AWS Key Management Service melhores práticas

AWS Recomendações

AWS Recomendações: AWS Key Management Service melhores práticas

Table of Contents

AWS Key Management Service melhores práticas

Amazon Web Services (colaboradores)

Março de 2025 (histórico do documento)

O AWS Key Management Service (AWS KMS) é um serviço gerenciado que facilita a criação e o controle de chaves criptográficas usadas para proteger seus dados. Este guia descreve como usar com eficiência AWS KMS e fornece as melhores práticas. Ele ajuda você a comparar as opções de configuração e escolher o melhor conjunto para suas necessidades.

Este guia inclui recomendações sobre como sua organização pode usar AWS KMS para proteger informações confidenciais e implementar a assinatura para vários casos de uso. Ele considera as recomendações atuais que usam as seguintes dimensões:

- Gerenciamento de chaves — opções de delegação para opções de gerenciamento e armazenamento de chaves
- Proteção de dados — Criptografar dados em seus próprios aplicativos em vez de Serviços da AWS fazer isso em seu nome
- Gerenciamento de acesso — Usando políticas AWS KMS chave e políticas AWS Identity and Access Management (IAM) para implementar controle de acesso baseado em função (RBAC) ou controle de acesso baseado em atributos (ABAC).
- Arquitetura de várias contas e várias regiões — recomendações para implantações em grande escala.
- Gerenciamento de faturamento e custos — Entendendo seu custo e uso e recomendações sobre formas de reduzir custos.
- Controles de detetive — Monitorando o status de suas chaves KMS, configurações de criptografia e dados criptografados.
- Resposta a incidentes — Corrigindo configurações incorretas que resultam em não conformidade com suas políticas de proteção de dados.

Resultados de negócios desejados

Seus dados são um ativo essencial e confidencial para sua empresa. Com AWS KMS, você gerencia as chaves criptográficas usadas para proteger e verificar seus dados. Você controla como seus dados são usados, quem tem acesso a eles e como eles são criptografados. Este guia tem como

objetivo ajudar desenvolvedores, administradores de sistemas e profissionais de segurança a implementar as melhores práticas de criptografia que ajudam a proteger dados confidenciais armazenados ou transmitidos por meio Serviços da AWS dele. Ao compreender e implementar as recomendações deste guia, você pode promover a confidencialidade e a integridade dos dados em todo o seu AWS ambiente. Você pode atender aos seus requisitos de proteção de dados, independentemente de esses requisitos serem formulados internamente ou se você tiver requisitos específicos para um programa de conformidade ou validação. Para obter mais informações sobre como você AWS KMS pode ajudar a proteger dados em seu AWS ambiente, consulte Usando AWS KMS criptografia Serviços da AWS na AWS KMS documentação.

Sobre AWS KMS keys

AWS Key Management Service (AWS KMS) permite criar chaves criptográficas que podem ser usadas nos dados que você passa para o serviço. O tipo de recurso principal é a chave KMS, da qual existem três tipos:

- Chaves simétricas do Advanced Encryption Standard (AES) — Essas são chaves de 256 bits usadas no modo Galois Counter Mode (GCM) do AES. Essas chaves fornecem criptografia e descriptografia autenticadas de dados com menos de 4 KB de tamanho. Esse é o tipo de chave mais comum. Ele é usado para proteger outras chaves de dados, como aquelas usadas em seus aplicativos ou para criptografar dados em seu nome. Serviços da AWS
- Chaves assimétricas de curva elíptica ou RSA — Essas teclas estão disponíveis em vários tamanhos e oferecem suporte a vários algoritmos. Dependendo do algoritmo, eles podem ser usados para criptografia e decodificação e para operações de assinatura e verificação.
- Chaves simétricas para realizar operações de código de autenticação de mensagem (HMAC) baseado em hash — Essas chaves são chaves de 256 bits usadas para operações de assinatura e verificação.

Não é possível exportar as chaves do KMS do serviço em texto simples. Eles são gerados e só podem ser usados nos módulos de segurança de hardware (HSMs) usados pelo serviço. Essa é uma propriedade de segurança fundamental AWS KMS para evitar o comprometimento de chaves. Nas regiões da China (Pequim) e China (Ningxia), elas HSMs são certificadas pela OSCCA. Em todas as outras regiões, os HSMs usados em AWS KMS são validados pelo programa FIPS 140 do NIST no nível de segurança 3. Para obter mais informações sobre design e controles AWS KMS que ajudam a proteger suas chaves, consulte Detalhes AWS Key Management Service criptográficos.

Você pode enviar dados AWS KMS usando vários criptográficos para realizar APIs operações de criptografia, descriptografia, assinatura ou verificação com chaves KMS. Você também pode optar por fazer com que uma chave KMS atue como uma chave de criptografia, que protege um tipo de chave chamado chave de dados. Uma chave de dados pode ser exportada AWS KMS para uso em seu aplicativo local ou uma AWS service (Serviço da AWS) que esteja protegendo dados em seu nome. O uso de chaves de dados é comum em todos os sistemas de gerenciamento de chaves e geralmente é chamado de criptografia de envelope. A criptografia de envelope permite que uma chave de dados seja usada no sistema remoto que está manipulando seus dados confidenciais, em vez de precisar enviá-los AWS KMS para criptografia diretamente sob uma chave KMS.

Para obter mais informações, consulte AWS KMS keysos fundamentos da AWS KMS criptografia na AWS KMS documentação.

Melhores práticas de gerenciamento de chaves para AWS KMS

Ao usar AWS Key Management Service (AWS KMS), há algumas decisões fundamentais de design que você deve tomar. Isso inclui o uso de um modelo centralizado ou descentralizado para gerenciamento e acesso de chaves, o tipo de chaves a serem usadas e o tipo de armazenamento de chaves a ser usado. As seções a seguir ajudam você a tomar decisões adequadas para sua organização e seus casos de uso. Esta seção termina com considerações importantes para desativar e excluir chaves KMS, incluindo ações que você deve tomar para ajudar a proteger seus dados e chaves.

Esta seção contém os seguintes tópicos:

- Escolha de um modelo centralizado ou descentralizado
- Escolha de chaves gerenciadas pelo cliente, chaves AWS gerenciadas ou chaves AWS próprias
- Escolhendo uma loja de AWS KMS chaves
- Excluindo e desativando chaves KMS

Escolha de um modelo centralizado ou descentralizado

AWS recomenda que você use várias Contas da AWS e gerencie essas contas como uma única organização em AWS Organizations. Há duas abordagens amplas para o gerenciamento AWS KMS keys em ambientes com várias contas.

A primeira abordagem é uma abordagem descentralizada, na qual você cria chaves em cada conta que usa essas chaves. Quando você armazena as chaves do KMS nas mesmas contas dos recursos que elas protegem, é mais fácil delegar permissões a administradores locais que entendem os requisitos de acesso para seus AWS diretores e chaves. Você pode autorizar o uso de chaves usando apenas uma política de chaves ou pode combinar uma política de chaves e políticas baseadas em identidade no AWS Identity and Access Management (IAM).

A segunda abordagem é uma abordagem centralizada, na qual você mantém as chaves KMS em uma ou algumas designadas. Contas da AWS Você permite que outras contas usem as chaves somente para operações criptográficas. Você gerencia as chaves, seu ciclo de vida e suas permissões a partir da conta centralizada. Você permite que outras Contas da AWS pessoas usem a chave, mas não permite outras permissões. As contas externas não conseguem gerenciar

nada sobre o ciclo de vida da chave ou a permissão de acesso. Esse modelo centralizado pode ajudar a minimizar o risco de exclusão não intencional de chaves ou aumento de privilégios por administradores ou usuários delegados.

A opção escolhida depende de vários fatores. Considere o seguinte ao escolher uma abordagem:

1. Você tem um processo automático ou manual para provisionar o acesso à chave e aos recursos? Isso inclui recursos como pipelines de implantação e modelos de infraestrutura como código (IaC). Essas ferramentas podem ajudar você a implantar e gerenciar recursos (como chaves do KMS, políticas de chaves, funções do IAM e políticas do IAM) em muitos Contas da AWS. Se você não tiver essas ferramentas de implantação, uma abordagem centralizada para o gerenciamento de chaves pode ser mais gerenciável para sua empresa.
2. Você tem controle administrativo sobre tudo o Contas da AWS que contém recursos que usam chaves KMS? Nesse caso, um modelo centralizado pode simplificar o gerenciamento e eliminar a necessidade de mudar Contas da AWS para gerenciar chaves. Observe, no entanto, que as funções do IAM e as permissões do usuário para usar chaves ainda precisam ser gerenciadas por conta.
3. Você precisa oferecer acesso para usar suas chaves KMS a clientes ou parceiros que tenham recursos próprios Contas da AWS ? Para essas chaves, uma abordagem centralizada pode reduzir a carga administrativa de seus clientes e parceiros.
4. Você tem requisitos de autorização para acesso a AWS recursos que são melhor resolvidos por meio de uma abordagem de acesso centralizada ou local? Por exemplo, se diferentes aplicativos ou unidades de negócios forem responsáveis por gerenciar a segurança de seus próprios dados, uma abordagem descentralizada para o gerenciamento de chaves é melhor.
5. Você está excedendo as cotas de recursos de serviço para? AWS KMS Como essas cotas são definidas por Conta da AWS, um modelo descentralizado distribui a carga entre as contas, multiplicando efetivamente as cotas de serviço.

> **Note**
>
> O modelo de gerenciamento de chaves é irrelevante quando se considera as cotas de solicitação porque essas cotas são aplicadas ao principal da conta que faz uma solicitação contra a chave, não à conta que possui ou gerencia a chave.

Em geral, recomendamos que você comece com uma abordagem descentralizada, a menos que possa articular a necessidade de um modelo de chave KMS centralizado.

Escolha de chaves gerenciadas pelo cliente, chaves AWS gerenciadas ou chaves AWS próprias

As chaves KMS que você cria e gerencia para uso em seus próprios aplicativos criptográficos são conhecidas como chaves gerenciadas pelo cliente. Serviços da AWS pode usar chaves gerenciadas pelo cliente para criptografar os dados que o serviço armazena em seu nome. As chaves gerenciadas pelo cliente são recomendadas se você quiser ter controle total sobre o ciclo de vida e o uso de suas chaves. Há um custo mensal para ter uma chave gerenciada pelo cliente em sua conta. Além disso, as solicitações para usar ou gerenciar a chave incorrem em um custo de uso. Para obter mais informações, consulte Preços do AWS KMS.

Se você quiser AWS service (Serviço da AWS) criptografar seus dados, mas não quiser as despesas gerais ou os custos do gerenciamento de chaves, você pode usar uma chave AWS gerenciada. Esse tipo de chave existe na sua conta, mas só pode ser usado em determinadas circunstâncias. Ele só pode ser usado no contexto em AWS service (Serviço da AWS) que você está operando e só pode ser usado por diretores na conta que contém a chave. Você não pode gerenciar nada sobre o ciclo de vida ou as permissões dessas chaves. Alguns Serviços da AWS usam chaves AWS gerenciadas. O formato de um alias de chave AWS gerenciada é`aws/<service code>`. Por exemplo, uma `aws/ebs` chave só pode ser usada para criptografar volumes do Amazon Elastic Block Store (Amazon EBS) na mesma conta da chave e só pode ser usada por diretores do IAM nessa conta. Uma chave AWS gerenciada só pode ser usada por usuários nessa conta e para recursos nessa conta. Você não pode compartilhar recursos criptografados sob uma chave AWS gerenciada com outras contas. Se isso for uma limitação para seu caso de uso, recomendamos usar uma chave gerenciada pelo cliente; você pode compartilhar o uso dessa chave com qualquer outra conta. Você não é cobrado pela existência de uma chave AWS gerenciada em sua conta, mas é cobrado por qualquer uso desse tipo de chave pela AWS service (Serviço da AWS) pessoa atribuída à chave.

Uma chave AWS gerenciada é um tipo de chave herdada que não está mais sendo criada para novas a Serviços da AWS partir de 2021. Em vez disso, os novos (e os antigos) Serviços da AWS estão usando AWS uma chave própria para criptografar seus dados por padrão. AWS chaves de propriedade são uma coleção de chaves KMS que um AWS service (Serviço da AWS) possui e gerencia para uso em várias Contas da AWS. Embora essas chaves não estejam na sua Conta da AWS, AWS service (Serviço da AWS) você pode usá-las para proteger os recursos da sua conta.

Recomendamos que você use chaves gerenciadas pelo cliente quando o controle granular for mais importante e use chaves AWS próprias quando a conveniência for mais importante.

A tabela a seguir descreve as principais diferenças de política, registro, gerenciamento e preços entre cada tipo de chave. Para obter mais informações sobre os tipos de chaves, consulte AWS KMS conceitos.

Consideração	Chaves gerenciadas pelo cliente	AWS chaves gerenciadas	AWS chaves de propriedade
Política de chave	Controlada exclusiva mente pelo cliente	Controlada pelo serviço; visível para o cliente	Controlado exclusiva mente e visível apenas pelo AWS service (Serviço da AWS) que criptografa seus dados
Registro em log	AWS CloudTrai l rastreamento de clientes ou armazenamento de dados de eventos	CloudTrail rastreame nto de clientes ou armazenamento de dados de eventos	Não visível para o cliente
Gerenciamento do ciclo de vida	O cliente gerencia a rotação, a exclusão e Região da AWS	AWS service (Serviço da AWS) gerencia rotação (anual), exclusão e região	AWS service (Serviço da AWS) gerencia rotação (anual), exclusão e região
Preços	Taxa mensal pela existência da chave (proporcional por hora); o chamador é cobrado pelo uso da API	Sem cobrança pela existência da chave; o chamador é cobrado pelo uso da API	Sem cobranças para o cliente

Escolhendo uma loja de AWS KMS chaves

Um armazenamento de chaves é um local seguro para armazenar e usar material de chave criptográfica. A melhor prática do setor para armazenamentos de chaves é usar um dispositivo conhecido como módulo de segurança de hardware (HSM) que foi validado pelo Programa de

Validação de Módulo Criptográfico dos Padrões Federais de Processamento de Informações (FIPS) 140 do NIST no nível de segurança 3. Existem outros programas de suporte às principais lojas usadas para processar pagamentos. AWS Payment Cryptographyé um serviço que você pode usar para proteger dados relacionados às suas cargas de trabalho de pagamento.

AWS KMS suporta vários tipos de armazenamento de chaves para ajudar a proteger seu material de chaves ao usá-lo AWS KMS para criar e gerenciar suas chaves de criptografia. Todas as opções de armazenamento de chaves fornecidas pela AWS KMS são continuamente validadas de acordo com o FIPS 140 no nível de segurança 3. Eles foram projetados para impedir que qualquer pessoa, incluindo AWS operadores, acesse suas chaves de texto simples ou as use sem sua permissão. Para obter mais informações sobre os tipos disponíveis de armazenamentos de chaves, consulte Armazenamentos de chaves na AWS KMS documentação.

O armazenamento de chaves AWS KMS padrão é a melhor opção para a maioria das cargas de trabalho. Se você precisar escolher um tipo diferente de armazenamento de chaves, considere cuidadosamente se os requisitos regulatórios ou outros (como internos) exigem essa escolha e avalie cuidadosamente os custos e benefícios.

Excluindo e desativando chaves KMS

A exclusão de uma chave KMS pode ter um impacto significativo. Antes de excluir uma chave KMS que você não pretende mais usar, considere se é adequado definir o estado da chave como Desativado. Enquanto uma chave está desativada, ela não pode ser usada para operações criptográficas. Ele ainda existe e você pode reativá-lo no futuro, se necessário. AWS As chaves desativadas continuam incorrendo em taxas de armazenamento. Recomendamos que você desative as chaves em vez de excluí-las até ter certeza de que a chave não protege nenhum dado ou chave de dados.

> **Important**
>
> A exclusão de uma chave deve ser planejada com cuidado. Os dados não podem ser descriptografados se a chave correspondente tiver sido excluída. AWS não tem como recuperar uma chave excluída depois que ela foi excluída. Assim como em outras operações críticas em AWS, você deve aplicar uma política que limite quem pode programar chaves para exclusão e exigir autenticação multifator (MFA) para exclusão de chaves.

Para ajudar a evitar a exclusão acidental da chave, AWS KMS impõe um período de espera mínimo padrão de sete dias após a execução de uma `DeleteKey` chamada antes de excluir a chave. Você pode definir o período de espera para um valor máximo de 30 dias. Durante o período de espera, a chave ainda está armazenada AWS KMS no estado de exclusão pendente. Ele não pode ser usado para operações de criptografia ou descriptografia. Qualquer tentativa de usar uma chave que esteja no estado de exclusão pendente para criptografia ou decodificação é registrada. AWS CloudTrail Você pode definir um CloudWatch alarme da Amazon para esses eventos em seus CloudTrail registros. Se você receber alarmes sobre esses eventos, poderá optar por cancelar o processo de exclusão, se necessário. Até que o período de espera expire, você pode recuperar a chave do estado Exclusão pendente e restaurá-la para o estado Desativado ou Ativado.

A exclusão de uma chave multirregional exige que você exclua as réplicas antes da cópia original. Para obter mais informações, consulte Excluindo chaves multirregionais.

Se você estiver usando uma chave com material de chave importado, poderá excluir o material de chave importado imediatamente. Isso é diferente de excluir uma chave KMS de várias maneiras. Quando você executa a `DeleteImportedKeyMaterial` ação, AWS KMS exclui o material da chave e o estado da chave muda para Importação pendente. Depois de excluir o material da chave, a chave fica imediatamente inutilizável. Não há período de espera. Para habilitar o uso da chave novamente, você precisa importar o mesmo material de chave novamente. O período de espera para a exclusão da chave KMS também se aplica às chaves KMS com material de chave importado.

Se as chaves de dados estiverem protegidas por uma chave KMS e estiverem ativamente em uso Serviços da AWS, elas não serão afetadas imediatamente se a chave KMS associada for desativada ou se o material da chave importada for excluído. Por exemplo, digamos que uma chave com material importado tenha sido usada para criptografar um objeto com SSE-KMS. Você está fazendo o upload do objeto em um bucket do Amazon Simple Storage Service (Amazon S3). Antes de fazer o upload do objeto no bucket, você importa o material para sua chave. Depois que o objeto é carregado, você exclui o material da chave importada dessa chave. O objeto permanece no bucket em um estado criptografado, mas ninguém pode acessar o objeto até que o material da chave excluída seja reimportado para a chave. Embora esse fluxo exija automação precisa para importar e excluir o material chave de uma chave, ele pode fornecer um nível adicional de controle em um ambiente.

AWS oferece orientação prescritiva para ajudá-lo a monitorar e corrigir (se necessário) a exclusão programada das chaves KMS. Para obter mais informações, consulte Monitorar e corrigir a exclusão programada de AWS KMS chaves.

Melhores práticas de proteção de dados para AWS KMS

Esta seção ajuda você a fazer escolhas sobre o uso da chave AWS Key Management Service (AWS KMS) para proteção de dados, como quais chaves usar para cada tipo de dados. Ele também fornece exemplos específicos de uso AWS KMS com diferentes Serviços da AWS. Essas recomendações e exemplos ajudam você a entender quantas chaves você pode precisar e quais diretores precisam de permissões para usar essas chaves.

A seção também discute a rotação de chaves. A rotação de chaves é a prática de substituir uma chave KMS existente por uma nova chave ou substituir o material criptográfico associado a uma chave KMS existente por um novo material. Este guia fornece exemplos e instruções sobre como girar chaves KMS para uso comum. Serviços da AWS As recomendações e os exemplos foram elaborados para ajudá-lo a fazer escolhas informadas sobre sua estratégia de rotação de chaves.

Por fim, esta seção faz recomendações sobre como usar o AWS Encryption SDK, uma ferramenta para implementar a criptografia do lado do cliente em seus aplicativos. Esta seção inclui opções de design que você pode fazer com base no conjunto de recursos e nos recursos do AWS Encryption SDK.

Esta seção aborda os seguintes tópicos de criptografia:

- Criptografia com AWS KMS
- Rotação de chaves AWS KMS e escopo do impacto
- Recomendações para usar o AWS Encryption SDK

Criptografia com AWS KMS

A criptografia é uma prática recomendada geral para proteger a confidencialidade e a integridade de informações confidenciais. Você deve usar seus níveis de classificação de dados existentes e ter pelo menos uma chave AWS Key Management Service (AWS KMS) por nível. Por exemplo, você pode definir uma chave KMS para dados classificados como Confidenciais, uma para Somente Internos e outra para Sensíveis. Isso ajuda você a garantir que somente usuários autorizados tenham permissões para usar as chaves associadas a cada nível de classificação.

> **Note**
>
> Uma única chave KMS gerenciada pelo cliente pode ser usada em qualquer combinação Serviços da AWS ou em seus próprios aplicativos que armazenam dados de uma

classificação específica. O fator limitante do uso de uma chave em várias cargas de trabalho Serviços da AWS é a complexidade das permissões de uso para controlar o acesso aos dados em um conjunto de usuários. O documento JSON da política de AWS KMS chaves deve ter menos de 32 KB. Se essa restrição de tamanho se tornar uma limitação, considere o uso de AWS KMS concessões ou a criação de várias chaves para minimizar o tamanho do documento de política de chaves.

Em vez de confiar apenas na classificação de dados para particionar sua chave KMS, você também pode optar por atribuir uma chave KMS a ser usada para uma classificação de dados em uma única. AWS service (Serviço da AWS) Por exemplo, todos os dados marcados `Sensitive` no Amazon Simple Storage Service (Amazon S3) devem ser criptografados com uma chave KMS com um nome como. `S3-Sensitive` Você pode distribuir ainda mais seus dados em várias chaves KMS dentro de sua classificação de dados definida AWS service (Serviço da AWS) e/ou aplicativo. Por exemplo, você pode excluir alguns conjuntos de dados em um período específico e excluir outros conjuntos de dados em um período diferente. Você pode usar tags de recursos para ajudá-lo a identificar e classificar dados criptografados com chaves KMS específicas.

Se você escolher um modelo de gerenciamento descentralizado para chaves KMS, deverá aplicar grades de proteção para garantir que novos recursos com uma determinada classificação sejam criados e usem as chaves KMS esperadas com as permissões corretas. Para obter mais informações sobre como você pode impor, detectar e gerenciar a configuração de recursos usando a automação, consulte a Detecção e monitoramento seção deste guia.

Esta seção aborda os seguintes tópicos de criptografia:

- Criptografia de dados de log com AWS KMS
- Criptografia por padrão
- criptografia de banco de dados com AWS KMS
- Criptografia de dados PCI DSS com AWS KMS
- Usando chaves KMS com o Amazon EC2 Auto Scaling

Criptografia de dados de log com AWS KMS

Muitos Serviços da AWS, como Amazon GuardDuty e AWS CloudTrail, oferecem opções para criptografar dados de log enviados para o Amazon S3. Ao exportar descobertas GuardDuty para o Amazon S3, você deve usar uma chave KMS. Recomendamos que você criptografe todos os

dados de registro e conceda acesso de decodificação somente aos responsáveis autorizados, como equipes de segurança, equipes de resposta a incidentes e auditores.

A Arquitetura de Referência de AWS Segurança recomenda a criação de uma central Conta da AWS para registro. Ao fazer isso, você também pode reduzir sua sobrecarga de gerenciamento de chaves. Por exemplo, com CloudTrail, você pode criar uma trilha organizacional ou um armazenamento de dados de eventos para registrar eventos em toda a sua organização. Ao configurar sua trilha organizacional ou armazenamento de dados de eventos, você pode especificar um único bucket do Amazon S3 e uma chave KMS na sua conta de registro designada. Essa configuração se aplica a todas as contas de membros na organização. Todas as contas então enviam seus CloudTrail registros para o bucket do Amazon S3 na conta de registro, e os dados de log são criptografados com a chave KMS especificada. Você precisa atualizar a política de chaves dessa chave KMS para conceder CloudTrail as permissões necessárias para usar a chave. Para obter mais informações, consulte Configurar políticas de AWS KMS chaves CloudTrail na CloudTrail documentação.

Para ajudar a proteger os CloudTrail registros GuardDuty e, o bucket do Amazon S3 e a chave KMS devem estar no mesmo lugar. Região da AWS A Arquitetura AWS de Referência de Segurança também fornece orientação sobre arquiteturas de registro e de várias contas. Ao agregar registros em várias regiões e contas, consulte Criar uma trilha para uma organização na CloudTrail documentação para saber mais sobre regiões opcionais e garantir que seu registro centralizado funcione conforme projetado.

Criptografia por padrão

Serviços da AWS que armazenam ou processam dados normalmente oferecem criptografia em repouso. Esse recurso de segurança ajuda a proteger seus dados criptografando-os quando não estão em uso. Usuários autorizados ainda podem acessá-lo quando necessário.

As opções de implementação e criptografia variam entre si Serviços da AWS. Muitos fornecem criptografia por padrão. É importante entender como a criptografia funciona para cada serviço que você usa. Veja os seguintes exemplos:

- Amazon Elastic Block Store (Amazon EBS) — Quando você ativa a criptografia por padrão, todos os novos volumes e cópias de snapshot do Amazon EBS são criptografados. AWS Identity and Access Management As funções ou os usuários (IAM) não podem iniciar instâncias com volumes não criptografados ou volumes que não oferecem suporte à criptografia. Esse recurso ajuda na segurança, conformidade e auditoria, garantindo que todos os dados armazenados nos volumes do Amazon EBS sejam criptografados. Para obter mais informações sobre criptografia nesse serviço, consulte Criptografia do Amazon EBS na documentação do Amazon EBS.

- Amazon Simple Storage Service (Amazon S3) — Todos os novos objetos são criptografados por padrão. O Amazon S3 aplica automaticamente a criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3) para cada novo objeto, a menos que você especifique uma opção de criptografia diferente. Os diretores do IAM ainda podem fazer upload de objetos não criptografados para o Amazon S3 declarando isso explicitamente na chamada da API. No Amazon S3, para aplicar a criptografia SSE-KMS, você deve usar uma política de bucket com condições que exijam criptografia. Para obter um exemplo de política, consulte Exigir SSE-KMS para todos os objetos gravados em um bucket na documentação do Amazon S3. Alguns buckets do Amazon S3 recebem e servem um grande número de objetos. Se esses objetos forem criptografados com chaves KMS, um grande número de operações do Amazon S3 resultará em um grande número `GenerateDataKey` de chamadas `Decrypt` e para. AWS KMS Isso pode aumentar as cobranças que você incorre pelo AWS KMS uso. Você pode configurar as chaves de bucket do Amazon S3, o que pode reduzir significativamente seus AWS KMS custos. Para obter mais informações sobre criptografia nesse serviço, consulte Proteção de dados com criptografia na documentação do Amazon S3.
- Amazon DynamoDB — O DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que permite a criptografia do lado do servidor em repouso por padrão, e você não pode desativá-la. Recomendamos que você use uma chave gerenciada pelo cliente para criptografar suas tabelas do DynamoDB. Essa abordagem ajuda você a implementar privilégios mínimos com permissões granulares e separação de tarefas, visando usuários e funções específicos do IAM em suas AWS KMS principais políticas. Você também pode escolher chaves AWS gerenciadas ou AWS próprias ao definir as configurações de criptografia para suas tabelas do DynamoDB. Para dados que exigem um alto grau de proteção (em que os dados só devem ser visíveis como texto não criptografado para o cliente), considere usar a criptografia do lado do cliente com o AWS SDK de criptografia de banco de dados. Para obter mais informações sobre criptografia nesse serviço, consulte Proteção de dados na documentação do DynamoDB.

criptografia de banco de dados com AWS KMS

O nível no qual você implementa a criptografia afeta a funcionalidade do banco de dados. A seguir estão as vantagens e desvantagens que você deve considerar:

- Se você usa somente AWS KMS criptografia, o armazenamento que faz backup de suas tabelas é criptografado para o DynamoDB e o Amazon Relational Database Service (Amazon RDS). Isso significa que o sistema operacional que executa o banco de dados vê o conteúdo do armazenamento como texto não criptografado. Todas as funções do banco de dados, incluindo

a geração de índices e outras funções de ordem superior que exigem acesso aos dados de texto não criptografado, continuam funcionando conforme o esperado.

- O Amazon RDS baseia-se na Criptografia do Amazon Elastic Block Store (Amazon EBS) para fornecer criptografia total de disco para volumes de banco de dados. Quando você cria uma instância de banco de dados criptografada com o Amazon RDS, o Amazon RDS cria um volume criptografado do Amazon EBS em seu nome para armazenar o banco de dados. Os dados armazenados em repouso no volume, nos instantâneos do banco de dados, nos backups automatizados e nas réplicas de leitura são todos criptografados sob a chave KMS que você especificou ao criar a instância do banco de dados.
- O Amazon Redshift se integra AWS KMS e cria uma hierarquia de chaves de quatro camadas que são usadas para criptografar o nível do cluster por meio do nível de dados. Ao iniciar seu cluster, você pode optar por usar AWS KMS criptografia. Somente o aplicativo Amazon Redshift e os usuários com as permissões apropriadas podem ver texto não criptografado quando as tabelas são abertas (e descriptografadas) na memória. Isso é amplamente análogo aos recursos de criptografia de dados transparente ou baseada em tabela (TDE) que estão disponíveis em alguns bancos de dados comerciais. Isso significa que todas as funções do banco de dados, incluindo a geração de índices e outras funções de ordem superior que exigem acesso aos dados de texto não criptografado, continuam funcionando conforme o esperado.
- A criptografia em nível de dados do lado do cliente implementada por meio do SDK AWS de criptografia de banco de dados (e ferramentas similares) significa que tanto o sistema operacional quanto o banco de dados veem somente texto cifrado. Os usuários só podem visualizar texto não criptografado se acessarem o banco de dados de um cliente que tenha o SDK AWS de criptografia de banco de dados instalado e tenham acesso à chave relevante. Funções de banco de dados de ordem superior que exigem acesso a texto não criptografado para funcionar conforme o esperado, como geração de índice, não funcionarão se forem direcionadas para operar em campos criptografados. Ao escolher usar a criptografia do lado do cliente, certifique-se de usar um mecanismo de criptografia robusto que ajude a evitar ataques comuns contra dados criptografados. Isso inclui o uso de um algoritmo de criptografia robusto e técnicas apropriadas, como sal, para ajudar a mitigar ataques de texto cifrado.

Recomendamos usar os recursos de criptografia AWS KMS integrados para serviços AWS de banco de dados. Para cargas de trabalho que processam dados confidenciais, a criptografia do lado do cliente deve ser considerada para os campos de dados confidenciais. Ao usar a criptografia do lado do cliente, você deve considerar o impacto no acesso ao banco de dados, como junções em consultas SQL ou criação de índices.

Criptografia de dados PCI DSS com AWS KMS

Os controles de segurança e qualidade AWS KMS foram validados e certificados para atender aos requisitos do Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS). Isso significa que você pode criptografar os dados do número da conta primária (PAN) com uma chave KMS. O uso de uma chave KMS para criptografar dados elimina parte da carga de gerenciar bibliotecas de criptografia. Além disso, as chaves KMS não podem ser exportadas AWS KMS, o que reduz a preocupação com o armazenamento inseguro das chaves de criptografia.

Há outras maneiras que você pode usar AWS KMS para atender aos requisitos do PCI DSS. Por exemplo, se você estiver usando AWS KMS com o Amazon S3, você pode armazenar dados PAN no Amazon S3 porque o mecanismo de controle de acesso para cada serviço é diferente do outro.

Como sempre, ao analisar seus requisitos de conformidade, certifique-se de obter aconselhamento de partes devidamente experientes, qualificadas e verificadas. Esteja ciente das cotas de AWS KMS solicitação ao criar aplicativos que usam a chave diretamente para proteger os dados de transações com cartões que estão no escopo do PCI DSS.

Como todas as AWS KMS solicitações estão registradas AWS CloudTrail, você pode auditar o uso da chave revisando os CloudTrail registros. No entanto, se você usa chaves de bucket do Amazon S3, não há nenhuma entrada que corresponda a cada ação do Amazon S3. Isso ocorre porque a chave do bucket criptografa as chaves de dados que você usa para criptografar os objetos no Amazon S3. Embora o uso de uma chave de bucket não elimine todas as chamadas de API para AWS KMS, ele reduz o número delas. Como resultado, não há mais uma one-to-one correspondência entre as tentativas de acesso a objetos do Amazon S3 e as chamadas de API para. AWS KMS

Usando chaves KMS com o Amazon EC2 Auto Scaling

O Amazon EC2 Auto Scaling é um serviço recomendado para automatizar a escalabilidade de suas instâncias do Amazon EC2. Isso ajuda você a garantir que você tenha o número correto de instâncias disponíveis para lidar com a carga do seu aplicativo. O Amazon EC2 Auto Scaling usa uma função vinculada ao serviço que fornece permissões apropriadas para o serviço e autoriza suas atividades em sua conta. Para usar chaves KMS com o Amazon EC2 Auto Scaling, AWS KMS suas políticas de chaves devem permitir que a função vinculada ao serviço use sua chave KMS com algumas operações de API, `Decrypt` como, por exemplo, para que a automação seja útil. Se a política de AWS KMS chaves não autorizar o diretor do IAM que está executando a operação a realizar uma ação, essa ação será negada. Para obter mais informações sobre como aplicar

corretamente as permissões na política de chaves para permitir o acesso, consulte Proteção de dados no Amazon EC2 Auto Scaling na documentação do Amazon EC2 Auto Scaling.

Rotação de chaves AWS KMS e escopo do impacto

Não recomendamos a rotação de chaves AWS Key Management Service (AWS KMS), a menos que você precise alternar as chaves para conformidade regulatória. Por exemplo, talvez seja necessário alternar suas chaves KMS devido a políticas comerciais, regras contratuais ou regulamentações governamentais. O design do reduz AWS KMS significativamente os tipos de risco que a rotação de chaves normalmente é usada para mitigar. Se você precisar girar as chaves KMS, recomendamos usar a rotação automática de chaves e usar a rotação manual de chaves somente se a rotação automática de chaves não for suportada.

Esta seção discute os seguintes tópicos principais de rotação:

- AWS KMS rotação simétrica da chave
- Rotação de chaves para volumes do Amazon EBS
- Rotação de chaves para Amazon RDS
- Rotação de chaves para Amazon S3 e replicação na mesma região
- Chaves KMS rotativas com material importado

AWS KMS rotação simétrica da chave

AWS KMS suporta rotação automática de chaves somente para chaves KMS de criptografia simétrica com material de chave que AWS KMS cria. A rotação automática é opcional para chaves KMS gerenciadas pelo cliente. Anualmente, AWS KMS alterna o material de chaves para chaves KMS AWS gerenciadas. AWS KMS salva todas as versões anteriores do material criptográfico perpetuamente, para que você possa descriptografar todos os dados criptografados com essa chave KMS. AWS KMS não exclui nenhum material de chave girada até que você exclua a chave KMS. Além disso, quando você descriptografa um objeto usando AWS KMS, o serviço determina o material de apoio correto a ser usado na operação de descriptografia; nenhum parâmetro de entrada adicional precisa ser fornecido.

Como AWS KMS retém versões anteriores do material da chave criptográfica e porque você pode usar esse material para descriptografar dados, a rotação de chaves não oferece nenhum benefício adicional de segurança. O mecanismo de rotação de chaves existe para facilitar a rotação de chaves

se você estiver operando uma carga de trabalho em um contexto em que os requisitos regulatórios ou outros o exijam.

Rotação de chaves para volumes do Amazon EBS

Você pode alternar as chaves de dados do Amazon Elastic Block Store (Amazon EBS) usando uma das seguintes abordagens. A abordagem depende de seus fluxos de trabalho, métodos de implantação e arquitetura do aplicativo. Talvez você queira fazer isso ao mudar de uma chave AWS gerenciada para uma chave gerenciada pelo cliente.

Para usar as ferramentas do sistema operacional para copiar os dados de um volume para outro

1. Crie a nova chave KMS. Para obter instruções, consulte Criar uma chave KMS.
2. Crie um novo volume do Amazon EBS que seja do mesmo tamanho ou maior que o original. Para criptografia, especifique a chave KMS que você criou. Para obter instruções, consulte Criar um volume do Amazon EBS.
3. Monte o novo volume na mesma instância ou contêiner do volume original. Para obter instruções, consulte Anexar um volume do Amazon EBS a uma instância do Amazon EC2.
4. Usando sua ferramenta de sistema operacional preferida, copie os dados do volume existente para o novo volume.
5. Quando a sincronização estiver concluída, durante uma janela de manutenção pré-agendada, interrompa o tráfego para a instância. Para obter instruções, consulte Parar e iniciar manualmente suas instâncias.
6. Desmonte o volume original. Para obter instruções, consulte Separar um volume do Amazon EBS de uma instância do Amazon EC2.
7. Monte o novo volume no ponto de montagem original.
8. Verifique se o novo volume está funcionando corretamente.
9. Exclua o volume original. Para obter instruções, consulte Excluir um volume do Amazon EBS.

Para usar um snapshot do Amazon EBS para copiar os dados de um volume para outro

1. Crie a nova chave KMS. Para obter instruções, consulte Criar uma chave KMS.
2. Crie um snapshot do Amazon EBS do volume original. Para obter instruções, consulte Criar snapshots do Amazon EBS.
3. Crie um novo volume a partir do snapshot. Para criptografia, especifique a nova chave KMS que você criou. Para obter instruções, consulte Criar um volume do Amazon EBS.

> **Note**
>
> Dependendo da sua carga de trabalho, talvez você queira usar a restauração rápida de snapshots do Amazon EBS para minimizar a latência inicial no volume.

4. Crie uma nova instância do Amazon EC2. Para obter instruções, consulte Iniciar uma instância do Amazon EC2.
5. Anexe o volume que você criou à instância do Amazon EC2. Para obter instruções, consulte Anexar um volume do Amazon EBS a uma instância do Amazon EC2.
6. Transforme a nova instância em produção.
7. Retire a instância original da produção e exclua-a. Para obter instruções, consulte Excluir um volume do Amazon EBS.

> **Note**
>
> É possível copiar instantâneos e modificar a chave de criptografia usada para a cópia de destino. Depois de copiar o snapshot e criptografá-lo com suas chaves KMS preferidas, você também pode criar uma Amazon Machine Image (AMI) a partir de snapshots. Para obter mais informações, consulte a criptografia do Amazon EBS na documentação do Amazon EC2.

Rotação de chaves para Amazon RDS

Para alguns serviços, como o Amazon Relational Database Service (Amazon RDS), a criptografia de dados ocorre dentro do serviço e é fornecida por. AWS KMS Use as instruções a seguir para alternar uma chave para uma instância de banco de dados do Amazon RDS.

Para alternar uma chave KMS para um banco de dados do Amazon RDS

1. Crie um instantâneo do banco de dados criptografado original. Para obter instruções, consulte Gerenciamento de backups manuais na documentação do Amazon RDS.
2. Copie o instantâneo em um novo instantâneo. Para criptografia, especifique a nova chave KMS. Para obter instruções, consulte Cópia de um DB snapshot para o Amazon RDS.

3. Use o novo snapshot para criar um novo cluster do Amazon RDS. Para obter instruções, consulte Restauração em uma instância de banco de dados na documentação do Amazon RDS. Por padrão, o cluster usa a nova chave KMS.
4. Verifique a operação do novo banco de dados e os dados nele contidos.
5. Transforme o novo banco de dados em produção.
6. Retire o banco de dados antigo da produção e exclua-o. Para obter instruções, consulte Excluir uma instância de banco de dados.

Rotação de chaves para Amazon S3 e replicação na mesma região

Para o Amazon Simple Storage Service (Amazon S3), para alterar a chave de criptografia de um objeto, você precisa ler e reescrever o objeto. Ao reescrever o objeto, você especifica explicitamente a nova chave de criptografia na operação de gravação. Para fazer isso com muitos objetos, você pode usar o Amazon S3 Batch Operations. Nas configurações do trabalho, para a operação de cópia, especifique as novas configurações de criptografia. Por exemplo, você pode escolher SSE-KMS e inserir o KeyID.

Como alternativa, você pode usar o Amazon S3 Same-Region Replication (SRR). O SSR pode recriptografar os objetos em trânsito.

Chaves KMS rotativas com material importado

AWS KMS não recupera nem gira seu material de chave importado. Para girar uma chave KMS com material de chave importado, você deve girar a chave manualmente.

Recomendações para usar o AWS Encryption SDK

AWS Encryption SDKÉ uma ferramenta poderosa para implementar a criptografia do lado do cliente em seus aplicativos. As bibliotecas estão disponíveis para Java JavaScript, C, Python e outras linguagens de programação. Ele se integra com AWS Key Management Service (AWS KMS). Você também pode usá-lo como um SDK independente sem fazer referência às chaves do KMS.

As práticas recomendadas para usar essa ferramenta incluem considerar cuidadosamente os requisitos do seu aplicativo. Equilibre esses requisitos com os riscos que podem ser introduzidos por determinadas configurações, como a introdução do cache de chaves em seu aplicativo. Para obter mais informações sobre o armazenamento em cache da chave de dados, consulte Cache da chave de dados na AWS Encryption SDK documentação.

Considere as seguintes questões ao determinar se você deve usar o AWS Encryption SDK:

- Existe um requisito de criptografia do lado do cliente que não pode ser atendido pela criptografia do lado do servidor com serviços que se integram com? AWS KMS
- Você pode proteger adequadamente as chaves usadas para criptografar dados do lado do cliente, e como você fará isso?
- Existem outras bibliotecas de fit-for-purpose criptografia que podem se adequar mais adequadamente ao seu caso de uso? Considere AWS ofertas alternativas, como a criptografia do lado do cliente do Amazon S3 e AWS o SDK de criptografia de banco de dados.

Encontre mais informações sobre como escolher o serviço certo para seu caso de uso, consulte a documentação do AWS Crypto Tools.

Melhores práticas de gerenciamento de identidade e acesso para AWS KMS

Para usar AWS Key Management Service (AWS KMS), você deve ter credenciais que AWS possam ser usadas para autenticar e autorizar suas solicitações. Nenhum AWS diretor tem permissões para uma chave KMS, a menos que essa permissão seja fornecida explicitamente e nunca negada. Não há permissões implícitas ou automáticas para usar ou gerenciar uma chave KMS. Os tópicos desta seção definem as melhores práticas de segurança para ajudá-lo a determinar quais controles de gerenciamento de AWS KMS acesso você deve usar para proteger sua infraestrutura.

Esta seção aborda os seguintes tópicos de gerenciamento de identidade e acesso:

- AWS KMS políticas principais e políticas do IAM
- Permissões com privilégios mínimos para AWS KMS
- Controle de acesso baseado em funções para AWS KMS
- Controle de acesso baseado em atributos para AWS KMS
- Contexto de criptografia para AWS KMS
- Solução de problemas de AWS KMS permissões

AWS KMS políticas principais e políticas do IAM

A principal forma de gerenciar o acesso aos seus AWS KMS recursos é com políticas. Políticas são documentos que descrevem quais entidades principais podem acessar recursos específicos. As políticas anexadas a uma identidade AWS Identity and Access Management (IAM) (usuários, grupos de usuários ou funções) são chamadas de políticas baseadas em identidade. As políticas do IAM vinculadas aos recursos são chamadas de políticas baseadas em recursos. AWS KMS as políticas de recursos para chaves KMS são chamadas de políticas de chaves. Além das políticas do IAM e das AWS KMS principais políticas, AWS KMS apoia subsídios. As concessões oferecem uma maneira flexível e poderosa de delegar permissões. Você pode usar concessões para emitir acesso por chave KMS com prazo determinado aos diretores do IAM em sua empresa Conta da AWS ou em outras. Contas da AWS

Todas as chaves do KMS têm uma política de chaves. Se você não fornecer um, AWS KMS cria um para você. A política de chaves padrão AWS KMS usada difere dependendo se você cria a chave usando o AWS KMS console ou usa a AWS KMS API. Recomendamos que você edite a

política de chaves padrão para se alinhar aos requisitos de permissões de privilégios mínimos da sua organização. Isso também deve estar alinhado à sua estratégia de usar as políticas do IAM em conjunto com as principais políticas. Para obter mais recomendações sobre o uso de políticas do IAM com AWS KMS, consulte Melhores práticas para políticas do IAM na AWS KMS documentação.

Você pode usar a política de chaves para delegar a autorização de um diretor do IAM à política baseada em identidade. Você também pode usar a política de chaves para refinar a autorização em conjunto com a política baseada em identidade. Em ambos os casos, tanto a política principal quanto a política baseada em identidade determinam o acesso, juntamente com quaisquer outras políticas aplicáveis que definem o acesso, como políticas de controle de serviços (SCPs), políticas de controle de recursos (RCPs) ou limites de permissão. Se o principal estiver em uma conta diferente da chave KMS, basicamente, somente ações criptográficas e de concessão serão suportadas. Para obter mais informações sobre esse cenário entre contas, consulte Permitir que usuários em outras contas usem uma chave KMS na AWS KMS documentação.

Você deve usar políticas baseadas em identidade do IAM em combinação com políticas de chaves para controlar o acesso às suas chaves do KMS. As concessões também podem ser usadas em combinação com essas políticas para controlar o acesso a uma chave KMS. Para usar uma política baseada em identidade para controlar o acesso a uma chave KMS, a política de chaves deve permitir que a conta use políticas baseadas em identidade. Você pode especificar uma declaração de política de chave que habilite as políticas do IAM ou pode especificar as entidades principais permitidas explicitamente na política de chave.

Ao redigir políticas, certifique-se de ter controles fortes que restrinjam quem pode realizar as seguintes ações:

- Atualizar, criar e excluir políticas do IAM e políticas de chaves do KMS
- Anexe e separe políticas baseadas em identidade de usuários, funções e grupos
- Anexe e desanexe políticas de AWS KMS chaves de KMS
- Crie concessões para suas chaves KMS — Se você controla o acesso às suas chaves KMS exclusivamente com políticas de chaves ou combina políticas de chaves com políticas de IAM, você deve restringir a capacidade de modificar as políticas. Implemente um processo de aprovação para alterar qualquer política existente. Um processo de aprovação pode ajudar a evitar o seguinte:
  - Perda acidental das permissões principais do IAM — É possível fazer alterações que impeçam os diretores do IAM de gerenciar a chave ou usá-la em operações criptográficas. Em cenários extremos, é possível revogar as permissões de gerenciamento de chaves de todos os usuários.

Se isso acontecer, você precisará entrar em contato AWS Supportpara recuperar o acesso à chave.

- Alterações não aprovadas nas políticas de chaves do KMS — Se um usuário não autorizado obtiver acesso à política de chaves, ele poderá modificá-la para delegar permissões a uma pessoa não intencional ou principal. Conta da AWS
- Alterações não aprovadas nas políticas do IAM — Se um usuário não autorizado obtiver um conjunto de credenciais com permissões para gerenciar a associação de um grupo, ele poderá elevar suas próprias permissões e fazer alterações em suas políticas de IAM, políticas de chaves, configuração de chaves KMS ou outras configurações de recursos. AWS

Analise cuidadosamente as funções e os usuários do IAM associados aos diretores do IAM que são designados como seus administradores de chaves do KMS. Isso pode ajudar a evitar exclusões ou alterações não autorizadas. Se você precisar alterar os diretores que têm acesso às suas chaves do KMS, verifique se os novos administradores principais foram adicionados a todas as políticas de chaves necessárias. Teste suas permissões antes de excluir o diretor administrativo anterior. É altamente recomendável seguir todas as melhores práticas de segurança do IAM e usar credenciais temporárias em vez das credenciais de longo prazo.

Recomendamos emitir acesso com limite de tempo por meio de subsídios se você não souber os nomes dos diretores no momento em que as políticas foram criadas ou se os diretores que exigem acesso mudarem com frequência. O principal beneficiário pode estar na mesma conta da chave KMS ou em uma conta diferente. Se o principal e a chave KMS estiverem em contas diferentes, você deverá especificar uma política baseada em identidade além da concessão. As concessões exigem gerenciamento adicional porque você precisa chamar uma API para criar a concessão e retirar ou revogar a concessão quando ela não for mais necessária.

Nenhum AWS diretor, incluindo o usuário raiz da conta ou o criador da chave, tem qualquer permissão para uma chave KMS, a menos que seja explicitamente permitida e não explicitamente negada em uma política de chaves, política do IAM ou concessão. Por extensão, você deve considerar o que aconteceria se um usuário obtivesse acesso não intencional para usar uma chave KMS e qual seria o impacto. Para mitigar esse risco, considere o seguinte:

- Você pode manter chaves KMS diferentes para diferentes categorias de dados. Isso ajuda você a separar as chaves e manter políticas de chaves mais concisas que contêm declarações de política que visam especificamente o acesso principal a essa categoria de dados. Isso também significa que, se as credenciais relevantes do IAM forem acessadas involuntariamente, a identidade

vinculada a esse acesso terá acesso somente às chaves especificadas na política do IAM e somente se a política de chaves permitir o acesso a esse principal.

- Você pode avaliar se um usuário com acesso não intencional à chave pode acessar os dados. Por exemplo, com o Amazon Simple Storage Service (Amazon S3), o usuário também deve ter as permissões apropriadas para acessar objetos criptografados no Amazon S3. Como alternativa, se um usuário tiver acesso não intencional (usando RDP ou SSH) a uma EC2 instância da Amazon que tenha um volume criptografado com uma chave KMS, o usuário poderá acessar os dados usando ferramentas do sistema operacional.

> **Note**
>
> Serviços da AWS esse uso AWS KMS não expõe o texto cifrado aos usuários (a maioria das abordagens atuais de criptoanálise requer acesso ao texto cifrado). Além disso, o texto cifrado não está disponível para exame físico fora de um AWS data center porque toda a mídia de armazenamento é destruída fisicamente quando é desativada, de acordo com os requisitos do NIST 00-88. SP8

Permissões com privilégios mínimos para AWS KMS

Como suas chaves KMS protegem informações confidenciais, recomendamos seguir o princípio do acesso menos privilegiado. Delegue as permissões mínimas necessárias para executar uma tarefa ao definir as políticas de chave. Permita todas as ações (`kms:*`) em uma política de chaves do KMS somente se você planeja restringir ainda mais as permissões com políticas adicionais baseadas em identidade. Se você planeja gerenciar permissões com políticas baseadas em identidade, limite quem tem a capacidade de criar e anexar políticas do IAM aos diretores do IAM e monitorar as mudanças nas políticas.

Se você permitir todas as ações (`kms:*`) na política de chaves e na política baseada em identidade, o diretor terá permissões administrativas e de uso para a chave KMS. Como prática recomendada de segurança, recomendamos delegar essas permissões somente a diretores específicos. Pense em como você atribui permissões aos diretores que gerenciarão suas chaves e aos diretores que usarão suas chaves. Você pode fazer isso nomeando explicitamente o principal na política de chaves ou limitando a quais princípios a política baseada em identidade está anexada. Você também pode usar chaves de condição para restringir as permissões. Por exemplo, você pode usar o aws:

PrincipalTag para permitir todas as ações se o principal que está fazendo a chamada de API tiver a tag especificada na regra de condição.

Para ajudar a entender como as declarações de política são avaliadas AWS, consulte Lógica de avaliação de políticas na documentação do IAM. Recomendamos revisar esse tópico antes de redigir políticas para ajudar a reduzir a chance de sua política ter efeitos indesejados, como fornecer acesso a diretores que não deveriam ter acesso.

> **Tip**
>
> Ao testar um aplicativo em um ambiente que não seja de produção, use AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) para ajudá-lo a aplicar permissões de privilégio mínimo em suas políticas do IAM.

Se você usa usuários do IAM em vez de funções do IAM, é altamente recomendável usar a autenticação AWS multifator (MFA) para mitigar a vulnerabilidade das credenciais de longo prazo. Você pode usar o MFA para:

- Exija que os usuários validem suas credenciais com a MFA antes de realizar ações privilegiadas, como agendar a exclusão da chave.
- Divida a propriedade de uma conta de administrador, senha e dispositivo de MFA entre indivíduos para implementar a autorização dividida.

Para exemplos de políticas que podem ajudar você a configurar permissões com privilégios mínimos, consulte exemplos de políticas do IAM na documentação. AWS KMS

Controle de acesso baseado em funções para AWS KMS

O controle de acesso baseado em funções (RBAC) é uma estratégia de autorização que fornece aos usuários somente as permissões necessárias para realizar suas tarefas e nada mais. É uma abordagem que pode ajudá-lo a implementar o princípio do menor privilégio.

AWS KMS suporta RBAC. Ele permite que você controle o acesso às suas chaves especificando permissões granulares nas políticas de chaves. As políticas de chave especificam um recurso, ação, efeito, entidade principal e condições opcionais para conceder acesso às chaves. Para implementar o RBAC em AWS KMS, recomendamos separar as permissões dos principais usuários e administradores de chaves.

Para os principais usuários, atribua somente as permissões de que o usuário precisa. Use as perguntas a seguir para ajudá-lo a refinar ainda mais as permissões:

- Quais diretores do IAM precisam acessar a chave?
- Quais ações cada entidade principal precisa realizar com a chave? Por exemplo, o diretor precisa apenas `Encrypt` de `Sign` permissões?
- Quais recursos o diretor precisa acessar?
- A entidade é humana ou humana AWS service (Serviço da AWS)? Se for um serviço, você pode usar a chave de ViaService condição kms: para restringir o uso da chave a um serviço específico.

Para administradores de chaves, atribua somente as permissões de que o administrador precisa. Por exemplo, as permissões de um administrador podem variar dependendo se a chave é usada em ambientes de teste ou de produção. Se você usar permissões menos restritivas em determinados ambientes que não sejam de produção, implemente um processo para testar as políticas antes que elas sejam liberadas para produção.

Para exemplos de políticas que podem ajudá-lo a configurar o controle de acesso baseado em funções para os principais usuários e administradores, consulte RBAC for. AWS KMS

Controle de acesso baseado em atributos para AWS KMS

O controle de acesso baseado em atributos (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Como o RBAC, é uma abordagem que pode ajudá-lo a implementar o princípio do menor privilégio.

AWS KMS oferece suporte ao ABAC, permitindo que você defina permissões com base nas tags associadas ao recurso de destino, como uma chave KMS, e nas tags associadas ao principal que está fazendo a chamada da API. Em AWS KMS, você pode usar tags e aliases para controlar o acesso às chaves gerenciadas pelo cliente. Por exemplo, você pode definir políticas do IAM que usam chaves de condição de tag para permitir operações quando a tag do principal corresponde à tag associada à chave KMS. Para ver um tutorial, consulte Definir permissões para acessar AWS recursos com base em tags na AWS KMS documentação.

Como prática recomendada, use estratégias ABAC para simplificar o gerenciamento de políticas do IAM. Com o ABAC, os administradores podem usar tags para permitir o acesso a novos recursos em vez de atualizar as políticas existentes. O ABAC exige menos políticas porque você não precisa

criar políticas diferentes para diferentes funções de trabalho. Para obter mais informações, consulte Comparação do ABAC com o modelo RBAC tradicional na documentação do IAM.

Aplique as melhores práticas de permissões de privilégio mínimo ao modelo ABAC. Forneça aos diretores do IAM somente as permissões necessárias para realizar seus trabalhos. Controle cuidadosamente o acesso às marcações APIs que permitiriam aos usuários modificar as tags em funções e recursos. Se você usar chaves de condição de alias de chave para oferecer suporte ao ABAC AWS KMS, verifique se você também tem controles fortes que restrinjam quem pode criar chaves e modificar aliases.

Você também pode usar tags para vincular uma chave específica a uma categoria comercial e verificar se a chave correta está sendo usada para uma determinada ação. Por exemplo, você pode usar AWS CloudTrail registros para verificar se a chave usada para realizar uma AWS KMS ação específica pertence à mesma categoria de negócios do recurso em que ela está sendo usada.

> **Warning**
>
> Não inclua informações confidenciais ou sigilosas na chave ou no valor da tag. As tags não são criptografadas. Eles são acessíveis a muitos Serviços da AWS, incluindo o faturamento.

Antes de implementar uma abordagem ABAC para seu controle de acesso, considere se os outros serviços que você usa oferecem suporte a essa abordagem. Para obter ajuda para determinar quais serviços oferecem suporte ao ABAC, consulte Serviços da AWS esse trabalho com o IAM na documentação do IAM.

Para obter mais informações sobre a implementação do ABAC para AWS KMS e as chaves de condições que podem ajudá-lo a configurar políticas, consulte ABAC para. AWS KMS

Contexto de criptografia para AWS KMS

Todas as operações AWS KMS criptográficas com chaves KMS de criptografia simétrica aceitam um contexto de criptografia. O contexto de criptografia é um conjunto opcional de pares de chave-valor não secretos que podem conter informações contextuais adicionais sobre os dados. Como prática recomendada, você pode inserir o contexto de criptografia nas `Encrypt` operações AWS KMS para aprimorar a autorização e a auditabilidade de suas chamadas de API de descriptografia para. AWS KMS AWS KMS usa o contexto de criptografia como dados autenticados adicionais (AAD) para oferecer suporte à criptografia autenticada. O contexto de criptografia é associado de

maneira criptográfica ao texto cifrado, de modo que o mesmo contexto de criptografia é necessário para descriptografar os dados.

O contexto de criptografia não é secreto nem criptografado. Ele aparece em texto simples nos AWS CloudTrail registros para que você possa usá-lo para identificar e categorizar suas operações criptográficas. Como o contexto de criptografia não é secreto, você deve permitir que somente diretores autorizados acessem seus dados de CloudTrail registro.

Você também pode usar as EncryptionContextKeys chaves de condição kms ::context-key EncryptionContext e kms: para controlar o acesso a uma chave KMS de criptografia simétrica com base no contexto de criptografia. Você também pode usar essas chaves de condição para exigir que contextos de criptografia sejam usados em operações criptográficas. Para essas chaves de condição, revise as orientações sobre o uso `ForAnyValue` ou `ForAllValues` defina operadores para garantir que suas políticas reflitam as permissões pretendidas.

Solução de problemas de AWS KMS permissões

Ao escrever políticas de controle de acesso para uma chave KMS, considere como a política do IAM e a política de chaves funcionam juntas. As permissões efetivas para um diretor são as permissões concedidas (e não negadas explicitamente) por todas as políticas efetivas. Em uma conta, as permissões para uma chave KMS podem ser afetadas por políticas baseadas em identidade do IAM, políticas de chaves, limites de permissões, políticas de controle de serviços ou políticas de sessão. Por exemplo, se você usar políticas baseadas em identidade e políticas de chave para controlar o acesso à chave KMS, todas as políticas relacionadas ao principal e ao recurso serão avaliadas para determinar a autorização do principal para realizar uma determinada ação. Para obter mais informações, consulte Lógica de avaliação de políticas na documentação do IAM.

Para obter informações detalhadas e um fluxograma para solucionar problemas de acesso por chave, consulte Solução de problemas de acesso por chave na AWS KMS documentação.

Para solucionar uma mensagem de erro de acesso negado

1. Confirme se as políticas baseadas em identidade do IAM e as políticas de chaves do KMS permitem o acesso.
2. Confirme se um limite de permissões no IAM não está restringindo o acesso.
3. Confirme se uma política de controle de serviço (SCP) ou política de controle de recursos (RCP) em não AWS Organizations está restringindo o acesso.
4. Se você estiver usando VPC endpoints, confirme se as políticas de endpoint estão corretas.

5. Nas políticas baseadas em identidade e nas políticas de chaves, remova quaisquer condições ou referências de recursos que restrinjam o acesso à chave. Depois de remover essas restrições, confirme se o principal pode chamar com sucesso a API que falhou anteriormente. Se for bem-sucedido, reaplique as condições e as referências de recursos uma de cada vez e, após cada uma, verifique se o principal ainda tem acesso. Isso ajuda você a identificar a condição ou a referência do recurso que está causando o erro.

Para obter mais informações, consulte Solução de problemas de mensagens de erro de acesso negado na documentação do IAM.

Melhores práticas de detecção e monitoramento para AWS KMS

A detecção e o monitoramento são uma parte importante da compreensão da disponibilidade, do estado e do uso das suas chaves AWS Key Management Service (AWS KMS). O monitoramento ajuda a manter a segurança, a confiabilidade, a disponibilidade e o desempenho de suas AWS soluções. AWS fornece várias ferramentas para monitorar suas chaves e AWS KMS operações do KMS. Esta seção descreve como configurar e usar essas ferramentas para obter maior visibilidade em seu ambiente e monitorar o uso de suas chaves KMS.

Esta seção aborda os seguintes tópicos de detecção e monitoramento:

- AWS KMS Operações de monitoramento com AWS CloudTrail
- Monitorando o acesso às chaves KMS com o IAM Access Analyzer
- Monitorando as configurações de criptografia de outros Serviços da AWS com AWS Config
- Monitorando chaves KMS com alarmes da Amazon CloudWatch
- Automatizando respostas com a Amazon EventBridge

AWS KMS Operações de monitoramento com AWS CloudTrail

AWS KMS é integrado com AWS CloudTrail, um serviço que pode gravar todas as chamadas feitas AWS KMS por usuários, funções e outros Serviços da AWS. CloudTrail captura todas as chamadas de API para AWS KMS como eventos, incluindo chamadas do AWS KMS console AWS KMS APIs, AWS CloudFormation,, the AWS Command Line Interface (AWS CLI) e. Ferramentas da AWS para PowerShell

CloudTrail registra todas AWS KMS as operações, incluindo operações somente para leitura, como e. `ListAliases` `GetKeyRotationStatus` Ele também registra operações que gerenciam chaves KMS, como `CreateKey` `PutKeyPolicy, and cryptographic operations, such as GenerateDataKey` e e. `Decrypt` Ele também registra operações internas que AWS KMS chamam por você`DeleteExpiredKeyMaterial`, como `DeleteKeySynchronizeMultiRegionKey`,, `RotateKey` e.

CloudTrail é ativado no seu Conta da AWS quando você o cria. Por padrão, o histórico de eventos fornece um registro visível, pesquisável, baixável e imutável dos últimos 90 dias da atividade

registrada da API de eventos de gerenciamento em um. Região da AWS Para monitorar ou auditar o uso de suas chaves KMS além dos 90 dias, recomendamos criar uma CloudTrail trilha para você Conta da AWS. Se você criou uma organização em AWS Organizations, você pode criar uma trilha da organização ou um armazenamento de dados de eventos que registre eventos para todos Contas da AWS nessa organização.

Depois de estabelecer uma trilha para sua conta ou organização, você pode usar outra Serviços da AWS para armazenar, analisar e responder automaticamente aos eventos registrados na trilha. Por exemplo, você pode fazer o seguinte:

- Você pode configurar CloudWatch alarmes da Amazon para notificá-lo sobre determinados eventos na trilha. Para obter mais informações, consulte Monitorando chaves KMS com alarmes da Amazon CloudWatch neste guia.
- Você pode criar EventBridge regras da Amazon que executam automaticamente uma ação quando ocorre um evento na trilha. Para obter mais informações, consulte Automatização de respostas com a Amazon EventBridge neste guia.
- Você pode usar o Amazon Security Lake para coletar e armazenar registros de vários Serviços da AWS, inclusive CloudTrail. Para obter mais informações, consulte Coleta de dados Serviços da AWS no Security Lake na documentação do Amazon Security Lake.
- Para aprimorar sua análise da atividade operacional, você pode consultar CloudTrail registros com o Amazon Athena. Para obter mais informações, consulte AWS CloudTrail Registros de consulta na documentação do Amazon Athena.

Para obter mais informações sobre AWS KMS as operações de monitoramento com CloudTrail, consulte o seguinte:

- Registrando chamadas de AWS KMS API com AWS CloudTrail
- Exemplos de entradas de AWS KMS registro
- Monitore as chaves KMS com a Amazon EventBridge
- CloudTrail integração com a Amazon EventBridge

Monitorando o acesso às chaves KMS com o IAM Access Analyzer

AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) ajuda você a identificar os recursos em sua organização e contas (como chaves KMS) que são compartilhados com uma entidade externa. Esse serviço pode ajudá-lo a identificar o acesso não intencional ou

excessivamente amplo aos seus recursos e dados, o que é um risco de segurança. O IAM Access Analyzer identifica recursos que são compartilhados com entidades externas usando o raciocínio baseado em lógica para analisar as políticas baseadas em recursos em seu ambiente. AWS

Você pode usar o IAM Access Analyzer para identificar quais entidades externas têm acesso às suas chaves do KMS. Ao ativar o IAM Access Analyzer, você cria um analisador para toda a organização ou para uma conta de destino. A organização ou conta escolhida é conhecida como zona de confiança do analisador. O analisador monitora os recursos suportados dentro da zona de confiança. Qualquer acesso aos recursos por parte dos diretores dentro da zona de confiança é considerado confiável.

Para chaves KMS, o IAM Access Analyzer analisa as principais políticas e concessões aplicadas a uma chave. Ele gera uma descoberta se uma política ou concessão de chave permite que uma entidade externa acesse a chave. Use o IAM Access Analyzer para determinar se entidades externas têm acesso às suas chaves do KMS e, em seguida, verifique se essas entidades devem ter acesso.

Para obter mais informações sobre como usar o IAM Access Analyzer para monitorar o acesso à chave KMS, consulte o seguinte:

- Como usar o AWS Identity and Access Management Access Analyzer
- Tipos de recursos do IAM Access Analyzer para acesso externo
- Tipos de recursos do IAM Access Analyzer: AWS KMS keys
- Conclusões para acesso externo e não utilizado

Monitorando as configurações de criptografia de outros Serviços da AWS com AWS Config

AWS Configfornece uma visão detalhada da configuração dos AWS recursos em seu Conta da AWS. Você pode usar AWS Config para verificar se aqueles Serviços da AWS que usam suas chaves KMS têm suas configurações de criptografia definidas adequadamente. Por exemplo, você pode usar a AWS Config regra de volumes criptografados para validar se seus volumes do Amazon Elastic Block Store (Amazon EBS) estão criptografados.

AWS Config inclui regras gerenciadas que ajudam você a escolher rapidamente as regras com as quais avaliar seus recursos. Verifique AWS Config se as regras gerenciadas de que você precisa são suportadas nessa região. Regiões da AWS As regras gerenciadas disponíveis incluem verificações de configuração de snapshots do Amazon Relational Database Service (Amazon RDS), criptografia

de trilhas CloudTrail , criptografia padrão para buckets do Amazon Simple Storage Service (Amazon S3), criptografia de tabelas do Amazon DynamoDB e muito mais.

Você também pode criar regras personalizadas e aplicar sua lógica de negócios para determinar se seus recursos estão em conformidade com seus requisitos. O código-fonte aberto para muitas regras gerenciadas está disponível no Repositório de AWS Config Regras em GitHub. Esses podem ser um ponto de partida útil para desenvolver suas próprias regras personalizadas.

Quando um recurso não está em conformidade com uma regra, você pode iniciar ações responsivas. AWS Config inclui ações de remediação que a AWS Systems Manager automação realiza. Por exemplo, se você aplicou a cloud-trail-encryption-enabledregra e a regra retorna um `NON_COMPLIANT` resultado, AWS Config pode iniciar um documento de automação que corrija o problema criptografando os CloudTrail registros para você.

AWS Config permite que você verifique proativamente a conformidade com AWS Config as regras antes de provisionar recursos. A aplicação de regras no modo proativo ajuda você a avaliar as configurações dos seus recursos de nuvem antes de serem criados ou atualizados. A aplicação de regras no modo proativo como parte do pipeline de implantação permite testar as configurações dos recursos antes de implantá-los.

Você também pode implementar AWS Config regras como controles por meio de AWS Security Hub CSPM. O Security Hub CSPM oferece padrões de segurança que você pode aplicar ao seu. Contas da AWS Esses padrões ajudam você a avaliar seu ambiente em relação às práticas recomendadas. O padrão AWS Foundational Security Best Practices inclui controles dentro da categoria de controle de proteção para verificar se a criptografia em repouso está configurada e se as políticas de chaves do KMS seguem as práticas recomendadas.

Para obter mais informações sobre como usar AWS Config para monitorar as configurações de criptografia em Serviços da AWS, consulte o seguinte:

- Getting started with AWS Config
- AWS Config regras gerenciadas
- Regras personalizadas do AWS Config
- Corrigindo recursos não compatíveis com AWS Config

Monitorando chaves KMS com alarmes da Amazon CloudWatch

A Amazon CloudWatch monitora seus AWS recursos e os aplicativos em que você executa AWS em tempo real. Você pode usar CloudWatch para coletar e rastrear métricas, que são variáveis que você pode medir.

A expiração do material de chave importado ou a exclusão de uma chave são eventos potencialmente catastróficos se não forem intencionais ou não forem planejados adequadamente. Recomendamos que você configure CloudWatch alarmes para alertá-lo sobre esses eventos antes que eles ocorram. Também recomendamos que você configure políticas AWS Identity and Access Management (IAM) ou políticas AWS Organizations de controle de serviço (SCPs) para evitar a exclusão de chaves importantes.

CloudWatch os alarmes ajudam você a tomar medidas corretivas, como cancelar a exclusão de chaves, ou ações de remediação, como reimportar material de chave excluído ou expirado.

Automatizando respostas com a Amazon EventBridge

Você também pode usar EventBridge a Amazon para notificá-lo sobre eventos importantes que afetam suas chaves KMS. EventBridge é um AWS service (Serviço da AWS) que fornece um fluxo quase em tempo real de eventos do sistema que descrevem mudanças nos AWS recursos. EventBridgerecebe automaticamente eventos de um CloudTrail CSPM do Security Hub. Em EventBridge, você pode criar regras que respondam aos eventos registrados por CloudTrail.

AWS KMS os eventos incluem o seguinte:

- O material da chave em uma chave KMS foi rotacionado automaticamente
- O material da chave importada em uma chave KMS expirou
- Uma chave KMS que estava programada para exclusão foi excluída

Esses eventos podem iniciar ações adicionais em seu Conta da AWS. Essas ações são diferentes dos CloudWatch alarmes descritos na seção anterior porque só podem ser acionadas após a ocorrência do evento. Por exemplo, talvez você queira excluir recursos conectados a uma chave específica após a exclusão dessa chave, ou talvez queira informar a uma equipe de conformidade ou auditoria que a chave foi excluída.

Você também pode filtrar por qualquer outro evento de API que esteja conectado CloudTrail usando EventBridge. Isso significa que, se as principais ações de API relacionadas à política forem de

interesse específico, você poderá filtrá-las. Por exemplo, você pode filtrar EventBridge a ação `PutKeyPolicy` da API. De forma mais ampla, você pode filtrar qualquer ação de API que comece com `Disable*` ou `Delete*` inicie respostas automatizadas.

Usando EventBridge, você pode monitorar (que é um controle de detetive), investigar e responder (que são controles responsivos) a eventos inesperados ou selecionados. Por exemplo, você pode alertar as equipes de segurança e realizar ações específicas se um usuário ou função do IAM for criado, quando uma chave KMS for criada ou quando uma política de chaves for alterada. Você pode criar uma regra de EventBridge evento que filtra as ações de API que você especifica e, em seguida, associar alvos à regra. Exemplos de alvos incluem AWS Lambda funções, notificações do Amazon Simple Notification Service (Amazon SNS), filas do Amazon Simple Queue Service (Amazon SQS) e muito mais. Para obter mais informações sobre o envio de eventos para destinos, consulte Objetivos de barramento de eventos na Amazon EventBridge.

Para obter mais informações sobre monitoramento AWS KMS EventBridge e automação de respostas, consulte Monitorar chaves KMS com a Amazon EventBridge na documentação. AWS KMS

Melhores práticas de gerenciamento de custos e faturamento para AWS KMS

Por meio de amplitude e profundidade, Serviços da AWS ofereça a flexibilidade de gerenciar seus custos e, ao mesmo tempo, atender aos requisitos de negócios. Esta seção aborda os preços do armazenamento de chaves em AWS Key Management Service (AWS KMS) e fornece recomendações para reduzir custos, como por meio do armazenamento de chaves em cache. Você também pode analisar o uso da chave KMS para determinar se há oportunidades adicionais para reduzir custos.

Esta seção aborda os seguintes tópicos de gerenciamento de custos e faturamento:

- AWS KMS preços para armazenamento de chaves
- Chaves de bucket do Amazon S3 com criptografia padrão
- Armazenando chaves de dados em cache usando o AWS Encryption SDK
- Alternativas ao cache de chaves e às chaves de bucket do Amazon S3
- Gerenciando os custos de registro para o uso da chave KMS

AWS KMS preços para armazenamento de chaves

Cada um AWS KMS key que você cria AWS KMS incorre em uma cobrança. A cobrança mensal é a mesma para chaves simétricas, chaves assimétricas, chaves HMAC, chaves multirregionais (cada chave primária e cada réplica de várias chaves), chaves com material de chave importado e chaves KMS com uma origem de chave de um ou de um armazenamento de chaves externo. AWS CloudHSM

Para chaves KMS que você gira automaticamente ou sob demanda, a primeira e a segunda rotação da chave adicionam uma cobrança mensal adicional (rateada por hora) no custo. Após a segunda rotação, as rotações subsequentes nesse mês não serão cobradas. Consulte os AWS KMS preços para obter as informações mais recentes sobre preços.

Você pode usar AWS Budgetspara configurar um orçamento de uso. AWS Budgets pode alertá-lo quando os gastos em sua conta excederem determinados limites. Para custos relacionados a AWS KMS, você pode criar um orçamento de uso para alertar com base nas chaves ou solicitações do KMS. Isso pode melhorar sua visibilidade dos custos de armazenamento e uso de AWS KMS chaves.

Chaves de bucket do Amazon S3 com criptografia padrão

Em alguns casos de uso, cargas de trabalho que acessam ou geram um grande número de objetos no Amazon Simple Storage Service (Amazon S3) podem gerar grandes volumes de solicitações AWS KMS, o que aumenta seus custos. A configuração das chaves de bucket do Amazon S3 pode ajudar você a reduzir custos em até 99%. Essa é uma alternativa recomendada à desativação da criptografia para ajudar a reduzir os custos associados a. AWS KMS

Armazenando chaves de dados em cache usando o AWS Encryption SDK

Ao usar o AWS Encryption SDKpara realizar a criptografia do lado do cliente, o armazenamento em cache da chave de dados pode ajudar a melhorar o desempenho do seu aplicativo, reduzir o risco de que as solicitações do seu aplicativo AWS KMS sejam limitadas e ajudar a reduzir custos. Para obter mais informações sobre como começar, consulte Como usar o cache de chaves de dados.

Alternativas ao cache de chaves e às chaves de bucket do Amazon S3

Se o armazenamento de chaves em cache não for uma opção para você devido aos seus requisitos de tratamento de dados, você também pode solicitar aumentos de AWS KMS cota usando a API Service Quotas Console de gerenciamento da AWS ou a Service Quotas API. Considere o volume de chamadas de API que você pode fazer. O número de chamadas de API que você faz é um fator significativo nos AWS KMS preços. Se você aumentar a cota da taxa de solicitação para escalar seu desempenho, o aumento do número de solicitações AWS KMS incorrerá em custos adicionais.

Gerenciando os custos de registro para o uso da chave KMS

Todas as chamadas de AWS KMS API são registradas AWS CloudTrail. Aplicativos e serviços podem gerar grandes volumes de chamadas de AWS KMS API (como para operações criptográficas, incluindo criptografia e descriptografia). Pode ser difícil revisar CloudTrail registros sem uma ferramenta que ajude você a organizar esses dados, investigar tendências e pesquisar atividades anômalas de API. O Amazon Athena fornece estruturas de dados predefinidas que podem ajudá-lo a configurar rapidamente tabelas para CloudTrail logs e começar a analisar seus dados de log. É especialmente útil para análises ad hoc ou investigações adicionais durante a resposta a incidentes.

Para obter mais informações, consulte AWS CloudTrail Registros de consultas na documentação do Athena.

Como você paga por consulta pelo Athena, você pode configurar suas mesas com antecedência, sem nenhum custo. Não há cobranças por declarações de linguagem de definição de dados. Quando você está respondendo a um incidente, isso ajuda a garantir que muitos pré-requisitos já tenham sido atendidos. Para ajudá-lo a se preparar, é uma prática recomendada escrever suas consultas depois de criar sua tabela, testá-las e garantir que elas estejam produzindo os resultados desejados. Você pode salvar suas consultas no Athena para uso futuro. Para obter mais informações sobre como começar a usar o Athena, consulte Introdução ao Amazon Athena.

Os eventos de dados fornecem visibilidade das operações que são realizadas em ou dentro de um recurso. Elas também são conhecidas como operações de plano de dados. Os exemplos incluem `PutObject` eventos do Amazon S3 ou chamadas de API de operação da função Lambda. Os eventos de dados geralmente são atividades de alto volume, e você incorre em cobranças por registrá-los. Para ajudar a controlar o volume de eventos de dados que são registrados em trilhas ou armazenamentos de dados de eventos CloudTrail, você pode otimizar seu registro para CloudTrail reduzir os custos do Amazon S3 e do Amazon S3 configurando seletores de eventos avançados para limitar quais eventos de dados devem ser registrados. AWS KMS CloudTrail Para obter mais informações, consulte Como otimizar AWS CloudTrail custos usando seletores de eventos avançados (postagem AWS no blog).

Recursos

AWS Key Management Service (AWS KMS) documentação

- AWS KMS Guia do desenvolvedor
- Referência de API do AWS KMS
- AWS KMS na AWS CLI Referência

Ferramentas

- AWS Encryption SDK

AWS Orientação prescritiva

Estratégias

- Criação de uma estratégia de criptografia para dados em repouso

Guias

- Melhores práticas e recursos de criptografia para Serviços da AWS
- AWS Arquitetura de referência de privacidade (AWS PRA)

Padrões

- Criptografe automaticamente os volumes do Amazon EBS
- Corrija automaticamente instâncias e clusters de banco de dados não criptografados do Amazon RDS
- Monitore e corrija a exclusão programada de AWS KMS keys

Colaboradores

Autoria

- Frank Phillis, arquiteto sênior de soluções especialista em GTM, AWS
- Ken Beer, diretor AWS KMS e bibliotecas criptográficas, AWS
- Michael Miller, arquiteto sênior de soluções, AWS
- Jeremy Stieglitz, gerente de produto principal, AWS
- Zach Miller, arquiteto principal de soluções, AWS
- Peter M. O'Donnell, arquiteto principal de soluções, AWS
- Patrick Palmer, arquiteto principal de soluções, AWS
- Dave Walker, arquiteto principal de soluções, AWS

Analisando

- Manigandan Shri, consultor sênior de entrega, AWS

Redação técnica

- Lilly AbouHarb, redatora técnica sênior, AWS
- Kimberly Garmoe, redatora técnica sênior, AWS

Histórico do documento

A tabela a seguir descreve alterações significativas feitas neste guia. Se desejar receber notificações sobre futuras atualizações, inscreva-se em um feed RSS.

Alteração	Descrição	Data
Publicação inicial	—	24 de março de 2025

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.