transcoder decritta la chiave chiamando l'operazione Decrypt nell'API AWS KMS, passando la chiave crittografata come testo cifrato.
4. Elastic Transcoder utilizza la chiave AES decrittografata per crittografare l'output di file multimediali e quindi elimina la chiave AES decrittata dalla memoria. Solo la copia crittografata originariamente definita nel processo viene salvata su disco.
5. È possibile scaricare il file di output crittografato e decrittografarlo localmente utilizzando la chiave AES originale definita.

> **Important**
>
> AWS non memorizza le chiavi di crittografia private. Pertanto, è importante gestire le proprie chiavi in modo sicuro. Se le chiavi vengono smarrite, non sarà più possibile decrittografare i propri dati.

Protezione dei contenuti per il protocollo HLS

HTTP Live Streaming (HLS) è un protocollo di streaming adattivo. Elastic Transcoder supporta HLS scomponendo il file di input in più file singoli denominati segmenti di file multimediali. Un set di segmenti di file multimediali singoli corrispondenti contengono lo stesso materiale codificato a velocità bit diverse e, di conseguenza, consentono al lettore di selezionare il flusso che si adatta meglio alla

larghezza di banda disponibile. Elastic Transcoder crea inoltre playlist che contengono metadati per i vari segmenti disponibili per lo streaming.

Quando si abilita la protezione dei contenuti HLS, ogni segmento multimediale è crittografato utilizzando una chiave di crittografia AES-128. Quando i contenuti vengono visualizzati, durante il processo di riproduzione il lettore scarica la chiave e decrittografa i segmenti di file multimediali.

Vengono utilizzati due tipi di chiavi: una chiave KMS e una chiave di dati. È necessario creare una chiave di chiavi da utilizzare per crittografare e decrittare la chiave di dati. Elastic Transcoder utilizza la chiave di dati per crittografare e decrittare i segmenti di file multimediali. La chiave di dati deve essere AES-128. Tutte le variazioni e i segmenti dello stesso contenuto sono crittografati utilizzando la stessa chiave di dati. È possibile fornire una chiave di dati o fare in modo che Elastic Transcoder ne crei una automaticamente.

La chiave KMS può essere utilizzata per crittografare la chiave di dati nei seguenti punti:

- Se fornisci la tua chiave di dati, è necessario crittografarla prima di trasferirla a Elastic Transcoder.
- Se richiedi a Elastic Transcoder di generare la chiave di dati, Elastic Transcoder crittografa la chiave di dati per te.

La chiave KMS può essere utilizzata per decrittare la chiave di dati nei seguenti punti:

- Elastic Transcoder decrittografa la chiave di dati fornita quando è necessario utilizzare tale chiave per crittografare il file di output o decrittare il file di input.
- Per decrittare una chiave di dati generata da Elastic Transcoder e utilizzarla per decrittare i file di output.

Per ulteriori informazioni, consulta Protezione dei contenuti HLS nella Guida per sviluppatori di Amazon Elastic Transcoder.

Contesto di crittografia di Elastic Transcoder

Un contesto di crittografia è un set di coppie chiave-valore che contiene dati arbitrari non segreti. Quando includi un contesto di crittografia in una richiesta di crittografia dei dati, AWS KMS lega il contesto di crittografia ai dati crittografati, in modo che lo stesso contesto di crittografia sia necessario per decrittografare i dati.

Elastic Transcoder usa lo stesso contesto di crittografia in tutte le richieste API AWS KMS per generare chiavi di dati, per la crittografia e la decrittografia.

```
"service" : "elastictranscoder.amazonaws.com"
```

Il contesto di crittografia viene scritto CloudTrail nei log per aiutarti a capire come è stata utilizzata una determinata chiave AWS KMS KMS. Nel `requestParameters` campo di un file di CloudTrail registro, il contesto di crittografia è simile al seguente:

```
"encryptionContext": {
  "service" : "elastictranscoder.amazonaws.com"
}
```

Per ulteriori informazioni su come configurare i processi Elastic Transcoder per usare una delle opzioni di crittografia supportate, consulta Opzioni di crittografia dei dati nella Guida per gli sviluppatori di Amazon Elastic Transcoder.

Come Amazon EMR utilizza AWS KMS

Quando si utilizza un cluster Amazon EMR, è possibile configurare il cluster per crittografare i dati inattivi prima di salvarli in una posizione di storage persistente. È possibile crittografare i dati inattivi su EMR File System (EMRFS), sui volumi di storage dei nodi del cluster o su entrambi. Per crittografare i dati a riposo è possibile utilizzare una AWS KMS key. Gli argomenti seguenti descrivono come un cluster Amazon EMR utilizza una chiave KMS per crittografare i dati inattivi.

> **Important**
>
> Amazon EMR supporta solo chiavi KMS simmetriche. Non è possibile utilizzare una chiave KMS asimmetrica per crittografare i dati inattivi in un cluster Amazon EMR. Per informazioni su come determinare se una chiave KMS è simmetrica o asimmetrica, consulta Individuazione di chiavi KMS asimmetriche.

I cluster Amazon EMR crittografano anche i dati in transito, il che significa che il cluster crittografa i dati prima dell'invio in rete. Non è possibile utilizzare una chiave KMS per crittografare i dati in transito. Per ulteriori informazioni, consulta Crittografia dei dati in transito nella Guida alla gestione di Amazon EMR.

Per ulteriori informazioni su tutte le opzioni di crittografia disponibili in Amazon EMR, consulta Opzioni di crittografia nella Guida alla gestione di Amazon EMR.

Argomenti

Crittografia dei dati su EMR File System (EMRFS)

I cluster Amazon EMR usano due file system distribuiti:

- Hadoop Distributed File System (HDFS). La crittografia HDFS non utilizza una chiave KMS in AWS KMS.
- File system EMR (EMRFS). EMRFS è un'implementazione di HDFS che consente ai cluster Amazon EMR di archiviare dati in Amazon Simple Storage Service (Amazon S3). EMRFS supporta quattro opzioni di crittografia, due delle quali utilizzano una chiave KMS in AWS KMS. Per ulteriori informazioni su tutte le opzioni di crittografia disponibili in Amazon EMRFS, consulta Opzioni di crittografia nella Guida alla gestione di Amazon EMR.

Le due opzioni di crittografia EMRFS che usano una chiave KMS utilizzano le seguenti caratteristiche di crittografia offerte da Amazon S3:

- Protezione dei dati utilizzando la crittografia lato server con AWS Key Management Service (SSE-KMS). Il cluster Amazon EMR invia i dati ad Amazon S3. Amazon S3 utilizza una chiave KMS per crittografare i dati prima di salvarli in un bucket S3. Per ulteriori informazioni su come effettuare tale operazione, consulta Processo di crittografia dei dati su EMRFS con SSE-KMS.
- Protezione dei dati con la crittografia lato client (CSE-KMS). I dati in un Amazon EMR sono crittografati con una AWS KMS keyprima di essere inviati ad Amazon S3 per l'archiviazione. Per ulteriori informazioni su come effettuare tale operazione, consulta Processo di crittografia dei dati su EMRFS con CSE-KMS.

Quando si configura un cluster Amazon EMR per crittografare i dati su EMRFS con una chiave KMS, si sceglie la chiave KMS che si desidera sia utilizzata da Amazon S3 o dal cluster Amazon EMR. Con SSE-KMS, puoi scegliere la Chiave gestita da AWS per Amazon S3 con l'alias aws/s3 o una chiave simmetrica gestita dal cliente che crei. Con la crittografia lato client, è necessario scegliere una chiave gestita dal cliente simmetrica creata dall'utente. Quando scegli una chiave gestita dal cliente, devi assicurarti che il cluster Amazon EMR abbia le autorizzazioni per utilizzare la chiave

KMS. Per ulteriori informazioni, consulta Utilizzo di AWS KMS keys per la crittografia nella Guida alla gestione di Amazon EMR.

Per la crittografia lato server e lato client, la chiave KMS scelta è la chiave root in un flusso di lavoro di crittografia envelope. I dati sono crittografati con una chiave di dati univoca che è crittografata con la chiave KMS in AWS KMS. I dati crittografati e una copia crittografata della chiave di dati vengono archiviati insieme come un singolo oggetto crittografato in un bucket S3. Per ulteriori informazioni sul funzionamento, consulta gli argomenti indicati di seguito.

Argomenti

- Processo di crittografia dei dati su EMRFS con SSE-KMS
- Processo di crittografia dei dati su EMRFS con CSE-KMS

Processo di crittografia dei dati su EMRFS con SSE-KMS

Quando configuri un cluster Amazon EMR per utilizzare SSE-KMS, il processo di crittografia lavora come segue:

1. Il cluster invia i dati ad Amazon S3 per lo storage in un bucket S3.
2. Amazon S3 invia una GenerateDataKeyrichiesta aAWS KMS, specificando l'ID della chiave KMS che hai scelto quando hai configurato il cluster per l'utilizzo di SSE-KMS. La richiesta include il contesto di crittografia, per ulteriori informazioni consulta Contesto di crittografia.
3. AWS KMS genera una chiave di crittografia dei dati univoca (chiave di dati), quindi invia due copie di questa chiave di dati ad Amazon S3. Una copia non è crittografata (testo normale) e l'altra copia viene crittografata con la chiave KMS.
4. Amazon S3 utilizza la chiave di dati in testo in chiaro per crittografare i dati ricevuti nella fase 1, quindi rimuove il prima possibile la chiave di dati in testo normale dalla memoria dopo l'utilizzo.
5. Amazon S3 archivia i dati crittografati e una copia crittografata della chiave di dati insieme come un singolo oggetto crittografato in un bucket S3.

Il processo di decrittografia avviene in questo modo:

1. Il cluster richiede un oggetto dati crittografati da un bucket S3.
2. Amazon S3 estrae la chiave di dati crittografati dall'oggetto S3, quindi invia la chiave di dati crittografati a AWS KMS con una richiesta Decrypt. La richiesta include un contesto di crittografia.

3. AWS KMS decritta la chiave di dati crittografati utilizzando la stessa chiave KMS usata per crittografarli, quindi invia la chiave di dati decrittata (testo normale) ad Amazon S3.
4. Amazon S3 utilizza la chiave di dati in testo normale per decrittografare i dati crittografati, quindi rimuove il prima possibile la chiave di dati in testo in chiaro dalla memoria dopo l'utilizzo.
5. Amazon S3 invia i dati decrittografati al cluster.

Processo di crittografia dei dati su EMRFS con CSE-KMS

Quando configuri un cluster Amazon EMR per utilizzare CSE-KMS, il processo di crittografia lavora come segue:

1. Quando è pronto per archiviare i dati in Amazon S3, il cluster invia una GenerateDataKeyrichiesta aAWS KMS, specificando l'ID chiave della chiave KMS che hai scelto quando hai configurato il cluster per l'utilizzo di CSE-KMS. La richiesta include il contesto di crittografia, per ulteriori informazioni consulta Contesto di crittografia.
2. AWS KMS genera una chiave di crittografia dei dati univoca (chiave di dati), quindi invia due copie di questa chiave di dati al cluster. Una copia non è crittografata (testo normale) e l'altra copia viene crittografata con la chiave KMS.
3. Il cluster utilizza la chiave di dati in testo normale per crittografare i dati, quindi rimuove il prima possibile la chiave di dati in testo normale dalla memoria dopo l'utilizzo.
4. Il cluster abbina i dati crittografati e una copia crittografata della chiave di dati insieme in un singolo oggetto crittografato.
5. Il cluster invia l'oggetto crittografato ad Amazon S3 per lo storage.

Il processo di decrittografia avviene in questo modo:

1. Il cluster richiede un oggetto dati crittografati a un bucket S3.
2. Amazon S3 invia l'oggetto crittografato al cluster.
3. Il cluster estrae la chiave di dati crittografati dall'oggetto crittografato, quindi invia la chiave di dati crittografati a AWS KMS con una richiesta Decrypt. La richiesta include il contesto di crittografia.
4. AWS KMS decritta la chiave di dati crittografati utilizzando la stessa chiave KMS usata per crittografarli, quindi invia la chiave di dati decrittati (testo in chiaro) al cluster.
5. Il cluster utilizza la chiave di dati in testo normale per decrittografare i dati crittografati, quindi rimuove il prima possibile la chiave di dati in testo normale dalla memoria dopo l'utilizzo.

Crittografia dei dati su volumi di storage di nodi cluster

Un cluster Amazon EMR è una raccolta di istanze Amazon Elastic Compute Cloud (Amazon EC2). Ogni istanza nel cluster viene chiamata nodo cluster o nodo. Ogni nodo può avere due tipi di volumi di archiviazione: volumi di archiviazione di istanze e volumi Amazon Elastic Block Store (Amazon EBS). È possibile configurare il cluster per l'utilizzo di Linux Unified Key Setup (LUKS) per crittografare entrambi i tipi di volumi di storage sui nodi (ma non il volume di avvio di ogni nodo). Questa si chiama la crittografia dei dati su disco locale.

Quando si abilita la crittografia dei dati su disco locale per un cluster, è possibile scegliere di crittografare la chiave LUKS con una chiave KMS in AWS KMS. Devi scegliere una chiave gestita dal cliente che hai creato; non è possibile utilizzare una Chiave gestita da AWS. Se scegli una gestita dal cliente, devi assicurarti che il cluster Amazon EMR abbia le autorizzazioni per utilizzare la chiave KMS. Per ulteriori informazioni, consulta Utilizzo di AWS KMS keys per la crittografia nella Guida alla gestione di Amazon EMR.

Quando abiliti la crittografia dei dati su disco locale utilizzando una chiave KMS, il processo di crittografia funziona in questo modo:

1. All'avvio di ogni nodo del cluster, invia una GenerateDataKeyrichiesta aAWS KMS, specificando l'ID della chiave KMS che hai scelto quando hai abilitato la crittografia del disco locale per il cluster.
2. AWS KMS genera una chiave di crittografia dei dati univoca (chiave di dati), quindi invia due copie di questa chiave di dati al nodo. Una copia non è crittografata (testo normale) e l'altra copia viene crittografata con la chiave KMS.
3. Il nodo utilizza una versione con codifica base64 della chiave di dati di testo normale come password che protegge la chiave LUKS. Il nodo salva la copia crittografata della chiave di dati per il volume di avvio.
4. Se il nodo si riavvia, il nodo riavviato invia la chiave di dati crittografati a AWS KMS con la richiesta Decrypt.
5. AWS KMS decritta la chiave di dati crittografati utilizzando la stessa chiave KMS usata per crittografarli, quindi invia la chiave di dati decrittati (testo in chiaro) al nodo.
6. Il nodo utilizza una versione con codifica base64 della chiave di dati di testo normale come password per sbloccare la chiave LUKS.

Contesto di crittografia

Ogni servizio AWS integrato con AWS KMS può specificare un contesto di crittografia quando utilizza AWS KMS per generare chiavi di dati o per crittografare o decrittare i dati. Il contesto di crittografia rappresenta informazioni autenticate supplementari utilizzate da AWS KMS per verificare l'integrità dei dati. Quando un servizio specifica un contesto di crittografia per un'operazione di crittografia, il servizio deve specificare lo stesso contesto di crittografia anche per l'operazione di decrittografia corrispondente o la decrittografia non riuscirà. Il contesto di crittografia viene scritto anche nei file di log AWS CloudTrail per aiutarti a comprendere perché è stata utilizzata una determinata chiave KMS.

La sezione seguente spiega il contesto di crittografia utilizzato in ogni scenario di crittografia Amazon EMR che utilizza una chiave KMS.

Contesto di crittografia per la crittografia EMRFS con SSE-KMS

Con SSE-KMS, il cluster Amazon EMR invia i dati ad Amazon S3, quindi Amazon S3 utilizza una chiave KMS per crittografare i dati prima di salvarli in un bucket S3. In questo caso, Amazon S3 utilizza l'Amazon Resource Name (ARN) dell'oggetto S3 come contesto di crittografia per ogni richiesta GenerateDataKeyand Decrypt a cui viene inviata. AWS KMS L'esempio seguente mostra una rappresentazione JSON del contesto di crittografia che Amazon S3 utilizza.

```
{ "aws:s3:arn" : "arn:aws:s3:::S3_bucket_name/S3_object_key" }
```

Contesto di crittografia per la crittografia EMRFS con CSE-KMS

Con CSE-KMS, il cluster Amazon EMR utilizza una chiave KMS per crittografare i dati prima di inviarli a Amazon S3 per l'archiviazione. In questo caso, il cluster utilizza l'Amazon Resource Name (ARN) della chiave KMS come contesto di crittografia per ogni richiesta GenerateDataKeyand Decrypt a cui invia. AWS KMS L'esempio seguente mostra una rappresentazione JSON del contesto di crittografia che il cluster utilizza.

```
{ "kms_cmk_id" : "arn:aws:kms:us-
east-2:111122223333:key/0987ab65-43cd-21ef-09ab-87654321cdef" }
```

Contesto di crittografia per la crittografia su disco locale con LUKS

Quando un cluster Amazon EMR utilizza la crittografia del disco locale con LUKS, i nodi del cluster non specificano il contesto di crittografia con le richieste GenerateDataKeye Decrypt a cui inviano. AWS KMS

Come AWS Nitro Enclaves usa AWS KMS

AWS KMS supporta l'attestazione crittografica per enclavi Nitro AWS. Le applicazioni che supportano enclavi Nitro AWS richiamano le seguenti operazioni crittografiche AWS KMS con un documento di attestazione firmato per l'enclave. Queste API AWS KMS verificano che il documento di attestazione provenga da un'enclave Nitro. Per tale motivo, invece di restituire dati in testo normale nella risposta, queste API eseguono la crittografia del testo normale con la chiave pubblica dal documento di attestazione e restituiscono testo criptato che può essere decrittato solo dalla chiave privata corrispondente nell'enclave.

- Decrypt
- GenerateDataKey
- GenerateDataKeyPair
- GenerateRandom

La tabella seguente illustra le differenze tra la risposta alle richieste di enclavi Nitro e la risposta standard per ogni operazione dell'API.

Operazione AWS KMS	Risposta standard	Risposta per enclavi Nitro AWS
`Decrypt`	Restituisce dati in testo normale	Restituisce i dati di testo normale crittografati dalla chiave pubblica dal documento di attestazione
`GenerateDataKey`	Restituisce una copia in testo normale della chiave dati (Restituisce anche una copia della chiave dati crittografata da una chiave KMS)	Restituisce una copia della chiave dati crittografata dalla chiave pubblica dal documento di attestazione (Restituisce anche una copia della chiave dati crittografata da una chiave KMS)
`GenerateDataKeyPair`	Restituisce una copia in testo normale della chiave privata	Restituisce una copia della chiave privata crittografata

Operazione AWS KMS	Risposta standard	Risposta per enclavi Nitro AWS
	(Restituisce anche la chiave pubblica e una copia della chiave privata crittografata da una chiave KMS)	dalla chiave pubblica dal documento di attestazione (Restituisce anche la chiave pubblica e una copia della chiave privata crittografata da una chiave KMS)
`GenerateRandom`	Restituisce una stringa di byte casuali	Restituisce la stringa di byte casuali crittografata dalla chiave pubblica dal documento di attestazione

AWS KMS supporta chiavi di condizione della policy che puoi utilizzare per consentire o negare operazioni dell'enclave con una chiave AWS KMS basata sul contenuto del documento di attestazione. Puoi monitorare le richieste a AWS KMS per la tua enclave Nitro anche nei log di AWS CloudTrail.

Argomenti

- Come richiamare le API AWS KMS per un'enclave Nitro
- Chiavi di condizione AWS KMS per AWS Nitro Enclaves
- Richieste di monitoraggio per enclavi Nitro

Come richiamare le API AWS KMS per un'enclave Nitro

Per richiamare le API AWS KMS per un'enclave Nitro, usa il parametro `Recipient` nella richiesta in modo da fornire il documento di attestazione firmato per l'enclave e l'algoritmo di crittografia da utilizzare con la chiave pubblica dell'enclave. Quando una richiesta include il parametro `Recipient` con un documento di attestazione firmato, la risposta include un campo `CiphertextForRecipient` con il testo criptato crittografato dalla chiave pubblica. Il campo di testo normale è nullo o vuoto.

Il parametro `Recipient` deve specificare un documento di attestazione firmato da un'enclave Nitro AWS. AWS KMS si basa sulla firma digitale per il documento di attestazione dell'enclave per

dimostrare che la chiave pubblica nella richiesta proviene da un'enclave valida. Non è possibile fornire il proprio certificato per firmare digitalmente il documento di attestazione.

Per specificare il parametro `Recipient`, usa l'SDK per enclavi Nitro AWS o qualunque SDK AWS. L'SDK per enclavi Nitro AWS, supportato solo in un'enclave Nitro, aggiunge automaticamente il parametro `Recipient` e i relativi valori a ogni richiesta AWS KMS. Per effettuare richieste di enclavi Nitro negli SDK AWS, devi specificare il parametro `Recipient` e i relativi valori. Il supporto per l'attestazione crittografica di enclavi Nitro negli SDK AWS è stato introdotto a marzo 2023.

AWS KMS supporta chiavi di condizione della policy che puoi utilizzare per consentire o negare operazioni dell'enclave con una chiave AWS KMS basata sul contenuto del documento di attestazione. Puoi monitorare le richieste a AWS KMS per la tua enclave Nitro anche nei log di AWS CloudTrail.

Per informazioni dettagliate sul `Recipient` parametro e sul campo di `CiphertextForRecipient` risposta AWS, consulta Decrypt e GenerateRandomgli argomenti nell'AWS Key Management ServiceAPI Reference GenerateDataKeyGenerateDataKeyPair, nell'SDK AWSNitro Enclaves o in qualsiasi SDK. AWS Per informazioni sull'impostazione dei dati e delle chiavi dati per la crittografia, consulta Utilizzo dell'attestazione crittografica con AWS KMS.

Chiavi di condizione AWS KMS per AWS Nitro Enclaves

Puoi specificare chiavi di condizione nelle policy delle chiavi e nelle policy IAM che controllano l'accesso alle tue risorse AWS KMS. Le dichiarazioni delle policy che includono una chiave di condizione sono efficaci solo quando sono soddisfatte le relative condizioni.

AWS KMSfornisce chiavi di condizione che limitano le autorizzazioni per Decrypt e le GenerateRandomoperazioni in base al contenuto GenerateDataKeydel GenerateDataKeyPairdocumento di attestazione firmato contenuto nella richiesta. Queste chiavi di condizione funzionano solo quando una richiesta di un'operazione AWS KMS include il parametro `Recipient` con un documento di attestazione valido proveniente da un'enclave Nitro AWS. Per specificare il parametro `Recipient`, usa l'SDK per enclavi Nitro di AWS o qualunque SDK di AWS.

Le chiavi di condizione AWS KMS specifiche delle enclavi sono valide nelle dichiarazioni della policy della chiave e nelle dichiarazioni della policy IAM anche se non appaiono nella console IAM o nella Guida di riferimento sull'autorizzazione del servizio IAM.

km: 384 RecipientAttestation ImageSha

Chiavi di condizione AWS KMS	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy

`kms:RecipientAttestation:ImageSha384`	Stringa	A valore singolo	`Decrypt`
			`GenerateDataKey`
			`GenerateDataKeyPair`
			`GenerateRandom`
				Policy delle chiavi e policy IAM

La chiave di condizione `kms:RecipientAttestation:ImageSha384` controlla l'accesso a `Decrypt`, `GenerateDataKey`, `GenerateDataKeyPair` e `GenerateRandom` con una chiave KMS quando il digest immagine del documento di attestazione firmato nella richiesta corrisponde al valore nella chiave di condizione. Il valore `ImageSha384` corrisponde a PCR0 nel documento di attestazione. Questa chiave di condizione è efficace solo quando il parametro `Recipient` nella richiesta specifica un documento di attestazione firmato per un'enclave Nitro AWS.

Questo valore è incluso anche negli CloudTraileventi per le richieste alle AWS KMS enclavi Nitro.

> **Note**
>
> Questa chiave di condizione è valida nelle istruzioni delle policy delle chiavi e nelle istruzioni delle policy IAM, anche se non viene visualizzata nella console IAM o nella Documentazione di riferimento dell'autorizzazione del servizio IAM.

Ad esempio, la seguente dichiarazione di politica chiave consente al `data-processing` ruolo di utilizzare la chiave KMS per Decrypt,, e le operazioni. GenerateDataKeyGenerateDataKeyPairGenerateRandom La chiave di condizione `kms:RecipientAttestation:ImageSha384` consente le operazioni solo quando il valore del digest immagine (PCR0) del documento di attestazione nella richiesta corrisponde al valore del digest

nella condizione. Questa chiave di condizione è efficace solo quando il parametro `Recipient` nella richiesta specifica un documento di attestazione firmato per un'enclave Nitro AWS.

Se la richiesta non include un documento di attestazione valido da un'enclave Nitro AWS, l'autorizzazione viene negata perché questa condizione non è soddisfatta.

```
{
  "Sid" : "Enable enclave data processing",
  "Effect" : "Allow",
  "Principal" : {
    "AWS" : "arn:aws:iam::111122223333:role/data-processing"
  },
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey",
    "kms:GenerateDataKeyPair",
    "kms:GenerateRandom"
  ],
  "Resource" : "*",
  "Condition": {
    "StringEqualsIgnoreCase": {
      "kms:RecipientAttestation:ImageSha384":
 "9fedcba8abcdef7abcdef6abcdef5abcdef4abcdef3abcdef2abcdef1abcdef1abcdef0abcdef1abcdef2abcdef3a
    }
  }
}
```

kms:: PCR RecipientAttestation <PCR_ID>

Chiavi di condizione AWS KMS	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy

`kms:RecipientAttestation:PCR<PCR_ID>`	Stringa	A valore singolo	`Decrypt`
			`GenerateDataKey`
			`GenerateDataKeyPair`
				Policy delle chiavi e policy IAM

Chiavi di condizione AWS KMS	Tipo di condizioni	Value type (Tipo di valore)	Operazioni API	Tipo di policy
			`GenerateRandom`	

La chiave di condizione `kms:RecipientAttestation:PCR<PCR_ID>` controlla l'accesso a `Decrypt`, `GenerateDataKey`, `GenerateDataKeyPair` e `GenerateRandom` con una chiave KMS solo quando i registri di configurazione della piattaforma (PCR) dal documento di attestazione firmato nella richiesta corrispondono ai registri PCR nella chiave di condizione. Questa chiave di condizione è efficace solo quando il parametro `Recipient` nella richiesta specifica un documento di attestazione firmato da un'enclave Nitro AWS.

Questo valore è incluso anche negli CloudTraileventi che rappresentano le richieste alle enclavi di Nitro. AWS KMS

> **Note**
>
> Questa chiave di condizione è valida nelle istruzioni delle policy delle chiavi e nelle istruzioni delle policy IAM, anche se non viene visualizzata nella console IAM o nella Documentazione di riferimento dell'autorizzazione del servizio IAM.

Per specificare un valore PCR, utilizzare il formato seguente. Concatena l'ID PCR al nome della chiave di condizione. Il valore PCR deve essere una stringa esadecimale minuscola di un massimo di 96 byte.

```
"kms:RecipientAttestation:PCRPCR_ID": "PCR_value"
```

Ad esempio, la seguente chiave di condizione specifica un valore particolare per PCR1, che corrisponde all'hash del kernel utilizzato per l'enclave e il processo di bootstrap.

```
kms:RecipientAttestation:PCR1:
 "0x1abcdef2abcdef3abcdef4abcdef5abcdef6abcdef7abcdef8abcdef9abcdef8abcdef7abcdef6abcdef5abcdef
```

Il seguente esempio di istruzione della policy della chiave consente al ruolo `data-processing` di utilizzare la chiave KMS per l'operazione Decrypt.

La chiave di condizione `kms:RecipientAttestation:PCR` in questa istruzione consente l'operazione solo quando il valore PCR1 nel documento di attestazione firmato nella richiesta corrisponde al valore `kms:RecipientAttestation:PCR1` nella condizione. Usa l'operatore di policy `StringEqualsIgnoreCase` per richiedere un confronto senza distinzione tra maiuscole e minuscole dei valori PCR.

Se la richiesta non include un documento di attestazione, l'autorizzazione viene negata perché questa condizione non è soddisfatta.

```
{
  "Sid" : "Enable enclave data processing",
  "Effect" : "Allow",
  "Principal" : {
    "AWS" : "arn:aws:iam::111122223333:role/data-processing"
  },
  "Action": "kms:Decrypt",
  "Resource" : "*",
  "Condition": {
    "StringEqualsIgnoreCase": {
      "kms:RecipientAttestation:PCR1":
 "0x1de4f2dcf774f6e3b679f62e5f120065b2e408dcea327bd1c9dddaea6664e7af79355814748447674530 82c6f15
    }
  }
}
```

Richieste di monitoraggio per enclavi Nitro

Puoi usare i tuoi AWS CloudTrail log per monitorare Decrypt,, GenerateDataKeye GenerateRandomle operazioni per un'enclave GenerateDataKeyPairNitro. AWS In queste voci di log, il campo `additionalEventData` contiene un campo `recipient` con l'ID del modulo (`attestationDocumentModuleId`), il digest dell'immagine (`attestationDocumentEnclaveImageDigest`) e i registri di configurazione della piattaforma (PCR) dal documento di attestazione nella richiesta. Questi campi sono inclusi solo quando il parametro `Recipient` nella richiesta specifica un documento di attestazione firmato da un'enclave Nitro AWS.

L'ID del modulo è l'ID enclave dell'enclave Nitro. Il digest dell'immagine è l'hash SHA384 dell'immagine dell'enclave. Puoi possibile utilizzare il digest dell'immagine e i valori PCR in condizioni per le policy delle chiavi e le policy IAM. Per informazioni sui PCR, consulta Dove reperire le misurazioni di un'enclave nella Guida per l'utente di enclavi Nitro di AWS.

Questa sezione mostra un esempio di voce di CloudTrail registro per ciascuna delle richieste di enclave Nitro supportate a. AWS KMS

Decrypt (per un'enclave)

L'esempio seguente mostra una voce del log di AWS CloudTrail per un'operazione Decrypt per un'enclave Nitro di AWS.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2020-07-27T22:58:24Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": null,
    "additionalEventData": {
        "recipient": {
            "attestationDocumentModuleId": "i-123456789abcde123-enc123456789abcde12",
            "attestationDocumentEnclaveImageDigest": "<AttestationDocument.PCR0>",
            "attestationDocumentEnclavePCR1": "<AttestationDocument.PCR1>",
            "attestationDocumentEnclavePCR2": "<AttestationDocument.PCR2>",
            "attestationDocumentEnclavePCR3": "<AttestationDocument.PCR3>",
            "attestationDocumentEnclavePCR4": "<AttestationDocument.PCR4>",
            "attestationDocumentEnclavePCR8": "<AttestationDocument.PCR8>"
        }
    },
    "requestID": "b4a65126-30d5-4b28-98b9-9153da559963",
    "eventID": "e5a2f202-ba1a-467c-b4ba-f729d45ae521",
```

```
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

GenerateDataKey (per un'enclave)

L'esempio seguente mostra una voce di AWS CloudTrail registro di un'GenerateDataKeyoperazione per un'enclave AWS Nitro.

```
{
    "eventVersion": "1.02",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2014-11-04T00:52:40Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "numberOfBytes": 32
    },
    "responseElements": null,
    "additionalEventData": {
        "recipient": {
            "attestationDocumentModuleId": "i-123456789abcde123-enc123456789abcde12",
            "attestationDocumentEnclaveImageDigest": "<AttestationDocument.PCR0>",
```

```
            "attestationDocumentEnclavePCR1": "<AttestationDocument.PCR1>",
            "attestationDocumentEnclavePCR2": "<AttestationDocument.PCR2>",
            "attestationDocumentEnclavePCR3": "<AttestationDocument.PCR3>",
            "attestationDocumentEnclavePCR4": "<AttestationDocument.PCR4>",
            "attestationDocumentEnclavePCR8": "<AttestationDocument.PCR8>"
        }
    },
    "requestID": "e0eb83e3-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "a9dea4f9-8395-46c0-942c-f509c02c2b71",
    "readOnly": true,
    "resources": [{
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "accountId": "111122223333"
    }],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

GenerateDataKeyPair (per un'enclave)

L'esempio seguente mostra una voce di AWS CloudTrail registro di un'GenerateDataKeyPairoperazione per un'AWSenclave Nitro.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::111122223333:user/Alice",
            "accountId": "111122223333",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice"
    },
    "eventTime": "2020-07-27T18:57:57Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKeyPair",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyPairSpec": "RSA_3072",
        "encryptionContext": {
```

```
            "Project": "Alpha"
        },
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": null,
    "additionalEventData": {
        "recipient": {
            "attestationDocumentModuleId": "i-123456789abcde123-enc123456789abcde12",
            "attestationDocumentEnclaveImageDigest": "<AttestationDocument.PCR0>",
            "attestationDocumentEnclavePCR1": "<AttestationDocument.PCR1>",
            "attestationDocumentEnclavePCR2": "<AttestationDocument.PCR2>",
            "attestationDocumentEnclavePCR3": "<AttestationDocument.PCR3>",
            "attestationDocumentEnclavePCR4": "<AttestationDocument.PCR4>",
            "attestationDocumentEnclavePCR8": "<AttestationDocument.PCR8>"
        }
    },
    "requestID": "52fb127b-0fe5-42bb-8e5e-f560febde6b0",
    "eventID": "9b6bd6d2-529d-4890-a949-593b13800ad7",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

GenerateRandom (per un'enclave)

L'esempio seguente mostra una voce di AWS CloudTrail registro di un'GenerateRandomoperazione per un'enclave AWS Nitro.

```
{
    "eventVersion": "1.02",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
```

```
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2014-11-04T00:52:37Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateRandom",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "recipient": {
            "attestationDocumentModuleId": "i-123456789abcde123-enc123456789abcde12",
            "attestationDocumentEnclaveImageDigest": "<AttestationDocument.PCR0>",
            "attestationDocumentEnclavePCR1": "<AttestationDocument.PCR1>",
            "attestationDocumentEnclavePCR2": "<AttestationDocument.PCR2>",
            "attestationDocumentEnclavePCR3": "<AttestationDocument.PCR3>",
            "attestationDocumentEnclavePCR4": "<AttestationDocument.PCR4>",
            "attestationDocumentEnclavePCR8": "<AttestationDocument.PCR8>"
        }
    },
    "requestID": "df1e3de6-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "239cb9f7-ae05-4c94-9221-6ea30eef0442",
    "readOnly": true,
    "resources": [],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

Come Amazon Redshift utilizza AWS KMS

Questo argomento descrive il modo in cui Amazon Redshift utilizza AWS KMS per crittografare i dati.

Argomenti

- Crittografia di Amazon Redshift
- Contesto di crittografia

Crittografia di Amazon Redshift

Un data warehouse Amazon Redshift è costituito da un insieme di risorse di calcolo denominate nodi, strutturate in un gruppo denominato cluster. Ciascun cluster esegue un motore Amazon Redshift e contiene uno o più database.

Per la crittografia Amazon Redshift usa un'architettura a quattro livelli basata su chiavi. L'architettura consiste in chiavi di crittografia dei dati, una chiave di database, una chiave del cluster e una chiave root. È possibile utilizzare una AWS KMS key come chiave root.

Le chiavi di crittografia dei dati crittografano i blocchi di dati nel cluster. Ogni blocco di dati viene assegnato una chiave AES-256 generata in modo casuale. Queste chiavi sono crittografate utilizzando la chiave di database per il cluster.

La chiave di database crittografa le chiavi di crittografia dei dati nel cluster. La chiave del database è una chiave AES-256 generata in modo casuale. È archiviata su disco in una rete separata dal cluster Amazon Redshift e passata al cluster attraverso un canale sicuro.

La chiave del cluster crittografa la chiave di database per il cluster Amazon Redshift. È possibile utilizzare AWS KMS, AWS CloudHSM o un modulo di sicurezza hardware (HSM) esterno per gestire la chiave del cluster. Consulta la documentazione di Amazon Redshift Database Encryption per ulteriori dettagli.

È possibile richiedere la crittografia selezionando la casella appropriata nella console Amazon Redshift. Puoi specificare una chiave gestita dal cliente da utilizzare scegliendone una dall'elenco che appare sotto la casella di crittografia. Se non specifichi una chiave gestita dal cliente, Amazon Redshift utilizza la Chiave gestita da AWS per Amazon Redshift sotto l'account.

> **Important**
>
> Amazon Redshift supporta solo chiavi KMS di crittografia simmetrica. Non è possibile utilizzare una chiave KMS asimmetrica come chiave master in un flusso di lavoro di crittografia Amazon Redshift. Per informazioni su come determinare se una chiave KMS è simmetrica o asimmetrica, consulta Individuazione di chiavi KMS asimmetriche.

Contesto di crittografia

Ogni servizio integrato con AWS KMS specifica un contesto di crittografia quando richiede le chiavi dei dati, la crittografia e la decrittografia. Il contesto di crittografia rappresenta dati autenticati

supplementari (AAD) utilizzati da AWS KMS per verificare l'integrità dei dati. Questo significa che, quando viene specificato un contesto di crittografia per un'operazione di crittografia, il servizio specifica lo stesso contesto di crittografia anche per l'operazione di decrittografia o la decrittografia non riuscirà. Amazon Redshift utilizza l'ID cluster e il tempo di creazione per il contesto di crittografia. Nel `requestParameters` campo di un file di CloudTrail registro, il contesto di crittografia sarà simile a questo.

```
"encryptionContext": {
    "aws:redshift:arn": "arn:aws:redshift:region:account_ID:cluster:cluster_name",
    "aws:redshift:createtime": "20150206T1832Z"
},
```

Puoi cercare il nome del cluster nei tuoi CloudTrail log per capire quali operazioni sono state eseguite utilizzando una AWS KMS key (chiave KMS). Le operazioni includono la crittografia e la decrittografia dei cluster e la generazione di chiavi di dati.

Come Amazon Relational Database Service (Amazon RDS) usa AWS KMS

Puoi utilizzare Amazon Relational Database Service (Amazon RDS) per configurare, utilizzare e dimensionare un database relazionale nel cloud. Puoi crittografare le tue risorse Amazon RDS con una Chiave gestita da AWS o una chiave gestita dal cliente. Amazon RDS è integrato nella crittografia Amazon Elastic Block Store (Amazon EBS) per fornire la crittografia completa del disco per volumi di database.

Per informazioni dettagliate su come Amazon RDS utilizza le chiavi KMS per proteggere le tue risorse, consulta la sezione Crittografia delle risorse Amazon RDS e Gestione delle chiavi AWS KMS nella Guida per l'utente di Amazon RDS.

Come AWS Secrets Manager utilizza AWS KMS

AWS Secrets Manager è un servizio AWS che esegue la crittografia, archivia i segreti e li decrittografa e restituisce in modo trasparente in testo normale. È concepito soprattutto per archiviare i segreti dell'applicazione, ad esempio le credenziali di accesso, che cambiano periodicamente e non devono essere hardcoded o archiviate in testo normale nell'applicazione. In alternativa alle credenziali hardcoded o alle ricerche della tabella, l'applicazione chiama Secrets Manager.

Secrets Manager supporta anche funzionalità che periodicamente ruotano i segreti associati ai database utilizzati di frequente. Crittografa sempre i segreti appena ruotati prima che vengano archiviati.

Secrets Manager si integra con AWS Key Management Service (AWS KMS) per crittografare ogni versione di ogni valore segreto con una chiave dati univoca protetta da una AWS KMS key. Questa integrazione protegge i segreti con le chiavi di crittografia che fanno in modo che AWS KMS sia sempre crittografato. Consente inoltre di impostare autorizzazioni personalizzate sulla chiave KMS e controllare le operazioni che generano, crittografano e decrittano le chiavi di dati che proteggono i segreti.

Per informazioni su come Secrets Manager utilizza le chiavi KMS per proteggere i segreti, consulta Crittografia e decrittografia dei segreti nella Guida per l'utente di AWS Secrets Manager.

Come Amazon Simple Email Service (Amazon SES) usa AWS KMS

È possibile usare Amazon Simple Email Service (Amazon SES) per ricevere e-mail, e (facoltativamente) per crittografare i messaggi delle e-mail ricevuti prima di archiviarli nel bucket di Amazon Simple Storage Service (Amazon S3) che hai scelto. Quando si configura Amazon SES per crittografare i messaggi delle e-mail, è necessario scegliere la AWS KMS key AWS KMS nella quale Amazon SES crittografa i messaggi. È possibile scegliere la Chiave gestita da AWS per Amazon SES (il suo alias è `aws/ses`), oppure scegliere una chiave gestita da un cliente creata in AWS KMS.

> **Important**
>
> Amazon SES supporta solo chiavi simmetriche KMS. Non è possibile utilizzare una chiave asimmetrica KMS per crittografare i tuoi messaggi della e-mail di Amazon SES. Per informazioni su come determinare se una chiave KMS è simmetrica o asimmetrica, consulta Individuazione di chiavi KMS asimmetriche.

Per ulteriori informazioni sulla ricezione di e-mail tramite Amazon SES, consulta nelle e-mail ricevute con Amazon SES nella Guida dello Sviluppatore di Amazon Simple Email Service.

Argomenti

- Panoramica della crittografia di Amazon SES usando AWS KMS

- Contesto di crittografia di Amazon SES
- Concessione ad Amazon SES l'autorizzazione a utilizzare la tua chiave AWS KMS key
- Ricezione e decrittografia di messaggi e-mail

Panoramica della crittografia di Amazon SES usando AWS KMS

Quando si configura Amazon SES per la ricezione di e-mail e la crittografia di messaggi e-mail prima di salvarli nel bucket S3, il processo funziona in questo modo:

1. Puoi creare una regola di ricezione per Amazon SES, specificando l'operazione S3, un bucket S3 per lo storage e una AWS KMS key per la crittografia.
2. Amazon SES riceve un messaggio e-mail che soddisfa la regola di ricezione.
3. Amazon SES richiede una chiave di dati univoca crittografata con la chiave KMS specificata nella regola di ricezione applicabile.
4. AWS KMS crea una nuova chiave di dati, esegue la crittografia utilizzando la chiave KMS specificata e invia le copie crittografate e in testo normale della chiave di dati ad Amazon SES.
5. Amazon SES utilizza la chiave di dati in testo normale per crittografare il messaggio e-mail, quindi rimuove il prima possibile la chiave di dati in testo normale dalla memoria dopo l'utilizzo.
6. Amazon SES mette il messaggio e-mail crittografato e la chiave di dati crittografati nel bucket S3 specificato. La chiave di dati crittografata viene archiviata come metadati con il messaggio e-mail crittografato.

Per realizzare Step 3 attraverso Step 6, Amazon SES utilizza il AWS-client di crittografia Amazon S3 fornito. Utilizza lo stesso client per recuperare i tuoi messaggi e-mail crittografati da Amazon S3 e decrittografarli. Per ulteriori informazioni, consulta Ricezione e decrittografia di messaggi e-mail.

Contesto di crittografia di Amazon SES

Quando Amazon SES richiede una chiave di dati per crittografare i messaggi e-mail ricevuti (Step 3 in Panoramica della crittografia di Amazon SES usando AWS KMS), include nella richiesta un contesto di crittografia. Il contesto di crittografia fornisce dati autenticati supplementari (AAD) utilizzati da AWS KMS per garantire l'integrità dei dati. Il contesto di crittografia viene scritto anche nei file di log AWS CloudTrail per aiutarti a comprendere perché è stata utilizzata una determinata AWS KMS key (chiave KMS). Amazon SES utilizza il seguente contesto di crittografia:

- L'ID dell'Account AWS in cui hai configurato Amazon SES per ricevere messaggi e-mail

- Il nome della regola di ricezione di Amazon SES che ha invocato l'azione S3 nel messaggio e-mail
- L'ID del messaggio di Amazon SES per il messaggio delle e-mail

L'esempio seguente mostra una rappresentazione JSON del contesto di crittografia che Amazon SES utilizza:

```
{
  "aws:ses:source-account": "111122223333",
  "aws:ses:rule-name": "example-receipt-rule-name",
  "aws:ses:message-id": "d6iitobk75ur44p8kdnnp7g2n800"
}
```

Concessione ad Amazon SES l'autorizzazione a utilizzare la tua chiave AWS KMS key

Per crittografare i messaggi e-mail, è possibile utilizzare la Chiave gestita da AWS nel proprio account per Amazon SES (`aws/ses`) oppure usare una chiave gestita dal cliente creata dall'utente. Amazon SES ha già l'autorizzazione di utilizzare la Chiave gestita da AWS nel tuo conto. Tuttavia, per specificare una chiave gestita dal cliente quando aggiungi l'operazione S3 alla regola di ricezione Amazon SES, devi accertarti che Amazon SES abbia l'autorizzazione a utilizzare la chiave KMS per crittografare i messaggi e-mail.

Per offrire ad Amazon SES l'autorizzazione a utilizzare la tua chiave gestita dal cliente, aggiungi la seguente istruzione alla policy delle chiavi della tua KMS:

```
{
  "Sid": "Allow SES to encrypt messages using this KMS key",
  "Effect": "Allow",
  "Principal": {"Service": "ses.amazonaws.com"},
  "Action": [
    "kms:Encrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:ses:rule-name": false,
      "kms:EncryptionContext:aws:ses:message-id": false
    },
```

```
    "StringEquals": {"kms:EncryptionContext:aws:ses:source-account": "ACCOUNT-ID-
WITHOUT-HYPHENS"}
  }
}
```

Sostituisci *ACCOUNT-ID-WITHOUT-HYPHENS* con l'ID di 12 cifre dell'Account AWS in cui hai configurato Amazon SES per ricevere i messaggi e-mail. Questa istruzione di policy consente ad Amazon SES di crittografare i dati con questa chiave KMS solo in queste condizioni:

- Amazon SES deve specificare `aws:ses:rule-name` e `aws:ses:message-id` nel `EncryptionContext` delle richieste API AWS KMS.
- Amazon SES deve specificare `aws:ses:source-account` nel `EncryptionContext` delle richieste API AWS KMS e il valore per `aws:ses:source-account` deve corrispondere all' ID Account AWS specificato nella policy delle chiavi.

Per ulteriori informazioni sul contesto di crittografia che Amazon SES utilizza per crittografare i messaggi e-mail, consulta Contesto di crittografia di Amazon SES. Per informazioni generali su come AWS KMS usa il contesto di crittografia, consulta contesto di crittografia.

Ricezione e decrittografia di messaggi e-mail

Amazon SES non dispone di autorizzazioni per decrittare i messaggi e-mail crittografati e non è in grado di decrittografarli per te. È necessario scrivere codice per ricevere messaggi e-mail da Amazon S3 e decrittografarli. Per rendere questa operazione più semplice, utilizza il client di crittografia di Amazon S3. I seguenti SDK di AWS includono il client di crittografia di Amazon S3:

- AWS SDK for Java — Consulta AmazonS3EncryptionClient e AmazonS3EncryptionClientV2 nella Documentazione di riferimento API di AWS SDK for Java.
- AWS SDK for Ruby — Consulta Aws::S3::Encryption::Client nella Documentazione di riferimento API di AWS SDK for Ruby.
- AWS SDK for .NET — Consulta AmazonS3EncryptionClient nella Documentazione di riferimento API di AWS SDK for .NET.
- AWS SDK for Go — Consulta s3crypto nella Documentazione di riferimento API di AWS SDK for Go.

Il client di crittografia Amazon S3 semplifica il lavoro di formulare le richieste necessarie ad Amazon S3 per recuperare il messaggio e-mail crittografato e a AWS KMS per decrittografare la chiave di dati

crittografata del messaggio e di decrittografare il messaggio e-mail. Ad esempio, per decrittografare la chiave di dati crittografati correttamente è necessario superare lo stesso contesto di crittografia superato da Amazon SES quando richiede la chiave di dati da AWS KMS (Step 3 nella Panoramica della crittografia di Amazon SES usando AWS KMS). Il client di crittografia di Amazon S3 gestisce questa operazione e molto altro lavoro per te.

Per un codice di esempio che utilizza il client di crittografia di Amazon S3 in AWS SDK for Java per eseguire la decrittografia, consulta quanto segue:

- Utilizzo di una chiave KMS archiviata in AWS KMS nella Guida per l'utente di Amazon Simple Storage Service.
- Crittografia di Amazon S3 con AWS Key Management Service sul Blog per gli sviluppatori di AWS.

Come Amazon Simple Storage Service (Amazon S3) usa AWS KMS

Amazon Simple Storage Service (Amazon S3) è un servizio di archiviazione oggetti che consente di archiviare dati come oggetti all'interno dei bucket. I bucket e gli oggetti che contengono sono privati e accessibili solo se concedi esplicitamente le autorizzazioni di accesso.

Amazon S3 si integra con AWS Key Management Service (AWS KMS) per fornire la crittografia lato server degli oggetti Amazon S3. Amazon S3 utilizza le chiavi AWS KMS per crittografare gli oggetti Amazon S3. Le chiavi di crittografia che proteggono i tuoi oggetti non lasciano mai la AWS KMS non crittografata. Questa integrazione consente inoltre di impostare le autorizzazioni personalizzate sulla chiave AWS KMS e verificare le operazioni che generano, crittografano e decrittano le chiavi di dati che proteggono i segreti.

Per ridurre il volume delle chiamate ad Amazon S3AWS KMS, usa le bucket key di Amazon S3, che sono key-encryption-keys protette da chiavi KMS e che vengono riutilizzate per un periodo di tempo limitato in Amazon S3. Le chiavi del bucket possono ridurre i costi delle richieste AWS KMS fino al 99%. È possibile configurare una chiave del bucket per tutti gli oggetti in un bucket Amazon S3, oppure per un determinato oggetto. in un bucket Amazon S3.

Per ulteriori informazioni su come Amazon S3 utilizza AWS KMS, consultare Protezione dei dati mediante la crittografia lato server con chiavi KMS (SSE-KMS) nella Guida per l'utente di Amazon S3.

Utilizzo di AWS KMS da parte di AWS Systems Manager Parameter Store

Con AWS Systems Manager Parameter Store, è possibile creare parametri di stringa sicura, parametri che hanno un nome parametro in testo in chiaro e un valore di parametro crittografato. Parameter Store utilizza AWS KMS per crittografare e decrittare i valori di parametro dei parametri di stringa sicura.

Con Parameter Store è possibile creare, archiviare e gestire i dati come parametri con valori. È possibile creare un parametro in Parameter Store e utilizzarlo in più applicazioni e servizi soggetti a policy e autorizzazioni che tu stesso stabilisci. Quando è necessario modificare il valore di un parametro, è possibile modificare un'istanza piuttosto che gestire modifiche soggette a errore in numerose origini. Parameter Store supporta una struttura gerarchica per i nomi dei parametri, in modo da definire un parametro per utilizzi specifici.

Per gestire i dati sensibili, è possibile creare parametri di stringa sicura. Parameter Store utilizza AWS KMS keys per crittografare i valori di parametri dei parametri di stringa sicura quando vengono creati o modificati. Utilizza inoltre le chiavi KMS per decrittare i valori dei parametri al momento dell'accesso. Puoi utilizzare la Chiave gestita da AWS che Parameter Store crea per l'account o specificare la tua chiave gestita dal cliente.

> **Important**
>
> Parameter Store supporta solo chiavi KMS simmetriche. Non puoi utilizzare una chiave KMS asimmetrica per crittografare i parametri. Per informazioni su come determinare se una chiave KMS è simmetrica o asimmetrica, consulta Individuazione di chiavi KMS asimmetriche.

Parameter Store supporta i parametri nei livelli standard e avanzato. I parametri standard, che non possono superare i 4096 byte, sono crittografati e decrittati direttamente con la chiave KMS specificata. Per crittografare e decrittografare i parametri di stringa sicura avanzati, Parameter Store utilizza la crittografia envelope con AWS Encryption SDK. È possibile convertire un parametro di stringa sicura standard in un parametro avanzato, ma non è possibile convertire un parametro avanzato in uno standard. Per ulteriori informazioni sulla differenza tra parametri di stringa sicura standard e avanzati, consulta Informazioni sui parametri avanzati di Systems Manager nella Guida per l'utente di AWS Systems Manager.

Argomenti

Protezione dei parametri di stringa sicura standard

Parameter Store non esegue alcuna operazione di crittografia. Al contrario, si basa su AWS KMS per crittografare e decrittare i valori dei parametri di stringa sicura. Quando si crea o si modifica un valore di parametro stringa sicura standard, Parameter Store chiama l'operazione AWS KMS Encrypt. Questa operazione usa una chiave KMS di crittografia simmetrica direttamente per crittografare il valore del parametro anziché utilizzare la chiave KMS per generare una chiave dei dati.

È possibile selezionare la chiave di KMS utilizzata da Parameter Store per crittografare il valore dei parametri. Se non specifichi una chiave KMS, Parameter Store usa la Chiave gestita da AWS che Systems Manager crea automaticamente nel tuo account. Questa chiave KMS ha l'alias `aws/ssm`.

Per visualizzare la chiave `aws/ssm` KMS predefinita per il tuo account, utilizza l'DescribeKeyoperazione nell'AWS KMSAPI. L'esempio seguente utilizza il comando `describe-key` in AWS Command Line Interface (AWS CLI) con il nome di alias `aws/ssm`.

```
aws kms describe-key --key-id alias/aws/ssm
```

Per creare un parametro di stringa sicuro standard, utilizzare l'PutParameteroperazione nell'API Systems Manager. Ometti il parametro `Tier` o specifica un valore `Standard`, che è l'impostazione predefinita. Includi un parametro `Type` con un valore `SecureString`. Per specificare una chiave KMS, utilizza il parametro `KeyId`. L'impostazione predefinita è la Chiave gestita da AWS per il tuo account: `aws/ssm`.

Parameter Store quindi chiama l'operazione AWS KMS `Encrypt` con la chiave KMS e il valore del parametro in testo in chiaro. AWS KMS restituisce il valore del parametro crittografato che Parameter Store memorizza con il nome del parametro.

L'esempio seguente utilizza il comando put-parameter di Systems Manager e il relativo parametro `--type` in AWS CLI per creare un parametro di stringa sicura. Poiché il comando omette i parametri

opzionali `--tier` e `--key-id`, Parameter Store crea un parametro di stringa sicura standard e lo crittografa con la Chiave gestita da AWS.

```
aws ssm put-parameter --name MyParameter --value "secret_value" --type SecureString
```

Il seguente esempio simile utilizza il parametro `--key-id` per specificare una chiave gestita dal cliente. Nell'esempio viene utilizzato un ID chiave KMS per identificare la chiave KMS, ma è possibile utilizzare qualsiasi identificatore di chiave KMS valido. Poiché il comando omette il parametro `Tier` (`--tier`), Parameter Store crea un parametro di stringa sicura standard, non uno avanzato.

```
aws ssm put-parameter --name param1 --value "secret" --type SecureString --key-id
 1234abcd-12ab-34cd-56ef-1234567890ab
```

Quando si ottiene un parametro di stringa sicura da Parameter Store, il suo valore è crittografato. Per ottenere un parametro, utilizzare l'GetParameter operazione nell'API Systems Manager.

L'esempio seguente utilizza il comando get-parameter di Systems Manager in AWS CLI per ottenere il parametro `MyParameter` da Parameter Store senza decrittarne il valore.

```
$  aws ssm get-parameter --name MyParameter

{
    "Parameter": {
        "Type": "SecureString",
        "Name": "MyParameter",
        "Value":
 "AQECAHgnOkMROh5LaLXkA4j0+vYi6tmM17Lg/9E464VRo68cvwAAAG8wbQYJKoZIhvcNAQcGoGAwXgIBADBZBgkqhkiG9
    }
}
```

Per decrittografare il valore del parametro prima di restituirlo, imposta il parametro `WithDecryption` di `GetParameter` su `true`. Quando si utilizza `WithDecryption`, Parameter Store chiama l'operazione AWS KMS Decrypt a tuo nome per decrittare il valore del parametro. Di conseguenza, la richiesta `GetParameter` restituisce il parametro con un valore di parametro in testo normale, come mostrato nel seguente esempio.

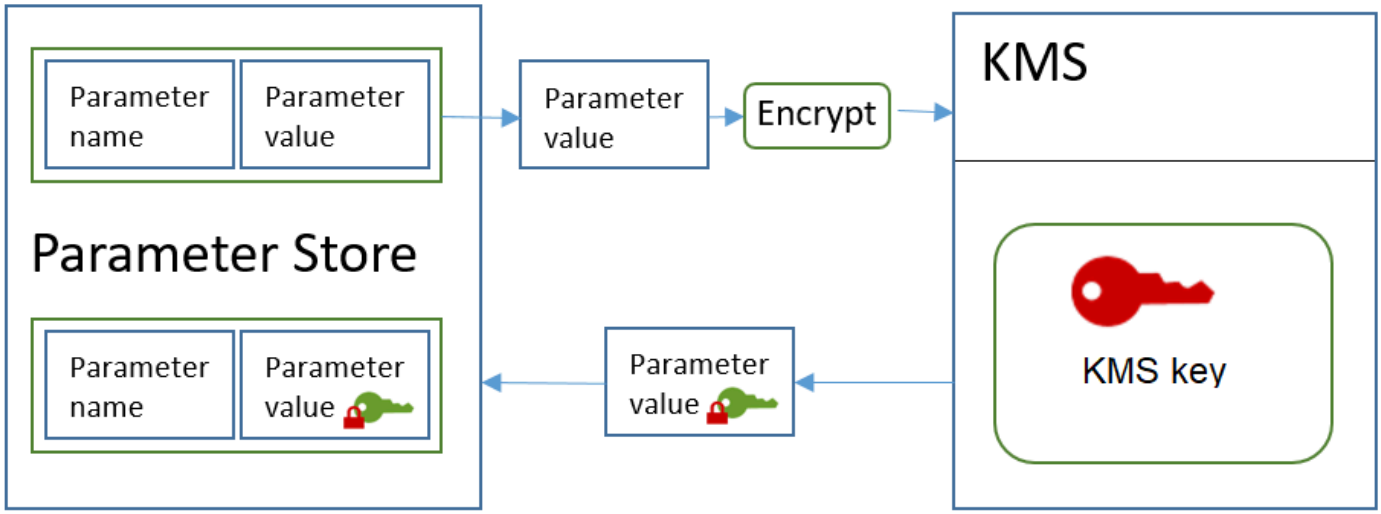
```
$  aws ssm get-parameter --name MyParameter --with-decryption

{
```

```
    "Parameter": {
        "Type": "SecureString",
        "Name": "MyParameter",
        "Value": "secret_value"
    }
}
```

Il seguente flusso di lavoro mostra il modo in cui Parameter Store utilizza una chiave KMS per crittografare e decrittare un parametro di stringa sicura standard.

Crittografare un parametro standard

1. Quando usi `PutParameter` per creare un parametro di stringa sicura, Parameter Store invia una richiesta `Encrypt` a AWS KMS. Questa richiesta include il valore del parametro in testo in chiaro, la chiave KMS scelta e il contesto di crittografia di Parameter Store. Durante la trasmissione a AWS KMS, il valore di testo non crittografato nel parametro di stringa sicura è protetto dal Transport Layer Security (TLS).
2. AWS KMS crittografa il valore del parametro con la chiave KMS specificata e il contesto di crittografia. Restituisce il testo cifrato a Parameter Store, che memorizza il nome e il valore crittografato del parametro.



Decrittografia di un parametro standard

1. Quando includi il parametro `WithDecryption` in una richiesta `GetParameter`, Parameter Store invia una richiesta `Decrypt` a AWS KMS con il valore di parametro di stringa sicura crittografato e il contesto di crittografia di Parameter Store.

2. AWS KMS usa la stessa chiave KMS e il contesto di crittografia fornito per decrittare il valore crittografato. Restituisce il valore del parametro in testo in chiaro (decrittografato) a Parameter Store. Durante la trasmissione, i dati in testo normale sono protetti da TLS.
3. Parameter Store restituisce il valore del parametro in testo in chiaro nella risposta `GetParameter`.

Protezione dei parametri di stringa sicura avanzati

Quando usi `PutParameter` per creare un parametro di stringa sicura avanzato, Parameter Store utilizza la crittografia envelope con AWS Encryption SDK e una AWS KMS key di crittografia simmetrica per proteggere il valore del parametro. Ogni valore di parametro avanzato è crittografato con una chiave di dati univoca e la chiave di dati è crittografata con una chiave KMS. Puoi utilizzare la Chiave gestita da AWS per l'account (`aws/ssm`) o qualsiasi chiave gestita dal cliente.

AWS Encryption SDK è una libreria open source lato client, che consente di crittografare e decrittografare i dati utilizzando gli standard di settore e le best practice. È supportata su più piattaforme e in più linguaggi di programmazione, compresa un'interfaccia a riga di comando. È possibile visualizzare il codice sorgente e contribuire al suo sviluppo in GitHub.

Per ogni valore di parametro di stringa sicura, Parameter Store chiama AWS Encryption SDK per crittografare il valore del parametro utilizzando una chiave dati univoca che AWS KMS genera (GenerateDataKey). AWS Encryption SDK restituisce a Parameter Store un messaggio crittografato che include il valore di parametro crittografato e una copia crittografata della chiave di dati univoca. Parameter Store archivia l'intero messaggio crittografato nel valore del parametro stringa sicura. Quindi, quando ottieni un valore di parametro di stringa sicura avanzato, Parameter Store usa AWS Encryption SDK per decrittarne il valore di parametro. Ciò richiede una chiamata a AWS KMS per decrittografare la chiave di dati crittografata.

Per creare un parametro di stringa sicuro avanzato, utilizzare l'PutParameteroperazione nell'API Systems Manager. Imposta il valore del parametro `Tier` su `Advanced`. Includi un parametro `Type` con un valore `SecureString`. Per specificare una chiave KMS, utilizza il parametro `KeyId`. L'impostazione predefinita è la Chiave gestita da AWS per il tuo account: `aws/ssm`.

```
aws ssm put-parameter --name MyParameter --value "secret_value" --type SecureString --
tier Advanced
```

Il seguente esempio simile utilizza il parametro `--key-id` per specificare una chiave gestita dal cliente. Questo esempio utilizza l'Amazon Resource Name (ARN) della chiave KMS, ma puoi usare qualunque identificatore di chiave KMS valido.

```
aws ssm put-parameter --name MyParameter --value "secret_value"
 --type SecureString --tier Advanced --key-id arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Quando si ottiene un parametro di stringa sicura da Parameter Store, il valore è il messaggio crittografato che AWS Encryption SDK ha restituito. Per ottenere un parametro, utilizzare l'GetParameter operazione nell'API Systems Manager.

L'esempio seguente utilizza l'operazione `GetParameter` di Systems Manager per ottenere il parametro `MyParameter` da Parameter Store senza decrittarne il valore.

```
$  aws ssm get-parameter --name MyParameter

{
    "Parameter": {
        "Type": "SecureString",
        "Name": "MyParameter",
        "Value":
 "AQECAHgnOkMROh5LaLXkA4j0+vYi6tmM17Lg/9E464VRo68cvwAAAG8wbQYJKoZIhvcNAQcGoGAwXgIBADBZBgkqhkiG9
    }
}
```

Per decrittografare il valore del parametro prima di restituirlo, imposta il parametro `WithDecryption` di `GetParameter` su `true`. Quando si utilizza `WithDecryption`, Parameter Store chiama l'operazione AWS KMS Decrypt a tuo nome per decrittare il valore del parametro. Di conseguenza, la richiesta `GetParameter` restituisce il parametro con un valore di parametro in testo normale, come mostrato nel seguente esempio.

```
$  aws ssm get-parameter --name MyParameter --with-decryption

{
    "Parameter": {
        "Type": "SecureString",
        "Name": "MyParameter",
        "Value": "secret_value"
    }
}
```

Non è possibile convertire un parametro di stringa sicura avanzato in uno standard, ma è possibile convertire un parametro di stringa sicura standard in uno avanzato. Per convertire un parametro

di stringa sicura standard in uno avanzato, utilizza l'operazione `PutParameter` con il parametro `Overwrite`. `Type` deve essere `SecureString` e il valore `Tier` deve essere `Advanced`. Il parametro `KeyId` che identifica una chiave gestita dal cliente è facoltativo. Se si omette, Parameter Store utilizza la Chiave gestita da AWS per l'account. Puoi specificare qualsiasi chiave KMS che il principale è autorizzato a utilizzare, anche se è stata utilizzata un'altra chiave KMS per crittografare il parametro standard.

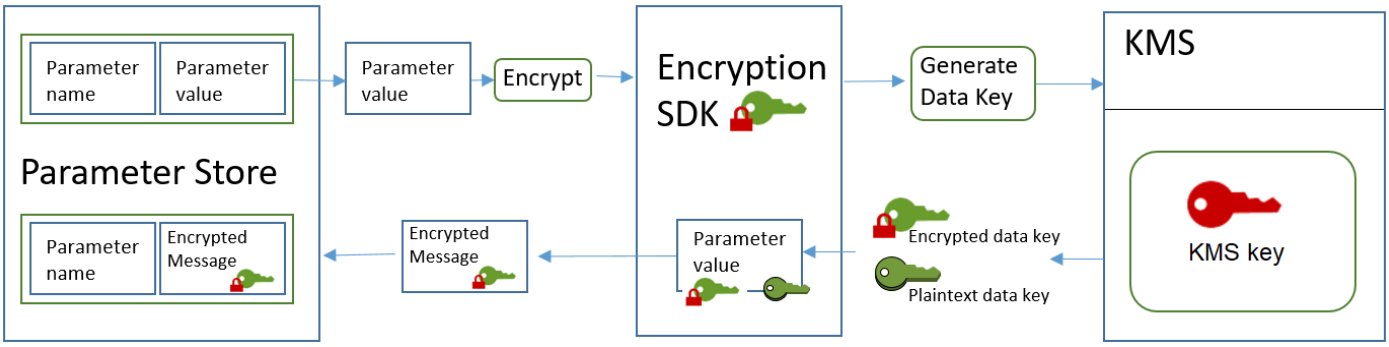
Quando si utilizza il parametro `Overwrite`, Parameter Store utilizza AWS Encryption SDK per crittografare il valore del parametro. Quindi memorizza il nuovo messaggio crittografato in Parameter Store.

```
$ aws ssm put-parameter --name myStdParameter --value "secret_value"  --type
 SecureString --tier Advanced --key-id 1234abcd-12ab-34cd-56ef-1234567890ab --overwrite
```

Il seguente flusso di lavoro mostra il modo in cui Parameter Store utilizza una chiave KMS per crittografare e decrittare un parametro di stringa sicura avanzato.

Crittografare un parametro avanzato

1. Quando usi `PutParameter` per creare un parametro di stringa sicura avanzato, Parameter Store utilizza AWS Encryption SDK e AWS KMS per crittografare il valore del parametro. Parameter Store chiama AWS Encryption SDK con il valore del parametro, la chiave KMS specificata e il contesto di crittografia di Parameter Store.
2. AWS Encryption SDKinvia una GenerateDataKeyrichiesta a AWS KMS con l'identificatore della chiave KMS specificata e il contesto di crittografia Parameter Store. AWS KMSrestituisce due copie della chiave dati univoca: una in testo semplice e una crittografata con la chiave KMS. Il contesto di crittografia viene utilizzato per crittografare la chiave di dati.
3. AWS Encryption SDK utilizza la chiave di dati in testo normale per crittografare il valore del parametro. Restituisce un messaggio crittografato che include il valore di parametro crittografato, la chiave di dati crittografata e altri dati, tra cui il contesto di crittografia di Parameter Store.
4. Parameter Store archivia il messaggio crittografato come valore del parametro.



Decrittografare un parametro avanzato

1. È possibile includere il parametro `WithDecryption` in una richiesta `GetParameter` per ottenere un parametro di stringa sicura avanzato. In questo caso, Parameter Store trasmette il messaggio crittografato dal valore di parametro a un metodo di decrittografia dell'AWS Encryption SDK.
2. AWS Encryption SDK chiama l'operazione KMS AWS KMS Decrypt. Trasferisce la chiave di dati crittografata e il contesto di crittografia di Parameter Store dal messaggio crittografato.
3. AWS KMS utilizza la chiave KMS e il contesto di crittografia di Parameter Store per decrittare la chiave di dati crittografata. Quindi restituisce la chiave di dati in testo normale (decrittografato) a AWS Encryption SDK.
4. AWS Encryption SDK utilizza la chiave di dati in testo normale per decrittografare il valore di parametro. Restituisce il valore del parametro in testo in chiaro a Parameter Store.
5. Parameter Store verifica il contesto di crittografia e restituisce il valore del parametro in testo in chiaro nella risposta `GetParameter`.

Impostazione delle autorizzazioni per crittografare e decrittografare i valori dei parametri

Per crittografare un valore di parametro di stringa sicura standard, l'utente necessita dell'autorizzazione `kms:Encrypt`. Per crittografare un valore di parametro di stringa sicura avanzato, l'utente necessita dell'autorizzazione `kms:GenerateDataKey`. Per decrittografare entrambi i tipi di valori di parametri di stringa sicura, l'utente necessita dell'autorizzazione `kms:Decrypt`.

È possibile usare le policy IAM per consentire o negare le autorizzazioni a un utente per chiamare le operazioni `PutParameter` e `GetParameter` di Systems Manager.

Inoltre, se si utilizzano chiavi gestite dal cliente per crittografare i valori dei parametri di stringa sicura, puoi utilizzare le policy IAM e le policy delle chiavi per gestire le autorizzazioni di crittografia e decrittazione. Tuttavia, non puoi definire policy di controllo degli accessi per la chiave KMS `aws/ssm` predefinita. Per ulteriori informazioni sul controllo degli accessi alle chiavi gestite dal cliente, consulta Autenticazione e controllo degli accessi per AWS KMS.

L'esempio seguente mostra una policy IAM progettata per parametri di stringa sicura standard. Questa consente all'utente di chiamare l'operazione `PutParameter` di Systems Manager su tutti i parametri nel percorso `FinancialParameters`. La policy, inoltre, consente all'utente di chiamare l'operazione AWS KMS `Encrypt` su una chiave gestita dal cliente di esempio.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:PutParameter"
            ],
            "Resource": "arn:aws:ssm:us-west-2:111122223333:parameter/
FinancialParameters/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt"
            ],
            "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ]
}
```

L'esempio seguente mostra una policy IAM progettata per parametri di stringa sicura avanzati. Questa consente all'utente di chiamare l'operazione `PutParameter` di Systems Manager su tutti i parametri nel percorso `ReservedParameters`. La policy, inoltre, consente all'utente di chiamare l'operazione AWS KMS `GenerateDataKey` su una chiave gestita dal cliente di esempio.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": [
                "ssm:PutParameter"
            ],
            "Resource": "arn:aws:ssm:us-west-2:111122223333:parameter/
ReservedParameters/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ]
}
```

L'esempio finale mostra anche una policy IAM che può essere utilizzata per parametri di stringa sicura standard o avanzati. Questa consente all'utente di chiamare le operazioni `GetParameter` di Systems Manager (e le operazioni correlate) su tutti i parametri nel percorso `ITParameters`. La policy, inoltre, consente all'utente di chiamare l'operazione AWS KMS `Decrypt` su una chiave gestita dal cliente di esempio.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetParameter*"
            ],
            "Resource": "arn:aws:ssm:us-west-2:111122223333:parameter/ITParameters/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
```

```
    ]
}
```

Contesto di crittografia di Parameter Store

Un contesto di crittografia è un set di coppie chiave-valore che contiene dati arbitrari non segreti. Quando includi un contesto di crittografia in una richiesta di crittografia dei dati, AWS KMS lega il contesto di crittografia ai dati crittografati, in modo che lo stesso contesto di crittografia sia necessario per decrittografare i dati.

È inoltre possibile utilizzare il contesto di crittografia per identificare un'operazione di crittografia nei record e nei log di controllo. Il contesto di crittografia viene visualizzato in testo normale nei log, ad esempio nei log di AWS CloudTrail.

Anche AWS Encryption SDK richiede un contesto di crittografia, sebbene lo gestisca in modo diverso. Parameter Store fornisce il contesto di crittografia al metodo di crittografia. AWS Encryption SDK associa crittograficamente il contesto di crittografia ai dati crittografati. Include il contesto di crittografia in testo normale nell'intestazione del messaggio crittografato restituito. Tuttavia, a differenza di AWS KMS, i metodi di decrittografia di AWS Encryption SDK non prendono un contesto di crittografia come input. Invece, quando decritta i dati, AWS Encryption SDK ottiene il contesto di crittografia dal messaggio crittografato. Parameter Store verifica che il contesto di crittografia includa il valore atteso prima di restituire il valore del parametro in testo in chiaro.

Parameter Store usa il seguente contesto di crittografia in tutte le operazioni di crittografia:

- Chiave: `PARAMETER_ARN`
- Valore: l'ARN (Amazon Resource Name) del parametro crittografato.

Il formato del contesto di crittografia è il seguente:

```
"PARAMETER_ARN":"arn:aws:ssm:<REGION_NAME>:<ACCOUNT_ID>:parameter/<parameter-name>"
```

Ad esempio, Parameter Store include questo contesto di crittografia nelle chiamate per crittografare e decrittografare il parametro `MyParameter` in un Account AWS e in una regione di esempio.

```
"PARAMETER_ARN":"arn:aws:ssm:us-west-2:111122223333:parameter/MyParameter"
```

Se il parametro è in un percorso gerarchico di Parameter Store, il nome e il percorso sono inclusi nel contesto di crittografia. Ad esempio, questo contesto di crittografia viene utilizzato per crittografare e

decrittare il parametro `MyParameter` nel percorso `/ReadableParameters` in un Account AWS e in una regione di esempio.

```
"PARAMETER_ARN":"arn:aws:ssm:us-west-2:111122223333:parameter/ReadableParameters/
MyParameter"
```

È possibile decrittografare un valore di parametro di stringa sicura crittografato richiamando l'operazione AWS KMS `Decrypt` con il corretto contesto di crittografia e il valore del parametro crittografato che l'operazione `GetParameter` di Systems Manager restituisce. Tuttavia, consigliamo di decrittare i valori del parametro `GetParameter` di Parameter Store usando l'operazione con il parametro `WithDecryption`.

Puoi anche includere il contesto di crittografia nella policy IAM. Ad esempio, è possibile consentire a un utente di decrittografare solo un determinato valore di parametro o un set di valori di parametri.

La seguente istruzione di esempio della policy IAM consente all'utente di ottenere il valore del parametro `MyParameter` e di decrittarne il valore utilizzando la chiave KMS specificata. Tuttavia le autorizzazioni si applicano solo quando il contesto di crittografia corrisponde alla stringa specificata. Queste autorizzazioni non si applicano a qualsiasi altro parametro o chiave KMS e la chiamata a `GetParameter` ha esito negativo se il contesto di crittografia non corrisponde alla stringa.

Prima di usare un'istruzione di policy simile a questa, sostituisci l'ARN di esempio con valori validi.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetParameter*"
            ],
            "Resource": "arn:aws:ssm:us-west-2:111122223333:parameter/MyParameter"
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "Condition": {
                "StringEquals": {
```

```
                    "kms:EncryptionContext:PARAMETER_ARN":"arn:aws:ssm:us-
west-2:111122223333:parameter/MyParameter"
                }
            }
        }
    ]
}
```

Risoluzione dei problemi delle chiavi KMS in Parameter Store

Per eseguire qualsiasi operazione su un parametro di stringa sicura, Parameter Store deve essere in grado di utilizzare la chiave KMS AWS KMS specificata per l'operazione. La maggior parte degli errori di Parameter Store relativi alle chiavi KMS sono causati da uno dei seguenti motivi:

- Le credenziali utilizzate da un'applicazione non hanno l'autorizzazione per eseguire l'operazione specificata sulla chiave KMS.

  Per risolvere questo errore, eseguire l'applicazione con credenziali differenti o modificare la policy IAM o della chiave che impedisce l'operazione. Per aiuto con le policy IAM e delle chiavi AWS KMS, consulta Autenticazione e controllo degli accessi per AWS KMS.
- La chiave KMS non è stata trovata.

  In genere questo accade quando si utilizza un identificatore errato per la chiave KMS. Trova gli identificatori corretti per la chiave KMS e riprova il comando.
- La chiave KMS non è abilitata. Quando ciò si verifica, Parameter Store restituisce un'InvalidKeyIdeccezione con un messaggio di errore dettagliato da. AWS KMS Se lo stato della chiave KMS è `Disabled`, abilitalo. Se è `Pending Import`, completa la procedura di importazione. Se lo stato di chiave è `Pending Deletion`, annulla l'eliminazione della chiave o utilizza un'altra chiave KMS.

  Per trovare lo stato di chiave di una chiave KMS nella console AWS KMS, nella pagina Chiavi gestite cliente o Chiavi gestite da AWS, consulta la colonna Stato. Per utilizzare l'AWS KMSAPI per trovare lo stato di una chiave KMS, utilizza l'DescribeKeyoperazione.

Come WorkMail utilizza Amazon AWS KMS

Questo argomento illustra in che modo Amazon WorkMail utilizza AWS KMS per crittografare i messaggi di posta elettronica.

Argomenti

WorkMail Panoramica di Amazon

Amazon WorkMail è un servizio di posta elettronica e calendario aziendale sicuro e gestito con supporto per client di posta elettronica desktop e mobili esistenti. Puoi creare un' WorkMail organizzazione Amazon e assegnarle uno o più domini e-mail di tua proprietà. Quindi è possibile creare caselle di posta per gli utenti e-mail e i gruppi di distribuzione dell'organizzazione.

Amazon crittografa in WorkMail modo trasparente tutti i messaggi nelle caselle di posta di tutte le WorkMail organizzazioni Amazon prima che i messaggi vengano scritti su disco e decrittografa in modo trasparente i messaggi quando gli utenti vi accedono. Non è possibile disabilitare la crittografia. Per proteggere le chiavi di crittografia che proteggono i messaggi, Amazon WorkMail è integrato con AWS Key Management Service (AWS KMS).

Amazon offre WorkMail anche un'opzione per consentire agli utenti di inviare e-mail firmate o crittografate. Questa caratteristica di crittografia non utilizza AWS KMS.

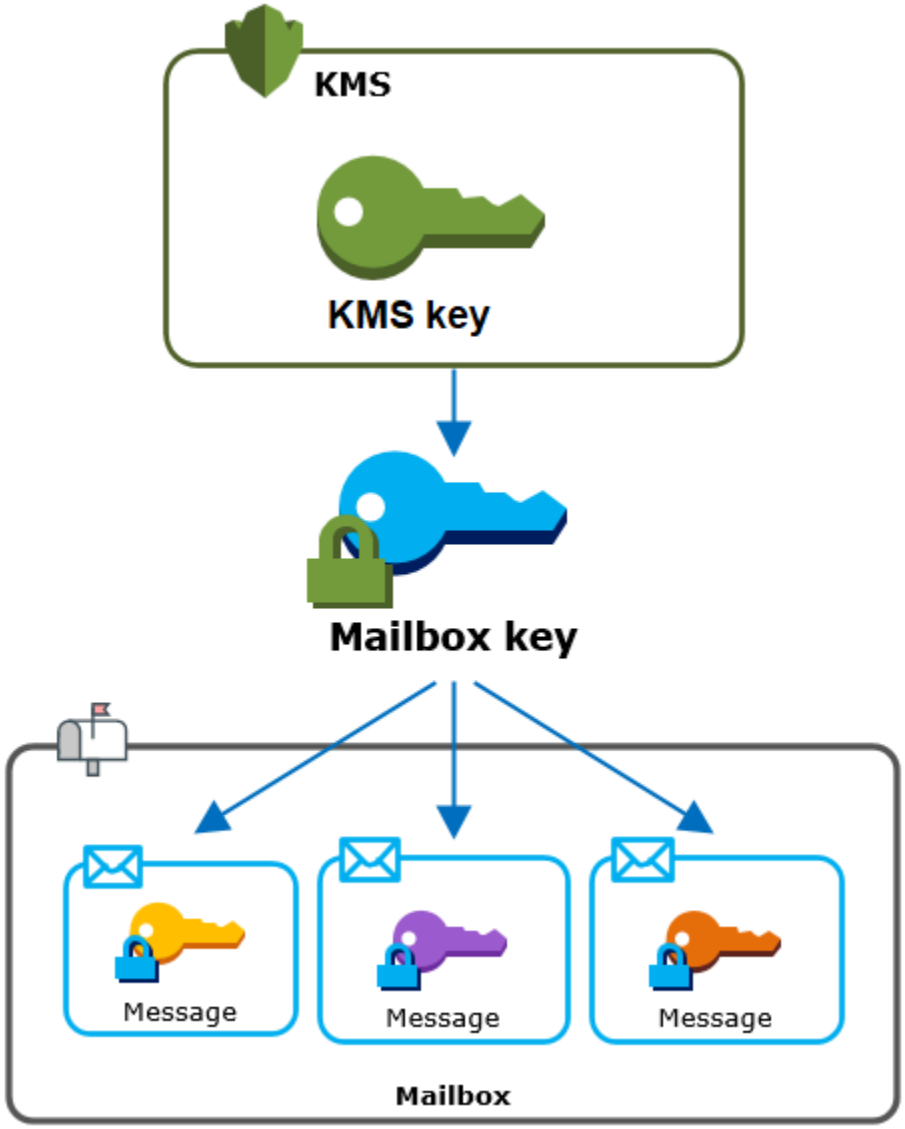
WorkMail Crittografia Amazon

In Amazon WorkMail, ogni organizzazione può contenere più caselle di posta, una per ogni utente dell'organizzazione. Tutti i messaggi, inclusi gli elementi di calendario ed e-mail, vengono archiviati nella casella di posta dell'utente.

Per proteggere il contenuto delle caselle di posta nelle tue WorkMail organizzazioni Amazon, Amazon WorkMail crittografa tutti i messaggi delle caselle di posta prima che vengano scritti su disco. Nessuna informazione fornita dai clienti viene archiviata in testo non crittografato.

Ogni messaggio viene crittografato con una chiave di crittografia dei dati univoca. La chiave del messaggio è protetta da una chiave della casella di posta, che è una chiave di crittografia univoca che viene utilizzata solo per quella casella. La chiave della casella di posta viene crittografata con una AWS KMS key per l'organizzazione che non lascia mai AWS KMS non crittografato. Il seguente

diagramma mostra la relazione dei messaggi crittografati, le chiavi dei messaggi crittografati, la chiave della casella di posta crittografata e la chiave KMS per l'organizzazione in AWS KMS.



Una chiave KMS per l'organizzazione

Quando crei un' WorkMail organizzazione Amazon, puoi selezionarne una AWS KMS key per l'organizzazione. Questa chiave KMS protegge tutte le chiavi delle caselle di posta in quell'organizzazione.

Se utilizzi la procedura di configurazione rapida per creare la tua organizzazione, Amazon WorkMail utilizza Chiave gestita da AWSfor Amazon WorkMail (`aws/workmail`) nella tuaAccount AWS. Se utilizzi la configurazione standard, puoi selezionare la chiave Chiave gestita da AWS per Amazon WorkMail o una chiave gestita dal cliente che possiedi e gestisci. Puoi selezionare la stessa chiave

KMS o una chiave KMS diversa per ognuna delle organizzazioni, ma non puoi modificare la chiave KMS una volta selezionata.

> **Important**
>
> Amazon WorkMail supporta solo chiavi KMS con crittografia simmetrica. Non puoi utilizzare una chiave KMS asimmetrica per crittografare i dati in Amazon. WorkMail Per informazioni su come determinare se una chiave KMS è simmetrica o asimmetrica, consulta Individuazione di chiavi KMS asimmetriche.

Per trovare la chiave KMS per la tua organizzazione, usa la voce di log AWS CloudTrail che registra le chiamate a AWS KMS.

Una chiave di crittografia univoca per ogni casella di posta

Quando crei una nuova casella di posta, Amazon WorkMail genera una chiave di crittografia simmetrica Advanced Encryption Standard (AES) unica a 256 bit per la casella di posta, nota come chiave della casella di posta, all'esterno di. AWS KMS Amazon WorkMail utilizza la chiave della casella di posta per proteggere le chiavi di crittografia per ogni messaggio nella casella di posta.

Per proteggere la chiave della casella di posta, Amazon WorkMail chiede di AWS KMS crittografare la chiave della casella di posta sotto la chiave KMS dell'organizzazione. Quindi archivia la chiave della casella di posta crittografata nei metadati della casella.

> **Note**
>
> Amazon WorkMail utilizza una chiave di crittografia simmetrica delle caselle di posta per proteggere le chiavi dei messaggi. In precedenza, Amazon WorkMail proteggeva ogni casella di posta con una coppia di chiavi asimmetrica. Usava la chiave pubblica per crittografare ogni chiave di messaggio e la chiave privata per decrittografarla. La chiave della casella di posta privata era protetta dalla chiave KMS per l'organizzazione. Le caselle di posta esistenti possono comunque utilizzare una coppia di chiavi di casella asimmetrica. Questa modifica non influisce sulla sicurezza della casellla di posta o dei messaggi.

Una chiave di crittografia univoca per ogni messaggio

Quando un messaggio viene aggiunto alla casella di posta, Amazon WorkMail genera una chiave di crittografia simmetrica AES a 256 bit unica per il messaggio esterno. AWS KMS Usa questa chiave del messaggio per crittografare il messaggio. Amazon WorkMail crittografa la chiave del messaggio sotto la chiave della casella di posta e archivia la chiave del messaggio crittografato con il messaggio. Quindi, crittografa la chiave della casella di posta con la chiave KMS per l'organizzazione.

Creazione di una nuova casella di posta

Quando Amazon WorkMail crea una nuova casella di posta, utilizza il seguente processo per preparare la cassetta postale a contenere messaggi crittografati.

- Amazon WorkMail genera un'esclusiva chiave di crittografia simmetrica AES a 256 bit per la casella di posta esterna. AWS KMS
- Amazon WorkMail chiama l'operazione AWS KMS Encrypt. Trasferisce la chiave della casella di posta e l'identificatore della AWS KMS key per l'organizzazione. AWS KMS restituisce un testo cifrato della chiave della casella crittografata con la chiave KMS.
- Amazon WorkMail archivia la chiave crittografata della casella di posta con i metadati della casella di posta.

Crittografia di un messaggio di casella di posta

Per crittografare un messaggio, Amazon WorkMail utilizza il seguente processo.

1. Amazon WorkMail genera una chiave simmetrica AES unica a 256 bit per il messaggio. Utilizza la chiave del messaggio in testo normale e l'algoritmo Advanced Encryption Standard (AES) per crittografare il messaggio al di fuori di AWS KMS.
2. Per proteggere la chiave del messaggio contenuta nella chiave della casella di posta, Amazon WorkMail deve decrittografare la chiave della casella di posta, che viene sempre archiviata in forma crittografata.

   Amazon WorkMail chiama l'operazione AWS KMS Decrypt e inserisce la chiave della casella di posta crittografata. AWS KMSutilizza la chiave KMS per l'organizzazione per decrittografare la chiave della casella di posta e restituisce la chiave della casella di posta in testo semplice ad Amazon. WorkMail
3. Amazon WorkMail utilizza la chiave della casella di posta in chiaro e l'algoritmo Advanced Encryption Standard (AES) per crittografare la chiave del messaggio all'esterno di. AWS KMS

4. Amazon WorkMail memorizza la chiave del messaggio crittografato nei metadati del messaggio crittografato in modo che sia disponibile per la decrittografia.

Decrittografia di un messaggio di casella di posta

Per decrittografare un messaggio, Amazon WorkMail utilizza il seguente processo.

1. Amazon WorkMail chiama l'operazione AWS KMS Decrypt e inserisce la chiave della casella di posta crittografata. AWS KMSutilizza la chiave KMS per l'organizzazione per decrittografare la chiave della casella di posta e restituisce la chiave della casella di posta in testo semplice ad Amazon. WorkMail
2. Amazon WorkMail utilizza la chiave della casella di posta in testo semplice e l'algoritmo Advanced Encryption Standard (AES) per decrittografare la chiave del messaggio crittografato all'esterno di. AWS KMS
3. Amazon WorkMail utilizza la chiave del messaggio in testo semplice per decrittografare il messaggio crittografato.

Memorizzazione delle chiavi delle caselle di posta

Per migliorare le prestazioni e ridurre al minimo le chiamate aAWS KMS, Amazon WorkMail memorizza nella cache ogni chiave della casella di posta in testo semplice per ogni client localmente per un massimo di un minuto. Al termine del periodo di memorizzazione, la chiave della casella di posta viene rimossa. Se la chiave della casella di posta per quel client è richiesta durante il periodo di memorizzazione nella cache, Amazon WorkMail può recuperarla dalla cache anziché chiamare. AWS KMS La chiave è protetta nella cache e non viene mai scritta su disco in testo non crittografato.

Autorizzazione dell'utilizzo della chiave KMS

Quando Amazon WorkMail utilizza un AWS KMS key nelle operazioni crittografiche, agisce per conto dell'amministratore della casella di posta.

Per utilizzare la AWS KMS key per un segreto per tuo conto, l'amministratore deve disporre delle autorizzazioni seguenti. È possibile specificare queste autorizzazioni necessarie in una policy IAM o delle chiavi.

- `kms:Encrypt`
- `kms:Decrypt`

- `kms:CreateGrant`

Per consentire l'utilizzo della chiave KMS solo per le richieste che provengono da Amazon WorkMail, puoi utilizzare la chiave kms: ViaService condition con il `workmail.<region>.amazonaws.com` valore.

Puoi inoltre utilizzare le chiavi o i valori nel contesto di crittografia come condizione per utilizzare la chiave KMS per le operazioni di crittografia. Ad esempio, è possibile utilizzare un operatore di condizione stringa in un documento di policy IAM o delle chiavi oppure utilizzare un vincolo di concessione in una concessione.

Policy della chiave per Chiave gestita da AWS

La politica chiave Chiave gestita da AWS per Amazon WorkMail consente agli utenti di utilizzare la chiave KMS per operazioni specifiche solo quando Amazon WorkMail effettua la richiesta per conto dell'utente. La policy delle chiavi non consente ad alcun utente di utilizzare la chiave KMS direttamente.

Questa policy delle chiavi, come le policy di tutte le Chiavi gestite da AWS, viene stabilita dal servizio. Non è possibile modificarla, ma è possibile visualizzarla in qualsiasi momento. Per informazioni dettagliate, vedi Visualizzazione di una policy di chiave.

Le istruzioni di policy nella policy delle chiavi hanno l'effetto seguente:

- Consenti agli utenti dell'account e della regione di utilizzare la chiave KMS per operazioni crittografiche e creare concessioni, ma solo quando la richiesta proviene da Amazon per loro WorkMail conto. La chiave di condizione `kms:ViaService` applica questa limitazione.
- Consente all'account Account AWS di creare policy IAM che consentono agli utenti di visualizzare le proprietà della chiave KMS e revocare le autorizzazioni.

Di seguito è riportata una politica chiave per un esempio Chiave gestita da AWS per Amazon WorkMail.

```
{
  "Version" : "2012-10-17",
  "Id" : "auto-workmail-1",
  "Statement" : [ {
    "Sid" : "Allow access through WorkMail for all principals in the account that are
 authorized to use WorkMail",
```

```
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "*"
    },
    "Action" : [ "kms:Decrypt", "kms:CreateGrant", "kms:ReEncrypt*", "kms:DescribeKey",
 "kms:Encrypt" ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "kms:ViaService" : "workmail.us-east-1.amazonaws.com",
        "kms:CallerAccount" : "111122223333"
      }
    }
  }, {
    "Sid" : "Allow direct access to key metadata to the account",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "arn:aws:iam::111122223333:root"
    },
    "Action" : [ "kms:Describe*", "kms:List*", "kms:Get*", "kms:RevokeGrant" ],
    "Resource" : "*"
  } ]
}
```

Utilizzo delle sovvenzioni per autorizzare Amazon WorkMail

Oltre alle politiche chiave, Amazon WorkMail utilizza le sovvenzioni per aggiungere autorizzazioni alla chiave KMS per ogni organizzazione. Per visualizzare le sovvenzioni sulla chiave KMS nel tuo account, utilizza l'operazione. ListGrants

Amazon WorkMail utilizza le sovvenzioni per aggiungere le seguenti autorizzazioni alla chiave KMS dell'organizzazione.

- Aggiungi l'`kms:Encrypt`autorizzazione per consentire ad Amazon di WorkMail crittografare la chiave della casella di posta.
- Aggiungi l'`kms:Decrypt`autorizzazione per consentire ad Amazon di WorkMail utilizzare la chiave KMS per decrittografare la chiave della casella di posta. Amazon WorkMail richiede questa autorizzazione in una concessione perché la richiesta di lettura dei messaggi della casella di posta utilizza il contesto di sicurezza dell'utente che sta leggendo il messaggio. La richiesta non utilizza le credenziali diAccount AWS. Amazon WorkMail crea questa concessione quando selezioni una chiave KMS per l'organizzazione.

Per creare le sovvenzioni, Amazon WorkMail chiama per CreateGrantconto dell'utente che ha creato l'organizzazione. L'autorizzazione a creare la concessione proviene dalla policy delle chiavi. Questa politica consente agli utenti dell'account di richiamare `CreateGrant` la chiave KMS dell'organizzazione quando Amazon WorkMail effettua la richiesta per conto di un utente autorizzato.

La policy delle chiavi, inoltre, consente all'account root di revocare la concessione sulla chiave gestita da Chiave gestita da AWS. Tuttavia, se revochi la concessione, Amazon WorkMail non può decrittografare i dati crittografati nelle tue caselle di posta.

Contesto WorkMail di crittografia Amazon

Un contesto di crittografia è un set di coppie chiave-valore che contiene dati arbitrari non segreti. Quando includi un contesto di crittografia in una richiesta di crittografia dei dati, AWS KMS lega il contesto di crittografia ai dati crittografati, in modo che lo stesso contesto di crittografia sia necessario per decrittografare i dati.

Amazon WorkMail utilizza lo stesso formato di contesto di crittografia in tutte le operazioni AWS KMS crittografiche. È possibile utilizzare il contesto di crittografia per identificare un'operazione di crittografia in record e log di audit, ad esempio AWS CloudTrail, nonché come una condizione per l'autorizzazione in policy e concessioni.

Nelle sue richieste Encrypt and Decrypt a, AWS KMS Amazon WorkMail utilizza un contesto di crittografia in cui la chiave `aws:workmail:arn` e il valore è l'Amazon Resource Name (ARN) dell'organizzazione.

```
"aws:workmail:arn":"arn:aws:workmail:region:account ID:organization/organization ID"
```

Ad esempio, il seguente contesto di crittografia include un esempio di ARN di organizzazione nella regione Stati Uniti orientali (Ohio) (`us-east-2`).

```
"aws:workmail:arn":"arn:aws:workmail:us-east-2:111122223333:organization/
m-68755160c4cb4e29a2b2f8fb58f359d7"
```

Monitoraggio WorkMail dell'interazione di Amazon con AWS KMS

Puoi utilizzare AWS CloudTrail Amazon CloudWatch Logs per tenere traccia delle richieste a cui Amazon WorkMail invia per tuo AWS KMS conto.

Crittografa

Quando crei una nuova casella di posta, Amazon WorkMail genera una chiave della casella di posta e chiama AWS KMS per crittografare la chiave della casella di posta. Amazon WorkMail invia una richiesta Encrypt a AWS KMS con la chiave della casella di posta in testo semplice e un identificatore per la chiave KMS dell'organizzazione Amazon. WorkMail

L'evento che registra l'operazione `Encrypt` è simile a quello del seguente evento di esempio. L'utente è il WorkMail servizio Amazon. I parametri includono l'ID della chiave KMS (`keyId`) e il contesto di crittografia per l' WorkMail organizzazione Amazon. Amazon WorkMail inserisce anche la chiave della casella di posta, ma questa non viene registrata nel CloudTrail registro.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "workmail.eu-west-1.amazonaws.com"
    },
    "eventTime": "2019-02-19T10:01:09Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Encrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "workmail.eu-west-1.amazonaws.com",
    "userAgent": "workmail.eu-west-1.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:workmail:arn": "arn:aws:workmail:eu-west-1:111122223333:organization/
m-c6981ff7642446fa8772ba99c690e455"
        },
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d"
    },
    "responseElements": null,
    "requestID": "76e96b96-7e24-4faf-a2d6-08ded2eaf63c",
    "eventID": "d5a59c18-128a-4082-aa5b-729f7734626a",
    "readOnly": true,
    "resources": [
        {
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d",
            "accountId": "111122223333",
            "type": "AWS::KMS::Key"
```

```
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333",
    "sharedEventID": "d08e60f1-097e-4a00-b7e9-10bc3872d50c"
}
```

Decrypt

Quando aggiungi, visualizzi o elimini un messaggio della casella di posta, Amazon WorkMail chiede di decrittografare la AWS KMS chiave della casella di posta. Amazon WorkMail invia una richiesta Decrypt a AWS KMS con la chiave della casella di posta crittografata e un identificatore per la chiave KMS dell'organizzazione Amazon. WorkMail

L'evento che registra l'operazione `Decrypt` è simile a quello del seguente evento di esempio. L'utente è il WorkMail servizio Amazon. I parametri includono la chiave della casella di posta crittografata (come blob di testo cifrato), che non è registrata nel registro, e il contesto di crittografia per l'organizzazione Amazon. WorkMail AWS KMSricava l'ID della chiave KMS dal testo cifrato.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "workmail.eu-west-1.amazonaws.com"
    },
    "eventTime": "2019-02-20T11:51:10Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "workmail.eu-west-1.amazonaws.com",
    "userAgent": "workmail.eu-west-1.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:workmail:arn": "arn:aws:workmail:eu-west-1:111122223333:organization/
m-c6981ff7642446fa8772ba99c690e455"
        }
    },
    "responseElements": null,
    "requestID": "4a32dda1-34d9-4100-9718-674b8e0782c9",
    "eventID": "ea9fd966-98e9-4b7b-b377-6e5a397a71de",
    "readOnly": true,
    "resources": [
```

```
        {
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d",
            "accountId": "111122223333",
            "type": "AWS::KMS::Key"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333",
    "sharedEventID": "241e1e5b-ff64-427a-a5b3-7949164d0214"
}
```

Come si WorkSpaces usa AWS KMS

Puoi utilizzarlo WorkSpacesper fornire un desktop basato sul cloud (a WorkSpace) per ciascuno dei tuoi utenti finali. Quando ne avvii uno nuovo WorkSpace, puoi scegliere di crittografarne i volumi e decidere quali utilizzare AWS KMS keyper la crittografia. Puoi scegliere la chiave Chiave gestita da AWSfor WorkSpaces (aws/workspaces) o una chiave simmetrica gestita dal cliente.

> **Important**
>
> WorkSpaces supporta solo chiavi KMS con crittografia simmetrica. Non è possibile utilizzare una chiave KMS asimmetrica per crittografare i volumi in un. WorkSpaces Per informazioni su come determinare se una è simmetrica o asimmetrica, consulta Individuazione di chiavi KMS asimmetriche.

Per ulteriori informazioni sulla creazione WorkSpaces con volumi crittografati, consulta Encrypt a WorkSpace nella Amazon WorkSpaces Administration Guide.

Argomenti

- Panoramica sull'utilizzo della WorkSpaces crittografia AWS KMS
- WorkSpaces contesto di crittografia
- WorkSpaces Autorizzazione all'uso di una chiave KMS per conto dell'utente

Panoramica sull'utilizzo della WorkSpaces crittografia AWS KMS

Quando crei WorkSpaces con volumi crittografati, WorkSpaces utilizza Amazon Elastic Block Store (Amazon EBS) per creare e gestire tali volumi. Entrambi i servizi utilizzano AWS KMS key per usare i volumi crittografati. Per ulteriori informazioni sulla crittografia dei volumi EBS, consulta la seguente documentazione:

- Come Amazon Elastic Block Store (Amazon EBS) usa AWS KMS in questa guida
- Crittografia Amazon EBS nella Guida per l'utente di Amazon EC2 per le istanze Windows

Quando si avvia WorkSpaces con volumi crittografati, il end-to-end processo funziona in questo modo:

1. È necessario specificare la chiave KMS da utilizzare per la crittografia, nonché l' WorkSpaceutente e la directory. Questa azione crea una concessione che consente di WorkSpaces utilizzare la chiave KMS solo per questo scopo, WorkSpace ovvero solo per le persone WorkSpace associate all'utente e alla directory specificati.
2. WorkSpaces crea un volume EBS crittografato per WorkSpace e specifica la chiave KMS da utilizzare, nonché l'utente e la directory del volume (le stesse informazioni specificate in). Step 1 Questa azione crea una concessione che consente ad Amazon EBS di utilizzare la chiave KMS solo per questo WorkSpace e il volume, ovvero solo per l'utente e la directory WorkSpace associati all'utente e alla directory specificati e solo per il volume specificato.
3. Amazon EBS richiede una chiave di dati di volume crittografata con la tua chiave KMS e specifica l'ID dell' WorkSpace utente `Sid` e della directory, nonché l'ID del volume come contesto di crittografia.
4. AWS KMS crea una nuova chiave di dati, la crittografa con la chiave KMS e quindi invia la chiave di dati crittografata a Amazon EBS.
5. WorkSpaces utilizza Amazon EBS per allegare il volume crittografato al tuo WorkSpace. Amazon EBS invia la chiave dati crittografata a AWS KMS con una `Decrypt`richiesta e specifica l'ID dell' WorkSpace utente`Sid`, il relativo ID di directory e l'ID del volume, che viene utilizzato come contesto di crittografia.
6. AWS KMS usa la chiave KMS per decrittare la chiave di dati e quindi invia la chiave di dati in testo normale ad Amazon EBS.
7. Amazon EBS utilizza la chiave di dati in testo normale per crittografare tutti i dati da e verso il volume crittografato. Amazon EBS mantiene la chiave di dati in chiaro in memoria per tutto il tempo in cui il volume è collegato a. WorkSpace

8. Amazon EBS memorizza la chiave dati crittografata (ricevuta pressoStep 4) con i metadati del volume per usi futuri in caso di riavvio o ricostruzione di. WorkSpace
9. Quando usi AWS Management Console per rimuovere un WorkSpace (o usi l'`TerminateWorkspaces`azione nell' WorkSpaces API) WorkSpaces e Amazon EBS ritira le sovvenzioni che hanno consentito loro di utilizzare la tua chiave KMS a tale scopo. WorkSpace

WorkSpaces contesto di crittografia

WorkSpaces non utilizza AWS KMS key direttamente il tuo per operazioni crittografiche (come `Encrypt`, `Decrypt`, ecc.) `GenerateDataKey`, il che significa che WorkSpaces non invia richieste AWS KMS che includono un contesto di crittografia. Tuttavia, quando Amazon EBS richiede una chiave dati crittografata per i volumi crittografati del tuo WorkSpaces (Step 3inPanoramica sull'utilizzo della WorkSpaces crittografia AWS KMS) e quando richiede una copia in testo semplice di quella chiave dati (Step 5), include il contesto di crittografia nella richiesta. Il contesto di crittografia fornisce dati autenticati supplementari (AAD) utilizzati da AWS KMS per garantire l'integrità dei dati. Il contesto di crittografia viene scritto anche nei file di log AWS CloudTrail per aiutarti a comprendere perché è stata utilizzata una determinata AWS KMS key. Amazon EBS utilizza quanto segue per il contesto di crittografia:

- `sid`L'AWS Directory Serviceutente associato al WorkSpace
- L'ID della AWS Directory Service directory associata a WorkSpace
- L'ID del volume crittografato

L'esempio seguente mostra una rappresentazione JSON del contesto di crittografia che Amazon EBS utilizza:

```
{
  "aws:workspaces:sid-directoryid":
 "[S-1-5-21-277731876-1789304096-451871588-1107]@[d-1234abcd01]",
  "aws:ebs:id": "vol-1234abcd"
}
```

WorkSpaces Autorizzazione all'uso di una chiave KMS per conto dell'utente

Puoi proteggere i dati del tuo spazio di lavoro utilizzando il Chiave gestita da AWS form WorkSpaces (aws/workspaces) o una chiave gestita dal cliente. Se utilizzi una chiave gestita dal cliente, devi

WorkSpaces autorizzare l'uso della chiave KMS per conto degli amministratori del tuo account. WorkSpaces Chiave gestita da AWSPer impostazione predefinita, il modulo WorkSpaces dispone delle autorizzazioni richieste.

Per preparare la chiave gestita dal cliente da utilizzare con WorkSpaces, utilizzate la procedura seguente.

1. Aggiungi gli WorkSpaces amministratori all'elenco degli utenti chiave nella politica chiave della chiave KMS
2. Concedi agli WorkSpaces amministratori autorizzazioni aggiuntive con una policy IAM

WorkSpaces gli amministratori hanno inoltre bisogno dell'autorizzazione per l'uso. WorkSpaces Per ulteriori informazioni su queste autorizzazioni, consulta la sezione Controlling Access to WorkSpaces Resources nella Amazon WorkSpaces Administration Guide.

Parte 1: aggiunta di WorkSpaces amministratori agli utenti chiave di una chiave KMS

Per concedere WorkSpaces agli amministratori le autorizzazioni necessarie, puoi utilizzare l'AWS Management ConsoleAPI o. AWS KMS

Per aggiungere WorkSpaces amministratori come utenti chiave per una chiave KMS (console)

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.
4. Scegli l'alias o l'ID chiave gestita dal cliente preferita.
5. Scegli la scheda Policy della chiave. Su Utenti chiave, scegliere Add (Aggiungi).
6. Nell'elenco degli utenti e dei ruoli IAM, seleziona gli utenti e i ruoli che corrispondono ai tuoi WorkSpaces amministratori, quindi scegli Allega.

Per aggiungere WorkSpaces amministratori come utenti chiave per una chiave KMS (API) AWS KMS

1. Utilizza l'GetKeyPolicyoperazione per ottenere la politica chiave esistente, quindi salva il documento relativo alla policy in un file.

2. Apri il documento della policy nell'editor di testo preferito. Aggiungi gli utenti e i ruoli IAM che corrispondono ai tuoi WorkSpaces amministratori alle dichiarazioni politiche che autorizzano gli utenti chiave. Quindi salvare il file.
3. Usa l'PutKeyPolicyoperazione per applicare la politica chiave alla chiave KMS.

Parte 2: Concedere WorkSpaces agli amministratori autorizzazioni aggiuntive

Se utilizzi una chiave gestita dal cliente per proteggere WorkSpaces i tuoi dati, oltre alle autorizzazioni nella sezione utenti chiave della politica delle chiavi predefinita, gli WorkSpaces amministratori hanno bisogno dell'autorizzazione per creare concessioni sulla chiave KMS. Inoltre, se utilizzano l'opzione AWS Management Consoleper creare WorkSpaces con volumi crittografati, WorkSpaces gli amministratori devono disporre dell'autorizzazione per elencare alias e chiavi di elenco. Per ulteriori informazioni generali sulle policy IAM gestite e create, consulta Policy gestite e policy Inline nella Guida per l'utente di IAM.

Per concedere queste autorizzazioni ai tuoi WorkSpaces amministratori, utilizza una policy IAM. Aggiungi una dichiarazione di policy simile al seguente esempio alla policy IAM per ogni WorkSpaces amministratore. Sostituisci l'ARN della chiave KMS di esempio (*arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab*) con uno valido. Se i tuoi WorkSpaces amministratori utilizzano solo l' WorkSpaces API (non la console), puoi omettere la seconda dichiarazione di policy con le autorizzazioni `"kms:ListAliases"` and`"kms:ListKeys"`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "kms:CreateGrant",
      "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource": "*"
    }
  ]
```

```
}
```

Programmazione dell'API AWS KMS

È possibile utilizzare l'API AWS KMS per creare e gestire chiavi KMS e caratteristiche speciali, come archivi delle chiavi personalizzate, e usare le chiavi KMS in operazioni di crittografia. Per informazioni dettagliate, consultare Documentazione di riferimento dell'API AWS Key Management Service.

Il codice di esempio nei seguenti argomenti mostra come utilizzare gli SDK AWS per chiamare l'API AWS KMS.

Per informazioni sull'utilizzo della console AWS KMS per eseguire alcune di queste attività, consulta Gestione delle chiavi .

Argomenti

Creazione di un client

Per utilizzare il AWS SDK for Java, the AWS SDK for .NET, the AWS SDK for Python (Boto3)AWS SDK for RubyAWS SDK for PHP, the o l'AWSSDK JavaScript in Node.js per scrivere codice che utilizza l'API AWS Key Management Service (AWS KMS), inizia creando un AWS KMS client.

L'oggetto client creato viene utilizzato nel codice di esempio negli argomenti riportati di seguito.

Java

Per creare un client AWS KMS in Java, utilizzare il client builder.

```
AWSKMS kmsClient = AWSKMSClientBuilder.standard().build();
```

Per ulteriori informazioni sull'utilizzo del client builder Java, consulta le seguenti risorse.

- Fluent Client Builders sul Blog AWS per sviluppatori
- Creazione di client del servizio nella Guida per gli sviluppatori di AWS SDK for Java
- AWSKMSClientBuilder nel documento di riferimento delle API AWS SDK for Java

C#

```
AmazonKeyManagementServiceClient kmsClient = new AmazonKeyManagementServiceClient();
```

Python

```
kms_client = boto3.client('kms')
```

Ruby

```
require 'aws-sdk-kms'  # in v2: require 'aws-sdk'

kmsClient = Aws::KMS::Client.new
```

PHP

Per creare un client AWS KMS in PHP, utilizzare un oggetto client AWS KMS e specificare la versione `2014-11-01`. Per ulteriori informazioni, consulta Classe KMSClient nella Documentazione di riferimento di AWS SDK for PHP.

```
// Create a KMSClient
$KmsClient = new Aws\Kms\KmsClient([
    'profile' => 'default',
    'version' => '2014-11-01',
    'region'  => 'us-east-1'
]);
```

Node.js

```
const kmsClient = new AWS.KMS();
```

Utilizzo delle chiavi

Gli esempi in questo argomento utilizzano l'API AWS KMS per creare, visualizzare, abilitare e disabilitare AWS KMS AWS KMS keys e per generare chiavi dei dati.

Argomenti

Creazione di una chiave KMS

Per creare una AWS KMS key(chiave KMS), utilizzare l'CreateKeyoperazione. Gli esempi in questa sezione creano una chiave KMS di crittografia simmetrica. Il parametro `Description` utilizzato in questi esempi è opzionale.

Nelle lingue che richiedono un oggetto client, questi esempi utilizzano l'oggetto client AWS KMS creato in Creazione di un client.

Per informazioni sulla creazione di chiavi KMS nella console AWS KMS, consulta Creazione di chiavi.

Java

Per ulteriori informazioni, consulta il metodo createKey nella Documentazione di riferimento dell'API AWS SDK for Java.

```
// Create a KMS key
//
String desc = "Key for protecting critical data";

CreateKeyRequest req = new CreateKeyRequest().withDescription(desc);
CreateKeyResult result = kmsClient.createKey(req);
```

C#

Per maggiori dettagli, consultare il metodo CreateKey in AWS SDK for .NET.

```
// Create a KMS key
//
String desc = "Key for protecting critical data";

CreateKeyRequest req = new CreateKeyRequest()
{
    Description = desc
};
CreateKeyResponse response = kmsClient.CreateKey(req);
```

Python

Per maggiori dettagli, consultare il metodo `create_key` in AWS SDK for Python (Boto3).

```
# Create a KMS key

desc = 'Key for protecting critical data'

response = kms_client.create_key(
    Description=desc
)
```

Ruby

Per maggiori dettagli, consultare il metodo dell'istanza `create_key` in AWS SDK for Ruby.

```
# Create a KMS key

desc = 'Key for protecting critical data'

response = kmsClient.create_key({
  description: desc
})
```

PHP

Per maggiori dettagli, consultare il metodo CreateKey in AWS SDK for PHP.

```
// Create a KMS key
//
$desc = "Key for protecting critical data";
```

```
$result = $KmsClient->createKey([
    'Description' => $desc
]);
```

Node.js

Per i dettagli, vedete la proprietà CreateKey nell'SDK JavaScript per AWS Node.js.

```
// Create a KMS key
//
const Description = 'Key for protecting critical data';

kmsClient.createKey({ Description }, (err, data) => {
  ...
});
```

PowerShell

Per creare una chiave KMS PowerShell, utilizzare il cmdlet New-. KmsKey

```
# Create a KMS key

$desc = 'Key for protecting critical data'
New-KmsKey -Description $desc
```

Per utilizzare i AWS KMS PowerShell cmdlet, installa AWS.Tools. KeyManagementServicemodulo. Per ulteriori informazioni, consulta la AWS Tools for Windows PowerShellGuida per l'utente.

Generazione di una chiave di dati

Per generare una chiave dati simmetrica, usa l'GenerateDataKeyoperazione. Questa operazione restituisce una chiave di dati di testo normale e una copia di tale chiave di dati crittografata sotto la chiave KMS di crittografia simmetrica specificata. È necessario specificare `KeySpec` o `NumberOfBytes` (ma non entrambi) in ogni comando.

Per informazioni sull'utilizzo della chiave di dati per crittografare i dati, consultare AWS Encryption SDK. Puoi utilizzare la chiave di dati anche nelle operazioni HMAC.

Nelle lingue che richiedono un oggetto client, questi esempi utilizzano l'oggetto client AWS KMS creato in Creazione di un client.

Java

Per i dettagli, consulta il generateDataKey metodo nell'AWS SDK for JavaAPI Reference.

```
// Generate a data key
//
// Replace the following example key ARN with any valid key identfier
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

GenerateDataKeyRequest dataKeyRequest = new GenerateDataKeyRequest();
dataKeyRequest.setKeyId(keyId);
dataKeyRequest.setKeySpec("AES_256");

GenerateDataKeyResult dataKeyResult = kmsClient.generateDataKey(dataKeyRequest);

ByteBuffer plaintextKey = dataKeyResult.getPlaintext();

ByteBuffer encryptedKey = dataKeyResult.getCiphertextBlob();
```

C#

Per maggiori dettagli, consultare il metodo GenerateDataKey in AWS SDK for .NET.

```
// Generate a data key
//
// Replace the following example key ARN with any valid key identfier
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
GenerateDataKeyRequest dataKeyRequest = new GenerateDataKeyRequest()
{
    KeyId = keyId,
    KeySpec = DataKeySpec.AES_256
};

GenerateDataKeyResponse dataKeyResponse = kmsClient.GenerateDataKey(dataKeyRequest);

MemoryStream plaintextKey = dataKeyResponse.Plaintext;

MemoryStream encryptedKey = dataKeyResponse.CiphertextBlob;
```

Python

Per maggiori dettagli, consultare il metodo `generate_data_key` in AWS SDK for Python (Boto3).

```
# Generate a data key

# Replace the following example key ARN with any valid key identfier
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

response = kms_client.generate_data_key(
    KeyId=key_id,
    KeySpec='AES_256'
)

plaintext_key = response['Plaintext']

encrypted_key = response['CiphertextBlob']
```

Ruby

Per maggiori dettagli, consultare il metodo dell'istanza `generate_data_key` in AWS SDK for Ruby.

```
# Generate a data key

# Replace the following example key ARN with any valid key identfier
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

response = kmsClient.generate_data_key({
  key_id: key_id,
  key_spec: 'AES_256'
})

plaintext_key = response.plaintext

encrypted_key = response.ciphertext_blob
```

PHP

Per maggiori dettagli, consultare il metodo GenerateDataKey in AWS SDK for PHP.

```
// Generate a data key
//
// Replace the following example key ARN with any valid key identfier
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
$keySpec = 'AES_256';

$result = $KmsClient->generateDataKey([
    'KeyId' => $keyId,
    'KeySpec' => $keySpec,
]);

$plaintextKey = $result['Plaintext'];

$encryptedKey = $result['CiphertextBlob'];
```

Node.js

Per i dettagli, consultate la generateDataKey proprietà nell'AWSSDK per JavaScript Node.js.

```
// Generate a data key
//
// Replace the following example key ARN with any valid key identfier
const KeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
const KeySpec = 'AES_256';
kmsClient.generateDataKey({ KeyId, KeySpec }, (err, data) => {
  if (err) console.log(err, err.stack);
  else {
    const { CiphertextBlob, Plaintext } = data;
      ...
  }
});
```

PowerShell

Per generare una chiave dati simmetrica, utilizzare il cmdlet New-KMS. DataKey

Nell'output, la chiave in chiaro (nella `Plaintext` proprietà) e la chiave crittografata (nella proprietà) sono oggetti. `CiphertextBlob` MemoryStream Per convertirli in stringhe, utilizzate i metodi della `MemoryStream` classe oppure un cmdlet o una funzione che converte

`MemoryStream` gli oggetti in stringhe, ad esempio le funzioni ConvertFrom- MemoryStream e ConvertFrom -Base64 nel modulo Convert.

```
# Generate a data key

# Replace the following example key ARN with any valid key identfier
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
$keySpec = 'AES_256'

$response = New-KmsDataKey -KeyId $keyId -KeySpec $keySpec
$plaintextKey = $response.Plaintext
$encryptedKey = $response.CiphertextBlob
```

Per utilizzare i cmdlet, installa AWS.Tools. AWS KMS PowerShell KeyManagementServicemodulo. Per ulteriori informazioni, consulta la AWS Tools for Windows PowerShellGuida per l'utente.

Visualizzazione di un AWS KMS key

Per ottenere informazioni dettagliate su un ARNAWS KMS key, tra cui l'ARN della chiave KMS e lo stato della chiave, utilizzare l'DescribeKeyoperazione.

`DescribeKey` non ottiene alias. Per ottenere gli alias, usa l'operazione. ListAliases Per alcuni esempi, consulta Utilizzo degli alias.

Nelle lingue che richiedono un oggetto client, questi esempi utilizzano l'oggetto client AWS KMS creato in Creazione di un client.

Per informazioni sulla visualizzazione delle chiavi KMS nella console AWS KMS, consulta Visualizzazione di chiavi.

Java

Per ulteriori informazioni, consulta il metodo describeKey nella Documentazione di riferimento dell'API AWS SDK for Java.

```
// Describe a KMS key
//
// Replace the following example key ARN with any valid key identfier
```

```
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

DescribeKeyRequest req = new DescribeKeyRequest().withKeyId(keyId);
DescribeKeyResult result = kmsClient.describeKey(req);
```

C#

Per maggiori dettagli, consultare il metodo DescribeKey in AWS SDK for .NET.

```
// Describe a KMS key
//
// Replace the following example key ARN with any valid key identfier
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

DescribeKeyRequest describeKeyRequest = new DescribeKeyRequest()
{
    KeyId = keyId
};

DescribeKeyResponse describeKeyResponse = kmsClient.DescribeKey(describeKeyRequest);
```

Python

Per maggiori dettagli, consultare il metodo `describe_key` in AWS SDK for Python (Boto3).

```
# Describe a KMS key

# Replace the following example key ARN with any valid key identfier
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

response = kms_client.describe_key(
    KeyId=key_id
)
```

Ruby

Per maggiori dettagli, consultare il metodo dell'istanza `describe_key` in AWS SDK for Ruby.

```
# Describe a KMS key
```

```
# Replace the following example key ARN with any valid key identfier
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

response = kmsClient.describe_key({
  key_id: key_id
})
```

PHP

Per maggiori dettagli, consultare il metodo DescribeKey in AWS SDK for PHP.

```
// Describe a KMS key
//
// Replace the following example key ARN with any valid key identfier
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';

$result = $KmsClient->describeKey([
    'KeyId' => $keyId,
]);
```

Node.js

Per i dettagli, vedete la proprietà DescribeKey nell'SDK JavaScript per in AWS Node.js.

```
// Describe a KMS key
//
// Replace the following example key ARN with any valid key identfier
const KeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
kmsClient.describeKey({ KeyId }, (err, data) => {
  ...
});
```

PowerShell

Per ottenere informazioni dettagliate su una chiave KMS, utilizzare il cmdlet Get-. KmsKey

```
# Describe a KMS key

# Replace the following example key ARN with any valid key identfier
```

```
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
Get-KmsKey -KeyId $keyId
```

Per utilizzare i AWS KMS PowerShell cmdlet, installa AWS.Tools.KeyManagementServicemodulo. Per ulteriori informazioni, consulta la AWS Tools for Windows PowerShellGuida per l'utente.

Ottenimento degli ID e degli ARN delle chiavi KMS

Per ottenere gli ID delle chiavi e gli ARN delle chiavi diAWS KMS keys, utilizzare l'ListKeysoperazione. Questi esempi utilizzano il parametro `Limit` opzionale, che imposta il numero massimo di chiavi KMS restituite in ogni chiamata. Per informazioni sull'identificazione di una chiave KMS in un'operazione AWS KMS, consulta Identificatori chiave () KeyId.

Nelle lingue che richiedono un oggetto client, questi esempi utilizzano l'oggetto client AWS KMS creato in Creazione di un client.

Per informazioni sulla ricerca di ID chiave e ARN della chiave nella console AWS KMS, consulta Individuazione dell'ID e dell'ARN della chiave.

Java

Per ulteriori informazioni, consulta il metodo listKeys nella Documentazione di riferimento dell'API AWS SDK for Java.

```
// List KMS keys in this account
//
Integer limit = 10;

ListKeysRequest req = new ListKeysRequest().withLimit(limit);
ListKeysResult result = kmsClient.listKeys(req);
```

C#

Per maggiori dettagli, consultare il metodo ListKeys in AWS SDK for .NET.

```
// List KMS keys in this account
//
int limit = 10;
```

```
ListKeysRequest listKeysRequest = new ListKeysRequest()
{
    Limit = limit
};
ListKeysResponse listKeysResponse = kmsClient.ListKeys(listKeysRequest);
```

Python

Per maggiori dettagli, consultare il metodo `list_keys` in AWS SDK for Python (Boto3).

```
# List KMS keys in this account

response = kms_client.list_keys(
    Limit=10
)
```

Ruby

Per maggiori dettagli, consultare il metodo dell'istanza `list_keys` in AWS SDK for Ruby.

```
# List KMS keys in this account

response = kmsClient.list_keys({
  limit: 10
})
```

PHP

Per maggiori dettagli, consultare il metodo ListKeys in AWS SDK for PHP.

```
// List KMS keys in this account
//
$limit = 10;

$result = $KmsClient->listKeys([
    'Limit' => $limit,
]);
```

Node.js

Per i dettagli, vedete la proprietà ListKeys nell'AWSSDK per JavaScript in Node.js.

```
// List KMS keys in this account
//
const Limit = 10;
kmsClient.listKeys({ Limit }, (err, data) => {
  ...
});
```

PowerShell

Per ottenere l'ID della chiave e l'ARN della chiave di tutte le chiavi KMS nell'account e nella regione, utilizzare il cmdlet Get -. KmsKeyList

Per limitare il numero di oggetti di output, in questo esempio viene utilizzato il cmdlet Select-Object anziché il parametro `Limit`, che viene considerato obsoleto nei cmdlet list. Per informazioni sull'impaginazione dell'output in AWS Tools for PowerShell, consulta Paginazione output con AWS Tools for PowerShell.

```
# List KMS keys in this account

$limit = 10
Get-KmsKeyList | Select-Object -First $limit
```

Per utilizzare i AWS KMS PowerShell cmdlet, installa AWS.Tools.KeyManagementServicemodulo. Per ulteriori informazioni, consulta la AWS Tools for Windows PowerShellGuida per l'utente.

Abilitazione di AWS KMS keys

Per abilitare un disabileAWS KMS key, usa l'EnableKeyoperazione.

Nelle lingue che richiedono un oggetto client, questi esempi utilizzano l'oggetto client AWS KMS creato in Creazione di un client.

Per informazioni su come abilitare e disabilitare le chiavi KMS nella console AWS KMS, consulta Abilitazione e disabilitazione delle chiavi.

Java

Per ulteriori informazioni sull'implementazione Java, consulta il metodo enableKey nella Documentazione di riferimento dell'API AWS SDK for Java.

```
// Enable a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

EnableKeyRequest req = new EnableKeyRequest().withKeyId(keyId);
kmsClient.enableKey(req);
```

C#

Per maggiori dettagli, consultare il metodo EnableKey in AWS SDK for .NET.

```
// Enable a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

EnableKeyRequest enableKeyRequest = new EnableKeyRequest()
{
    KeyId = keyId
};
kmsClient.EnableKey(enableKeyRequest);
```

Python

Per maggiori dettagli, consultare il metodo `enable_key` in AWS SDK for Python (Boto3).

```
# Enable a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

response = kms_client.enable_key(
    KeyId=key_id
)
```

Ruby

Per maggiori dettagli, consultare il metodo dell'istanza `enable_key` in AWS SDK for Ruby.

```
# Enable a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

response = kmsClient.enable_key({
  key_id: key_id
})
```

PHP

Per maggiori dettagli, consultare il metodo EnableKey in AWS SDK for PHP.

```
// Enable a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';

$result = $KmsClient->enableKey([
    'KeyId' => $keyId,
]);
```

Node.js

Per i dettagli, vedete la proprietà EnableKey nell'SDK JavaScript per in AWS Node.js.

```
// Enable a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
const KeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
kmsClient.enableKey({ KeyId }, (err, data) => {
  ...
});
```

PowerShell

Per abilitare una chiave KMS, utilizzare il cmdlet Enable-. KmsKey

```
# Enable a KMS key
```

```
# Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
Enable-KmsKey -KeyId $keyId
```

Per utilizzare i AWS KMS PowerShell cmdlet, installa AWS.Tools.KeyManagementServicemodulo. Per ulteriori informazioni, consulta la AWS Tools for Windows PowerShellGuida per l'utente.

Disabilitazione di AWS KMS key

Per disabilitare una chiave KMS, usa l'DisableKeyoperazione. La disabilitazione di una chiave KMS impedisce che venga utilizzata nelle operazioni di crittografia.

Nelle lingue che richiedono un oggetto client, questi esempi utilizzano l'oggetto client AWS KMS creato in Creazione di un client.

Per informazioni su come abilitare e disabilitare le chiavi KMS nella console AWS KMS, consulta Abilitazione e disabilitazione delle chiavi.

Java

Per ulteriori informazioni, consulta il metodo disableKey nella Documentazione di riferimento dell'API AWS SDK for Java.

```
// Disable a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

DisableKeyRequest req = new DisableKeyRequest().withKeyId(keyId);
kmsClient.disableKey(req);
```

C#

Per maggiori dettagli, consultare il metodo DisableKey in AWS SDK for .NET.

```
// Disable a KMS key
//
```

```
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

DisableKeyRequest disableKeyRequest = new DisableKeyRequest()
{
    KeyId = keyId
};
kmsClient.DisableKey(disableKeyRequest);
```

Python

Per maggiori dettagli, consultare il metodo `disable_key` in AWS SDK for Python (Boto3).

```
# Disable a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

response = kms_client.disable_key(
    KeyId=key_id
)
```

Ruby

Per maggiori dettagli, consultare il metodo dell'istanza `disable_key` in AWS SDK for Ruby.

```
# Disable a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

response = kmsClient.disable_key({
  key_id: key_id
})
```

PHP

Per maggiori dettagli, consultare il metodo DisableKey in AWS SDK for PHP.

```
// Disable a KMS key
```

```
//
// Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';

$result = $KmsClient->disableKey([
    'KeyId' => $keyId,
]);
```

Node.js

Per i dettagli, vedete la proprietà DisableKey nell'SDK JavaScript per in AWS Node.js.

```
// Disable a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
const KeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
kmsClient.disableKey({ KeyId }, (err, data) => {
  ...
});
```

PowerShell

Per disabilitare una chiave KMS, utilizzare il cmdlet Disable-. KmsKey

```
# Disable a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
Disable-KmsKey -KeyId $keyId
```

Per utilizzare i AWS KMS PowerShell cmdlet, installa AWS.Tools. KeyManagementServicemodulo. Per ulteriori informazioni, consulta la Guida per l'utente AWS Tools for Windows PowerShell.

Utilizzo degli alias

Gli esempi in questo argomento utilizzano l'API AWS KMS per creare, visualizzare, aggiornare ed eliminare gli alias. Per ulteriori informazioni sugli alias, consulta the section called “Utilizzo di alias”.

Argomenti

Creazione di un alias

Quando si crea una AWS KMS key nella AWS Management Console, devi creare un alias. Tuttavia, l'CreateKeyoperazione che crea una chiave KMS non crea un alias.

Per creare un alias, usa l'operazione. CreateAlias L'alias deve essere univoco nell'account e nella regione. Non è possibile creare un alias che inizia con `aws/`. Il prefisso `aws/` viene riservato da Amazon Web Services alle Chiavi gestite da AWS.

Nelle lingue che richiedono un oggetto client, questi esempi utilizzano l'oggetto client AWS KMS creato in Creazione di un client.

Java

Per ulteriori informazioni, consulta il metodo createAlias nella Documentazione di riferimento dell'API AWS SDK for Java.

```
// Create an alias for a KMS key
//
String aliasName = "alias/projectKey1";
// Replace the following example key ARN with a valid key ID or key ARN
String targetKeyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

CreateAliasRequest req = new
 CreateAliasRequest().withAliasName(aliasName).withTargetKeyId(targetKeyId);
kmsClient.createAlias(req);
```

C#

Per maggiori dettagli, consultare il metodo CreateAlias in AWS SDK for .NET.

```
// Create an alias for a KMS key
```

```
//
String aliasName = "alias/projectKey1";
// Replace the following example key ARN with a valid key ID or key ARN
String targetKeyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

CreateAliasRequest createAliasRequest = new CreateAliasRequest()
{
    AliasName = aliasName,
    TargetKeyId = targetKeyId
};
kmsClient.CreateAlias(createAliasRequest);
```

Python

Per maggiori dettagli, consultare il metodo `create_alias` in AWS SDK for Python (Boto3).

```
# Create an alias for a KMS key

alias_name = 'alias/projectKey1'
# Replace the following example key ARN with a valid key ID or key ARN
target_key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

response = kms_client.create_alias(
    AliasName=alias_name,
    TargetKeyId=key_id
)
```

Ruby

Per maggiori dettagli, consultare il metodo dell'istanza `create_alias` in AWS SDK for Ruby.

```
# Create an alias for a KMS key

alias_name = 'alias/projectKey1'
# Replace the following example key ARN with a valid key ID or key ARN
target_key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

response = kmsClient.create_alias({
  alias_name: alias_name,
  target_key_id: target_key_id
```

```
})
```

PHP

Per maggiori dettagli, consultare il metodo CreateAlias in AWS SDK for PHP.

```
// Create an alias for a KMS key
//
$aliasName = "alias/projectKey1";
// Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';


$result = $KmsClient->createAlias([
    'AliasName' => $aliasName,
    'TargetKeyId' =>  $keyId,
]);
```

Node.js

Per i dettagli, vedete la proprietà CreateAlias nell'SDK per in AWS Node.js. JavaScript

```
// Create an alias for a KMS key
//
const AliasName = 'alias/projectKey1';

// Replace the following example key ARN with a valid key ID or key ARN
const TargetKeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
kmsClient.createAlias({ AliasName, TargetKeyId }, (err, data) => {
  ...
});
```

PowerShell

Per creare un alias, utilizzare il cmdlet New-KMSalias. Il nome alias fa distinzione tra maiuscole e minuscole.

```
# Create an alias for a KMS key

$aliasName = 'alias/projectKey1'
# Replace the following example key ARN with a valid key ID or key ARN
```

```
$targetKeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

New-KMSAlias -TargetKeyId $targetKeyId -AliasName $aliasName
```

Per utilizzare i AWS KMS PowerShell cmdlet, installa AWS.Tools.KeyManagementServicemodulo. Per ulteriori informazioni, consulta la AWS Tools for Windows PowerShellGuida per l'utente.

Elenco degli alias

Per elencare gli alias nell'account e nella regione, usa l'ListAliasesoperazione.

Per impostazione predefinita, il comando ListAliases restituisce tutti gli alias nell'account e nella regione. Sono inclusi gli alias creati e associati alle chiavi gestite dal cliente e gli alias creati da AWS e associati alle tue Chiavi gestite da AWS. La risposta potrebbe anche includere alias che non hanno alcun campo `TargetKeyId`. Questi sono alias predefiniti che AWS ha creato, ma che non ha ancora associato a una chiave KMS.

Nelle lingue che richiedono un oggetto client, questi esempi utilizzano l'oggetto client AWS KMS creato in Creazione di un client.

Java

Per ulteriori informazioni sull'implementazione Java, consulta il metodo listAliases nella Documentazione di riferimento dell'API AWS SDK for Java.

```
// List the aliases in this Account AWS
//
Integer limit = 10;

ListAliasesRequest req = new ListAliasesRequest().withLimit(limit);
ListAliasesResult result = kmsClient.listAliases(req);
```

C#

Per maggiori dettagli, consultare il metodo ListAliases in AWS SDK for .NET.

```
// List the aliases in this Account AWS
//
```

```
int limit = 10;

ListAliasesRequest listAliasesRequest = new ListAliasesRequest()
{
    Limit = limit
};
ListAliasesResponse listAliasesResponse = kmsClient.ListAliases(listAliasesRequest);
```

Python

Per maggiori dettagli, consultare il metodo `list_aliases` in AWS SDK for Python (Boto3).

```
# List the aliases in this Account AWS

response = kms_client.list_aliases(
    Limit=10
)
```

Ruby

Per maggiori dettagli, consultare il metodo dell'istanza `list_aliases` in AWS SDK for Ruby.

```
# List the aliases in this Account AWS

response = kmsClient.list_aliases({
  limit: 10
})
```

PHP

Per ulteriori informazioni, consulta il metodo List Aliases nella AWS SDK for PHP.

```
// List the aliases in this Account AWS
//
$limit = 10;

$result = $KmsClient->listAliases([
    'Limit' => $limit,
]);
```

Node.js

Per i dettagli, vedete la proprietà ListAliases nell'SDK JavaScript per in AWS Node.js.

```
// List the aliases in this Account AWS
//
const Limit = 10;
kmsClient.listAliases({ Limit }, (err, data) => {
  ...
});
```

PowerShell

Per elencare gli alias nell'account e nella regione, utilizzare il cmdlet Get-KMS. AliasList

Per limitare il numero di oggetti di output, in questo esempio viene utilizzato il cmdlet Select-Object anziché il parametro `Limit`, che viene considerato obsoleto nei cmdlet list. Per informazioni sull'impaginazione dell'output in AWS Tools for PowerShell, consulta Paginazione output con AWS Tools for PowerShell.

```
# List the aliases in this Account AWS
$limit = 10

$result = Get-KMSAliasList | Select-Object -First $limit
```

Per utilizzare i cmdlet, installa AWS.Tools. AWS KMS PowerShell KeyManagementServicemodulo. Per ulteriori informazioni, consulta la AWS Tools for Windows PowerShellGuida per l'utente.

Per elencare solo gli alias associati a una determinata chiave KMS, utilizza il parametro `KeyId`. Il valore può essere l'ID chiave o l'ARN chiave di qualsiasi chiave KMS nella Regione. Non è possibile specificare un nome dell'alias o un ARN dell'alias.

Java

Per ulteriori informazioni sull'implementazione Java, consulta il metodo listAliases nella Documentazione di riferimento dell'API AWS SDK for Java.

```
// List the aliases for one KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
```

```
ListAliasesRequest req = new ListAliasesRequest().withKeyId(keyId);
ListAliasesResult result = kmsClient.listAliases(req);
```

C#

Per maggiori dettagli, consultare il metodo ListAliases in AWS SDK for .NET.

```
// List the aliases for one KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

ListAliasesRequest listAliasesRequest = new ListAliasesRequest()
{
    KeyId = keyId
};
ListAliasesResponse listAliasesResponse = kmsClient.ListAliases(listAliasesRequest);
```

Python

Per maggiori dettagli, consultare il metodo `list_aliases` in AWS SDK for Python (Boto3).

```
# List the aliases for one KMS key

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

response = kms_client.list_aliases(
    KeyId=key_id
)
```

Ruby

Per maggiori dettagli, consultare il metodo dell'istanza `list_aliases` in AWS SDK for Ruby.

```
# List the aliases for one KMS key

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
```

```
response = kmsClient.list_aliases({
  key_id: key_id
})
```

PHP

Per ulteriori informazioni, consulta il metodo List Aliases nella AWS SDK for PHP.

```
// List the aliases for one KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';

$result = $KmsClient->listAliases([
    'KeyId' => $keyId,
]);
```

Node.js

Per i dettagli, vedete la proprietà ListAliases nell'SDK JavaScript per in AWS Node.js.

```
// List the aliases for one KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
const KeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
kmsClient.listAliases({ KeyId }, (err, data) => {
  ...
});
```

PowerShell

Per elencare gli alias per una chiave KMS, utilizzare il `KeyId` parametro del cmdlet Get-KMS. AliasList

```
# List the aliases for one KMS key

# Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
```

```
$response = Get-KmsAliasList -KeyId $keyId
```

Per utilizzare i cmdlet, installa AWS.Tools. AWS KMS PowerShell KeyManagementServicemodulo. Per ulteriori informazioni, consulta la AWS Tools for Windows PowerShellGuida per l'utente.

Aggiornamento di un alias

Per associare un alias esistente a una chiave KMS diversa, usa l'UpdateAliasoperazione.

Nelle lingue che richiedono un oggetto client, questi esempi utilizzano l'oggetto client AWS KMS creato in Creazione di un client.

Java

Per ulteriori informazioni sull'implementazione Java, consulta il metodo updateAlias nella Documentazione di riferimento dell'API AWS SDK for Java.

```
// Updating an alias
//
String aliasName = "alias/projectKey1";
// Replace the following example key ARN with a valid key ID or key ARN
String targetKeyId = "arn:aws:kms:us-
west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321";

UpdateAliasRequest req = new UpdateAliasRequest()
     .withAliasName(aliasName)
     .withTargetKeyId(targetKeyId);

kmsClient.updateAlias(req);
```

C#

Per maggiori dettagli, consultare il metodo UpdateAlias in AWS SDK for .NET.

```
// Updating an alias
//
String aliasName = "alias/projectKey1";
// Replace the following example key ARN with a valid key ID or key ARN
```

```
String targetKeyId = "arn:aws:kms:us-
west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321";

UpdateAliasRequest updateAliasRequest = new UpdateAliasRequest()
{
    AliasName = aliasName,
    TargetKeyId = targetKeyId
};

kmsClient.UpdateAlias(updateAliasRequest);
```

Python

Per maggiori dettagli, consultare il metodo `update_alias` in AWS SDK for Python (Boto3).

```
# Updating an alias

alias_name = 'alias/projectKey1'
# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321'

response = kms_client.update_alias(
    AliasName=alias_name,
    TargetKeyID=key_id
)
```

Ruby

Per maggiori dettagli, consultare il metodo dell'istanza `update_alias` in AWS SDK for Ruby.

```
# Updating an alias

alias_name = 'alias/projectKey1'
# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321'

response = kmsClient.update_alias({
  alias_name: alias_name,
  target_key_id: key_id
})
```

PHP

Per maggiori dettagli, consultare il metodo UpdateAlias in AWS SDK for PHP.

```
// Updating an alias
//
$aliasName = "alias/projectKey1";

// Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321';

$result = $KmsClient->updateAlias([
    'AliasName' => $aliasName,
    'TargetKeyId' =>  $keyId,
]);
```

Node.js

Per i dettagli, vedete la proprietà UpdateAlias nell'SDK per in AWS Node.js. JavaScript

```
// Updating an alias
//
const AliasName = 'alias/projectKey1';

// Replace the following example key ARN with a valid key ID or key ARN
const TargetKeyId = 'arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321';
kmsClient.updateAlias({ AliasName, TargetKeyId }, (err, data) => {
  ...
});
```

PowerShell

Per modificare la chiave KMS associata a un alias utilizza il cmdlet Update-KMSAlias. Il nome alias fa distinzione tra maiuscole e minuscole.

Il cmdlet `Update-KMSAlias` non restituisce alcun output. Per verificare che il comando abbia funzionato, utilizzare il cmdlet Get-KMS. AliasList

```
# Updating an alias

$aliasName = 'alias/projectKey1'
```

```
# Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321'

Update-KMSAlias -AliasName $aliasName -TargetKeyID $keyId
```

Per utilizzare i AWS KMS PowerShell cmdlet, installa AWS.Tools.KeyManagementServicemodulo. Per ulteriori informazioni, consulta la AWS Tools for Windows PowerShellGuida per l'utente.

Eliminazione di un alias

Per eliminare un alias, usa l'DeleteAliasoperazione. L'eliminazione di un alias non ha alcun effetto sulla chiave KMS associata.

Nelle lingue che richiedono un oggetto client, questi esempi utilizzano l'oggetto client AWS KMS creato in Creazione di un client.

Java

Per ulteriori informazioni, consulta il metodo deleteAlias nella Documentazione di riferimento dell'API AWS SDK for Java.

```
// Delete an alias for a KMS key
//
String aliasName = "alias/projectKey1";

DeleteAliasRequest req  = new DeleteAliasRequest().withAliasName(aliasName);
kmsClient.deleteAlias(req);
```

C#

Per maggiori dettagli, consultare il metodo DeleteAlias in AWS SDK for .NET.

```
// Delete an alias for a KMS key
//
String aliasName = "alias/projectKey1";

DeleteAliasRequest deleteAliasRequest = new DeleteAliasRequest()
{
    AliasName = aliasName
```

```
};
kmsClient.DeleteAlias(deleteAliasRequest);
```

Python

Per maggiori dettagli, consultare il metodo `delete_alias` in AWS SDK for Python (Boto3).

```
# Delete an alias for a KMS key

alias_name = 'alias/projectKey1'

response = kms_client.delete_alias(
    AliasName=alias_name
)
```

Ruby

Per maggiori dettagli, consultare il metodo dell'istanza `delete_alias` in AWS SDK for Ruby.

```
# Delete an alias for a KMS key

alias_name = 'alias/projectKey1'

response = kmsClient.delete_alias({
  alias_name: alias_name
})
```

PHP

Per maggiori dettagli, consultare il metodo DeleteAlias in AWS SDK for PHP.

```
// Delete an alias for a KMS key
//
$aliasName = "alias/projectKey1";

$result = $KmsClient->deleteAlias([
    'AliasName' => $aliasName,
]);
```

Node.js

Per i dettagli, vedete la proprietà deleteAlias) nell'SDK per in AWS Node.js. JavaScript

```
// Delete an alias for a KMS key
//
const AliasName = 'alias/projectKey1';
kmsClient.deleteAlias({ AliasName }, (err, data) => {
  ...
});
```

PowerShell

Per eliminare un alias, utilizzare il cmdlet Remove-KMSAlias. Il nome alias fa distinzione tra maiuscole e minuscole.

Poiché questo cmdlet elimina definitivamente l'alias, richiede di confermare il comando. PowerShell `ConfirmImpact` è `High`, quindi non è possibile utilizzare `ConfirmPreference` per annullare questo prompt. Se è necessario annullare il prompt di conferma, aggiungere il parametro comune `Confirm` con un valore `$false`, ad esempio: `-Confirm:$false`.

Il cmdlet `Remove-KMSAlias` non restituisce alcun output. Per verificare l'efficacia del comando, utilizzare il cmdlet Get-KMS. AliasList

```
# Delete an alias for a KMS key

$aliasName = 'alias/projectKey1'
Remove-KMSAlias -AliasName $aliasName
```

Per utilizzare i AWS KMS PowerShell cmdlet, installa AWS.Tools. KeyManagementServicemodulo. Per ulteriori informazioni, consulta la Guida per l'utente AWS Tools for Windows PowerShell.

Crittografia e decrittografia delle chiavi di dati

Gli esempi in questo argomento utilizzano Encrypt, Decrypt e ReEncryptle operazioni nell'API. AWS KMS

Queste operazioni sono progettate per crittografare e decrittografare le chiavi dei dati. Usano una AWS KMS keys nelle operazioni di crittografia e non possono accettare più di 4 KB (4096 byte) di dati. Anche se è possibile utilizzarli per crittografare piccole quantità di dati, ad esempio una password o la chiave RSA, non sono state progettate per crittografare i dati delle applicazioni.

Per crittografare i dati delle applicazioni, utilizza le funzionalità di crittografia lato server di un servizio AWS o una libreria di crittografia lato client, come il client di crittografia AWS Encryption SDK o quello di Amazon S3.

Argomenti

- Crittografia di una chiave di dati
- Decrittografia di una chiave di dati
- Ricrittografia di una chiave di dati in un'altra AWS KMS key

Crittografia di una chiave di dati

L'operazione Encrypt è progettata per crittografare le chiavi dei dati, ma non viene utilizzata di frequente. Le GenerateDataKeyWithoutPlaintextoperazioni GenerateDataKeyand restituiscono chiavi di dati crittografate. Puoi utilizzare questo metodo quando desideri spostare dati crittografati in una diversa regione e vuoi crittografare i dati con una chiave KMS nella nuova regione.

Nelle lingue che richiedono un oggetto client, questi esempi utilizzano l'oggetto client AWS KMS creato in Creazione di un client.

Java

Per ulteriori informazioni, consulta il metodo encrypt nella Documentazione di riferimento dell'API AWS SDK for Java.

```
// Encrypt a data key
//
// Replace the following example key ARN with any valid key identfier
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
ByteBuffer plaintext = ByteBuffer.wrap(new byte[]{1,2,3,4,5,6,7,8,9,0});

EncryptRequest req = new EncryptRequest().withKeyId(keyId).withPlaintext(plaintext);
ByteBuffer ciphertext = kmsClient.encrypt(req).getCiphertextBlob();
```

C#

Per ulteriori informazioni, consulta il metodo di crittografia nella AWS SDK for .NET.

```
// Encrypt a data key
```

```
//
// Replace the following example key ARN with any valid key identfier
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
MemoryStream plaintext = new MemoryStream();
plaintext.Write(new byte[] { 1, 2, 3, 4, 5, 6, 7, 8, 9, 0 }, 0, 10);

EncryptRequest encryptRequest = new EncryptRequest()
{
    KeyId = keyId,
    Plaintext = plaintext
};
MemoryStream ciphertext = kmsClient.Encrypt(encryptRequest).CiphertextBlob;
```

Python

Per ulteriori informazioni, consulta il metodo di crittografia nella AWS SDK for Python (Boto3).

```
# Encrypt a data key

# Replace the following example key ARN with any valid key identfier
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
plaintext = b'\x01\x02\x03\x04\x05\x06\x07\x08\x09\x00'

response = kms_client.encrypt(
    KeyId=key_id,
    Plaintext=plaintext
)

ciphertext = response['CiphertextBlob']
```

Ruby

Per ulteriori informazioni, consulta il metodo dell'istanza encrypt nella AWS SDK for Ruby.

```
# Encrypt a data key

# Replace the following example key ARN with any valid key identfier
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
plaintext = "\x01\x02\x03\x04\x05\x06\x07\x08\x09\x00"
```

```
response = kmsClient.encrypt({
  key_id: key_id,
  plaintext: plaintext
})

ciphertext = response.ciphertext_blob
```

PHP

Per ulteriori informazioni, consulta il metodo di crittografia nella AWS SDK for PHP.

```
// Encrypt a data key
//
// Replace the following example key ARN with any valid key identfier
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
$message = pack('c*',1,2,3,4,5,6,7,8,9,0);

$result = $KmsClient->encrypt([
    'KeyId' => $keyId,
    'Plaintext' => $message,
]);

$ciphertext = $result['CiphertextBlob'];
```

Node.js

Per i dettagli, consulta la proprietà encrypt nell'AWSSDK per JavaScript in Node.js.

```
// Encrypt a data key
//
// Replace the following example key ARN with any valid key identfier
const KeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
const Plaintext = Buffer.from([1, 2, 3, 4, 5, 6, 7, 8, 9, 0]);
kmsClient.encrypt({ KeyId, Plaintext }, (err, data) => {
  if (err) console.log(err, err.stack); // an error occurred
  else {
    const { CiphertextBlob } = data;
      ...
  }
});
```

PowerShell

Per crittografare una chiave di dati in una chiave KMS, utilizza il cmdlet Invoke-KMSEncrypt. Restituisce il testo cifrato come (System.IO. MemoryStream MemoryStream) oggetto. È possibile utilizzare l'oggetto `MemoryStream` come input del cmdlet Invoke-KmsDecrypt.

AWS KMS restituisce anche chiavi dati come oggetti `MemoryStream`. In questo esempio, per simulare una chiave di dati in testo normale, creiamo un array di byte e lo scriviamo su un oggetto `MemoryStream`.

Si noti che il parametro `Plaintext`di `Invoke-KMSEncrypt` accetta un array di byte (`byte[]`); non richiede un oggetto `MemoryStream`. A partire dalla AWSPowerShell versione 4.0, i parametri in tutti i AWSPowerShell moduli che accettano array e `MemoryStream` oggetti di byte accettano array di byte, oggetti, stringhe, `MemoryStream` array di stringhe e (System.IO. `FileInfo` FileInfo) oggetti. È possibile passare uno qualsiasi di questi tipi a `Invoke-KMSEncrypt`.

```
# Encrypt a data key

# Replace the following example key ARN with any valid key identfier
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

# Simulate a data key
 # Create a byte array
[byte[]] $bytes = 1, 2, 3, 4, 5, 6, 7, 8, 9, 0

 # Create a MemoryStream
$plaintext = [System.IO.MemoryStream]::new()

 # Add the byte array to the MemoryStream
$plaintext.Write($bytes, 0, $bytes.length)

# Encrypt the simulated data key
$response = Invoke-KMSEncrypt -KeyId $keyId -Plaintext $plaintext

# Get the ciphertext from the response
$ciphertext = $response.CiphertextBlob
```

Per utilizzare i AWS KMS PowerShell cmdlet, installa AWS.Tools. KeyManagementServicemodulo. Per ulteriori informazioni, consulta la AWS Tools for Windows PowerShellGuida per l'utente.

Decrittografia di una chiave di dati

Per decrittografare una chiave di dati, utilizza l'operazione Decrypt.

Il `ciphertextBlob` valore specificato deve essere il valore del `CiphertextBlob` campo di una risposta GenerateDataKeyGenerateDataKeyWithoutPlaintext, o Encrypt, o il `PrivateKeyCiphertextBlob` campo di una GenerateDataKeyPairWithoutPlaintextrisposta GenerateDataKeyPairor. Puoi inoltre utilizzare l'operazione `Decrypt` per decrittare i dati crittografati all'esterno di AWS KMS dalla chiave pubblica in una chiave KMS asimmetrica.

Il parametro `KeyId` non è richiesto quando per la decrittografia si utilizzano chiavi KMS di crittografia simmetrica. AWS KMS può ottenere la chiave KMS utilizzata per crittografare i dati dai metadati nel blob in testo cifrato. Tuttavia è sempre consigliabile specificare la chiave KMS che stai utilizzando. Questa procedura garantisce di utilizzare la chiave KMS desiderata e impedisce di decrittare inavvertitamente un testo cifrato utilizzando una chiave KMS non attendibile.

Nelle lingue che richiedono un oggetto client, questi esempi utilizzano l'oggetto client AWS KMS creato in Creazione di un client.

Java

Per ulteriori informazioni, consulta il metodo decrypt nella Documentazione di riferimento dell'API AWS SDK for Java.

```
// Decrypt a data key
//
// Replace the following example key ARN with any valid key identfier
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

ByteBuffer ciphertextBlob = Place your ciphertext here;

DecryptRequest req = new
 DecryptRequest().withCiphertextBlob(ciphertextBlob).withKeyId(keyId);
ByteBuffer plainText = kmsClient.decrypt(req).getPlaintext();
```

C#

Per ulteriori informazioni, consulta il metodo di decrittografia nella AWS SDK for .NET.

```
// Decrypt a data key
//
```

```
// Replace the following example key ARN with any valid key identfier
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

MemoryStream ciphertextBlob = new MemoryStream();
// Write ciphertext to memory stream

DecryptRequest decryptRequest = new DecryptRequest()
{
    CiphertextBlob = ciphertextBlob,
    KeyId = keyId
};
MemoryStream plainText = kmsClient.Decrypt(decryptRequest).Plaintext;
```

Python

Per ulteriori informazioni, consulta il metodo di decrittografia nella AWS SDK for Python (Boto3).

```
# Decrypt a data key

# Replace the following example key ARN with any valid key identfier
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
ciphertext = 'Place your ciphertext here'

response = kms_client.decrypt(
    CiphertextBlob=ciphertext,
    KeyId=key_id
)

plaintext = response['Plaintext']
```

Ruby

Per ulteriori informazioni, consulta il metodo dell'istanza decrypt nella AWS SDK for Ruby.

```
# Decrypt a data key

# Replace the following example key ARN with any valid key identfier
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

ciphertext = 'Place your ciphertext here'
```

```
ciphertext_packed = [ciphertext].pack("H*")

response = kmsClient.decrypt({
  ciphertext_blob: ciphertext_packed,
  key_id: key_id
})

plaintext = response.plaintext
```

PHP

Per ulteriori informazioni, consulta il metodo di decrittografia nella AWS SDK for PHP.

```
// Decrypt a data key
//
// Replace the following example key ARN with any valid key identfier
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
$ciphertext = 'Place your cipher text blob here';

$result = $KmsClient->decrypt([
     'CiphertextBlob' => $ciphertext,
     'KeyId' => $keyId,
]);

$plaintext = $result['Plaintext'];
```

Node.js

Per i dettagli, consulta la proprietà decrypt nell'AWSSDK per in Node.js. JavaScript

```
// Decrypt a data key
//
// Replace the following example key ARN with any valid key identfier
const KeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
const CiphertextBlob = 'Place your cipher text blob here';
kmsClient.decrypt({ CiphertextBlob, KeyId }, (err, data) => {
  if (err) console.log(err, err.stack); // an error occurred
  else {
    const { Plaintext } = data;
    ...
  }
```

```
});
```

PowerShell

Per decrittare una chiave dati, utilizzare il cmdlet Invoke-KMSEncrypt.

Questo cmdlet restituisce il testo semplice come (System.IO). `MemoryStream` MemoryStream) oggetto. Per convertirlo in un array di byte, utilizzare cmdlet o funzioni che convertono oggetti `MemoryStream` in array di byte, ad esempio le funzioni del modulo Convert.

Poiché in questo esempio viene utilizzato il testo cifrato restituito da un cmdlet di crittografia AWS KMS, viene utilizzato un oggetto `MemoryStream` per il valore del parametro `CiphertextBlob`. Tuttavia, il parametro `CiphertextBlob` di `Invoke-KMSDecrypt` accetta un array di byte (`byte[]`); non richiede un oggetto `MemoryStream`. A partire dalla AWSPowerShell versione 4.0, i parametri in tutti i AWSPowerShell moduli che accettano array e `MemoryStream` oggetti di byte accettano array di byte, oggetti, stringhe, `MemoryStream` array di stringhe e (System.IO. `FileInfo` FileInfo) oggetti. È possibile passare uno qualsiasi di questi tipi a `Invoke-KMSDecrypt`.

```
# Decrypt a data key
# Replace the following example key ARN with any valid key identfier
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

[System.IO.MemoryStream]$ciphertext = Read-Host 'Place your cipher text blob here'

$response = Invoke-KMSDecrypt -CiphertextBlob $ciphertext -KeyId $keyId
$plaintext = $response.Plaintext
```

Per utilizzare i AWS KMS PowerShell cmdlet, installa AWS.Tools. KeyManagementServicemodulo. Per ulteriori informazioni, consulta la AWS Tools for Windows PowerShellGuida per l'utente.

Ricrittografia di una chiave di dati in un'altra AWS KMS key

Per decrittografare una chiave dati crittografata e quindi ricrittografare immediatamente la chiave dati con un'altraAWS KMS key, utilizzare l'operazione. ReEncrypt Le operazioni vengono eseguite interamente su lato server all'interno di AWS KMS, in modo che il testo normale non dovrà mai essere esposto all'esterno di AWS KMS.

`ciphertextBlob`Ciò che specifichi deve essere il valore del `CiphertextBlob` campo di una GenerateDataKeyrisposta o Encrypt o il `PrivateKeyCiphertextBlob` campo di una risposta or. GenerateDataKeyWithoutPlaintextGenerateDataKeyPairGenerateDataKeyPairWithoutPlaintext Puoi inoltre utilizzare l'operazione `ReEncrypt` per crittografare nuovamente i dati crittografati all'esterno di AWS KMS dalla chiave pubblica in una chiave KMS asimmetrica.

Il parametro `SourceKeyId` non è richiesto quando si crittografa nuovamente con chiavi KMS di crittografia simmetrica. AWS KMS può ottenere la chiave KMS utilizzata per crittografare i dati dai metadati nel blob in testo cifrato. Tuttavia è sempre consigliabile specificare la chiave KMS che stai utilizzando. Questa procedura garantisce di utilizzare la chiave KMS desiderata e impedisce di decrittare inavvertitamente un testo cifrato utilizzando una chiave KMS non attendibile.

Nelle lingue che richiedono un oggetto client, questi esempi utilizzano l'oggetto client AWS KMS creato in Creazione di un client.

Java

Per ulteriori informazioni, consulta il metodo reEncrypt nella Documentazione di riferimento dell'API AWS SDK for Java.

```
// Re-encrypt a data key

ByteBuffer sourceCiphertextBlob = Place your ciphertext here;

// Replace the following example key ARNs with valid key identfiers
String sourceKeyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
String destinationKeyId = "arn:aws:kms:us-
west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321";

ReEncryptRequest req = new ReEncryptRequest();
req.setCiphertextBlob(sourceCiphertextBlob);
req.setSourceKeyId(sourceKeyId);
req.setDestinationKeyId(destinationKeyId);
ByteBuffer destinationCipherTextBlob = kmsClient.reEncrypt(req).getCiphertextBlob();
```

C#

Per maggiori dettagli, consultare il metodo ReEncrypt in AWS SDK for .NET.

```
// Re-encrypt a data key
```

```
MemoryStream sourceCiphertextBlob = new MemoryStream();
// Write ciphertext to memory stream

// Replace the following example key ARNs with valid key identfiers
String sourceKeyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
String destinationKeyId = "arn:aws:kms:us-
west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321";

ReEncryptRequest reEncryptRequest = new ReEncryptRequest()
{
    CiphertextBlob = sourceCiphertextBlob,
    SourceKeyId = sourceKeyId,
    DestinationKeyId = destinationKeyId
};
MemoryStream destinationCipherTextBlob =
 kmsClient.ReEncrypt(reEncryptRequest).CiphertextBlob;
```

Python

Per maggiori dettagli, consultare il metodo `re_encrypt` in AWS SDK for Python (Boto3).

```
# Re-encrypt a data key
ciphertext = 'Place your ciphertext here'

# Replace the following example key ARNs with valid key identfiers
source_key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
destination_key_id = 'arn:aws:kms:us-
west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321'

response = kms_client.re_encrypt(
    CiphertextBlob=ciphertext,
    SourceKeyId=source_key_id,
    DestinationKeyId=destination_key_id
)

destination_ciphertext_blob = response['CiphertextBlob']
```

Ruby

Per maggiori dettagli, consultare il metodo dell'istanza `re_encrypt` in AWS SDK for Ruby.

```
# Re-encrypt a data key

ciphertext = 'Place your ciphertext here'
ciphertext_packed = [ciphertext].pack("H*")

# Replace the following example key ARNs with valid key identfiers
source_key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
destination_key_id = 'arn:aws:kms:us-
west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321'

response = kmsClient.re_encrypt({
  ciphertext_blob: ciphertext_packed,
  source_key_id: source_key_id,
  destination_key_id: destination_key_id
})

destination_ciphertext_blob = response.ciphertext_blob.unpack('H*')
```

PHP

Per maggiori dettagli, consultare il metodo ReEncrypt in AWS SDK for PHP.

```
// Re-encrypt a data key

$ciphertextBlob = 'Place your ciphertext here';

// Replace the following example key ARNs with valid key identfiers
$sourceKeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
$destinationKeyId = 'arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321';

$result = $KmsClient->reEncrypt([
    'CiphertextBlob' => $ciphertextBlob,
    'SourceKeyId' => $sourceKeyId,
    'DestinationKeyId' => $destinationKeyId,
]);
```

Node.js

Per i dettagli, vedete la proprietà ReEncrypt nell'SDK JavaScript per AWS Node.js.

```
// Re-encrypt a data key
const CiphertextBlob = 'Place your cipher text blob here';
// Replace the following example key ARNs with valid key identfiers
const SourceKeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
const DestinationKeyId = 'arn:aws:kms:us-
west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321';

kmsClient.reEncrypt({ CiphertextBlob, SourceKeyId, DestinationKeyId }, (err, data)
 => {
  ...
});
```

PowerShell

Per crittografare nuovamente un testo cifrato con la stessa chiave KMS o con una chiave diversa, utilizzare il cmdlet Invoke-KMS. ReEncrypt

Poiché in questo esempio viene utilizzato il testo cifrato restituito da un cmdlet di crittografia AWS KMS, viene utilizzato un oggetto `MemoryStream` per il valore del parametro `CiphertextBlob`. Tuttavia, il parametro `CiphertextBlob` di `Invoke-KMSReEncrypt` accetta un array di byte (`byte[]`); non richiede un oggetto `MemoryStream`. A partire dalla AWSPowerShell versione 4.0, i parametri in tutti i AWSPowerShell moduli che utilizzano matrici di byte e gli `MemoryStream` oggetti accettano array di byte, oggetti, stringhe, matrici di stringhe e (System.IO. `MemoryStreamFileInfo` FileInfo) oggetti. È possibile passare uno qualsiasi di questi tipi a `Invoke-KMSReEncrypt`.

```
# Re-encrypt a data key

[System.IO.MemoryStream]$ciphertextBlob = Read-Host 'Place your cipher text blob
 here'

# Replace the following example key ARNs with valid key identfiers
$sourceKeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
$destinationKeyId = 'arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321'

$response = Invoke-KMSReEncrypt -Ciphertext $ciphertextBlob -SourceKeyId
 $sourceKeyId -DestinationKeyId $destinationKeyId
$reEncryptedCiphertext = $response.CiphertextBlob
```

Per utilizzare i AWS KMS PowerShell cmdlet, installa AWS.Tools.KeyManagementServicemodulo. Per ulteriori informazioni, consulta la Guida per l'utente AWS Tools for Windows PowerShell.

Utilizzo di policy delle chiavi

Negli esempi riportati in questo argomento viene utilizzata l'API AWS KMS per visualizzare e modificare le policy delle chiavi di AWS KMS keys.

Per ulteriori informazioni su come utilizzare le policy delle chiavi e le policy IAM per gestire l'accesso alle tue chiavi KMS, consulta Autenticazione e controllo degli accessi per AWS KMS. Per informazioni sulla scrittura e sulla formattazione di un documento di policy JSON, consulta la Documentazione di riferimento sulla policy IAM JSON nella Guida per l'utente di IAM.

Argomenti

- Elenco dei nomi delle policy delle chiavi
- Recupero di una policy delle chiavi
- Impostazione di una policy delle chiavi

Elenco dei nomi delle policy delle chiavi

Per ottenere i nomi delle politiche chiave per anAWS KMS key, usa l'ListKeyPoliciesoperazione. L'unico nome della policy delle chiavi restituito è quello predefinito.

Nelle lingue che richiedono un oggetto client, questi esempi utilizzano l'oggetto client AWS KMS creato in Creazione di un client.

Java

Per i dettagli sull'implementazione di Java, consulta il listKeyPolicies metodo nell'AWS SDK for JavaAPI Reference.

```
// List key policies
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
```

```
ListKeyPoliciesRequest req = new ListKeyPoliciesRequest().withKeyId(keyId);
ListKeyPoliciesResult result = kmsClient.listKeyPolicies(req);
```

C#

Per maggiori dettagli, consultare il metodo ListKeyPolicies in AWS SDK for .NET.

```
// List key policies
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

ListKeyPoliciesRequest listKeyPoliciesRequest = new ListKeyPoliciesRequest()
{
    KeyId = keyId
};
ListKeyPoliciesResponse listKeyPoliciesResponse =
 kmsClient.ListKeyPolicies(listKeyPoliciesRequest);
```

Python

Per maggiori dettagli, consultare il metodo `list_key_policies` in AWS SDK for Python (Boto3).

```
# List key policies

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

response = kms_client.list_key_policies(
    KeyId=key_id
)
```

Ruby

Per maggiori dettagli, consultare il metodo dell'istanza `list_key_policies` in AWS SDK for Ruby.

```
# List key policies
```

```
# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

response = kmsClient.list_key_policies({
  key_id: key_id
})
```

PHP

Per maggiori dettagli, consultare il metodo ListKeyPolicies in AWS SDK for PHP.

```
// List key policies
//
// Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';

$result = $KmsClient->listKeyPolicies([
    'KeyId' => $keyId
]);
```

Node.js

Per i dettagli, consultate la listKeyPolicies proprietà nell'AWSSDK di JavaScript Node.js.

```
// List key policies
//
// Replace the following example key ARN with a valid key ID or key ARN
const KeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';

kmsClient.listKeyPolicies({ KeyId }, (err, data) => {
  ...
});
```

PowerShell

Per elencare il nome della politica di chiave predefinita, utilizzare il cmdlet KeyPolicyList Get-KMS.

```
# List key policies
```

```
# Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
$response = Get-KMSKeyPolicyList -KeyId $keyId
```

Per utilizzare i AWS KMS PowerShell cmdlet, installa AWS.Tools.KeyManagementServicemodulo. Per ulteriori informazioni, consulta la AWS Tools for Windows PowerShellGuida per l'utente.

Recupero di una policy delle chiavi

Per ottenere la politica chiave per anAWS KMS key, usa l'GetKeyPolicyoperazione.

GetKeyPolicy richiede un nome di politica. L'unico nome valido per la policy è quello predefinito.

Nelle lingue che richiedono un oggetto client, questi esempi utilizzano l'oggetto client AWS KMS creato in Creazione di un client.

Java

Per i dettagli, consulta il getKeyPolicy metodo nell'AWS SDK for JavaAPI Reference.

```
// Get the policy for a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
String policyName = "default";

GetKeyPolicyRequest req = new
 GetKeyPolicyRequest().withKeyId(keyId).withPolicyName(policyName);
GetKeyPolicyResult result = kmsClient.getKeyPolicy(req);
```

C#

Per maggiori dettagli, consultare il metodo GetKeyPolicy in AWS SDK for .NET.

```
// Get the policy for a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
```

```
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
String policyName = "default";

GetKeyPolicyRequest getKeyPolicyRequest = new GetKeyPolicyRequest()
{
    KeyId = keyId,
    PolicyName = policyName
};
GetKeyPolicyResponse getKeyPolicyResponse =
 kmsClient.GetKeyPolicy(getKeyPolicyRequest);
```

Python

Per maggiori dettagli, consultare il metodo `get_key_policy` in AWS SDK for Python (Boto3).

```
# Get the policy for a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
policy_name = 'default'

response = kms_client.get_key_policy(
    KeyId=key_id,
    PolicyName=policy_name
)
```

Ruby

Per maggiori dettagli, consultare il metodo dell'istanza `get_key_policy` in AWS SDK for Ruby.

```
# Get the policy for a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
policy_name = 'default'

response = kmsClient.get_key_policy({
  key_id: key_id,
  policy_name: policy_name
})
```

PHP

Per maggiori dettagli, consultare il metodo GetKeyPolicy in AWS SDK for PHP.

```
// Get the policy for a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
$policyName = "default";

$result = $KmsClient->getKeyPolicy([
    'KeyId' => $keyId,
    'PolicyName' => $policyName
]);
```

Node.js

Per i dettagli, consultate la getKeyPolicy proprietà nell'AWSSDK per JavaScript Node.js.

```
// Get the policy for a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
const KeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
const PolicyName = 'default';
kmsClient.getKeyPolicy({ KeyId, PolicyName }, (err, data) => {
  ...
});
```

PowerShell

Per ottenere la politica chiave per una chiave KMS, utilizzare il cmdlet KeyPolicy Get-KMS. Questo cmdlet restituisce la politica chiave come stringa (System.String) che è possibile utilizzare in un comando Write-KMS (). KeyPolicy `PutKeyPolicy` Per convertire le politiche nella stringa JSON in oggetti, utilizzare il cmdlet -JSON. `PSCustomObject` ConvertFrom

```
# Get the policy for a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
$policyName = 'default'
```

```
$response = Get-KMSKeyPolicy -KeyId $keyId -PolicyName $policyName
```

Per utilizzare i AWS KMS PowerShell cmdlet, installa AWS.Tools.KeyManagementServicemodulo. Per ulteriori informazioni, consulta la AWS Tools for Windows PowerShellGuida per l'utente.

Impostazione di una policy delle chiavi

Per creare o sostituire la politica chiave per una chiave KMS, usa l'PutKeyPolicyoperazione.

`PutKeyPolicy` richiede un nome per la policy. L'unico nome valido per la policy è quello predefinito.

Nelle lingue che richiedono un oggetto client, questi esempi utilizzano l'oggetto client AWS KMS creato in Creazione di un client.

Java

Per i dettagli, consulta il putKeyPolicy metodo nell'AWS SDK for JavaAPI Reference.

```
// Set a key policy for a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
String policyName = "default";
String policy = "{" +
                "  \"Version\": \"2012-10-17\"," +
                "  \"Statement\": [{" +
                "    \"Sid\": \"Allow access for ExampleRole\"," +
                "    \"Effect\": \"Allow\"," +
                // Replace the following example user ARN with a valid one
                "    \"Principal\": {\"AWS\": \"arn:aws:iam::111122223333:role/
ExampleKeyUserRole\"}," +
                "    \"Action\": [" +
                "      \"kms:Encrypt\"," +
                "      \"kms:GenerateDataKey*\"," +
                "      \"kms:Decrypt\"," +
                "      \"kms:DescribeKey\"," +
                "      \"kms:ReEncrypt*\"" +
                "    ]," +
                "    \"Resource\": \"*\"" +
```

```
                "  }]" +
                "}";

PutKeyPolicyRequest req = new
 PutKeyPolicyRequest().withKeyId(keyId).withPolicy(policy).withPolicyName(policyName);
kmsClient.putKeyPolicy(req);
```

C#

Per maggiori dettagli, consultare il metodo PutKeyPolicy in AWS SDK for .NET.

```
// Set a key policy for a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
String policyName = "default";
String policy = "{" +
                "  \"Version\": \"2012-10-17\"," +
                "  \"Statement\": [{" +
                "    \"Sid\": \"Allow access for ExampleUser\"," +
                "    \"Effect\": \"Allow\"," +
                // Replace the following example user ARN with a valid one
                "    \"Principal\": {\"AWS\": \"arn:aws:iam::111122223333:role/
ExampleKeyUserRole\"}," +
                "    \"Action\": [" +
                "      \"kms:Encrypt\"," +
                "      \"kms:GenerateDataKey*\"," +
                "      \"kms:Decrypt\"," +
                "      \"kms:DescribeKey\"," +
                "      \"kms:ReEncrypt*\"" +
                "    ]," +
                "    \"Resource\": \"*\"" +
                "  }]" +
                "}";

PutKeyPolicyRequest putKeyPolicyRequest = new PutKeyPolicyRequest()
{
    KeyId = keyId,
    Policy = policy,
    PolicyName = policyName
};
kmsClient.PutKeyPolicy(putKeyPolicyRequest);
```

Python

Per maggiori dettagli, consultare il metodo put_key_policy in AWS SDK for Python (Boto3).

```
# Set a key policy for a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
policy_name = 'default'
policy = """
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "Allow access for ExampleUser",
        "Effect": "Allow",
        "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleKeyUserRole"},
        "Action": [
            "kms:Encrypt",
            "kms:GenerateDataKey*",
            "kms:Decrypt",
            "kms:DescribeKey",
            "kms:ReEncrypt*"
        ],
        "Resource": "*"
    }]
}"""

response = kms_client.put_key_policy(
    KeyId=key_id,
    Policy=policy,
    PolicyName=policy_name
)
```

Ruby

Per maggiori dettagli, consultare il metodo dell'istanza put_key_policy in AWS SDK for Ruby.

```
# Set a key policy for a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
policy_name = 'default'
```

```
policy = "{" +
  "  \"Version\": \"2012-10-17\"," +
  "  \"Statement\": [{" +
  "    \"Sid\": \"Allow access for ExampleUser\"," +
  "    \"Effect\": \"Allow\"," +
  # Replace the following example user ARN with a valid one
  "    \"Principal\": {\"AWS\": \"arn:aws:iam::111122223333:role/ExampleKeyUserRole
\"}," +
  "    \"Action\": [" +
  "      \"kms:Encrypt\"," +
  "      \"kms:GenerateDataKey*\"," +
  "      \"kms:Decrypt\"," +
  "      \"kms:DescribeKey\"," +
  "      \"kms:ReEncrypt*\"" +
  "    ]," +
  "    \"Resource\": \"*\"" +
  "  }]" +
  "}"

response = kmsClient.put_key_policy({
  key_id: key_id,
  policy: policy,
  policy_name: policy_name
})
```

PHP

Per maggiori dettagli, consultare il metodo PutKeyPolicy in AWS SDK for PHP.

```
// Set a key policy for a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
$policyName = "default";

$result = $KmsClient->putKeyPolicy([
    'KeyId' => $keyId,
    'PolicyName' => $policyName,
    'Policy' => '{
        "Version": "2012-10-17",
        "Id": "custom-policy-2016-12-07",
        "Statement": [
            { "Sid": "Enable IAM User Permissions",
```

```
            "Effect": "Allow",
            "Principal":
               { "AWS": "arn:aws:iam::111122223333:user/root" },
            "Action": [ "kms:*" ],
            "Resource": "*" },
            { "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal":
               { "AWS": "arn:aws:iam::111122223333:role/ExampleKeyUserRole" },
            "Action": [
                "kms:Encrypt*",
                "kms:GenerateDataKey*",
                "kms:Decrypt*",
                "kms:DescribeKey*",
                "kms:ReEncrypt*"
            ],
            "Resource": "*" }
        ]
    } '
]);
```

Node.js

Per i dettagli, consultate la putKeyPolicy proprietà nell'AWSSDK per JavaScript Node.js.

```
// Set a key policy for a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
const KeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
const PolicyName = 'default';
const Policy = `{
    "Version": "2012-10-17",
    "Id": "custom-policy-2016-12-07",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
```

```
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/ExampleKeyUserRole"
            },
            "Action": [
                "kms:Encrypt*",
                "kms:GenerateDataKey*",
                "kms:Decrypt*",
                "kms:DescribeKey*",
                "kms:ReEncrypt*"
            ],
            "Resource": "*"
        }
    ]
}`; // The key policy document

kmsClient.putKeyPolicy({ KeyId, Policy, PolicyName }, (err, data) => {
  ...
});
```

PowerShell

Per impostare una politica chiave per una chiave KMS, utilizzare il cmdlet KeyPolicyWrite-KMS. Questo cmdlet non restituisce alcun output. Per verificare l'efficacia del comando, utilizzare il cmdlet Get-KMS. KeyPolicy

Il parametro `Policy` accetta una stringa. Racchiudere la stringa tra virgolette singole per renderla una stringa letterale. Non è necessario utilizzare caratteri di continuazione o caratteri di escape nella stringa letterale.

```
# Set a key policy for a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
$policyName = 'default'
$policy = '{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
```

```
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/ExampleKeyUserRole"
            },
            "Action": [
                "kms:Encrypt*",
                "kms:GenerateDataKey*",
                "kms:Decrypt*",
                "kms:DescribeKey*",
                "kms:ReEncrypt*"
            ],
            "Resource": "*"
        }]
    }'

Write-KMSKeyPolicy -KeyId $keyId -PolicyName $policyName -Policy $policy
```

Per utilizzare i AWS KMS PowerShell cmdlet, installa AWS.Tools.KeyManagementServicemodulo. Per ulteriori informazioni, consulta la Guida per l'utente AWS Tools for Windows PowerShell.

Utilizzo delle concessioni

Gli esempi in questo argomento utilizzano l'API AWS KMS per creare, visualizzare, ritirare e revocare le concessioni su AWS KMS keys. Per ulteriori informazioni sull'utilizzo delle concessioni in AWS KMS, consulta Concessioni in AWS KMS.

Argomenti

- Creazione di una concessione
- Visualizzazione di una concessione
- Ritiro di una concessione

- Revoca di una concessione

Creazione di una concessione

Per creare una sovvenzione per unAWS KMS key, usa l'CreateGrantoperazione. La risposta include solo l'ID e il token della concessione. Per ottenere informazioni dettagliate sulla sovvenzione, utilizzate l'ListGrantsoperazione, come illustrato inVisualizzazione di una concessione.

Questi esempi creano una concessione che consente agli utenti che possono assumere il `ExampleKeyUser` ruolo di richiamare l'GenerateDataKeyoperazione sulla chiave KMS identificata dal `KeyId` parametro.

Nelle lingue che richiedono un oggetto client, questi esempi utilizzano l'oggetto client AWS KMS creato in Creazione di un client.

Java

Per ulteriori informazioni, consulta il metodo createGrant nella Documentazione di riferimento dell'API AWS SDK for Java.

```
// Create a grant
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
String granteePrincipal = "arn:aws:iam::111122223333:role/ExampleKeyUser";
String operation = GrantOperation.GenerateDataKey.toString();

CreateGrantRequest request = new CreateGrantRequest()
    .withKeyId(keyId)
    .withGranteePrincipal(granteePrincipal)
    .withOperations(operation);

CreateGrantResult result = kmsClient.createGrant(request);
```

C#

Per maggiori dettagli, consultare il metodo CreateGrant in AWS SDK for .NET.

```
// Create a grant
//
// Replace the following example key ARN with a valid key ID or key ARN
```

```
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
String granteePrincipal = "arn:aws:iam::111122223333:role/ExampleKeyUser";
String operation = GrantOperation.GenerateDataKey;

CreateGrantRequest createGrantRequest = new CreateGrantRequest()
{
    KeyId = keyId,
    GranteePrincipal = granteePrincipal,
    Operations = new List<string>() { operation }
};

CreateGrantResponse createGrantResult = kmsClient.CreateGrant(createGrantRequest);
```

Python

Per maggiori dettagli, consultare il metodo `create_grant` in AWS SDK for Python (Boto3).

```
# Create a grant

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
grantee_principal = 'arn:aws:iam::111122223333:role/ExampleKeyUser'
operation = ['GenerateDataKey']

response = kms_client.create_grant(
    KeyId=key_id,
    GranteePrincipal=grantee_principal,
    Operations=operation
)
```

Ruby

Per maggiori dettagli, consultare il metodo dell'istanza `create_grant` in AWS SDK for Ruby.

```
# Create a grant

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
grantee_principal = 'arn:aws:iam::111122223333:role/ExampleKeyUser'
operation = ['GenerateDataKey']
```

```
response = kmsClient.create_grant({
  key_id: key_id,
  grantee_principal: grantee_principal,
  operations: operation
})
```

PHP

Per maggiori dettagli, consultare il metodo CreateGrant in AWS SDK for PHP.

```
// Create a grant
//
// Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
$granteePrincipal = "arn:aws:iam::111122223333:role/ExampleKeyUser";
$operation = ['GenerateDataKey']

$result = $KmsClient->createGrant([
    'GranteePrincipal' => $granteePrincipal,
    'KeyId' => $keyId,
    'Operations' => $operation
]);
```

Node.js

Per i dettagli, vedete la proprietà CreateGrant nell'SDK JavaScript per AWS Node.js.

```
// Create a grant
//
// Replace the following example key ARN with a valid key ID or key ARN
const KeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
const GranteePrincipal = 'arn:aws:iam::111122223333:role/ExampleKeyUser';
const Operations: ["GenerateDataKey"];
kmsClient.createGrant({ KeyId, GranteePrincipal, Operations }, (err, data) => {
  ...
});
```

PowerShell

Per creare una concessione, utilizzare il cmdlet New-KMSGrant.

```
# Create a grant

# Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
$granteePrincipal = 'arn:aws:iam::111122223333:role/ExampleKeyUser'
$operation = 'GenerateDataKey'

$response = New-KMSGrant -GranteePrincipal $granteePrincipal -KeyId $keyId -
Operation $operation
```

Per utilizzare i AWS KMS PowerShell cmdlet, installa AWS.Tools.KeyManagementServicemodulo. Per ulteriori informazioni, consulta la AWS Tools for Windows PowerShellGuida per l'utente.

Visualizzazione di una concessione

Per ottenere informazioni dettagliate sulle sovvenzioni su una chiave KMS, usa l'ListGrantsoperazione.

> **Note**
>
> Il campo `GranteePrincipal` nella risposta `ListGrants` contiene solitamente il principal dell'assegnatario della concessione. Tuttavia, quando il principale dell'assegnatario della concessione è un servizio AWS, il campo `GranteePrincipal` contiene il principale del servizio, che potrebbe rappresentare più principali dell'assegnatario diversi.

Nelle lingue che richiedono un oggetto client, questi esempi utilizzano l'oggetto client AWS KMS creato in Creazione di un client.

Questi esempi utilizzano il parametro `Limits` opzionale che determina il numero di concessioni restituite dall'operazione.

Java

Per ulteriori informazioni sull'implementazione Java, consulta il metodo listGrants nella Documentazione di riferimento dell'API AWS SDK for Java.

```
// Listing grants on a KMS key
```

```
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
Integer limit = 10;

ListGrantsRequest req = new ListGrantsRequest().withKeyId(keyId).withLimit(limit);
ListGrantsResult result = kmsClient.listGrants(req);
```

C#

Per maggiori dettagli, consultare il metodo ListGrants in AWS SDK for .NET.

```
// Listing grants on a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
int limit = 10;

ListGrantsRequest listGrantsRequest = new ListGrantsRequest()
{
    KeyId = keyId,
    Limit = limit
};
ListGrantsResponse listGrantsResponse = kmsClient.ListGrants(listGrantsRequest);
```

Python

Per maggiori dettagli, consultare il metodo `list_grants` in AWS SDK for Python (Boto3).

```
# Listing grants on a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

response = kms_client.list_grants(
    KeyId=key_id,
    Limit=10
)
```

Ruby

Per maggiori dettagli, consultare il metodo dell'istanza `list_grants` in AWS SDK for Ruby.

```
# Listing grants on a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

response = kmsClient.list_grants({
  key_id: key_id,
  limit: 10
})
```

PHP

Per maggiori dettagli, consultare il metodo ListGrants in AWS SDK for PHP.

```
// Listing grants on a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
$limit = 10;

$result = $KmsClient->listGrants([
    'KeyId' => $keyId,
    'Limit' => $limit,
]);
```

Node.js

Per i dettagli, vedete la proprietà ListGrants nell'SDK JavaScript per in AWS Node.js.

```
// Listing grants on a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
const KeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
const Limit = 10;
kmsClient.listGrants({ KeyId, Limit }, (err, data) => {
  ...
```

```
});
```

PowerShell

Per visualizzare i dettagli di tutte le AWS KMS concessioni per una chiave KMS, utilizzare il cmdlet Get-KMS. GrantList

Per limitare il numero di oggetti di output, in questo esempio viene utilizzato il cmdlet Select-Object anziché il parametro `Limit`, che viene considerato obsoleto nei cmdlet list. Per informazioni sull'impaginazione dell'output in AWS Tools for PowerShell, consulta Paginazione output con AWS Tools for PowerShell.

```
# Listing grants on a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
$limit = 10

$response = Get-KMSGrantList -KeyId $keyId | Select-Object -First $limit
```

Per utilizzare i cmdlet, installa AWS.Tools. AWS KMS PowerShell KeyManagementServicemodulo. Per ulteriori informazioni, consulta la AWS Tools for Windows PowerShellGuida per l'utente.

È necessario specificare la chiave KMS chiave in ogni operazione `ListGrants`. Tuttavia, è possibile filtrare ulteriormente l'elenco delle concessioni specificando l'ID di concessione o un assegnatario principale. Negli esempi seguenti vengono ottenute solo le concessioni per una chiave KMS in cui il ruolo `test-engineer` è l'assegnatario principale.

Java

Per ulteriori informazioni sull'implementazione Java, consulta il metodo listGrants nella Documentazione di riferimento dell'API AWS SDK for Java.

```
// Listing grants on a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
```

```
String grantee = "arn:aws:iam::111122223333:role/test-engineer";

ListGrantsRequest req = new
 ListGrantsRequest().withKeyId(keyId).withGranteePrincipal(grantee);
ListGrantsResult result = kmsClient.listGrants(req);
```

C#

Per maggiori dettagli, consultare il metodo ListGrants in AWS SDK for .NET.

```
// Listing grants on a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
String grantee = "arn:aws:iam::111122223333:role/test-engineer";

ListGrantsRequest listGrantsRequest = new ListGrantsRequest()
{
    KeyId = keyId,
    GranteePrincipal = grantee
};
ListGrantsResponse listGrantsResponse = kmsClient.ListGrants(listGrantsRequest);
```

Python

Per maggiori dettagli, consultare il metodo `list_grants` in AWS SDK for Python (Boto3).

```
# Listing grants on a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
grantee = 'arn:aws:iam::111122223333:role/test-engineer'

response = kms_client.list_grants(
    KeyId=key_id,
    GranteePrincipal=grantee
)
```

Ruby

Per maggiori dettagli, consultare il metodo dell'istanza `list_grants` in AWS SDK for Ruby.

```
# Listing grants on a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
grantee = 'arn:aws:iam::111122223333:role/test-engineer'

response = kmsClient.list_grants({
  key_id: keyId,
  grantee_principal: grantee
})
```

PHP

Per maggiori dettagli, consultare il metodo ListGrants in AWS SDK for PHP.

```
// Listing grants on a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
$grantee = 'arn:aws:iam::111122223333:role/test-engineer';

$result = $KmsClient->listGrants([
    'KeyId' => $keyId,
    'GranteePrincipal' => $grantee,
]);
```

Node.js

Per i dettagli, vedete la proprietà ListGrants nell'SDK JavaScript per in AWS Node.js.

```
// Listing grants on a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
const KeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
const Grantee = 'arn:aws:iam::111122223333:role/test-engineer';

kmsClient.listGrants({ KeyId, Grantee }, (err, data) => {
  ...
});
```

PowerShell

Per visualizzare i dettagli di tutte le AWS KMS concessioni per una chiave KMS, utilizzare il cmdlet Get-KMS. GrantList

```
# Listing grants on a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
$grantee = 'arn:aws:iam::111122223333:role/test-engineer'
$response = Get-KMSGrantList -KeyId $keyId -GranteePrincipal $grantee
```

Per utilizzare i cmdlet, installa AWS.Tools. AWS KMS PowerShell KeyManagementServicemodulo. Per ulteriori informazioni, consulta la AWS Tools for Windows PowerShellGuida per l'utente.

Ritiro di una concessione

Per ritirare una concessione per una chiave KMS, usa l'RetireGrantoperazione. È consigliabile ritirare una concessione dopo aver terminato il suo utilizzo.

Per ritirare una concessione specifica il token di concessione oppure sia l'ID di concessione che l'ID chiave della chiave KMS. Per questa operazione, l'ID della chiave KMS deve essere l'Amazon Resource Name (ARN) della chiave KMS. Il token di concessione viene restituito dall'CreateGrantoperazione. L'ID della concessione viene restituito dalle ListGrantsoperazioni CreateGrant and.

RetireGrant non restituisce una risposta. Per verificare che sia efficace, usa l'ListGrantsoperazione.

Nelle lingue che richiedono un oggetto client, questi esempi utilizzano l'oggetto client AWS KMS creato in Creazione di un client.

Java

Per ulteriori informazioni, consulta il metodo retireGrant nella Documentazione di riferimento dell'API AWS SDK for Java.

```
// Retire a grant
```

```
//
String grantToken = Place your grant token here;

RetireGrantRequest req = new RetireGrantRequest().withGrantToken(grantToken);
kmsClient.retireGrant(req);
```

C#

Per maggiori dettagli, consultare il metodo RetireGrant in AWS SDK for .NET.

```
// Retire a grant
//
String grantToken = "Place your grant token here";

RetireGrantRequest retireGrantRequest = new RetireGrantRequest()
{
    GrantToken = grantToken
};
kmsClient.RetireGrant(retireGrantRequest);
```

Python

Per maggiori dettagli, consultare il metodo `retire_grant` in AWS SDK for Python (Boto3).

```
# Retire a grant

grant_token = Place your grant token here

response = kms_client.retire_grant(
    GrantToken=grant_token
)
```

Ruby

Per maggiori dettagli, consultare il metodo dell'istanza `retire_grant` in AWS SDK for Ruby.

```
# Retire a grant

grant_token = Place your grant token here

response = kmsClient.retire_grant({
  grant_token: grant_token
```

```
})
```

PHP

Per maggiori dettagli, consultare il metodo RetireGrant in AWS SDK for PHP.

```
// Retire a grant
//
$grantToken = 'Place your grant token here';

$result = $KmsClient->retireGrant([
    'GrantToken' => $grantToken,
]);
```

Node.js

Per i dettagli, vedete la proprietà RetireGrant nell'SDK JavaScript per in AWS Node.js.

```
// Retire a grant
//
const GrantToken = 'Place your grant token here';
kmsClient.retireGrant({ GrantToken }, (err, data) => {
  ...
});
```

PowerShell

Per ritirare una concessione, utilizzare il cmdlet Disable-KMSGrant. Per ottenere il token di concessione, utilizzare il cmdlet New-KMSGrant. Il parametro `GrantToken` accetta una stringa, quindi non è necessario convertire l'output restituito dal cmdlet Read-Host.

```
# Retire a grant

$grantToken = Read-Host -Message Place your grant token here
Disable-KMSGrant -GrantToken $grantToken
```

Per utilizzare i AWS KMS PowerShell cmdlet, installa AWS.Tools.KeyManagementServicemodulo. Per ulteriori informazioni, consulta la AWS Tools for Windows PowerShellGuida per l'utente.

Revoca di una concessione

Per revocare una concessione a una chiave KMS, usa l'operazione. RevokeGrant Puoi revocare una concessione per negare esplicitamente le operazioni che dipendono da essa.

Nelle lingue che richiedono un oggetto client, questi esempi utilizzano l'oggetto client AWS KMS creato in Creazione di un client.

Java

Per ulteriori informazioni, consulta il metodo revokeGrant nella Documentazione di riferimento dell'API AWS SDK for Java.

```
// Revoke a grant on a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

// Replace the following example grant ID with a valid one
String grantId = "grant1";

RevokeGrantRequest req = new
 RevokeGrantRequest().withKeyId(keyId).withGrantId(grantId);
kmsClient.revokeGrant(req);
```

C#

Per maggiori dettagli, consultare il metodo RevokeGrant in AWS SDK for .NET.

```
// Revoke a grant on a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

// Replace the following example grant ID with a valid one
String grantId = "grant1";

RevokeGrantRequest revokeGrantRequest = new RevokeGrantRequest()
{
    KeyId = keyId,
```

```
    GrantId = grantId
};
kmsClient.RevokeGrant(revokeGrantRequest);
```

Per utilizzare i AWS KMS PowerShell cmdlet, installa AWS.Tools.KeyManagementServicemodulo. Per ulteriori informazioni, consulta la AWS Tools for Windows PowerShellGuida per l'utente.

Python

Per maggiori dettagli, consultare il metodo `revoke_grant` in AWS SDK for Python (Boto3).

```
# Revoke a grant on a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

# Replace the following example grant ID with a valid one
grant_id = 'grant1'

response = kms_client.revoke_grant(
    KeyId=key_id,
    GrantId=grant_id
)
```

Ruby

Per maggiori dettagli, consultare il metodo dell'istanza `revoke_grant` in AWS SDK for Ruby.

```
# Revoke a grant on a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

# Replace the following example grant ID with a valid one
grant_id = 'grant1'

response = kmsClient.revoke_grant({
  key_id: key_id,
  grant_id: grant_id
})
```

PHP

Per maggiori dettagli, consultare il metodo RevokeGrant in AWS SDK for PHP.

```
// Revoke a grant on a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';

// Replace the following example grant ID with a valid one
$grantId = "grant1";

$result = $KmsClient->revokeGrant([
    'KeyId' => $keyId,
    'GrantId' => $grantId,
]);
```

Node.js

Per i dettagli, vedete la proprietà Revokegrant nell'AWSSDK per Node.js. JavaScript

```
// Revoke a grant on a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
const KeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';

// Replace the following example grant ID with a valid one
const GrantId = 'grant1';
kmsClient.revokeGrant({ GrantId, KeyId }, (err, data) => {
  ...
});
```

PowerShell

Per revocare una concessione, utilizzare il cmdlet Revoke-KMSGrant.

```
# Revoke a grant on a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
```

```
# Replace the following example grant ID with a valid one
$grantId = 'grant1'

Revoke-KMSGrant -KeyId $keyId -GrantId $grantId
```

Per utilizzare i AWS KMS PowerShell cmdlet, installa AWS.Tools.KeyManagementServicemodulo. Per ulteriori informazioni, consulta la Guida per l'utente AWS Tools for Windows PowerShell.

Test delle chiamate API AWS KMS

Per utilizzare AWS KMS, devi disporre di credenziali che AWS può utilizzare per autenticare le richieste API. Le credenziali devono includere l'autorizzazione per accedere alle chiavi KMS e agli alias. Le autorizzazioni sono determinate dalle policy delle chiavi, dalle policy IAM, dalle concessioni e dai controlli di accesso multi-account. Oltre a controllare l'accesso alle chiavi KMS, puoi controllare l'accesso al tuo CloudHSM e ai tuoi archivi di chiavi personalizzate.

Puoi specificare il parametro dell'API `DryRun` per controllare se disponi delle autorizzazioni necessarie a utilizzare le chiavi AWS KMS. Puoi utilizzare anche `DryRun` per controllare se i parametri della richiesta in una chiamata API AWS KMS sono specificati correttamente.

Argomenti

- Qual è il DryRun parametro?
- Specificazione DryRun con l'API

Qual è il DryRun parametro?

`DryRun` è un parametro dell'API opzionale specificato per controllare se l'esito delle chiamate API AWS KMS sarà positivo. Usa `DryRun` per testare la chiamata API, prima di effettuare realmente la chiamata a AWS KMS. Puoi effettuare i controlli seguenti:

- che disponi delle autorizzazioni necessarie per utilizzare le chiavi AWS KMS;
- che hai specificato correttamente i parametri nella chiamata.

AWS KMS supporta l'utilizzo del parametro `DryRun` in determinate azioni dell'API:

- CreateGrant
- Decrypt
- Encrypt
- GenerateDataKey
- GenerateDataKeyPair
- GenerateDataKeyPairWithoutPlaintext
- GenerateDataKeyWithoutPlaintext
- GenerateMac
- ReEncrypt
- RetireGrant
- RevokeGrant
- Sign
- Verify
- VerifyMac

L'utilizzo del parametro `DryRun` comporterà dei costi e verrà fatturato come richiesta API standard. Per ulteriori informazioni sui prezzi di AWS KMS, consulta Prezzi di AWS Key Management Service.

Tutte le richieste API con il parametro `DryRun` si applicano alla quota della richiesta API e possono comportare un'eccezione di limitazione della larghezza di banda della rete se superi la quota della richiesta API. Ad esempio, la chiamata Decrypt con `DryRun` o senza `DryRun` viene conteggiata sulla stessa quota delle operazioni crittografiche. Per ulteriori informazioni, consulta Limitazione delle richieste AWS KMS.

Ogni chiamata indirizzata a un'operazione dell'API AWS KMS viene acquisita come evento e registrata in un log di AWS CloudTrail. L'output di tutte le operazioni che specificano il `DryRun` parametro viene visualizzato nel CloudTrail registro. Per ulteriori informazioni, consulta Registrazione delle chiamate API AWS KMS con AWS CloudTrail.

Specificazione DryRun con l'API

Per utilizzare `DryRun`, specifica il parametro `–dry-run` nei comandi della AWS CLI e nelle chiamate API AWS KMS che supportano il parametro. In tal modo, AWS KMS controllerà se l'esito della chiamata sarà positivo. L'esito delle chiamate AWS KMS che utilizzano `DryRun` sarà sempre

negativo e verrà restituito un messaggio con informazioni sul motivo dell'esito negativo della chiamata. Il messaggio può includere le seguenti eccezioni:

- `DryRunOperationException`: l'esito della richiesta sarebbe stato positivo se non fosse stato specificato `DryRun`.
- `ValidationException`: l'esito della richiesta è negativo perché è stato specificato un parametro dell'API errato.
- `AccessDeniedException`: non disponi delle autorizzazioni per l'esecuzione dell'azione dell'API specificata sulla risorsa KMS.

Ad esempio, il comando seguente utilizza l'CreateGrantoperazione e crea una concessione che consente agli utenti autorizzati ad assumere il `keyUserRole` ruolo di chiamare l'operazione Decrypt su una chiave KMS simmetrica specificata. Il parametro `DryRun` è specificato.

```
$  aws kms create-grant \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/keyUserRole \
    --operations Decrypt \
    --dry-run
```

Consistenza finale di AWS KMS

L'API AWS KMS segue un modello di consistenza finale dovuto alla natura distribuita del sistema. Di conseguenza, le modifiche alle risorse AWS KMS potrebbero non essere immediatamente visibili ai successivi comandi eseguiti.

Quando esegui chiamate API AWS KMS, potrebbe verificarsi un breve ritardo prima che la modifica sia disponibile in AWS KMS. Generalmente, occorrono pochissimi secondi per la propagazione della modifica in tutto il sistema, ma in alcuni casi possono essere necessari diversi minuti. Durante questo periodo, potrebbero verificarsi errori imprevisti, ad esempio `NotFoundException` o `InvalidStateException`. AWS KMS, ad esempio, potrebbe restituire `NotFoundException` se richiami `GetParametersForImport` subito dopo la chiamata `CreateKey`.

È consigliabile configurare una strategia di ripetizione dei tentativi sui tuoi client AWS KMS affinché le operazioni vengano ritentate automaticamente dopo un breve periodo di attesa. Per ulteriori informazioni, consulta Comportamento della ripetizione dei tentativi negli SDK AWS e nella Guida di riferimento degli strumenti.

Per le chiamate API correlate all'autorizzazione, puoi usare un token di concessione per evitare potenziali ritardi e utilizzare subito le autorizzazioni incluse in una concessione. Per ulteriori informazioni, consulta Consistenza finale (per concessioni).

Riferimenti

I seguenti riferimenti forniscono informazioni utili sull'utilizzo e sulla gestione delle chiavi KMS.

- Documentazione di riferimento dei tipi di chiave. Elenca il tipo di chiave KMS che supporta ciascuna operazione API AWS KMS.

  Per scoprire: è possibile abilitare e disabilitare una chiave KMS di firma RSA?

- Tabella dello stato delle chiavi. Mostra come lo stato chiave di una chiave KMS influisce sul suo utilizzo nelle operazioni API AWS KMS.

  Per scoprire: è possibile modificare l'alias di una chiave KMS in attesa di eliminazione?

- Documentazione di riferimento delle autorizzazioni dell'API AWS KMS. Fornisce informazioni sulle autorizzazioni richieste per ciascuna operazione dell'API AWS KMS.

  Per trovare: Posso eseguire GetKeyPolicyl'esecuzione con una chiave in un altro AWS account? È possibile concedere l'autorizzazione `kms:Decrypt` in una policy IAM?

  - ViaService riferimento. Elenca i servizi AWS che supportano la chiave di condizione `kms:ViaService`.

    Per trovare: posso utilizzare la chiave di `kms:ViaService` condizione per consentire un'autorizzazione solo quando proviene da Amazon ElastiCache? E per Amazon Neptune?

- Prezzi di AWS KMS. Elenca e spiega il prezzo delle chiavi KMS.

  Per scoprire: quanto costa usare le chiavi asimmetriche?

- Quote di richieste AWS KMS. Elenca le quote al secondo per le richieste API AWS KMS in ogni account e Regione.

  Per scoprire: quante richieste Decrypt possono essere eseguite al secondo? Quante richieste Decrypt richieste possono essere eseguite sulle chiavi KMS in un archivio chiavi personalizzate?

- Quote di risorse AWS KMS. Elenca le quote delle risorse AWS KMS.

  Per scoprire: quante chiavi KMS è possibile avere in ogni Regione dell'account? Quanti alias è possibile avere su ogni chiave KMS?

- Servizi AWS integrati con AWS KMS. Elenca i servizi AWS che utilizzano le chiavi KMS per proteggere le risorse che creano, archiviano e gestiscono.

Per scoprire: Amazon Connect utilizza le chiavi KMS per proteggere le risorse Connect?

Cronologia dei documenti

Questo argomento descrive gli aggiornamenti importanti alla Guida per gli sviluppatori di AWS Key Management Service.

Argomenti

Aggiornamenti recenti

La tabella seguente descrive le modifiche importanti apportate a questa documentazione a partire da gennaio 2018. Oltre alle modifiche maggiori elencate qui, aggiorniamo la documentazione di frequente per migliorare le descrizioni e gli esempi e per dar spazio al feedback inviatoci. Per ricevere una notifica sulle modifiche rilevanti, iscriversi al feed RSS.

Potrebbe essere necessario scorrere orizzontalmente o verticalmente per visualizzare tutti i dati di questa tabella.

Modifica	Descrizione	Data
Aggiornamenti alla politica gestita	Sono state aggiunte nuove autorizzazioni `AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy` che consentono di AWS KMS monitorare le modifiche nel VPC che contiene AWS CloudHSM il cluster in modo da AWS KMS fornire messaggi di errore chiari in caso di errori.	10 novembre 2023

Aggiornamento funzionalità	È stato aggiunto il supporto per il parametro dell'API `DryRun`.	5 luglio 2023
Aggiornamento funzionalità	È stato aggiunto il supporto per l'importazione del materiale della chiave per tutti i tipi di chiavi AWS KMS, ad eccezione degli archivi di chiavi personalizzate.	5 giugno 2023
Aggiornamento funzionalità	Aggiornamenti alle APi AWS KMS per enclavi Nitro	10 marzo 2023
Aggiornamento funzionalità	L'algoritmo di wrapping `RSAES_PKCS1_V1_5` è obsoleto. AWS KMS interromperà tutto il supporto per `RSAES_PKCS1_V1_5` entro il 1° ottobre 2023, in conformità alla guida alla gestione delle chiavi crittografiche del National Institute of Standards and Technology (NIST). Ti consigliamo di iniziare immediatamente a utilizzare un algoritmo di wrapping diverso.	28 febbraio 2023
Aggiornamento funzionalità	È stato aggiunto il supporto per gli archivi delle chiavi esterne, una funzionalità che consente di proteggere le risorse AWS utilizzando le chiavi crittografiche al di fuori di AWS.	29 novembre 2022

Modifica della quota	Aumento della quota delle risorse AWS KMS keys a 100.000 chiavi KMS in ogni account e regione.	8 luglio 2022
Aggiornamento funzionalità	Aggiunto il supporto per le chiavi KMS HMAC in più Regioni AWS	8 luglio 2022
Nuovo argomento	È stato aggiunto l'argomento Resilienza in AWS Key Management Service al capitolo Sicurezza della Guida per gli sviluppatori AWS KMS.	14 giugno 2022
Nuova caratteristica	È stato aggiunto il supporto per le chiavi AWS KMS e le operazioni API che generano e verificano i codici HMAC.	19 aprile 2022
Modifica della documentazione	Sostituzione del termine chiave master cliente (CMK) con AWS KMS key e chiave KMS.	30 agosto 2021
Nuova caratteristica	Aggiunto il supporto per le chiavi multi-regione, un insieme di chiavi KMS interoperabili in diverse Regioni con lo stesso ID chiave e materiale chiave. È possibile utilizzare le chiavi multi-regione per crittografare i dati in una Regione e decrittografare i dati in una Regione diversa.	8 giugno 2021

Nuova caratteristica	È stato aggiunto il supporto per il controllo degli accessi basato sugli attributi (ABAC). Puoi utilizzare i tag e gli alias per controllare l'accesso alle AWS KMS keys.	17 dicembre 2020
Nuova caratteristica	Aggiunto il supporto per le policy di endpoint VPC.	9 luglio 2020
Nuovo contenuto	Spiega le proprietà di sicurezza di AWS KMS.	18 giugno 2020
Nuova caratteristica	Aggiunto il supporto per le chiavi di dati asimmetriche e le AWS KMS keys asimmetriche.	25 novembre 2019
Funzionalità aggiornata	Puoi visualizzare le policy chiavi delle Chiavi gestite da AWS nella console AWS KMS. Questa funzione era limitata alle chiavi gestite dal cliente.	15 novembre 2019
Nuova caratteristica	Illustra utilizzare gli algoritmi di scambio di chiavi post-quantistiche ibride in TLS per le chiamate a AWS KMS.	4 novembre 2019
Modifica della quota	Aumentate le quote di risorse per alcune API che gestiscono le chiavi KMS.	18 settembre 2019
Modifica della quota	Modificate le quote di risorse per le chiavi KMS, gli alias e le concessioni per ogni chiave KMS.	27 marzo 2019

Modifica della quota	Modificata la quota di richieste al secondo condivisa per le operazioni di crittografia che utilizzano le AWS KMS keys in un archivio delle chiavi personalizzate.	7 marzo 2019
Nuova caratteristica	Illustra come creare e amministrare archivi di chiavi personalizzate AWS KMS. Ogni store delle chiavi è supportato da un cluster AWS CloudHSMche possiedi e controlli.	26 novembre 2018
Nuova console	Illustra come utilizzare la nuova console AWS KMS, che è indipendente dalla console IAM. La console originari aoriginalecone le relative istruzioni persul'usocome utilizzarla saranno disponibi li per un breve periodo di tempo per consentirti di acquisire familiarità con la nuova console.	7 novembre 2018
Modifica della quota	Modificate le quote di richieste condivise per l'uso delle AWS KMS keys.	21 agosto 2018
Nuovo contenuto	Illustra in che modo AWS Secrets Manager utilizza chiavi AWS KMS per crittogra fare il valore del segreto in un segreto.	13 luglio 2018

Nuovo contenuto	Illustra in che modo DynamoDB utilizza AWS KMS AWS KMS keys per supportare l'opzione di crittografia lato server.	23 maggio 2018
Nuova caratteristica	Illustra come utilizzare un endpoint privato nel VPC per connetterti direttamente a AWS KMS anziché tramite Internet.	22 gennaio 2018

Aggiornamenti precedenti

Nella tabella seguente sono descritte le modifiche importanti apportate alla Guida per sviluppatori di AWS Key Management Service prima del 2018.

Potrebbe essere necessario scorrere orizzontalmente o verticalmente per visualizzare tutti i dati di questa tabella.

Modifica	Descrizione	Data
Nuovo contenuto	È stata aggiunta la documentazione relativa a Chiavi di tagging.	15 febbraio 2017
Nuovo contenuto	È stata aggiunta la documentazione relativa a Monitoraggio di AWS KMS keys e a Monitoraggio con Amazon CloudWatch.	31 agosto 2016
Nuovo contenuto	È stata aggiunta la documentazione relativa a Materiale della chiave importato.	11 agosto 2016

Modifica	Descrizione	Data
Nuovo contenuto	È stata aggiunta la documentazione Policy IAM, Riferimento per le autorizzazioni e Chiavi di condizione.	5 luglio 2016
Update	Sono state aggiornate porzioni della documentazione nel capitolo Autenticazione e controllo degli accessi.	5 luglio 2016
Update	È stata aggiornata la pagina Quote per riflettere le nuove quote predefinite.	31 maggio 2016
Update	Aggiornata la pagina Quote per riflettere le nuove quote predefinite e aggiornata la documentazione token di concessione per migliorare la chiarezza e la precisione.	11 aprile 2016
Nuovo contenuto	È stata aggiunta la documentazione relativa a Autorizzazione per più principali IAM di accedere a una chiave KMS e a Utilizzo della condizione con indirizzo IP.	17 febbraio 2016
Update	Sono state aggiornate le pagine Policy delle chiavi in AWS KMS e Modifica di una policy delle chiavi per migliorarne la chiarezza e la precisione.	17 febbraio 2016

Modifica	Descrizione	Data
Update	Sono state aggiornate le pagine dell'argomento Gestione delle chiavi per migliorarne la chiarezza.	5 gennaio 2016
Nuovo contenuto	È stata aggiunta la documentazione relativa a Come AWS CloudTrail utilizza AWS KMS.	18 novembre 2015
Nuovo contenuto	Sono state aggiunte istruzioni per Modifica di una policy delle chiavi.	18 novembre 2015
Update	È stata aggiornata la documentazione relativa a Come Amazon Relational Database Service (Amazon RDS) usa AWS KMS.	18 novembre 2015
Nuovo contenuto	È stata aggiunta la documentazione relativa a Come si WorkSpaces usa AWS KMS.	6 novembre 2015
Update	È stata aggiornata la pagina Policy delle chiavi in AWS KMS per migliorarne la chiarezza.	22 ottobre 2015
Nuovo contenuto	È stata aggiunta la documentazione su Eliminazione di AWS KMS keys, inclusa la documentazione di supporto relativa a Creazione di un allarme e Stabilire l'utilizzo passato di una chiave KMS.	15 ottobre 2015

Modifica	Descrizione	Data
Nuovo contenuto	È stata aggiunta la documentazione relativa a Determinazione dell'accesso a una AWS KMS keys.	15 ottobre 2015
Nuovo contenuto	È stata aggiunta la documentazione relativa a Stati chiave delle chiavi AWS KMS.	15 ottobre 2015
Nuovo contenuto	È stata aggiunta la documentazione relativa a Come Amazon Simple Email Service (Amazon SES) usa AWS KMS.	1° ottobre 2015
Update	Aggiornata la pagina Quote per spiegare le nuove quote di richieste.	31 agosto 2015
Nuovo contenuto	Sono state aggiunte informazioni sui costi per l'utilizzo di AWS KMS. Consulta Prezzi di AWS KMS.	14 agosto 2015
Nuovo contenuto	Aggiunte le quote di richiesta a AWS KMS Quote.	11 giugno 2015
Nuovo contenuto	È stato aggiunto un nuovo codice Java di esempio che mostra l'utilizzo dell'operazione `UpdateAlias`. Per informazioni, consultare Aggiornamento di un alias.	1° giugno 2015

Modifica	Descrizione	Data
Aggiornamento	È stata spostata la tabella delle regioni AWS Key Management Service in Riferimenti generali di AWS.	29 maggio 2015
Nuovo contenuto	È stata aggiunta la documentazione relativa a Come Amazon EMR utilizza AWS KMS.	28 gennaio 2015
Nuovo contenuto	È stata aggiunta la documentazione relativa a Come WorkMail utilizza Amazon AWS KMS.	28 gennaio 2015
Nuovo contenuto	È stata aggiunta la documentazione relativa a Come Amazon Relational Database Service (Amazon RDS) usa AWS KMS.	6 gennaio 2015
Nuovo contenuto	È stata aggiunta la documentazione relativa a Come Amazon Elastic Transcoder utilizza AWS KMS.	24 novembre 2014
Nuova guida	Introduzione della Guida per gli sviluppatori di AWS Key Management Service.	12 novembre 2014

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.